CARNEGIE MELLON UNIVERSITY

# An Analysis Of Security Incidents On The Internet 1989 - 1995

A dissertation submitted to the graduate school
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

in

Engineering and Public Policy

by

John D. Howard

Pittsburgh, Pennsylvania 15213 USA
April 7, 1997

## *Abstract*

This research analyzed trends in Internet security through an investigation of 4,299 security-related incidents on the Internet reported to the CERT® Coordination Center (CERT®/CC) from 1989 to 1995. Prior to this research, our knowledge of security problems on the Internet was limited and primarily anecdotal. This information could not be effectively used to determine what government policies and programs should be, or to determine the effectiveness of current policies and programs. This research accomplished the following: 1) development of a taxonomy for the classification of Internet attacks and incidents, 2) organization, classification, and analysis of incident records available at the CERT®/CC, and 3) development of recommendations to improve Internet security, and to gather and distribute information about Internet security.

With the exception of denial-of-service attacks, security incidents were generally found to be decreasing relative to the size of the Internet. The probability of any severe incident not being reported to the CERT®/CC was estimated to be between 0% and 4%. The probability that an incident would be reported if it was above average in terms of duration and number of sites, was around 1 out of 2.6. Estimates based on this research indicated that a typical Internet domain was involved in no more than around one incident per year, and a typical Internet host in around one incident every 45 years.

The taxonomy of computer and network attacks developed for this research was used to present a summary of the relative frequency of various methods of operation and corrective actions. This was followed by an analysis of three subgroups: 1) a case study of one site that reported all incidents, 2) 22 incidents that were identified by various measures as being the most severe in the records, and 3) denial-of-service incidents. Data from all incidents and these three subgroups were used to estimate the total Internet incident activity during the period of the research. This was followed by a critical evaluation of the utility of the taxonomy developed for this research. The analysis concludes with recommendations for Internet users, Internet suppliers, response teams, and the U.S. government.



Keywords: Internet, computer, network, computer security, hacker, public policy, taxonomy, Unix, CERT®

THIS PAGE INTENTIONALLY LEFT BLANK

## *Acknowledgments*

My thanks goes first and foremost to my family, Diane Howard, and our children, Jessica, Rachel, Luke and Nathan. They gave me their support during my studies at Carnegie Mellon University, while enduring poverty and neglect. I am indebted to them for their understanding and their encouragement.

I am indebted also to my dissertation committee. Dr. Paul S. Fischbeck was my advisor throughout my studies at CMU, and he was chairman of the committee. Thanks to him for his insight, instruction, support and patience. He has high standing among that rare breed of professors who always place their students as their first priority. Thanks also to Dr. Thomas A. Longstaff of the CERT®/CC. He introduced me to the CERT®/CC records, was instrumental in providing me a place to work, and helped me understand the records and the operation of his organization. He also provided me valuable insight which I was able to apply to the research. Thanks also to Dr. M. Granger Morgan, Department Head, Engineering and Public Policy (EPP). He supported me when I needed it, and was always a learned instructor. I also appreciate the help from Dr. Alex Hills, head of CMU Computing Services. Thanks particularly to him for teaching me about telecommunications policy. And much thanks to the entire committee for their timely insights, particularly the suggestions each of them made for adding more conclusions and recommendations. With a few questions to me, they were able to allow me to see that my research had broader and more important implications than I had initially realized.

Many thanks also to the other members of the CERT®/CC team who cheerfully responded to my many needs during the research, particularly Katherine Fithen, who acted as a liaison with Site A and carefully read the completed dissertation for accuracy and to check that all the material could be released, and Howard Lipson, who helped me with many technical questions and with the procedures and software for safeguarding the records. Thanks also to Richard Pethia, Barbara Fraser, Moira West-Brown, James Ellis, Ed DeHart, Derek Simmel, and James Stevens.

Thanks to the Engineering and Public Policy Department for their support, both intellectually and financially. Dr. Indira Nair, in particular, helped me throughout the EPP program. Thanks to her for her encouragement in applying to EPP, her advice and insight, and for reminding me of the importance of ethics in our professional and personal lives. Thanks also to my other instructors,

Dr. Benoit Morel, Dr. Michael Meyer, Dr. Mitchell Small, Dr. Mark Fichman, and Dr. Jon Peha, and the EPP staff, particularly Vicki Massimino, Patti Steranchak and Denise Murrin-Macey.

During the 1996-97 academic year, I was Visiting Professor in the Computer Science Department at the US Air Force Academy. Thanks to the members of the department for their encouragement and understanding while I completed the dissertation, and particularly to Colonel Samuel Grier, Department Head and Permanent Professor, who allowed me time for the research. Thanks also to Major Rick Mraz for his encouragement, help and insight while I struggled to conceptualize the taxonomy, to Captain Jonathan Robinson for his help on the statistics, and Lieutenant Colonel Greg White for his understanding of Information Warfare.

And finally, my warmest thanks to my fellow traveler through CMU, my friend and confidant, Dr. Karen Jenni. She provided me support and sanity that was much needed, and much relied on.

## *Table of Contents - Summary*


Abstract ..... iii

Acknowledgments ..... v

Table of Contents - Summary ..... vii

Table of Contents ..... ix

List of Figures ..... xvii

List of Tables ..... xxv

Chapter 1. Introduction ..... 1

Chapter 2. Internet Characteristics ..... 7

Chapter 3. CERT®/CC History and Policies ..... 25

Chapter 4. CERT®/CC Records ..... 33

Chapter 5. A Formal Definition of Computer Security ..... 43

Chapter 6. A Taxonomy of Computer and Network Attacks ..... 53

Chapter 7. Classification of Internet Incidents and Internet Activity ..... 75

Chapter 8. Methods of Operation and Corrective Actions ..... 95

Chapter 9. Case Study - Site A ..... 117

Chapter 10. Severe Incidents ..... 133

Chapter 11. Denial-of-Service Incidents ..... 159

Chapter 12. Estimates of Total Internet Incident Activity ..... 171

Chapter 13. The Utility of the Taxonomy of Computer and Network Attacks ..... 193

Chapter 14. Policy Implications and Recommendations ..... 205

Chapter 15. Future Research ..... 233

Chapter 16. Conclusions and Recommendations ..... 235

References ..... 243

Appendix A. Summary of Methods of Operation ..... 247

Appendix B. Summary of Corrective Actions ..... 281

Glossary ..... 287

THIS PAGE INTENTIONALLY LEFT BLANK

## *Table of Contents*

**Abstract** ..... iii

**Acknowledgments** ..... v

**Table of Contents** ..... vii

**List of Figures** ..... xvii

**List of Tables** ..... xxv

**Chapter 1. Introduction** ..... 1

1.1. A Scary Place? ..... 1

1.2. Contributions of this Research ..... 1

1.3. Recommended Actions ..... 2

1.4. Why Comprehensive Information Was Not Available on Internet Incidents ..... 4

1.5. Overview ..... 4

**Chapter 2. Internet Characteristics** ..... 7

2.1. Description and Origins of the Internet ..... 7

2.2. Internet Hosts and Domains ..... 8

*2.2.1. IP addresses* ..... 8

*2.2.2. Domain Names* ..... 9

*2.2.3. Domains* ..... 9

2.3. Domain Name System (DNS) Terminology ..... 12

2.4. Site Names ..... 14

2.5. The Internet Domain Survey ..... 15

2.6. Estimated Growth of the Internet ..... 16

2.7. Summary of Internet Characteristics ..... 21

**Chapter 3. CERT®/CC History and Policies** ..... 25

3.1. Origins of the CERT®/CC ..... 25

3.2. CERT®/CC Purpose ..... 25

3.3. Operating Procedures and Policies ..... 26

3.4. Other Incident Response and Security Teams ..... 27

3.5. Summary of CERT®/CC History and Policies ..... 28

**Chapter 4. CERT®/CC Records** ..... **33**
4.1. CERT®/CC Incident Response ..... 33
*4.1.1. Early, Informal Period – November, 1988 to January, 1992* ..... 33
*4.1.2. Transition Period – January, 1992 to September, 1993* ..... 34
*4.1.3. Formal Period – September, 1993 to December, 1995* ..... 35
4.2. CERT®/CC Record Characteristics and Methods of Analysis ..... 35
*4.2.1. Early Period Records – November, 1988 to May, 1992* ..... 36
*4.2.2. Later Period Records – May, 1992 to December, 1995* ..... 37
4.3. Data Extraction ..... 39
4.4. Summary of CERT®/CC Records ..... 41
**Chapter 5. A Formal Definition of Computer Security** ..... **43**
5.1. Simple Computer Security Definitions ..... 43
5.2. Narrowing the Definition of Computer Security ..... 44
5.3. Toward a More Formal Definition ..... 46
*5.3.1. What resources are we trying to protect?* ..... 47
*5.3.2. Against what?* ..... 48
5.4. A Formal Definition of Computer Security ..... 50
**Chapter 6. A Taxonomy of Computer and Network Attacks** ..... **53**
6.1. Characteristics of Satisfactory Taxonomies ..... 53
6.2. Toward a Taxonomy of Computer and Network Attacks ..... 53
6.3. Current Computer and Network Security Taxonomies ..... 54
*6.3.1. Lists of Terms* ..... 54
*6.3.2. Lists of Categories* ..... 55
*6.3.3. Results Categories* ..... 56
*6.3.4. Empirical Lists* ..... 56
*6.3.5. Matrices* ..... 57
*6.3.6. A Process-Based Taxonomy* ..... 60
6.4. A Taxonomy of Computer and Network Attacks ..... 61
*6.4.1. Attackers and Their Objectives* ..... 62
*6.4.2. Access* ..... 64
*6.4.3. Results* ..... 65
*6.4.4. Tools* ..... 66

*6.4.4.1 User Command* ..... 66
*6.4.4.2 Script or Program* ..... 66
*6.4.4.3 Autonomous Agent* ..... 67
*6.4.4.4 Toolkit* ..... 67
*6.4.4.5 Distributed Tool* ..... 68
*6.4.4.6 Data Tap* ..... 68
*6.4.5. The Complete Taxonomy of Computer and Network Attacks* ..... 69
6.5. Summary of the Taxonomy of Computer and Network Attacks ..... 70
**Chapter 7. Classification of Internet Incidents and Internet Activity ..... 75**
7.1. Number of CERT®/CC Incidents ..... 75
7.2. Classification of Incidents ..... 77
*7.2.1. False Alarms* ..... 78
*7.2.2. Unauthorized Access Incidents* ..... 79
*7.2.3. Unauthorized Use Incidents* ..... 83
*7.2.4. Inadequacies of this Classification* ..... 88
7.3. Alternate Measures of Severity ..... 88
7.4. Sites per Day Recorded in the CERT®/CC Incidents ..... 89
7.5. Summary of the Classification of Internet Incidents and Internet Activity ..... 93
**Chapter 8. Methods of Operation and Corrective Actions ..... 95**
8.1. Methods of Operation ..... 95
*8.1.1. Attackers* ..... 96
*8.1.2. Tools* ..... 97
*8.1.3. Access* ..... 99
*8.1.3.1 Password Vulnerabilities* ..... 100
*8.1.3.2 SMTP* ..... 101
*8.1.3.3 Mail* ..... 102
*8.1.3.4 Trusted hosts* ..... 102
*8.1.3.5 Configuration* ..... 102
*8.1.3.6 TFTP* ..... 102
*8.1.3.7 NIS* ..... 103
*8.1.3.8 FTP* ..... 103
*8.1.3.9 NFS* ..... 104

*8.1.3.10 Other vulnerabilities* ..... 104
*8.1.3.11. Types of Accounts* ..... 104
*8.1.4. Results* ..... 105
*8.1.5. Objectives* ..... 106
*8.1.6. Summary of Methods of Operation* ..... 106
8.2. Corrective Actions ..... 110
*8.2.1. Internal Actions* ..... 111
*8.2.2. External Actions* ..... 111
8.3. Some Things the CERT®/CC Incidents Do Not Include ..... 112
8.4. Summary of Methods of Operation and Corrective Actions ..... 113
**Chapter 9. Case Study - Site A** ..... **117**
9.1. Description of Site A ..... 117
9.2. Site A Reporting Criteria ..... 118
9.3. Classification of Site A Incidents ..... 118
*9.3.1. False Alarms* ..... 118
*9.3.2. Unauthorized Access Incidents at Site A* ..... 120
*9.3.3. Unauthorized Use Incidents at Site A* ..... 123
9.4. Sites per Day ..... 127
9.5. Summary of Case Study - Site A ..... 131
**Chapter 10. Severe Incidents** ..... **133**
10.1. Selection of the Severe Incidents ..... 133
10.2. Description of the Severe Incidents Chosen ..... 138
*10.2.1. Incident #1 - Dutch Hackers* ..... 140
*10.2.2. Incident #9 - Danish Hackers* ..... 144
*10.2.3. Incidents #2, 3, 4, and 8 - Other Command Line Incidents* ..... 145
*10.2.4. Incident #5 - FTP Abuse and Software Piracy* ..... 147
*10.2.5. Incident #7 - TFTP Attacks* ..... 147
*10.2.6. Incidents #6, 10, 11, 12, 13, 14, 17 - Sniffer Attacks* ..... 148
*10.2.7. Incident #15, 18, 19, 21, 22 - Toolkit and Sniffer Attacks* ..... 151
*10.2.8. Incident #16 - Toolkit, Sniffer and IRC* ..... 154
*10.2.9. Incident #20 - IP Spoofing* ..... 155
10.3. Summary of Severe Incidents ..... 157

**Chapter 11. Denial-of-Service Incidents** ..... **159**
11.1. Denial-of-service Definition and Types ..... 159
*11.1.1 Destruction* ..... 161
*11.1.2 Process Degradation* ..... 162
*11.1.3 Storage Degradation* ..... 163
*11.1.4. Shutdowns* ..... 164
11.2. History of Internet Denial-of-Service Attacks ..... 165
*11.2.1. Numbers of Attacks* ..... 165
*11.2.2. Methods of Attack* ..... 167
*11.2.3. Additional Denial-of-service Attack Characteristics* ..... 169
11.3. Summary of Denial-of-Service Incidents ..... 170

**Chapter 12. Estimates of Total Internet Incident Activity** ..... **171**
12.1. Relationship of Attacks, Incidents and Total Activity ..... 171
12.2. Estimates of Total Internet Attack Activity ..... 172
*12.2.1. Monitoring Sites For Attack Activity* ..... 172
*12.2.2. Reports of Attack Activity From Representative Sites* ..... 172
*12.2.3. Vulnerability Studies* ..... 173
*12.2.3.1. DISA Vulnerability Studies* ..... 174
*12.2.3.2. AFIWC Security Posture Studies* ..... 175
12.3. Estimates of Total Internet Incident Activity ..... 177
*12.3.1. Monitoring Sites For Incident Activity* ..... 178
*12.3.2. Reports of Incident Activity From Representative Sites* ..... 178
*12.3.3. Estimates of Attack Reporting Rate and Attacks per Incident* ..... 181
*12.3.3.1. Estimates of Attack Reporting Rate* ..... 182
*12.3.3.2. Estimates of Attacks per Incident Using All CERT®/CC Incident* ..... 182
*12.3.3.3. Estimates of Attacks per Incident Using CERT®/CC Incidents by Type* ..... 185
*12.3.4. Summary of Incident Estimates* ..... 189
12.4. Severe and Above Average Incidents ..... 189
12.5. Estimated Number of Internet Denial-of-service Incidents ..... 190
12.6. Summary of the Estimates of Total Internet Incident Activity ..... 190

**Chapter 13. The Utility of the Taxonomy of Computer and Network Attacks ..... 193**
13.1. Review of the Characteristics of Satisfactory Taxonomies ..... 193
13.2. Evaluation of the taxonomy relative to the taxonomy criteria ..... 193
*13.2.1. Categories that are Mutually Exclusive* ..... 194
*13.2.2. Categories that are Exhaustive* ..... 195
*13.2.3. Categories that are Unambiguous* ..... 196
*13.2.4. Categories that are Repeatable* ..... 197
*13.2.5. Categories that are Accepted* ..... 197
*13.2.6. Categories that are Useful* ..... 198
13.3. Classifications of Incidents ..... 198
*13.3.1 Classifications at the CERT®/CC during the period of research* ..... 199
*13.3.2. Classification of Incidents for this Research* ..... 200
*13.3.3. Recommended Process for Classifying Incidents* ..... 201
*13.3.3.1. Determining Incident Scope* ..... 201
*13.3.3.2. Determining Incident Characteristics* ..... 201
*13.3.3.3. Classification of Incidents* ..... 202
13.4. Summary of the Utility of the Taxonomy of Computer and Network Attacks .... 203

**Chapter 14. Policy Implications and Recommendations ..... 205**
14.1. General Implications of This Research ..... 205
14.2. Implications for Internet Users ..... 208
*14.2.1. Basic Precautions All Users Should Take to Protect Files* ..... 209
*14.2.2. Advanced Precautions to Protect Files* ..... 211
*14.2.3. Precautions to Protect Data in Transit* ..... 211
*14.2.4. Additional Considerations for Commercial Internet Users* ..... 212
*14.2.5. Summary of the Implications for Internet Users* ..... 212
14.3. Implications for Internet Suppliers ..... 213
*14.3.1. Password Problems* ..... 213
*14.3.2. Shipping Software in an Insecure State* ..... 213
*14.3.3. Additional Actions Suppliers Should Take* ..... 214
*14.3.4. Summary of Implications for Suppliers* ..... 214

14.4. Implications for the Government ..... 214
*14.4.1. The Government's Role in Providing Information* ..... 215
*14.4.2. Government Information Policies and the Computer Security Market* ..... 216
*14.4.3. Funding of Incident Response Supported by This Research* ..... 216
*14.4.4. Other Government Policies Supported by This Research* ..... 219
14.5. Implications for Response Teams ..... 219
*14.5.1. Objectives of Incident Response* ..... 219
*14.5.2. Possible Alternative Courses of Action* ..... 220
*14.5.2.1. Disclosure of Site Names* ..... 221
*14.5.2.1.1. Alternative 1.1 - Full Disclosure of Site Names* ..... 221
*14.5.2.1.2. Alternative 1.2 - Partial Disclosure of Site Names* ..... 222
*14.5.2.1.3. Alternative 1.3 - Delayed Disclosure of Site Names* ..... 222
*14.5.2.1.4. Alternative 1.4 - No Disclosure of Site Names* ..... 223
*14.5.2.1.5. Recommended Alternative for the Disclosure of Site Names* ..... 223
*14.5.2.2. Disclosure of Incident Activity* ..... 223
*14.5.2.2.1. Alternative 2.1 - Disclosure of CERT® Summaries* ..... 224
*14.5.2.2.2. Alternative 2.2 - Creation and Disclosure of Incident Files* ..... 224
*14.5.2.2.3. Alternative 2.3 - Development and Disclosure of Incident Data based on Incident Summaries* ..... 225
*14.5.2.2.4. Alternative 2.4 - Development and Disclosure of Incident Data based on a Taxonomy* ..... 225
*14.5.2.2.5. Alternative 2.5 - Limited Disclosure of Incident Activity* ..... 226
*14.5.2.2.6. Recommended Alternative for the Disclosure of Incident Activity* ..... 226
*14.5.2.3. Disclosure of Vulnerabilities* ..... 227
*14.5.3. Other Implications for Response Teams* ..... 228
14.6. Implications for the CERT®/CC ..... 228
14.7. Summary of Policy Implications and Recommendations ..... 229

**Chapter 15. Future Research ..... 233**

**Chapter 16. Conclusions and Recommendations ..... 235**
16.1. Contributions of this Research ..... 235
16.2. A Taxonomy of Computer and Network Attacks ..... 235
16.3. Classification of Internet Incidents and Internet Activity ..... 235

16.4. Tools and Vulnerabilities ..... 236
16.5. Severe Incidents ..... 237
16.6. Denial-of-Service Incidents ..... 237
16.7. Estimates of Total Internet Incident Activity ..... 238
16.8. Policy Implications and Recommendations ..... 238
16.9. Future Research ..... 241

**References** ..... **243**

**Appendix A. Summary of Methods of Operation** ..... **247**

**Appendix B. Summary of Corrective Actions** ..... **281**

**Glossary** ..... **287**

## *List of Figures*

**Chapter 2**


Figure 2.1. Typical Internet Domain Name Tree ..... 12
Figure 2.2. Growth in Internet Hosts ..... 16
Figure 2.3. Projected Internet Growth ..... 17
Figure 2.4. Growth of Top-Level Domains with Predominantly U.S. Hosts ..... 17
Figure 2.5. Growth of Top-Level Domains with Predominantly U.S. Hosts ..... 18
Figure 2.6. Top-Level Domains as a Percentage of the Internet ..... 19
Figure 2.7. Growth in DNS domains ..... 19
Figure 2.8. Trends in Internet Hosts per DNS domain ..... 20
Figure 2.9. Growth of the World Wide Web ..... 21


**Chapter 6**


Figure 6.1. Example Two-Dimensional Attack Matrix ..... 57
Figure 6.2. Security flaw taxonomy: Flaws by Genesis ..... 59
Figure 6.3. Security Attacks ..... 61
Figure 6.4. Operational Sequence of Computer and Network Attack ..... 61
Figure 6.5. Attackers and their Primary Motivations ..... 63
Figure 6.6. Access for Attack ..... 64
Figure 6.7. Results of Attack ..... 65
Figure 6.8. Tools of Attack ..... 66
Figure 6.9. Complete Computer and Network Attack Taxonomy ..... 73


**Chapter 7**


Figure 7.1. CERT®/CC Incidents per Year ..... 76
Figure 7.2. CERT®/CC Incidents by Month, 1989 - 1995 ..... 76
Figure 7.3. CERT®/CC Incidents and False Alarms per Year ..... 78
Figure 7.4. False Alarms as a Percentage of CERT®/CC Incidents ..... 79
Figure 7.5. Access for Attack ..... 79
Figure 7.6. CERT®/CC Access Incidents by Month Averaged Over Quarters ..... 80
Figure 7.7. CERT®/CC Access Incidents per 100,000 domains by Month Averaged Over Quarters ..... 81
Figure 7.8. CERT®/CC Access Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 81

Figure 7.9. CERT®/CC Successful Access Incidents by Month Averaged Over Quarters ..... 82
Figure 7.10. CERT®/CC Successful Access Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 83
Figure 7.11. CERT®/CC Total Unauthorized Use Incidents by Month Averaged Over Quarters ..... 85
Figure 7.12. CERT®/CC Abuse Incidents by Month Averaged Over Quarters ..... 85
Figure 7.13. CERT®/CC Total Unauthorized Use Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 86
Figure 7.14. CERT®/CC Abuse Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 86
Figure 7.15. CERT®/CC Denial-of-service Incidents by Month Averaged Over Quarters ..... 87
Figure 7.16. CERT®/CC Denial-of-service Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 87
Figure 7.17. CERT®/CC Spoofing Incidents by Month Averaged Over Quarters ..... 88
Figure 7.18. CERT®/CC Spoofing Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 88
Figure 7.19. CERT®/CC Sites per Day - All Incidents ..... 89
Figure 7.20. CERT®/CC Sites per Day - All Incidents, Averaged Over Months ..... 90
Figure 7.21. CERT®/CC Sites per Day - All Incidents, Averaged Over Quarters ..... 90
Figure 7.22. CERT®/CC Sites per Day - Root and Account Break-ins, Averaged Over Months ..... 91
Figure 7.23. CERT®/CC Sites per Day - Root and Account Break-ins, Averaged Over Quarters ..... 91
Figure 7.24. CERT®/CC Sites per Day per 10,000,000 Hosts - All Incidents, Averaged Over Quarters ..... 92
Figure 7.25. CERT®/CC Sites per Day per 10,000,000 Hosts - Root and Account Break-ins, Averaged Over Quarters ..... 92

**Chapter 8**

Figure 8.1. Range and Mean Incident Reporting Dates for Methods of Operation - Attackers ..... 96
Figure 8.2. Range and Mean Incident Reporting Dates for Methods of Operation - Tools ..... 98
Figure 8.3. Range and Mean Incident Reporting Dates for Methods of Operation - Access - Part 1 ..... 100

Figure 8.4. Range and Mean Incident Reporting Dates for Methods of Operation - Access - Part 2 ..... 101
Figure 8.5. Range and Mean Incident Reporting Dates for Methods of Operation - Access - Part 3 ..... 103
Figure 8.6. Range and Mean Incident Reporting Dates for Methods of Operation - Access - Part 4 ..... 104
Figure 8.7. Range and Mean Incident Start for Methods of Operation - Access - Type of Account ..... 105
Figure 8.8. Range and Mean Incident Reporting Dates for Methods of Operation - Results ..... 106
Figure 8.9. Range and Mean Incident Reporting Dates for Methods of Operation - Objectives ..... 107
Figure 8.10. Range and Mean Incident Reporting Dates for Corrective Actions ..... 110

**Chapter 9**

Figure 9.1. Site A Incidents and False Alarms per Year ..... 118
Figure 9.2. False Alarms as a Percentage of Site A Incidents ..... 119
Figure 9.3. Site A Incidents per Month (with and without false alarms) ..... 119
Figure 9.4. Site A Access Incidents by Month Averaged Over Quarters ..... 120
Figure 9.5. Site A Access Incidents per 100,000 domains by Month Averaged Over Quarters ..... 121
Figure 9.6. Site A Access Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 121
Figure 9.7. Site A Successful Access Incidents by Month Averaged Over Quarters ..... 122
Figure 9.8. Site A Successful Access Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 123
Figure 9.9. Site A Total Unauthorized Use Incidents by Month Averaged Over Quarters ..... 124
Figure 9.10. Site A Total Unauthorized Use Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 124
Figure 9.11. Site A Abuse Incidents by Month Averaged Over Quarters ..... 125
Figure 9.12. Site A Abuse Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 125
Figure 9.13. Site A Denial-of-service Incidents by Month Averaged Over Quarters ..... 126
Figure 9.14. Site A Denial-of-service Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 126
Figure 9.15. Site A Spoofing Incidents by Month Averaged Over Quarters ..... 126

Figure 9.16. Site A Spoofing Incidents per 10,000,000 Hosts by Month Averaged Over Quarters ..... 127
Figure 9.17. Site A Sites per Day - All Incidents ..... 127
Figure 9.18. Site A Sites per Day - All Incidents, Averaged Over Months ..... 128
Figure 9.19. Site A Sites per Day - All Incidents, Averaged Over Quarters ..... 128
Figure 9.20. Site A Sites per Day per 10,000,000 Hosts - All Incidents, Averaged Over Quarters ..... 129
Figure 9.21. Site A Sites per Day - Root and Account Break-ins, Averaged Over Months ..... 129
Figure 9.22. Site A Sites per Day - Root and Account Break-ins, Averaged Over Quarters ..... 130
Figure 9.23. Site A Sites per Day per 10,000,000 Hosts - Root and Account Break-ins, Averaged Over Quarters ..... 130

**Chapter 10**

Figure 10.1. Number of Sites versus Number of Incidents ..... 134
Figure 10.2. Number of Sites versus Number of Incidents (Less than 200 sites and less than 500 Incidents) ..... 134
Figure 10.3. Incident Duration versus Number of Incidents ..... 135
Figure 10.4. Incident Duration versus Number of Incidents (200 or Less Days and less than 1000 Incidents) ..... 135
Figure 10.5. Number of Messages versus Number of Incidents ..... 136
Figure 10.6. Number of Messages versus Number of Incidents (Less than 200 messages and less than 500 Incidents) ..... 136
Figure 10.7. Distribution of Root Break-in Incidents With ≥ 79 Days Duration, ≥ 62 Sites, ≥ 87 Messages ..... 138
Figure 10.8. Sites per Day versus Duration for 22 "Severe" Incidents ..... 139

**Chapter 11**

Figure 11.1. Denial-of-Service Attack Methods ..... 160
Figure 11.2. Internet Protocol Layering Compared to Network Process Categories ..... 162
Figure 11.3. Sites per Day Involved in Denial-of-service Attacks, Averaged Over Each Quarter, as Recorded in CERT®/CC Records ..... 165
Figure 11.4. Sites per Day Involved in Denial-of-service Attacks, per 100,000 Internet Domains Averaged Over Each Quarter, as Recorded in CERT®/CC Records ..... 166

Figure 11.5. Sites per Day Involved in Denial-of-service Attacks, per 10,000,000 Internet Hosts Averaged Over Each Quarter, as Recorded in CERT®/CC Records ..... 166

Figure 11.6. Denial-of-service Attacks by Method, as Recorded in CERT®/CC Records ..... 167

Figure 11.7. Primary Category of Denial-of-service Attacks, as Recorded in CERT®/CC Records ..... 168

**Chapter 12**

Figure 12.1. Results of DISA Vulnerability Assessments, 1992 - 1995 ..... 174

Figure 12.2. On-Line Survey Results from 1,248 Hosts at 15 USAF Bases, Air Force Information Warfare Center, Jan 95 ..... 175

Figure 12.3. Estimates of the Number of Incidents per Host at Site A ..... 178

Figure 12.4. Estimates of the Number of Internet Incidents based on Site A Data ..... 179

Figure 12.5. Average Sites per Incident by Year ..... 182

**Appendix A**

Figure A.1. Range and Mean Incident Start for Methods of Operation - Attackers ..... 259

Figure A.2. Range and Mean Incident Start for Methods of Operation - Tools - Part 1 ... 259

Figure A.3. Range and Mean Incident Start for Methods of Operation - Tools - Part 2 ... 260

Figure A.4. Range and Mean Incident Start for Methods of Operation - Tools - Part 3 ... 260

Figure A.5. Range and Mean Incident Start for Methods of Operation - Tools - Part 4 ... 261

Figure A.6. Range and Mean Incident Start for Methods of Operation - Tools - Part 5 ... 261

Figure A.7. Range and Mean Incident Start for Methods of Operation - Tools - Part 6 ... 262

Figure A.8. Range and Mean Incident Start for Methods of Operation - Tools - Part 7 ... 262

Figure A.9. Range and Mean Incident Start for Methods of Operation - Access - Part 1... 263

Figure A.10. Range and Mean Incident Start for Methods of Operation - Access - Part 2.. 263

Figure A.11. Range and Mean Incident Start for Methods of Operation - Access - Part 3.. 264

Figure A.12. Range and Mean Incident Start for Methods of Operation - Access - Part 4.. 264

Figure A.13. Range and Mean Incident Start for Methods of Operation - Access - Part 5.. 265

Figure A.14. Range and Mean Incident Start for Methods of Operation - Access - Part 6.. 265

Figure A.15. Range and Mean Incident Start for Methods of Operation - Access - Part 7.. 266

Figure A.16. Range and Mean Incident Start for Methods of Operation - Access - Part 8.. 266

Figure A.17. Range and Mean Incident Start for Methods of Operation - Access - Part 9.. 267

Figure A.18. Range and Mean Incident Start for Methods of Operation - Access - Part 10.. 267

Figure A.19. Range and Mean Incident Start for Methods of Operation - Access - Part 11. . 268
Figure A.20. Range and Mean Incident Start for Methods of Operation - Access - Part 12. . 268
Figure A.21. Range and Mean Incident Start for Methods of Operation - Access - Part 13. . 269
Figure A.22. Range and Mean Incident Start for Methods of Operation - Access - Part 14. . 269
Figure A.23. Range and Mean Incident Start for Methods of Operation - Access - Part 15. . 270
Figure A.24. Range and Mean Incident Start for Methods of Operation - Access - Part 16. . 270
Figure A.25. Range and Mean Incident Start for Methods of Operation - Access - Part 17. . 271
Figure A.26. Range and Mean Incident Start for Methods of Operation - Access - Part 18. . 271
Figure A.27. Range and Mean Incident Start for Methods of Operation - Access - Part 19. . 272
Figure A.28. Range and Mean Incident Start for Methods of Operation - Access - Part 20. . 272
Figure A.29. Range and Mean Incident Start for Methods of Operation - Access - Part 21. . 273
Figure A.30. Range and Mean Incident Start for Methods of Operation - Access - Part 22. . 273
Figure A.31. Range and Mean Incident Start for Methods of Operation - Access - Part 23. . 274
Figure A.32. Range and Mean Incident Start for Methods of Operation - Access - Part 24. . 274
Figure A.33. Range and Mean Incident Start for Methods of Operation - Access - Part 25. . 275
Figure A.34. Range and Mean Incident Start for Methods of Operation - Access - Part 26. . 275
Figure A.35. Range and Mean Incident Start for Methods of Operation - Access - Part 27. . 276
Figure A.36. Range and Mean Incident Start for Methods of Operation - Access - Part 28. . 276
Figure A.37. Range and Mean Incident Start for Methods of Operation - Access - Part 29. . 277
Figure A.38. Range and Mean Incident Start for Methods of Operation - Results - Part 1. . 277
Figure A.39. Range and Mean Incident Start for Methods of Operation - Results - Part 2. . 278
Figure A.40. Range and Mean Incident Start for Methods of Operation - Results - Part 3. . 278
Figure A.41. Range and Mean Incident Start for Methods of Operation - Objectives .... 279

**Appendix B**

Figure B.1. Range and Mean Incident Reporting Dates for Corrective Actions - Restrict System Hardware/Software ..... 283
Figure B.2. Range and Mean Incident Reporting Dates for Corrective Actions - Configure System Hardware/Software ..... 283
Figure B.3. Range and Mean Incident Reporting Dates for Corrective Actions - Upgrade System Hardware/Software ..... 284
Figure B.4. Range and Mean Incident Reporting Dates for Corrective Actions - Preventive Measures ..... 284

Figure B.5. Range and Mean Incident Reporting Dates for Corrective Actions - Take Action Against Intruder ..... 285
Figure B.6. Range and Mean Incident Reporting Dates for Corrective Actions - Law Enforcement ..... 285

THIS PAGE INTENTIONALLY LEFT BLANK

## *List of Tables*

**Chapter 2**

Table 2.1. Internet Network Classes ..... 9

Table 2.2. Summary of */etc/hosts* file at Carnegie Mellon University, September 7, 1996 ... 11

Table 2.3. Linear Regression Slopes of Growth Rates of Top-Level Internet Domains ... 18

Table 2.4. Growth of the World Wide Web ..... 21

Table 2.5. Summary of Internet Growth Rates Over Six-Month Intervals ..... 23

**Chapter 3**

Table 3.1. Internet and Other Network Response Teams in FIRST, and their Constituencies ..... 29

Table 3.2. Other U.S. Government Agency Response Teams in FIRST, and their Constituencies ..... 29

Table 3.3. U.S. Military Response Teams in FIRST, and their Constituencies ..... 30

Table 3.4. U.S. Educational Response Teams in FIRST, with Constituencies ..... 30

Table 3.5. Foreign Government Response Teams in FIRST, with Constituencies ..... 30

Table 3.6. Computer and Communications Vendor Response Teams in FIRST, with Constituencies ..... 31

Table 3.7. Other Commercial Response Teams in FIRST, with Constituencies ..... 31

**Chapter 5**

Table 5.1 Example Attacks ..... 49

**Chapter 8**

Table 8.1. Methods of Operation ..... 107

Table 8.2. Corrective Actions ..... 112

**Chapter 9**

Table 9.1. Estimated Number of Hosts at Site A ..... 117

Table 9.2. Access Incidents at Site A ..... 120

Table 9.3. Unauthorized Use Incidents at Site A ..... 123

**Chapter 10**

Table 10.1. Mean and Standard Deviations of Measurements ..... 137

Table 10.2. Summary of Root Break-in Incidents With ≥ 79 Days Duration, ≥ 62 Sites, ≥ 87 Messages ..... 138

Table 10.3. Reporting and Other Sites for Severe Incident Number 1 ..... 141

Table 10.4. Reporting and Other Sites for Severe Incident Number 9 ..... 144

Table 10.5. Reporting and Other Sites for Severe Incident Number 2. . . . . 145
Table 10.6. Reporting and Other Sites for Severe Incident Number 3. . . . . 145
Table 10.7. Reporting and Other Sites for Severe Incident Number 4. . . . . 146
Table 10.8. Reporting and Other Sites for Severe Incident Number 8. . . . . 146
Table 10.9. Reporting and Other Sites for Severe Incident Number 5. . . . . 147
Table 10.10. Reporting and Other Sites for Severe Incident Number 7. . . . . 148
Table 10.11. Reporting and Other Sites for Severe Incident Number 6. . . . . 148
Table 10.12. Reporting and Other Sites for Severe Incident Number 10. . . . . 149
Table 10.13. Reporting and Other Sites for Severe Incident Number 11. . . . . 149
Table 10.14. Reporting and Other Sites for Severe Incident Number 12. . . . . 150
Table 10.15. Reporting and Other Sites for Severe Incident Number 13. . . . . 150
Table 10.16. Reporting and Other Sites for Severe Incident Number 14. . . . . 151
Table 10.17. Reporting and Other Sites for Severe Incident Number 17. . . . . 151
Table 10.18. Reporting and Other Sites for Severe Incident Number 15. . . . . 152
Table 10.19. Reporting and Other Sites for Severe Incident Number 18. . . . . 152
Table 10.20. Reporting and Other Sites for Severe Incident Number 19. . . . . 153
Table 10.21. Reporting and Other Sites for Severe Incident Number 21. . . . . 153
Table 10.22. Reporting and Other Sites for Severe Incident Number 22. . . . . 154
Table 10.23. Reporting and Other Sites for Severe Incident Number 16. . . . . 155
Table 10.24. Reporting and Other Sites for Severe Incident Number 20. . . . . 156

**Chapter 12**

Table 12.1. Estimates of Total Internet Attacks per Year in 1995 . . . . . 177
Table 12.2. Estimate of the Ratio of Total Internet Incidents to Reported Incidents . . . . . 179
Table 12.3. All CERT®/CC Incidents Compared To Incidents at Site A . . . . . 180
Table 12.4. Estimate of Incident Reporting Rates from Site A Data, Assuming All Root Break-ins Reported . . . . . 181
Table 12.5. Example Weighted Estimates of Attacks per Incident . . . . . 184
Table 12.6. Assumed Values for an Estimate of the Number of Attacks for Each CERT®/CC Incident . . . . . 185
Table 12.7. Estimate Average Attacks/Incident Derived From Each CERT®/CC Incident Using Assumed Parameters . . . . . 186
Table 12.8. Adjustments to the Probability of Report, Based on Site A Information . . . . . 186

Table 12.9. Estimates of the Average Percentage of Report of an Incident and the Total Number of Internet Incidents Based on an AFWIC Estimated Average Probability of Report of Attack ..... 187

Table 12.10. Estimates of the Average Probability of Report of an Incident Based on an AFWIC Estimated Average Probability of Report of Attack ..... 187

Table 12.11. Estimates of the Average Percentage of Report of an Incident and the Total Number of Internet Incidents Based on an DISA Estimated Average Probability of Report of Attack ..... 188

Table 12.12. Estimates of the Average Probability of Report of an Incident Based on an DISA Estimated Average Probability of Report of Attack ..... 188

Table 12.13. Summary of Estimates of Total Internet Incident Activity ..... 189

Table 12.14. Estimates of the Probability of Incident Report, Rate of Incident Reports, and Total Internet incidents for Incidents with Above Average Duration and Number of Sites ..... 189

Table 12.15. Estimates of Total Internet Attacks per Year in 1995 ..... 191

Table 12.16. Summary of Estimates of Total Internet Incident Activity ..... 192

**Chapter 14**

Table 14.1. Estimated Rate that an Internet Domain or Host was Involved in an Incident in 1995 ..... 206

Table 14.2. Comparison of Estimated Rates That Risks Occur ..... 208

Table 14.3. Estimated Rate that an Internet Domain or Host was Involved in an Incident in 1995 ..... 230

**Chapter 16**

Table 16.1. Summary of Estimates of Total Internet Incident Activity ..... 238

Table 16.2. Estimated Rate that an Internet Domain or Host was Involved in an Incident in 1995 ..... 239

Table 16.3. Comparison of Estimated Rates That Risks Occur ..... 239

**Appendix A**

Table A.1. Methods of Operation ..... 248

**Appendix B**

Table B.1. Corrective Actions ..... 282

THIS PAGE INTENTIONALLY LEFT BLANK

*Chapter 1*

# Introduction

> . . . despite our greater reliance on network computing, the Internet isn't a safer place today than it was in 1991. If anything, the Internet is quickly becoming the Wild West of cyberspace. Although academics and industry leaders have long known about fundamental vulnerabilities of computers connected to the Internet, these flaws have been accommodated rather than corrected. As a result, we have seen many cases within the past few years of wide-scale security infractions throughout the network.
>
> Simson Garfinkel and Gene Spafford in *Practical UNIX & Internet Security* [GaS96:xiii]

> At one point, if not already, you will be the victim of Information Warfare. If not you, then a member of your family or a close friend. Your company will become a designated target of Information Warfare. If not yesterday or today, then definitely tomorrow. You will be hit.
>
> Winn Schwartau in *Information Warfare: Chaos on the Electronic Superhighway* [Sch94:11]

## 1.1. A Scary Place?

The Internet is a scary place. At least that's what we've been told by numerous authors -- scholars and sensationalists alike. In the Spring of 1994, I visited with Richard Pethia and Tom Longstaff at the CERT® Coordination Center (CERT®/CC[1]), Carnegie Mellon University (CMU). As part of my growing interest in the Internet and Information Warfare, I was in search of some information on just what had been happening on the Internet in terms of security. It was a fortuitous meeting – not because they were able to answer my question, but because they wanted to know the answer to that question also.

Security *is* a problem on the Internet. The thousands of successful break-ins over the years are a testimony to that. But just how much of a problem is it? The answer to this question is important for two reasons. First, with information about Internet security problems, we could determine to what extent, and in what areas, government programs and policies should be instituted to devote society's resources to protecting the Internet. Second, trends over time could be used to determine the effectiveness of these policies and resources.

## 1.2. Contributions of this Research

Prior to this research, our knowledge of security problems on the Internet was incomplete and primarily anecdotal. Despite our increasing reliance on the computer networks, there had been no

[1] CERT® is a registered trade mark of Carnegie Mellon University. The original name of the CERT® Coordination Center was the Computer Emergency Response Team Coordination Center.

systematic and coordinated program for gathering and distributing information about Internet security incidents. As a result, the limited information available could not be effectively used to determine either what government policies and programs should be, or the effectiveness of current policies and programs. This research brings us toward improved Internet security through:

1) development of a taxonomy for the classification of Internet attacks and Internet incidents
2) organization, classification (using the taxonomy), and analysis of the records available at the CERT®/CC concerning Internet security incidents
3) development of recommendations to improve Internet security and to gather and distribute useful information concerning Internet security

### 1.3. Recommended Actions

The following actions were recommended based on this research:

**Recommendations for all Internet users are as follows:**

1. Back up important files.
2. Use a good password for network access controls.
3. Ensure permissions are set properly on files that can be accessed by others.
4. Encrypt, or store off-line, files that are particularly sensitive.
5. Do not send sensitive user identifications, such as a social security number, address, phone number, personal data, or credit card number across the Internet unless it is encrypted at the source (prior to being sent across the Internet).
6. Use an encryption program, such as Pretty Good Privacy (PGP), if you want e-mail to be private.

**An additional recommendation for commercial Internet users is as follows:**

7. Conduct some form of risk analysis to determine the cost effective level of security.

**Recommendations for Internet suppliers are as follows:**

1. Provide protocols and software that encrypt user name, password and IP address combinations at the source, or provide an alternative to system that does not require passwords to be sent in the clear across the Internet.
2. Provide protocols and software that prevent access to files of encrypted passwords, or provide an alternative system that does not require encrypted passwords to be stored in files on systems accessible across the Internet.
3. Deliver systems to customers in a secure state.
4. Develop protocols and programs with reasonable protections against denial-of-service attacks.
5. Accelerate development of protocols and programs that provide reasonable privacy for such user programs as e-mail.

**Recommendations for the U.S. government are as follows:**

1. Increase funding for incident response, particularly the CERT®/CC.
2. Encourage Internet users to take simple security precautions.
3. Encourage Internet suppliers to improve Internet security.
4. Require government employees to take reasonable security precautions to protect sensitive data.

**Recommendations for Internet response teams are as follows:**

1. Do not disclose sites names reported to response teams (the status quo).
2. Disclose incident data based on a taxonomy.
3. Reexamine policies on the release of vulnerability information with the objective of seeing the degree to which more disclosure would benefit the Internet community.
4. Evaluate the taxonomy for computer and network attacks developed for this research.

**Recommendations for the CERT®/CC are as follows:**

1. Maintain only one internal incident summary for each incident, open or closed.
2. Record a standard set of keywords and phrases that are defined, systematic and consistent, in each summary, such as reporting date, starting date, ending date, number of reporting sites, reporting sites, number of other sites, other sites, number of messages, attackers, tools, vulnerabilities, level, results, objectives, and corrective actions.
3. Classify each incident according to the worst level of unauthorized access or use.
4. Post the data set used in this research on line at www.cert.org.
5. Evaluate the taxonomy for computer and network attacks developed for this research.
6. Develop and implement a program to better estimate total Internet incident activity. Such a program should involve the voluntary reporting of all incident activity at representative Internet sites. This program should include coordination and/or participation from other response teams and related organizations, such as DISA and AFIWC.
7. Estimate average number of attackers per incident, and their typical activity, in cooperation with personnel from DISA, AFIWC, and other response teams, in order to improve estimates of total Internet incident activity.
8. Do not disclose sites names that appear in the CERT®/CC records or are otherwise reported to the CERT®/CC (this is the status quo).
9. Disclose incident data based on a taxonomy. Suggested steps are as follows:
    1. *Methodology development at the CERT®/CC*
    2. *Trial implementation at the CERT®/CC*
    3. *Methodology development with other response teams*
    4. *Trial implementation at other response teams*
    5. *Public release and formalization*

10. Reexamine policies toward the release of vulnerability information with the objective of seeing the degree to which more disclosure would benefit the Internet community.

### 1.4. Why Comprehensive Information Was Not Available on Internet Incidents

While CERT®/CC personnel were exposed to numerous incidents during the period of time studied in this research, their perspective and understanding was mission oriented -- a perspective that was naturally myopic. Their primary mission was to provide real-time incident response to the Internet. The information they accumulated and distributed was tailored for this. For example, the records of the CERT®/CC were maintained on-line for personnel to search during an incident. Each incident recorded contained only the information necessary for Incident response. When an incident was closed, the record was marked closed, with no further action to gather or analyze the information.

The "big picture" has been difficult for CERT®/CC personnel to see from this perspective. This is a case of seeing the individual trees (incidents) in the forest, but having difficulty seeing the pattern of the forest (the overall state of Internet security). CERT®/CC personnel conducted research, but it was primarily a technical focus on current security problems. Their focus was also not policy-oriented, such as toward determining the effectiveness of Internet security policies. This is most likely the reason that, when asked for a sense of the overall Internet security activity, CERT®/CC personnel were not able to provide comprehensive information.

### 1.5. Overview

This research project analyzed trends in Internet security, primarily through an investigation of security-related incidents on the Internet from 1989 to 1995, as reported to the CERT®/CC. The CERT®/CC has been responsible for Internet-related incident response since November, 1988 [ISV95:14].[2] This research also produced recommendations to improve Internet security.

This dissertation begins with a description of relevant Internet characteristics (Chapter 2), and then proceeds in the next chapter (Chapter 3) to present a history of the CERT®/CC, along with a description of their policies. This is followed in Chapter 4 by a discussion of the evolution of CERT®/CC incident response, the characteristics of the CERT®/CC records, the methods used to construct the individual incident records, and the categories of data extracted from these constructed incident records.

---

[2] References in this paper are placed within brackets at the end of the referenced passage. The reference starts with three letters that identify the author(s), followed by a two digit number for the year, a colon, and specific page number(s).

The next seven chapters of the dissertation involve the classification and analysis of the CERT®/CC incidents. This begins with the development of a formal definition of computer security (Chapter 5), followed in the next chapter with a development of a taxonomy for computer and network security (Chapter 6). The development of a comprehensive taxonomy in the field of computer security has been a relatively intractable problem of increased interest [Amo94:31]. It is, however, a necessary prerequisite for systematic studies of computer and network attacks and incidents.

An *attack* is a single unauthorized access attempt, or unauthorized use attempt, regardless of success. An *incident*, on the other hand, involves a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing. The taxonomy developed for this research was to classify *attacks*. Along with other measures of severity, this taxonomy was used in Chapter 7 to classify Internet *incidents*. Chapter 7 also used the taxonomy to present a history of the incidents in the CERT®/CC records.

This research was concerned primarily with an analysis of Internet *incidents* and not Internet *vulnerabilities*, which is a related field of inquiry. More specifically, an attacker exploits vulnerabilities in order to conduct unauthorized actions. As such, vulnerability information was, to an extent, part of this research. This was, however, limited to the existence and frequency of use of vulnerabilities, and not further details concerning the vulnerabilities themselves. This was considered to be beyond the scope of this research.

The taxonomy of computer and network attacks is used in Chapter 8 to present a summary of the relative frequency that various methods of operation and corrective actions appear in the CERT®/CC incident records. More detailed data are presented in Appendix A and B. Chapter 8 also discusses some of the things the CERT®/CC records do not include.

Nearly 10% of all incidents in the CERT®/CC records examined for this research involved one Internet site, which was termed Site A. Chapter 9 presents an analysis of the subgroup of incidents reported to the CERT®/CC that involved Site A. This is followed in Chapter 10 by a more detailed description of a different subgroup: 22 incidents that were identified by various measures as being the most severe in the CERT®/CC records. A third subgroup is examined in Chapter 11: denial-of-service incidents.

The data from all incidents and the three subgroups were used to estimate the total Internet incident activity during the period of the research. This is presented in Chapter 12, followed in Chapter 13 by a critical evaluation of the utility of the taxonomy developed for this research.

The dissertation concludes with a discussion of the implications of this research, (Chapter 14), with recommendations for future research (Chapter 15), and with a summary of conclusions and recommendations (Chapter 15).

*Chapter 2*

# Internet Characteristics

The CERT® Coordination Center (CERT®/CC) was responsible for incident response on the Internet during the period of this research. As such, it was important, as part of this research, to understand the extent and characteristics of the rapidly growing and changing Internet. These will be described in this chapter. This chapter also explains why the organizational level at which the analysis was conducted of the CERT®/CC records was the *site* level, which is the level where the CERT®/CC could expect to be working with the site administrator or other authority with responsibility for the computers and networks at that site.

In addition, the growth of the Internet will be quantified for comparison to the trends in Internet incidents described in later chapters. The growth in the Internet has not been uniform across the top-level domains. While the number of hosts is growing in all of these domains, the growth in the commercial domains (*.com*, *.net*) is more rapid than the growth in those domains associated with education and government (*.edu*, *.gov*, *.org*, *.mil*).

## 2.1. Description and Origins of the Internet

An internetwork, or internet, is a network of networks which has established methods of communication. *The* Internet is the "world's largest collection of networks that reaches universities, government labs, commercial enterprises, and military installations in many countries [Hug95:348]." Although the Internet connects large networks, such as those belonging to large communications companies, the Internet consists primarily of local area networks (LANs) [GaS96:456]. The principle method of communication on the Internet is the TCP/IP protocol suite (Transmission Control/Internet Protocol). The Internet, however, is increasingly becoming an environment with multiple protocols [Cer93:80].

The Internet is rapidly growing and evolving, which makes it difficult to define. Lynch and Rose describe it this way:

> The Internet community spans every continent across the globe. The Internet is so large that its size can only be estimated, and it is evolving so quickly that its rate of growth can only be guessed. It is so diverse that it uses hundreds of different technologies, and is so decentralized that its administrators don't even know each other. The Internet is an electronic infrastructure that enables intense communications between colleagues, competitors, and disciplines. Despite these extremes, the Internet community is bound together by a framework of computer communications networking protocols and infrastructure [LyR93:xiii].

The basis for the Internet was an experiment begun in 1968 by the Defense Department's Information Processing Techniques Office (ARPA/IPTO) to connect computers over a network in order to ensure command and control communications in the event of a nuclear war. The original network was known as the ARPAnet, and the project quickly became a "straight research project without a specific application [Lyn93:5]." In the 1980s, the number of local area networks increased significantly and this stimulated rapid growth of interconnections to the ARPAnet and other networks. These networks and interconnections are known today as the Internet [Til96:168].

### 2.2. Internet Hosts and Domains

Computers that communicate across the Internet are known as a host computers, or simply *hosts* [GaS96:455].[1] A host's connection to the Internet can be continuous or part-time, and it can be through dialup or direct connections [Lot96:defs.html]. Each host computer is identified by both a unique 32-bit *IP address*[2] (Internet Protocol address) and a unique *domain name*. Each of these has two parts, one part that specifies the host computer, and a second part that specifies the location (either physical or organizational) of the host computer [ABH96:7].

**2.2.1. IP addresses** - IP addresses are generally written as four decimal numbers *vvv*, *www*, *xxx*, and *yyy*, each between 0 and 255, and each representing an 8-bit octet of the address. The numbers are grouped together separated by "dots" (periods) in the form *vvv.www.xxx.yyy*, with the most significant (leftmost) digits representing the physical network, and the least significant digits (the rightmost ) representing the individual host. An example is 192.2.200.34.

There are two predominant methods currently used to divide the 32 bits of an IP address into the host and network portions [CaS96:456]. The original addressing scheme was to use the first octet to identify the network and then to use the other 3 octets to identify the host. This limited the Internet to 256 networks. With the rapid growth in the number of LANs, this addressing scheme was abandoned in favor of an addressing scheme with three primary classes. This remains the most widely used addressing scheme [Cer93:91-92]. In this "classical" addressing scheme, the division between the network bits and the host bits are as shown in Table 2.1.

---

[1] The term *host* has sometimes been used specifically to refer computers that communicate or are "visible" outside the local network. I have found, however, that authors generally call all computers with Internet communications capability *hosts*. The computers visible to the Internet may be further differentiated as *routers*, *gateways*, etc. [Cer93:81]. The term host has also changed in recent years to include "virtual hosts," where "a single machine acts like multiple systems (and has multiple domain names and IP addresses). Ideally, a virtual host will act and look exactly like a regular host...[Lot96:notes.html]." In this research, we count virtual hosts equally with other hosts.

[2] Some hosts have more than one connection to the Internet, each of which must have a unique IP address, and therefore, these hosts have more than one IP address [GaS96:455].

| Class | Leftmost (class) Bits | Number of Network Bits | Maximum Number of Networks | Octets for Hosts | Maximum Number of Hosts per Network |
|---|---|---|---|---|---|
| A | *0* | 7 | 127 | *www.xxx.yyy* | 16,777,216 |
| B | *10* | 14 | 16,384 | *xxx.yyy* | 65,536 |
| C | *110* | 21 | 2,097,152 | *yyy* | 256 |
| D (multicast) | *1110* | *N/A* | *N/A* | *N/A* | *N/A* |
| E (experimental) | *1111* | *N/A* | *N/A* | *N/A* | *N/A* |

**Table 2.1. Internet Network Classes [Cer93:92]**

A newer Internet addressing scheme, the Classless InterDomain Routing (CIDR) method, has recently come into use. Using CIDR, the most significant *k* bits of each address specifies the network, and the remaining (32 - *k*) bits specify the host. The size of *k* is unrestricted [GaS96:458].

**2.2.2. Domain Names -** Each host computer's *domain name* is a group of labels (words or letters) separated by dots. Domain names are assigned because users find it easier to work with symbolic names rather than IP addresses [Cer93:95]. Similar to IP addresses, domain names are divided into a host portion and a location portion. The leftmost label or group of labels identifies the host [Sob95:150], and the rest usually refer to the location. An example is *howard.epp.cmu.edu*, which is a *fully qualified domain name* because it has complete host and domain portions.

**2.2.3. Domains -** The network portion of IP addresses and domain names identify a partition of host computers. Both of these partitions are sometimes referred to as the *domain* of the host. This domain distinction was originally intended to separate the protocols in the Internet into two parts: an *interdomain* protocol between domains, and an *intradomain* protocol within domains [Per93:161]. This separation of protocols is not a universal distinction, which is part of the reason there is no generally accepted definition of domain. For some, the domain is the entire network portion of an IP address or domain name. For others, the domain refers only to the highest partition of the Internet into educational (.edu), commercial (.com), military (.mil), etc., networks. These are sometimes called the top-level domain names. Perlman states, however, that none of these definitions are particularly intelligible or accurate [Per93:180]."[3] He suggests instead using a definition based more on functionality: a domain is a partition of networks "that is administrated by a single administrative plan [Per93:180]."

A typical university or company illustrates the confusion between the terms IP address, domain name, domain, host, and network. An example is my computer at CMU, which was assigned an IP

[3] Perlman goes on to say, "It would be an interesting denial-of-service threat on the networking community to lock a bunch of us in a room until we came up with a definition we all agreed on [Per93:180]."

address of "128.2.19.200" and a domain name of "howard.epp.cmu.edu." As is usually the case, there is a direct correspondence between the host portions of both the IP address ("200") and domain name ("howard"). There is usually not, however, a one-to-one correspondence between the network portions of the IP address and domain. In this example, "128.2" indicates a large (class B) network at CMU and the "19" indicates a subnetwork within this large network. This is the most common IP address arrangement [Sob95:150]. In the domain name, "cmu.edu" indicates the host is on the CMU network, and "epp" indicates the host is administered by the EPP Department.

This does not mean, though, that "128.2" = "cmu.edu" or "19" = "epp". While the "128.2" network is the largest network partition at CMU, "cmu.edu" identifies hosts on both this network and on 15 other networks. The "128.2.19" subnetwork contains most of the EPP department's computers, but "epp" computers are located on other subnetworks, and at least one other department has computers on the "128.2.19" subnetwork. In addition, CMU uses portions of each domain name to identify the *functional* location of the host computers. For example, the "128.2.19" subnetwork has computers that are identified as being in campus "clusters" for student use (such as "pc.cc.cmu.edu" or "mac.cc.cmu.edu" computers), in campus-wide functional networks (such as the "andrew.cmu.edu" UNIX network), or part of the campus "backbone" network ("net.cmu.edu").

CMU IP addresses and domain names also illustrate three other sources of confusion. First, many hosts on the Internet have multiple connections, and therefore one host can have multiple IP addresses, often on different networks.[4] Second, different domain names can be assigned to the same host computer, and even the same IP address. Finally, a single domain name can refer to more than one IP address [GaS96:459; Lot96:notes.html].

IP addresses and domain names are related by keeping a list. At the local level, the */etc/hosts* file on UNIX systems associate IP addresses and domain names for routing within networks. Specifically, this file lists the IP addresses, domain names and aliases for the computers authorized to be within a network. The Domain Name System (DNS), which consists of name servers on thousands of computers throughout all levels of the Internet, provides a hierarchically organized distributed database relating IP addresses and domain names for routing on the Internet.

As shown in Table 2.2, the */etc/hosts* file at CMU on September 7, 1996, listed a total of 19,888 IP addresses distributed among 16 large networks and 206 subnetworks. The actual number of

[4] Hosts that connect between networks must have multiple IP addresses – Up to nearly 40 for routers at CMU.

computers at CMU is less than the 19,888 IP addresses because many of the computers have multiple IP addresses, and not all the computers are connected to the network at any one time.

| Large Network | No. of IP Addresses | No. of Subnets | Organizations Identified in Domain name |
|---|---|---|---|
| 128.2 | 19,105 | 170 | acs.cmu.edu, andrew.cmu.edu, arc.cmu.edu, as.cmu.edu, bap.cmu.edu, bio.cmu.edu, cc.cmu.edu, ce.cmu.edu, cec.cmu.edu, cfa.cmu.edu, chem.cmu.edu, cheme.cmu.edu, cit.cmu.edu, cmri.cmu.edu, cnbc.cmu.edu, csw.cmu.edu, ece.cmu.edu, epp.cmu.edu, erdc.cmu.edu, gsia.cmu.edu, heinz.cmu.edu, hss.cmu.edu, ini.cmu.edu, itc.cmu.edu, library.cmu.edu, math.cmu.edu, mcs.cmu.edu, me.cmu.edu, mems.cmu.edu, net.cmu.edu, phil.cmu.edu, phys.cmu.edu, psy.cmu.edu, res.cmu.edu, ri.cmu.edu, stat.cmu.edu, stc.cmu.edu |
| 128.119 | 1 | 1 | cs.cmu.edu |
| 128.182 | 14 | 7 | cs.cmu.edu, stc.cmu.edu, psc.edu |
| 128.237 | 631 | 14 | sei.cmu.edu |
| 129.13 | 1 | 1 | cs.cmu.edu |
| 129.105 | 2 | 1 | cs.cmu.edu |
| 129.250 | 2 | 1 | cs.cmu.edu |
| 167.231 | 2 | 1 | cs.cmu.edu |
| 192.5 | 4 | 1 | tartan.com |
| 192.17 | 5 | 1 | net.cmu.edu, uiuc.edu, evo.org |
| 192.58 | 30 | 1 | sei.cmu.edu |
| 192.70 | 27 | 1 | cs.cmu.edu |
| 192.77 | 1 | 1 | net.cmu.edu |
| 192.80 | 43 | 1 | cs.cmu.edu |
| 192.88 | 1 | 1 | net.cmu.edu |
| 204.194 | 18 | 3 | net.cmu.edu, netbill.com |
| Totals: | | | |
| 16 | 19,888 | 206 | 44 total organizations: 39 in cmu.edu, 2 others in .edu, 2 in .com, and 1 in .org |

**Table 2.2. Summary of *letc/hosts* file at Carnegie Mellon University, September 7, 1996**

The data in Table 2.2 puts this discussion in perspective by illustrating a fundamental distinction between IP addresses and domain names: the location portion of IP addresses correspond in general to the *physical* location of a host computer, while the location portion of domain names correspond to the *organizational* location. An example is the CMU campus-wide network of UNIX computers known as the Andrew System. These host computers can be found all over the CMU campus. The IP addresses of these computers reflect the subnetwork that they are physically connected to. As such, the Andrew System hosts near the EPP Department have subnetwork IP addresses of either 128.2.19 or 128.2.58. If they are connected to a different subnetwork in a different location, then their IP addresses have a different subnetwork number. In other words, the IP addresses of the Andrew hosts is based on their physical location. With respect to their domain names, however, every one of the Andrew hosts have a domain name of the form

*host.andrew.cmu.edu*. This reflects their organizational location within the Andrew System and not their physical location.[5]

Another interesting example is the entry for the IP addresses beginning with 192.17 in Table 2.2. These hosts are physically located at CMU, but are functionally part of two other organizations: The Evolution Group (evo.org) located elsewhere in Pittsburgh, and the University of Illinois at Urbana-Champaign, Illinois (uiuc.edu). Shown also are two connections to the commercial part of the Internet: tartan.com and netbill.com.

The network, subnetwork and host pattern described above is typical of large Internet sites.

### 2.3. Domain Name System (DNS) Terminology

Returning to the question of what a domain is, Sobell defines domain to be a "name associated with an organization, or part of an organization, to help identify systems uniquely [Sob95:772]." This relates to the location portion of a domain name and not to an IP address. This is consistent with the Domain Name System (DNS) which identifies all of the domain name that is not the name of the host itself as the *domain*. In other words, the location portion of the domain name is defined to be the domain. Using the previous example, in the domain name *howard.epp.cmu.edu*, the domain is *epp.cmu.edu*. In the domain name like *pc6.mac.cc.andrew.cmu.edu*, the domain is *mac.cc.andrew.cmu.edu*.

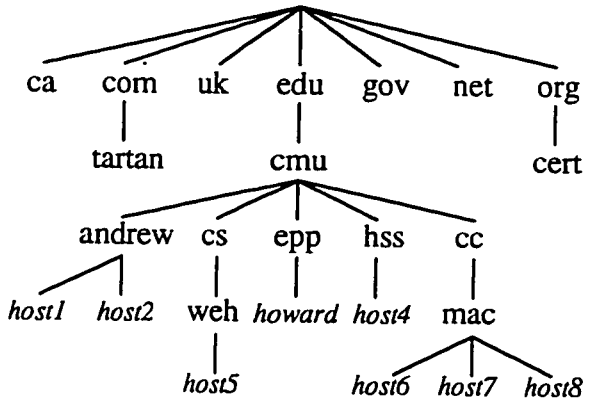


**Figure 2.1. Typical Internet Domain Name Tree**

The DNS database is arranged in a hierarchy, which is a name-space tree such as shown in Figure 2.1. Each node in the tree is identified with a *label*, and the domain name at each node is the ordered list of the label for that node, plus the label for every node on the path back to the to the top or root node of the tree (separated by dots) [Moc93:478]. For example, *host6* in Figure 2.1 has a domain name of *mac.cc.cmu.edu*, which makes the fully qualified domain name *host6.mac.cc.cmu.edu*.

---

[5] IP addresses are becoming less associated with physical locations with the increase in mobile systems and systems which dynamically allocate IP addresses.

Mockapetris defines a *domain* to be the subtree that is included under a domain name. For example, the *cmu.edu* domain is all the hosts located in the subtree under the *cmu* node as shown in Figure 2.1. Therefore, each node in the tree corresponds to a domain name (the path back to the root of the tree), and a domain (the subtree under the node). The concept in structuring the tree is that any portion of the tree "should parallel the administrative organization using it [Moc93:478]."

The DNS terms *host*, *domain*, and *domain name* will be used for domain names in this research. The term *domain* will not refer to IP addresses. Instead, the terminology for IP addresses will be *network*, *subnetwork*, and *host*. For example, as stated earlier, my computer at CMU (with the IP address of 128.2.19.200), is on the "128.2" network, and the "128.2.19" subnetwork, and has the host number "200." This same computer (with the fully qualified domain name *howard.epp.cmu.edu*), is the host *howard*, in the *epp.cmu.edu* domain.

Each of the nodes in the hierarchy of the DNS tree is also referred to as being at a specific *level* of the tree, with the domains at the highest level in the tree referred to as *top-level domains*. As of July, 1996, the DNS had 183 top-level domains. Of these top-level domains, one had a four-letter label (*nato*), and seven had three-letter labels: commercial (*com*), educational (*edu*), network (*net*), military (*mil*), government (*gov*), organization (*org*), and international (*int*). With the exception of *int*, these three-letter, top-level domains contained hosts primarily located in the United States. The remaining 175 top-level domain labels were the International Standards Organizations (ISO) two-letter country codes [Lot96:dist-bynum.html].

A point to be emphasized is that domain names do not necessarily indicate the physical location of the host (unlike IP addresses[6]). Lottor gives the following caution regarding domain names and the location of the host:

> Note, there is not necessarily any correlation between a host's domain name and where it is actually located. A host with a .NL domain name [the Netherlands] could easily be located in the U.S. or any other country. In addition, hosts under domains EDU/ORG/NET/COM/INT could be located anywhere. There is no way to determine where a host is without asking its administrator [Lot96:notes.html].

The level of the tree where particular organizations are placed also varies, and therefore, this does not indicate the size of the organization. As an example, assume there is a commercial company called *Widgets* that has a host computer called *pc1*. If this company is located in the United States, its domain name might be *pc1.widgets.com*, and if it were located in Canada, it might be

[6] Again, IP addresses are becoming less associated with physical locations with the increase in mobile systems and systems which dynamically allocate IP addresses.

*pc1.widgets.ca*, both at the second level of the DNS tree. If the company were in the United Kingdom, a similar commercial domain name would be *pc1.widgets.co.uk*, one level further down in the tree. The host could be even further down in the tree, such as *pc1.dept5.widgets.denver.co.us*, which would indicate that the host *might* be located in Widget's Department 5 in Denver, Colorado. This illustrates that the level of a domain name does not necessarily indicate the size of the domain.

### 2.4. Site Names

During the preliminary analysis of the CERT®/CC records,[7] an attempt was made to conduct the analysis at the level of individual host computers. It was felt that, had this been possible, it would have provided the most detailed and useful information for analysis. This proved infeasible for several reasons. First, information on individual hosts was incomplete. The records for many incidents did not provide any information on individual hosts. When records had host information, it could generally not be determined if the list of hosts was complete. Attempts to estimate the data at the host level were also not successful.

Second, even if the data were available at the host level, analysis at this level would have been very difficult. Take for example, CMU. As was previously discussed, CMU had nearly 20,000 IP addresses in 1996. This number alone illustrates that keeping track of incidents at the host level would be several orders of magnitude more difficult than keeping track of incidents at a higher level, such as the "CMU" organizational level.

Finally, CERT®/CC personnel did not track incidents at the host level. They instead recorded information at an organizational level that matched their interactions with the organization involved in the incident. If a host computer at CMU were involved in an incident, then an incident record was opened in the CERT®/CC files for *CMU* and not for the individual host, nor for the specific organization where the host was located (such as "EPP").

The organizational level used to track incidents was generally referred to in the CERT®/CC records as a *site*. This is the level at which the analysis was conducted of the CERT®/CC records. More specifically, a *site name* was defined to be the domain name for the organization involved in the incident, and *site* referred to the domain under that site name. For sites in the United States and Canada, site names were generally at the second level of the DNS tree. Examples would be *cmu.edu* or *widgets.com*. In other countries, the site name was the third or lower level of the DNS tree, such as *widgets.co.uk*. A site was also the organizational level where the CERT®/CC could expect to be

[7] See Chapter 4 for a description of the CERT®/CC records.

working with the site administrator or other authority with responsibility for the computers and networks at that site.

Some organizations, such as larger universities and companies, were large enough to be physically divided into more than one location, with separate administration. This separation could not be determined from CERT®/CC records, because these different locations generally had the same site name. Therefore, different locations with the same site name were treated as one site.

For some incidents, site names were not listed for all of the sites involved (around 6% of sites). These were typically not reporting sites, but other sites known to be involved. In these incidents, IP addresses of the other sites were often available instead. As discussed earlier, IP addresses do not have a direct correlation with domain names, and therefore they may have limited relationship to site names. However, for many organizations, there is a level of agreement between the network portion of the IP address and the site name. For example, IP addresses beginning with "128.2" were generally part of the "cmu.edu" domain. As such, it was assumed that the first two octets of an IP address corresponded to a site name when the actual site name was not available.

### 2.5. The Internet Domain Survey

Lottor has estimated the growth in the number of hosts and domains on the Internet from 1981 through the period of this research. Between 1981 and 1986, this estimate was taken from the host table maintained at the Internet's Network Information Center (SRI-NIC) [Lot92:1]. After 1986, estimates were made using the ZONE (Zealot of Name Edification) program. The ZONE program gathered information by "walking" through the DNS tree as it recorded domain names and IP addresses, creating a table of hosts. The ZONE program repeated this process until the program had cycled through the entire list of domains without receiving any new information [Lot92:2-3].

Counting hosts that have multiple domain names or IP addresses more than once is prevented by the groupings in the DNS. The number of domains is determined by including all domains referenced by a record in the DNS [Lot92:4]. This process is assumed to *underestimate* the number of hosts. This is primarily because not all hosts on the Internet are registered in a domain server. On the other hand, errors and duplicates (under different names) in the DNS cause the results of ZONE to be higher. The former effect (underestimate) is seen by Lottor to be the larger effect.

> Manual scanning of the data indicates that the additional entries are insignificant compared to the missing entries. ... ZONE data can thus be viewed as the minimum number of Internet hosts, and not the actual figures [Lot92:3].

Lottor's evaluation of the accuracy of the ZONE program and it's ability to estimate the number of hosts and domains is as follows:

> We consider the numbers presented in the domain survey to be fairly good estimates of the *minimum* size of the Internet. *We cannot tell if there are hosts or domains we could not locate.* In summary, it is not possible to determine the exact size of the Internet, [or] where hosts are located.... [Lot96:notes.html]

At the time of this research, the Internet Domain Survey was produced by Network Wizards. The data was available on the Internet at http://www.nw.com/ [Lot96:report.html]. Statistics prior to 1992 were found in Request for Comments (RFC) 1296, published by SRI International, and also available at the same Network Wizards Web site [Lot92].

### 2.6. Estimated Growth of the Internet

As of July, 1996, the Internet connected together a minimum of approximately 13 million host computers [Lot96:report.html]. The Internet's current growth rate, shown in Figure 2.2, results in its size doubling every 12 to 15 months [Lot96:notes.html].

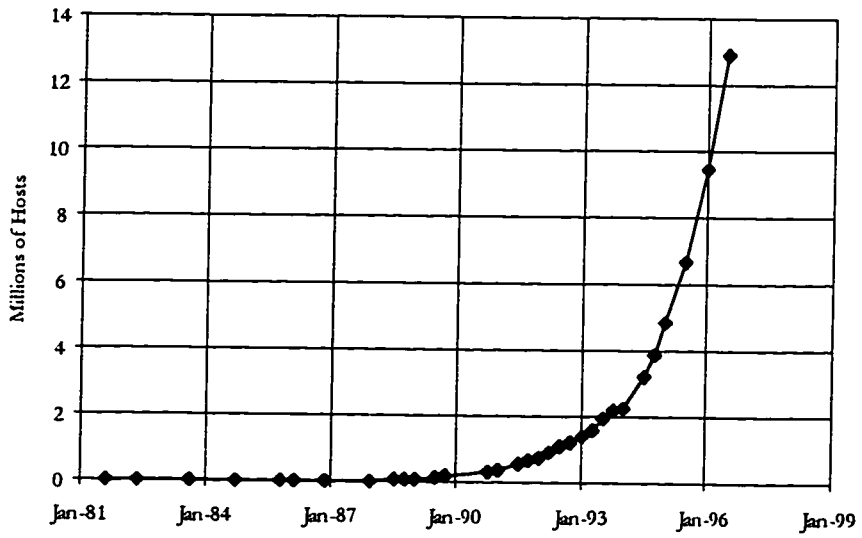


**Figure 2.2. Growth in Internet Hosts [Lot92; Lot96]**

If this current trend continues, this would result in the Internet having around 200 million host computers at the turn of the century (January, 2001), as shown in Figure 2.3. A common method of estimating the *number of people* that use the Internet host computers is to multiply the number of hosts by a factor of 10 [Mer95:history.hosts].

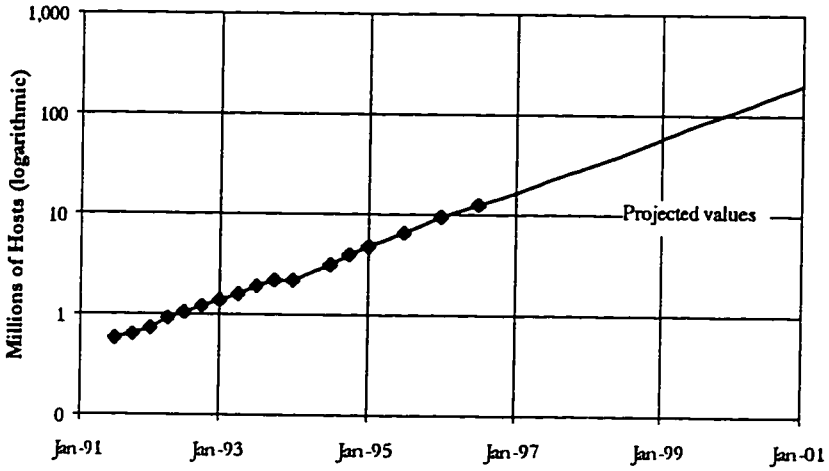


**Figure 2.3. Projected Internet Growth [Lot92; Lot96]**

This seems to be a high estimate, particularly considering the reduced percentage of Internet hosts that are found at educational institutions (discussed later in this section). This is because students would tend to share hosts computers more than other classes of users, such as users at commercial sites or in private homes. In any case, the number of users would certainly be greater than one user per host computer, and therefore, it is possible that between 200 million to 2 billion people will be using the Internet by the turn of the century.

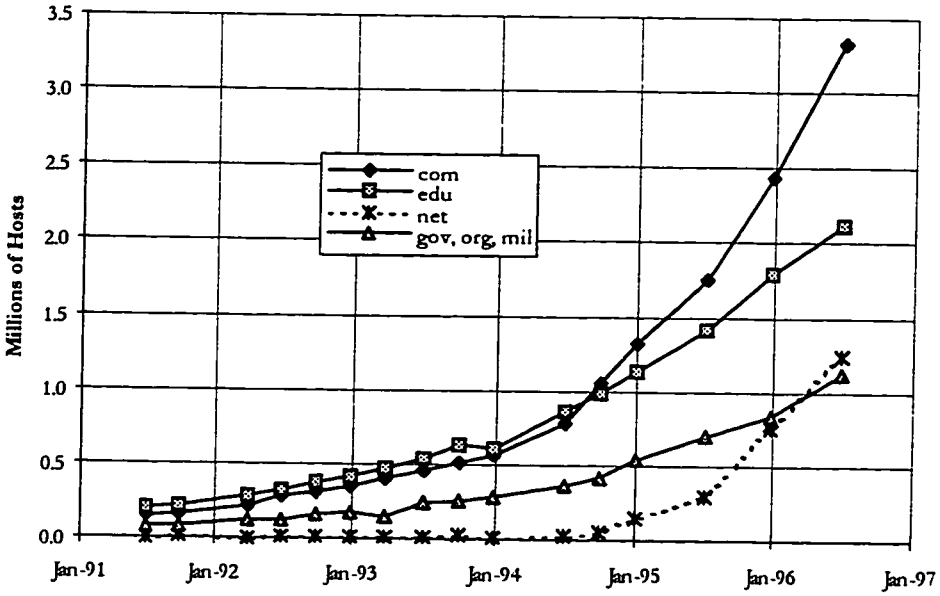


**Figure 2.4. Growth of Top-Level Domains with Predominantly U.S. Hosts [Lot96]**

The growth in the Internet has not been uniform across the top-level domains. For example, most of the three-letter, top-level domains contain hosts predominantly in the United States. Figure 2.4 shows the growth of these domains. While the number of hosts is growing in all of these

domains, the growth in the commercial domains (*.com*, *.net*) appears more rapid than those domains associated with education and government (*.edu*, *.gov*, *.org*, *.mil*).

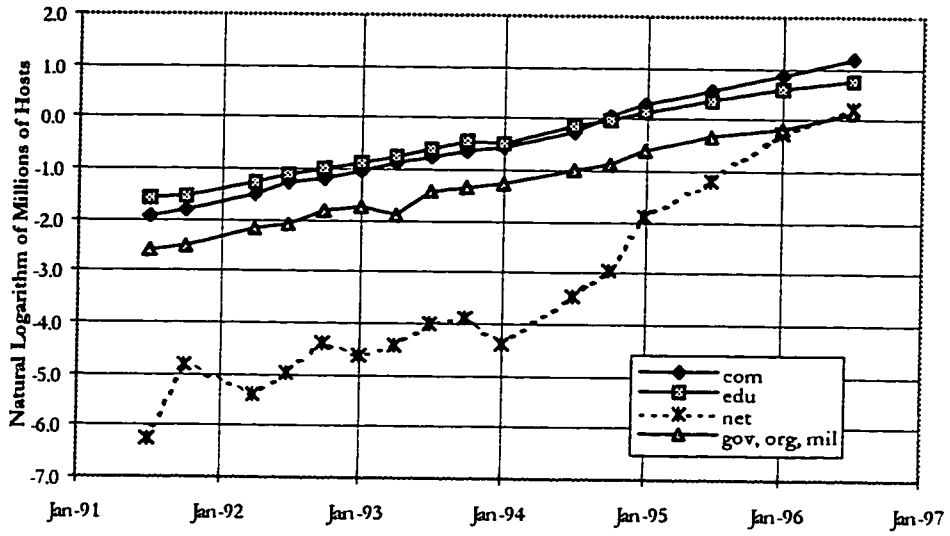


**Figure 2.5. Growth of Top-Level Domains with Predominantly U.S. Hosts [Lot96]**

Figure 2.5 shows the natural logarithm of the same data in Figure 2.4. Table 2.3 shows the estimates for the slope of these lines obtained from linear regression, and the percentage these slopes are greater than the slope for the *.edu* domain. The growth in the *.com* domain was about 30% greater than in the *.edu* domain, but the most significant growth was in the *.net* domain, which was 144% greater.

| Top-Level Domain | Slope | Percentage Greater than *.edu* domain |
|---|---|---|
| *.edu* | .001322 | - - - |
| *.gov*, *.org*, *.mil* | .001501 | + 14% |
| *.com* | .001722 | + 30% |
| *.net* | .003227 | + 144% |

**Table 2.3. Linear Regression Slopes of Growth Rates of Top-Level Internet Domains**

These trends can also be seen in the entire Internet. Figure 2.6 shows the size of all of the top-level domains as a percentage of the entire Internet. The domains with predominantly U.S. government hosts (*.gov*, *.org*, *.mil*) have declined as a percentage of the total Internet from about 13% in 1991, to 9% in 1996. The trend is even more pronounced in the U.S. educational institutions which have declined as a percentage of the total Internet from about 36% in 1991, to 16% in 1996. Growth has been experienced in the top-level domains that contain primarily North American commercial hosts (*.com*, *.net*, *.us*, *.ca*) which have grown from approximately 29% to 42%, and in the

other domains located outside of North America, which have grown from 22% to 33%. These last two domain groups now represent 75% of the Internet.

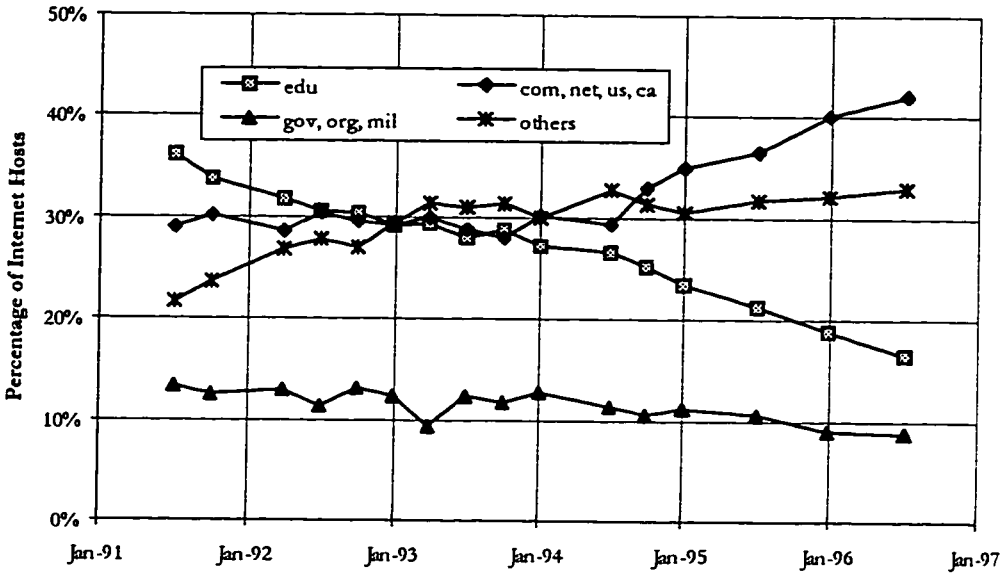


**Figure 2.6. Top-Level Domains as a Percentage of the Internet [Lot96]**

As discussed previously, CERT℠/CC incidents were analyzed at the site level. The Domain Survey estimates both the number of hosts and the number of domains. The site level is between the top-level domains and the lowest-level domains in the DNS system, both of which were estimated by the Domain Survey. The trends in both Internet hosts and Internet domains as estimated by the Domain Survey will be compared to the trends in incidents at the site level in later chapters. As such, it is appropriate to examine the trends in Internet domains.

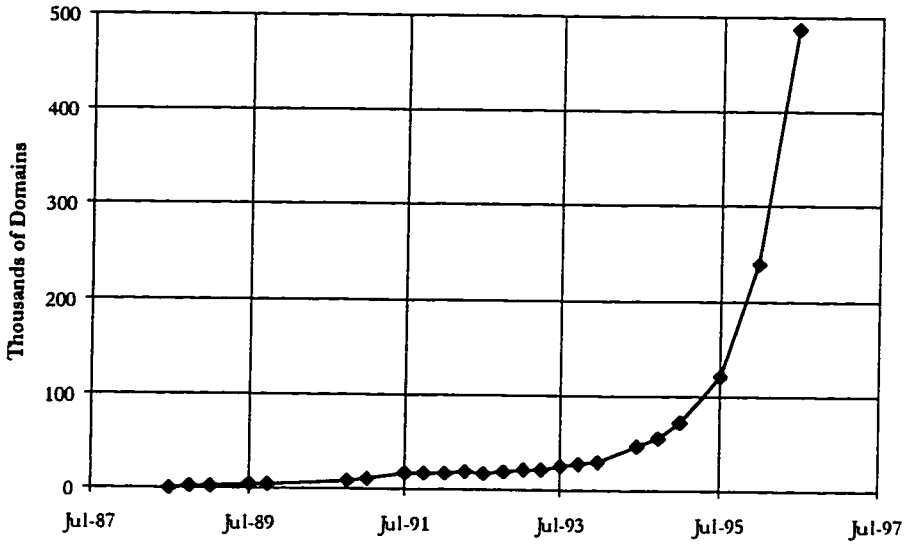


**Figure 2.7. Growth in DNS domains [Lot92; Lot96]**

Figure 2.7 shows the growth in the number of Internet Domains in the DNS system. As of July, 1996, there were estimated to be 488,000 of these domains. The average growth rate in domains was 36% per year, but in the first half of 1995, it was 69% per year, and during both the second half of 1995 and the first half of 1996, the growth rate was 100% per year. The trend in domains looks similar to the trend in hosts (Figure 2.2), but there are significant differences.

The number of hosts per DNS domain has declined in the last three years as shown in Figure 2.8. Perhaps this trend reflects the increased growth in the *.com* and *.net* Internet domains. A new commercial site is more likely to have less hosts per site than either an established commercial or educational site. This may also reflect an increase in domain names that was not accompanied by an increase in IP addresses (recall that an IP address may have more than one domain name). For example, several organizations may share a host computer and its access to the Internet, while appearing to be separate sites, and also appearing in DNS servers as separate domains.

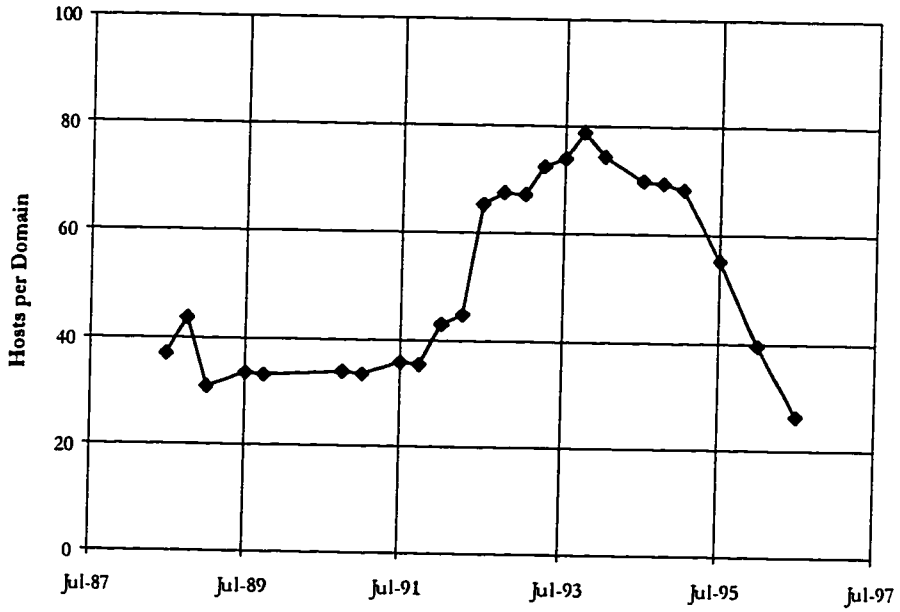


**Figure 2.8. Trends in Internet Hosts per DNS domain [Lot92; Lot96]**

One final trend of interest is the change in the World Wide Web, an Internet service that has grown rapidly in the last few years. The Web has its origins in research by Berners-Lee at the European Physics Laboratory (CERN) beginning in 1989. He created client-server software for conveniently publishing and retrieving formatted documents on the Internet. The client portion of this software is commonly called a Web browser. Documents are published at sites with Web server software and are retrieved using one of these Web browsers [Til96:140].

A Web site is not the same as an Internet site. An Internet site was defined previously to be a network of computers under the administrative control of an organization. A Web site is instead a set of files on a host computer that can be linked to over the Internet using a Web browser. There may be numerous Web sites on a single network or on the same host computer.

| Date | Number of Web Sites | % .com sites | Internet Hosts per Web Site |
|---|---|---|---|
| Jan-93 | 50 | 0.0% | 28,205 |
| Jun-93 | 130 | 1.5% | 12,282 |
| Dec-93 | 623 | 4.6% | 3,576 |
| Jun-94 | 2,738 | 13.5% | 1,178 |
| Dec-94 | 10,022 | 18.3% | 484 |
| Jun-95 | 23,500 | 31.3% | 283 |
| Jan-96 | 100,000 | 50.0% | 95 |
| Jun-96 | 230,000 | -- | 56 |

**Table 2.4. Growth of the World Wide Web [Gra96; Lot96; Til96:140]**

The growth in the World Wide Web was estimated by Matthew Gray of the Massachusetts Institute of Technology as shown in Table 2.4 and Figure 2.9 [Gra96]. The World Wide Web grew significantly faster than the Internet, although that trend had been slowing. In the second half of 1993, the Web was doubling in less than three months. The 1995 growth rate resulted in doubling in under 6 months, which was more than twice the growth rate of the Internet [Gra96].

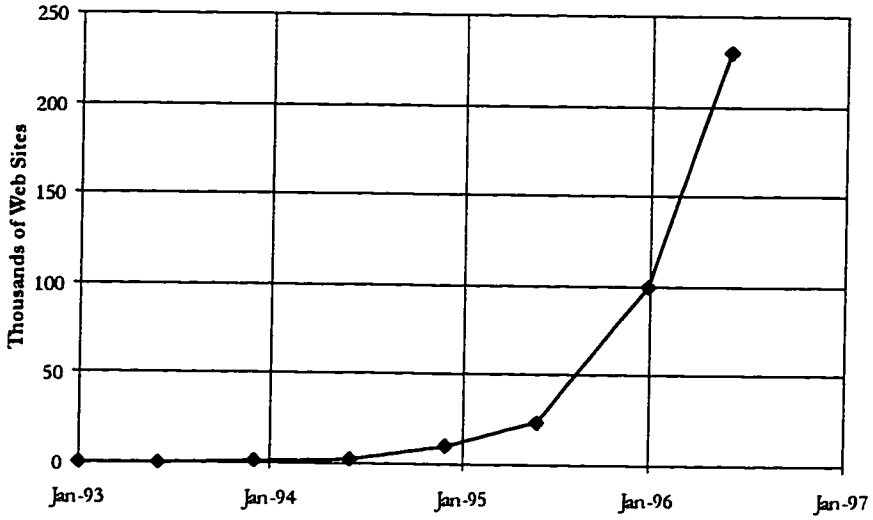


**Figure 2.9. Growth of the World Wide Web [Gra96; Til96:140]**

## 2.7. Summary of Internet Characteristics

*The* Internet is the world's largest network of networks. It consists primarily of local area networks that communicate with each other using the TCP/IP protocol suite. Computers that

communicate across the Internet are known as a host computers, or simply *hosts*. Each host computer is identified by both a unique 32-bit *IP address* (generally written as four decimal numbers *vvv*, *www*, *xxx*, and *yyy*, each between 0 and 255) and a unique *domain name* (a group of labels separated by dots). IP addresses and domain names are both divided into a portion identifying the host, and portion identifying a partition of host computers. For IP addresses, this partition is known as a network. For domain names, it is known as the domain.

The Domain Name System (DNS) provides an Internet service that relates domain names to IP addresses. The DNS terms *host*, *domain*, and *domain name* will be used for domain names in this research. The terminology for IP addresses will be *network*, *subnetwork*, and *host*. As of July, 1996, the DNS had 183 top-level domains. Of these top-level domains, one had a four-letter label (*nato*), and seven had three-letter labels: commercial (*com*), educational (*edu*), network (*net*), military (*mil*), government (*gov*), organization (*org*), and international (*int*). With the exception of *int*, these three-letter, top-level domains contained hosts primarily located in the United States. The remaining 175 top-level domain labels were the International Standards Organizations (ISO) two-letter country codes.

The organizational level at which the analysis was conducted of the CERT℠/CC records was at the *site* level, which is the level where the CERT℠/CC could expect to be working with the site administrator or other authority with responsibility for the computers and networks at that site. The analysis of the CERT℠/CC records was not conducted at the level of host computers for three reasons: information on individual hosts was incomplete, an analysis at this level would have been very difficult, and CERT℠/CC personnel did not track incidents at the host level.

Lottor has estimated the growth in the number of hosts and domains on the Internet since 1981. Since 1986, estimates were made using the ZONE (Zealot of Name Edification) program. As of July, 1996, the Internet connected together a minimum of approximately 13 million host computers. The Internet's current growth rate results in it's size doubling every 12 to 15 months. If this current trend continues, this would result in the Internet having around 200 million host computers at the turn of the century (January, 2001).

The growth in the Internet has not been uniform across the top-level domains. For example, most of the three-letter, top-level domains contain hosts predominantly in the United States. Figure 2.4 shows the growth of these domains. While the number of hosts is growing in all of these domains, the growth in the commercial domains (*.com*, *.net*) appears more rapid than those domains

associated with education and government (*.edu*, *.gov*, *.org*, *.mil*). These trends can also be seen in the entire Internet. The various Internet growth rates are summarized in Table 2.5.

| Date | Hosts | % Change | Domains | % Change | Web Sites | % Change |
|---|---|---|---|---|---|---|
| 1-Jul-88 | 33,000 | -- | 900 | | -- | -- |
| 1-Jan-89 | 80,000 | 142% | 2,600 | 189% | -- | -- |
| 1-Jul-89 | 130,000 | 63% | 3,900 | 50% | -- | -- |
| 1-Jan-90 | 203,200 | 56% | 6,100 | 56% | -- | -- |
| 1-Jul-90 | 276,400 | 36% | 8,200 | 34% | -- | -- |
| 1-Jan-91 | 376,000 | 20% | 11,200 | 20% | -- | -- |
| 1-Jul-91 | 569,373 | 51% | 16,000 | 43% | -- | -- |
| 1-Jan-92 | 727,000 | 28% | 17,000 | 6% | -- | -- |
| 1-Jul-92 | 1,067,588 | 47% | 16,300 | -4% | -- | -- |
| 1-Jan-93 | 1,410,243 | 32% | 21,000 | 29% | 50 | -- |
| 1-Jul-93 | 1,923,304 | 36% | 26,000 | 24% | 150 | 200% |
| 1-Jan-94 | 2,227,730 | 16% | 30,000 | 15% | 720 | 380% |
| 1-Jul-94 | 3,225,177 | 45% | 46,000 | 53% | 3,140 | 336% |
| 1-Jan-95 | 4,851,843 | 50% | 71,000 | 54% | 11,400 | 263% |
| 1-Jul-95 | 6,641,541 | 37% | 120,000 | 69% | 28,200 | 147% |
| 1-Jan-96 | 9,472,224 | 43% | 240,000 | 100% | 100,000 | 255% |
| 1-Jul-96 | 12,880,699 | 36% | 488,000 | 103% | 230,000 | 130% |

**Table 2.5. Summary of Internet Growth Rates Over Six-Month Intervals**

*Chapter 3*

# CERT®/CC History and Policies

The CERT®/CC, located at CMU's Software Engineering Institute (SEI), has been on the "front lines" in defense of the Internet since November, 1988. This chapter presents a history of CERT®/CC and a description of their policies, particularly regarding advisories and the disclosure of other information. This also includes a brief discussion of other CERT®-like organizations.

## 3.1. Origins of the CERT®/CC

In November, 1988, a graduate student at Cornell University released a self-replicating computer program on the Internet. This program, which has come to be known as the "Internet Worm," exploited several software bugs in the UNIX operating system to penetrate host computers across the network. [RuG91:4]. At the time, the Internet consisted of approximately 60,000 computers [Lot92]. Although not programmed to damage computers or their files, apparently due to an error in the program, the Internet Worm replicated rapidly within host computers. Infected computers were rendered useless because their processing capability was absorbed by multiple copies of the worm program. While only 2,100 to 2,600 host computers were infected,[1] this effectively "shut down" the Internet for several days as defensive measures were taken (which included many sites disconnecting from the network) [RuG91:4, Hug95:142].

In order to eliminate the Internet Worm, an ad hoc response team was created consisting of experts at MIT, Berkeley, Purdue and other sites. The Worm code was reverse engineered and fixes for the software bugs and procedures for eradication of the Worm were developed and disseminated [RuG91:4]. Following this incident, the Defense Advanced Research Projects Agency (DARPA), sponsors of the Internet, decided to institutionalize the concept of an Internet emergency response team. The CERT® Coordination Center (CERT®/CC) was therefore established at CMU's Software Engineering Institute (SEI), near the end of November, 1988 [ISV95:14; RuG91:5].

## 3.2. CERT®/CC Purpose

The purpose of the CERT®/CC is to provide the Internet community a single organization that can coordinate responses to security incidents on the Internet. CERT®/CC accomplishes this during a security incident by establishing and maintaining communication with the affected sites, and with experts who can diagnose and solve security problems [HoR91:25].

---

[1] The original and most common estimate is 6,000 hosts, but later research indicates this is incorrect [RuG91:4].

The CERT® charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems [CER96:1].

The CERT®/CC organization is made up of three closely related groups, each providing related products and services for the Internet community:

1) *Operations* - a single point of contact for system and network security
   a) 24-hour technical assistance hot-line for responding to computer security incidents
   b) advisories of Internet vulnerabilities through the CERT® Advisories mailing list, as well as through an anonymous FTP server and a Web site
   c) additional product vulnerability assistance through a database of vulnerabilities
   d) vendor relations
2) *Education and Training* - help organizations form response teams, train users, improve security
   a) security-related technical documents, summaries, and vendor-initiated bulletins
   b) security-related seminars and workshops
3) *Research and Development* - to stimulate the development of trustworthy systems
   a) security research and engineering
   b) security-related tools [CER92:2; CER96:1-5]

### 3.3. Operating Procedures and Policies[2]

The CERT®/CC currently consists of approximately 35 people who work in an isolated area of the SEI. To conduct operations as outlined above, CERT®/CC personnel perform the following:

a) Incident Response - The CERT®/CC hot-line is manned for incident response Monday through Friday during normal business hours. At other times, CERT®/CC personnel assigned to incident response are "on call," and can be reached through the hot-line. CERT®/CC personnel currently respond to an average of 15 incident reports a day. Most incidents are limited, and involve the use of known techniques. These can be handled by CERT®/CC personnel. If necessary, CERT®/CC personnel will coordinate by adding volunteer experts within the Internet community to form a larger response team.

b) Vulnerabilities Database - The CERT®/CC maintains a database consisting of known Internet software security vulnerabilities, along with fixes for these vulnerabilities. Vulnerability reports are collected from the Internet community at large and then, if confirmed by CERT®/CC personnel, they are entered into the database.

---

[2] The information in this section was gathered primarily through interviews with CERT®/CC personnel in 1995-96.

c) Information Response - A large percentage of CERT®/CC inquiries have been for information. Many of these inquiries involve neither incident response nor vulnerabilities, and are more properly handled by software or hardware vendors. This CERT®/CC service is, therefore, being phased out.

Since its inception, CERT®/CC has maintained strict rules of confidentiality. Information provided by the CERT®/CC to the Internet community is limited to advisories about vulnerabilities. These advisories give general information about the nature of the vulnerabilities and specific details of how these vulnerabilities may be eliminated or mitigated. The CERT®/CC does not publish information on the specific details of vulnerabilities or on how these vulnerabilities may be exploited. In order to prevent aiding attackers in exploiting these vulnerabilities, this information is only given to the appropriate vendors and individuals requiring the information in order to correct the vulnerabilities.

Information about actual incidents, particularly the sites involved and the techniques used, are strictly confidential. CERT®/CC rules require that site confidentiality be maintained for two reasons. First, if sites were to be identified, particularly during an incident, they may become targets for additional attacks. In addition, the CERT®/CC may receive fewer reports if confidentiality were not guaranteed. Sites reporting to the CERT®/CC desire this confidentiality not only to prevent additional attacks, but also to prevent adverse effects from publicity. Because of this policy, CERT®/CC personnel will generally 1) not acknowledge the existence of an incident outside of the response team and the sites involved, and 2) not inform sites involved in an incident of the involvement of other sites, unless those sites give specific permission. Occasionally, the CERT®/CC issued advisories warning about significant Internet intruder activity, but with no details about the incidents themselves.

### 3.4. Other Incident Response and Security Teams

The Internet is a diverse community of cultures, needs, policies, and technologies. There are a variety of constituencies for incident response and security ranging from the Internet, to military services, other government agencies, other networks, and commercial companies – all of which may be located in foreign countries. As a result, since the CERT®/CC was established, a variety of computer security incident response teams have been established in various government, commercial and academic organizations around the world. The CERT®/CC continues to be the largest and best known of these organizations. Also, since the Internet has become ubiquitous, it is

unlikely that any large incident response effort would be outside the responsibility of the CERT®/CC.

Some coordination takes place between these incident response and security teams, primarily through informal arrangements. The Forum of Incident Response and Security Teams (FIRST) provides an avenue for more formal interaction between these organizations. FIRST is a non-profit corporation that was established to exchange information and coordinate response activities. As of October, 1996, FIRST had 57 members. These are shown in Table 3.1 through Table 3.7.

As can be seen in these tables, the CERT®/CC has a considerably larger responsibility than the other organizations that are part of FIRST. In addition, the responsibilities of the CERT®/CC overlaps most of these organizations. This is further evidence that we should expect that most large incidents that took place on the Internet should appear in the CERT®/CC records. This may not be the case, however, with smaller incidents that fall within the more limited responsibility of one of the other organizations.

### 3.5. Summary of CERT®/CC History and Policies

Following the Internet Worm incident in November, 1988, the Defense Advanced Research Projects Agency (DARPA), established the CERT® Coordination Center (CERT®/CC) at CMU's Software Engineering Institute (SEI) in order to provide the Internet community a single organization that can coordinate responses to security incidents on the Internet.

The CERT®/CC maintains strict rules of confidentiality. Information provided by the CERT®/CC to the Internet community is limited to advisories about vulnerabilities. Information about actual incidents, particularly sites involved and techniques used, are strictly confidential. Throughout the CERT®/CC history, this high level of confidentiality has been controversial.

A variety of computer security incident response teams have been established in various government, commercial and academic organizations around the world, although the CERT®/CC continues to be the largest and best known of these organizations. These response teams coordinate informally, and through the Forum of Incident Response and Security Teams (FIRST).

| Internet and Other Network Response Teams in FIRST | |
|---|---|
| **Organization** | **Constituency** |
| AUSCERT (Australian Computer Emergency Resp. Team) | Australia |
| CARNet-CERT | CARNet connected sites |
| CERT® Coordination Center | The Internet |
| CERT-IT, Computer Emergency Response Team Italiano | Italian Internet |
| CERT-NL | SURFnet connected sites |
| DFN CERT | Germany |
| Israeli Academic Network | Israeli University users |
| JANET-CERT | All UK organizations connected to JANET network |
| MxCERT (Mexican CERT) | Mexico (.mx domain) |
| NORDUnet | NORDUnet |
| SWITCH-CERT | Sites connected to SWITCH |

**Table 3.1. Internet and Other Network Response Teams in FIRST, and their Constituencies [FIR96]**

| Other U.S. Government Agency Response Teams in FIRST | |
|---|---|
| **Organization** | **Constituency** |
| Department of Energy's CIAC | U.S. Department of Energy (DOE) and DOE Contractor sites, plus the Energy Science Network (ESnet) |
| Goddard Space Flight Center | Goddard Space Flight Center |
| NASA (Ames Research Center) | NASA (Ames Research Center) |
| NASA Auto. Sys. Incid. Resp. Capability (NASIRC) | NASA & the International Aerospace Comm. |
| NCSA-IRST (National Center for Supercomputing Applications IRST) | National Supercomputing Community, in particular our Industrial Partners, Collaborators, the State of Illinois, and K-12 Illinois Learning Mosaic community |
| U. S. National Institutes of Health | Employees of the U.S. National Institutes of Health |
| NIST/CSRC | NIST and civilian U.S. agencies (guidance only) |
| U.S. Social Security Administration | U.S. Social Security Administration |
| Small Business Administration (SBACERT) | Small Business Community Nationwide |
| Vet. Health Admin. Forum of Incid. Resp. Sec. Team | Veteran's Health Administration |

**Table 3.2. Other U.S. Government Agency Response Teams in FIRST, and their Constituencies [FIR96]**

| U.S. Military Incident Response Teams in FIRST | |
|---|---|
| **Organization** | **Constituency** |
| AFCERT (Air Force CERT) | Air Force Users |
| Department of Defense ASSIST | DOD - Interest systems |
| Defense Information Systems Agency | MILNET |
| NAVCIRT (Naval Computer Incident Response Team) | U. S. Department of Navy |

**Table 3.3. U.S. Military Response Teams in FIRST, and their Constituencies [FIR96]**

| U.S. Educational Response Teams in FIRST | |
|---|---|
| **Organization** | **Constituency** |
| Northwestern University | Northwestern University Faculty/Staff/Students |
| Ohio State University Incident Response Team(OSU-IRT) | The Ohio State University |
| Pennsylvania State University | Pennsylvania State University |
| Purdue Computer Emergency Resp. Team (PCERT) | Purdue University |
| Stanford University Network Security Team | Stanford University Networks and Systems |

**Table 3.4. U.S. Educational Response Teams in FIRST, with Constituencies [FIR96]**

| Foreign Government Response Teams in FIRST | |
|---|---|
| **Organization** | **Constituency** |
| BSI/GISA | German Government Institutions |
| CCTA | All UK Government and Agencies |
| Defence Research Agency, Malvern | Defense Research Agency |
| Renater | Minister of Research & Education, France |

**Table 3.5. Foreign Government Response Teams in FIRST, with Constituencies [FIR96]**

| Computer and Communications Vendor Response Teams in FIRST | |
|---|---|
| **Organization** | **Constituency** |
| Apple Computer | Apple Computer (worldwide) |
| Cisco Systems | Cisco Systems (employees/contractors) |
| Digital Equipment Corporation (SSRT) | DEC and customers |
| FreeBSD, Inc. | users of FreeBSD or other UNIX operating systems |
| Hewlett-Packard Company | All HP-UX and MPE Customers |
| IBM-ERS | IBM internal and external customers |
| MCI | MCI Employees, Contractors and Alliance Partners |
| Micro-BIT Virus Center | Anyone Calling |
| Motorola Comp. Emergency Resp. Team | Motorola |
| Silicon Graphics Inc. | Silicon Graphics' User Community |
| SUN Microsystems, Inc. | Customers of Sun Microsystems |
| UNISYS Computer Emer. Response Team (UCERT) | Unisys Internal/External Users |
| Sprint | Sprint Net (X.25) and Sprint Link (TCP/IP) |

**Table 3.6. Computer and Communications Vendor Response Teams in FIRST, with Constituencies [FIR96]**

| Other Commercial Response Teams in FIRST | |
|---|---|
| **Organization** | **Constituency** |
| ANS CO+RE Systems, Inc. | ANS Customers |
| Bellcore | Bellcore |
| Boeing CERT (BCERT) | Boeing |
| EDS | EDS and EDS Customers |
| General Electric Company | Thirteen GE businesses |
| Goldman, Sachs and Company | Goldman, Sachs offices worldwide |
| JP Morgan | JP Morgan Employees/Consultants |
| SAIC Security Emergency Response Center | Commercial and government customers |
| TRW Inc. | TRW Network and System Administrators |
| Westinghouse Electric Corporation | Entire Corporation |

**Table 3.7. Other Commercial Response Teams in FIRST, with Constituencies [FIR96]**

*Chapter 4*

# CERT®/CC Records

This chapter begins with a discussion of the evolution of CERT®/CC incident response. This is followed by a discussion of the characteristics of the CERT®/CC records, and the methods used to construct the individual incident records. The categories of data extracted from these constructed incident records is then presented.[1]

## 4.1. CERT®/CC Incident Response

The organization and operation of the CERT®/CC appears to have gone roughly through three periods: 1) an early, informal period from November, 1988 to around January, 1992, 2) a transitional period for the next year and a half, and 3) a more formal period beginning in the summer of 1993. CERT®/CC records reflect these changes in organization and operation.

**4.1.1. Early, Informal Period -- November, 1988 to January, 1992 -** After the Internet Worm incident in November, 1988, DARPA quickly moved to establish the CERT®/CC in order to institutionalize the incident response capability that was spontaneously formed during the incident. Within weeks, the CERT®/CC was functioning at the Software Engineering Institute (SEI) of Carnegie Mellon University, Pittsburgh. Beginning in these early weeks, and continuing for this early period, the CERT®/CC responded to incidents in an ad hoc, informal manner. Communications were primarily through electronic-mail (e-mail), supplemented by the telephone.

Records during this early period reflect resistance from CERT®/CC personnel to efforts to formalize incident responses, although there were continuous efforts to formalize the process of *formulating* responses. The rationale was to maintain the greatest flexibility for CERT®/CC personnel, who could then use their own judgment in determining the correct course of action during any incident. This system remained in place throughout the period studied in this research.

CERT®/CC personnel have never formalized the rules of incident response beyond that necessary for a very basic training in incident response. Instead, CERT®/CC personnel relied on an extensive and lengthy apprenticeship training program, as well as prior experience, for new personnel to learn incident response.

Consensus was achieved in the early period in some areas of the incident response process. The ground rules for confidentiality discussed in Chapter 3 and 14 were established fairly quickly. Patterns were also developed for personnel scheduling, as the number of people responding to

[1] Information for this chapter was obtained from the CERT®/CC records and from discussions with CERT®/CC personnel during 1995.

incidents increased in the first year from the initial two to around a half dozen. Incidents were responded to by personnel who were assigned to the hot-line position for one to two weeks at a time. When "on point" at the hot-line, CERT®/CC personnel handled all aspects of all the open incidents. At the end of their period on point at the hot-line, they would brief the incoming personnel on the open incidents and then hand over the incident response function. As a result, during this period, all incidents were handled by different people every one to two weeks.

Incident response was the initial motivation to establish the CERT®/CC. This is a reactive role with CERT®/CC personnel waiting for an incident to be reported before taking action. From the beginning, however, the CERT®/CC charter also included the more proactive role of providing security information to the Internet community. As a result, CERT®/CC quickly became a repository for information on vulnerabilities in Internet systems.

Information on possible vulnerabilities came into the CERT®/CC from both the Internet user community, and from hardware and software suppliers. CERT®/CC personnel would then test the reported vulnerabilities to see if they were real. CERT®/CC personnel maintained records of these vulnerabilities. These records evolved into a vulnerability database that was maintained throughout the period studied in this research. CERT®/CC personnel included both the vulnerabilities, and the "fixes" or "work-arounds" that were developed either by CERT®/CC personnel, by the software and hardware suppliers, or by others in the Internet community.

This established the position of the CERT®/CC as a single point of contact for system and network security as described in Chapter 3. CERT®/CC personnel on point at the hot-line were, therefore, responsible for three types of contacts from Internet constituents: 1) requests for assistance during an incident (incident response), 2) information *from* Internet users and vendors on vulnerabilities, and 3) requests from Internet users *for* information on how to reduce vulnerabilities and to increase security.

**4.1.2. Transition Period -- January, 1992 to September, 1993 -** By the beginning of 1992, the number of incidents grew to where the ad hoc process of incident response was not satisfactory. CERT®/CC personnel were overwhelmed in two ways. First, the method of keeping track of incidents was informal, involving handwritten notes and electronic mail (e-mail). Incidents were not tracked by numbers, nor by specific sites. As the number of incidents increased, CERT®/CC personnel had increasing difficulty keeping track of information and responding effectively. Second, passing the responsibility for all incidents to the incoming team was increasingly difficult, time-consuming and confusing.

The first adjustment for CERT®/CC personnel was to begin tracking incidents by site. As discussed below, this primarily involved manually summarizing e-mail into one file under a site name. Also, CERT®/CC personnel began numbering e-mail messages to aid in referring to them. This procedure was continued through 1992. However, the adjustment proved to be inadequate, and in the beginning of 1993, the CERT®/CC began tracking incidents by assigning a single, random number, such as CERT®#1234, to each incident, in addition to continuing the assigning of other numbers to individual messages. Inquiries for information were assigned information numbers (example: INFO#45612), and information involving vulnerabilities was assigned a vulnerability number (example: VUL#789). During the first half of 1993, an automatic e-mail sorting and summarizing system was developed based on these numbers. This was an improved system, although the summaries were terse and generally required CERT®/CC personnel to refer frequently back to the original messages.

The second adjustment made by the CERT®/CC during this period was to transition the response team away from handing off incidents to different people every week or two. Instead, each incident was assigned to one person in the CERT®/CC to handle comprehensively from the beginning until the incident was closed. This helped to ensure continuity in incident response. The assignments were made according to the workload of CERT®/CC personnel.

**4.1.3. Formal Period -- September, 1993 to December, 1995 -** By the end of the transition period, incident response was formalized. CERT®/CC personnel responding to the hot-line and e-mail inquiries were now known as technical coordinators. One change that was made during 1994 was to improve the program used to sort and summarize e-mail. This included having the program copy more of the body of each message into the summary file for that incident number. This significantly reduced the need to refer to the original messages.

### 4.2. CERT®/CC Record Characteristics and Methods of Analysis

The CERT®/CC records reflect the purpose of the CERT®/CC to respond to Internet incidents, investigate vulnerabilities, and disseminate information. As discussed, this required the development of a vulnerability database that could be accessed by CERT®/CC personnel during an incident, and when information was requested. CERT®/CC also disseminated information through the CERT® Advisories mailing list (e-mail listserver), through an anonymous FTP (file transfer protocol) site, and later through a World Wide Web site.

For incident response, all CERT®/CC records were maintained "on-line" in the CERT®/CC local area network. These records could be searched for key words in order to find similar events. In addition, as discussed above, beginning in 1992, each message that arrived at the CERT®/CC was assigned a unique number in the incident summary file. This number could be used to view the original message.

While the CERT®/CC records were useful for the "real-time" CERT®/CC operation, the records did not represent a source of information valuable for analysis. For example, the actual number of incidents reported to the CERT®/CC could not easily be determined. This was because, even in the period after the transition, multiple records could be opened for the same incident, if it was reported by more than one site. The records themselves usually indicated the relationship between these records, but this required reading the individual incident summaries.

**4.2.1. Early Period Records -- November, 1988 to May, 1992 -** Records from the early period and the beginning months of the transition period consist primarily of the e-mail and other files sent to the CERT®/CC. These messages and files were archived together in chronological order, without any other organization. For the first two years, the records also include a limited number of DARPA-requested periodic summaries. These summaries proved to be of limited use.

In order to gather data about incidents during this period, I had to create the incident records from the more than 10,000 messages in the CERT®/CC archive. Since there was no organization to the file, I read each message in chronological order, and then processed it as follows:

1) If the message did not contain information about an incident, it was eliminated from consideration. Examples of eliminated messages include information from a user or vendor about a vulnerability, or a request for information from a user.

2) Unix search tools, such as the *grep* utility, were used to relate key words and phrases to the incidents already created. The primary key word used was the site name, but searches were also conducted using other distinctive words or phrases, such as the method of attack, or the name or location of the attacker.

3) If a match of key words or phrases was found, the message was compared to the incident it matched with in order to judge whether it was part of the same incident. If the message was determined to be part of that incident:

   a) The message was appended to the end of the incident's file.

   b) Keywords in the message were then used to search the remaining CERT®/CC records near this time frame for further matches. If other messages were found to be related, they were also appended to the incident's file.

4) If a match of key words or phrases was not found for a message, a new incident file was created and the message was copied into it. The file was assigned a unique number that indicated the reporting date of the incident. For example, the incident file 90-054-06

would indicate the incident was first reported to the CERT®/CC on the 54th day of 1990 (February 23rd). The last number, 06, indicates that it was the 6th incident reported to the CERT®/CC that day.

**4.2.2. Later Period Records -- May, 1992 to December, 1995** - Starting in May, 1992, summaries were available for the incidents reported to the CERT®/CC. These summaries were originated or "opened" when CERT®/CC personnel determined that an incident had probably begun or taken place. These summaries were kept on-line in a large file of open incidents that could be accessed by all CERT®/CC personnel. When it was determined that an incident was completed, it was marked "closed." Once a week, the CERT®/CC archived records as follows:

1) All closed incidents were removed from the open file and placed in a separate file of closed incidents for that week.
2) The file with the remaining open incidents was then copied into a separate archived file.

In 1992, the summaries were created and maintained through manual entries by CERT®/CC personnel. These entries included notes and excerpts from e-mail and other files sent to the CERT®/CC. The completeness of these summaries depended upon who created and maintained them, with some being relatively detailed in their entries, which meant the summary could be used without reference to the original e-mail. Other CERT®/CC personnel were less detailed in their entries, which made the summary shorter, but also required more frequent references to the original messages. These summaries were sometimes an incomplete record of an incident.

In 1993, the CERT®/CC incident summaries were changed to include the CERT®, INFO, and VUL numbers. This allowed the summaries to be initiated and maintained through an automated e-mail sorting program. Unfortunately, until the middle of 1994, this program appeared to excerpt very little from the incoming e-mail – often only the subject line. This probably required CERT®/CC personnel to reference the original e-mail frequently. This also made the summaries a relatively incomplete record during this year.

In the summer of 1994, the summaries became more extensive. Throughout the remaining records, the summaries generally contained the bodies of the e-mails sent to the CERT®/CC. Response personnel could probably use these summaries without reference to the original messages. In this last period, the summaries represent a relatively complete incident record.

As stated earlier, the correspondence between incidents and summaries was not one-to-one. An incident summary was opened when an incident report was received by the CERT®/CC. Many of these summaries later proved to be related to each other. Once CERT®/CC personnel determined that two or more summaries were related, the usual course of action was to indicate this

relationship in the summaries, but to keep all the summaries open. As such, the number of summaries in the CERT®/CC records is greater than the number of actual incidents. Occasionally, a summary was closed and the information from that summary was copied to a related summary.

In order to gather data about incidents during this period, I had to create the incident records from the CERT®/CC summaries. Because there was more organization to the summaries than to the e-mail, it was easier to reconstruct the incidents using the summaries. I processed each CERT®, INFO and VUL summary as follows:

1) If the summary did not contain information about an incident, it was eliminated from consideration.

2) Unix search tools, such as the *grep* utility, were used to relate key words and phrases to the incidents already created. For the early summaries, the primary key word used was the site name, with searches also conducted using other distinctive words or phrases, such as the method of attack, or the name or location of the attacker. After CERT®, INFO, and VUL numbers were assigned to the summaries beginning in 1993, these numbers became the primary key words for searching.

3) If a match of key words or phrases was found, the summary was compared to the incident it matched in order to judge whether it was part of the same incident. In this process, any notes in the summary relating to other summaries were used to aid in determining the relationship. The judgment of CERT®/CC personnel was given strong weight. For example, a common phrase was "related to CERT®#XXX." This usually resulted in the summaries being combined into one incident. The phrases "may be related to CERT®#XXX," or "possibly related to CERT®#XXX" were given less weight. If the summary was determined to be part of the same incident:

   a) The summary was appended to the end of the incident's file.

   b) Keywords in the summary were then used to search the remaining CERT®/CC records near this time frame for further matches. If other summaries were found to be related, they were also appended to the incident's file.

4) If a match of key words or phrases was not found for a summary, a new incident file was created and the summary was copied into it. The file was assigned a unique number that indicated the reporting date of the incident. For example, the incident file 93-035-05 would indicate the incident was reported to the CERT®/CC on the 35th day of 1993 (February 4th). The last number, 05, indicates that it was the 5th incident reported to the CERT®/CC that day.

As noted earlier, the incident summaries from the Spring of 1993 to the Summer of 1994 were incomplete. Because of the number of incidents in this period (over 1,400), time did not allow extracting information from the original messages for these incidents. As such, for this period, the incident records created as part of this research did not give complete details.

### 4.3. Data Extraction

After the incidents were reconstructed from the CERT®/CC records, I examined each of the incidents 1) to ensure that the incident was reconstructed correctly, and 2) to extract data from each incident. The following fields of data were then placed in a summary file:

1) ***Reporting Date*** - The first field in the summary file was the incident file identifier, which indicated the date the incident was reported to the CERT®/CC. The field contained three numbers separated by the letter "i" and two dashes. Using the example file name cited earlier, an example of an entry in this data field is "i93-035-05," which indicates the incident was reported to the CERT®/CC on the 35th day of 1993 (February 4th). The last number, 05, indicates that it was the 5th incident reported to the CERT®/CC that day.

2) ***Starting Date (SD)*** - The starting date was assumed to be the same as the reporting date, unless there was some other information in the file to indicate the incident actually began at an earlier date. If there was such information, this was used to determine the starting date. This field in the file contained two numbers separated by a dash. An example is "92-015," which indicates the incident began on the 15th day of 1992 (January 15th).

3) ***Ending Date (ED)*** - The ending date of an incident was more difficult to determine, particularly in the later files. Some preference was given to the date the incident was closed, but closing the incident in the CERT®/CC summaries was an administrative function that was not necessarily related to the actual ending date of the incident. Other possibilities were to use the date of the last activity recorded in the file, or to use a date discussed in the narrative of the file. These possibilities were examined in each of the incident files to make a judgment as to the ending date. This field was also entered as two numbers separated by a dash.

4) ***Number of Sites (NS)*** - This field listed the total number of sites involved in the incident. This included both the sites that reported the incident, and the other sites involved. The majority of incidents involved two sites (60.2%): the attacking site and the attacked site. Some incidents (91 incidents, 2.1%) involved only one site, which meant the attacker was located at the site being attacked. The remaining 1,699 incidents (37.7%) involved more than two sites. More than 100 sites were involved in 31 of the incidents, and the largest incident involved more than 1,500 sites. This field was recorded as a positive integer.

5) ***Number of Messages (NM)*** - The number of messages received by the CERT®/CC may give some indication of the CERT®/CC workload. In some instances, the CERT®/CC was involved in an incident only to a limited degree, even if the incident was large. For example, an

incident that involved 100 sites, but only two messages to the CERT®/CC may indicate limited CERT®/CC involvement or workload. This field was recorded as a positive integer.

6) ***Reporting Sites (RS)*** - The site name was recorded for each site that reported the incident. In the records after 1992, this generally corresponded to the sites that were assigned a CERT® number for the incident. The site names listed were as discussed in Chapter 2, such as *cmu.edu* or *widgets.co.uk*. For some of the sites, the site name was not available, but the IP address was. In these cases, the first two octets of the IP address were recorded instead of the site name. For example, for an IP address of "111.222.333.444," the octets "111.222" would be recorded. All of the reporting sites were listed in this field of the summary file. After the data for all incidents were extracted from the records, the site names were replaced with numbers and top-level domain names. For example, *widgets.co.uk* might have been replaced with *123.uk*. IP addresses were replaced with a "z" domain, such as *123.z*.

7) ***Other Sites (OS)*** - The incident file was examined to determine if there were other sites involved that had not reported the incident. If there were other sites that could be determined, they were listed in this field. If site names were not available, and the IP address was, then the first two octets of the IP address were entered in the field. As with reporting sites, after the data for all incidents were extracted from the records, the other site names were replaced with numbers and top-level domain names.

8) ***Level (LV)*** - Each incident was classified as discussed in Chapter 7. This was recorded as a single integer as follows:

| | | | |
|---|---|---|---|
| 1 | root break-in | 5 | access attempt |
| 2 | account break-in | 6 | disclosure of information incident |
| 3 | denial-of-service incident | 7 | false alarm |
| 4 | corruption of information incident | | |

9) ***Methods of Operation (MO)*** - CERT®/CC personnel began recording a field of information in the CERT®/CC incidents in 1992 called "MO." CERT®/CC personnel used this field for two types of information. First, they recorded their judgment as to the severity of the attack. This was the level of attack which, for this research, was separated out into the Level (LV) field (discussed above). Second, CERT®/CC personnel recorded in this field the tools and vulnerabilities used for access as depicted in Figure 6.9 in Chapter 6. If information was available in this field of the record, or in the text of the record, regarding the methods of operation used in the incident, they were recorded in the MO field of the summary file in the form of key words. In addition, the level of attack was written in key words in this MO field. Finally, a limited amount of

information about attackers, results and objectives (defined in Chapter 6, and shown in Figure 6.9) were also recorded in this field. The keywords used and their frequency of occurrence are discussed in Chapter 8.

10) ***Corrective Actions (CA)*** - CERT®/CC records gave little information as to the corrective action taken in each incident. If information was available on corrective actions taken, it was recorded in the form of key words in this field of the summary. The keywords used and their frequency of occurrence are discussed in Chapter 8.

11) ***CERT® Number (CN)*** - The last field of data extracted from the incidents was the number or numbers assigned to the incident by CERT®/CC personnel. As discussed earlier, assignment of these numbers began in 1993. If an incident was reported by multiple sites, typically there were multiple CERT® numbers assigned to the incident. In addition, incidents sometimes also had VUL (vulnerability) or INFO (information) numbers assigned to them. All numbers that were assigned by CERT®/CC personnel to the incident were listed in this field of the summary. For incidents prior to 1993, this field in the summary record is blank.

An example of a record in the summary file is shown below. This is an incident that was reported to the CERT®/CC toward the end of 1995. The incident began four days before it was reported and it ended 40 days into 1996. Three sites reported the incident, which caused CERT®/CC personnel to assign three CERT® numbers to the incident. An additional 18 sites were involved. This incident was a level 3, denial-of-service incident, with methods of operation and corrective actions as shown. The example incident record is as follows:

> i95-362-01 SD: 95-358 ED: 96-040 NS: 0021 NM: 0042 RS: 006.edu, 468.net, 192.net OS: 775.com, 595.com, 316.com, 348.com, 945.com, 600.com, 405.com, 1763.com, 347.com, 150.com, 011.fi, 1764.com, 815.com, 1309.com, 055.net, 097.com, 1765.com, 772.com LV: 3 MO: dos attack, mail spoofing, mail subscribing, majordomo CA: notify site, filter, police, close account CN: CERT#6995, CERT#16821, CERT#16470

### 4.4. Summary of CERT®/CC Records

The organization and operation of the CERT®/CC appears to have gone roughly through three periods: 1) an early, informal period from November 1988 to around January 1992, 2) a transitional period for the next year and a half, and 3) a more formal period beginning in the summer of 1993. CERT®/CC records reflect these changes in organization and operation.

For incident response, all CERT®/CC records were maintained "on-line" in the CERT®/CC local area network. While the CERT®/CC records were useful for the "real-time" CERT®/CC operation, the records did not represent a source of information valuable for analysis. For this research, I had to construct the incident records from these records. In the early period, the

records consisted primarily of the e-mail and other files sent to the CERT®/CC archived together in chronological order, without any other organization. Starting in May 1992, summaries were manually created for each site reporting an incident to the CERT®/CC. Since multiple sites could report the same incident, multiple summaries could be open for a single incident. In 1993, the CERT®/CC incident summaries were changed to include the CERT®, INFO, and VUL numbers. This allowed the summaries to be initiated and maintained through an automated e-mail sorting program.

Data were extracted from each incident after the incidents were reconstructed from the CERT®/CC records. These data included reporting date, starting date, ending date, number of sites, number of messages, reporting sites, other sites, level of attack, methods of operation, corrective actions, and CERT® number.

The next chapter develops a definition of computer security. This is followed by the development of a taxonomy of attacks in Chapter 6. In the remaining chapters, the incident records described in this chapter (Chapter 4) will be analyzed.

*Chapter 5*

# A Formal Definition of Computer Security

Development of agreed upon terminologies and principles of classification (a taxonomy) are two of the necessary prerequisites to systematic studies in any field of inquiry [McK82:3]. The development of a comprehensive taxonomy in the field of computer security has been an intractable problem of increasing interest [Amo94:31]. Even the potential for partial success in this area makes this effort valuable.[1]

The first step in the development of a comprehensive taxonomy for the classification of computer and network security attacks and incidents was to define *computer security*. This was done by first examining alternative definitions of computer security and then narrowing the definitions toward the following formal definition: *Computer security* is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks. This formal definition provided a boundary to the computer and network security field that was then expanded into the taxonomy described in Chapter 6.

## 5.1. Simple Computer Security Definitions

In the early days of computing, computer security was of little concern. The number of computers and the number of people with access to those computers was limited [GaS96:11; Amo94:1]. The first computer security problems, however, emerged as early as the 1950's, when computers began to be used for classified information. *Confidentiality* (also termed *secrecy*) was the primary security concern [RuG91:9], and the primary threats were *espionage* and the *invasion of privacy*. At that time, and up until recently, computer security was primarily a military problem, which was viewed as essentially being synonymous with *information security*. From this perspective, security is obtained by protecting the information itself.

By the late 1960's, the sharing of computer resources and information, both within a computer and across networks, presented additional security problems. Computer systems with multiple users required operating systems that could keep users from intentionally or inadvertently interfering with each other [GaS96:15]. Network connections also provided additional potential avenues of attack that could not generally be secured physically. Disclosure of information was no longer the only security concern. Added to this was concern over maintaining the integrity of the information. Conventional wisdom dating from this period was that governments are primarily

[1] Personal communication from Dr. Thomas A. Longstaff, CERT®/CC.

concern with preventing the disclosure of information, while businesses are primarily concerned with protecting the integrity of the information, although this is becoming less the case [Amo94:4].

In their popular text on Internet security and firewalls, Cheswick and Bellovin define computer security to be "keeping anyone from doing things you do not want them to do to, with, on, or from your computers or any peripheral devices [ChB94:3]." Using this definition, computers are seen to be targets that can be attacked ("do to"), or tools that can be used ("do . . . with, on, or from"). From this perspective, computer security is distinguished from information security. "Computer security is not a goal, it is a means toward a goal: information security [ChB94:4]."

A more operational definition is presented by Garfinkel and Spafford in their text on Unix and Internet security: "A computer is secure if you can depend on it and its software to behave as you expect . . . . This concept is often called *trust*: you trust the system to preserve and protect your data [GaS96:6]." The authors intend for this definition to include natural disasters and buggy software as security concerns, but to exclude software development and testing issues.

These definitions are relatively informal, and as a result, they are not adequate to the development of a taxonomy of computer security problems. Ideally, a definition would unambiguously demarcate the boundaries of the field of concern. For example, natural disasters and buggy software both can result in damage to computer files, and, therefore, a very broad definition of computer security would include both of these. As a practical matter, however, the computer security field is not usually considered to be this inclusive. Garfinkel and Spafford include these concerns in their definition of computer security, but they narrow their focus on "techniques to help keep your system safe from other people – including both insiders and outsiders, those bent on destruction, and those who are simply ignorant or untrained [GaS96:7]."

### 5.2. Narrowing the Definition of Computer Security

There are many events that could result in damage to of loss of computer files that are included in the broad, informal definitions of computer security, but they are more appropriately considered part of related security fields. Theft of computer equipment would certainly result in the loss of computer files, but this type of theft is similar to the theft of the copy machine, telephone, jewelry, or any other physical object. Methods to provide security for physical objects are well-developed, and are not unique to computer equipment.[2] Environmental threats, such as earthquakes, floods,

[2] I do not consider physical security as part of "computer security" unless it concerns access control. The distinction intended here is between the physical security of the hardware and physical security that protects computer and network processes, files, and data in transit. The physical security of the hardware from theft, vandalism, etc. is not

lightning, power fluctuations, humidity, dust, varying temperatures, and fire, can also result in damage to computer files, but they also can cause damage to other property. It seems customary for authors to include these threats within their broad computer security definitions, but they then proceed to exclude discussions of these problems in their texts or papers on computer security. The definition of computer security developed here is intended to explicitly exclude these areas.

Another similar area involves software. "Buggy" software is certainly a threat to computer files. Improperly implemented software could cause files to be damaged or lost. But this does not, of course, mean that we should include software development as a subset of the computer security field. Most software development issues, instead, fall outside of the computer security field. Software errors, however, clearly lead to security problems: they sometimes create vulnerabilities that can then be exploited. In fact, software that operates correctly can also be a security problem when it is operated in a manner which was not intended. Software problems will be included in the taxonomy developed in Chapter 6 as a method for the introduction of system vulnerabilities that could be exploited to breach computer security.

A common method to narrow the definition of computer security is to concentrate on the three categories of computer security: confidentiality, integrity, and availability [RuG91:9, Lan81:251].[3]

> Confidentiality requires that information be accessible only to those authorized for it, integrity requires that information remain unaltered by accidents or malicious attempts, and availability means that the computer system remains working without degradation of access and provides resources to authorized users when they need it [Kum95:1].

This concentration focuses computer security on the protection of computer files, and ensuring the availability of the computer and network system. This focus is too narrow for at least two reasons. First, as will be shown in Chapters 7 and 10, the most common type of attack seen on the Internet appears to be motivated by the objective to gain access to a *superuser* or *root* account on a Unix-based computer system.[4] More specifically, the access sought is to a command interpreter or *shell* which has full access to the computer. In other words, the access sought is to a *process* that is

---

unique to computer equipment, and is similar to the physical security needs relative to all high-value equipment, and, therefore, it is a general law-enforcement problem. Physical security required to prevent access to computer and network processes and files, on the other hand, *is* unique to computers and networks. I, therefore, separate these physical security needs and include only the second in the definition of computer security.

[3] As discussed earlier, different authors use different terms for these three categories, some using "opposite" terms.

[4] Computers using the Unix operating system or using an operating system derived from Unix form the basis of the infrastructure of the Internet. Internet incidents during the period of this study almost exclusively involved Unix-based systems. For those who are unfamiliar with Unix, there are numerous texts available that describe the system. Examples include [Gil92] for Unix System V and its derivatives, and [Sob95] for BSD and its derivatives.

operating (the shell) and not necessarily to the *files*. Many attackers indeed are attempting to use the process access to gain access to the files, but many are simply after the process access itself.

The other reason this focus is too narrow is found in the security architecture of Unix-based computer systems, where security is based on protection of *objects*, which includes both processes and files. Access to processes is commonly restricted by accounts to which the user must log in, such as by entering the correct user name and password. Once an attacker gains access to a process, then the process must be used to gain access to files. In other words, access to a file system requires two steps: access to a process, then access to the file. This is illustrated by a typical Unix process, such as the */bin/cp* utility (used to copy files). A user gets access to this utility upon successfully logging into an account. Access to the */bin/cp* utility, however, does not mean that the user can now use this process to copy any file. When a process runs, it may access only a limited collection of files that are associate with the user [Tan92:193]. The user may, therefore, use the */bin/cp* utility only to copy files for which that user has the appropriate permission.

In addition to using processes to access files, processes may also be used to access data that is in transit across a network. In this case, these data are not contained in files which would be located in primary memory (the computer's volatile random-access memory), or in secondary memory (storage disks). They are instead a stream of data packets in transit. These can be accessed by processes operating at the origin host for the data transmissions, at the destination host, or at hosts in between through which the data pass.

In summary, conceptualizing computer security as being based on providing confidentiality, integrity, and availability in a computer system [Kum95:1] narrows the focus to the *files* in a system. Confidentiality and integrity specifically refer to the prevention of disclosure, alteration or deletion of the information contained in computer files [RuG91:9-10]. As discussed above, however, this is only one of the levels of access in a typical computer security system. Access controls are used to restrict access to processes, files, and data in transit.

### 5.3. Toward a More Formal Definition

With these criticisms in mind, I used the following two questions as a starting point for developing a more formal definition of computer security:

1. What resources are we trying to protect?
2. Against what must the computer systems be defended?[5]

[5] The first of these questions came from the three questions that Cheswick and Bellovin used to attempt to define computer security [ChB94:4]: The second of their questions, "Against whom must the computer systems be

**5.3.1. What resources are we trying to protect?** - As the previous discussion suggests, the resources that we want to protect are the *processes*, *files* and *data in transit*, on computers and networks. As stated by Tanenbaum,

> A process is basically a program in execution. It consists of the executable program, the program's data and stack, its program counter, stack pointer, and other registers, and all other information needed to run the program [Tan92:12].

A *file* is "a collection of records or data designated by name and considered as a unit by the user [LaL96:441]." These are usually stored in secondary memory (disks). *Data in transit* are packets of data that are being transmitted across a network.

Some authors suggest including other objects, such as *databases*, or *semaphores* [Tan92:193].[6] At the level of abstraction required for this research, it seemed unnecessary to make these distinctions. As such, processes were assumed to include their variables (such as semaphores) and the temporary files in volatile memory, and files were assumed to include databases, directories, etc. that are stored in secondary memory.

From the operational viewpoint, processes, files, and data in transit are not independent categories. While processes can be targeted separately, files and data in transit can only be reached through processes. On the other hand, before a process is activated, it is stored as a file. The important point, however, is that processes, files, and data in transit are secured separately. Because of this, it is appropriate to include all three separately as the "resources we are trying to protect."

The exception to this is physical attacks. In these cases, files or data in transit could be reached without first accessing a process. An example of this would be stealing floppy disks, hard disks or entire computers. As stated earlier, methods to provide security for physical objects are well-developed, and are not unique to computer equipment. As such, theft of hardware will not be included in this definition of computer security. Another possibility, however, would be the use of a *data tap* where a cable carrying network traffic is "listened" to by a device external to the network. Even the electromagnetic emanations surrounding a computer, sometimes called *Van Eck radiation* [Sch94:141], can be "listened" to for data being processed on the computer. These types of

---

defended?," is not addressed as part of this research, primarily because there is little information in the CERT® records about the identity of attackers. The third of the Cheswick and Bellovin questions, "How much security can you afford?," brings up the important problem of the affordability of security. Clearly, tradeoffs must be made between security and cost. It is widely claimed that greater security results in greater cost. The research reported here, however, was concerned with identifying security problems rather than defenses, particularly with respect to the Internet and national security. As such, the subject of the affordability of defensive measures was not researched.

[6] A database is a "collection of interrelated data files or libraries, or a data bank, organized for ease of access, update and retrieval [LaL96:438]." A semaphore is an example of a variable in a software program, particularly an operating system. In this case, it is an integer variable used for counting [Tan92:41].

physical attacks are of concern in this research, although later chapters show that there is no example of such attacks in any of the CERT®/CC records. Of course, they would be hard to detect if they had occurred.

**5.3.2. Against what?** - This question could be interpreted in several ways. One way is as a question about what is being used to perform an attack. For example, an attacker could use a self-replicating computer code, such as a virus or worm, or the attacker could run a shell script that exploits a software bug to defeat access controls on a process. These are all "tools" that the attacker may use to accomplish an objective (discussed in Chapter 6). From the operational viewpoint, this interpretation is on the "means" portion of "means, ways, and ends," which is a common paradigm in military strategy that "defines objectives, identifies courses of action to achieve them, and provides the resources to support each course of action [Gue93:xv]."[7]

The somewhat opposite perspective is to interpret "against what?" to mean the "ends" part of "means, ways, and ends." Computers must, therefore, be protected against the "ultimate objective," "purpose" or "target" of an attack. From this perspective, computer security is about preventing such crimes such as theft, fraud, espionage, extortion, vandalism, and terrorism.

A third interpretation, also from the "ends" part of "means, ways, and ends," has already been discussed: computer and network files and data in transit must be protected from being read, altered or deleted (Section 5.2). In addition, computers and networks must be available when we want them [Amo94:3]. Cohen presents this viewpoint as follows:

> I have taken the perspective that, regardless of the cause of a protection failure, there are three and only three sorts of things that can result:
>
> 1. Otherwise defect-free information can become corrupt,
> 2. Services that should be available can be denied, and/or
> 3. Information can get to places it should not go. [Coh95:54]

Cohen terms each of these results as *disruptions*, which he specifically calls *corruption*, *denial*, and *leakage* [Coh95:54-55]. Steps taken to prevent disruption, which we can term *protections*, have already been discussed as *integrity*, *availability*, and *confidentiality*.

Each of these interpretations has its conceptual advantages, as well as its limitations. Computer and network processes, files, and data in transit must be protected from the "means" of attack, such as computer viruses, the exploitation of system vulnerabilities, etc. They must also be protected

---

[7] It is my feeling that such a process-oriented approach yields a satisfactory taxonomy because it tries to follow the thought process of the attacker. I did not use this approach because of its military connection.

from the "ends" of attack: crimes, including theft, fraud, espionage, extortion, vandalism, and terrorism. Files and data in transit must be protected from corruption or leakage, and computers and networks must be available for use. In short, all of these interpretations of "what" computer and network processes and files must be protected against should be included in the definition of computer security.

In order to provide such a comprehensive definition of computer security, I adopted an interpretation of "against what" as being against the "ways" of attacks. This perspective is between the "means" and "ends" perspectives presented above. Two example attacks will illustrate this interpretation. In the first example, an attacker copies a password file from the target system using TFTP (trivial file transfer protocol). The password cracking program *crack* is used on this password file to obtain the password of a user's account. The attacker then uses telnet to sign into this account. Once in this account, the attacker runs a shell script to exploit a vulnerability and gain root privileges which the attacker uses to copy sensitive files and software. In the second example, an attacker floods the target system with nuisance electronic mail (e-mail), which causes the target system's hard disk to reach its storage limits and the system to stop processing.

As shown in Table 5.1, in the first example, the "means" of attack include tftp, *crack*, telnet, a shell script, and the exploitation of vulnerabilities in the system. The "ends" of the attack are the leakage of sensitive files and software. In the second example, the "means" of attack is a flood of e-mail, with the "ends" being a denial-of-service shutdown of the system.

| Example Attack | "means" | "ways" | "ends" |
|---|---|---|---|
| copies password file, gains access to user account, then root privileges | tftp, *crack*, telnet, shell script, vulnerabilities | unauthorized access | copy files, software |
| sends e-mail to flood system | e-mail program | unauthorized use | denial-of-service |

**Table 5.1 Example Attacks**

Table 5.1 also shows the "ways" of each of the example attacks. In the first example, tftp, *crack*, telnet, etc., are all used to defeat the access controls on the system in order to accomplish the ends of the attack: to copy files and software. Here the attacker is not authorized for the access. This is different from the second attack where the access to the e-mail program and even the target system *is* authorized. The access, however, is used in an unauthorized manner in order to flood the target system with e-mail and cause it to shut down. This is the perspective taken in my definition of

computer security: on the "ways" of computer and network attacks. The two "ways" possible are either to gain unauthorized access, or, given an authorized access, to use that access in an unauthorized manner.

This separation of the "ways" into *unauthorized access* and *unauthorized use* is not mutually exclusive, and using one or the other term is not exhaustive. More specifically, *access* and *use* are not the same concept, although they are related in an attack. For example, when an attacker bypasses access controls (unauthorized access) in order to accomplish an objective, the attacker is also making inappropriate use of computers and networks (unauthorized use). An alternative would be to use the two terms *unauthorized access* and *authorized access*.[8] The problem with this combination is the use of the word "authorized" which implies not only the access but also the action (use) is authorized. Because I felt that it was more important to emphasize the *unauthorized* nature of an attackers activities, I chose to use the first pair of terms (*unauthorized access* and *unauthorized use*), but it should be understood that *unauthorized use* implies *authorized access*. In addition, it should be understood that *unauthorized access* implies that this access will result in an *unauthorized use*.

### 5.4. A Formal Definition of Computer Security

The choice of perspectives is not a neutral process. There is a dependence on the questions being answered and on the purpose of the investigation. As stated by Landwehr, et al.,

> A taxonomy is not simply a neutral structure for categorizing specimens. It implicitly embodies a theory of the universe from which those specimens are drawn. It defines what data are to be recorded and how like and unlike specimens are to be distinguished. In creating a taxonomy of computer program security flaws, we are in this way creating a theory of such flaws, and if we seek answers to particular questions from a collection of flaw instances, we must organize the taxonomy accordingly [LBM94:214].

The taxonomy presented as part of this research was influenced by wanting to describe, classify and analyze the observed Internet security incidents. That is one of the primary reasons that a taxonomy of *attacks* is being developed. It is also influenced by viewing attacks as processes that, when successful, lead attackers to their desired objectives. This influence, and the above discussions leads to a definition of computer security using the common characteristic of all attacks: the attacker is trying to achieve an objective. The definition used for this research is as follows:

> *Computer security* is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.

---

[8] Suggested by Dr. Thomas A. Longstaff at the CERT®/CC.

This definition provides the desired demarcation of the computer security field. Concerns about computer equipment theft and environmental threats are excluded. Software flaws are included, but only if they result in vulnerabilities to the system that could be exploited to provide unauthorized access or use. Both the means used to gain unauthorized access or use (virus, Trojan horse, telnet, etc.), as well as the ends of attacks (corruption, disclosure, or denial-of-service leading to theft, espionage, fraud, etc.), are included because they require unauthorized access or unauthorized use. The definition also excludes unintentional events [Amo94:2].

*Chapter 6*

# A Taxonomy of Computer and Network Attacks

This chapter presents a brief discussion of the desired characteristics of a taxonomy. This is followed by a critique of current taxonomies in the computer and network security field. These current taxonomies include lists of terms, lists of categories, results categories, empirical lists and matrices. A proposed taxonomy for computer and network *attacks* is then presented. This taxonomy was developed from the criticisms of the current taxonomies, from the definition of computer security presented in Chapter 5, and from a *process* or *operational* viewpoint of *means*, *ways*, and *ends*. From this viewpoint, an *attacker* on computers or networks attempts to reach or "link" to ultimate *objectives*. This link is established through an operational sequence of *tools*, *access*, and *results* that connects these attackers to their objectives. The next chapter uses this *attack* taxonomy, along with other parameters to classify Internet *incidents* (groups of attacks).

## 6.1. Characteristics of Satisfactory Taxonomies

A taxonomy should have classification categories with the following characteristics [Amo94:34]:

1) mutually exclusive - classifying in one category excludes all others because categories do not overlap,
2) exhaustive - taken together, the categories include all possibilities,
3) unambiguous - clear and precise so that classification is not uncertain, regardless of who is classifying,
4) repeatable - repeated applications result in the same classification, regardless of who is classifying,
5) accepted - logical and intuitive so that they could become generally approved,
6) useful - can be used to gain insight into the field of inquiry.

These characteristics can be used to evaluate possible taxonomies. It should be expected, however, for a satisfactory taxonomy to be limited in some of these characteristics. A taxonomy is an approximation of reality that is used to gain greater understanding in a field of study. Because it is an approximation, it will fall short in some characteristics. This may be particularly the case when the characteristics of the data being classified are imprecise and uncertain, as was the data for this study. Nevertheless, classification is an important and necessary process for systematic study.

## 6.2. Toward a Taxonomy of Computer and Network Attacks

As presented in Chapter 1, an *attack* is a single unauthorized access attempt, or unauthorized use attempt, regardless of success. An *incident*, on the other hand, involves a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing. Since incidents are made up of attacks, it is appropriate to develop a taxonomy for *attacks* which can then be used within a broader

classification of *incidents*. A taxonomy of attacks is, however, useful by itself. Such an attack taxonomy may facilitate the development of policy recommendations for increasing Internet security. An attack taxonomy is also useful both in the development of new systems, and in evaluating existing systems.

> By comparing possible categories of attack against the details of the target system of interest, one establishes a means for determining how well that system is likely to stand up to potential security attacks . . . [Amo94:33]

Finally, an attack taxonomy can be used to evaluate the effectiveness of mitigation efforts, such as law enforcement, investigation, disclosure of vulnerability information, incident response, etc.

For this research, the taxonomy will be used to determine the relative frequency of various attack activity. This is presented in Chapter 8.

### 6.3. Current Computer and Network Security Taxonomies

Computer and network security taxonomies do not necessarily focus on attacks, as will be done in the taxonomy developed for this research. For example, some authors focus more narrowly on security flaws or vulnerabilities, which could be used for attacks. Landwehr uses such an approach (to be discussed later). Regardless of whether the taxonomy focuses on attacks or not, they generally all *attempt* to classify attacks, which is the common element of these taxonomies. For purposes of being complete in this discussion, the focus will be on taxonomies involving computer and network security with the assumption that this will include attacks.

**6.3.1. Lists of Terms** - A popular and simple taxonomy of computer and network security attacks is a list of single, defined terms.[1] An example is the following from Cohen [Coh95:40-54]:

| | | | | |
|---|---|---|---|---|
| *Trojan horses* | *Toll fraud networks* | *Fictitious people* | *Infrastructure observation* | *E-mail overflow* |
| *Time bombs* | *Get a job* | *Protection limit poking* | *Infrastructure interference* | *Human engineering* |
| *Bribes* | *Dumpster diving* | *Sympathetic vibration* | *Password guessing* | *Packet insertion* |
| *Data diddling* | *Computer viruses* | *Invalid values on calls* | *Van Eck bugging* | *Packet watching* |
| *PBX bugging* | *Shoulder surfing* | *Open microphone listening* | *Old disk information* | *Video viewing* |
| *Backup theft* | *Data aggregation* | *Use or condition bombs* | *Process bypassing* | *False update disks* |
| *Input overflow* | *Hang-up hooking* | *Call forwarding fakery* | *Illegal value insertion* | *E-mail spoofing* |
| *Login spoofing* | *Induced stress failures* | *Network services attacks* | *Combined attacks* | |

Another list from Icove, et al. [ISV95:31-52]:

| | | | | |
|---|---|---|---|---|
| *Wiretapping* | *Dumpster diving* | *Eavesdropping on Emanations* | *Denial-of-service* | *Harassment* |
| *Masquerading* | *Software piracy* | *Unauthorized data copying* | *Degradation of service* | *Traffic analysis* |
| *Trap doors* | *Covert channels* | *Viruses and worms* | *Session hijacking* | *Timing attacks* |
| *Tunneling* | *Trojan horses* | *IP spoofing* | *Logic bombs* | *Data diddling* |
| *Salamis* | *Password sniffing* | *Excess privileges* | *Scanning* | |

[1] See the Glossary for some common definitions of these terms.

Lists of terms generally fail to have most of the characteristics of a satisfactory taxonomy. First, the terms tend not to be mutually exclusive. For example, the terms *virus* and *logic bomb* are generally found on these lists, but a virus may *contain* a logic bomb, so the categories overlap. Actual attackers also generally use multiple methods. This was confirmed by this research. As a result, developing a comprehensive list of methods for attack would not provide a classification scheme that yields mutually exclusive categories (even if the individual terms were mutually exclusive), because actual attacks would have to be classified into multiple categories. This serves to make the classification ambiguous and difficult to repeat.

A more fundamental problem is that, assuming an exhaustive list could be developed, the taxonomy would be unmanageably long and difficult to apply. It would also not indicate any relationship between different types of attacks. As stated by Cohen,

> ...a complete list of the things that can go wrong with information systems is impossible to create. People have tried to make comprehensive lists, and in some cases have produced encyclopedic volumes on the subject, but there are a potentially infinite number of different problems that can be encountered, so any list can only serve a limited purpose [Coh95:54].

None of these lists has become widely accepted. Part of the reason is that the definitions of individual terms is difficult to agree on. For example, even such widely used terms as *computer virus* have no accepted definition [Amo94:2]. In fact, it is common to find many different definitions.

Finally, this classification scheme provides no structure to the categories. This, combined with the above criticisms, limits its usefulness.

Because of these reasons, lists of terms with definitions are not satisfactory taxonomies for classifying actual attacks.

**6.3.2. Lists of Categories -** A variation of the list of terms with definitions is to list categories. An example of one of the more thoughtful lists of categories is given by Cheswick and Bellovin in their text on firewalls [ChB94:159-166]. They classify attacks into seven categories as follows:

1. Stealing passwords - methods used to obtain other users' passwords,
2. Social engineering - talking your way into information that you should not have,
3. Bugs and backdoors - taking advantage of systems that do not meet their specifications, or replacing software with compromised versions,
4. Authentication failures - defeating of mechanisms used for authentication,
5. Protocol failures - protocols themselves are improperly designed or implemented,
6. Information leakage - using systems such as *finger* or the *DNS* to obtain information that is necessary to administrators and the proper operation of the network, but could also be used by attackers,
7. Denial-of-service - efforts to prevent users from being able to use their systems.

Lists of categories are an improvement because some structure is provided, but this type of taxonomy suffers from many of the same problems as one large list of terms. Authors also tend to make lists within these lists, which makes the approach even more similar to the previous type.

**6.3.3. Results Categories** - Another variation of the list method is to group all attacks into basic categories that describe the results of an attack. An example is a list, such as *corruption*, *leakage*, and *denial*, as used by Cohen [Coh95:54; RuG91:10-11], where corruption is the unauthorized modification of information, leakage is when information ends up where it should not be, and denial is when computer or network services are not available for use [Coh95:55]. Russell and Gangemi use similar categories but define them using opposite terms: 1) *secrecy* and *confidentiality*, 2) *accuracy*, *integrity*, and *authenticity*, and 3) *availability* [RuG91:9-10]. Other authors use other terms, or use these terms differently.

This type of classification scheme has proven to be a useful framework because most individual attacks can be associated uniquely with one of these categories. However, this is not always the case. An example is an intruder who uses computer or network resources without degrading the service of others [Amo94:31]. This example could not be easily associated with one of the three typical categories.

**6.3.4. Empirical Lists** - A variation of the three-category taxonomy of results is to develop a longer list of categories based upon a classification of empirical data. An example of this is the taxonomy developed by Neumann and Parker to classify accounts of actual attacks sent to Neumann at SRI International as part of its Risks Forum ("Risks to the Public in Computers and Related Systems") [NeP89]. Neumann and Parker use eight categories to classify their data. One advantage of this approach is that attacks that would not logically fit into one of the three traditional categories can now be classified. The Neumann and Parker list is as follows (with examples by Amoroso [Amo94:37]):

- External Information Theft (glancing at someone's terminal)
- External Abuse of Resources (smashing a disk drive)
- Masquerading (recording and playing back network transmission)
- Pest Programs (installing a malicious program)
- Bypassing Authentication or Authority (password cracking)
- Authority Abuse (falsifying records)
- Abuse Through Inaction (intentionally bad administration)
- Indirect Abuse (using another system to create a malicious program) [Amo94:37]

Amoroso critiques this list as follows:

> A drawback of this attack taxonomy that should be mentioned is that the eight attack types are less intuitive and harder to remember than the three simple threat types in the simple threat categorization. This is unfortunate, but since the more complex list of attacks is based on actual occurrences, it is hard to dispute its suitability [Amo94:37].

Such a list appears to be suitable because it *can* classify a large number of actual attacks. If carefully constructed, such a list would have categories with the first four desired characteristics: mutually exclusive, exhaustive, unambiguous, and repeatable. However, simply being able to put all of the attacks into a category is not sufficient. As Amoroso notes, since the resulting list is not logical and intuitive, and there is no additional structure showing the relationship of the categories, its acceptance would be difficult and its use limited.

**6.3.5. Matrices** - Perry and Wallich present a classification scheme based on two dimensions: vulnerabilities and potential perpetrators. This allows categorization of incidents into a simple matrix as shown in Figure 6.1, where the individual cells of the matrix represent combinations of *potential perpetrators*: operators, programmers, data entry clerks, internal users, outside users, and intruders, and the *potential effects* : physical destruction, information destruction, data diddling, theft of services, browsing, and theft of information (vulnerabilities) [PeW84; Amo94:35].

| | **Operators** | **Programmers** | **Data Entry** | **Internal** | **Outside** | **Intruders** |
|---|---|---|---|---|---|---|
| **Physical Destruction** | *Bombing Short circuits* | | | | | |
| **Information Destruction** | *Erasing Disks* | *Malicious software* | | | *Malicious software* | *Via modem* |
| **Data Diddling** | | *Malicious software* | *False data entry* | | | |
| **Theft of Services** | | *Theft as user* | | *Unauthorized action* | *Via modem* | |
| **Browsing** | *Theft of media* | | | *Unauthorized access* | *Via modem* | |
| **Theft of Information** | | | | *Unauthorized access* | *Via modem* | |

**Figure 6.1. Example Two-Dimensional Attack Matrix [PeW84]**

The two dimensions of this matrix are an improvement over the single dimension of the results categories presented previously. The two dimensions appear to have mutually exclusive and

perhaps exhaustive categories. The use of the term vulnerability to describe the terms on the left is not generally accepted, and these might better be termed the *results* from exploiting vulnerabilities.

Perhaps more importantly, the terms inside the matrix do not appear to be logical or intuitive. For example, an *outside user* causing *information destruction* is labeled as using *malicious software*. This is a term generally assumed to mean computer viruses, worms or Trojan horses. An outside user, however, could use a variety of other methods to attack, such as commands at the user interface. The other terms inside the matrix have similar problems.

The connection of results to perpetrators is a useful concept which has similarities to a process approach which will be used for the development of a taxonomy in this chapter. The problem in this matrix is that the connection between the two is not properly made.

Perhaps the most ambitious matrix approach to a taxonomy is found in Landwehr et al. [LBM94]. They present a taxonomy of computer security flaws (conditions that can result in denial-of-service, or the unauthorized access to data [LBM94:211]) based on three dimensions: *Genesis* (how a security flaw finds its way into a program), *Time of Introduction* (in the life-cycle of the software or hardware), and *Location* (in software or hardware). The first of these three dimensions, *Genesis*, is shown in Figure 6.2. In this dimension, security flaws are divided into two broad categories. On the top of the figure are the flaws that are "intentionally" introduced into the software, either "maliciously," such as through a Trojan horse, trapdoor, logic/time bomb, or "non-maliciously," through a covert channel. The bottom of the figure shows the other broad category: "inadvertent" software programming errors.

The Landwehr, et al., taxonomy includes numerous terms, such as Trojan horse, virus, trapdoor, and logic/time bomb for which there are no accepted definitions. As a result, the taxonomy suffers from some of the same problems in ambiguity and repeatability found in the simpler taxonomies described earlier. For example, classifying a virus as a *Trojan horse* is not universally accepted. In fact, some authors view the terms as mutually exclusive. The taxonomy also includes several "other" categories, which means the flaws that are identified may not represent an exhaustive list. An example of an exploitable flaw would be a design error which is implemented correctly in the code. This does not appear to have a place in the taxonomy.

The procedure for classification using the Landwehr, et al., taxonomy is not unambiguous when actual attacks are classified. This can be seen by attempting to classify the Internet Worm[2] using the

[2] The Internet Worm is the common name given to a self-replicating program released on the Internet by a graduate student, Robert Morris, from Cornell University on November 2, 1988.

Genesis dimension shown in Figure 6.2. The Internet Worm program was self-replicating, so it would logically be classified as Intentional, Malicious, Trojan Horse and Replicating. However, the code took advantage of several known software bugs in the UNIX and VAX operating systems to bypass system security. The attack could, therefore, also be classified in several of the Inadvertent categories. In addition, the worm had provisions for a Logic Bomb (although one was not present), which is a different classification. Finally, the worm used a password cracking routine to bypass security which would be difficult to classify in this taxonomy [RuG91:3-5].

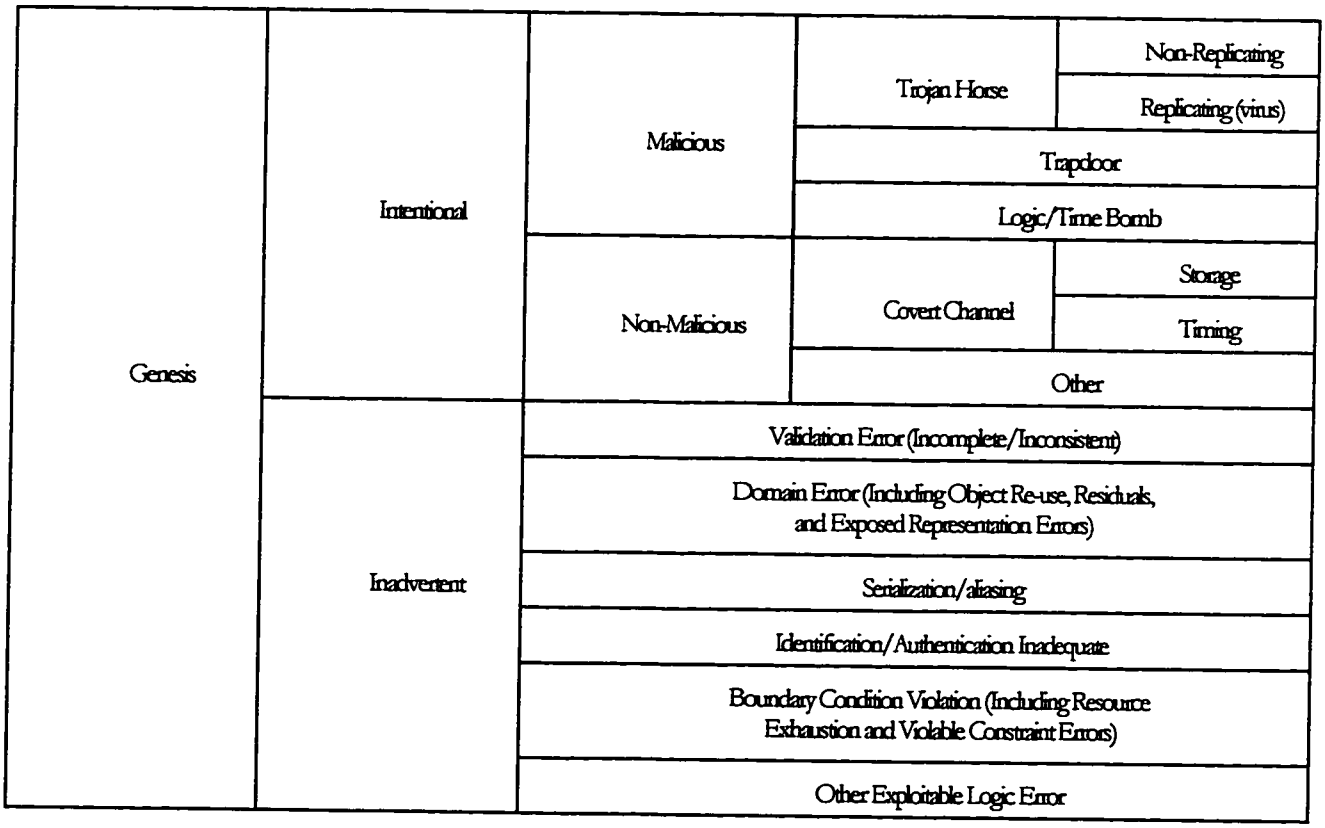


**Figure 6.2. Security flaw taxonomy: Flaws by Genesis [LBM94:251]**

It is likely that Landwehr, et al., would not recommend that an entire attack be classified in the manner just shown. Instead, the approach should be to classify the individual parts of the attack. Again using the Internet Worm as an example, each individual part should be classified. The Worm itself would be classified the same as above (intentional, malicious, Trojan horse, replicating), but the vulnerabilities exploited would be classified in other parts of the matrix. This means an attack would generally be classified in multiple categories. This problem is difficult, if not impossible, to eliminate. The reality of Internet attacks is that multiple methods are used. This same problem is found in the taxonomy developed for this research (Section 6.4). To help with this problem, the

taxonomy for this research is in two parts or levels: a taxonomy for individual attacks (this chapter), and a classification of incidents (groups of attacks) which uses the attack taxonomy along with other parameters.

Perhaps the most significant limitation of the Landwehr, et al., taxonomy is one of its basic logic. When dealing strictly with software errors (bugs), the taxonomy seems logical and intuitive (the *Inadvertent* part of Figure 6.2). The categories in the *Intentional* portion of Figure 6.2, however, are not so obvious. In this case, the logic that was apparently used was that various types of software can introduce flaws in the system which could then be exploited. The logic is not intuitive. For example, it does not logically follow that the introduction of a virus into a computer system results in the creation of a flaw in the system.

The last problem with the Landwehr, et al., taxonomy is a matter of usefulness. It appears perhaps to be limited to determining the rates at which each flaw occurs. This results from the limited logical connection between the various categories. For all of its complication, this means the Landwehr, et al., taxonomy is primarily a sophisticated list, which has the problems and limitations of the lists discussed earlier.

**6.3.6. A Process-Based Taxonomy** - The taxonomy developed as part of this research is broader in scope than Landwher, et al., because it does not attempt to enumerate all computer security flaws, or to enumerate all possible methods of attack, but rather attempts to provide a broad, inclusive framework. The intention was to reorient the focus of the taxonomy toward a process, rather than a single classification category, in order to provide both an adequate classification scheme for Internet attacks, and also a taxonomy that would aid in thinking about computer and network security.

Stallings presents a simple process model that classifies security threats [Sta95:7]. The model is narrowly focused on information in transit, but it is instructive to examine. Stallings defines four categories of attack as follows:

1. Interruption - An asset of the system is destroyed or becomes unavailable or unusable
2. Interception - An unauthorized party gains access to an asset
3. Modification - An unauthorized party not only gains access to, but tampers with an asset
4. Fabrication - An unauthorized party inserts counterfeit objects into the system [Sta95:7]

Interception is viewed by Stallings as a *passive* attack, and interruption, modification and fabrication are viewed as *active* attacks. These four categories are illustrated in Figure 6.3. While this is a simplified view with limited utility, its emphasis on the *process* of attack is useful. The approach

used in Section 6.4 to develop a more comprehensive taxonomy was to classify an attack based on the broader process or operational perspective of "means, ways, and ends," discussed in Chapter 5. In the following discussion, I refer to this perspective as an "operational" viewpoint or approach.

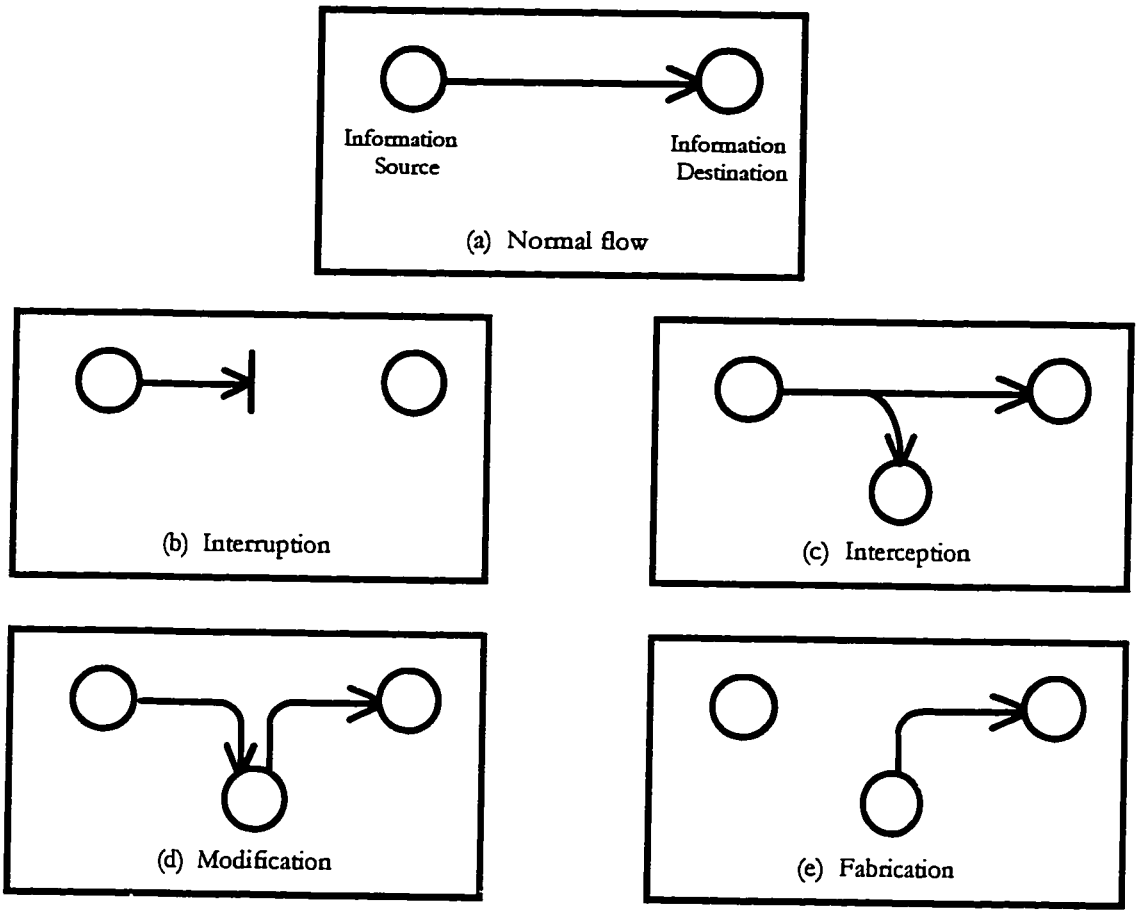


**Figure 6.3. Security Attacks [Sta95:8]**

### 6.4. A Taxonomy of Computer and Network Attacks

From an operational viewpoint, an attacker on computers or networks attempts to reach or "link" to ultimate objectives or motivations. This link is established through an operational sequence of "means, ways, and ends" that connects attackers to objectives. For the computer security field it is appropriate to use different, more descriptive, terms instead of "means, ways, and ends." For this taxonomy, the terms will be "tools, access, and results." These link together attackers and objectives in the process of computer and network attacks as shown in Figure 6.4.


**Figure 6.4. Operational Sequence of Computer and Network Attack**

This operational sequence will be expanded in this section to provide a taxonomy that will then be used to classify Internet attacks.

**6.4.1. Attackers and Their Objectives** - *People* attack computers. They do so through a variety of methods and for a variety of objectives. As stated by Icove, et al.,

> At one extreme there are the teenage "joyriders," playing around with their computers and modems. At the other extreme are ultra-dangerous criminals who break into classified military systems or corporate databases, for reasons of terrorism or military or corporate espionage. In the middle are disgruntled or fired employees, looking to wreak revenge on an employer, as well as hired [hackers] who break into systems under contract [ISV95:61].

Attackers are the obvious beginning point, the originators, for computer and network attacks. They could be identified by who they are and where they come from, such as being a high school student from a certain city, a former employee of a company, or a foreign national. They could also be identified by their capabilities, such as was done by Tiley, who states the "people you need to guard your data and hardware from fall into four basic categories:" thieves, the merely curious with low technical competence, the curious with high technical competence, and the determined hacker with high technical competence [Til96:49].

Russell and Gangemi present two broad categories of attackers (which they call "threats"): *insiders* and *outsiders*. Insiders include employees, former employees, students, etc. Outsiders consist of foreign intelligence agents, terrorists, criminals, corporate raiders and hackers [RuG91:14-15]. Cohen identifies 26 categories of "disrupters"[3] [Coh95:57-71]. Similar lists are presented by Schwartau [Sch94:215-248] and others.

An alternative approach, and the one taken here, is to identify attackers by what they typically do. Icove, et al., present a simple classification based on three categories: hackers, criminals, and vandals. They differentiate these categories as follows:

> To some extent, they are best differentiated by motivation: The main motivation of a [hacker] is *access* to a system or data; the main motivation of a criminal is *gain*; the main motivation of a vandal is *damage* [ISV95:62].

Hackers are distinguished because they are more interested in the challenge of defeating a system's security rather than by the potential for personal gain. Corporate raiders and professional criminals, on the other hand, are motivated by the potential for financial gain. Spies and terrorists

---

[3] Insiders, private detectives and reporters, consultants, whistle blowers, hackers, club initiates, crackers, tiger teams, competitors, maintenance people, professional thieves, hoods, vandals, activists, crackers for hire, deranged people, organized crime, drug cartels, terrorists, spies, police, government agencies, infrastructure warriors, nation states and economic rivals, military organizations, and information warriors.

seek political gain [RuG91:15], although terrorists are distinguished because they seek to gain politically by creating fear through provocative acts. Finally, vandals are characterized by anger directed "most often at a particular organization, but sometimes life in general [ISV95:64]."

One problem with classifying attackers motivations into these three categories (hackers, criminals, and vandals) is that, regardless of the motivation, all of these categories describe criminal behavior. As such, separating hackers and vandals from criminals is not consistent. I have avoided this inconsistency by not using the term criminal in the taxonomy. Instead, I have divided attackers into the following six categories:

1. Hackers - break into computers primarily for the challenge and status of obtaining access
2. Spies - break into computers primarily for information which can be used for political gain
3. Terrorists - break into computers primarily to cause fear which will aid in achieving political gain
4. Corporate raiders - employees of one company break into computers of competitors for financial gain
5. Professional Criminals - break into computers for personal financial gain (not as a corporate raider)
6. Vandals - break into computers primarily to cause damage

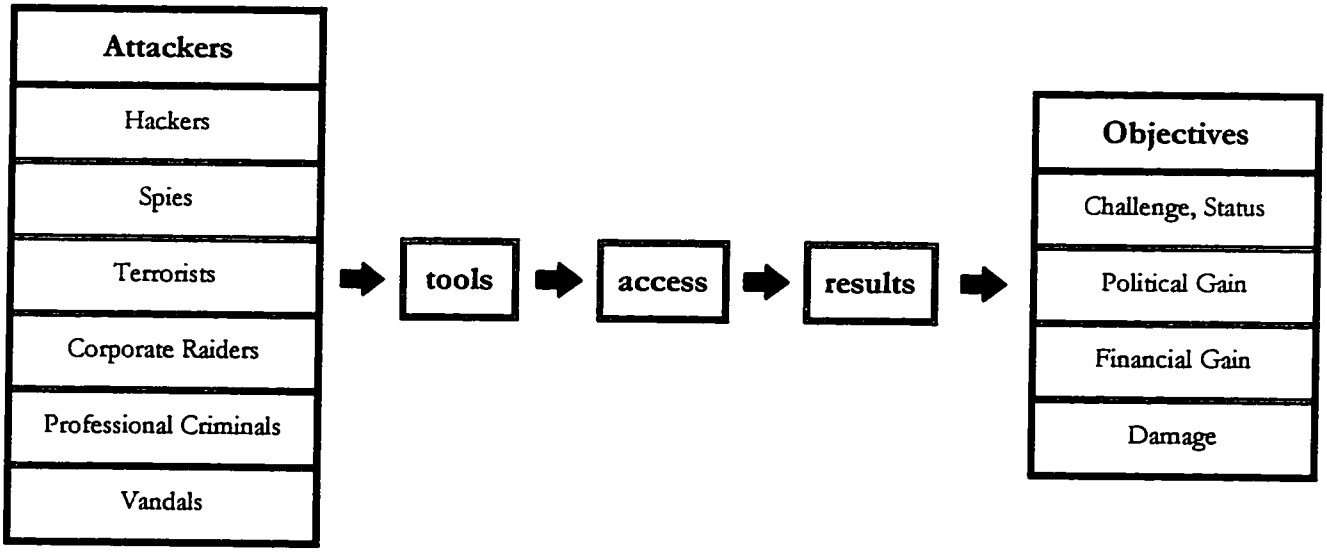


**Figure 6.5. Attackers and their Primary Motivations[4]**

These six categories of attackers and their four categories of primary motivations or objectives are shown in Figure 6.5. These categories of attackers and objectives serve as the two ends of the operational sequence of computer and network attacks. In between are the "tools, access, and results" which link attackers to their ultimate objectives, or motivations.

[4] I have elected to use the term "hacker" in this taxonomy because it is the most common and widely-understood term. I realize the term used to have a positive connotation.

**6.4.2. Access** - The definition of computer security (Chapter 5) leads directly to the center of the connection between attackers and their objectives in this taxonomy: unauthorized access or unauthorized use. This is shown in Figure 6.6, which is an expansion of the access block in Figure 6.5. The arrows show that all attackers must either obtain unauthorized access, or use a system in an unauthorized way, in order to make the connection to their objective. As was discussed in Chapter 5, the unauthorized access or use is to *processes*, or to files or data in transit *through processes*. These are depicted in Figure 6.6. CERT®/CC incidents were all classified according to the highest "level" of access the attacker achieved (see Chapter 5). The two highest levels were to superuser or root privileges, and to a user account.

It is important to include both unauthorized access and unauthorized use in the "ways" of attack. The most widely known Internet security incidents involve unauthorized access, but abusing authorized access may also be a widespread problem. Russell and Gangemi estimate that "as many as 80 percent of system penetrations are by fully authorized users who abuse their access." [RuG91:16]. The CERT®/CC incident records presented in Chapter 7, however, do not reflect this, although they do show it has been a problem, and it has the potential to be a greater problem.

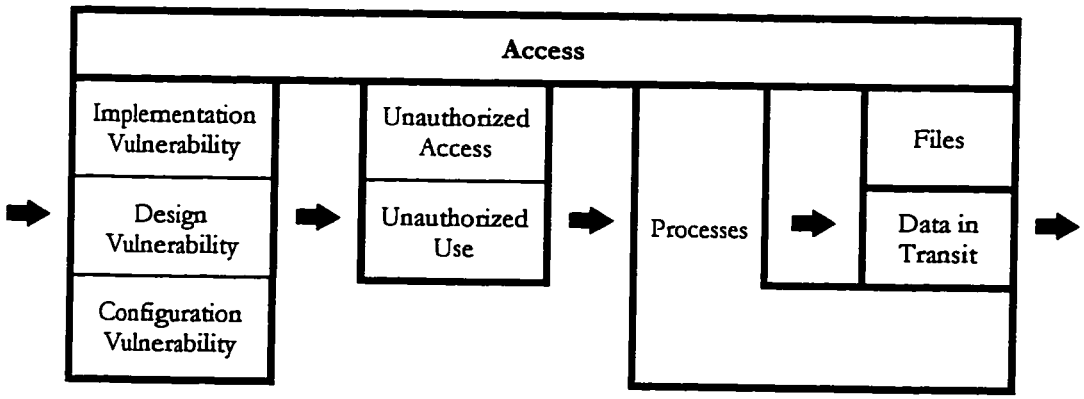


**Figure 6.6. Access for Attack**

In order to reach the desired process, an attacker must take advantage of a computer or network *vulnerability*, which is a flaw allowing the unauthorized access or use [Amo94:2]. A vulnerability may arise in three ways. The most well-known way is through a software bug, which is an implementation problem where the design is satisfactory, but an error has been made in its implementation in software or hardware. Numerous examples have occurred in the Unix systems which have formed the basis of the Internet, such as the many problems in the *sendmail* program which often could be used to gain unauthorized access to host computers [GaS96:497].

The second way a vulnerability may arise is from the design itself, which is potentially more serious and difficult to correct. In this case, the vulnerability is inherent in the design and therefore

even a perfect implementation of the design in software or hardware will result in a vulnerability. The Internet *sendmail* program is also an example of this. Even when it has no software errors, electronic mail generated by *sendmail* can be used in an unauthorized manner to attack a system, such as through repetitive mailings (*mail spam*) which cause a denial-of-service (see Chapter 11).[5]

The third way a vulnerability may arise is through a configuration error. These are very common occurrences. Many vendors ship their software in a "trusted" state which is convenient for users, but may also be highly vulnerable to attack. Configuration errors could include such security problems as system accounts with default (and well known) passwords, with default "world write" permission for new files, and with vulnerable services enabled [ABH96:196].

**6.4.3. Results** - Between obtaining access and the attacker's objectives, we conceptualize the *results* of attack. At this point in the sequence of an attack, the attacker has access to the desired processes, files, or data in transit. The attacker is now free to exploit this access to alter files, deny service, obtain information, or use the available services. Figure 6.7 depicts these results of attack, which includes the three traditional categories of corruption, disclosure and denial, but also includes a fourth category: theft of service [Amo94:3-4,31; RuG91:9-10; Coh95:55-56].

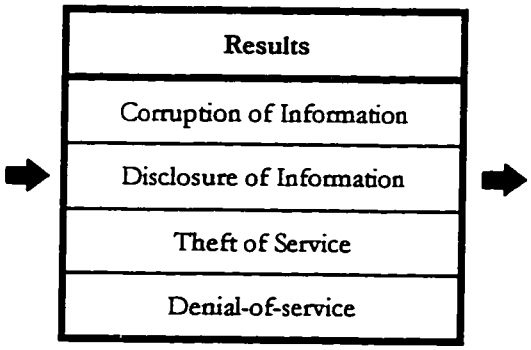


**Figure 6.7. Results of Attack**

The results of attack categories are defined as follows:

*Corruption of Information* - any unauthorized alteration of files stored on a host computer or data in transit across a network [Amo94:4].

*Disclosure of Information* - the dissemination of information to anyone who is not authorized to access that information [RuG91:9].

*Theft of Service* - the unauthorized use of computer or network services without degrading the service to other users [Amo94:31].

*Denial-of-service* - the intentional degradation or blocking of computer or network resources [Coh95:55].

---

[5] It could be argued that this example is a bounds checking problem that would therefore be classified as a implementation vulnerability. The point is, however, that if bounds checking were not part of the design, then this should be considered a design vulnerability.

**6.4.4. Tools** - The final connection to be made in the operational sequence that leads attackers to their objectives is the *tools* of attack. This is also the most difficult connection to make because of the wide variety of methods available to exploit vulnerabilities in computers and networks. When authors make lists of methods, they often are making lists of tools. As discussed earlier, these lists have limited utility. The approach taken here was to established the following categories (see Figure 6.8):

*User Command* - the attacker enters commands at a command line or graphical user interface.

*Script or Program* - scripts and programs initiated at the user interface to exploit vulnerabilities.

*Autonomous Agent* - the attacker initiates a program, or program fragment, which operates independently from the user to exploit vulnerabilities.

*Toolkit* - the attacker uses a software package which contains scripts, programs, or autonomous agents that exploit vulnerabilities.

*Distributed Tool* - the attacker distributes tools to multiple hosts, which are then coordinated to perform an attack on the target host simultaneously after some time delay.

*Data tap* - where the electromagnetic radiation from a cable carrying network traffic, or from a host computer is "listened" to by a device external to the network or computer.

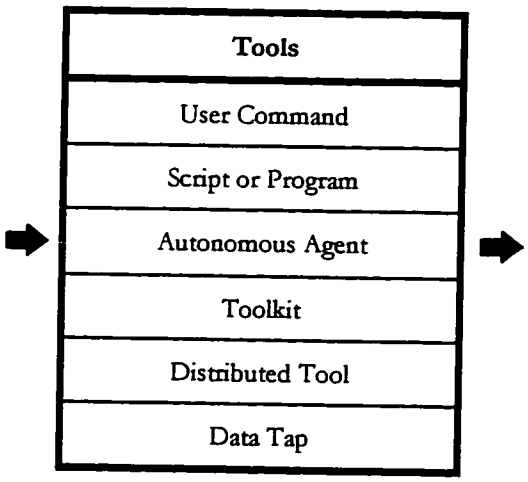


**Figure 6.8. Tools of Attack**

***6.4.4.1 User Command*** - Until recently, the most common means of attack was for the attacker to simply enter commands at the keyboard. An example is opening a *telnet* session to a target computer and attempting to log in to a user or the superuser account. Access could be gained by such widely-varying techniques as guessing passwords, or entering long strings of characters to take advantage of a software bug.

***6.4.4.2 Script or Program*** - At the user command interface, attackers can also make use of scripts or programs for the automation of commands. The simplest way to automate commands is

to use a *script*, which is a series of commands entered into a file which can be executed by a Unix shell. An example of a *program* in common use is *crack*, which is used by system administrators to check for bad passwords, but is also used by attackers to crack passwords on targeted hosts.

An additional type of tool often employed at the user command interface is known as a *Trojan horse*, which is a program that an attacker may copy over another program on the target system. Analogous to the wooden horse at the battle of Troy, a Trojan horse program performs like a real program a user may wish to run, such as *login*, a game, a spreadsheet, or an editor. In addition to performing as the user expects, however, the Trojan horse program also performs unauthorized actions, such erasing files, copying information, or logging user passwords in a file [ISV95:45].

***6.4.4.3 Autonomous Agent*** - Autonomous agents are the most widely publicized of the means of attack. What distinguishes an autonomous agent from other scripts or programs is that the program selects target systems on its own. For example, a *Trojan horse* program that has been placed on a target system may operate independently to say, record passwords, but it was placed on the host by a user. In contrast, an autonomous agent contains program logic to make an independent choice of what host to attack.

The most well-known autonomous agent is the *computer virus* [Par90:544]. Although there is no agreed upon definition, the general consensus is summarized by Spafford, et al.:

> ...a computer virus is a segment of machine code (typically 200-4,000 bytes) that will copy its code into one or more larger "host" programs when it is activated. When these infected programs are run, the viral code is executed and the virus spreads further. Viruses cannot spread by infecting pure data; pure data is not executed. However, some data, such as files with spreadsheet input or text files for editing, may be interpreted by application programs. For instance, text files may contain special sequences of characters that are executed as editor commands when the file is first read into the editor. Under these circumstances, the data is "executed" and may spread a virus. Data files may also contain "hidden" code that is executed when the data is used by an application, and this too may be infected. Technically speaking, however, pure data cannot itself be infected [SHF90:316].

An alternative type of autonomous agent does not insert itself into other programs. It is called a *worm*, which operates separately as described by Spafford, et al.:

> Unlike viruses, worms are programs that can run independently and travel from machine to machine across network connections; worms may have portions of themselves running on many different machines. Worms do not change other programs, although they may carry other code that does, such as a true virus [SHF90:317].

***6.4.4.4 Toolkit*** - In recent years, attackers have made increasing use of software packages commonly referred to as "toolkits." Toolkits group scripts, programs and autonomous agents together, often with a user-friendly graphical user interface. What distinguishes toolkits from user

commands, scripts or programs (the previous classifications) is that these are grouped together in a toolkit – a toolkit contains a group of tools. A widely used Internet toolkit is *rootkit*, which contains a sniffer and Trojan horse programs that can be used to hide activity and provide backdoors for later use.

***6.4.4.5 Distributed Tool*** [6] - A distributed tool is used to attack a host simultaneously from multiple hosts. An attack using a distributed tool is prepared by copying attack tools to surrogate sites distributed across the Internet. The attack itself begins with the synchronization of the clocks used by each of the surrogate attack tools. The timers are set so that each tool will attack a single victim site at a pre-defined time.

It is difficult to determine the origin of an attack that is the result of using a distributed tool. The site initiating the attack typically severs any connection to the surrogate sites before the attack begins. As a result, tracing the packets backwards through the routers to find the source of the attack will fail because the attack has multiple physical sources (not just multiple source IP addresses), and is not part of any intruder activity at the sites sending the attack packets.

> The difference between a coordinated attack tool and other attack tools is the distributed and time-delayed nature of the attack. It represents a meta-attack tool category that can be used to thwart common security mechanisms that rely on straight-forward attack strategies. Of course, new strategies can attempt to trace to the coordinated attack source, but that is much more difficult and the coordinated attacker has the advantage in the number of indirections that can be set up. It is also possible to spoof the source address of the coordination tool to prevent tracing from the mid-points to the actual origination point - and since that is not an active connection at the time of the attack, no active tracing is possible. The only response is to maintain a history of packet traces on the network, which is prohibitively expensive.[7]

A typical defense against attack is to trace incoming packets to their origin and then to block incoming attempts from that subnetwork. This creates a chance for an additional, denial-of-service form of attack. This is accomplished by the attacker using surrogate sites that correspond to clients of the attacked site. When the attacked site blocks the surrogate sites, legitimate clients are denied their service also.

***6.4.4.6 Data Tap*** - Electromagnetic devices such as host computers and network cables generate magnetic fields that can be exploited to reveal the information in the memory of the computer (particularly data displayed on the terminal), or to reveal data in transit. This is different

---

[6] This discussion relies heavily on information provided by Dr. Thomas A. Longstaff, CERT®/CC.

[7] Taken from e-mail by Dr. Thomas A. Longstaff, CERT®/CC, February 20, 1997.

from the other tools because it is a "physical" form of attack instead on an attack using software over a network. It is necessary to include this category for completeness, but as was stated earlier, the CERT®/CC records do not contain any evidence of such attacks.

There are numerous other tools that could be discussed, but they generally all fit into the categories shown in Figure 6.8. Admittedly, this takes what many authors have as a very long list of means and reduces it to five categories; however, it is hoped that this will be a more useful approach which may lead to some insights into computer security.

**6.4.5. The Complete Taxonomy of Computer and Network Attacks** - Figure 6.9 presents the complete taxonomy. This taxonomy depicts a simplification of the path an attacker must take in order to accomplish the attacker's objectives. To be successful, an attacker must find one or more paths that can be connected, perhaps simultaneously. As the formal definition presented earlier indicates, computer security is preventing attackers from achieving objectives by making any complete connections through the steps depicted. More specifically, computer security efforts are aimed at the six blocks of the taxonomy.

Aiming at the first block, *attackers*, law enforcement agencies, system administrators and others attempt to determine who the attackers are and where they are located. Once this is determined, the attackers could be subjected to investigation, prosecution and punishment. Other efforts can be made to prevent attackers from using computer and network resources, such as through closing of accounts or preventing access to network connections.

When *tools* are found in use they can be removed. For example, users and system administrators are encouraged to use *virus-checking* software to detect and eliminate autonomous agents. Systems can be monitored closely to detect the presence of Trojan horses, or other unauthorized files. Processing can be monitored for unauthorized operation of software, such as password crackers or sniffers. User commands can be monitored and logged. Such monitoring could be used to warn of attack, and logging could be used to investigate after an attack. Systems can also be monitored and filtered for the use of specific forms of attack. Examples of these are IP spoofing packets, mail spam, and attack tools found in common toolkits.

*Access* to systems can be prevented in two ways. First is by a vigorous program to discover and eliminate design, implementation and configuration vulnerabilities. Systems administrators are key to this effort. They must keep current on the latest problems that are discovered. They must ensure the system and all its files are configured correctly, that software bugs are patched, and insecure software is eliminated or restricted. The second method to prevent access is to ensure

access controls on files and processes are properly implemented. This includes a wide range of controls, from strong passwords and secure password files, to correct default permissions on files. Unauthorized access can also be reduced by narrowing the number of processes that do not have access controls, and by monitoring how processes are being used.

The *results* of an attack can be mitigated by limiting what a successful attack could accomplish. For example, sensitive files could be encrypted so, even if an attacker succeeds in accessing these files, information will not be disclosed -- although this may not provide any protection from the files being corrupted. Files can also be backed up, mitigating any corruption of information, and systems can be carefully monitored for any signs of theft or denial-of-service. Mitigation efforts can also be used in the last block, *objectives*.

### 6.5. Summary of the Taxonomy of Computer and Network Attacks

A taxonomy of computer and network attacks was developed for this research in order to classify Internet security incidents. The complete taxonomy is summarized in Figure 6.9.

A taxonomy is an approximation of reality that is used to gain greater understanding of a field of study. A taxonomy should have classification categories with the following characteristics:

1) mutually exclusive - classifying in one category excludes all others because categories do not overlap,
2) exhaustive - taken together, the categories include all possibilities,
3) unambiguous - clear and precise so that classification is not uncertain, regardless of who is classifying,
4) repeatable - repeated applications result in the same classification, regardless of who is classifying,
5) accepted - logical and intuitive so that they could become generally approved,
6) useful - can be used to gain insight in to the field of inquiry.

A popular and simple taxonomy of computer and network security attacks is a list of single, defined terms. Variations of this approach include lists of categories. There are several problems that limit the usefulness of these approaches including 1) the terms not being mutually exclusive, 2) an exhaustive list being difficult to develop and unmanageably long, 3) the definitions of individual terms being difficult to agree on, and 4) there being no structure to the categories.

An alternate categorization method is to structure the categories into a matrix. The procedure for classification using these taxonomies, however, is not unambiguous when actual attacks are classified. In addition, the logic is not intuitive, and the classifications are limited in their usefulness.

The taxonomy developed as part of this research does not attempt to enumerate all computer security flaws, or to enumerate all possible methods of attack, but rather to reorient the focus of the taxonomy toward a process, rather than a single classification category.

The final taxonomy presented was developed from the specific definition of computer security (Chapter 5), from the criticisms of the current taxonomies, and from a *process* or *operational* viewpoint. From this viewpoint, an *attacker* on computers or networks attempts to link to ultimate *objectives* or motivations. This link is established through an operational sequence of *tools*, *access*, and *results* that connects these attackers to their objectives as shown in Figure 6.9.

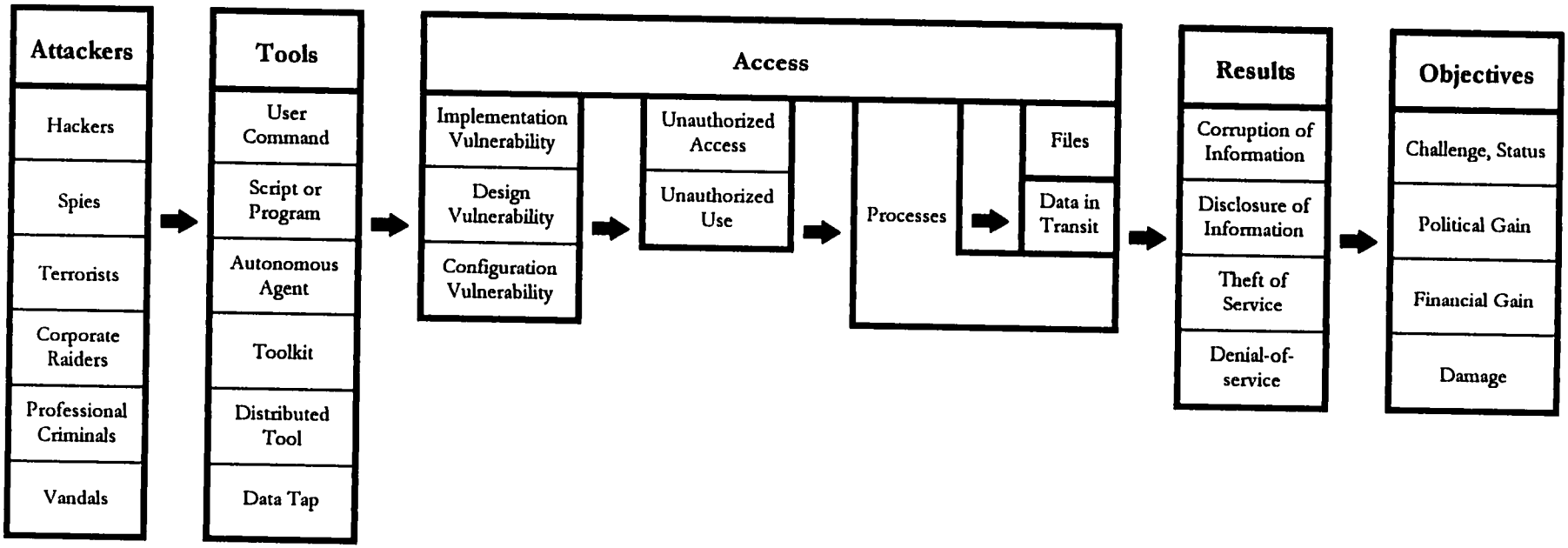


**Figure 6.9. Complete Computer and Network Attack Taxonomy**

*Chapter 7*

# Classification of Internet Incidents and Internet Activity

As stated in Chapter 1, an *attack* is a single unauthorized access attempt, or unauthorized use attempt, regardless of success. A taxonomy of such attacks was presented in the previous chapter. An *incident*, on the other hand, involves a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing. Because of these differences, a taxonomy of *attacks* is inadequate to classify actual Internet *incidents*, although it can be used to classify the attacks that are within an incident.

What we are really interested in, however, is even broader in scope: total Internet incident *activity*. A taxonomy of attacks is also inadequate to classify this total Internet *activity*. In some sense, the classification of an attack indicates something about the type or *quality* of an incident. What is also needed is some measure of *quantity* or severity that distinguishes incidents from one another, and when accumulated, gives an indication of overall Internet security.

This chapter discusses several alternative methods of classifying incidents both by using the taxonomy of attacks to give some indication of the type or quality of the incident, and with quantitative measures that indicate the severity of an incident, and of total Internet activity. At the most basic level, Internet activity is indicated by the number of incidents reported. Reporting date, however, is an inaccurate representation of total activity because of the lack of information about quality, time, duration, number of sites, and severity. One improvement is to classify each incident according to the type of unauthorized access or unauthorized use characteristic of the incident. Normalizing the number of incidents to the size of the Internet also gives some indication of whether security is becoming relatively more or less of a problem. Sites per day is an alternative measure that includes duration and number of sites for an improved indication of Internet activity.

## 7.1. Number of CERT®/CC Incidents

The number of incidents per year in the reconstructed CERT®/CC incident records is shown in Figure 7.1. The 8 incidents shown in 1988 all took place in December. Figure 7.1 therefore shows a total of 4,567 incidents over a 7 year period. These incidents range from false alarms to large incidents involving break-ins at the root level.

The low number of incidents reported to the CERT®/CC in 1989 perhaps indicates that the CERT®/CC took some period of time to become established and well known. After this time, the number of incidents increased each year at a rate between 41% (1991 to 1992) and 62% (1993 to

1994). The exception to this took place between 1994 and 1995 when the number of incidents actually decreased slightly.

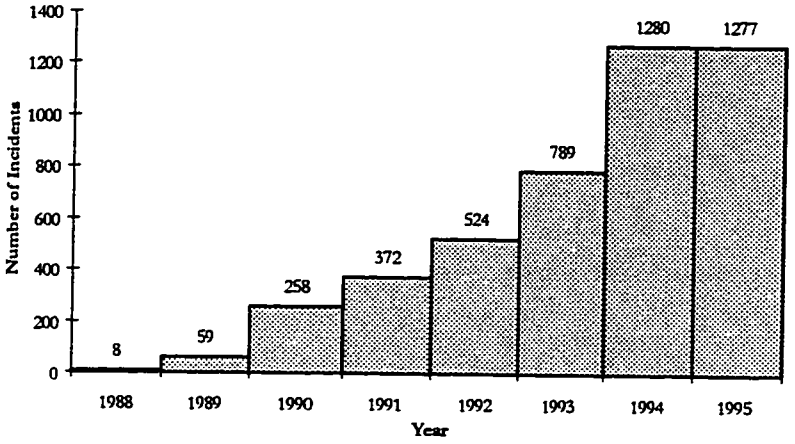


**Figure 7.1. CERT®/CC Incidents per Year**

The change in the number of incidents over this period is seen more clearly in Figure 7.2, which shows the number of incidents by month. This figure shows a relatively steady increase through 1989 and 1990, a leveling off during 1991, and sharp increases at the beginning of 1992 and at the end of 1993. The monthly incident rate peaks in the early part of 1994 at around 140 incidents per month. This drops off to an average of around 100 per month by the middle of 1995. Beginning in 1992, Figure 7.2 also appears to show some indication of seasonal variation, with apparent peaks in the winters and lower rates in the summers.

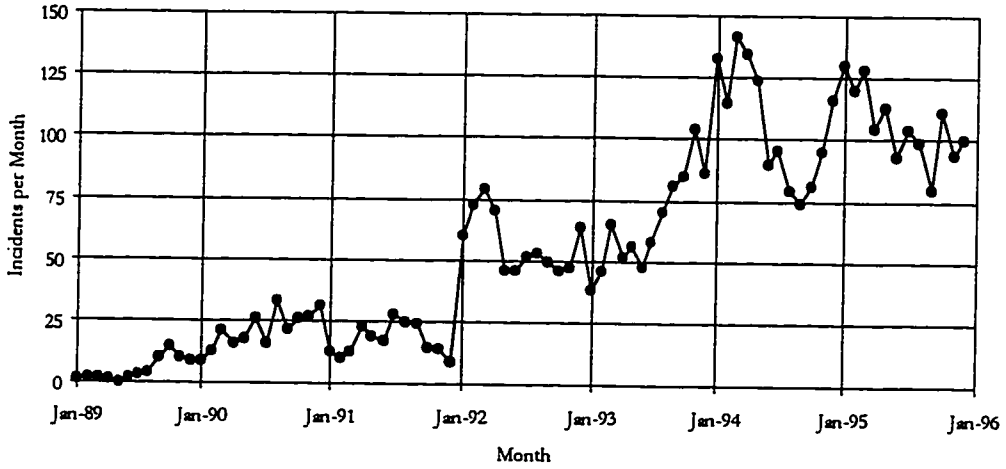


**Figure 7.2. CERT®/CC Incidents by Month, 1989 - 1995**

Although they use common approaches to reporting the numbers of incidents,[1] neither Figure 7.1 nor Figure 7.2 is a good indication of the activity at the CERT®/CC, or of security incidents on the Internet. There are several problems. First, the incidents were plotted according to the date they were reported to the CERT®/CC. But the reporting date to the CERT®/CC was often not the same date as the start of the actual incident. Sometimes an incident began on the same day it was discovered and reported. For other incidents, however, the actual beginning was well before it was discovered or reported. This could range from a few days to many months. This means that Figures 7.1 and 7.2 are an inaccurate representation of the incidents in *time*.

The other problems are more serious in that Figures 7.1 and 7.2 are based on the assumption that all the incidents are comparable – that they are all similar. This was in fact not the case. There were wide variations in duration, in the number of sites involved, and in the severity or success of the attack. With respect to duration, the incidents in the CERT®/CC records varied considerably. Many lasted only a day or two, while others lasted weeks or months. In fact, the longest incident in the CERT®/CC records lasted nearly two years. Although more than 60% of incidents involved only two sites (the attacking site and the attacked site),[2] there was considerable variation in the number of sites involved in the other incidents, with the largest incident actually involving more than 1,500 sites. Finally, and perhaps most importantly, the severity of the incidents ranged widely, from false alarms, through unsuccessful attempts, to successful attacks at the account level, or successful attacks at a level with system privileges (the root level). This means that Figures 7.1 and 7.2 are an inaccurate representation of the incidents in *duration*, *number of sites*, and *severity*.

### 7.2. Classification of Incidents

Chapter 6, Figure 6.9, presents the taxonomy developed as part of this research. This taxonomy was used as a guideline to classify each incident (discussed in this section), and to extract data from each incident (discussed in Chapter 8). The information in the CERT®/CC records was limited and, therefore, only a limited classification could be done. However, in 1992, CERT®/CC personnel began to classify the incidents according to "Method of Operation" (*MO*). This aided significantly in the classification process. This *MO* field was a list of terms entered into all summary

[1] A typical example of this approach is Icove, et al., who report that "Since the CERT® was first established, the organization has reported more computer security incidents each year – less than 200 in 1989, about 400 in 1991, 1,400 in 1993, and around 2,000 in 1994. And those sites reporting break-ins are only a small percentage of those affected [ISV95:14]."

[2] A little more than 2% of the incidents reported to the CERT®/CC actually involved only *one* site – where the target site was also the location of the attacker.

files which could be related to the taxonomy in two ways. First, it was generally used to describe the level to which unauthorized access was obtained at the site (along with the methods used to gain such access), or to describe the unauthorized use of the site (also along with methods used). As part of this research, incidents previous to 1992 were also classified using the same CERT®/CC *MO* terms. The remainder of this section divides the total Internet activity reported to the CERT®/CC into categories within the access block of the taxonomy (see Figure 6.9).

**7.2.1. False Alarms** - The broadest classification of CERT®/CC incidents was into "actual" incidents, and "false alarms." Of the 4,567 incidents reconstructed from the CERT®/CC records, 268 (5.9%) were determined to be false alarms. Typically in these false alarm incidents, a site reported some activity or anomaly that later proved not to be a security incident. Examples are a series of login attempts initially thought to be unauthorized, or anomalous system operation that later proved to be a local software bug or configuration error. Figures 7.1 and 7.2 included these false alarms, but they are plotted separately in Figure 7.3, which shows how small the number of false alarms was. They were, however, numerous enough (5%) to make the reduction in the number of actual incidents between 1994 and 1995 more pronounced, because the number of false alarms increased during this time, both in absolute numbers and as a percentage of total incidents.

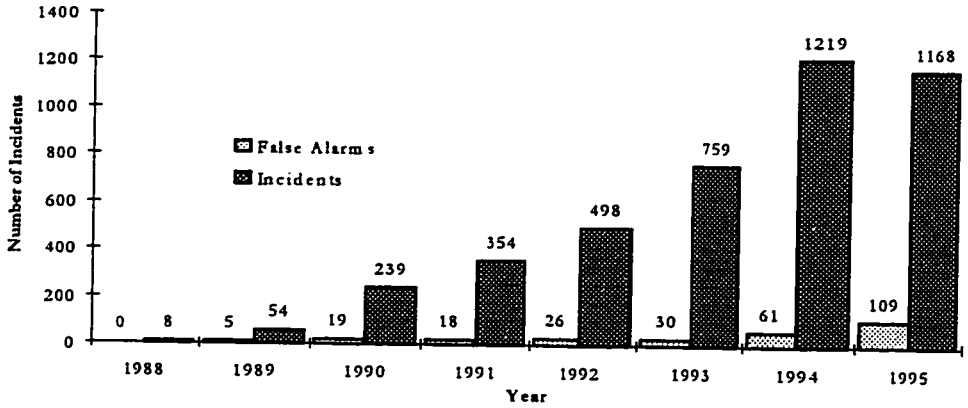


**Figure 7.3. CERT®/CC Incidents and False Alarms per Year**

Figure 7.4 shows the false alarms for each year as a percentage of total incidents. Unless otherwise noted, no false alarms are in any statistics or discussions in the remainder of this paper.

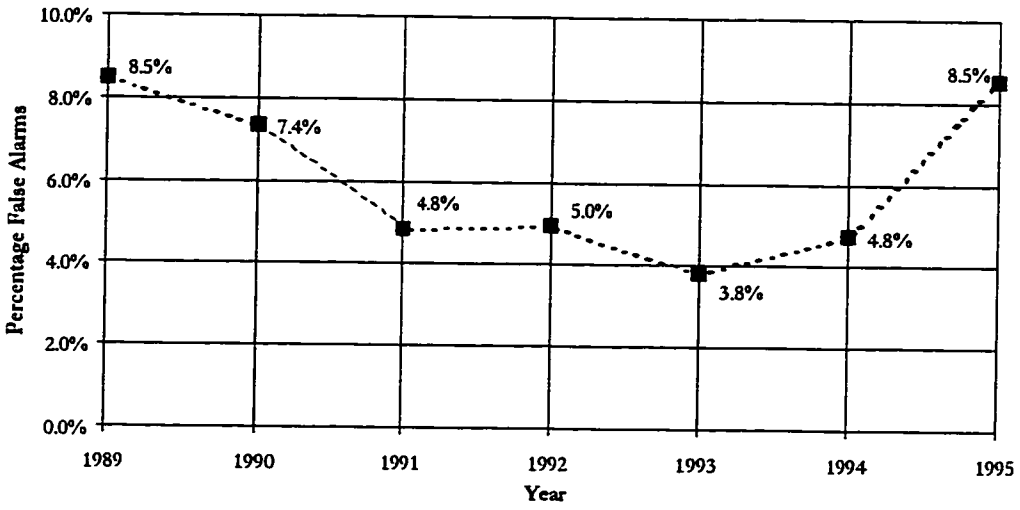


**Figure 7.4. False Alarms as a Percentage of CERT®/CC Incidents**

### 7.2.2. Unauthorized Access Incidents

As stated in Chapter 6, the center of the connection between attackers and their objectives is the attacker's requirement for unauthorized access or unauthorized use. This is shown in Figure 6.6, which is expanded in Figure 7.5 to show the two types of successful unauthorized access: root-level, and account-level. Most of the 4,299 CERT®/CC incidents were classified by CERT®/CC personnel as either being an unauthorized access incident, or as being an unauthorized use incident (discussed in the next section). Incidents that were not classified by CERT®/CC personnel were classified by reference to the text in the files for each incident.

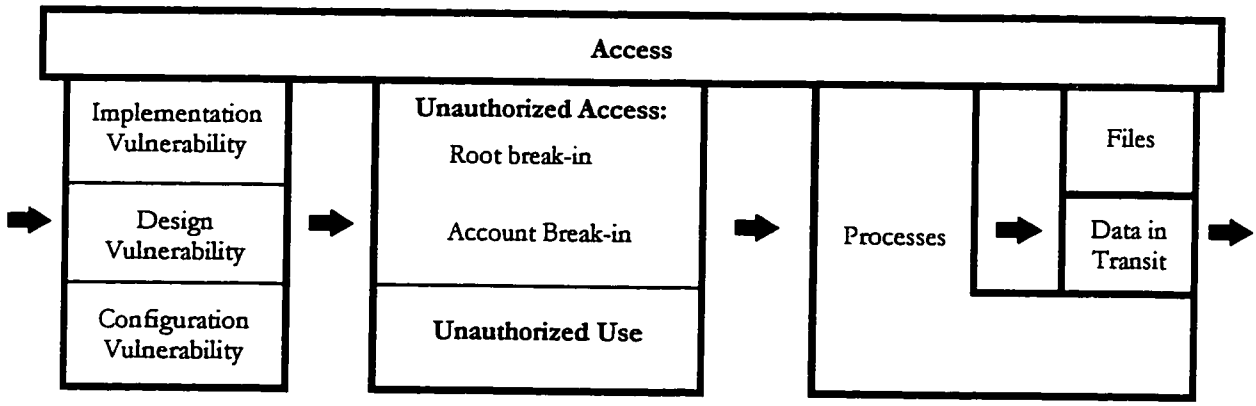


**Figure 7.5. Access for Attack**

The unauthorized access incidents were classified into their degree of success in obtaining access. The category describing the highest level of access is *root break-in*, which indicated that unauthorized privileged access was successfully obtained through at least one attack during the incident (i.e., root-level access was obtained on at least one host involved). The next level of

classification is *account break-in*, which indicated that unauthorized access to an account without privileged access was obtained through at least one attack during the incident (i.e., account-level access was obtained on at least one host involved). The final level of classification is *access attempt*, which indicated that access was attempted on at least one host, but no attempts were successful. This last category is not depicted in Figure 7.5 because it does not represent a successful path through the process.

These classifications have a wide variation in that a break-in or attempt could involve anywhere from one host to thousands of hosts, and from one site to hundreds of sites. But the classifications do give some indication of severity. An incident involving a root break-in was generally more severe than one that did not, and an incident that involved successful break-ins would certainly be considered more severe than one that involved only attempts.

Most of the CERT®/CC incidents (89.3%) were classified in these access categories. Of these, 1,189 (27.7% of total incidents, 31.0% of access incidents) were classified as *root break-ins*, 1,034 (24.1% of total, 26.9% of access incidents) were classified as *account break-ins*, and 1,618 (37.6% of total, 42.1% of access incidents) were unsuccessful *access attempts*.

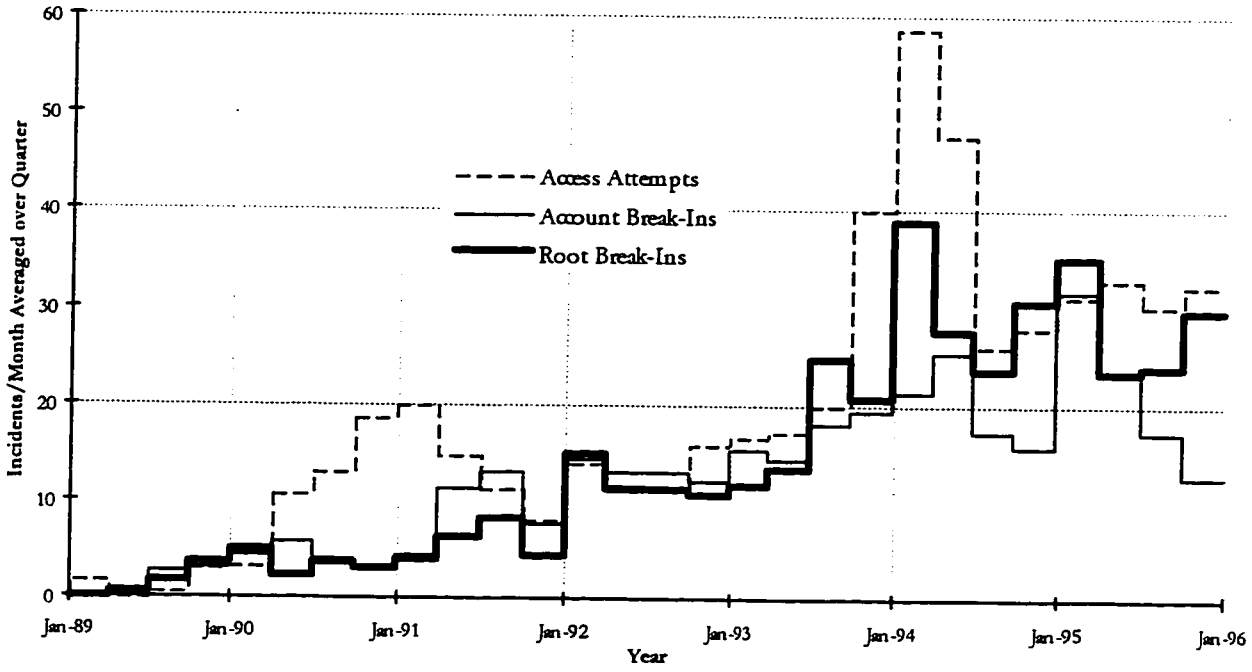


**Figure 7.6. CERT®/CC Access Incidents by Month Averaged Over Quarters**

Figure 7.6 shows the average number of incidents per quarter for each of the three access categories. The number of *root break-ins* per month reported to the CERT®/CC showed a steady increase until it peaked in the first quarter of 1994. In 1994 and 1995, the average number of root

break-ins per month reported the CERT®/CC was around 30. The rate at which lower-level *account break-ins* were reported was roughly the same as for root break-ins. Account break-ins, however, didn't reach a peak until the first quarter on 1995. The average during 1994 and 1995 was around 20 account break-ins per month reported to CERT®/CC. Although there are some similarities for *attempts*, there are interesting differences. Between the second quarter of 1990 to the third quarter of 1991, there is a significant peak, and the peak at the beginning of 1994 is significantly larger. Perhaps these indicate periods of increased "amateur" activity (but this is only speculation).

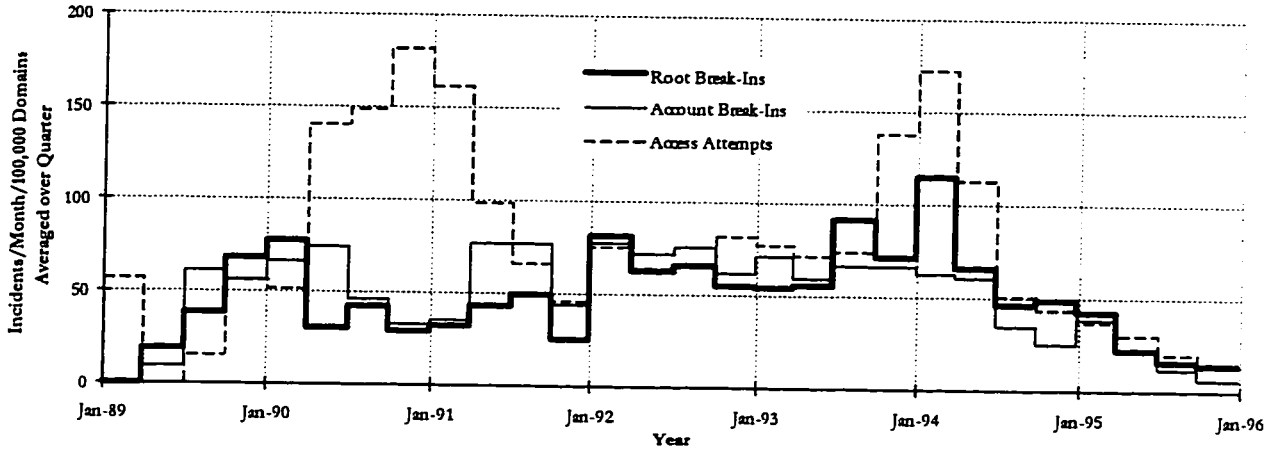


**Figure 7.7. CERT®/CC Access Incidents per 100,000 Domains by Month Averaged Over Quarters**

A comparison to the size of the Internet presents a different picture as shown in Figures 7.7 and Figure 7.8. For Figure 7.7, the growth in Internet *domains* (discussed in Chapter 2) was used to determine the average incidents per month per 100,000 Internet domains (averaged over quarters). If the rate of attacks matched the growth of Internet domains, we would expect to see a steady average. Instead, peaks occurred in 1990-1991, and 1993-1994, and there was a steady decline after the beginning of 1994.

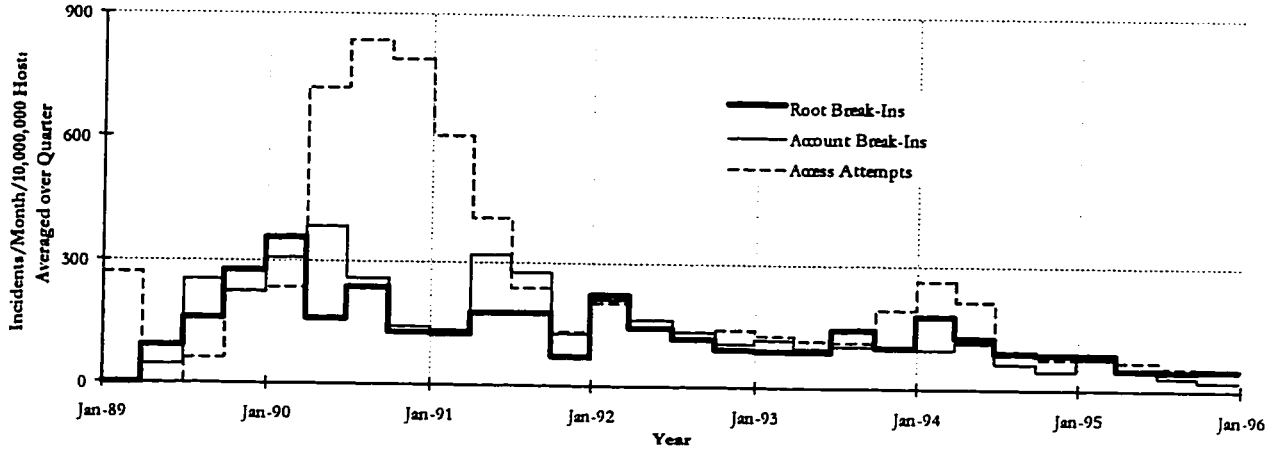


**Figure 7.8. CERT®/CC Access Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

A simple linear least squares fit to these data can determine whether, relative to the size of the Internet, the frequency of incidents in these categories are increasing or decreasing. Regressions of the three curves in Figure 7.8 reveal that, relative to the growth in Internet domains, each of these access categories is *increasing*. All of the slopes were found to be statistically greater than zero ($\alpha$ = 1%). Root-level break-ins were found to be increasing at a rate around 36% greater than the increase in Internet domains ($R^2$ = 90.1%). Account-level break-ins were increasing at a rate around 28% greater ($R^2$ = 75.8%), and access attempts at a rate around 29% greater ($R^2$ = 63.6%).

The pattern shown in Figure 7.7 may, however, have been influenced by the reduction in the number of Internet Hosts per Internet domain after 1993 (shown in Figure 2.7). For Figure 7.8, the growth in Internet *hosts* (see Chapter 2) was used to determine the average incidents per month per 10,000,000 Internet hosts. Again, if the rate of attacks matched the growth of Internet hosts, we would expect to see a steady average. Instead, we see a steady, although gradual, *decrease* in break-ins and access attempts from 1990 through 1995, with a large peak in attempts in 1990.

Simple linear regressions of the three curves in Figure 7.8 reveal that, relative to the growth in Internet hosts, each of these access categories was *decreasing*. All of the slopes were found to be less than zero ($\alpha$ = 1%). Root-level break-ins were found to be decreasing at a rate around 19% less than the increase in Internet hosts ($R^2$ = 16.1%). Account-level break-ins were decreasing at a rate around 11% less ($R^2$ = 14.3%), and access attempts at a rate around 17% less ($R^2$ = 24.2%).

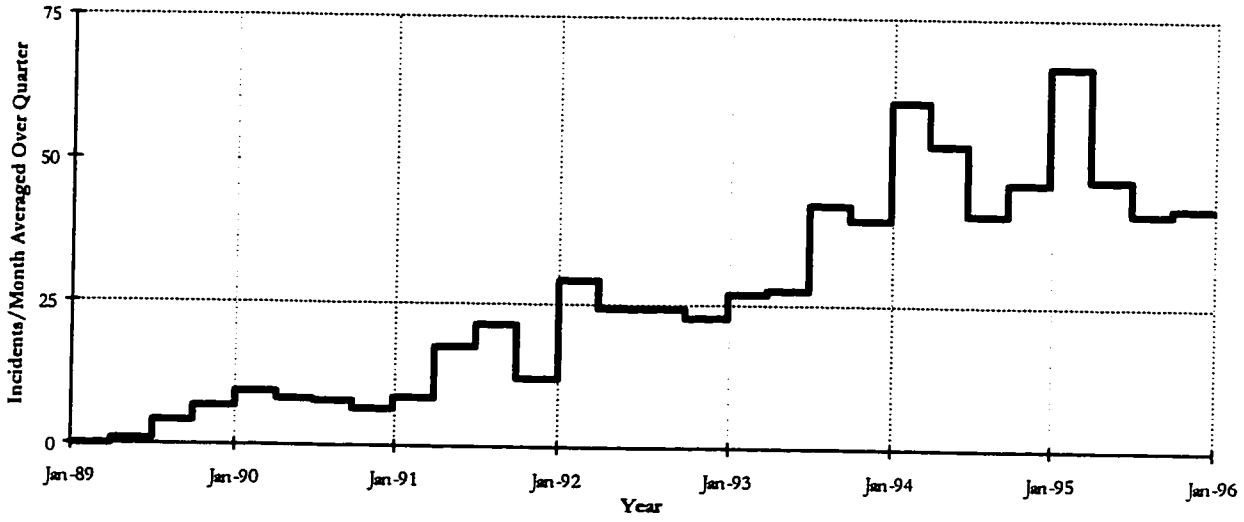


**Figure 7.9. CERT®/CC Successful Access Incidents by Month Averaged Over Quarters**

Figure 7.8, therefore, indicates that, relative to the number of hosts on the Internet, access incidents reported to the CERT®/CC gradually decreased over the period of this research. The

relative increases compared to the number of domains shown in Figure 7.8 were probably the result of the decrease in the average number of hosts in each domain (see Chapter 2).

The successful root-level and account-level break-ins are combined in Figure 7.9, which shows steady increases in successful access attacks through the beginning of 1994. In 4 of the 7 years, there appears to be a seasonal pattern, with apparent peaks during the winter months. The actual correlation between the month and the number of incidents, however, was only 7%.

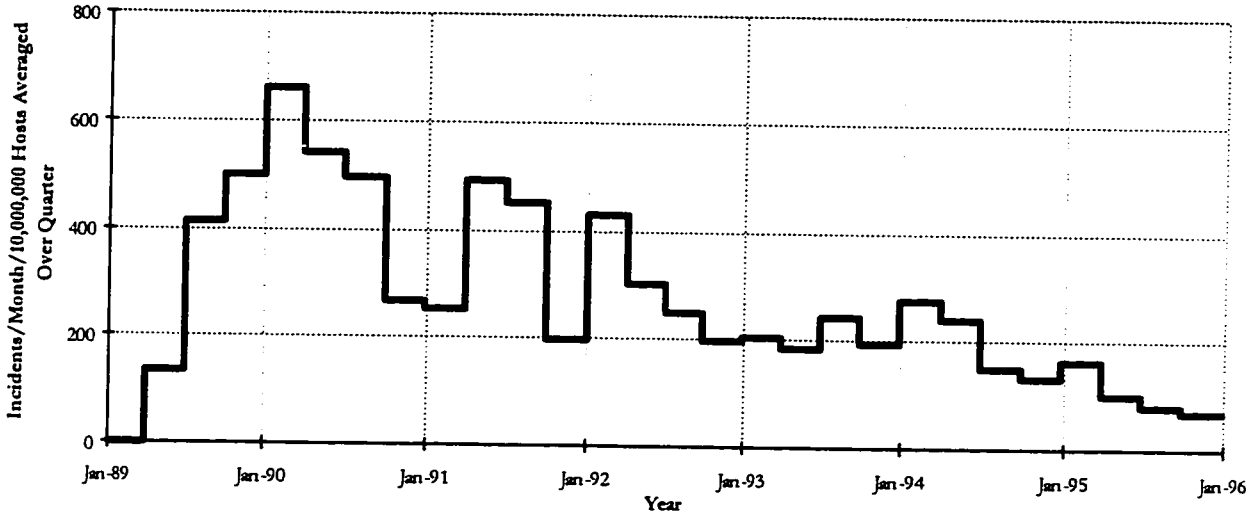


**Figure 7.10. CERT®/CC Successful Access Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

The pattern looks significantly different when normalized to the number of Internet hosts as shown in Figure 7.10. This shows that the number of incidents with successful attacks declined from 1990 through 1995. A simple linear least squares fit revealed the growth in successful access incidents to be around 14% less than the growth rate of Internet hosts ($\alpha = 1\%$, $R^2 = 22.0\%$).

**7.2.3. Unauthorized Use Incidents -** As stated above, the majority of the 4,299 CERT®/CC incidents were classified by CERT®/CC personnel as being unauthorized access incidents. As shown in Figure 7.5, and discussed in Chapter 6, attackers may also be able to obtain their objectives through the unauthorized use of systems which they have access to. Of the 4,299 actual incidents reported to the CERT®/CC, 458 (10.7%) were classified as unauthorized use incidents.

In order to gain further insight, the unauthorized use incidents were further classified into three other categories under the results block of the taxonomy (see Figure 6.9). The first of these categories is *denial-of-service attacks*. There were 104 denial-of-service incidents reported to the CERT®/CC, which represented 22.7% of unauthorized use incidents, and 2.4% of all incidents. Chapter 11 discusses these denial-of-service incidents in more detail.

The second classification of unauthorized use incidents is *corruption of information.* There were 135 unauthorized use incidents reported to the CERT®/CC having results in this category, which represented 29.5% of unauthorized use incidents, and 3.1% of all incidents. Most of these incidents (127) involved *mail spoofing,* where the "from" address was falsified in an e-mail message, or more often in a series of messages. An additional 8 incidents involved disguising the source of other types of Internet packets.

These 135 corruption of information incidents could all be categorized as *IP spoofing* attacks. IP spoofing is a broad classification of techniques that are used to falsify the Internet Protocol (IP) address of Internet packets. IP spoofing can be used in two categories of attacks. First, IP spoofing can be used simply to disguise the source of an otherwise *authorized use* of Internet resources. When this was the case, these incidents were classified as *unauthorized use incidents (corruption of information).* On the other hand, IP spoofing is also a method which can be used to gain *unauthorized access.* When this was the case, these incidents were classified as *unauthorized access* incidents, which were discussed in the previous sections.

One additional source of confusion might be between *mail spam* and *mail spoofing.* Mail spam is the most common form of denial-of-service attack, as discussed in Chapter 11. One way this is accomplished is by sending repeated messages to a mail server with the intent of exceeding the capacity of the system. Attackers will often also use mail spoofing to falsify the "from" address when sending mail spam. Such incidents were classified as denial-of-service attacks. Mail spoofing incidents that did not involve denial-of-service attacks were classified as *corruption of information* incidents.

The final category of unauthorized use incidents is 219 *disclosure of information incidents* that were reported to the CERT®/CC. These represented 47.8% of unauthorized use incidents, and 5.1% of all incidents. Nearly 80% (171) of these incidents involved the use of anonymous file transfer protocol (FTP) sites to deposit and transfer pirated software. CERT®/CC personnel did not consider software piracy a security incident. They recorded the incidents that were sent to them, but they did not pursue these incidents in the same way that other security incidents were handled. Beginning in 1993, they generally handled these incidents by recording the incident, sending the reporting site a standard e-mail letter giving suggestions, and then closing the incident in the CERT®/CC records.

The corruption of information incidents were categorized by CERT®/CC personnel as follows:

| | | | |
|---|---|---|---|
| 171 | software piracy, FTP abuse | 4 | FTP abuse (no software piracy) |
| 17 | mail abuse | 2 | account abuse/sharing |
| 12 | chain letter | 1 | credit card fraud |
| 6 | FSP abuse | 1 | mail fraud |
| 5 | IRC abuse | | |
| | | 219 | Total abuse incidents |

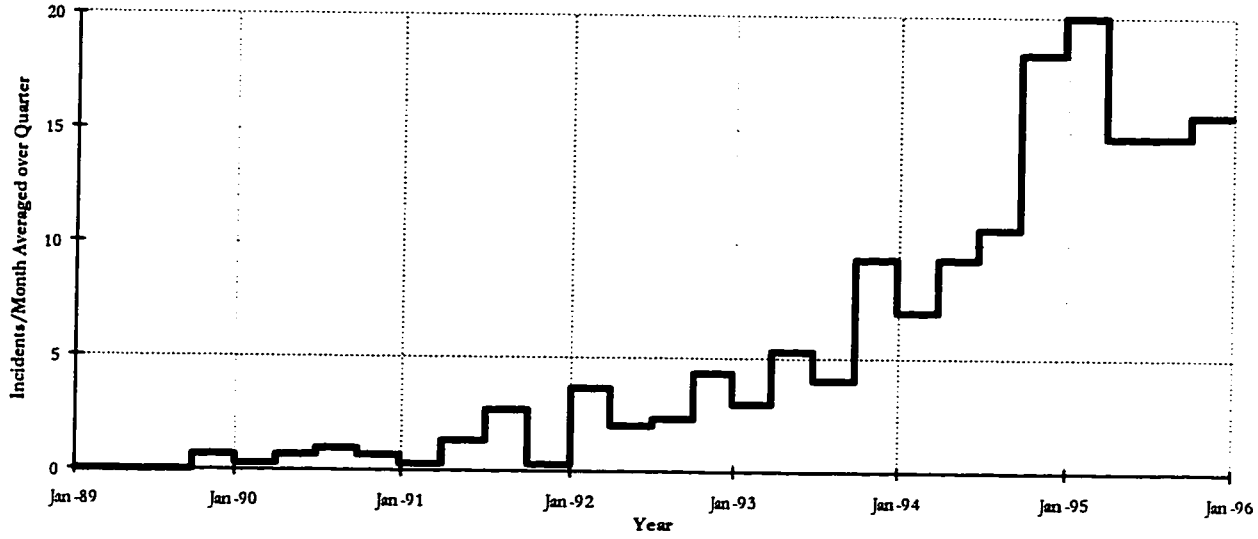


**Figure 7.11. CERT®/CC Total Unauthorized Use Incidents by Month Averaged Over Quarters**

The distribution of the unauthorized use incidents over time is somewhat different from the distribution of unauthorized access incidents. This can be seen in Figure 7.11, which shows the total unauthorized use incidents report to the CERT®/CC. The unauthorized use incidents increased steadily until they peaked at the beginning of 1995.

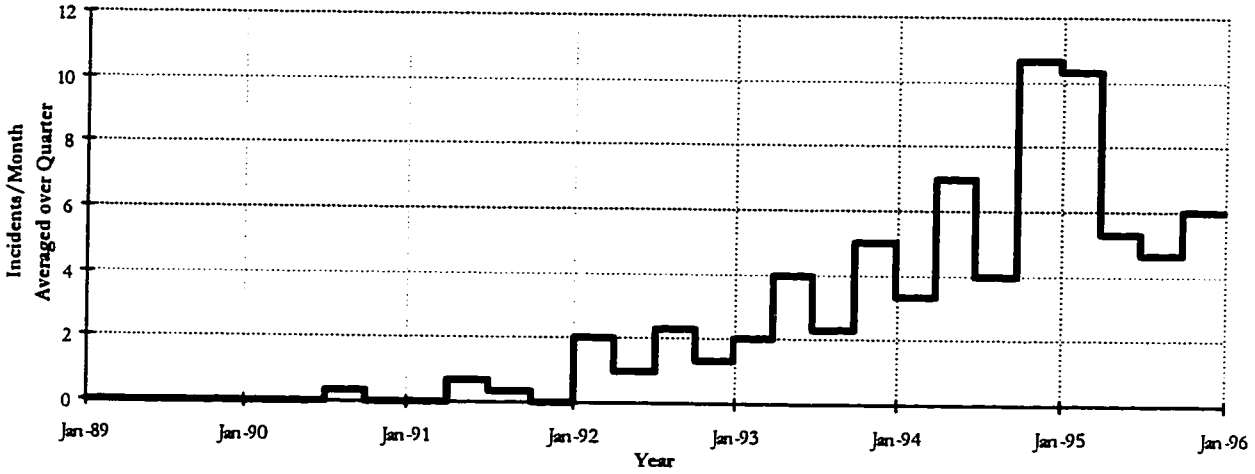


**Figure 7.12. CERT®/CC Disclosure of Information Incidents by Month Averaged Over Quarters**

This peak at the beginning of 1995 in Figure 7.11 is primarily the result of a significant peak in disclosure of information incidents at that time as shown in Figure 7.12. When normalized to the

size of the Internet, however, the data in Figures 7.11 and 7.12 do not show this peak. Figure 7.13 shows the unauthorized use incidents per 10,000,000 hosts. Their frequency appears relatively constant. A simple linear least squares fit showed, however, that the slope of these data were positive (for $\alpha = 5\%$, but not for $\alpha = 1\%$). The growth in total unauthorized use incidents was around 9% per year greater than the growth in Internet hosts ($R^2 = 11.5\%$).

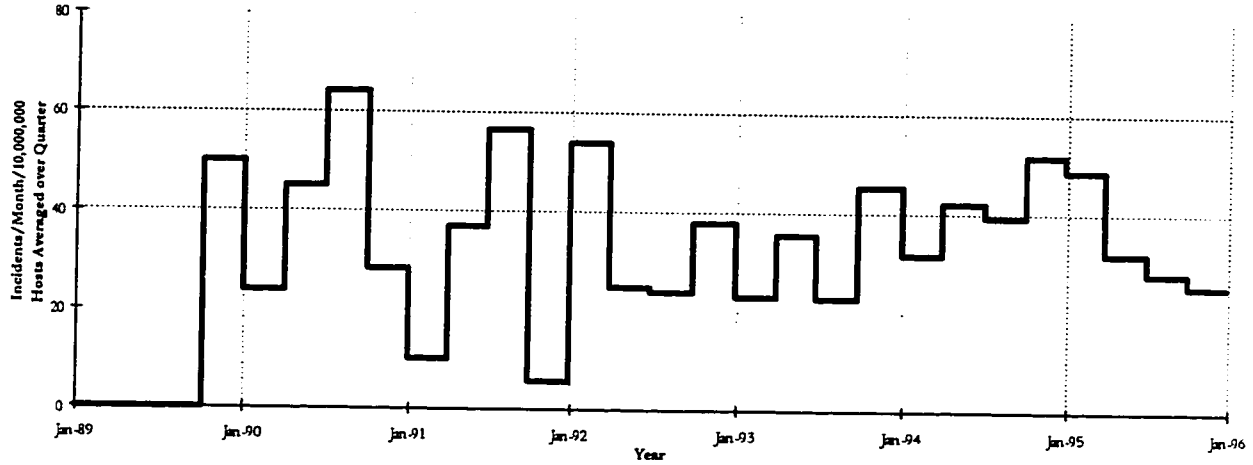


**Figure 7.13. CERT®/CC Total Unauthorized Use Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

The growth was more significant when the disclosure of information incidents are examined by themselves as shown in Figure 7.14, although it is interesting to note that these disclosure of information incidents appear more predominant in 1992 through 1994, than in 1995. A simple linear least squares fit did not show the slope of these data to be statistically different from zero.

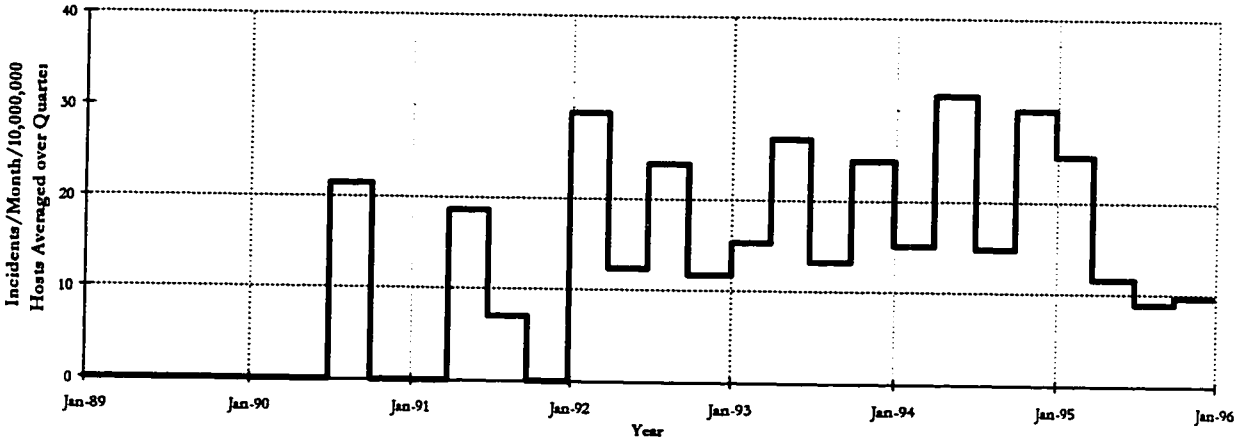


**Figure 7.14. CERT®/CC Disclosure of Information Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

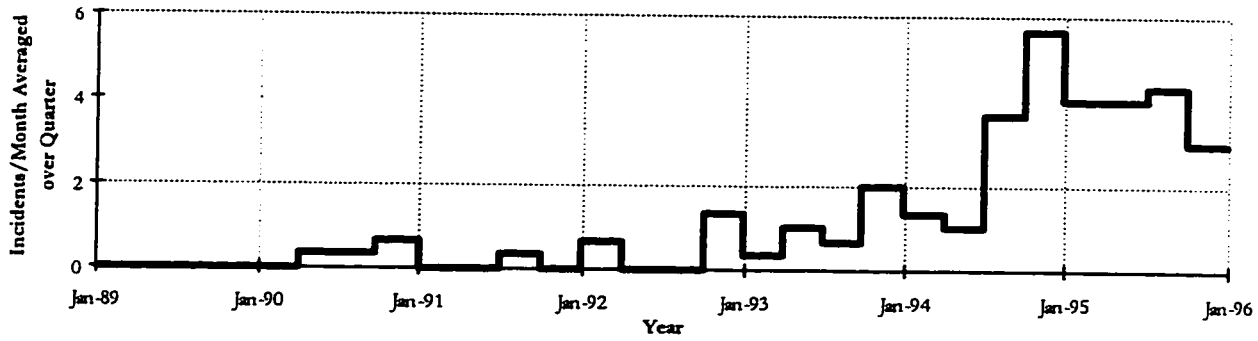


**Figure 7.15. CERT®/CC Denial-of-service Incidents by Month Averaged Over Quarters**

A peak also occurred in denial-of-service incidents at the end of 1994 (Figure 7.15), although the decline in denial-of-service incidents in 1995 is less significant.

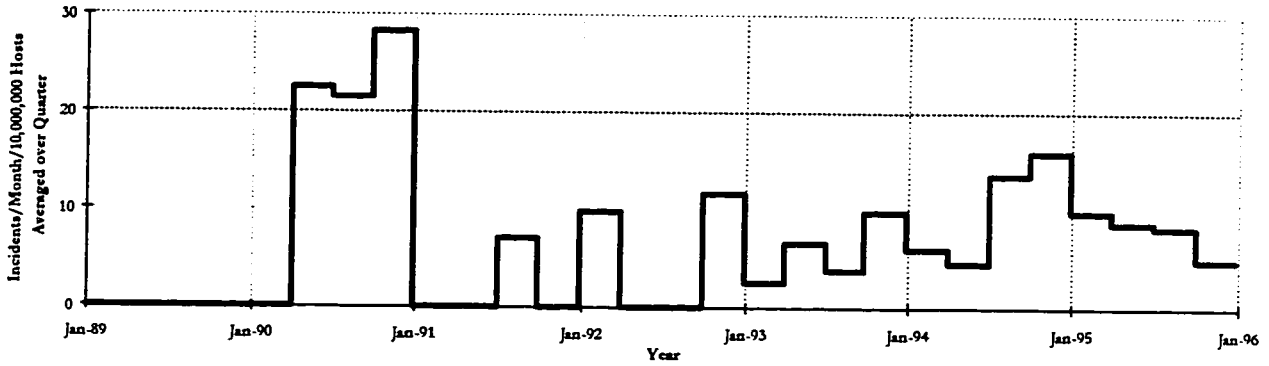


**Figure 7.16. CERT®/CC Denial-of-service Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

The 1994 peak is again less significant when the denial-of-service incidents are normalized for the size of the Internet (Figure 7.16). The frequency of denial-of-service incidents was also significantly higher in 1990. Simple linear regression did not show the slope of the curve in Figure 7.16 to be significantly different from zero. Denial-of-service incidents are discussed more fully in Chapter 11. In Figures 7.15 and 7.16, only the 104 incidents that were classified as "denial-of-service" incidents were used. Denial-of-service *methods* were recorded, however, in an additional 39 incidents that were classified as root- or account-level break-ins. These additional incidents were included in the analysis in Chapter 11, which provided a statistically significant slope that showed an increase of around 50% per year. See Chapter 11 for more information.

Corruption of information incidents show the most unusual pattern. They were the only one of the six categories of incidents that showed an increase continuing through 1995, as shown in Figure 7.17. Figure 7.18 shows a slight increase in these incidents in relative terms from 1993 through 1995 when normalized to the size of the Internet. However, the most significant feature of Figure 7.18 is the relatively larger number of incidents from the end of 1989 through 1991.

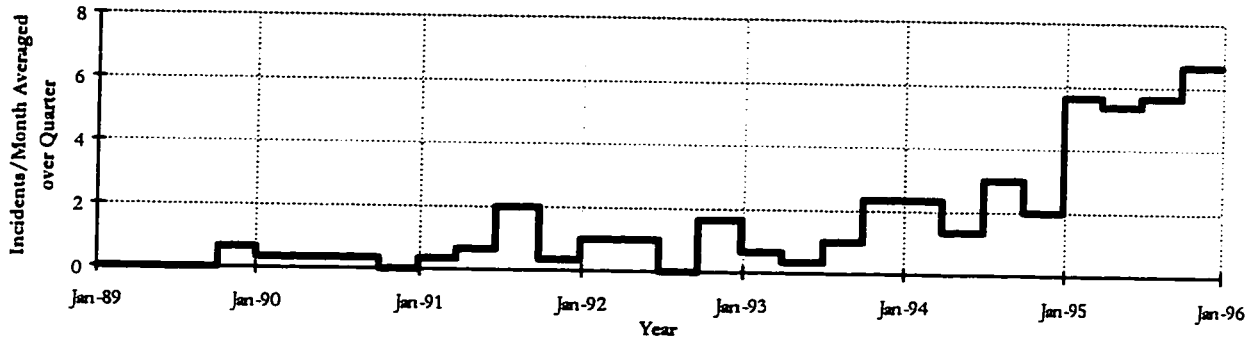


**Figure 7.17. CERT®/CC Corruption of information Incidents by Month Averaged Over Quarters**

A simple linear least squares fit did not show the slope of the curve for corruption of information incidents in Figure 7.18 to be significantly different from zero.

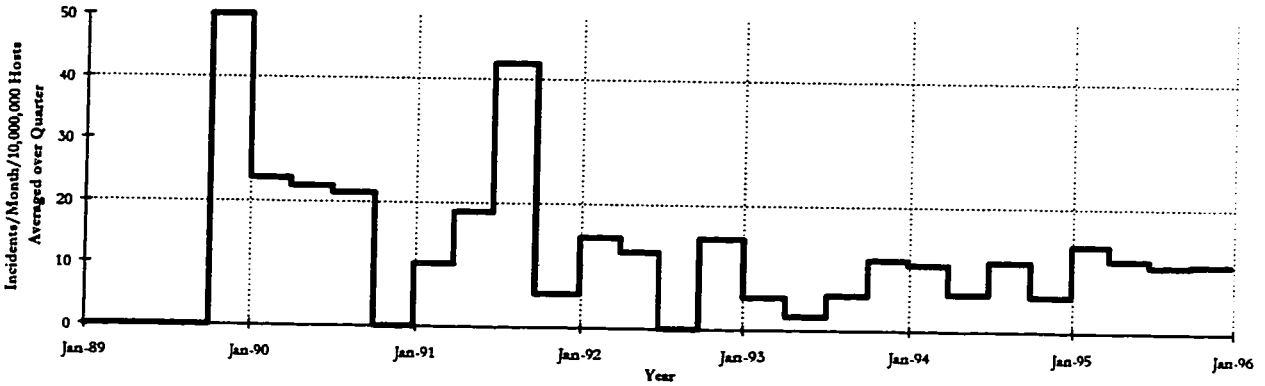


**Figure 7.18. CERT®/CC Corruption of Information Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

**7.2.4. Inadequacies of this Classification** - The incidents shown in Figures 7.1 and 7.2 were classified into types in Figures 7.6 through 7.18, which gives some indication of their severity. The other problems noted earlier, however, remain: 1) the incidents were plotted according the date they were reported to the CERT®/CC, which was often not when they actually began, 2) the incidents were of variable duration, and 3) the incidents involved different numbers of sites. This problem is discussed further in Section 7.3, where an alternate measure of severity is presented.

### 7.3. An Alternate Measure of Severity

An alternative method of presenting the CERT®/CC incident information was developed for this research. For each incident, the average sites per day were calculated using the starting date, ending date and the total number of sites involved. These were then combined through the use of a custom computer program to find the total average sites per day for each classification of attack.

Using sites per day to present the CERT®/CC incident information takes into consideration the beginning and the end of an incident, as well as the number of sites involved. The classification of the incidents can be taken into consideration by examining separate groups of incidents. One

inaccuracy with this approach is introduced by averaging the number of sites involved over the number of days in the incident. For this to be accurate, the involvement of all attackers and all sites must have been constant over the duration of the incident. This was generally not the case. Both in terms of the attackers and the sites, the involvement generally appeared much greater toward the beginning of an incident than it is toward the end. There was not, however, enough information in the CERT®/CC records to either determine the extent of this inaccuracy, or to compensate for it.

### 7.4. Sites per Day Recorded in the CERT®/CC Incidents

Figure 7.19 plots the sites per day for all incidents reported to the CERT®/CC. The most pronounced feature of this figure is the large "spike" in sites per day near the beginning of 1994. There are also smaller, but obvious spikes in 1995.

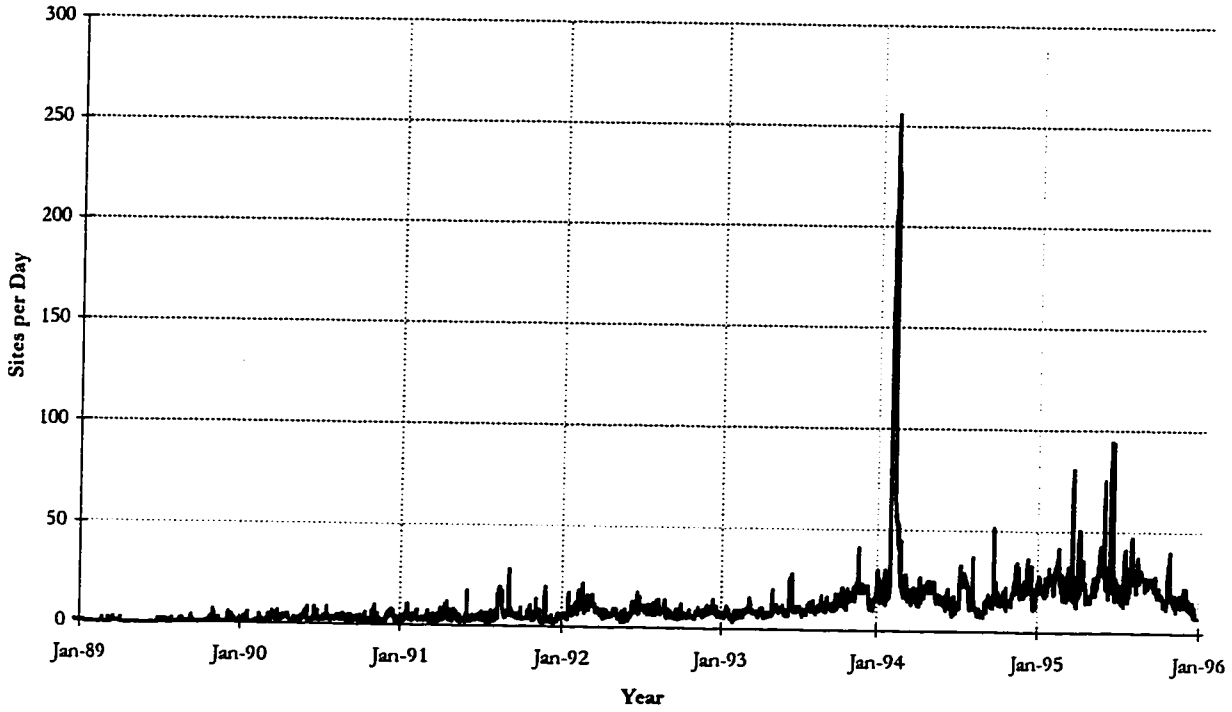


**Figure 7.19. CERT®/CC Sites per Day - All Incidents**

With the spikes in Figure 7.19 it is difficult to determine trends in the remaining data. These data can be smoothed by averaging over each month (Figure 7.20) or over each quarter (Figure 7.21). Even with this smoothing, however, there remains a large spike in the number of sites per day in February, 1994. This will be investigated further in Chapter 8, which discusses large incidents. It appears that the large spike in February, 1994 may explain the drop in incidents seen between 1994 and 1995. Other than this spike, both Figure 7.20 and 7.21 show smooth increases in sites per day through the first half of 1995.

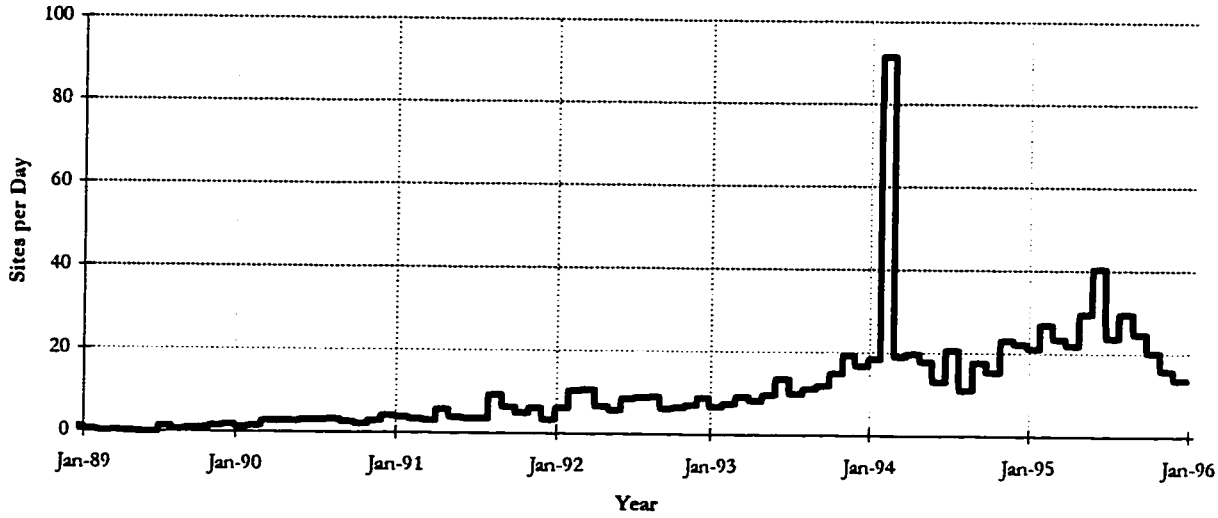


**Figure 7.20. CERT®/CC Sites per Day - All Incidents, Averaged Over Months**

Figures 7.20 and 7.21, however, appear to indicate a significant drop in the number of sites per day during the last half of 1995. This drop is less pronounced when only the successful access attacks are included (root and account-level break-ins). This is the case in Figures 7.22 and 7.23. In these Figures there are large spikes in February, 1994 and June, 1995. There is also a relatively smooth increase in sites per day in the rest of the data. There was not, however, much of a drop-off in incidents until the last quarter of 1995.

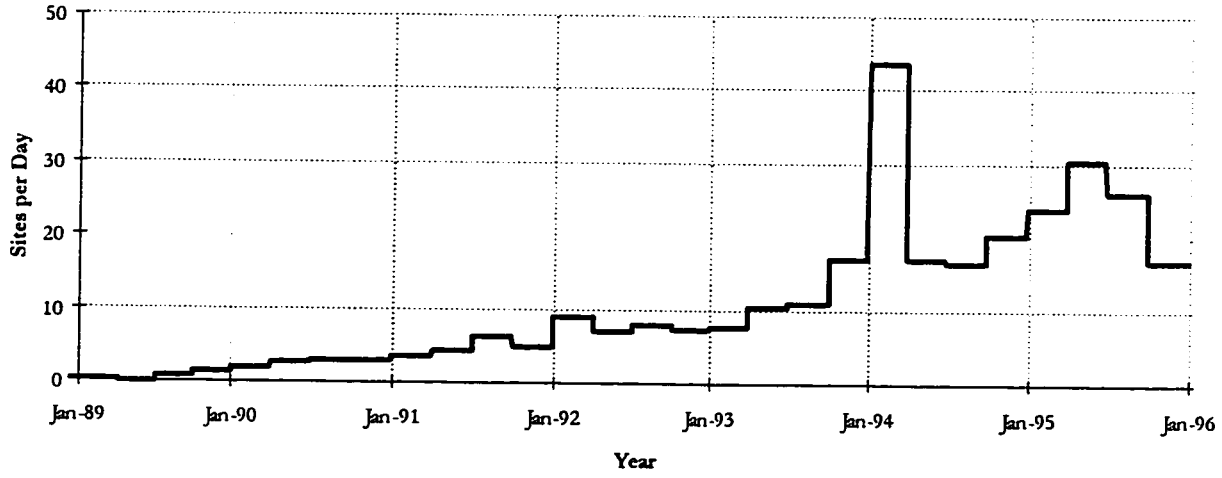


**Figure 7.21. CERT®/CC Sites per Day - All Incidents, Averaged Over Quarters**

One interesting thing to note in Figures 7.20 to 7.23 is that there is very little evidence of seasonality. Earlier figures present the reporting dates of incidents to the CERT®/CC, which match or are near the starting date of the incidents. The differences between these Figures seem to indicate that initiation of incidents may have slight seasonality, with more incidents starting after the

beginning of the calendar year. The total activity, measured by the sites involved in security incidents each day, seems to show little or no seasonal variation.

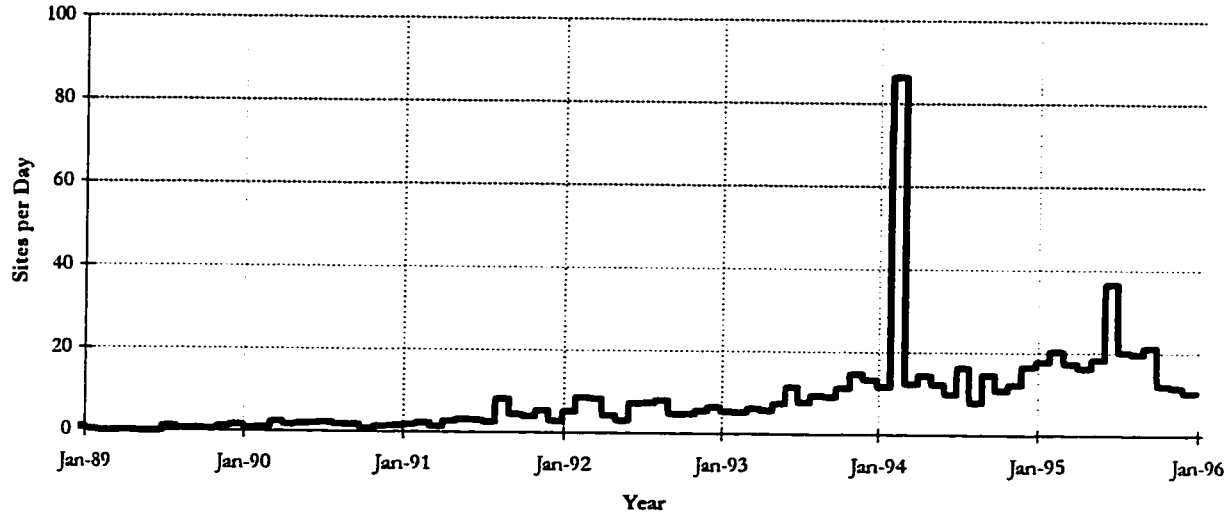


**Figure 7.22. CERT®/CC Sites per Day - Root and Account Break-ins, Averaged Over Months**

The final two figures of this chapter show the data from Figures 7.21 and 7.23 (the sites per day data averaged over quarters) normalized for the size of the Internet. Figures 7.24 and 7.25 show a steady decline in security activity reported to the CERT®/CC, compared to the size of the Internet, since peaking in 1990. The decline is not as pronounced in Figure 7.25 which shows the sites per day for successful root- and account-level break-ins. This may reflect a decline in the reporting of *unsuccessful* attacks compared to *successful* attacks. This is discussed further in Chapter 12 which estimates the total number of Internet incidents.

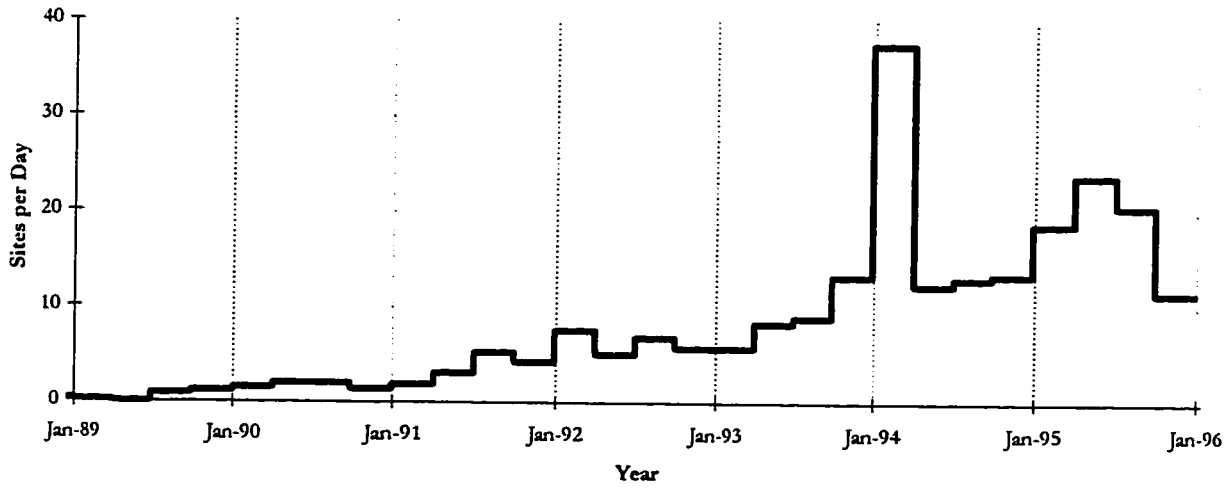


**Figure 7.23. CERT®/CC Sites per Day - Root and Account Break-ins, Averaged Over Quarters**

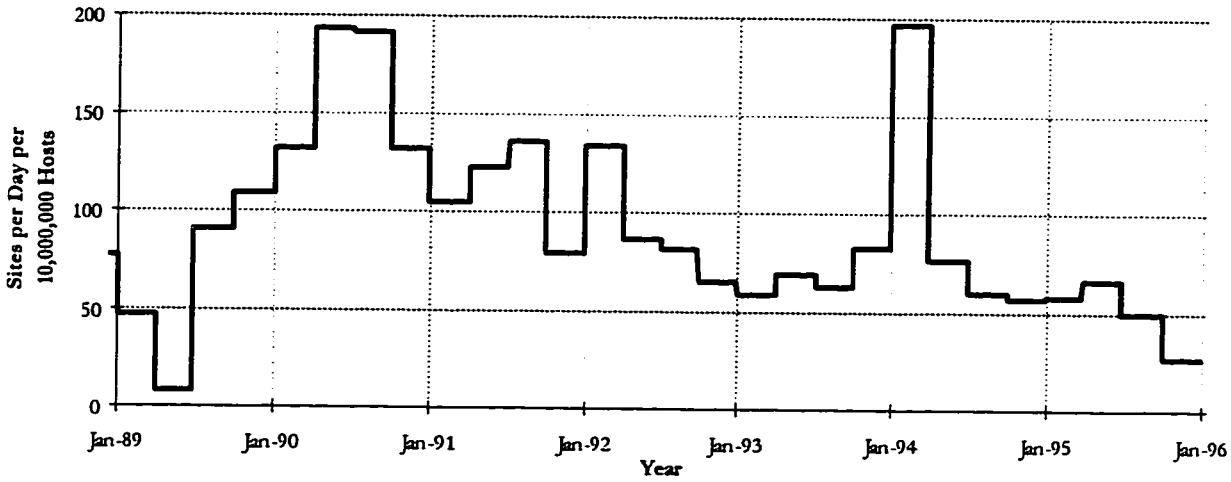


**Figure 7.24. CERT®/CC Sites per Day per 10,000,000 Hosts - All Incidents, Averaged Over Quarters**

It is interesting to note that all presentations of sites per day, including Figures 7.24 and 7.25 show the large peak in the first quarter of 1994. This appears to involve one or more large incidents. This is discussed further in Chapter 10 which examines severe incidents.

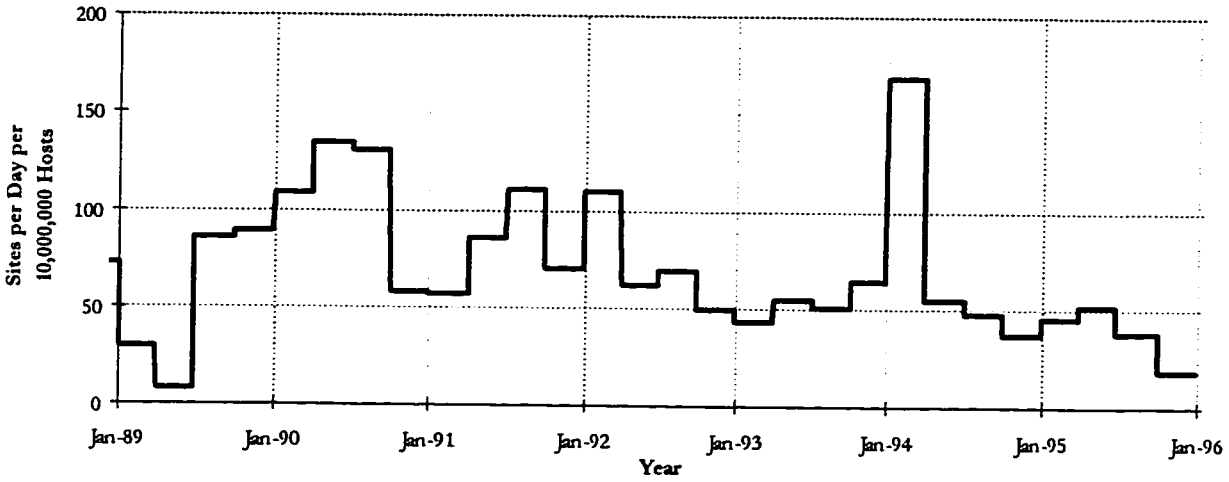


**Figure 7.25. CERT®/CC Sites per Day per 10,000,000 Hosts - Root and Account Break-ins, Averaged Over Quarters**

A simple linear least squares fit showed the slope of the growth in all sites per day for all incidents (Figure 7.24) and for successful break-ins (Figure 7.25) were both around 7% *less* than the growth rate of Internet hosts ($\alpha$ = 1%, $R^2$ = 7.66% Figure 7.24, $R^2$ = 9.39% Figure 7.24).[3]

[3] It should be noted that the process of smoothing the data by quarters may increase the statistical significance of the linear least squares fit over a fit of the data by month, or by day. This was not examined because the size of the Internet per month, or per day, was not available, and because the large size of the data set indicated that this should not be a problem.

### 7.5. Summary of the Classification of Internet Incidents and Internet Activity

A total of 4,567 incidents over this 7 year period were reconstructed from the CERT®/CC records. This included 268 false alarms (5.9%), and 4,299 actual incidents (94.1%) ranging from login attempts to large incidents involving break-ins at the root level. The number of incidents increased each year at a rate between 41% (1991 to 1992) and 62% (1993 to 1994). The exception to this took place between 1994 and 1995 when the number of incidents decreased slightly.

The number of incidents reported to the CERT®/CC was not a good indication of either the activity at the CERT®/CC, nor of security incidents on the Internet because 1) the incidents were presented according to reporting date, which is an inaccurate representation of the incidents in *time*, and 2) the incidents were not comparable due to wide variations in duration, in the number of sites involved, and in the severity or success of the attack.

As stated in Chapter 6, the center of the connection between attackers and their objectives is the attacker's requirement for unauthorized access or unauthorized use. Most of the CERT®/CC incidents (89.3%) were unauthorized access incidents, which were further classified into their degree of success in obtaining access: *root break-in* (27.7%), *account break-in* (24.1%), and *access attempts* (37.6%). Relative to the growth in Internet hosts, each of these access categories was found to be *decreasing* over the period of this research: root-level break-ins at a rate around 19% less than the increase in Internet hosts, account-level break-ins at a rate around 11% less, and access attempts at a rate around 17% less.

Of the 4,299 actual incidents reported to the CERT®/CC, 458 (10.7%) were classified as unauthorized use incidents. These were further classified into *denial-of-service attacks* (2.4%), *corruption of information incidents* (3.1%), and *disclosure of information incidents* (5.1%). The growth in total unauthorized use incidents was around 9% per year greater than the growth in Internet hosts.

An alternative method of presenting the CERT®/CC incident information was developed for this research. For each incident, the average sites per day were calculated using the starting date, ending date and the total number of sites involved. These were then combined through the use of a custom computer program to find the total average sites per day for each classification of attack.

The sites per day data showed there was a steady *decline* in security activity reported to the CERT®/CC, *compared to the size of the Internet*, since peaking in 1990. The slope of the growth in all sites per day for all incidents, and for root and account-level break-ins were both around 7% *less* than the growth rate in the number of Internet hosts.

*Chapter 8*

# Methods of Operation and Corrective Actions

As discussed in Chapter 5, one of the ways to use a taxonomy is to determine the relative frequency of occurrences in the taxonomy categories. In this chapter, the taxonomy of computer and network attacks is used to determine the relative frequency of various kinds of attack activity. This activity was recorded in the methods of operation (MO) and corrective actions (CA) fields in the CERT®/CC records (see Chapter 4).

Recording of the method of operation and corrective action data was not systematic or complete. As a result, this information is incomplete. Some valuable information, however, can be obtained by determining the relative frequency that various methods of operation and corrective actions appear in the CERT®/CC incident records. This chapter presents a summary of the classification of key words describing the methods of operation found in the CERT®/CC records. This classification uses the taxonomy developed in Chapter 6 (Figure 6.9). The complete methods of operation data are given in Appendix A. This chapter also includes a summary of corrective actions found in the CERT®/CC incident records (with the complete data in Appendix B). An additional section discusses some of the things the CERT®/CC records do not include, such as information about computer viruses.

## 8.1. Methods of Operation

As discussed in Chapter 4, the data extracted from the CERT®/CC incident records included a field for methods of operation. In this field, key words were placed that described the various methods recorded. These key words also are instances in the categories of the attack taxonomy (Figure 6.9). In each category shown in Figure 6.9, the total occurrences was determined, along with the average starting date for the incidents involved. For example, the well-known toolkit called *rootkit* was recorded in 68 incidents beginning at the end of January, 1994. The mean starting date for these 68 incidents was March 19, 1995. This contrasts with the mean starting date of October 24, 1993 for all incidents, which is a year and a half earlier. This indicates that, in terms of the CERT®/CC incident records, *rootkit* was a relatively new tool.

This type of information is interesting in several respects. First, it gives some indication of the relative importance of the method. In the above example, *rootkit* appeared in 1.6% of the incidents, which makes it relatively more important than the *chasin* or *gimme* tools , which appeared in 1.0% and 0.3% of the incidents respectively. Second, some indication can be seen of the placement of the method in time relative to other methods. For example, incidents in which *chasin* was recorded

had an mean starting date of September, 1994, which indicates *chasin* is an older problem than *rootkit*. The *gimme* tool is even earlier, with a mean starting date in December, 1993. Finally, some indication of a trend may be found in the relationship of the mean of the start dates for the incidents which include a particular method, and the mean starting date for all incidents. For example, a mean starting date prior to October, 1993 (the mean starting date for all incidents), may indicate the prevalence of that particular method has been reduced over time.

In the CERT®/CC records, more information was found about *Tools* and *Access* (see Figure 6.9), than the other categories. Very little information was in the records about the beginning and ending categories, *Attackers* and *Objectives*. The following sections give a summary of the methods of operation information available in the CERT®/CC records in each of the Figure 6.9 categories. More detailed information is given in Appendix A. It should be remembered that incidents typically included multiple attacks and therefore multiple methods of operation and corrective actions. In other words, the categories were not mutually exclusive when multiple attacks were considered. More specifically, in the figures presented in the remainder of this chapter and in Appendices A and B, the frequencies in the figures (number of occurrences) do not necessarily add up between categories and sub-categories.

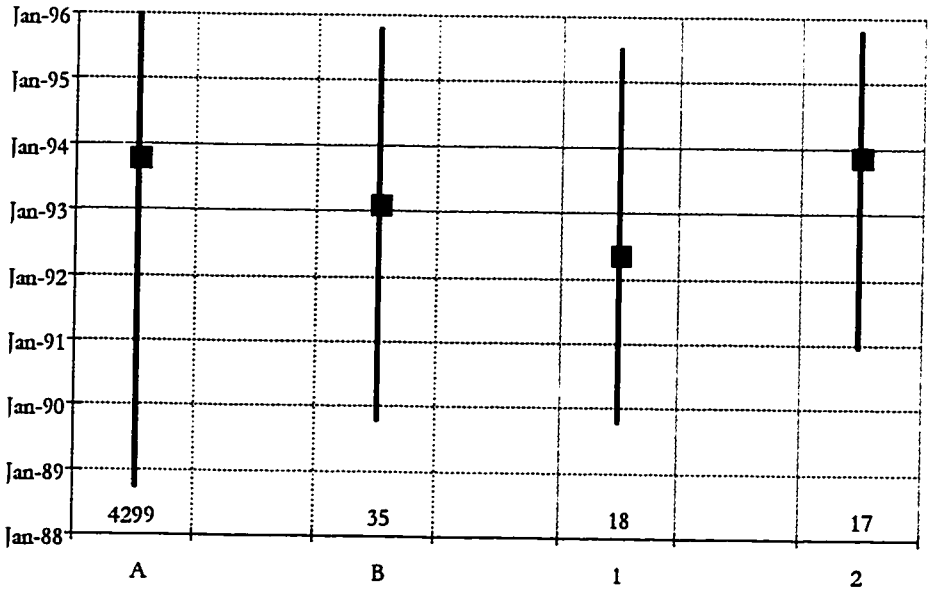


**Figure 8.1. Range and Mean Incident Reporting Dates for Methods of Operation - Attackers**
Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:
**A - All Incidents** **B - All Attackers** **1 - Hackers** **2 - Vandals - former employees**

**8.1.1. Attackers** - Very little information is found in the CERT®/CC records about who the attackers have been. Usually references in the records were not specific. Examples are "the

intruder was identified," "the attackers were found at xxxxxx," or "the system administrator has talked to the intruder." Only 35 (0.8%) of CERT®/CC incident records are more specific. These incidents are shown in column B of Figure 8.1 which shows the range of reporting dates for the incident reports that contain information about attackers. This figure (and other similar figures in this chapter and Appendices A and B) plots vertical lines showing the initial reporting date and the final reporting date in each of the categories. The large black squares indicate the mean reporting date in that category.[1] For comparison purposes, all of these figures plot the range for all incidents in the far left column. The data for all figures are listed in Table 8.1 at the end of this section.

Half of the 35 incidents in Figure 8.1 mention specific individuals (the 18 incidents in column 1). Most of these intruders were identified by location (*Dutch*, *Danish*, *Australian*, *Portland* hackers), or the by the intruder's nickname. One of the "Dutch" hackers in an incident beginning in 1989 was identified by name, and three incidents beginning in 1993 mention Kevin Mitnick.[2] The incidents that mention specific individuals (column 1 in Figure 8.1) generally occurred earlier than either the average of all incidents with attacker information (column B), or the average of all incidents. This is not the same for the 17 incidents which mention that the intruder was a former employee. These incidents occurred, on average, later in the data as shown in column 2 of Figure 8.1. The incidents involving former employees were classified in the taxonomy as *vandals*.

There are several possible reasons the CERT®/CC records do not contain more information about attackers. One possibility is that the attackers are rarely identified. This may not be the case because many of the incidents make reference to intruders being identified. A more likely possibility is related to the method of operation of the CERT®/CC itself. The CERT®/CC provides Internet users "real time" assistance with security incidents. Once an incident is under control, the interaction with the CERT®/CC and the sites involved is reduced. Less information is recorded toward the end of the incident, perhaps because this is not needed in order for the CERT®/CC to perform its duties. This may also be the same reason that little information is found in the CERT®/CC records on corrective actions as discussed in Section 8.2.

**8.1.2. Tools** - The second block in the taxonomy of Figure 6.9 is *Tools*. In Chapter 6, six categories of tools were described. Figure 8.2 shows the first, mean and last reporting date for CERT®/CC incident reports containing keywords referring to tools. A total of 778 incidents (18.1% of all incidents) reported the use of some tool.

---

[1] The median reporting date tended to be slightly later in time by an average of around 55 days.
[2] For a description of incidents involving Kevin Mitnick, see reference [TsM:96].

From these records, the largest category of tools was scripts or programs (661 incidents, 15.4% of all incidents, 85.0% of tools). These consisted primarily of *Trojan horses* (450 incidents, 10.5% of total, 57.8% of tools) and *sniffers* (245 incidents, 5.7% of total, 31.2% of tools). As can be seen in Figure 8.2, Trojan horses were used throughout the period of this research. The average reporting date was near the average for all incidents. Sniffers, on the other hand, were first reported in the second half of 1990, and their average reporting date was around a year later. Trojan horses were recorded in the CERT®/CC records as occurring in at least 45 different programs. The most common program was *login* which accounted for 56% of the Trojan horses recorded (in 251 incidents, 5.8% of total). Two other common programs for Trojan horses were *telnet* (70 incidents, 1.6% of incidents, 15.6% of Trojan horses), and *ps* (53 incidents, 1.2% of incidents, 11.8% of Trojan horses). See Appendix A for further details.

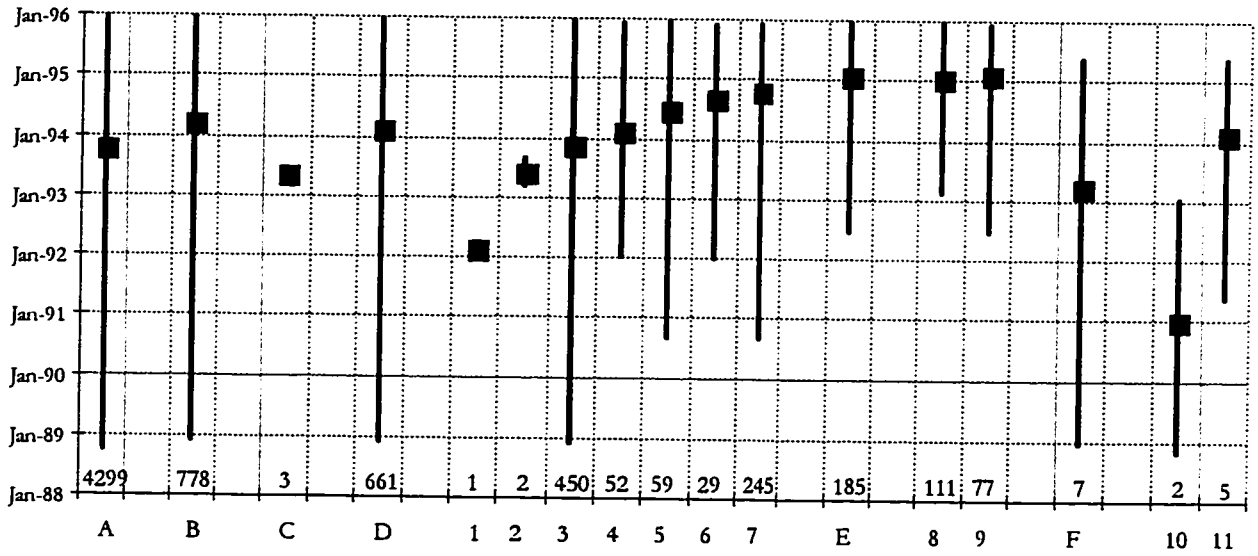


**Figure 8.2. Range and Mean Incident Reporting Dates for Methods of Operation - Tools**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Tools**
**C - All User commands**
**D - All Scripts or Programs**
**1 - logic bomb**
**2 - keystroke logging**
**3 - Trojan horse**
**4 - password cracker**
**5 - to get root**
**6 - denial-of-service tools**
**7 - sniffer**
**E - All toolkits**
**8 - scanners**
**9 - to get root**
**F - All Autonomous Agents**
**10 - worm**
**11 - virus**

It is interesting to note that the CERT®/CC records contain very few references to autonomous agents such as *worms*, and *viruses*. This may indicate these agents were of little use on the Internet during this period. This also may reflect that reports of these agents were not generally sent to the CERT®/CC. This is discussed further in Section 8.3.

Another tool that was found on average later in the CERT®/CC records was *toolkits*. As Figure 8.2 shows, toolkits were found generally in the same time frame as sniffers, which may indicate that toolkits and sniffers were generally used together. Some toolkits are known to contain sniffers and other tools such as Trojan horses.

Keywords describing toolkits (185 incidents, 4.3% of total, 23.8% of tools) were slightly less frequent than sniffers. The two general categories of toolkits were tools designed to exploit privileged or root access (such as *rootkit*), which were mentioned in 77 incidents (1.2% of total, 9.9% of tools), and *scanners* (such as *ISS*, and *SATAN*), mentioned in 111 incidents (2.6% of total, 14.3% of tools). These tools appeared relatively late in the CERT®/CC records. Toolkits to exploit root were not mentioned in the records until the middle of 1992, and scanners did not appear until 1993. One other category of tools worth noting is password cracking programs (such as *crack*) which were first recorded in the CERT®/CC records at the beginning of 1992 (52 incidents, 1.2%).

Only 3 incidents in the CERT®/CC records make specific references to intruders using *user commands*. This is clearly not a reflection of their frequency of use. For example, Chapter 7 indicated that 1,618 incidents were classified as *access attempts*. Of these, 1,080 incidents were more specifically classified as *login attempts* (see Appendix A), which is assumed to be initiated by user commands. It appears that CERT®/CC personnel did not usually record when intruders were using user commands, and that it is likely that user commands actually were the most common tool. Intruders, after all, must use some tool, and only 775 of the incidents (18.0%) mention other tools. If we assume the intruders in the remaining incidents used user commands, they were then used in a minimum of more than 80% of the incidents.

There was no mention in any of the CERT®/CC records of the use of the other two categories of tools: *Data taps*, or *Distributed tools*. Data taps are physical taps and not attacks across the Internet, which makes them much less likely to be reported to the CERT®/CC. Distributed tools do not appear in the CERT®/CC records until after the period of this research.

**8.1.3. Access** - The majority of method of operation information in the CERT®/CC records concerned the *access* block of the taxonomy. Most incidents (4,078 incidents, 94.9%) recorded some information about access. Referring to Figure 6.9 in Chapter 6, the access block has three parts. The middle part classifies incidents as either being *unauthorized access*, or *unauthorized use*, which was already discussed in Chapter 7. Some information is contained in the records as to which type of account was accessed. They are discussed at the end of this section. The type of account accessed may give some indication of the files that were accessed, but other than this, the CERT®/CC

records contain little direct information about which processes and files were involved in the CERT®/CC incidents. Which processes and files were involved in an incident were, to a certain extent, implied by the other information about the incident. For example, information that a *telnet* vulnerability was exploited for an attack would perhaps indicate that a telnet process was involved. The use of sniffers would indicate that data in transit was accessed. Trying to determine the processes and files involved in the incidents using this implicit information was not attempted as part of this research.

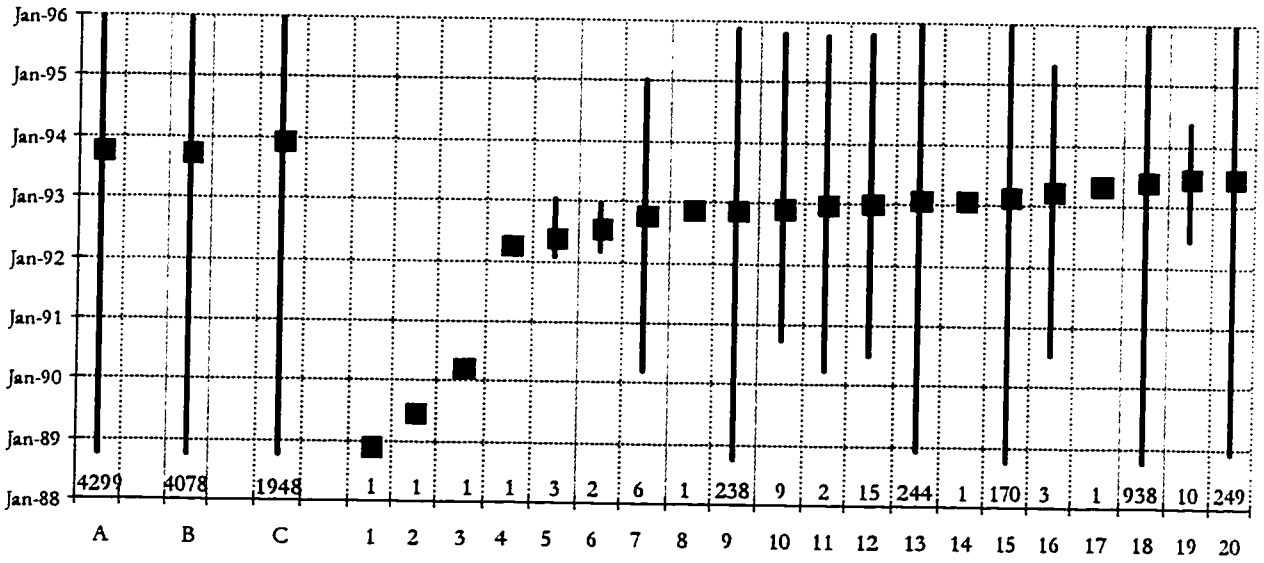


**Figure 8.3. Range and Mean Incident Reporting Dates for Methods of Operation - Access - Part 1**
Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **4 - netfind** | **10 - uucp** | **16 - mem** |
| **B - All Access** | **5 - motd** | **11 - chfn/chsh** | **17 - history** |
| **C - All Vulnerabilities** | **6 - shutdown** | **12 - bin/shell** | **18 - password vulnerability** |
| **1 - install** | **7 - .forward** | **13 - configuration** | **19 - mult** |
| **2 - rcp** | **8 - emacs** | **14 - fparel** | **20 - trusted hosts** |
| **3 - autofinder** | **9 - tftp** | **15 - ftp** | |

The first of the three parts in the access block of the taxonomy concerns vulnerabilities. Figures 8.3 through 8.6 present these vulnerabilities in order according to the average reporting date of the incidents which recorded those vulnerabilities. Nearly half of the incidents in the CERT®/CC records mention specific vulnerabilities (1,948 incidents, 45.3%). There was generally not enough information to determine whether the vulnerabilities were due to design or implementation problems, as divided in Figure 6.9. Some information on vulnerabilities due to configuration errors was available and is discussed in Section 8.1.3.5.

***8.1.3.1 Password Vulnerabilities*** - The most frequently recorded vulnerability involved various problems with passwords, which were mentioned in 938 incidents (21.8%, column 18, Figure 8.3).

There were 16 different combinations of keywords that indicated password problems. Most of the password vulnerabilities were in three categories: *password files*, generally indicating that a password file had been copied (592 incidents, 13.8%, 63.1% of password vulnerabilities), *password cracking*, which indicated that passwords had been determined by the operation of a password cracking tool (448 incidents, 10.4%, 47.8% of password vulnerabilities), and *weak passwords*, which could be easily guessed (156 incidents, 3.6%, 16.6% of password vulnerabilities). It is interesting to note that password cracking was recorded as an exploited vulnerability in nearly an order of magnitude *more* incidents than the tools used for the cracking (448 incidents mentioning password cracking, compared to 52 incidents mentioning password cracking *tools*). See Appendix A for further details.

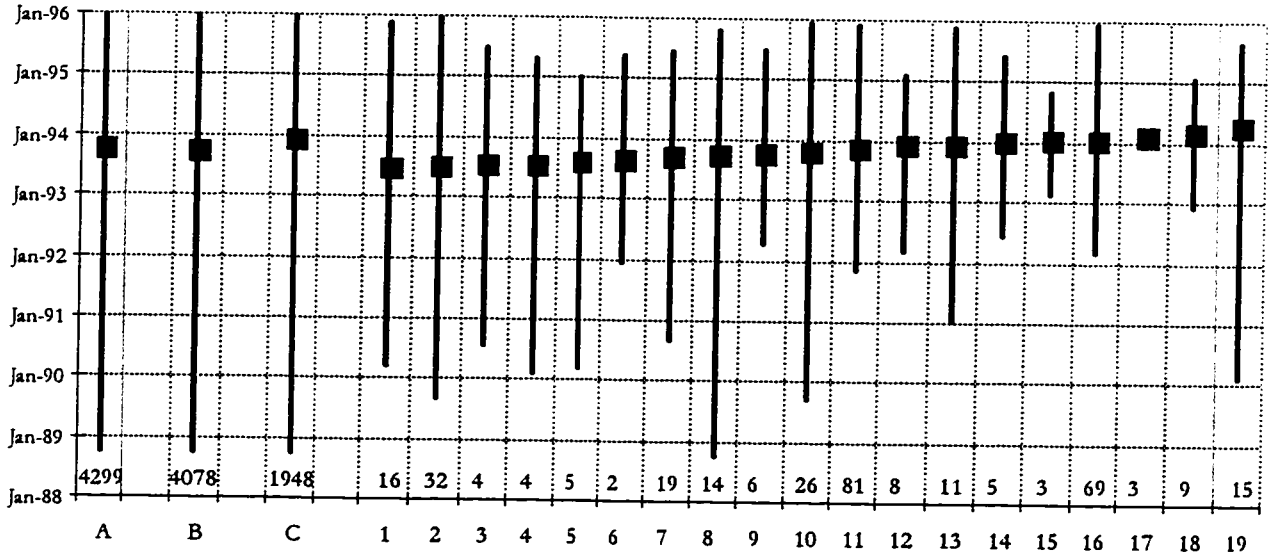


**Figure 8.4. Range and Mean Incident Reporting Dates for Methods of Operation - Access - Part 2**
Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **4 - crontab** | **10 - misc/unknown** | **15 - news** |
| **B - All Access** | **5 - rwall** | **11 -rdist** | **16 - yp** |
| **C - All vulnerabilities** | **6 - dev** | **12 - rexd** | **17 - modload** |
| **1 - decode, uudecode** | **7 - expreserve** | **13 - x** | **18 - gopher** |
| **2 - telnet** | **8 - ping** | **14 - dns** | **19 - smtp** |
| **3 - bugs** | **9 - libc** | | |

***8.1.3.2 SMTP*** - SMTP (Simple Mail Transfer Protocol), is the TCP/IP transport protocol for transferring mail messages between Mail Transfer Agents (MTAs) [LyR93:186]. The most well-known MTA is the *sendmail* program originally included in the Berkeley distribution of UNIX. Sendmail has the reputation of being the mailer that is the "most plagued with security problems" [GaS96:497]. This was confirmed in the CERT®/CC incident records which contain 447 incidents with references to *sendmail* (Figure 8.5 column 8, 10.4% of all incidents, 22.9% of vulnerabilities),

and an additional 15 incidents with references to *SMTP* (Figure 8.4 column 19, 0.4% of all incidents, 0.8% of vulnerabilities).

***8.1.3.3 Mail*** - Related closely to the SMTP and sendmail vulnerabilities are those vulnerabilities associated with the keyword *mail*, which were recorded in 333 incidents (Figure 8.5 column 5, 7.7% of all incidents, 17.1% of vulnerabilities). This category includes *mail spoofing* (210 incidents), *mail bombs* (44 incidents), *binmail* (39 incidents), *mailrace* (36 incidents), and *mail abuse* (28 incidents). Further information is given in Appendix A.

***8.1.3.4 Trusted hosts*** - Trusted host is described by Garfinkel and Spafford as follows:

> *Trusted host* is a term that was invented by the people who developed the Berkeley UNIX networking software. If one host trusts another host, then any user who has the same username on both hosts can log in from the trusted host to the other computer without typing a password [GaS96:516].

The CERT®/CC records indicate there were 249 incidents where a problem with an implementation of trusted hosts was recorded (Figure 8.3 column 20, 5.8% of all incidents, 12.8% of vulnerabilities). Appendix A indicates these problems primarily involved the use of the two files that are used to designate the trusted hosts. On a network basis, this is done in the *hosts.equiv* file, which was mentioned in 52 incidents (1.2% of all incidents, 2.7% of vulnerabilities). Individual users can establish trust for their username through the *.rhosts* file, which was mentioned in 210 incidents (4.9% of all incidents, 10.8% of vulnerabilities).

***8.1.3.5 Configuration*** - Network software must be configured properly in order for it to be secure. Some investigators have concluded that improper configuration may be the cause of most UNIX security problems [GaS96:273]. Although configuration problems appear significant, they were not identified in the majority of CERT®/CC incident records. Configuration was identified as a problem in a total of 244 incidents (Figure 8.3 column 13, 5.7% of all incidents, 12.5% of vulnerabilities). Of these, 158 incident records identify this problem through the keyword *configuration*, but an additional 96 incidents stated the configuration problem was specifically an *open server* which did not have proper access controls implemented to prevent its use (see Appendix A).

***8.1.3.6 TFTP*** - Many early versions of *TFTP*, the trivial file transfer protocol, did not restrict access to certain directories [GaS96:506]. These insecure versions of *TFTP* could then be used by anyone on the Internet to transfer critical files, such as the system's password file. Figure 8.3 column 9 depicts the reporting dates of the 238 incidents which recorded the exploitation of *TFTP* vulnerabilities (5.5% of all incidents, 12.2% of vulnerabilities). It is interesting to note that the

average reporting date for these incidents is nearly a year prior to the average for all incidents. Perhaps this indicates this vulnerability became less of a problem over time.

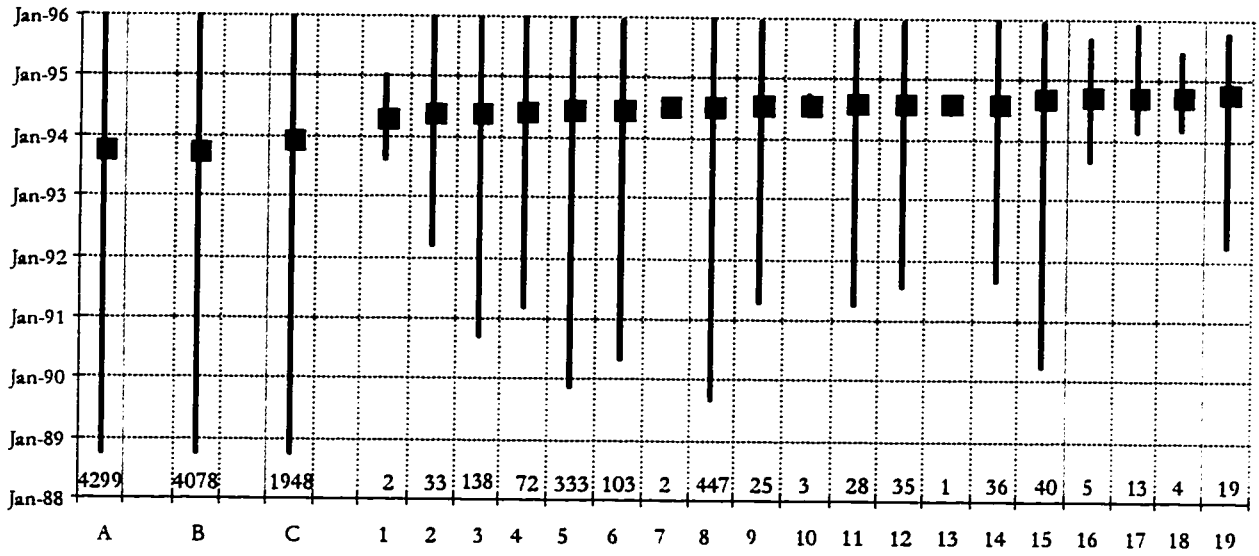


**Figure 8.5. Range and Mean Incident Reporting Dates for Methods of Operation - Access - Part 3**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **4 - irc** | **10 - time** | **15 - rsh/rlogin** |
| **B - All Access** | **5 - mail** | **11 - finger** | **16 - snmp** |
| **C - All vulnerabilities** | **6 - nis** | **12 - rpc** | **17 - autoreply** |
| **1 - inetd** | **7 - dump** | **13 - suid** | **18 - tcp** |
| **2 - icmp** | **8 - sendmail** | **14 - source hiding** | **19 - talk** |
| **3 - nfs** | **9 - lp** | | |

***8.1.3.7 NIS*** - The *Network Information Service (NIS)* is a client/server system developed by Sun Microsystems to simplify the administration of network system files [Sob95:163]. On networks using *NIS*, important information, such as user names and passwords are maintained in a centralized database shared within the network. Exploitation of *NIS* was recorded as a method of operation in 103 of the CERT®/CC incidents (Figure 8.5 column 6, 2.4% of all incidents, 5.3% of vulnerabilities). An additional 69 incidents recorded *YP* as a vulnerability (Figure 8.4 column 16, 1.6% of all incidents, 3.5% of vulnerabilities). *YP* was the name of the early version of the *NIS*. See Appendix A for additional details.

***8.1.3.8 FTP*** - The *File Transfer Protocol (FTP)* has more security features than *TFTP*. It was still identified in 170 of the CERT®/CC incident records (Figure 8.3 column 15, 4.0% of all incidents, 8.7% of vulnerabilities).

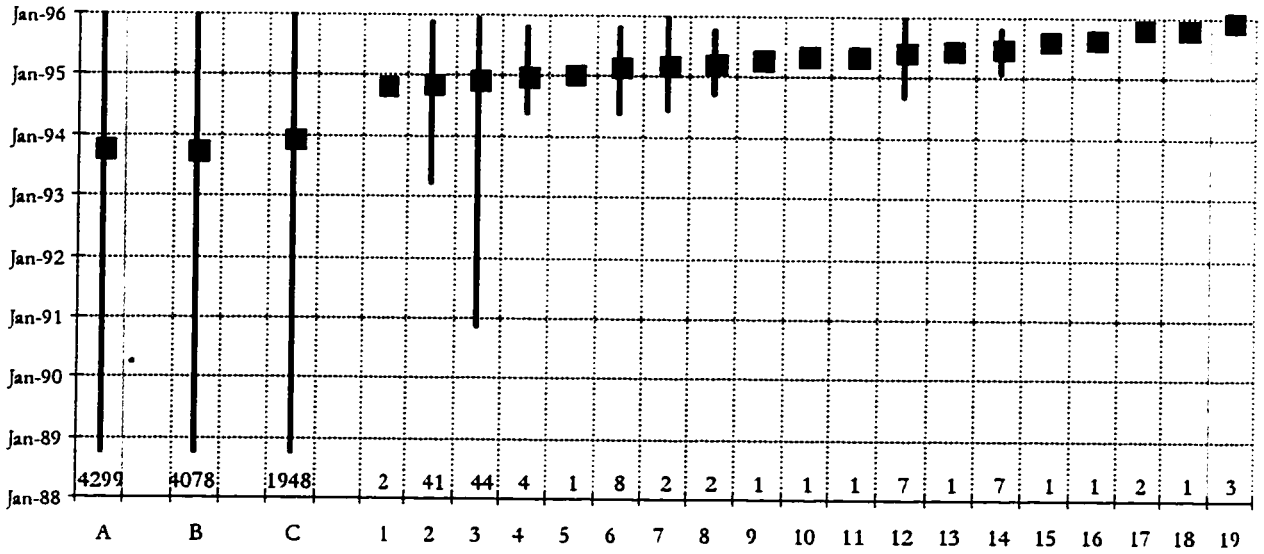


**Figure 8.6. Range and Mean Incident Reporting Dates for Methods of Operation - Access - Part 4**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **4 - login** | **10 - pipe** | **15 - domain** |
| **B - All Access** | **5 - utmp** | **11 - traceroute** | **16 - ps** |
| **C - All vulnerabilities** | **6 - udp** | **12 - http** | **17 - fork** |
| **1 - nntp** | **7 - majordomo** | **13 - ident** | **18 - syslog** |
| **2 - loadmodule** | **8 - mouse** | **14 - rexec** | **19 - windows nt** |
| **3 - portmap** | **9 - kernal** | | |

***8.1.3.9 NFS*** - Appendix A shows that a variety of *Network File System (NFS)* commands were used by intruders in 138 attacks on the Internet summarized in the CERT®/CC records (Figure 8.3 column 3, 3.2% of all incidents, 7.1% of vulnerabilities).

***8.1.3.10 Other vulnerabilities*** - Appendix A gives details of other vulnerabilities identified in the CERT®/CC records.

***8.1.3.11. Types of Accounts*** - Figure 8.7 summarizes information in the CERT®/CC records about the types of accounts attacked. As would be expected, *user accounts* were the most frequently identified (121 incidents, 2.8% of all incidents, 54.3% of identified accounts). Other accounts that were identified in multiple incidents included *system accounts*, (53 incidents, 1.2% of all incidents, 23.8% of identified accounts), *sync accounts* (38 incidents, 0.9% of all incidents, 17.0% of identified accounts), and *guest accounts* (35 incidents, 8.1% of all incidents, 15.7% of identified accounts). *Sync* and *guest* accounts became well-known vulnerabilities early in the period of the CERT®/CC records [GaS96:228]. While both of these accounts continued to be problems throughout the period, the average reporting dates were well prior to the average for all incidents, which may indicate these vulnerabilities were being corrected.

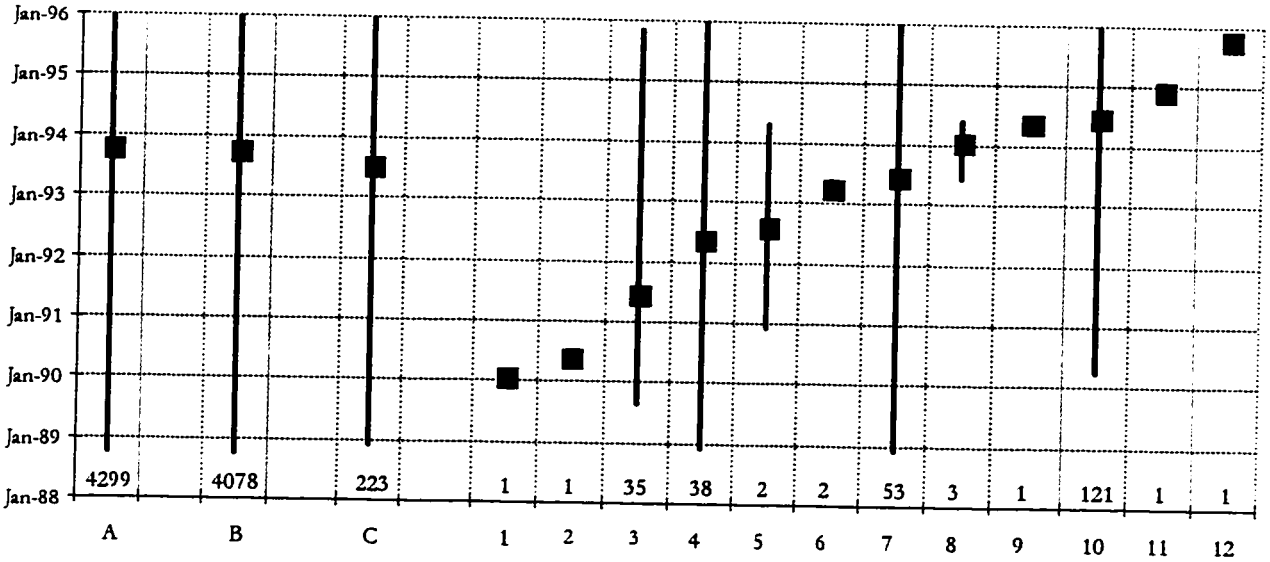


**Figure 8.7. Range and Mean Incident Start for Methods of Operation - Access - Type of Account**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **2 - demo account** | **6 - me account** | **10 - user account** |
| **B - All Access** | **3 - guest account** | **7 - system account** | **11 - uucp account** |
| **C - All Type of account** | **4 - sync, sync account** | **8 - lp account** | **12 - nobody account** |
| **1 - parity account** | **5 - field, field account** | **9 - bin account** | |

**8.1.4. Results** - The CERT®/CC incident records contain 419 incidents with some information about the *results* category of the taxonomy (Figure 8.8, 9.7%). The largest category of these results was *theft of service* (Figure 8.3 column 3, 290 incidents, 6.7% of all incidents, 69.2% of results), which primarily consisted of *FTP abuse* (263 incidents, 6.1% of all incidents, 62.8% of results).

Interestingly, *disclosure of information* was another large category of *results* (252 incidents, 5.9% of all incidents, 60.1% of results), which consisted primarily of *software piracy* (221 incidents, 5.1% of all incidents, 52.7% of results), and the nickname for pirate software, *warez* (73 incidents, 1.7% of all incidents, 17.4% of results). *FTP abuse*, *software piracy*, and *warez* are all related, so it makes sense that they were recorded in a similar number of incidents. Software piracy was not considered a security incident by the CERT®/CC, and their reporting was not encouraged. As such, this category may be underreported in the CERT®/CC records. In addition, very few other incidents reported anything else in the disclosure of information category.

There were 170 incidents in the CERT®/CC records that gave information about the *corruption of information* (4.0% of all incidents, 40.6% of results), which primarily consisted of *modifying or deleting logs* (103 incidents, 2.4% of all incidents, 24.6% of results), or of *deleting files* (71 incidents, 1.7% of all incidents, 17.0% of results).

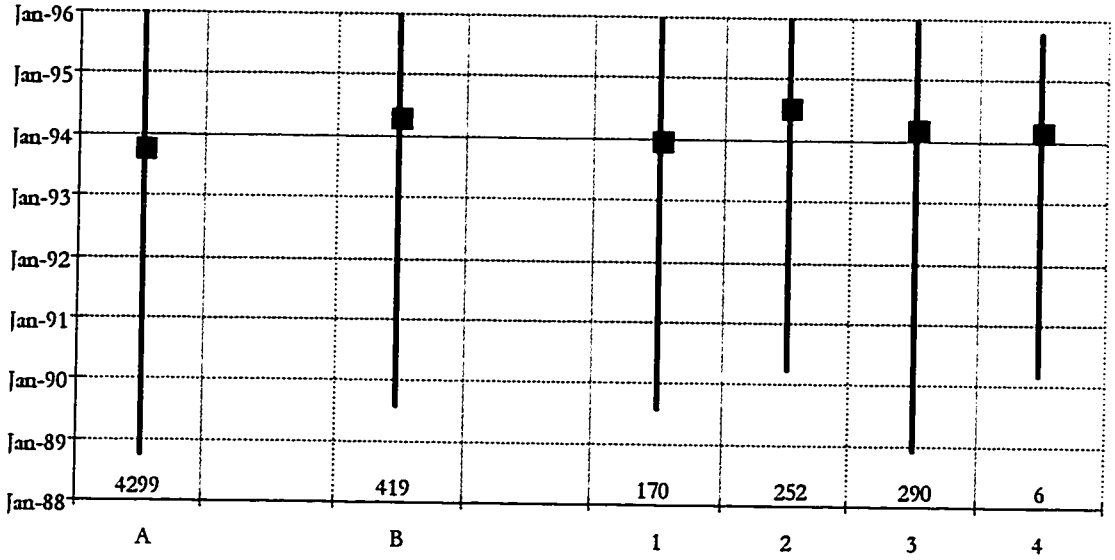


**Figure 8.8. Range and Mean Incident Reporting Dates for Methods of Operation - Results**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents** **1 - corruption of information** **3 - theft of service** **4 - denial-of-service**
**B - All Results** **2 - disclosure of information**

Figure 8.8 shows only 6 incidents in the *denial-of-service* category. As stated in Chapter 7 and 11, the number of *denial-of-service* incidents, or incidents in which denial-of-service was mentioned in the CERT®/CC records, was actually 143. The difference between these two numbers shows the lack of information in the CERT®/CC records about actual results. In other words, the CERT®/CC records recorded 143 denial-of-service *attacks* or *attempts*, but indicated *actual* denial-of-service resulted in only 6 incidents. It is not to say that the others did not result in successful *denial-of-service*, just that this information was not recorded in the CERT®/CC records.

**8.1.5. Objectives** - The last figure in this series, Figure 8.9 shows the information available in the CERT®/CC records concerning *objectives*. As with the *attacker* category on the opposite end of the taxonomy (Figure 6.9), little information was found in the CERT®/CC records concerning *objectives*. Only 56 incident records (1.3%) mention the achievement of *objectives*. Of these, 44 incidents mentioned *financial gain* (1.0% of all incidents, 78.6% of objectives), which was primarily *credit card fraud* (27 incidents, 0.6% of all incidents, 48.2% of objectives). The other 12 incidents mentioned *damage* (0.3% of all incidents, 21.4% of objectives).

**8.1.6. Summary of Methods of Operation** - This research revealed the CERT®/CC records to be inconsistent in the amount of information in the categories in the taxonomy for this research (Figure 6.9). *Tools* and *Access* had the most information, while the *results* category information was

limited to only one type of attack, and little information was recorded about the beginning and ending blocks of the taxonomy, *attackers* and *objectives*.

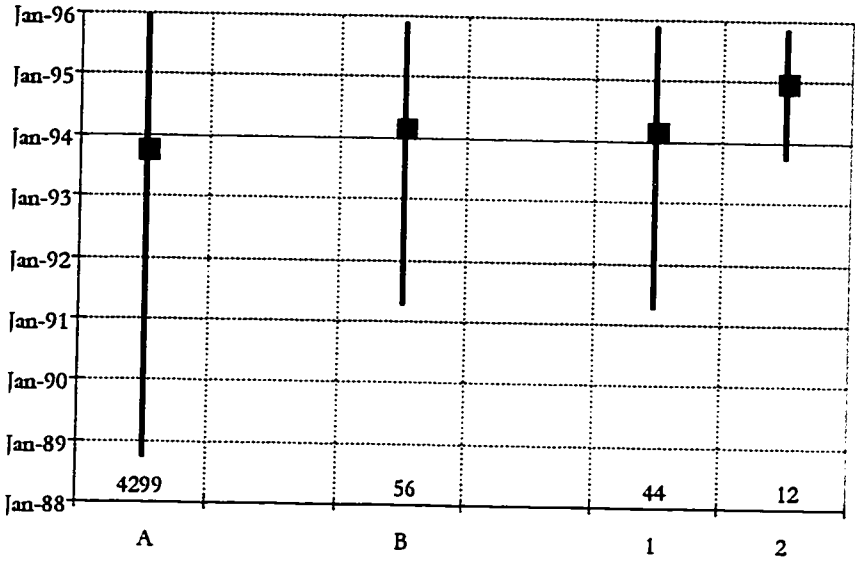


**Figure 8.9. Range and Mean Incident Reporting Dates for Methods of Operation - Objectives**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents** **B - All Objectives** **1 - financial gain** **2 - damage**

The data plotted above are given in numerical form in Table 8.1. More detailed information on the methods of operation is given in Appendix A. (NOTE: The "Delta" column indicates the differences between the mean report for that category and the mean report for all incidents).

**Table 8.1. Methods of Operation**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| all | 1-Oct-88 | 24-Oct-93 | 30-Dec-95 | 4299 | 0.0 |
| Attackers | 14-Oct-89 | 19-Feb-93 | 15-Oct-95 | 35 | -246.9 |
| hackers | 14-Oct-89 | 29-May-92 | 6-Jul-95 | 18 | -513.1 |
| vandals | 19-Dec-90 | 28-Nov-93 | 15-Oct-95 | 17 | 34.9 |
| Tools | 13-Sep-90 | 11-Oct-94 | 24-Dec-95 | 778 | 352.2 |
| user command | 14-Apr-93 | 10-May-93 | 25-Jun-93 | 3 | -167.4 |
| scripts or programs | 4-Dec-88 | 10-Feb-94 | 24-Dec-95 | 661 | 109.0 |
| to get root | 13-Sep-90 | 28-Jun-94 | 20-Dec-95 | 59 | -605.4 |
| keystroke logging | 10-Mar-93 | 6-Jun-93 | 2-Sep-93 | 2 | -140.4 |
| logic bomb | 27-Feb-92 | 27-Feb-92 | 27-Feb-92 | 1 | 28.3 |
| denial-of-service tools | 4-Jan-92 | 9-Sep-94 | 6-Dec-95 | 29 | 113.6 |
| password cracker | 14-Jan-92 | 15-Feb-94 | 19-Dec-95 | 52 | 247.2 |
| sniffer | 7-Sep-90 | 25-Oct-94 | 8-Dec-95 | 245 | 319.7 |
| Trojan horse | 4-Dec-88 | 21-Nov-93 | 24-Dec-95 | 450 | 365.7 |
| toolkit | 24-Jun-92 | 3-Feb-95 | 24-Dec-95 | 185 | 466.6 |
| to get root | 24-Jun-92 | 19-Feb-95 | 8-Dec-95 | 77 | 459.2 |
| scanners | 24-Feb-93 | 26-Jan-95 | 24-Dec-95 | 111 | 482.6 |

**Table 8.1. Methods of Operation (continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| autonomous agent | 22-Dec-88 | 30-Mar-93 | 20-May-95 | 7 | -208.3 |
| worm | 2-Nov-88 | 2-Jan-91 | 12-Jan-93 | 2 | 119.0 |
| viruses | 14-May-91 | 20-Feb-94 | 20-May-95 | 5 | -1026.4 |
| Access | 1-Oct-88 | 13-Oct-93 | 30-Dec-95 | 4078 | -11.0 |
| vulnerability | 1-Oct-88 | 15-Dec-93 | 30-Dec-95 | 1948 | 52.4 |
| install | 5-Dec-88 | 5-Dec-88 | 5-Dec-88 | 1 | -1784.4 |
| rcp | 29-Jun-89 | 29-Jun-89 | 29-Jun-89 | 1 | -1578.4 |
| autofinder | 2-Apr-90 | 2-Apr-90 | 2-Apr-90 | 1 | -1301.4 |
| netfind | 13-Apr-92 | 13-Apr-92 | 13-Apr-92 | 1 | -559.4 |
| motd | 3-Feb-92 | 5-Jun-92 | 21-Jan-93 | 3 | -505.7 |
| shutdown | 9-Mar-92 | 4-Aug-92 | 30-Dec-92 | 2 | -446.4 |
| forward | 15-Mar-90 | 20-Oct-92 | 13-Jan-95 | 6 | -369.4 |
| emacs | 30-Nov-92 | 30-Nov-92 | 30-Nov-92 | 1 | -328.4 |
| tftp | 1-Oct-88 | 5-Dec-92 | 25-Nov-95 | 238 | -322.7 |
| uucp | 27-Sep-90 | 9-Dec-92 | 23-Oct-95 | 9 | -319.3 |
| chfn/chsh | 1-Apr-90 | 4-Jan-93 | 10-Oct-95 | 2 | -293.4 |
| bin/shell | 29-Jun-90 | 12-Jan-93 | 23-Oct-95 | 15 | -285.1 |
| configuration | 5-Dec-88 | 6-Feb-93 | 28-Dec-95 | 244 | -259.9 |
| fparel | 16-Feb-93 | 16-Feb-93 | 16-Feb-93 | 1 | -250.4 |
| ftp | 1-Oct-88 | 7-Mar-93 | 24-Dec-95 | 170 | -230.7 |
| mem | 18-Jul-90 | 17-Apr-93 | 1-May-95 | 3 | -190.1 |
| history | 24-May-93 | 24-May-93 | 24-May-93 | 1 | -153.4 |
| password vulnerability | 1-Oct-88 | 15-Jun-93 | 28-Dec-95 | 938 | -131.1 |
| mult | 14-Jun-92 | 1-Jul-93 | 20-May-94 | 10 | -114.8 |
| trusted hosts | 5-Dec-88 | 4-Jul-93 | 24-Dec-95 | 249 | -112.2 |
| decode, uudecode | 15-Mar-90 | 6-Jul-93 | 17-Nov-95 | 16 | -110.0 |
| telnet | 1-Sep-89 | 14-Jul-93 | 20-Dec-95 | 32 | -102.2 |
| bugs | 2-Aug-90 | 30-Jul-93 | 25-Jun-95 | 4 | -85.6 |
| crontab | 5-Feb-90 | 3-Aug-93 | 2-May-95 | 4 | -81.9 |
| rwall | 14-Mar-90 | 17-Aug-93 | 11-Jan-95 | 5 | -68.2 |
| dev | 20-Dec-91 | 2-Sep-93 | 18-May-95 | 2 | -51.9 |
| expreserve | 2-Sep-90 | 24-Sep-93 | 16-Jun-95 | 19 | -29.6 |
| ping | 1-Oct-88 | 10-Oct-93 | 31-Oct-95 | 14 | -14.2 |
| libc | 13-Apr-92 | 23-Oct-93 | 28-Jun-95 | 6 | -0.9 |
| misc/unknown | 20-Sep-89 | 8-Nov-93 | 8-Dec-95 | 26 | 15.3 |
| rdist | 8-Nov-91 | 23-Nov-93 | 27-Nov-95 | 81 | 30.1 |
| rexd | 13-Mar-92 | 16-Dec-93 | 31-Jan-95 | 8 | 53.1 |
| x | 13-Jan-91 | 26-Dec-93 | 23-Nov-95 | 11 | 62.6 |
| dns | 14-Jun-92 | 10-Jan-94 | 5-Jun-95 | 5 | 78.4 |
| news | 22-Feb-93 | 25-Jan-94 | 4-Nov-94 | 3 | 93.3 |
| yp | 9-Mar-92 | 27-Jan-94 | 19-Dec-95 | 69 | 94.8 |
| modload | 30-Jan-94 | 16-Feb-94 | 28-Feb-94 | 3 | 115.3 |
| gopher | 14-Dec-92 | 18-Mar-94 | 27-Jan-95 | 9 | 145.0 |
| smtp | 15-Feb-90 | 22-Apr-94 | 25-Aug-95 | 15 | 180.3 |
| inetd | 21-Aug-93 | 3-May-94 | 14-Jan-95 | 2 | 191.1 |
| icmp | 24-Mar-92 | 9-Jun-94 | 26-Dec-95 | 33 | 228.3 |
| nfs | 20-Sep-90 | 10-Jun-94 | 20-Dec-95 | 138 | 229.5 |
| irc | 12-Mar-91 | 16-Jun-94 | 23-Dec-95 | 72 | 234.9 |
| mail | 14-Nov-89 | 26-Jun-94 | 28-Dec-95 | 333 | 245.2 |
| nis | 4-May-90 | 29-Jun-94 | 19-Dec-95 | 103 | 248.0 |
| dump | 7-Jul-94 | 24-Jul-94 | 10-Aug-94 | 2 | 272.6 |
| sendmail | 1-Sep-89 | 25-Jul-94 | 26-Dec-95 | 447 | 274.3 |
| lp | 15-Apr-91 | 8-Aug-94 | 17-Dec-95 | 25 | 288.2 |
| time | 14-Jun-94 | 12-Aug-94 | 23-Sep-94 | 3 | 292.3 |

**Table 8.1. Methods of Operation (continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| vulnerability (continued) | 1-Oct-88 | 15-Dec-93 | 30-Dec-95 | 1948 | 52.4 |
| finger | 4-Apr-91 | 15-Aug-94 | 14-Dec-95 | 28 | 295.1 |
| rpc | 25-Jul-91 | 16-Aug-94 | 13-Dec-95 | 35 | 295.9 |
| suid | 17-Aug-94 | 17-Aug-94 | 17-Aug-94 | 1 | 296.6 |
| source hiding | 29-Aug-91 | 19-Aug-94 | 27-Dec-95 | 36 | 298.7 |
| rsh/rlogin | 26-Mar-90 | 19-Sep-94 | 19-Dec-95 | 40 | 329.8 |
| snmp | 2-Sep-93 | 2-Oct-94 | 9-Sep-95 | 5 | 342.8 |
| autoreply | 5-Mar-94 | 10-Oct-94 | 27-Nov-95 | 13 | 350.7 |
| tcp | 17-Mar-94 | 11-Oct-94 | 19-Jun-95 | 4 | 352.4 |
| talk | 7-Apr-92 | 1-Nov-94 | 18-Oct-95 | 19 | 373.1 |
| nntp | 22-Oct-94 | 11-Nov-94 | 1-Dec-94 | 2 | 382.6 |
| loadmodule | 4-Apr-93 | 25-Nov-94 | 23-Nov-95 | 41 | 396.7 |
| portmap | 13-Nov-90 | 22-Dec-94 | 13-Dec-95 | 44 | 424.5 |
| login | 23-May-94 | 4-Jan-95 | 23-Oct-95 | 4 | 437.4 |
| utmp | 27-Jan-95 | 27-Jan-95 | 27-Jan-95 | 1 | 459.6 |
| udp | 23-May-94 | 11-Mar-95 | 22-Oct-95 | 8 | 503.5 |
| majordomo | 14-Jun-94 | 22-Mar-95 | 28-Dec-95 | 2 | 513.6 |
| mouse | 23-Sep-94 | 2-Apr-95 | 11-Oct-95 | 2 | 524.6 |
| kernal | 4-May-95 | 4-May-95 | 4-May-95 | 1 | 556.6 |
| pipe | 19-May-95 | 19-May-95 | 19-May-95 | 1 | 571.6 |
| traceroute | 27-May-95 | 27-May-95 | 27-May-95 | 1 | 579.6 |
| http | 14-Sep-94 | 10-Jun-95 | 28-Dec-95 | 7 | 594.5 |
| ident | 3-Jul-95 | 3-Jul-95 | 3-Jul-95 | 1 | 616.6 |
| rexec | 31-Jan-95 | 7-Jul-95 | 22-Oct-95 | 7 | 620.9 |
| domain | 24-Aug-95 | 24-Aug-95 | 24-Aug-95 | 1 | 668.6 |
| ps | 6-Sep-95 | 6-Sep-95 | 6-Sep-95 | 1 | 681.6 |
| fork | 27-Oct-95 | 4-Nov-95 | 13-Nov-95 | 2 | 741.1 |
| syslog | 12-Nov-95 | 12-Nov-95 | 12-Nov-95 | 1 | 748.6 |
| windows nt | 21-Dec-95 | 24-Dec-95 | 30-Dec-95 | 3 | 790.6 |
| Type of account | 5-Dec-88 | 22-Jul-93 | 24-Dec-95 | 223 | -94.4 |
| parity account | 31-Jan-90 | 31-Jan-90 | 31-Jan-90 | 1 | -1362.4 |
| demo account | 28-May-90 | 28-May-90 | 28-May-90 | 1 | -1245.4 |
| guest account | 25-Aug-89 | 15-Jun-91 | 13-Nov-95 | 35 | -861.5 |
| sync, sync account | 5-Dec-88 | 21-May-92 | 24-Dec-95 | 38 | -520.9 |
| field account, field | 7-Dec-90 | 10-Aug-92 | 15-Apr-94 | 2 | -439.9 |
| me account | 26-Feb-93 | 10-Apr-93 | 24-May-93 | 2 | -196.9 |
| system account | 5-Dec-88 | 23-Jun-93 | 21-Dec-95 | 53 | -123.0 |
| lp account | 13-Jun-93 | 29-Jan-94 | 25-May-94 | 3 | 97.3 |
| bin account | 25-May-94 | 25-May-94 | 25-May-94 | 1 | 212.6 |
| user account | 1-Apr-90 | 6-Jul-94 | 20-Dec-95 | 121 | 254.7 |
| uucp account | 21-Dec-94 | 21-Dec-94 | 21-Dec-94 | 1 | 422.6 |
| nobody | 27-Oct-95 | 27-Oct-95 | 27-Oct-95 | 1 | 732.6 |
| results | 2-Aug-89 | 5-May-94 | 26-Dec-95 | 419 | 193.2 |
| corruption of information | 2-Aug-89 | 3-Jan-94 | 26-Dec-95 | 170 | 71.2 |
| disclosure of information | 1-Apr-90 | 20-Jul-94 | 22-Dec-95 | 252 | 269.5 |
| theft of service | 6-Dec-88 | 29-Mar-94 | 22-Dec-95 | 290 | 155.9 |
| denial-of-service | 10-Mar-90 | 17-Mar-94 | 15-Oct-95 | 6 | 144.1 |
| objectives | 17-Apr-91 | 13-Mar-94 | 16-Nov-95 | 56 | 140.2 |
| financial gain | 17-Apr-91 | 15-Mar-94 | 16-Nov-95 | 44 | 141.7 |
| damage | 7-Oct-93 | 7-Jan-95 | 9-Nov-95 | 12 | 439.9 |

## 8.2. Corrective Actions

As was stated earlier, the records of the CERT®/CC are incomplete with respect to corrective actions taken during incidents. Of the 4,299 incidents, 63 incident records (14.7%) have no information on corrective actions. In another 2,848 incident records (66.2%), the only corrective action in the records, or that can be inferred from the records, is that the site or sites involved were notified.

Figure 8.10 and Table 8.2 summarizes the information about corrective actions from the 1,388 incidents (32.3%) that reported *additional* corrective actions. Appendix B presents these data in more detail. These corrective actions were classified into two broad categories: *internal actions*, and *external actions*. Internal actions are those actions that a system administrator might take to make a site or host more secure, such as restricting, configuring, or upgrading hardware or software, or by various preventive measures. External actions are those actions taken outside the organization, such as actions against the intruder, or actions involving law enforcement.

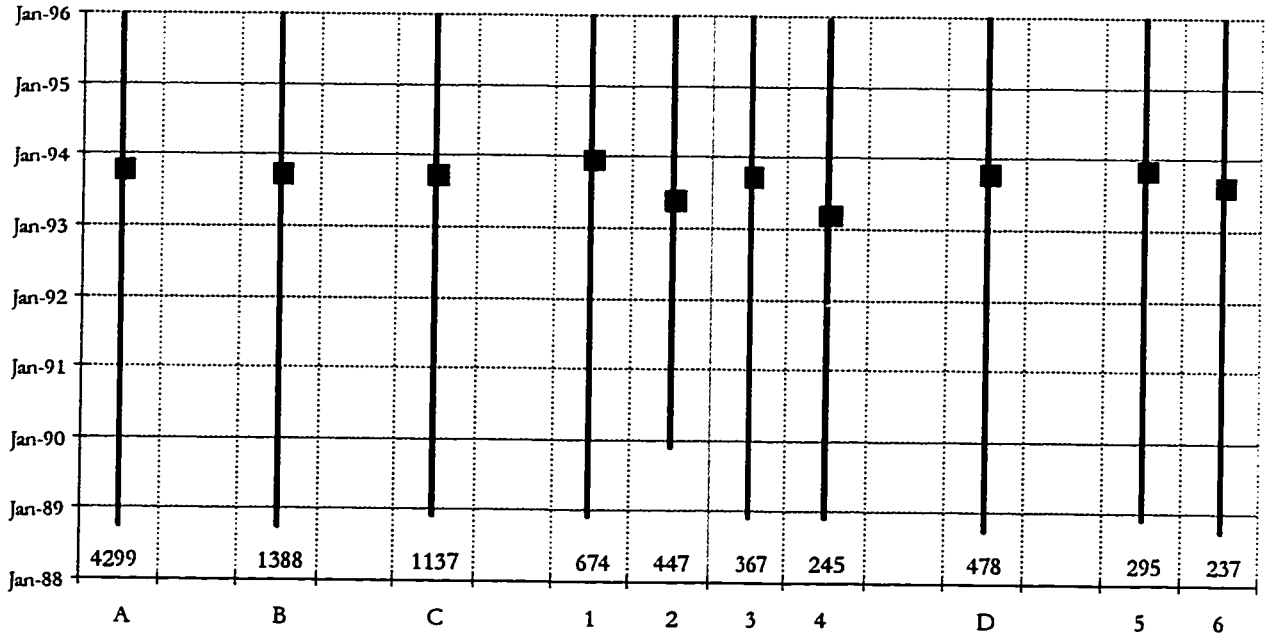


**Figure 8.10. Range and Mean Incident Reporting Dates for Corrective Actions**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Corrective Actions**
**C - All Internal Actions**
**1 - Restrict system hardware/software**
**2 - Configure system hardware/software**
**3 - Upgrade system hardware/software**
**4 - Preventive Measures**
**D - All External Actions**
**5 - Take action against intruders**
**6 - Law enforcement**

**8.2.1. Internal Actions** - Figure 8.10, columns C and 1 to 4 summarize the 1,137 CERT®/CC incidents which recorded *internal actions* (26.4% of all incidents, 81.9% of corrective actions). The most frequently mentioned corrective action was to *restrict hardware/software* (674 incidents, 15.7% of all incidents, 48.6% of corrective actions). This included actions such as *closing accounts* (460 incidents, 10.7% of all incidents, 33.1% of corrective actions), *filtering network traffic* (162 incidents, 3.8% of all incidents, 11.7% of corrective actions), and *disconnecting from the network* (124 incidents, 2.9% of all incidents, 89.3% of corrective actions).

Related to restricting systems were actions to *configure system hardware/software* (447 incidents, 10.4% of all incidents, 32.2% of corrective actions). These actions primarily involved *changing passwords* (310 incidents, 7.2% of all incidents, 22.3% of corrective actions), *securing servers/routers* (140 incidents, 3.3% of all incidents, 10.1% of corrective actions), and *restricting servers* (38 incidents, 0.9% of all incidents, 2.7% of corrective actions).

The third category of actions to correct or improve systems were actions to *upgrade system hardware/software* (367 incidents, 8.5% of all incidents, 26.4% of corrective actions). The primary actions were to *patch software* (200 incidents, 4.7% of all incidents, 14.4% of corrective actions), *reload software* (161 incidents, 3.7% of all incidents, 11.6% of corrective actions), and *upgrade software* (81 incidents, 1.9% of all incidents, 5.8% of corrective actions).

The final category of internal actions were *preventive measures* (245 incidents, 5.7% of all incidents, 17.7% of corrective actions). The primary action was to *increase monitoring* (143 incidents, 3.3% of all incidents, 10.3% of corrective actions). Software programs were also used, such as *cops* (75 incidents, 1.7% of all incidents, 5.4% of corrective actions), *crack* (28 incidents, 0.7% of all incidents, 2.0% of corrective actions), and *tripwire* (26 incidents, 0.6% of all incidents, 1.9% of corrective actions).

**8.2.2. External Actions** - Figure 8.10, columns D, 5 and 6 summarize the 478 CERT®/CC incidents which recorded *external actions* (11.1% of all incidents, 34.4% of corrective actions). These external actions were placed in two categories: *actions against intruders* (295 incidents, 6.9% of all incidents, 48.6% of corrective actions), and *law enforcement* (237 incidents, 5.5% of all incidents, 17.1% of corrective actions).

*Actions against intruders* included *talking to intruders* (273 incidents, 6.4% of all incidents, 19.7% of corrective actions), *punishment* (23 incidents, 0.5% of all incidents, 1.7% of corrective actions), and *arrest* (27 incidents, 0.6% of all incidents, 1.9% of corrective actions).

*Law enforcement* organizations identified included the *police* (141 incidents, 3.3% of all incidents, 10.2% of corrective actions), the *FBI* (110 incidents, 2.6% of all incidents, 10.2% of corrective actions), and the *Secret Service* (19 incidents, 0.4% of all incidents, 1.4% of corrective actions).

These data are summarized in Table 8.2. Further information about corrective actions can be found in Appendix B. (NOTE: The "Delta" column indicates the differences between the mean report for that category and the mean report for all incidents).

**Table 8.2. Corrective Actions**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| All Incidents | 1-Oct-88 | 24-Oct-93 | 30-Dec-95 | 4299 | 0.0 |
| All Corrective Actions | 1-Oct-88 | 10-Oct-93 | 30-Dec-95 | 1388 | -13.9 |
| Internal Actions | 30-Nov-88 | 4-Oct-93 | 30-Dec-95 | 1137 | -20.3 |
| Restrict System Hardware/Software | 5-Dec-88 | 30-Dec-93 | 30-Dec-95 | 674 | 66.6 |
| Configure System Hardware/Software | 30-Nov-89 | 8-Jun-93 | 24-Dec-95 | 447 | -137.5 |
| Upgrade System Hardware/Software | 30-Nov-88 | 11-Oct-93 | 28-Dec-95 | 367 | -13.0 |
| Preventive Measures | 5-Dec-88 | 22-Mar-93 | 19-Dec-95 | 245 | -215.9 |
| External Actions | 1-Oct-88 | 23-Oct-93 | 30-Dec-95 | 478 | -0.9 |
| Take Action Against Intruder | 5-Dec-88 | 14-Nov-93 | 30-Dec-95 | 295 | 20.7 |
| Law Enforcement | 1-Oct-88 | 30-Aug-93 | 28-Dec-95 | 237 | -55.4 |

## 8.3. Some Things the CERT®/CC Incidents Do Not Include

Chapter 7 and the previous sections of this Chapter have shown that the CERT®/CC records are inconsistent in completeness with respect to the taxonomy of Figure 6.9. For some parts of the taxonomy, the CERT®/CC records provided significant information. Very little information was found in the CERT®/CC records for some of the other categories of the taxonomy.

Reasons for this disparity vary. One likely cause was the relationship between the information and the mission of the CERT®/CC. As discussed previously, the CERT®/CC has been responsible for incident response on the Internet. In order to properly respond to incidents, CERT®/CC personnel needed to have access to information on current and past incidents. This did not mean, however, that recording information on all aspects of the incidents was necessary.

An example of information that would be important for incident response would be the information in the *access* category of the taxonomy, such as *vulnerabilities* and *access level*. This information would be necessary for CERT®/CC personnel to provide assistance in a timely manner. On the other hand, information in other categories such as *attackers*, *results*, and *objectives*, is not as important for the CERT®/CC mission. In addition, information in these categories tends

not to be available either as soon or as often. This may explain, to some extent, why little information was found in the CERT®/CC records in these three categories.

Another possible reason for the inconsistency of the information in the CERT®/CC records is that the information was assumed. An example of this, discussed in section 8.1.2, may be the lack of information about intruders using *user commands*. In that case, CERT®/CC may have generally made the assumption that intruders routinely used user commands, and therefore they only needed to record less universal tools, such as *toolkits* or *autonomous agents*.

A final possible reason for the inconsistency in the information in the CERT®/CC records may be that the CERT®/CC does not view itself as actually being responsible for *all* security problems on the Internet. For example, a well publicized *autonomous agent* used by intruders is *viruses*, but they were mentioned in only 5 of the 4,299 incidents in the CERT®/CC records. One possible explanation is that there were other avenues available to exchange information about computer viruses. An example was the *VIRUS-L* moderated mailing list which had a focus on computer virus issues. This list was begun in 1988, around the time the CERT®/CC was formed. Because this list was available, this may have made it less likely virus information was given to the CERT®/CC. As stated by the CERT®/CC:

> The CERT® Coordination Center focuses primarily on vulnerabilities in networked systems that intruders can exploit. Viruses, though they may be transmitted over a network, are generally outside the current scope of our work. However, we are interested in hearing reports of UNIX or other mainframe viruses and about worms that could propagate via the Internet. [CER96:6-7]

### 8.4. Summary of Methods of Operation and Corrective Actions

Recording of methods of operation and corrective actions in the CERT®/CC records was not systematic or complete. As a result, this information is incomplete. Some valuable information, however, can be obtained by determining the relative frequency that various methods of operation and corrective actions appear in the CERT®/CC incident records. In the CERT®/CC records, more information was found about *Tools* and *Access*, than the other categories of the taxonomy. Very little information was in the records about the beginning and ending categories, *Attackers* and *Objectives*.

A total of 778 incidents (18.1% of all incidents) reported the use of some tool. From these records, the largest category of tools was scripts or programs (15.4%). These consisted primarily of *Trojan horses* (10.5%) and *sniffers* (5.7%). The two general categories of toolkits were tools designed to exploit privileged or root access (1.2%), and *scanners* (2.6%). These tools appeared relatively late

in the CERT®/CC records. The CERT®/CC records contain very few references to autonomous agents such as *worms*, and *viruses*. There was no mention in any of the CERT®/CC records of the use of the other two categories of tools: *Data taps*, or *Distributed tools*. Data taps are physical taps and not attacks across the Internet, which makes them much less likely to be reported to the CERT®/CC. Distributed tools do not appear in the CERT®/CC records until after the period of this research.

Nearly half of the incidents in the CERT®/CC records mention specific vulnerabilities (45.3%). The most frequently recorded vulnerability involved various problems with passwords (21.8%). Most of the password vulnerabilities were in three categories: *password files*, which indicated that a password file had been copied (13.8%), *password cracking*, generally indicating that passwords had been determined by the operation of a password cracking tool (10.4%), and *weak passwords*, which could be easily guessed (3.6%).

The reputation of *sendmail* and other mail transfer agents for being "plagued with security problems" was confirmed in the CERT®/CC incident records, which contain numerous references to *sendmail* (10.4%), *SMTP* (0.4%) and *mail* (7.7%). Problems with implementation of trusted hosts (such as the *hosts.equiv* of *.rhosts* file) was recorded in a significant number of incidents (5.8%), as was *configuration* (5.7%), *TFTP* (5.5%), *NIS* and *YP* (4.0%), *FTP* (4.0%), and *NFS* (3.2%).

The CERT®/CC incident records contained 419 incidents with some information about the *results* category of the taxonomy (9.7%). The largest category of these results was *theft of service* (6.7%), which primarily consisted of *FTP abuse* (6.1%). *Disclosure of information* was another large category of *results* (5.9%), which consisted primarily of *software piracy* (5.1%). *FTP abuse*, *software piracy*, and *warez* are all related, so it makes sense that they were recorded in a similar number of incidents.

There were 170 incidents in the CERT®/CC records that gave information about *corruption of information* (4.0%), which primarily consisted of *modifying or deleting logs* (2.4%), or of *deleting files* (1.7%).

With regard to *corrective actions*, of the 4,299 incidents, 63 incident records (14.7%) had no information on corrective actions. In another 2,848 incident records (66.2%), the only corrective action in the records, or that can be inferred from the records, is that the site or sites involved were notified.

The corrective actions reported in the CERT®/CC records were classified into two broad categories: *internal actions* (actions to make a site or host more secure, 26.4%), and *external actions*

(actions taken outside the organization). The most frequently mentioned internal actions were to *restrict hardware/software* (15.7%). Other internal actions were actions to *configure system hardware/software* (10.4%), actions to *upgrade system hardware/software* (8.5%), and *preventive measures* (5.7%). CERT®/CC incidents which recorded *external actions* (11.1%) included *actions against intruders* (6.9%), and *law enforcement* (5.5%).

For some parts of the taxonomy, the CERT®/CC records provided significant information. Very little information was found in the CERT®/CC records for some of the other categories of the taxonomy. One likely cause was that only certain categories of information were necessary for the mission of the CERT®/CC, such as *vulnerabilities* and *access level*. Other possible reasons were that the information was assumed and that the CERT®/CC does not view itself as actually being responsible for *all* security problems on the Internet. For example, the *VIRUS-L* moderated mailing list had a focus on computer virus issues, which may explain the lack of virus information in the CERT®/CC records.

*Chapter 9*

# Case Study - Site A

Nearly 10% of all incidents in the CERT®/CC records from November, 1988 through December, 1995 involved one Internet site, which was termed Site A. This Chapter presents an analysis of CERT®/CC incidents reported to have involved Site A. The analysis proceeded in a parallel manner with the analysis presented in Chapter 7. This allowed comparisons between the incidents at Site A, and all incidents. The chapter begins with a description of Site A.

## 9.1. Description of Site A

Site A is a university located in the United States. It has around 30,000 users at its main campus. The number of hosts at Site A from 1989 through 1995 was not available in the CERT®/CC records, but it could be estimated using information from the current system administrator. Site A is a class B Internet network divided into subnetworks. At the end of 1996 the site administrator indicated that half of the subnetworks were near maximum capacity for IP addresses. If we assume these subnetworks have 90% of the addresses assigned in half the subnetworks, and 25% in the remaining, this would indicate approximately 38,000 assigned addresses near the end of 1996. The actual number of hosts on the network was probably less than that number (see Chapter 2), but the number is an approximation to the upper limit.

The system administrator was able to indicate how the number of router/gateway hosts changed over the period of interest. This was used for estimating the change in the number of hosts. These estimates are given in Table 9.1. The upper limits were determined by starting with 38,000 as the number of hosts in 1996, and then using the number of router/gateway hosts to project this number to the earlier years. The assumption was made that the number of hosts was proportional to the number of router/gateway hosts. The lower limits in Table 9.1 represent approximately 75% of the upper limit.

| Year | Upper Limit | Lower Limit |
|---|---|---|
| 1989 | 500 | 350 |
| 1990 | 1,000 | 750 |
| 1991 | 2,000 | 1,500 |
| 1992 | 11,000 | 8,000 |
| 1993 | 21,000 | 15,000 |
| 1994 | 30,000 | 22,000 |
| 1995 | 35,000 | 26,000 |

**Table 9.1. Estimated Number of Hosts at Site A**

### 9.2. Site A Reporting Criteria

Since their first contact with the CERT®/CC in 1989, the systems administrators at Site A routinely reported all security incidents involving the Internet. Site administrators made it a practice to contact sites that were the source of intrusions or intrusion attempts. These messages were copied to the CERT®/CC. Security incidents that were internal to Site A were not reported to the CERT®/CC.

Some of the criteria Site A used for determining whether an incident would be reported to the CERT®/CC included:

a) repeated login attempts (5 or more),

b) root login attempts,

c) attempts to exploit known vulnerabilities.

The CERT®/CC records show that until around 1992, several sites apparently were routinely reporting all incidents to the CERT®/CC. Site A was the only Internet site that continued to report all Internet security incidents to CERT®/CC after 1992.

### 9.3. Classification of Site A Incidents

As stated earlier, including false alarms, there were 4,567 incidents reconstructed from the CERT®/CC records. Of these, 443 incidents (9.7%) were either reported by Site A, or otherwise involved Site A.

**9.3.1. False Alarms** - The Site A incidents represent nearly 10% of the CERT®/CC incidents. Of these incidents, 6 (1.4%) were determined to be false alarms. This was well below the average of 5.9% for all incidents. The relationship of false alarms to incidents is shown in Figure 9.1. This shows peaks in the number of in 1990 and 1994.

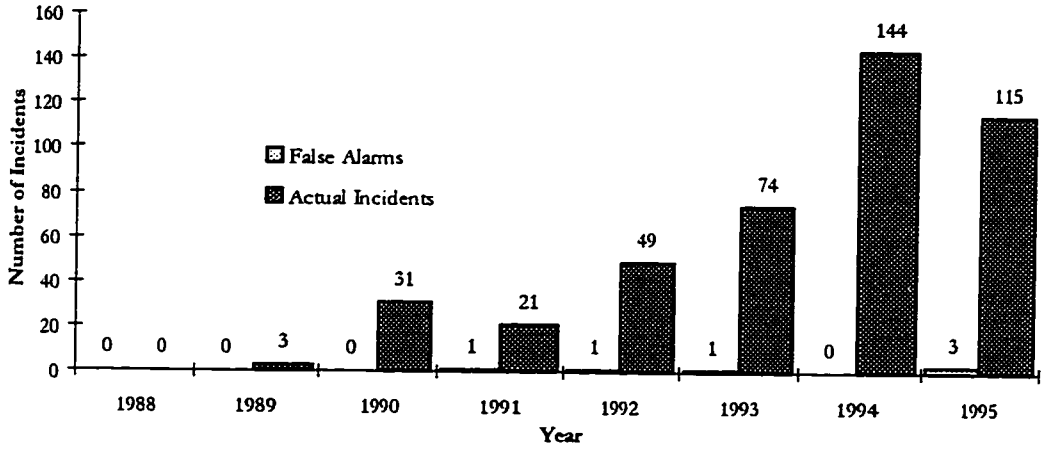


**Figure 9.1. Site A Incidents and False Alarms per Year**

The percentage of false alarms at Site A matched the rate for all incidents in 1991 (see Figure 7.4). In later years, the rate of false alarms at Site A was significantly lower than for all incidents. For example, in 1995, the rate of false alarms for all incidents was 8.5%, but only 2.5% at Site A. The correlation between the rate of false alarms at Site A and for all sites was only 20%. The small number of false alarms at Site A indicate their administrators either learned from experience, or were otherwise better able to distinguish between actual incidents and false alarms. False alarms were not included in the remaining analysis of Site A, unless otherwise indicated.

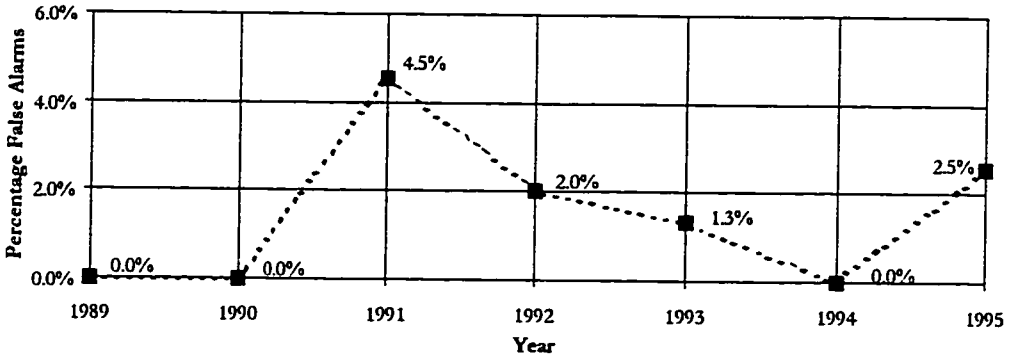


**Figure 9.2. False Alarms as a Percentage of Site A Incidents**

Figure 9.3. plots incidents per month for at Site A. This figure shows considerable difference with Figure 7.2, which plots the same information for all incidents. Like Figure 7.2, the Site A incidents peak in 1994. But Site A incidents do not show a sharp increase in 1992, nor a level off near the 1994 peak, as Figure 7.2 shows for all incidents. The correlation between incidents per month for Site A and all incidents was 76%. It is interesting, however, to note that the correlation is higher for incidents from 1988 through 1993 (73%) than for incidents from 1994 through 1995 (57%).

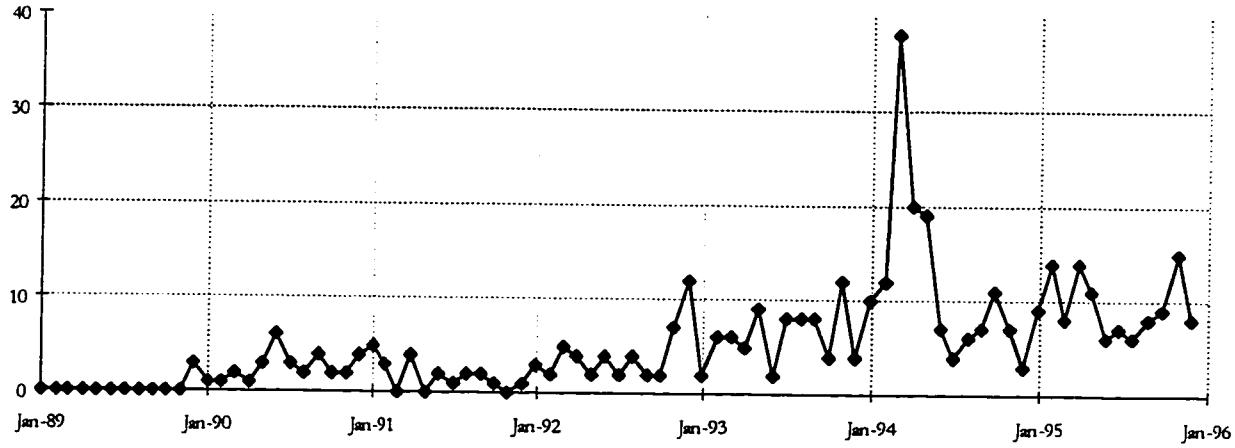


**Figure 9.3. Site A Incidents per Month**

### 9.3.2. Unauthorized Access Incidents at Site A

Most of the Site A incidents (412 incidents, 94.3% of Site A incidents) were classified as *access* incidents. Of these, 30 (6.9% of Site A incidents, 7.3% of access incidents) were classified as *root break-ins*, 61 (14.0% of Site A total, 14.8% of access incidents) were classified as *account break-ins*, and 321 (73.5% of total, 77.9% of access incidents) were unsuccessful *access attempts* (see Table 9.2).

| | Site A Incidents | |
|---|---|---|
| | **# of Incidents** | **% of Total** |
| Total Incidents | 437 | 100.0% |
| Total Access Incidents | 412 | 94.3% |
| Root break-ins | 30 | 6.9% |
| Account break-ins | 61 | 14.0% |
| Access attempts | 321 | 73.5% |

**Table 9.2. Access Incidents at Site A**

Figure 9.4 shows the average number of incidents per quarter at Site A for each of the three access categories. Unlike Figure 7.6, which shows the data for all incidents, the frequency of account and root level break-ins does not appear to show a steady increase. Access attempts, however, have a similar pattern in both figures. They both show significant peaks in activity in 1990-1991 and the first half of 1994. The correlation between the occurrence of access attempts at Site A and the occurrence for all incidents was 80%, while the correlations for root break-ins (49%) and account break-ins (53%) were considerably less.

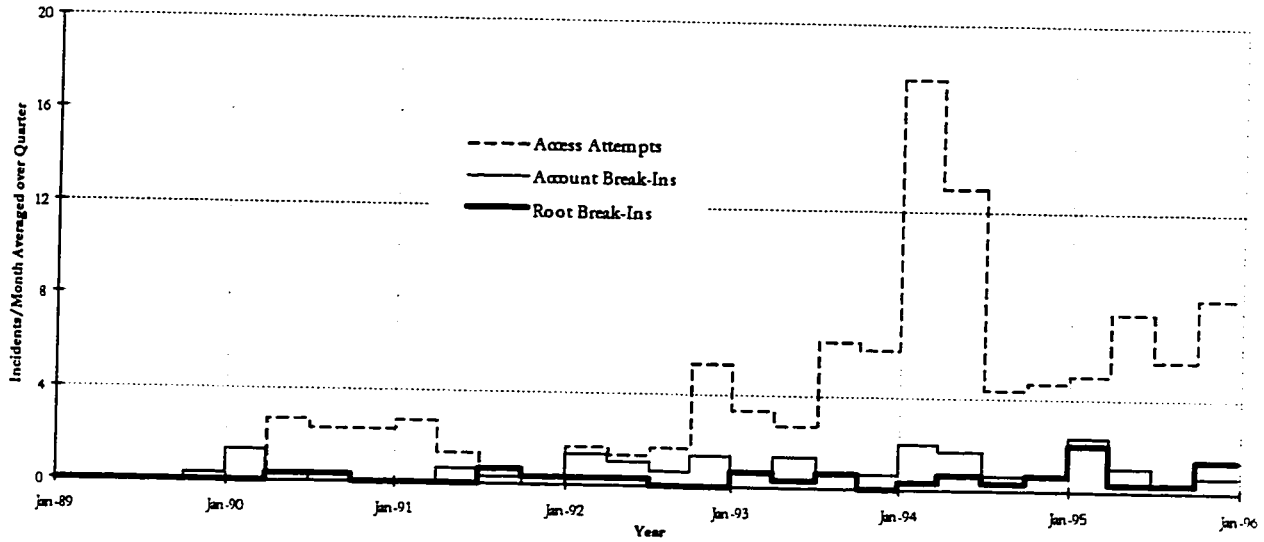


**Figure 9.4. Site A Access Incidents by Month Averaged Over Quarters**

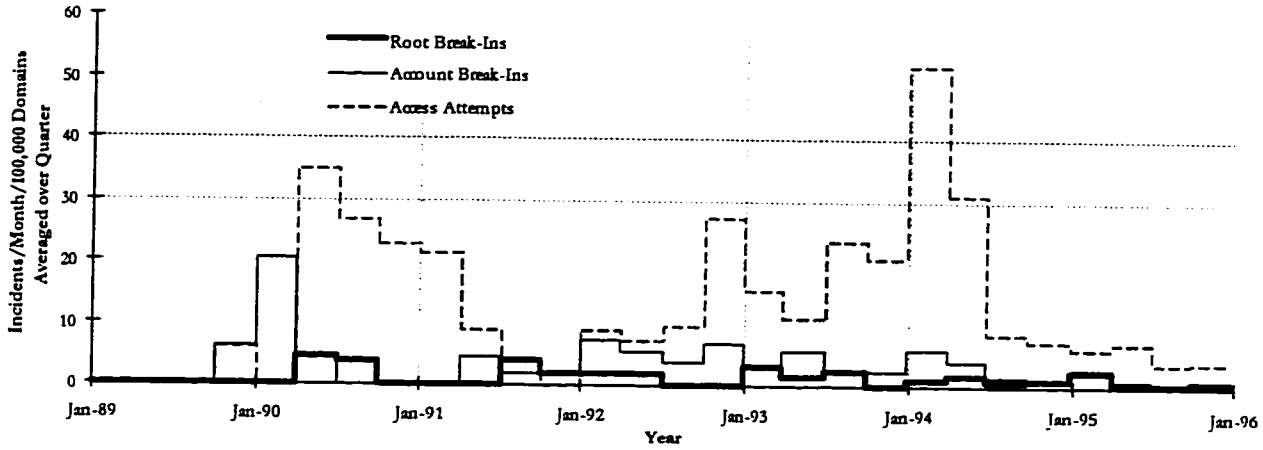


**Figure 9.5. Site A Access Incidents per 100,000 domains by Month Averaged Over Quarters**

In Figure 9.5, as in Figure 7.7, the frequency of access incidents was normalized to the growth of Internet domains. If the frequency of access incidents matched the growth of Internet domains, we would expect to see a steady average. Instead, we see significant variation in root and account level break-ins. For access attempts, peaks occur in 1990-1991, the end of 1992, and the beginning of 1994. The most notable difference between Figures 9.5 and 7.7 is that in Figure 7.7, the peak in access attempts from 1990-1991 is higher than the 1994 peak, which is not the case in Figure 9.5. A simple linear least squares fit showed none of the curves in Figure 9.5 had slopes statistically different from zero.

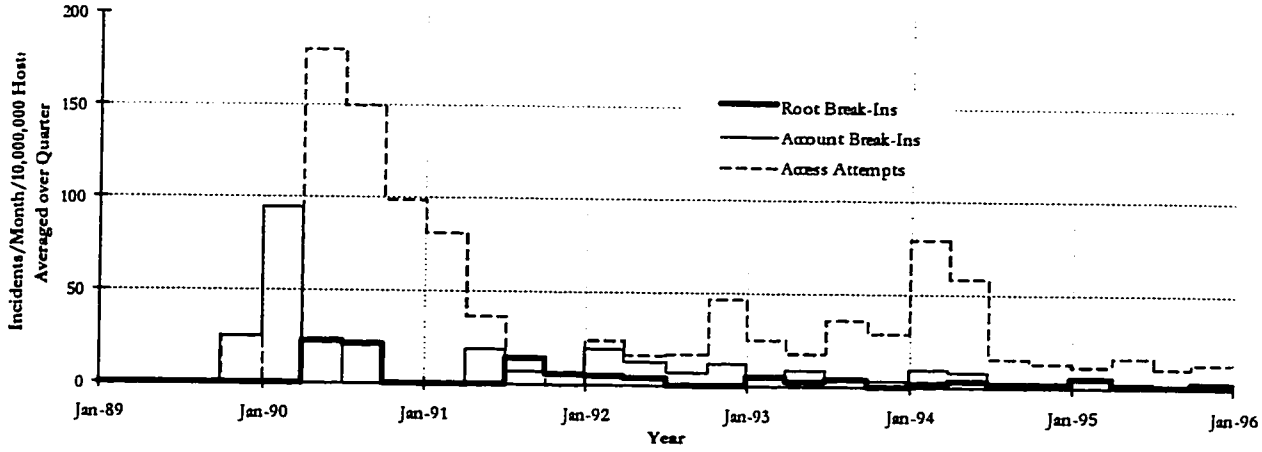


**Figure 9.6. Site A Access Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

As noted in Chapter 7, the patterns shown in Figures 7.7 and 9.5 may be influenced by the reduction in the number of Internet hosts per Internet domain after 1993. In Figures 7.8 and 9.6, the growth in Internet hosts was used to determine the average incidents per month per 10,000,000 Internet hosts. Again, if the rate of attacks matched the growth of Internet hosts, we would expect

to see a steady average. In Figure 9.6 we instead see what appears to be a steady decline in root and account level break-ins from peaks in 1990. Access attempts show peaks in 1990 and 1994. These are similar to those found in Figure 7.8. A simple linear least squares fit showed that the slope for neither the access attempts nor the root break-ins were statistically different from zero. The slope for account break-ins was statistically significant ($\alpha$ = 5%), showing that account break-ins at Site A grew over this period at a rate around 23% less than the growth of Internet hosts ($R^2$ = 6.83%).

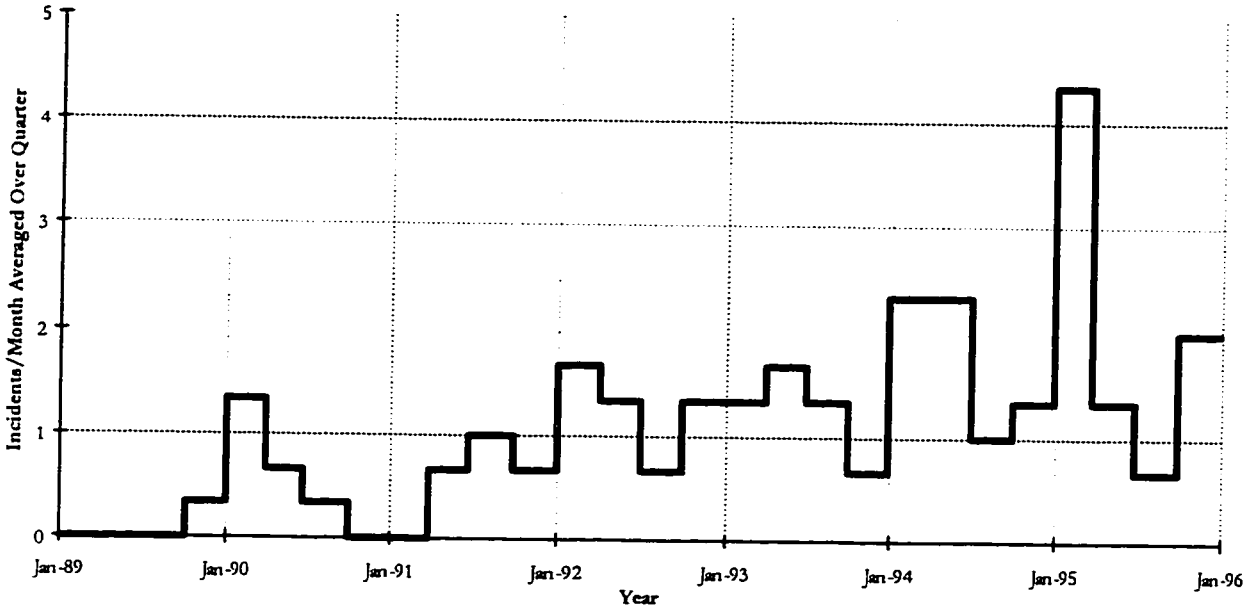


**Figure 9.7. Site A Successful Access Incidents by Month Averaged Over Quarters**

The successful root and account level break-ins are combined in Figure 9.7, as was done in Figure 7.9. Figure 9.7 shows more variation than Figure 7.9, as well as stronger seasonal variation. Five of the seven years in Figure 9.7 show more incidents in the first half of the year than in the second half. All the incidents (Figure 7.9), however, only showed a 7% correlation with month. The correlation was higher for Site A at 23%, although the effect was still not very large. The increase may result from the fact that Site A is a university with less students in the summer.

The overall pattern of access incidents looks different in Figure 9.8, which has the same data normalized to the number of hosts on the Internet (comparable to Figure 7.10). There was a strong peak when Site A first began reporting to the CERT®/CC, which was followed by a steady decline. A simple linear least squares fit showed that successful access incidents at Site A increased at a rate around 20% less than the growth of Internet hosts ($\alpha$ = 1%, $R^2$ = 20.3%).

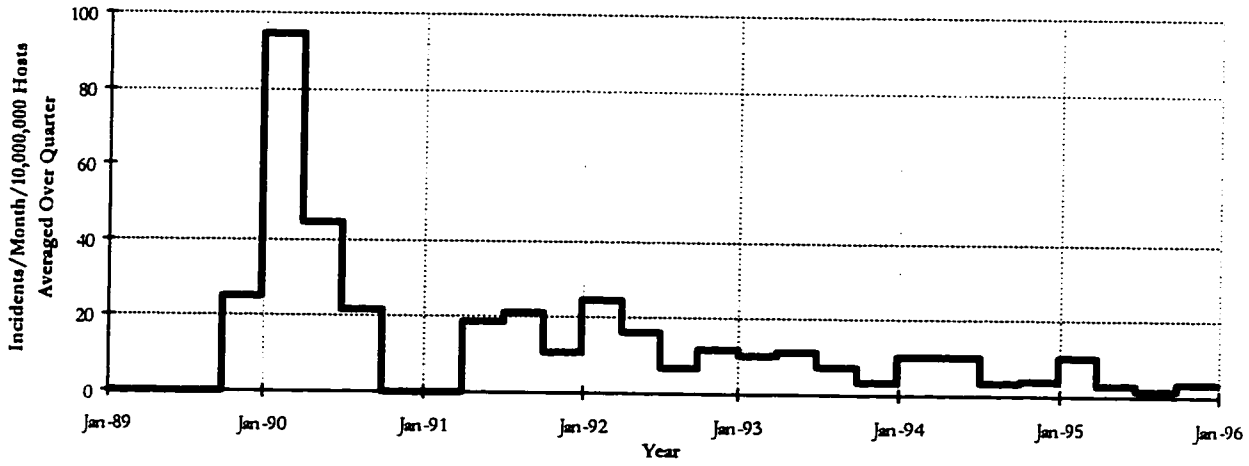


**Figure 9.8. Site A Successful Access Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

### 9.3.3. Unauthorized Use Incidents at Site A

Only a few of the Site A incidents (25 incidents, 5.7% of Site A total) were classified as *unauthorized use* incidents. Of these, 13 (3.0% of Site A total, 52.0% of use incidents) were classified as *disclosure of information* incidents, 6 (1.4% of Site A total, 24.0% of use incidents) were classified as *denial-of-service* incidents, and 6 (1.4% of Site A total, 24.0% of use incidents) were classified as *corruption of information* incidents. Table 9.3 summarizes the Site A unauthorized use incidents.

| | Site A Incidents | |
|---|---|---|
| | **# of Incidents** | **% of Total** |
| Total Incidents | 437 | 100.0% |
| Total Unauthorized Use Incidents | 25 | 5.7% |
| Disclosure Incidents | 13 | 3.0% |
| Denial-of-service Incidents | 6 | 1.4% |
| Corruption Incidents | 6 | 1.4% |

**Table 9.3. Unauthorized Use Incidents at Site A**

The small number of unauthorized use incidents makes accurate comparisons difficult between Site A and all incidents. It is still useful, however, to make the comparisons in order to see if there are significant, or important differences. The distribution of *unauthorized use* incidents at Site A was highly variable as shown in Figure 9.9, as compared to Figure 7.11 for all incidents. Both Figures, however, show increases in absolute numbers over the period.

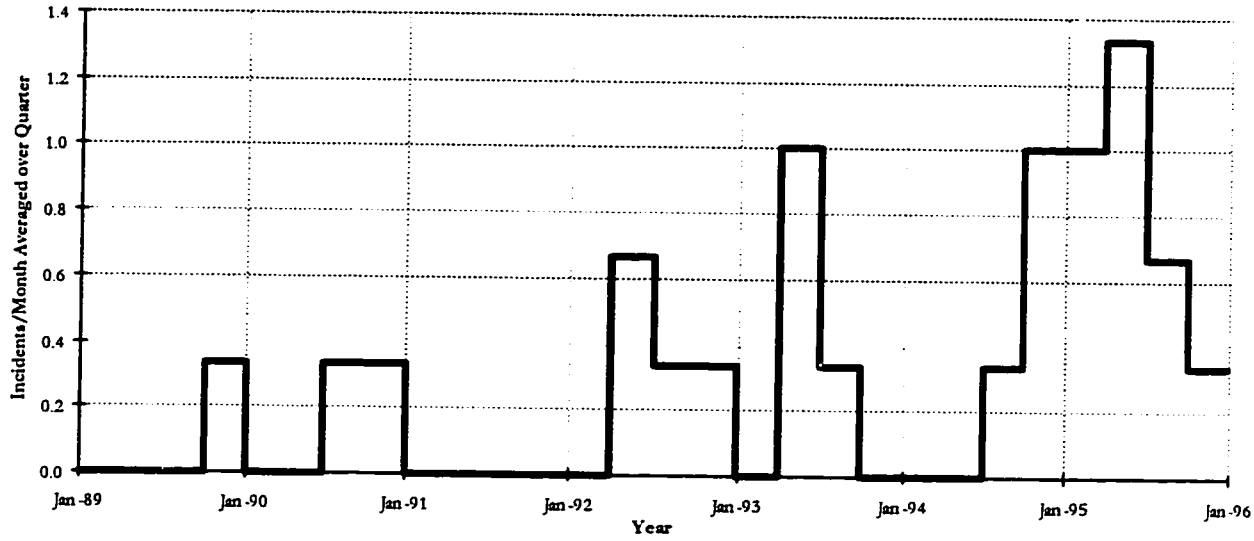


**Figure 9.9. Site A Total Unauthorized Use Incidents by Month Averaged Over Quarters**

When these data are normalized for the number of Internet hosts, a significant difference does emerge. For all incidents, as shown in Figure 7.13, the frequency of unauthorized use incidents was relatively constant. This was not the case with similar incidents at Site A, which Figure 9.10 shows decreased steadily over the period relative to the size of the Internet. This difference is reflected in a relatively low correlation between the frequency of incidents at Site A and for all incidents (45%).

A simple linear least squares fit did not show the slope of the curve in Figure 9.10 to be significantly different from zero. This would be expected with the small sample size.

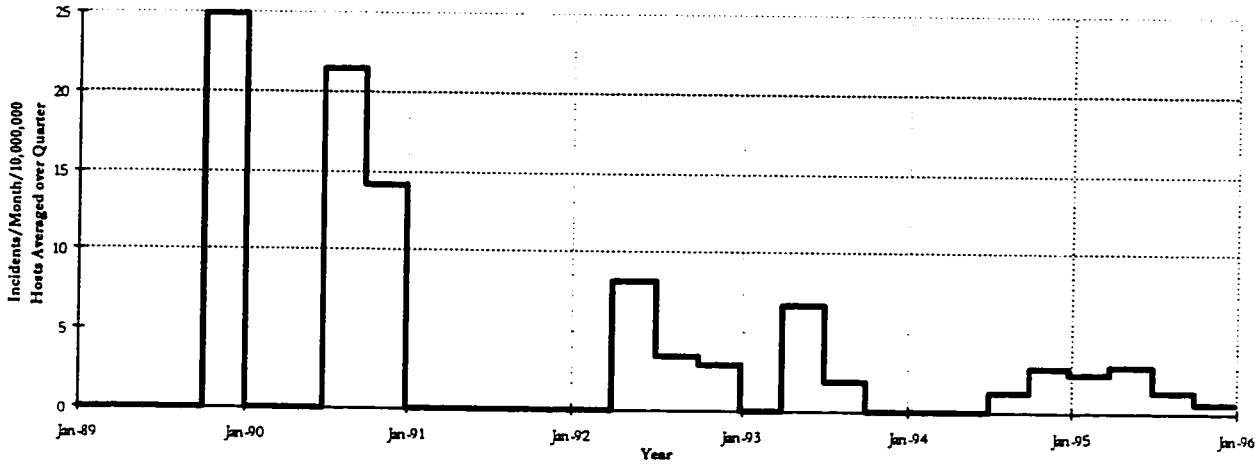


**Figure 9.10. Site A Total Unauthorized Use Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

The 13 unauthorized use incidents that were classified as *disclosure of information* incidents are shown in Figure 9.11. The rate in this Figure appears to be relatively constant after they began in 1992. This should indicate that, relative to the size of the Internet, these incidents have decreased.

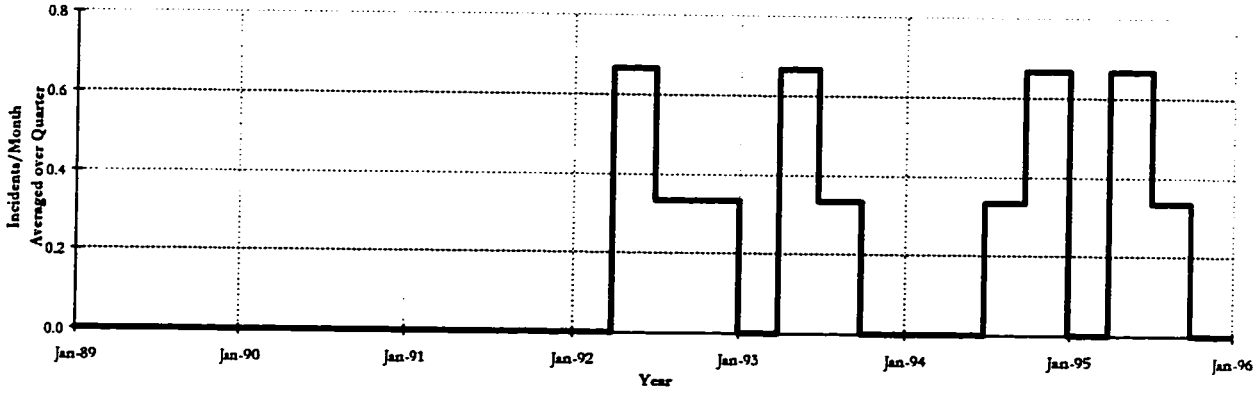


**Figure 9.11. Site A Disclosure of Information Incidents by Month Averaged Over Quarters**

This is confirmed in Figure 9.12. The sample size was small and the slope was not statistically different from zero. What patterns are seen in Figures 9.12 and 9.13 seem to differ from the pattern in Figures 7.12 and 7.14. These earlier figures show that, for all incidents, in absolute terms, there was a steady increase, and a relatively constant frequency compared to the size of the Internet.

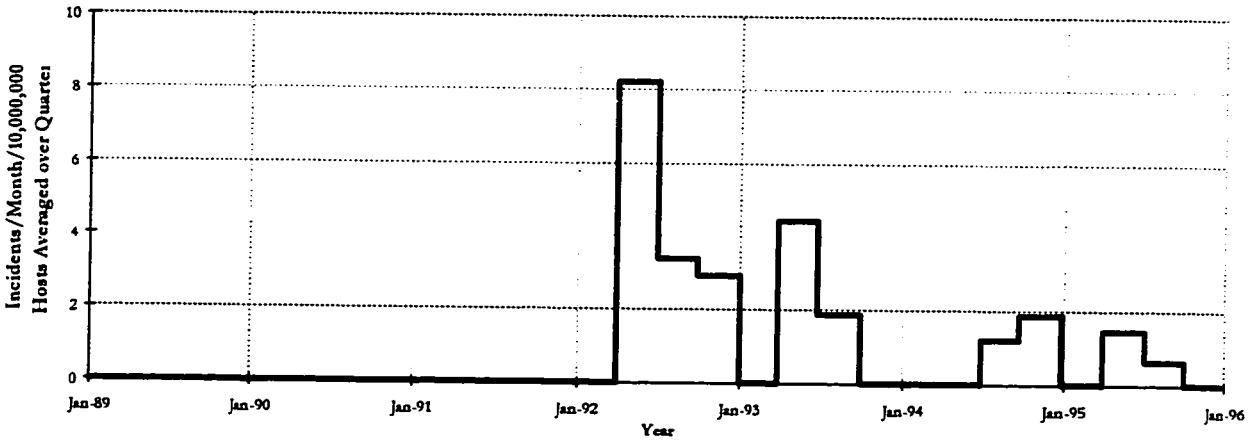


**Figure 9.12. Site A Disclosure of Information Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

There were only 6 *denial-of-service* incidents at Site A, which are plotted in absolute terms in Figure 9.13, and relative to the size of the Internet in Figure 9.14. These figures, along with figures 7.15 and 7.16 for all incidents, indicate the highest relative period for denial-of-service incidents was 1990. The small sample size, however, meant that the slope of the curve in Figure 9.14 was not statistically different from zero. At Site A, generally, denial-of-service did not appear to have been a significant problem during the period of this study.

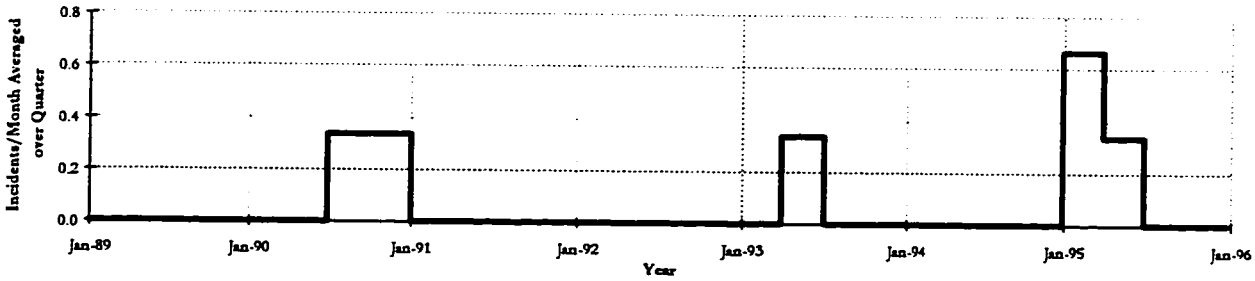


**Figure 9.13. Site A Denial-of-service Incidents by Month Averaged Over Quarters**

Of these six denial-of-service incidents at Site A, the first incident involved an attack against an Internet application. This was the same method used in once incident in 1995.

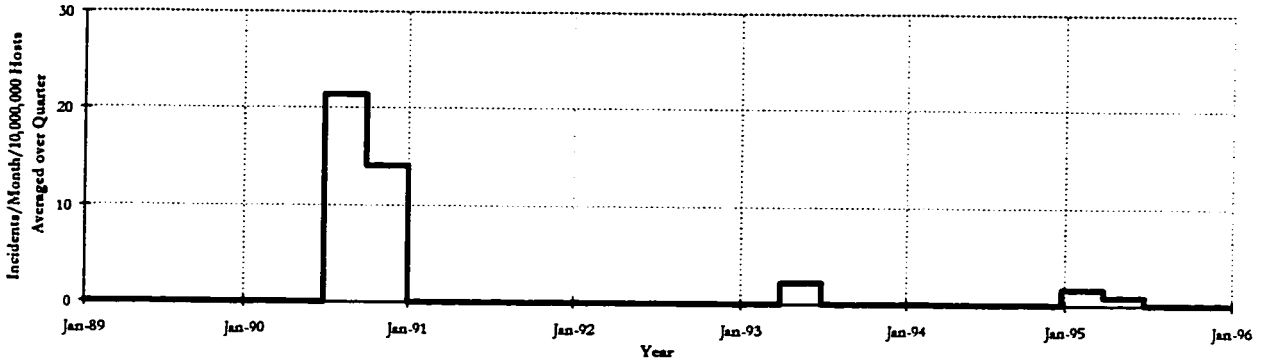


**Figure 9.14. Site A Denial-of-service Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

The second incident at Site A involved the use of *mail spam*, which indicates multiple e-mail messages were used in order to try to overwhelm a system's disk storage capacity. The 1993 incident, as well as the last incident at Site A (1995) both involved *ICMP bombs*, which overwhelm the network's control message protocol. The method of attack for the incident at the beginning of 1995 was a *talk bomb*, which is used to send ANSI escape sequences to a system in order to modify the file controlling the monitor display on a host computer. The final category of unauthorized use incidents is *corruption of information*. There were only 6 of these incidents at Site A as plotted in Figure 9.15. This shows some similarity to Figure 7.17 because of the increase in incidents in 1995.

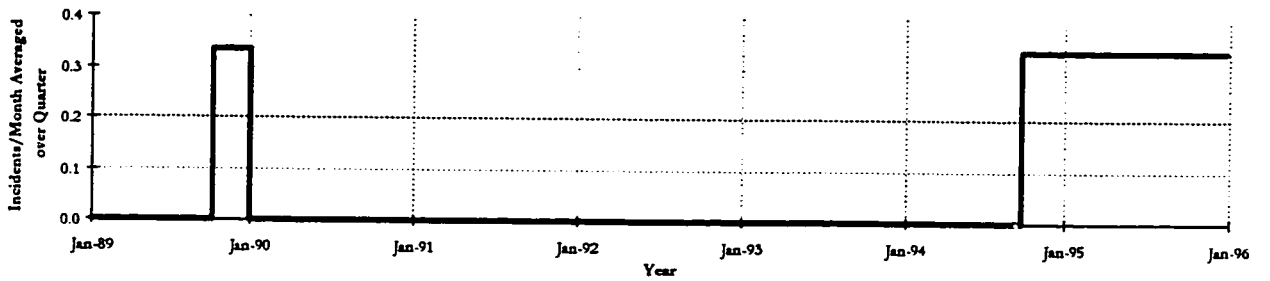


**Figure 9.15. Site A Corruption of Information Incidents by Month Averaged Over Quarters**

The corruption of information incidents are normalized for the size of the Internet in Figure 9.16, which showed these type of incidents were not a significant problem at Site A for this period.

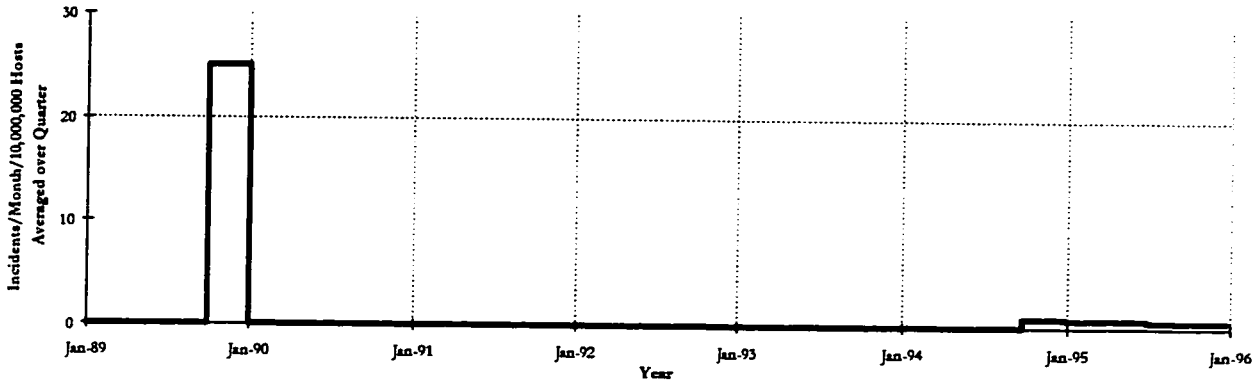


**Figure 9.16. Site A Corruption of Information Incidents per 10,000,000 Hosts by Month Averaged Over Quarters**

## 9.4. Sites per Day

Chapter 7 presented *sites per day* as an alternative measure of the severity of security incidents. Unlike the simple frequency of incidents, the sites per day measure of severity considers not only the number of incidents, but also the duration and number of sites involved. This measure still has significance when considering the activity at one site, because it indicates the severity of the incidents that the site was involved in. This can be used as a surrogate to give some indication of the severity of the incidents at that site.

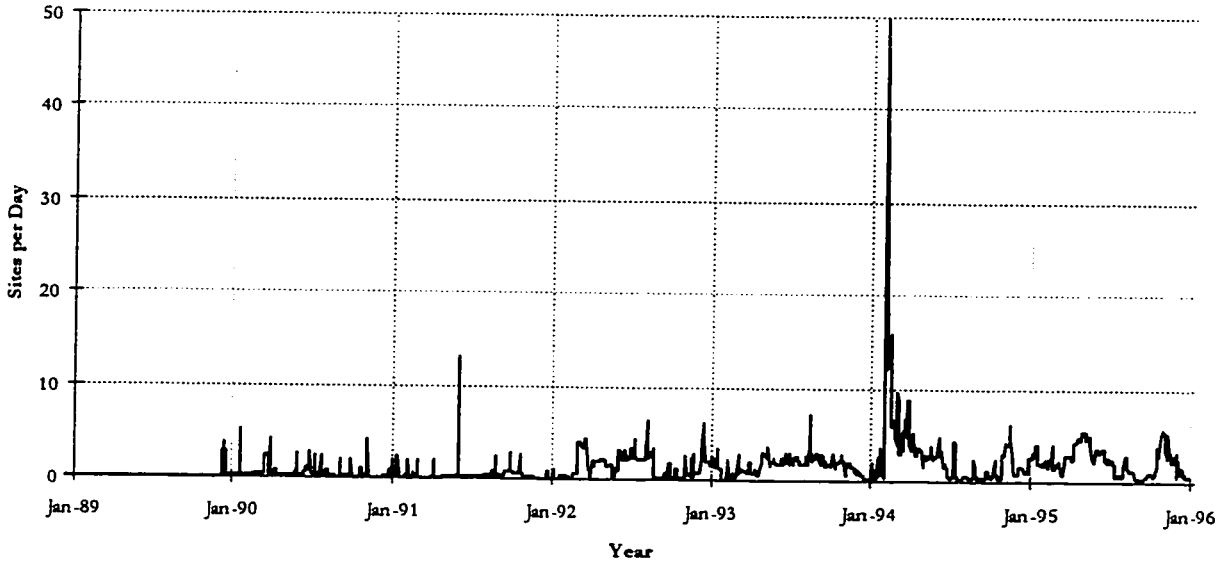


**Figure 9.17. Site A Sites per Day - All Incidents**

Figure 9.17 plots the sites per day for all incidents at Site A report to the CERT®/CC. This appears similar to all incidents as presented in Figure 7.19, particularly the large "spike" in sites per day in 1994. The correlation between the sites per day for all incidents and sites per day for Site A was 58%. Given the considerable variability of the data, this is a relatively high correlation.

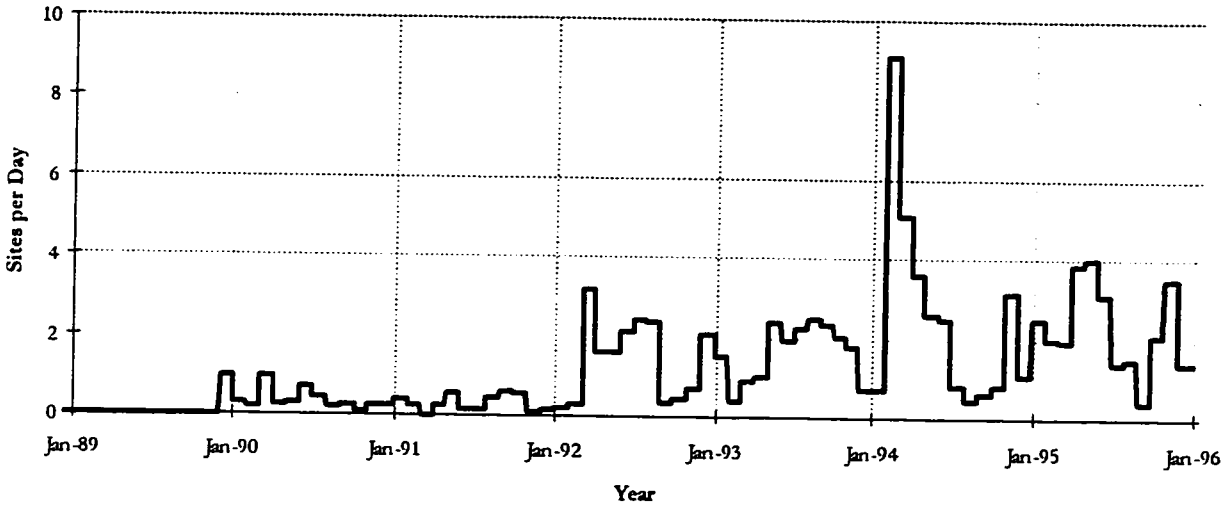


**Figure 9.18. Site A Sites per Day - All Incidents, Averaged Over Months**

As was done in Chapter 7, these data were smoothed by months and by quarter in order to more easily determine the trend in the data as shown in Figures 9.18 and 9.19. These figures look similar to the corresponding figures for all incidents, Figures 7.20 and 7.21. These all show similar spikes at the beginning of 1994, but Site A does not show a drop off in 1995. As expected, when the data are smoothed, the correlations between Site A and all incidents increase. For the monthly smoothing, the correlation was 81%, and this increased to 87% for smoothing by quarters.

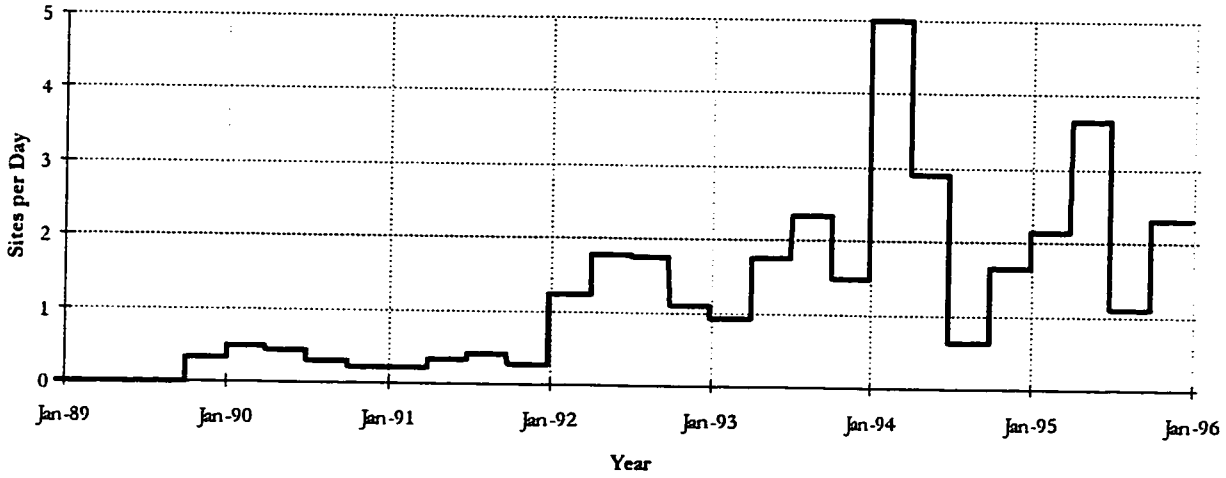


**Figure 9.19. Site A Sites per Day - All Incidents, Averaged Over Quarters**

Figure 9.20 shows the sites per day for all incidents at Site A, normalized for the size of the Internet. This shows the same pattern as Figure 7.24 for all incidents. A simple linear least squares fit showed that the growth rate of sites per day for all incidents at Site A was around 6% less than the growth rate for all Internet hosts ($\alpha$ = 1%, $R^2$ = 11.5%).

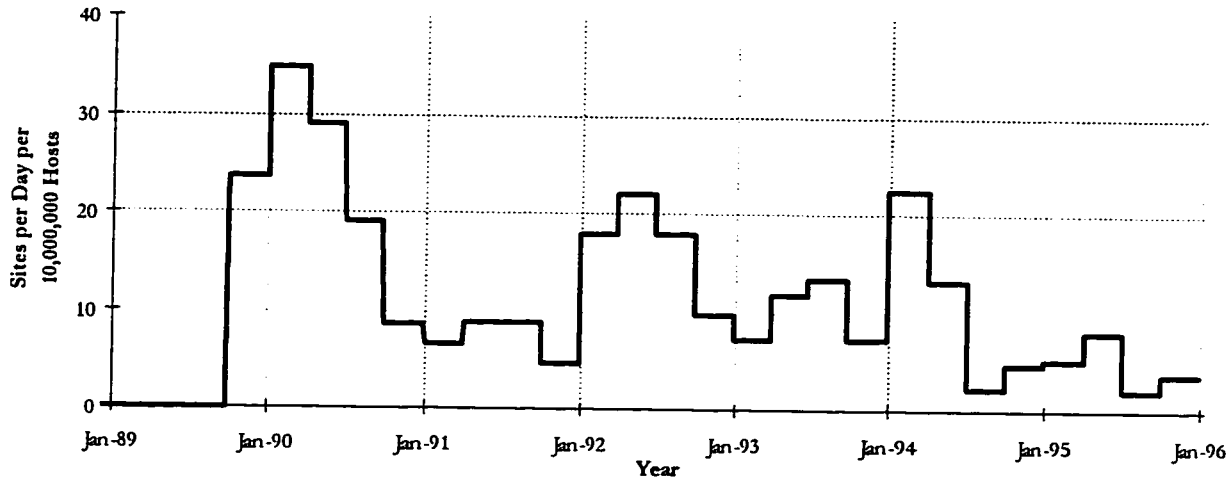


**Figure 9.20. Site A Sites per Day per 10,000,000 Hosts - All Incidents, Averaged Over Quarters**

The last three Figures of this chapter present this same information for root and account level break-ins at Site A. These correspond to the figures for all incidents (Figures 7.22, 7.23 and 7.25).

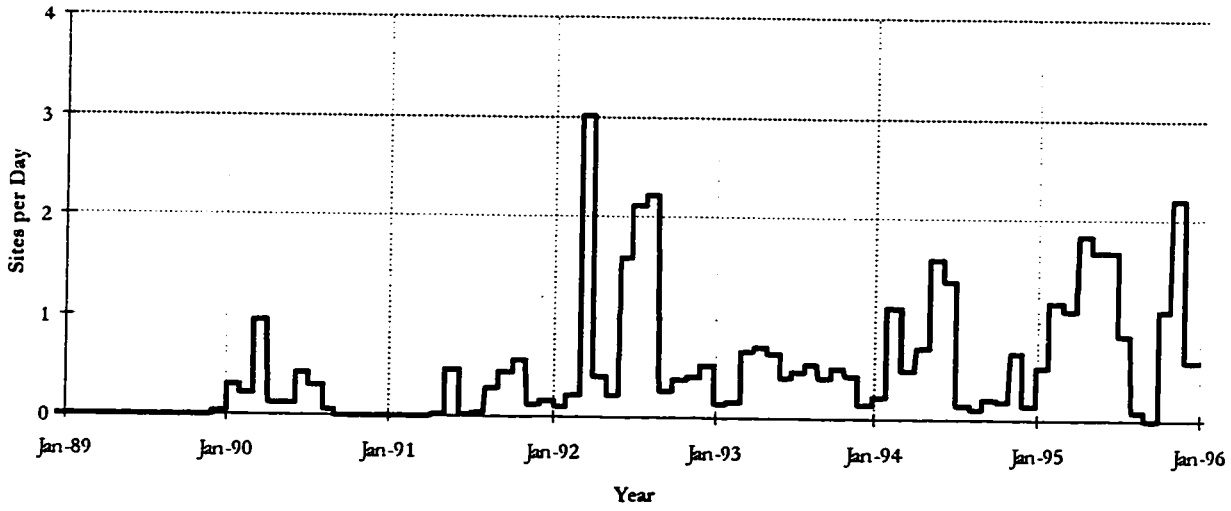


**Figure 9.21. Site A Sites per Day - Root and Account Break-ins, Averaged Over Months**

Figure 9.21 presents the Site A root and account level break-ins smoothed by month, and Figure 9.22 presents the data smoothed by quarter. These data show significant differences with the Figures in Chapter 7. The biggest difference is the lack of a "spike" in the early part of 1994. This indicates that the increased activity at this time in Figures 9.18 and 9.19 were primarily access attempts and not root or account level break-ins. This is reflected in the correlations between the

Site A data for root and account break-in incidents compared to the data for all incidents: 24% for data by days, 38% when smoothed by month, and 50% when smoothed by quarter. For the first two, these are less than half of the correlations presented earlier for all the incidents.

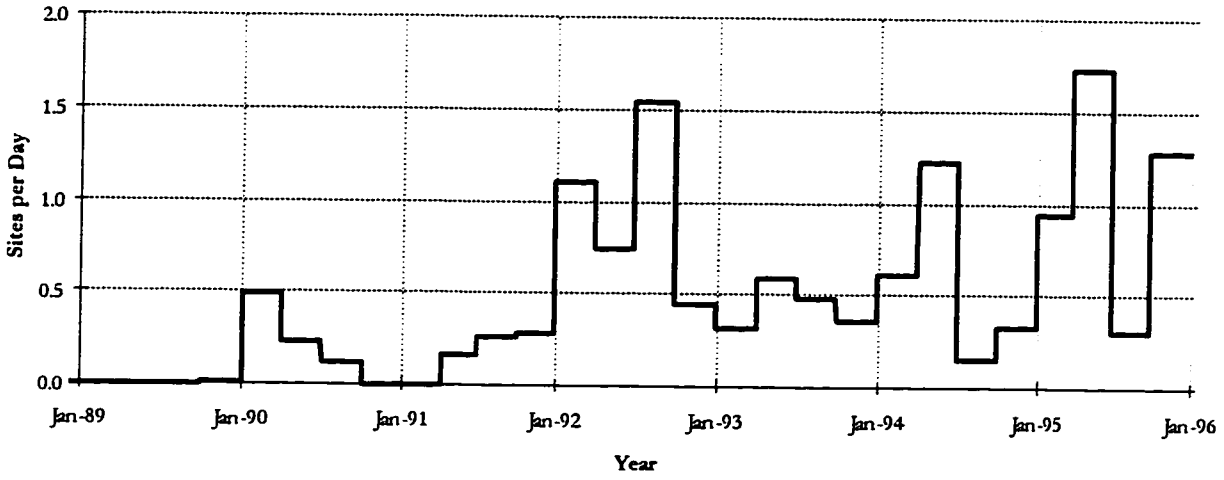


**Figure 9.22. Site A Sites per Day - Root and Account Break-ins, Averaged Over Quarters**

Figure 9.23 presents the data smoothed by quarters, but also normalized for the size of the Internet. These data show root and account level break-ins were the most significant problem in 1990, with another peak of activity in 1992. These successful intrusions were less significant relative to the size of the Internet in the years after that. A simple linear least squares fit of the curve in Figure 9.23 shows the rate of growth of sites per day for root and account level break-ins was around 12% less than the rate of growth of Internet hosts ($\alpha$ = 1%, $R^2$ = 2.99%).

These data from Site A presented in this chapter will be discussed further in Chapter 12, which will examine how representative the CERT®/CC records are of the total Internet intruder activity.

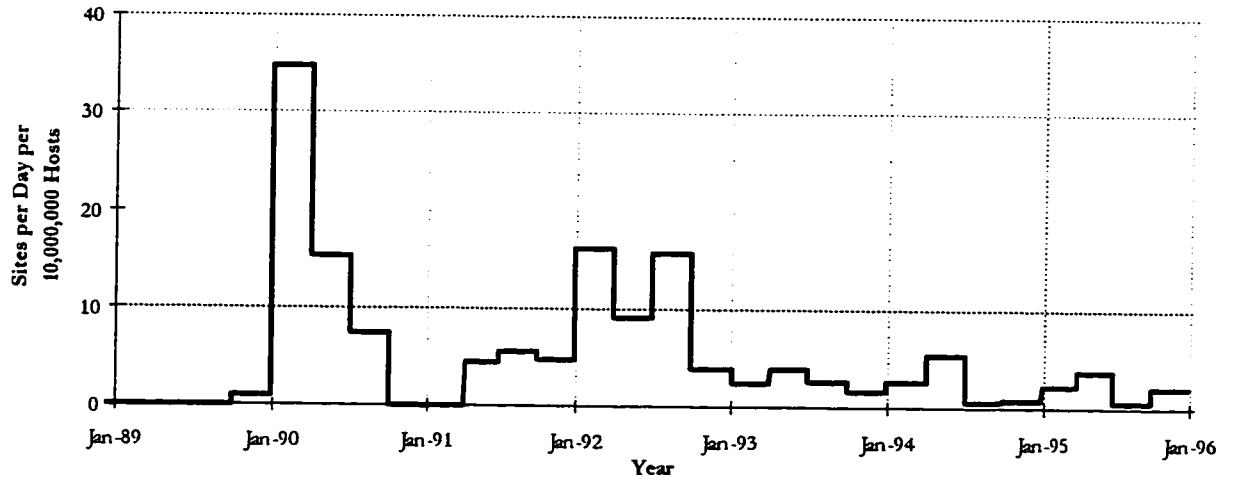


**Figure 9.23. Site A Sites per Day per 10,000,000 Hosts - Root and Account Break-ins, Averaged Over Quarters**

### 9.5. Summary of Case Study - Site A

Nearly 10% of all incidents in the CERT®/CC records from November, 1988 through December, 1995 involved one Internet site, which was termed Site A. Site A is a university located in the United States. It has around 30,000 users at its main campus. Since their first contact with the CERT®/CC in 1989, the systems administrators at Site A routinely reported all security incidents involving the Internet. Some of the criteria Site A used for determining whether an incident would be reported to the CERT®/CC included 1) repeated login attempts (5 or more), 2) root login attempts, and 3) attempts to exploit known vulnerabilities.

Of the 4,567 incidents reconstructed from the CERT®/CC records, 443 incidents (9.7%) were either reported by Site A, or otherwise involved Site A. Of these incidents, 6 (1.4%) were determined to be false alarms. Most of the Site A incidents (94.3%) were classified as *access* incidents: *root break-ins* (6.9% of Site A total), *account break-ins* (14.0% of Site A total), and *access attempts* (77.9%) were unsuccessful . The correlation between the occurrence of access attempts at Site A and the occurrence for all incidents was 80%, while the correlations for root break-ins (49%) and account break-ins (53%) were considerably less. As with all incidents, incidents in the three categories of access incidents at Site A grew at a rate less than the growth of Internet hosts, although this could only be shown statistically for account break-ins which grew over this period at a rate around 23% less than the growth of Internet hosts. Only a few of the Site A incidents (5.7% of Site A total) were classified as *unauthorized use* incidents.

Using sites per day as the measure of incident severity, the correlation between site per day for all incidents and for Site A was 58%. When the data were smoothed by month, the correlation increased to 81%, and this increased to 87% for smoothing by quarters. The growth rate of sites per day for all incidents at Site A was around 9% less than the growth rate for all Internet hosts. For root and account level break-ins it was around 12% less than the rate of growth of Internet hosts.

*Chapter 10*

# Severe Incidents

In previous chapters, CERT®/CC incidents were examined statistically with the populations being either all incidents, a subgroup of all incidents, all incidents at Site A, or a subgroup of the incidents at Site A. This chapter provides a more detailed description of a small number of the most severe incidents. This is preceded by a discussion of various measures of severity that might be used to determine which are the most "severe" incidents.

## 10.1 Selection of the Severe Incidents

As was discussed in Chapter 7, there is not one obvious measure of the severity of an Internet security incident. Two examples will make this point more clearly. In one incident reported to the CERT®/CC, the number of sites involved was 1,563. This incident also involved root break-ins. Using these measures, this was the most severe incident in the CERT®/CC records. Closer examination reveals, however, that this incident was actually relatively minor. The incident's duration was only 8 days, while the average duration for all CERT®/CC incidents was 16.5 days. The 23 messages to and from the CERT®/CC for this incident was only slightly above the average for all incidents (and well within the 54.4 standard deviation). The primary reason for this unusual set of numbers was that this incident involved a sniffer and the sites involved were recorded in the sniffer logs, but apparently not actually attacked. The incident was also quickly resolved.

A second example illustrates a more severe incident. This incident was characterized by the following data: 712 days duration, 383 sites, 158 messages to/from the CERT®/CC, and root-level break-ins. This incident had the longest duration of any incident in the CERT®/CC records, but all of the measures for this incident were also more than one standard deviation above their respective means. The intruders used numerous methods of operation including password cracking, Trojan horse login programs, deleting files, exploitation of open servers, social engineering, trusted hosts attacks, exploitation of sendmail bugs, mail spoofing and software piracy. It is the combination of all of these measures that makes this incident more severe than the first example given.

Figures 10.1 and 10.2 illustrate another difficulty with the individual measures of severity. In these plots, the number of sites for each incident are plotted from the greatest to the smallest number. Figure 10.1 plots the first 4,000 incidents. It is not clear from this Figure where the logical separation would be between the "severe" and "non-so-severe" incidents, based on the number of sites involved.

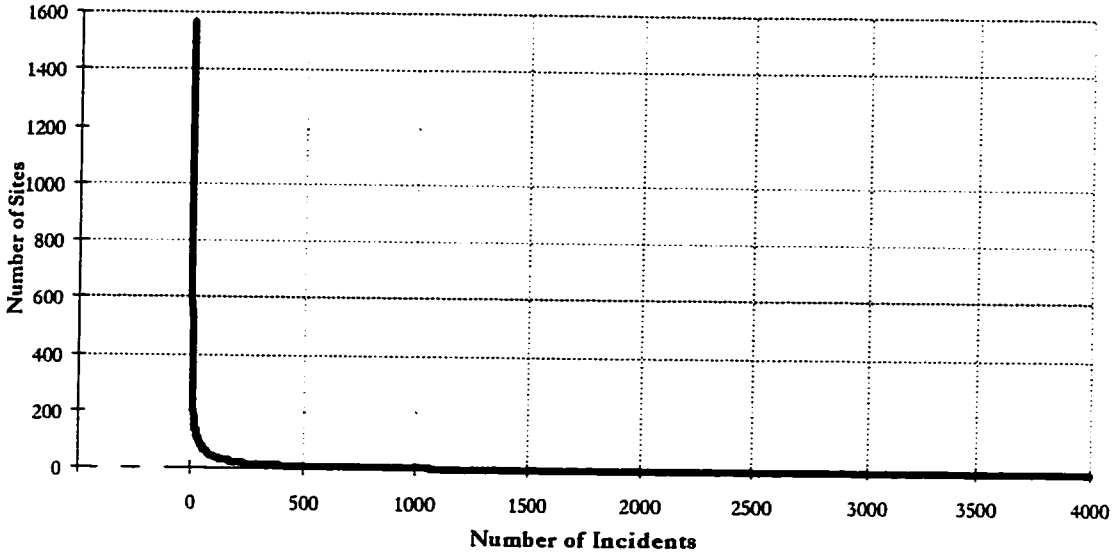


**Figure 10.1. Number of Sites versus Number of Incidents**

The "knee" of the plot in Figure 10.1 is expanded in Figure 10.2. Again this does not give an obvious separation point between severe and non-severe incidents. The center of the knee occurs when the incident number approximately equals the number of sites. This criteria identifies the first 62 incidents, but examination of these incident records shows that this includes many incidents that were not severe. Of these 62 incidents, 50 (81%) involved root break-ins, but 7 (11%) involved only account break-ins, 1 (2%) involved only access attempts, and 4 (7%) involved only FTP abuse and software piracy. One alternative to using the number of sites as the single criteria would be to also restrict the incidents to only those involving root break-ins.

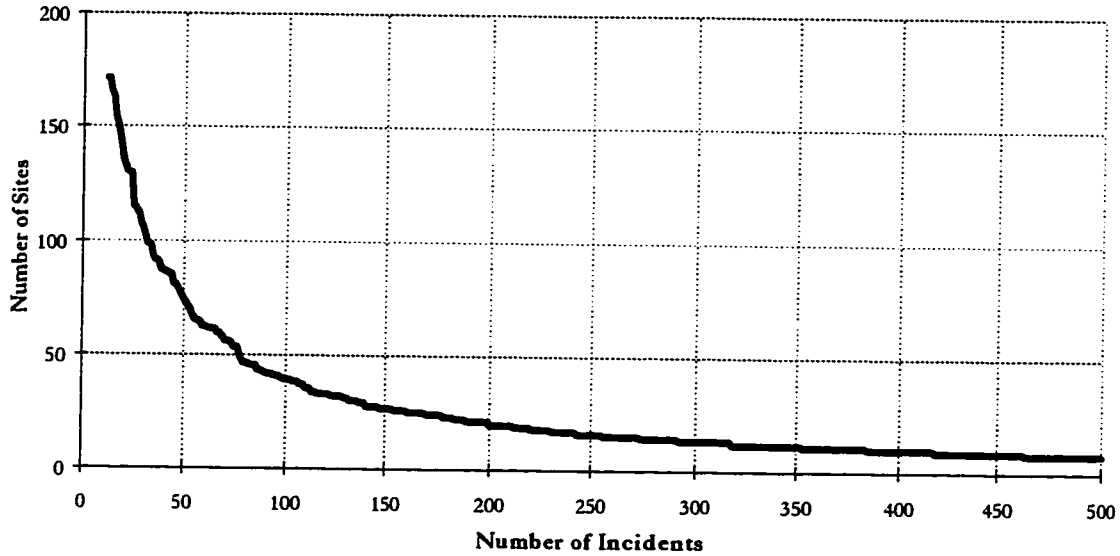


**Figure 10.2. Number of Sites versus Number of Incidents (Less than 200 sites and less than 500 Incidents)**

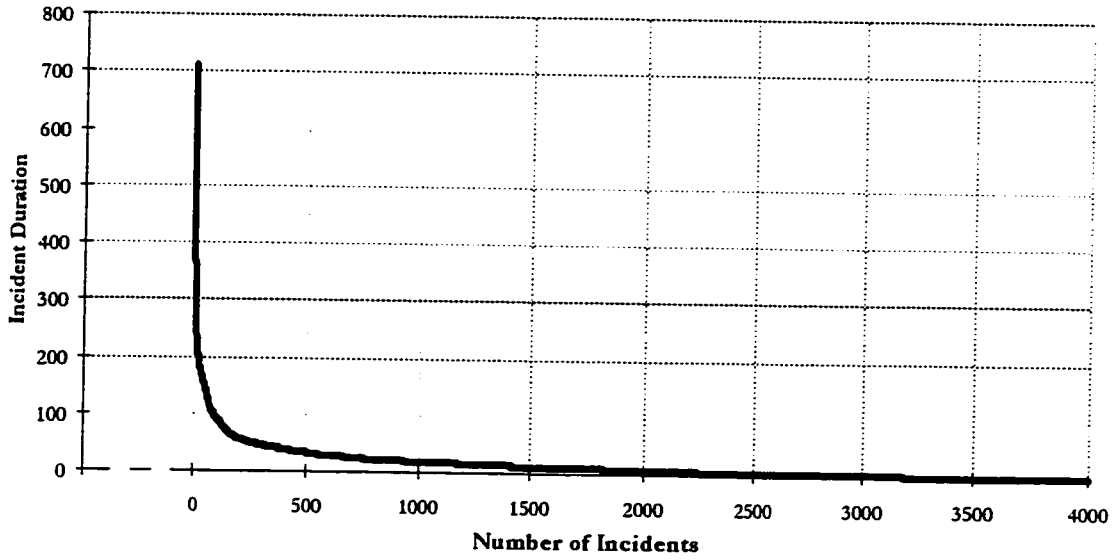


**Figure 10.3. Incident Duration versus Number of Incidents**

A similar approach can be taken with the duration of incidents as shown in Figure 10.3. The "knee" of this curve is expanded in Figure 10.4.

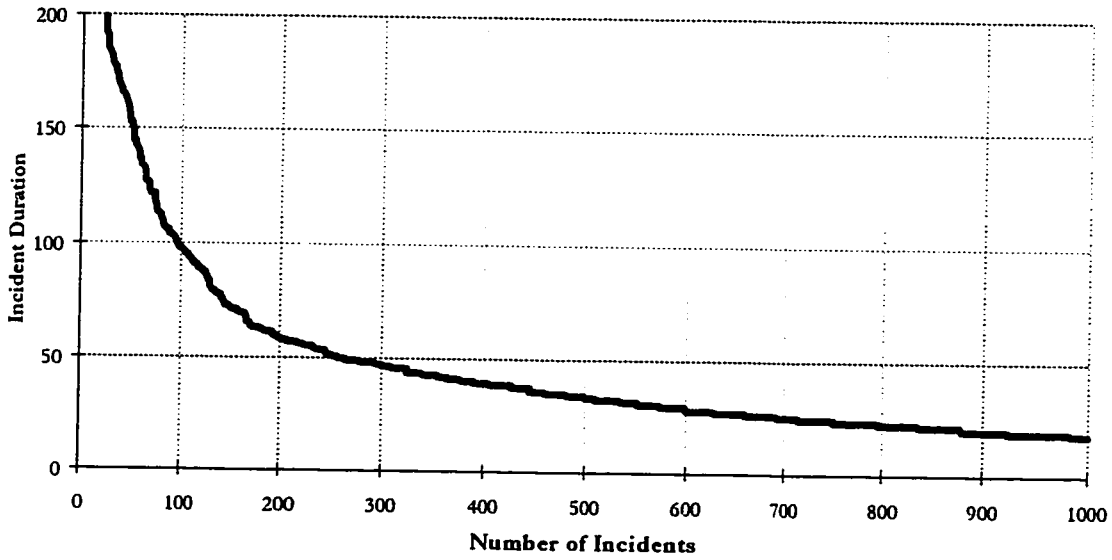


**Figure 10.4. Incident Duration versus Number of Incidents (200 or Less Days and less than 1000 Incidents)**

The center of the knee for incident duration occurs at 99 incidents, although only 74 involved root break-ins. Another 20 incidents involved account break-ins, three incidents involved access attempts, one incident involved source spoofing, and one incident involved FTP abuse and software piracy. Again, one alternative would be to also restrict these incidents to root break-ins.

Another dimension that may give some indication of severity is the number of messages to and from the CERT®/CC. As stated in Chapter 4, this may reflect CERT®/CC workload.

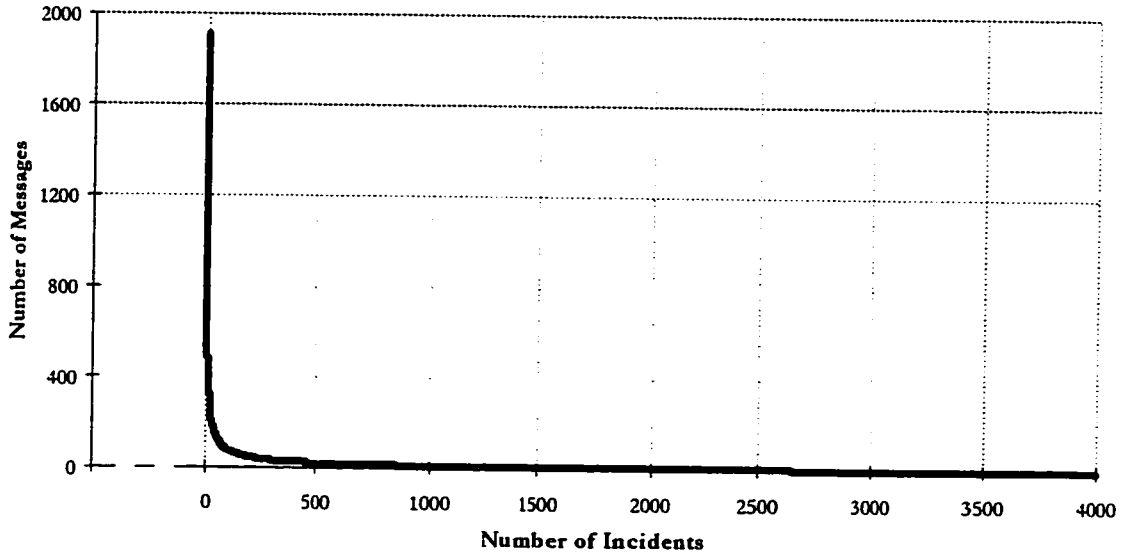


**Figure 10.5. Number of Messages versus Number of Incidents**

Figure 10.5 plots the number of messages sent to the CERT®/CC relative to the number of incidents. These data show the same distribution as the corresponding plots for duration and number of sites. Figure 10.6 isolates and expands the "knee" of Figure 10.5.

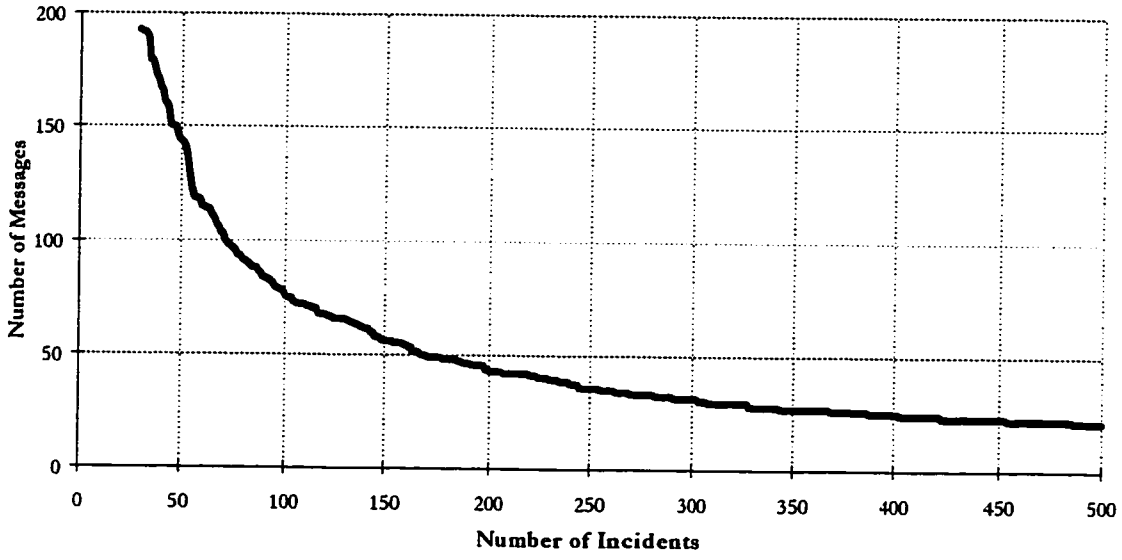


**Figure 10.6. Number of Messages versus Number of Incidents (Less than 200 messages and less than 500 Incidents)**

The center of the knee in Figures 10.5 and 10.6 occurred at the 87th incident. Of these incidents, 74 incidents (85.1%) were root break-ins, 9 incidents (10.3%) were account break-ins, 1 incident (1.1%) was an access attempt, 1 incident (1.1%) was a denial-of-service attack, and 2 incidents (2.3%) involved FTP abuse and software piracy.

None of these measures individually appears to be able to consistently isolate the most severe incidents. Combining these measures has the potential to improve the selection. There were 20 incidents (0.5%) that involved root break-ins and were also above the "knee" of all three dimensions.

An alternative to using the knee of these graphs to determine the severe incidents is to use the mean and standard deviations of the measurements. As shown in Table 10.1, if the standard deviation is added to the mean of each of the measurements, the resulting values are less than the respective values using the knee of the curves. There were 42 incidents with these minimum values.

| Measurement | Mean ($\mu$) | Standard Deviation ($\sigma$) | $\mu + \sigma$ | $\mu + 2\sigma$ | $\mu + 3\sigma$ |
|---|---|---|---|---|---|
| Duration | 16.5 | 31.2 | 47.7 | 78.9 | 110.1 |
| Number of Sites | 6.5 | 31.8 | 38.3 | 70.1 | 101.9 |
| Number of Messages | 14.2 | 54.4 | 68.6 | 123.0 | 177.4 |
| **Number of Incidents with These Minimum Values:** | | | 42 | 19 | 11 |

**Table 10.1. Mean and Standard Deviations of Measurements**

Even if we go to two standard deviations above the mean, one of the measurements, duration, is still below the value determined from the graphs. Only 19 incidents met this criteria. Of these 19, 17 were also in the 20 incidents identified from the graphs ($\geq$ 99 days duration, $\geq$ 62 sites, and $\geq$ 87 messages). If three standard deviations is chosen, all of the measurements are above the criteria from the graphs, but only 11 incidents meet this more restrictive criteria. The criteria from the knee of the graphs for duration (99 days) is 2.64 standard deviations above the mean, for the number of sites (62 sites) it is 1.45 standard deviations above the mean, and for the number of messages (87 messages) it is 1.34 standard deviations above the mean.

It is not clear which of these criteria would be the most appropriate to use to identify the severe incidents. Since this chapter is intended to be *descriptive* and not *statistical*, accuracy is not strictly critical. As such, we could use the *lower* of the values for the measurements from either criteria. Using the criteria from the graphs (the "knees"), along with two standard deviations above the mean, the lower values yield the following criteria: $\geq$ 79 days duration, $\geq$ 62 sites, and $\geq$ 87 messages. This selects 22 incidents as shown in Table 10.2. The average measurements of these 22 incidents were 203 days duration, 169 sites, and 466 messages.

| Incident # | Reporting Date | Start Date | Middle Date | Ending Date | Duration(Days) | # Sites | Sites/Day | # Messages |
|---|---|---|---|---|---|---|---|---|
| 1 | 2-Apr-90 | 2-Apr-90 | 24-Mar-91 | 14-Mar-92 | 713 | 383 | 0.54 | 158 |
| 2 | 18-Jun-92 | 9-Jun-92 | 19-Jul-92 | 28-Aug-92 | 81 | 162 | 2.00 | 227 |
| 3 | 16-Jun-92 | 12-Jun-92 | 16-Sep-92 | 21-Dec-92 | 193 | 107 | 0.55 | 458 |
| 4 | 28-Jul-92 | 28-Jul-92 | 25-Oct-92 | 22-Jan-93 | 179 | 66 | 0.37 | 229 |
| 5 | 2-Mar-93 | 1-Feb-93 | 18-Apr-93 | 4-Jul-93 | 154 | 264 | 1.71 | 486 |
| 6 | 29-May-93 | 5-Mar-93 | 22-Jul-93 | 9-Dec-93 | 280 | 93 | 0.33 | 476 |
| 7 | 12-Jul-93 | 12-Jul-93 | 11-Sep-93 | 11-Nov-93 | 123 | 141 | 1.15 | 288 |
| 8 | 11-Aug-93 | 25-Jun-93 | 12-Oct-93 | 29-Jan-94 | 219 | 113 | 0.52 | 141 |
| 9 | 13-Aug-93 | 12-Aug-93 | 31-Oct-93 | 19-Jan-94 | 161 | 164 | 1.02 | 918 |
| 10 | 20-Oct-93 | 20-Oct-93 | 11-Dec-93 | 1-Feb-94 | 105 | 248 | 2.36 | 648 |
| 11 | 27-May-94 | 27-May-94 | 22-Jul-94 | 17-Sep-94 | 114 | 62 | 0.54 | 167 |
| 12 | 3-May-94 | 3-May-94 | 28-Aug-94 | 24-Dec-94 | 236 | 103 | 0.44 | 367 |
| 13 | 16-Jul-94 | 28-Jun-94 | 25-Sep-94 | 23-Dec-94 | 179 | 130 | 0.73 | 394 |
| 14 | 18-May-94 | 1-May-94 | 11-Oct-94 | 24-Mar-95 | 328 | 112 | 0.34 | 118 |
| 15 | 2-Sep-94 | 2-Sep-94 | 28-Nov-94 | 24-Feb-95 | 176 | 100 | 0.57 | 192 |
| 16 | 15-Sep-94 | 15-Sep-94 | 4-Jan-95 | 26-Apr-95 | 224 | 515 | 2.30 | 1907 |
| 17 | 7-Dec-94 | 7-Dec-94 | 22-Jan-95 | 9-Mar-95 | 93 | 85 | 0.91 | 215 |
| 18 | 19-Jan-95 | 19-Jan-95 | 17-Apr-95 | 15-Jul-95 | 178 | 166 | 0.93 | 548 |
| 19 | 27-Jan-95 | 26-Jan-95 | 19-Apr-95 | 11-Jul-95 | 167 | 108 | 0.65 | 340 |
| 20 | 7-May-95 | 7-May-95 | 28-Jul-95 | 18-Oct-95 | 165 | 267 | 1.62 | 909 |
| 21 | 11-Oct-95 | 20-Aug-95 | 1-Dec-95 | 14-Mar-96 | 208 | 237 | 1.14 | 741 |
| 22 | 29-Sep-95 | 29-Sep-95 | 31-Dec-95 | 2-Apr-96 | 187 | 81 | 0.43 | 320 |

**Table 10.2. Summary of Root Break-in Incidents With ≥ 79 Days Duration, ≥ 62 Sites, ≥ 87 Messages**

## 10.2. Description of the Severe Incidents Chosen

Figure 10.7 presents how these incidents are distributed over time in the CERT®/CC records (using the year from the middle dates of Table 10.2). It is important to emphasize that *this should not be taken as a statistical sample of the CERT®/CC incidents.* There was a lot of variability in these data and the selection of these particular incidents as the most "severe" incidents was, at best, merely an approximation. Nevertheless, it is likely that a description of these incidents will provide valuable insight into the incidents reported to the CERT®/CC.

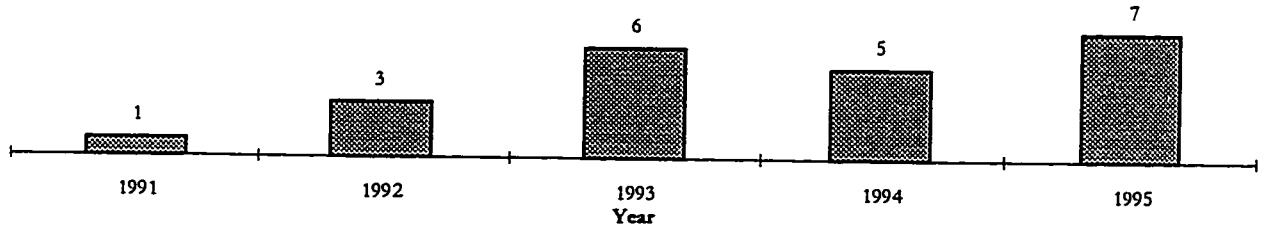


**Figure 10.7. Distribution of Root Break-in Incidents With ≥ 79 Days Duration, ≥ 62 Sites, ≥ 87 Messages**

The distribution of these incidents over time is further broken down in Figure 10.8 which plots a rectangle representing each incident. The horizontal dimension of each incident corresponds to the duration, and the height corresponds to the average sites per day as listed in Table 10.2.

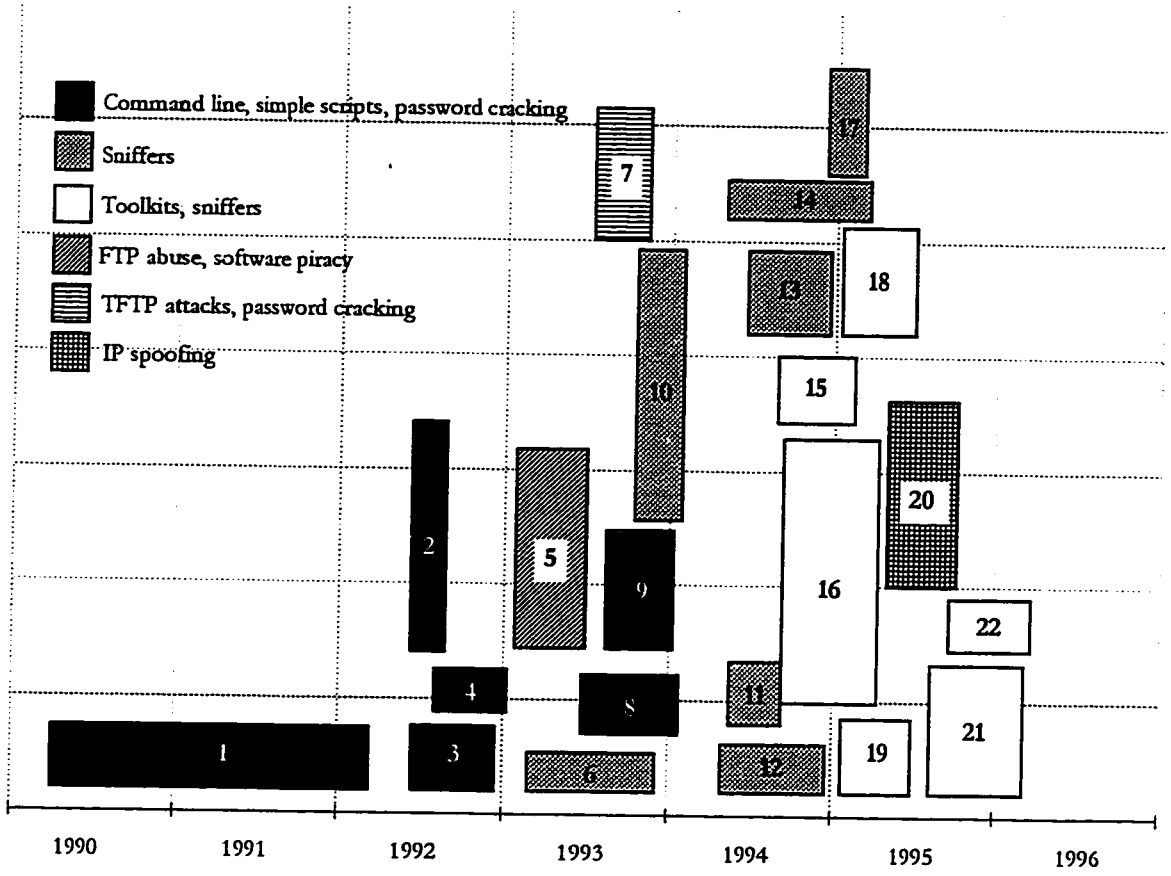


**Figure 10.8. Sites per Day versus Duration for 22 "Severe" Incidents**
**(Note: Numbers in each block indicate the order of the incident according to middle day as shown in Table 10.2, and the vertical dimension is average sites per day, one division = one site/day)**

Figure 10.8 gives a preliminary classification of the 22 severe incidents according to the predominant techniques intruders used during the incidents. Three classifications make up the bulk of the incidents (19 of the 22). In the early years, intruders in these severe incidents used primarily "manual" techniques through a command line interface. These techniques included individual user commands, simple shell scripts, and password cracking programs. Beginning in 1993, intruders became more sophisticated by gaining access to host computers using sniffers and then in 1994, they also used toolkits (such as *rootkit*). Three incidents did not fit into these categories. In the first half of 1993 there was a large incident that, although it involved some root break-ins, was primarily an incident of FTP abuse and software piracy. In the latter half of 1993, one severe incident primarily involved the use of a TFTP vulnerability which allowed an intruder to obtain a site's password file. Finally, one severe incident in 1995 involved primarily the use of sophisticated IP spoofing techniques.

In addition to this trend in intruder techniques, the 22 incidents show two other underlying trends. The first of these is that in the early incidents, the attackers tended to be a few individuals, tended to be confined to a specific location or group of locations, and as a consequence, tended to be easily identifiable. The later severe incidents tended to have more attackers operating in many different locations. This, combined with the more sophisticated techniques used by intruders, resulted in the intruders being harder to identify in the later incidents.

The other underlying characteristic of these severe incidents was the consistent use of a three-phase process of attack [ABH96:436-438]. In the first phase, the goal was to gain access to an account on the target system. For this, the intruder could obtain a user ID and password combination in a variety of ways, such as through various methods to crack passwords or in later incidents, through the use of a sniffer program. In the second phase, the intruder exploited vulnerabilities in the host system to gain privileged or root access on that system. In the final phase, the intruder often used this privileged access to attack other systems across the network. For these 22 severe incidents, this pattern of attack was consistent. Later incidents used more sophisticated tools, but the three phases were generally followed. The exception to this was the one incident of these 22 which was primarily characterized by IP spoofing. Using this method of attack , the intruder does not need to break into an account before gaining privileged access.

The following sections present more details about these 22 incidents.

**10.2.1. Incident #1 - Dutch Hackers** - The longest incident in the CERT®/CC records began April 1, 1990 with attempted penetrations at a U.S. *.mil* site. The attacks appeared to come from a U.S. *.edu* site, but this proved to be compromised. This was the beginning of an odyssey that lasted nearly two years, occupied countless hours of site administrator, law enforcement, and incident response personnel time, and caused damage and frustration for people using computers and networks on at least 383 commercial, educational, and military sites all over the world.

Two other characteristics combined to make this incident particularly unique. First, records show these attacks were carried out by a group of 4 young hackers operating out of their homes in a small area of the Netherlands. The later severe incidents generally involved more attackers located in many different areas. Also unlike later incidents, when it became increasingly difficult to identify intruders, in this incident the intruders were identified early in the incident – yet they were not arrested for nearly two years. The primary reason for this was the lack of Dutch laws against computer crime.

This Dutch hacker incident was one of the few CERT®/CC incidents to be widely reported in the press and in books. For example, Tsutomu Shimomura, a senior fellow at the San Diego Supercomputer Center, and John Markoff of the *New York Times*, wrote a book in 1996 giving an account of "the pursuit and capture of Kevin Mitnick," a well known hacker.[1] In this book and in an April 21, 1991 *Times* article, they describe hacking activity at Stanford University through an account with user ID of *adrian* and at Bell Labs in Murray Hill, New Jersey, through an account with user ID of *berferd* [ShM96:96-101]. These 1991 attacks were part of this CERT®/CC incident.

Unknown to Shimomura and Markoff, however, the hackers and this incident had been known to CERT®/CC since the previous year. CERT®/CC personnel and Wietse Venema[2], a systems administrator at one of the Dutch Universities, had been monitoring the hacker's activities. Their efforts were recorded in over 2,500 pages of text in the CERT®/CC record for this incident. Table 10.3 shows the top level domains for the reporting sites and other sites involved in the Dutch hacker incident. The majority of the attacked sites were in the U.S.[3]

| Reporting Sites | | |
|---|---|---|
| **domain** | **# sites** | **% sites** |
| .edu | 19 | 63.3% |
| .nl | 3 | 10.0% |
| .mil | 2 | 6.7% |
| .com | 1 | 3.3% |
| .org | 1 | 3.3% |
| .gov | 1 | 3.3% |
| .jp | 1 | 3.3% |
| .us | 1 | 3.3% |
| .fr | 1 | 3.3% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| **domain** | **# sites** | **% sites** | **domain** | **# sites** | **% sites** |
| .edu | 126 | 35.7% | .fr | 4 | 1.1% |
| .com | 93 | 26.3% | .se | 3 | 0.8% |
| .mil | 48 | 13.6% | .net | 2 | 0.6% |
| .ca | 12 | 3.4% | .ch | 1 | 0.3% |
| .gov | 10 | 2.8% | .es | 1 | 0.3% |
| .de | 9 | 2.5% | .gr | 1 | 0.3% |
| .uk | 9 | 2.5% | .ie | 1 | 0.3% |
| .nl | 7 | 2.0% | .il | 1 | 0.3% |
| .org | 6 | 1.7% | .it | 1 | 0.3% |
| .au | 5 | 1.4% | .jp | 1 | 0.3% |
| .fi | 5 | 1.4% | .nz | 1 | 0.3% |
| .no | 5 | 1.4% | .us | 1 | 0.3% |

**Table 10.3. Reporting and Other Sites for Severe Incident Number 1 (See Table 10.2 and Figure 10.8)**

Throughout this incident, the intruders followed a specific pattern for their attacks. First they would compromise a site, usually in the U.S., which would be used for attacks on other sites. Every few months they would move this base of operations to another site. During the initial months of

[1] Interestingly, the incident that Shimomura and Markoff wrote about in their 1996 book *Takedown* was not one of the severe incidents recorded in the CERT®/CC records. Instead, both Shimomura and Markoff's book and the CERT®/CC records both show that, although the incident was of long duration, it involved only a small number of sites. Perhaps this indicates the limitation of what could be done at that time by one individual hacker.

[2] During this incident, Wietse Venema wrote the well-known and widely-used *tcpwrapper* program for logging and intercepting TCP services started by *inetd* (first version in May, 1990) [GaS96:675]. He was also co-author of the *SATAN* automated network vulnerability search and report tool [ABH96:469].

[3] Note, however, that the majority of *all* Internet sites at the time were in the U.S.

the incident, security was limited at most sites. The intruders were often able to find accounts with default, weak, or missing passwords. Tracing of the attacks was relatively easy, and by May, 1990, both the FBI and local law enforcement agencies were actively investigating the incident.

The keywords used in the CERT®/CC record of this incident (Incident #1) to describe the methods of operation were as follows:

> weak passwords, no passwords, password files, password cracking, Trojan login, FTP, deleted files, open servers, social engineering, user accounts, system accounts, login attempts, hosts.equiv, .rhosts, sendmail attacks, debug, chsh/chfn, mail spoofing, rm -rf /, 87 socket, software piracy

These methods were implemented either by typing individual commands, or by using simple scripts or programs, such as password cracking programs. Most of these were well known methods. The exception is the "87 socket," which was unique to this incident. Intruders were often found to be telneting to socket 87. By the end of May, 1990, it was determined this was where the intruders placed a process which was a backdoor method for gaining root privileges.

During this incident, the hacking activities of these intruders were not specifically unlawful according to Dutch law. The intruders were very open about their activities. For example, at the beginning of May, 1990, one of the hackers gave a demonstration of their techniques by breaking into sites in France and the U.S. This demonstration included in-band signaling on the phone lines, which was a technique used to avoid toll charges. The hackers bragged about their activities on Usenet groups, signing their posts with the name *rcback* (the initials "rc" are used in the Netherlands to mean "computing center"). The hackers talked on-line about their activities with systems administrators like Wietse Venema. And finally, in June, 1990, one of the hackers requested a job in computer security at a U.S. military site in Europe. He sent that site a resume with his correct name and address.

There was a high level of activity by the Dutch hackers in May and June, 1990. This was followed by a period of inactivity until a "general wipeout" of all file systems at a Dutch University computing center toward the end of August. Break-in activity continued at this same Dutch site in September, and at several French sites and several U.S. *.edu* and *.mil* sites in November. This was followed by another quiet period until near the end of the year.

On December 30, 1990, numerous sites around the Internet received a message from one of the hackers requesting an account for himself on their system. One of these messages was sent to the CERT®/CC, which caused response personnel to investigate. This hacker would come to be

known as *fidelio* because this was the user ID of his account on one open U.S. site. He made no attempt, however, to disguise his identity, so his actual name was also widely known.

The period from January through April, 1991, was one of intense activity by the Dutch hackers, and of intense activity by CERT®/CC personnel, systems administrators and law enforcement agencies. Techniques used by the hackers became more sophisticated, including "trusted hosts" attacks involving *hosts.equiv* and *.rhosts* files. Sites attacked were military and civilian sites in the U.S., Europe and Japan. This was when Stanford, Bell Labs, Tsutomu Shimomura (SDSC), and John Markoff (*NY Times*) became involved.

In this time period Venema worked closely with Dutch law enforcement, but they were of little help because they "don't understand what a computer crime is." The situation in the U.S. was not much better. For example, the FBI was also unsure of what a computer crime was, and therefore, the CERT®/CC records indicate they were not very interested. Warrants were difficult to obtain. One site was reluctant to monitor the intruders within their own network because they were uncertain if a warrant was required for *internal* monitoring.

In February, 1991, the Dutch hackers broke into a site that was tracking them, and they found out the extent to which they had been monitored. They responded with increased attacks at already compromised sites, and at new sites. Some attacks were destructive. Venema contacted the group of hackers and tried to "scare" them with information about investigations by CERT®/CC and law enforcement agencies. This appeared to have little effect. During this same month, Dutch television news reported on the hacker group and even showed one member of the group breaking into what appeared to be a U.S. military computer [Mar91].

On April 21st, the *New York Times* reported on the Dutch hackers [Mar91], and on April 24th, Stanford was identified as a site by the *Stanford Daily* [Sta91]. That same day, one of the hackers exchanged e-mail with a system administrator at a U.S. site frequented by hackers. In it, he detailed the activities of the Dutch hackers over the previous 18 months.

Attacks continued from this group of intruders at a steady pace through July, 1991. The attacks resumed in October, 1991 and continued into 1992. During these periods, a debate was conducted among the attacked sites regarding selected sites that did not, as a matter of policy, secure their servers. These insecure servers were used by the intruders. Some applied pressure to have the sites secured. Others felt that the sites should be left open either because information and systems should be "free," or because it was easier to monitor intruders if they all funneled through only a few sites.

On January 27, 1992, two of the Dutch hackers were arrested by Dutch police. At the time, Dutch law was still in preparation and therefore, charges against the hackers were based on existing law: forgery (corrupting systems files in order to obtain root privileges), vandalism (rendering a computer system unusable), and racketeering (using stolen passwords). Following these arrests, there was an increase in intruder activity for the next few weeks, perhaps as a response by other members of the group, or by other hackers.

On February 17, 1992, the CERT®/CC issued an advisory of "Internet Intruder Activity" based on this incident (CA-92:03).[4] For the next month, sites investigated and reported back to the CERT®/CC as to whether they had been attacked. In March, 1992, Wietse Venema sent a message to the CERT®/CC summarizing his recent interview with the hackers, who indicated the incident had involved 4 individuals. This is the last entry in the CERT®/CC record for this incident.

**10.2.2. Incident #9 - Danish Hackers** - A smaller, but still severe incident began on the Internet in August, 1993. This incident was similar to the Dutch hacker incident in that it primarily consisted of attacks by a small group of individuals in a geographically small area -- Denmark in this case. Table 10.4 lists the top-level domain names for the sites known to be involved.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 2 | 33.3% |
| .il | 1 | 16.7% |
| .com | 1 | 16.7% |
| .mil | 1 | 16.7% |
| .dk | 1 | 16.7% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 56 | 35.4% | .gr | 2 | 1.3% |
| .com | 18 | 11.4% | .is | 2 | 1.3% |
| .mil | 15 | 9.5% | .net | 2 | 1.3% |
| .dk | 13 | 8.2% | .se | 2 | 1.3% |
| .tw | 7 | 4.4% | .us | 2 | 1.3% |
| .ca | 5 | 3.2% | .at | 1 | 0.6% |
| .il | 5 | 3.2% | .cs | 1 | 0.6% |
| .br | 4 | 2.5% | .fi | 1 | 0.6% |
| .de | 4 | 2.5% | .kr | 1 | 0.6% |
| .au | 3 | 1.9% | .nl | 1 | 0.6% |
| .gov | 3 | 1.9% | .no | 1 | 0.6% |
| .uk | 3 | 1.9% | .org | 1 | 0.6% |
| .be | 2 | 1.3% | .pl | 1 | 0.6% |
| .es | 2 | 1.3% | | | |

**Table 10.4. Reporting and Other Sites for Severe Incident Number 9 (See Table 10.2 and Figure 10.8)**

The attack methods consisted of user command and small scripts, and primarily involved exploiting vulnerabilities in the *sendmail* program as described in CERT® Advisories in October and November, 1993 (CA-93:15 and CA-93:16). The keywords used in the CERT®/CC record of

[4] CERT® Advisories are available from the CERT®/CC on-line at www.cert.org.

Incident #9 to describe the methods of operation were as follows: sendmail, ISS attack, password files, password cracking, files deleted, mail spoofing, and Trojans.

Law enforcement agencies became involved early in this incident. Their activities included phone tracing of the hackers. The hackers were arrested by Danish Police in December, 1993. The Danish press reported the incident as the "biggest Danish incident ever."

**10.2.3. Incidents #2, 3, 4, and 8 - Other Command Line Incidents** - There were 4 other severe incidents with intruders using primarily user commands and small scripts as methods of attack. These incidents were all similar to each other. The sites involved in Incident #2 are listed in Table 10.5.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 1 | 100.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 53 | 32.9% | .es | 2 | 1.2% |
| .fr | 19 | 11.8% | .jp | 2 | 1.2% |
| .com | 15 | 9.3% | .mil | 2 | 1.2% |
| .gov | 13 | 8.1% | .pt | 2 | 1.2% |
| .de | 10 | 6.2% | .uk | 2 | 1.2% |
| .ca | 9 | 5.6% | .at | 1 | 0.6% |
| .au | 5 | 3.1% | .be | 1 | 0.6% |
| .se | 4 | 2.5% | .cs | 1 | 0.6% |
| .br | 3 | 1.9% | .dk | 1 | 0.6% |
| .hk | 3 | 1.9% | .gr | 1 | 0.6% |
| .it | 3 | 1.9% | .net | 1 | 0.6% |
| .nl | 3 | 1.9% | .no | 1 | 0.6% |
| .org | 3 | 1.9% | .sg | 1 | 0.6% |

**Table 10.5. Reporting and Other Sites for Severe Incident Number 2 (See Table 10.2 and Figure 10.8)**

Attacks during this incident were successful many times because of lax security. In the early part of the incident, sites attacked were primarily in the U.S. This changed toward the end of the incident, when attacks concentrated more on overseas military sites and sites in Germany.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 4 | 33.3% |
| .ca | 3 | 25.0% |
| .com | 3 | 25.0% |
| .gov | 1 | 8.3% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 51 | 53.7% | .il | 2 | 2.1% |
| .com | 9 | 9.5% | .nl | 1 | 1.1% |
| .de | 6 | 6.3% | .org | 1 | 1.1% |
| .au | 6 | 6.3% | .mx | 1 | 1.1% |
| .mil | 4 | 4.2% | .it | 1 | 1.1% |
| .ca | 3 | 3.2% | .hk | 1 | 1.1% |
| .gov | 2 | 2.1% | .net | 1 | 1.1% |
| .uk | 2 | 2.1% | .br | 1 | 1.1% |
| .kr | 2 | 2.1% | .gr | 1 | 1.1% |

**Table 10.6. Reporting and Other Sites for Severe Incident Number 3 (See Table 10.2 and Figure 10.8)**

The keywords used in the CERT®/CC record of Incident #2 to describe the methods of operation were as follows: password cracking, *crack*, FTP abuse, software piracy, open server, NIS.

In June, 1992, a significant incident began (Incident #3) that used techniques described in CERT® Advisory CA-92:14, "Altered System Binaries Incident." The top-level domain of the sites involved are listed in Table 10.6.

Incident #3 activity occurred primarily in the U.S., Australia, and Canada, employing holes in the Unix rdist utility. One widely used method of exploiting this vulnerability was to use a program called *gimme* which was written by Tsutomu Shimomura. Law enforcement agencies involved in this incident included the FBI, Secret Service, Australian National Police, Royal Canadian Mounted Police, and local police. The keywords used in the CERT®/CC record of Incident #3 to describe the methods of operation were as follows:

rdist, modify logs, hosts.equiv, *gimme*, TFTP attack, NFS attack, Trojan login, password cracking, no password, password file, deleted files, Trojan telnet, sendmail

Rdist attacks were also used extensively in Incident #4 to attack the sites listed in Table 10.7.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 4 | 100.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 33 | 53.2% | .org | 2 | 3.2% |
| .com | 11 | 17.7% | .it | 2 | 3.2% |
| .mil | 3 | 4.8% | .hk | 1 | 1.6% |
| .ca | 6 | 9.7% | .net | 1 | 1.6% |
| .gov | 2 | 3.2% | .il | 1 | 1.6% |

**Table 10.7. Reporting and Other Sites for Severe Incident Number 4 (See Table 10.2 and Figure 10.8)**

The keywords used in the CERT®/CC record of Incident #4 to describe the methods of operation were as follows:

rdist, password files, password cracking, .rhosts, hosts.equiv, configuration, NFS exports, IRC, weak passwords, no passwords

In the final incident in this category, Incident #8, the rdist hole was again used against sites with top-level domains as listed in Table 10.8.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .ca | 1 | 50.0% |
| .com | 1 | 50.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 63 | 56.8% | .z | 2 | 1.8% |
| .gov | 16 | 14.4% | .ca | 1 | 0.9% |
| .com | 15 | 13.5% | .de | 1 | 0.9% |
| .mil | 7 | 6.3% | .fi | 1 | 0.9% |
| .fr | 2 | 1.8% | .it | 1 | 0.9% |
| .org | 2 | 1.8% | | | |

**Table 10.8. Reporting and Other Sites for Severe Incident Number 8 (See Table 10.2 and Figure 10.8)**

The FBI and local police were reluctant to get involved Incident #8 until several days into the incident when the first military site was attacked. The keywords used in the CERT®/CC record of Incident #8 to describe the methods of operation were as follows:

NIS attack, NFS attack, Trojan login, rdist, expreserve, .rhosts, ypserv, password file, password cracking, hosts.equiv, configuration

**10.2.4. Incident #5 - FTP Abuse and Software Piracy** - FTP abuse and software piracy were not generally considered security problems for the Internet by CERT®/CC personnel. Nevertheless, CERT®/CC recorded what information it received about these incidents, and one of these, Incident #5, met the criteria for classification as a severe incident. The top-level domains of the sites involved are listed in Figure 10.9.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .gov | 3 | 50.0% |
| .edu | 2 | 33.3% |
| .il | 1 | 16.7% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 120 | 46.5% | .no | 4 | 1.6% |
| .com | 23 | 8.9% | .se | 4 | 1.6% |
| .z | 13 | 5.0% | .ch | 3 | 1.2% |
| .au | 12 | 4.7% | .es | 3 | 1.2% |
| .de | 12 | 4.7% | .il | 3 | 1.2% |
| .net | 11 | 4.3% | .dk | 2 | 0.8% |
| .ca | 10 | 3.9% | .it | 2 | 0.8% |
| .uk | 7 | 2.7% | .at | 1 | 0.4% |
| .org | 6 | 2.3% | .cl | 1 | 0.4% |
| .fi | 5 | 1.9% | .jp | 1 | 0.4% |
| .fr | 4 | 1.6% | .mil | 1 | 0.4% |
| .gov | 4 | 1.6% | .nz | 1 | 0.4% |
| .nl | 4 | 1.6% | .sg | 1 | 0.4% |

**Table 10.9. Reporting and Other Sites for Severe Incident Number 5 (See Table 10.2 and Figure 10.8)**

The keywords used in the CERT®/CC record of Incident #5 to describe the methods of operation were as follows: FTP abuse, software piracy, configuration, wuarchive ftpd, *warez*, password cracking, password files. The CERT®/CC issued advisories on FTP abuse in April, 1993 (CA-93:06, "wuarchive ftpd Vulnerability"), and in July, 1993 (CA-93:10, "Anonymous FTP Activity"). Incident #8 began in August, 1993.

**10.2.5. Incident #7 - TFTP Attacks** - In October, 1991, the CERT®/CC issued an advisory on a vulnerability in the AIX TFTP Daemon (CA-91:19). Unless TFTP was properly restricted, this vulnerability allowed attackers to copy files, such as */etc/passwd*, from the site using TFTP. Nearly two years later, in July, 1993, Incident #7 began. In this incident, the intruders' primary method of attack was to exploit this TFTP vulnerability. The top-level domains of sites involved are listed in Table 10.10.

The keywords used in the CERT®/CC record of Incident #7 to describe the methods of operation were as follows: TFTP attack, password files, password cracking, *crack*, fraud, configuration. In this incident, the Secret Service became involved, and one of the intruders was arrested early in the incident (a 17 year old). The incident, however, continued for more than 4 months after that, with attacks from other intruders.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 1 | 25.0% |
| .ch | 1 | 25.0% |
| .jp | 1 | 25.0% |
| .gov | 1 | 25.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 48 | 35.0% | .gr | 2 | 1.5% |
| .com | 17 | 12.4% | .il | 2 | 1.5% |
| .ca | 7 | 5.1% | .net | 2 | 1.5% |
| .gov | 7 | 5.1% | .ch | 1 | 0.7% |
| .au | 4 | 2.9% | .cs | 1 | 0.7% |
| .fi | 4 | 2.9% | .es | 1 | 0.7% |
| .it | 4 | 2.9% | .kr | 1 | 0.7% |
| .mx | 4 | 2.9% | .nl | 1 | 0.7% |
| .no | 4 | 2.9% | .nz | 1 | 0.7% |
| .se | 4 | 2.9% | .org | 1 | 0.7% |
| .de | 3 | 2.2% | .pt | 1 | 0.7% |
| .pl | 3 | 2.2% | .sg | 1 | 0.7% |
| .tw | 3 | 2.2% | .si | 1 | 0.7% |
| .uk | 3 | 2.2% | .su | 1 | 0.7% |
| .at | 2 | 1.5% | .za | 1 | 0.7% |
| .fr | 2 | 1.5% | | | |

**Table 10.10. Reporting and Other Sites for Severe Incident Number 7 (See Table 10.2 and Figure 10.8)**

**10.2.6. Incidents #6, 10, 11, 12, 13, 14, 17 - Sniffer Attacks** - All of the remaining severe incidents used sniffers to attack Internet sites. For seven of these, this was the primary means of attack. The first of these seven incidents began in March, 1993 and involved sites primarily in the U.S., Europe, and South America with top-level domains as listed in Table 10.11.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 5 | 62.5% |
| .com | 3 | 37.5% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 44 | 51.8% | .br | 1 | 1.2% |
| .com | 10 | 11.8% | .cl | 1 | 1.2% |
| .dk | 7 | 8.2% | .de | 1 | 1.2% |
| .org | 3 | 3.5% | .fr | 1 | 1.2% |
| .se | 3 | 3.5% | .gov | 1 | 1.2% |
| .uk | 3 | 3.5% | .il | 1 | 1.2% |
| .es | 2 | 2.4% | .nl | 1 | 1.2% |
| .net | 2 | 2.4% | .su | 1 | 1.2% |
| .no | 2 | 2.4% | .tw | 1 | 1.2% |

**Table 10.11. Reporting and Other Sites for Severe Incident Number 6 (See Table 10.2 and Figure 10.8)**

The keywords used in the CERT®/CC record of Incident #6 to describe the methods of operation were as follows: Trojan telnet, Trojan login, password cracking, sniffer, *kc*, weak passwords, yp, deleted files.

The next sniffer incident began in October, 1993. This incident (Incident #10) involved a high percentage of *.com* sites as listed in Table 10.12. The keywords used in the CERT®/CC record of Incident #10 to describe the methods of operation were as follows: sniffer, mail spoofing.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 1 | 33.3% |
| org | 1 | 33.3% |
| .com | 1 | 33.3% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 89 | 36.3% | .ch | 2 | 0.8% |
| .com | 52 | 21.2% | .tw | 2 | 0.8% |
| .z | 20 | 8.2% | .us | 2 | 0.8% |
| .net | 12 | 4.9% | .cz | 1 | 0.4% |
| .gov | 10 | 4.1% | .fr | 1 | 0.4% |
| .au | 9 | 3.7% | .gr | 1 | 0.4% |
| .de | 8 | 3.3% | .hk | 1 | 0.4% |
| .org | 7 | 2.9% | .ie | 1 | 0.4% |
| .uk | 7 | 2.9% | .it | 1 | 0.4% |
| .ca | 6 | 2.4% | .jp | 1 | 0.4% |
| .se | 4 | 1.6% | .mil | 1 | 0.4% |
| .fi | 3 | 1.2% | .su | 1 | 0.4% |
| .nl | 3 | 1.2% | | | |

**Table 10.12. Reporting and Other Sites for Severe Incident Number 10 (See Table 10.2 and Figure 10.8)**

An additional sniffer incident, Incident #11, began in May, 1994 and continued until September, 1994, involving the sites with top-level domains as shown in Table 10.13.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .com | 1 | 33.3% |
| .edu | 1 | 33.3% |
| .it | 1 | 33.3% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 32 | 54.2% | .ch | 1 | 1.7% |
| .com | 7 | 11.9% | .mil | 1 | 1.7% |
| .ca | 4 | 6.8% | .mx | 1 | 1.7% |
| .gov | 3 | 5.1% | .net | 1 | 1.7% |
| .fr | 2 | 3.4% | .org | 1 | 1.7% |
| .jp | 2 | 3.4% | .su | 1 | 1.7% |
| .uk | 2 | 3.4% | .z | 1 | 1.7% |

**Table 10.13. Reporting and Other Sites for Severe Incident Number 11 (See Table 10.2 and Figure 10.8)**

The keywords used in the CERT®/CC record of Incident #11 to describe the methods of operation were as follows: sniffer, password cracking, password files, FTP abuse, *warez*.

Table 10.14 lists the top-level domains of the sites involved in Incident #12. The primary sites involved in this incident were in Hong Kong, which was relatively new to widespread Internet use. The keywords used in the CERT®/CC record of Incident #12 to describe the methods of operation were as follows: sniffer, ari.nit, mail spoofing, weak passwords, password cracking, Trojan

crontab, sendmail attack, *chasin*, rdist, *crack*, ICMP bombs, IRC, crack, telnet, SMTP attack. The use of the sendmail *chasin* script and of ICMP bombs make this incident unusual compared to the other sniffer incidents.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 1 | 20.0% |
| .hk | 1 | 20.0% |
| .com | 1 | 20.0% |
| .mil | 1 | 20.0% |
| .gov | 1 | 20.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 34 | 34.7% | .net | 2 | 2.0% |
| .com | 9 | 9.2% | .no | 2 | 2.0% |
| .ca | 8 | 8.2% | .th | 2 | 2.0% |
| .mil | 7 | 7.1% | .br | 1 | 1.0% |
| .hk | 5 | 5.1% | .cl | 1 | 1.0% |
| .au | 4 | 4.1% | .fi | 1 | 1.0% |
| .jp | 4 | 4.1% | .kr | 1 | 1.0% |
| .gov | 3 | 3.1% | .mx | 1 | 1.0% |
| .tw | 3 | 3.1% | .nz | 1 | 1.0% |
| .ch | 2 | 2.0% | .org | 1 | 1.0% |
| .de | 2 | 2.0% | .sg | 1 | 1.0% |
| .my | 2 | 2.0% | .uk | 1 | 1.0% |

**Table 10.14. Reporting and Other Sites for Severe Incident Number 12 (See Table 10.2 and Figure 10.8)**

Incident #13 was the first severe incident to introduce the use of the Internet Security Scanner (ISS) tool. This software package interrogates all computers within a specified IP address range, determining the security status of each relative to several common system vulnerabilities, as described in CERT® Advisory CA-93:14, "Internet Security Scanner (ISS)." The top-level domains of the sites involved in this incident are listed in Table 10.15.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 6 | 54.5% |
| .com | 2 | 18.2% |
| .uk | 2 | 18.2% |
| .de | 1 | 9.1% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .com | 33 | 27.7% | .ca | 2 | 1.7% |
| .edu | 32 | 26.9% | .z | 2 | 1.7% |
| .net | 13 | 10.9% | .fr | 1 | 0.8% |
| .org | 8 | 6.7% | .il | 1 | 0.8% |
| .br | 5 | 4.2% | .jp | 1 | 0.8% |
| .es | 5 | 4.2% | .lv | 1 | 0.8% |
| .uk | 5 | 4.2% | .nl | 1 | 0.8% |
| .de | 4 | 3.4% | .si | 1 | 0.8% |
| .gov | 3 | 2.5% | .sk | 1 | 0.8% |

**Table 10.15. Reporting and Other Sites for Severe Incident Number 13 (See Table 10.2 and Figure 10.8)**

The keywords used in the CERT®/CC record of Incident #13 to describe the methods of operation were as follows:

> sniffer, ISS attack, deleted files, modify logs, TFTP attacks, password cracking, password file, crack, NIS attack, FTP attack, sendmail attack, source route spoofing, rpc probes, mailrace, Trojan login, Trojan ifconfig, Trojan ps.

The last two sniffer incidents were Incident #14 and Incident #17. The top-level domain of the sites involved in Incident #14 are listed in Table 10.16. The keywords used in the CERT®/CC record of Incident #14 to describe the methods of operation were as follows: sniffer, Trojan login, Trojan telnet, weak password, .rhosts, ypx.

The top-level domain of the sites involved in Incident #17 are listed in Table 10.17. Incident #17 included the widespread use of techniques to exploit the trusted hosts system of Unix through the use of the .rhosts and hosts.equiv files.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .cl | 1 | 100.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .fr | 32 | 28.8% | .ar | 1 | 0.9% |
| .z | 14 | 12.6% | .au | 1 | 0.9% |
| .edu | 13 | 11.7% | .dk | 1 | 0.9% |
| .br | 11 | 9.9% | .es | 1 | 0.9% |
| .ca | 5 | 4.5% | .gr | 1 | 0.9% |
| .gov | 5 | 4.5% | .kr | 1 | 0.9% |
| .com | 4 | 3.6% | .lt | 1 | 0.9% |
| .net | 4 | 3.6% | .se | 1 | 0.9% |
| .ch | 3 | 2.7% | .si | 1 | 0.9% |
| .de | 3 | 2.7% | .tw | 1 | 0.9% |
| .it | 3 | 2.7% | .uk | 1 | 0.9% |
| .org | 2 | 1.8% | .ve | 1 | 0.9% |

**Table 10.16. Reporting and Other Sites for Severe Incident Number 14 (See Table 10.2 and Figure 10.8)**

The keywords used in the CERT®/CC record of Incident #17 to describe the methods of operation were as follows: sniffer, trusted hosts attack, login attempts, open server, no password, Trojan login, .rhosts, infrastructure attack, modify logs, hosts.equiv, configuration, NFS attack.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 3 | 37.5% |
| .net | 2 | 25.0% |
| .com | 2 | 25.0% |
| .gov | 1 | 12.5% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 42 | 54.5% | .ca | 1 | 1.3% |
| .com | 16 | 20.8% | .org | 1 | 1.3% |
| .gov | 8 | 10.4% | .uk | 1 | 1.3% |
| .net | 4 | 5.2% | .us | 1 | 1.3% |
| .mil | 3 | 3.9% | | | |

**Table 10.17. Reporting and Other Sites for Severe Incident Number 17 (See Table 10.2 and Figure 10.8)**

**10.2.7. Incident #15, 18, 19, 21, 22 - Toolkit and Sniffer Attacks** - The remainder of the severe incidents not only included the use of sniffers, but user-friendly toolkits. The most frequently used toolkit according to the CERT®/CC records was the program *rootkit*. This program contains source code for an Ethernet sniffer, for Trojan *login*, *ps*, *ls*, *du*, *ifconfig*, and *netstat*, as well as tools to alter the dates, permissions and checksums of these Trojan horse files, and to remove entries from the utmp, wtmp, and lastlog files [ABH96:438]. Five of these incidents are described

in this section. Incident #16 involved an unusually large number of sites, and Incident #20 was dominated by the use of IP spoofing, so they are discussed in separate sections.

The first of the severe incidents to record the use of *rootkit* began in the Fall of 1994. While this incident produced numerous attacks on U.S. sites, it also involved many sites connected to networks running the X.29 protocol, as well as sites in Italy, Argentina, and on the Tymnet network. The keywords used in the CERT®/CC record of Incident #15 to describe the methods of operation were as follows: *rootkit*, sniffer, sendmail attack, Trojan login, Trojan ps, Trojan netstat, mailrace, loadmodule.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 6 | 60.0% |
| .se | 1 | 10.0% |
| .com | 1 | 10.0% |
| .fr | 1 | 10.0% |
| .at | 1 | 10.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 27 | 30.0% | .ca | 2 | 2.2% |
| .it | 11 | 12.2% | .nl | 2 | 2.2% |
| .kr | 6 | 6.7% | .se | 2 | 2.2% |
| .com | 5 | 5.6% | .at | 1 | 1.1% |
| .net | 5 | 5.6% | .fi | 1 | 1.1% |
| .org | 5 | 5.6% | .fr | 1 | 1.1% |
| .ch | 4 | 4.4% | .hu | 1 | 1.1% |
| .gov | 4 | 4.4% | .il | 1 | 1.1% |
| .de | 3 | 3.3% | .mil | 1 | 1.1% |
| .jp | 3 | 3.3% | .pl | 1 | 1.1% |
| .uk | 3 | 3.3% | .z | 1 | 1.1% |

**Table 10.18. Reporting and Other Sites for Severe Incident Number 15 (See Table 10.2 and Figure 10.8)**

A group of intruders operating out of Brazil played a significant role in Incident #18. The top-level domains of the sites involved are listed in Table 10.19.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 5 | 41.7% |
| .br | 1 | 8.3% |
| .com | 1 | 8.3% |
| .es | 1 | 8.3% |
| .gov | 1 | 8.3% |
| .mil | 1 | 8.3% |
| .net | 1 | 8.3% |
| .org | 1 | 8.3% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .com | 42 | 27.3% | .il | 2 | 1.3% |
| .edu | 42 | 27.3% | .mil | 2 | 1.3% |
| .net | 10 | 6.5% | .nl | 2 | 1.3% |
| .ca | 9 | 5.8% | .org | 2 | 1.3% |
| .es | 5 | 3.2% | .at | 1 | 0.6% |
| .uk | 5 | 3.2% | .fr | 1 | 0.6% |
| .de | 4 | 2.6% | .gr | 1 | 0.6% |
| .gov | 4 | 2.6% | .in | 1 | 0.6% |
| .br | 3 | 1.9% | .jp | 1 | 0.6% |
| .ch | 3 | 1.9% | .kr | 1 | 0.6% |
| .it | 3 | 1.9% | .no | 1 | 0.6% |
| .tw | 3 | 1.9% | .us | 1 | 0.6% |
| .au | 2 | 1.3% | .ve | 1 | 0.6% |
| .fi | 2 | 1.3% | | | |

**Table 10.19. Reporting and Other Sites for Severe Incident Number 18 (See Table 10.2 and Figure 10.8)**

Incident #18 was unusual in that the some of the intruders were observed to be communicating on IRC. The incident record contains an IRC conversation where one experienced hacker convinces a novice to type "rm -rf /&". Although the conversation was humorous, this unfortunately resulted in the file system being deleted on a site that was compromised.

The keywords used in the CERT®/CC record of Incident #18 to describe the methods of operation were as follows: *rootkit*, sniffer, credit card fraud, password cracking, *crack*, weak passwords, mailrace, Trojan ls, Trojan finger, rdist, loadmodule, expreserve, IRC, deleted files. There was some speculation by those tracking the intruders in Incident #18 that IP spoofing was used, but this was not confirmed, and if it actually was used, it was not significant.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 3 | 42.9% |
| .com | 1 | 14.3% |
| .gov | 1 | 14.3% |
| .net | 1 | 14.3% |
| .org | 1 | 14.3% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .com | 36 | 35.6% | .gov | 5 | 5.0% |
| .edu | 34 | 33.7% | .us | 3 | 3.0% |
| .de | 12 | 11.9% | .org | 2 | 2.0% |
| .net | 8 | 7.9% | .au | 1 | 1.0% |

**Table 10.20. Reporting and Other Sites for Severe Incident Number 19 (See Table 10.2 and Figure 10.8)**

The top-level domains of the sites involved in Incident #19 are listed in Table 10.20, and keywords used in the CERT®/CC record of Incident #19 for the methods of operation were as follows: *rootkit*, sniffer, password files, modify logs, *crack*, rdist, Trojan login, Trojan ps, Trojan es, Trojan in.rexecd, NFS attack, NIS attack, expreserve, loadmodule, sendmail, deleted files, modify logs, rexd.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 6 | 60.0% |
| .gov | 1 | 10.0% |
| .com | 1 | 10.0% |
| .ca | 1 | 10.0% |
| .net | 1 | 10.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 79 | 34.8% | .us | 3 | 1.3% |
| .com | 61 | 26.9% | .ch | 2 | 0.9% |
| .net | 24 | 10.6% | .jp | 2 | 0.9% |
| .gov | 13 | 5.7% | .se | 2 | 0.9% |
| .org | 6 | 2.6% | .uk | 2 | 0.9% |
| .ca | 5 | 2.2% | .br | 1 | 0.4% |
| .mil | 5 | 2.2% | .es | 1 | 0.4% |
| .de | 4 | 1.8% | .fi | 1 | 0.4% |
| .fr | 3 | 1.3% | .is | 1 | 0.4% |
| .it | 3 | 1.3% | .pl | 1 | 0.4% |
| .kr | 3 | 1.3% | .ru | 1 | 0.4% |
| .nl | 3 | 1.3% | .su | 1 | 0.4% |

**Table 10.21. Reporting and Other Sites for Severe Incident Number 21 (See Table 10.2 and Figure 10.8)**

The techniques used in Incident #21 were described in CERT® Advisory CA-95:18, "Widespread Attacks on Internet Sites." Some IP spoofing was noted in the attacks, but the

incident was dominated by the use of sniffers and toolkits. The keywords used in the CERT®/CC record of Incident #21 to describe the methods of operation were as follows:

> *rootkit*, sniffer, password file, password cracking, weak passwords, Trojan login, Trojan ifconfig, Trojan ps, Trojan netstat, Trojan time, Trojan ls, modify logs, *watch*, FTP abuse, software piracy, configuration, mouse, sendmail attack, NFS attack, system accounts, loadmodule, chfn, IRC, credit card fraud, increase monitoring, NIS attack, IP spoofing, *ISS* attack, *SATAN* scans.

Incident #22 was unusual because the majority of sites involved were not in the U.S. This was primarily an Australian incident. Australian Federal Police investigated the incident and arrested intruders that were involved. Table 10.22 lists the top-level domains of the sites involved.

| Reporting Sites | | |
|---|---|---|
| **domain** | **# sites** | **% sites** |
| .au | 1 | 33.3% |
| .de | 1 | 33.3% |
| .uk | 1 | 33.3% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| **domain** | **# sites** | **% sites** | **domain** | **# sites** | **% sites** |
| .au | 37 | 47.4% | .tr | 2 | 2.6% |
| .edu | 16 | 20.5% | .uk | 2 | 2.6% |
| .com | 6 | 7.7% | .de | 1 | 1.3% |
| .ca | 5 | 6.4% | .in | 1 | 1.3% |
| .org | 4 | 5.1% | .kr | 1 | 1.3% |
| .net | 2 | 2.6% | .us | 1 | 1.3% |

**Table 10.22. Reporting and Other Sites for Severe Incident Number 22 (See Table 10.2 and Figure 10.8)**

The keywords used in the CERT®/CC record of Incident #22 to describe the methods of operation were as follows:

> NFS attack, password files, Trojan login, Trojan inetd, nfsbug, sniffer, *rootkit*, deleted files, .rhosts, FTP abuse, software piracy, warez, hosts.equiv, loadmodule, mailrace, rdist, rlogin, *chasin*, sendmail, Trojan rshd, weak passwords, password cracking.

**10.2.8. Incident #16 - Toolkit, Sniffer and IRC** - In September, 1994, an incident began which was unusually large. It involved at least 515 sites and 224 days. The number of messages to and from the CERT®/CC was over 1,900. The tools used by the intruders primarily were sniffers and the *rootkit* toolkit. But the incident also included some unusual uses of Internet Relay Chat (IRC). Several of the intruders spent a lot of time "chatting" with other hackers on IRC. Social engineering was used on IRC to convince other users on IRC to use an IRC client which had a back door enabling intruders to obtain access to the user's account. This method of attack is described in CERT® Advisory CA-94:14, "Trojan Horse in IRC Client for UNIX."

The top-level domains of the sites involved in Incident #16 are listed in Table 10.23. It is interesting to note that, not only were there a large number of sites involved, but 43 of these sites reported the incident to the CERT®/CC. The number of different methods of operation used was

also unusually large. The keywords used in the CERT®/CC record of Incident #16 to describe the methods of operation were as follows:

> *rootkit*, sniffer, user accounts, system accounts, *crack*, login attempts, NIS attack, rdist, social engineering, systems files deleted, Trojan IRC, Trojan ls, Trojan ifconfig, Trojan ps, Trojan login, Trojan mail, weak password, password file, password cracking, TFTP attack, uudecode alias, sendmail attack, IRC abuse, IRC flooding, password -f, mail spoofing, mail bombs, DOS attack, guest account, no password, FTP abuse, software piracy, telnet connections, rlogin connections, mailrace, NFS attack, halt system, chain letter, lpr print, expreserve, *SATAN*, configuration, gopher, httpd, uucp, rexd attack, *warez*, open servers.

| Reporting Sites | | |
|---|---|---|
| domain | # sites | % sites |
| .edu | 24 | 55.8% |
| .com | 8 | 18.6% |
| .ca | 4 | 9.3% |
| .org | 2 | 4.7% |
| .au | 1 | 2.3% |
| .de | 1 | 2.3% |
| .il | 1 | 2.3% |
| .net | 1 | 2.3% |
| .us | 1 | 2.3% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| domain | # sites | % sites | domain | # sites | % sites |
| .edu | 151 | 32.0% | .si | 3 | 0.6% |
| .com | 91 | 19.3% | .tw | 3 | 0.6% |
| .ca | 36 | 7.6% | .br | 2 | 0.4% |
| .net | 35 | 7.4% | .ch | 2 | 0.4% |
| .org | 25 | 5.3% | .gr | 2 | 0.4% |
| de | 19 | 4.0% | .hk | 2 | 0.4% |
| .au | 16 | 3.4% | .nz | 2 | 0.4% |
| .fi | 13 | 2.8% | .su | 2 | 0.4% |
| .gov | 7 | 1.5% | .z | 2 | 0.4% |
| .fr | 6 | 1.3% | .cz | 1 | 0.2% |
| .il | 6 | 1.3% | .ee | 1 | 0.2% |
| .mil | 6 | 1.3% | .ge | 1 | 0.2% |
| .nl | 5 | 1.1% | .hr | 1 | 0.2% |
| .no | 5 | 1.1% | .kw | 1 | 0.2% |
| .us | 5 | 1.1% | .mx | 1 | 0.2% |
| .uk | 4 | 0.8% | .sk | 1 | 0.2% |
| .at | 3 | 0.6% | .th | 1 | 0.2% |
| .it | 3 | 0.6% | .tr | 1 | 0.2% |
| .pl | 3 | 0.6% | .za | 1 | 0.2% |
| .se | 3 | 0.6% | | | |

**Table 10.23. Reporting and Other Sites for Severe Incident Number 16 (See Table 10.2 and Figure 10.8)**

As can be seen in Table 10.23, Incident #16 involved intrusions on systems throughout the world. Only Incident #1 was a more severe incident than this, but the pattern of attack and the widespread number of intruders in Incident #16 makes the incidents fundamentally different. What holds Incident #16 together – what makes it one incident instead of many smaller incidents – was a degree of similarity of techniques, and a degree of similar timing. Ultimately, the judgment of CERT®/CC personnel was what related these sites together in their record of the incident.

**10.2.9. Incident #20 - IP Spoofing** - The remaining severe CERT®/CC incident began in May, 1995. It was dominated by IP spoofing attacks as described in CERT® Advisory CA-95:01, "IP Spoofing Attacks and Hijacked Terminal Connections," which was released by the CERT®/CC

on January 23, 1995 – more than 4 months earlier. Interestingly, the attack method was described as early as 1989 in a published paper by Steve Bellovin [Bel89]. The description of the attack process given in CERT® advisory CA-95:01 is as follows:

> To gain access, intruders create packets with spoofed IP addresses. This exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. It is possible to route packets through filtering-router firewalls if they are not configured to filter incoming packets whose source address is in the local domain.

Most of the attacks in the early part of Incident #20 originated from a "handful" of sites on U.S. East Coast. The top-level domains of the sites involved are given in Table 10.24. The keywords used in the CERT®/CC record of Incident #20 to describe the methods of operation were as follows:

> IP spoofing, sniffer, Trojan login, Trojan ps, Trojan netstat, Trojan inetd, Trojan inetd, Trojan libkvm, Trojan libc, NIS attack, NFS attack, rdist, loadmodule, sendmail, selection service, .rhosts, hosts.equiv, files deleted, *chasin*, software piracy.

| Reporting Sites | | |
|---|---|---|
| **domain** | **# sites** | **% sites** |
| .edu | 2 | 50.0% |
| .net | 1 | 25.0% |
| .gov | 1 | 25.0% |

| Other Sites | | | | | |
|---|---|---|---|---|---|
| **domain** | **# sites** | **% sites** | **domain** | **# sites** | **% sites** |
| .edu | 131 | 49.8% | .il | 2 | 0.8% |
| .com | 39 | 14.8% | .my | 2 | 0.8% |
| .net | 29 | 11.0% | .no | 2 | 0.8% |
| .de | 14 | 5.3% | .ae | 1 | 0.4% |
| .jp | 6 | 2.3% | .au | 1 | 0.4% |
| .org | 6 | 2.3% | .be | 1 | 0.4% |
| .z | 5 | 1.9% | .ch | 1 | 0.4% |
| .ca | 4 | 1.5% | .kr | 1 | 0.4% |
| .us | 4 | 1.5% | .mil | 1 | 0.4% |
| .uk | 3 | 1.1% | .nl | 1 | 0.4% |
| .at | 2 | 0.8% | .se | 1 | 0.4% |
| .dk | 2 | 0.8% | .ve | 1 | 0.4% |
| .gov | 2 | 0.8% | .za | 1 | 0.4% |

**Table 10.24. Reporting and Other Sites for Severe Incident Number 20 (See Table 10.2 and Figure 10.8)**

IP spoofing is an attack that is particularly hard to detect. When an attack is discovered, its origin is even harder to determine. After all, the packets arriving at the attacked site have an incorrect IP address. The end result was that CERT®/CC response personnel theorized in the record of Incident #20 that they may only be seeing the "tip of the iceberg" in an attack such as this. An additional concern is that most of the attacks detected were both successful, and directed primarily against systems involved in the operation of the network. One member of the response team for this incident stated the problem this way in June, 1995:

> ...over the past few weeks we have been receiving reports of IP spoofing attacks against Internet sites internationally. The attacks have involved over a hundred sites and have been largely successful. Of particular concern is that a majority of the attacked sites are nameservers, routers, and other network operation systems.

On the other hand, this was the only severe incident in the CERT®/CC records involving IP spoofing. In addition, very few other incidents reported IP spoofing (see Chapter 7). Prevention of this type of attack is relatively straight forward. As described in CERT® Advisory CA-95:01,

> The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network.

### 10.3. Summary of Severe Incidents

A criteria was developed for this research in order to identify the most severe incidents in the CERT®/CC records. The criteria developed were as follows: ≥ 79 days duration, ≥ 62 sites, and ≥ 87 messages. This selected 22 incidents with an average of 203 days duration, which involved an average of 169 sites, and contained an average of 466 messages in the CERT®/CC record.

There were two predominant trends seen in the 22 severe incidents. First, the sophistication of intruder techniques progressed from simple user commands, scripts and password cracking, through the use of tools such as sniffers (1993) and toolkits (1994), and finally to intricate techniques that fool the basic operation of the Internet Protocol (1995). The second trend was that intruders became increasingly difficult to locate and identify. In the early incidents, the attackers tended to be a few individuals confined to a specific location or group of locations, and as a consequence, tended to be easily identifiable. As intruder tools became more sophisticated and the size of the Internet grew, the severe incidents involved more attackers operating in many different locations. The newest and most sophisticated techniques allowed the attackers to obtain nearly total obscurity.

For these 22 incidents, a three-phase process of attack was consistently used: 1) gain access to an account on the target system, 2) exploit vulnerabilities to gain privileged (root) access on that system, and 3) use this privileged access to attack other systems across the network.

*Chapter 11*

# Denial-of-Service Incidents

The Internet Worm incident during the first week of November 1988, was the incident that resulted in the establishment of the CERT®/CC as discussed in Chapter 3. It was also the first wide-spread denial-of-service attack on the Internet. Service was denied in two ways. First, infected hosts were rendered useless because their processing capability was absorbed by multiple copies of the worm program. Until all copies of the worm were removed, these hosts were not available for their intended use. Second, although most hosts on the Internet were never infected by the worm, the fear of infection effectively "shut down" the Internet for several days as many sites disconnected from the network as a defensive measure [Hug95:142].

Since the Internet Worm, there has not been another large-scale denial-of-service incident on the Internet. On the other hand, operating systems for host computers on the Internet provide few protections from denial-of-service attacks [GaS96:759]. It would, therefore, seem possible that denial-of-service incidents *could* become widespread on the Internet. As will be shown in this chapter, however, these type of incidents were apparently not widespread during the period of this study. This chapter presents the limited denial-of-service incidents that have been reported to the CERT®/CC.

## 11.1. Denial-of-service Definition and Types

The baseline security that every user needs from a computer system is *availability*. Hardware and software must be kept working efficiently or else they become useless [RuG91:10]. If computer hardware, software, and data are not kept available, productivity can be degraded, even if nothing has been damaged [ISV95:20]. Denial-of-service can be conceived to include both intentional and unintentional assaults on a system's availability. The most comprehensive perspective would be that regardless of the cause, if a service is supposed to be available and it is not, then service has been denied [Coh95:55].

An *attack*, however, is an intentional act. A *denial-of-service attack*, therefore, is considered to take place only when access to a computer or network resource is *intentionally* blocked or degraded as a result of malicious action taken by another user [Amo94:4]. These attacks don't necessarily damage data directly, or permanently (although they could), but they intentionally compromise the *availability* of the resources [RuG91:10].

An attacker carries out a denial-of-service attack by making a resource inoperative, by taking up so much of a shared resource that none of the resource is left for other users, or by degrading the resource so that it is less valuable to users. Those shared resources are reached through processes and can include other processes, shared files, disk space, percentage of CPU, modems, etc. [GaS96:759].

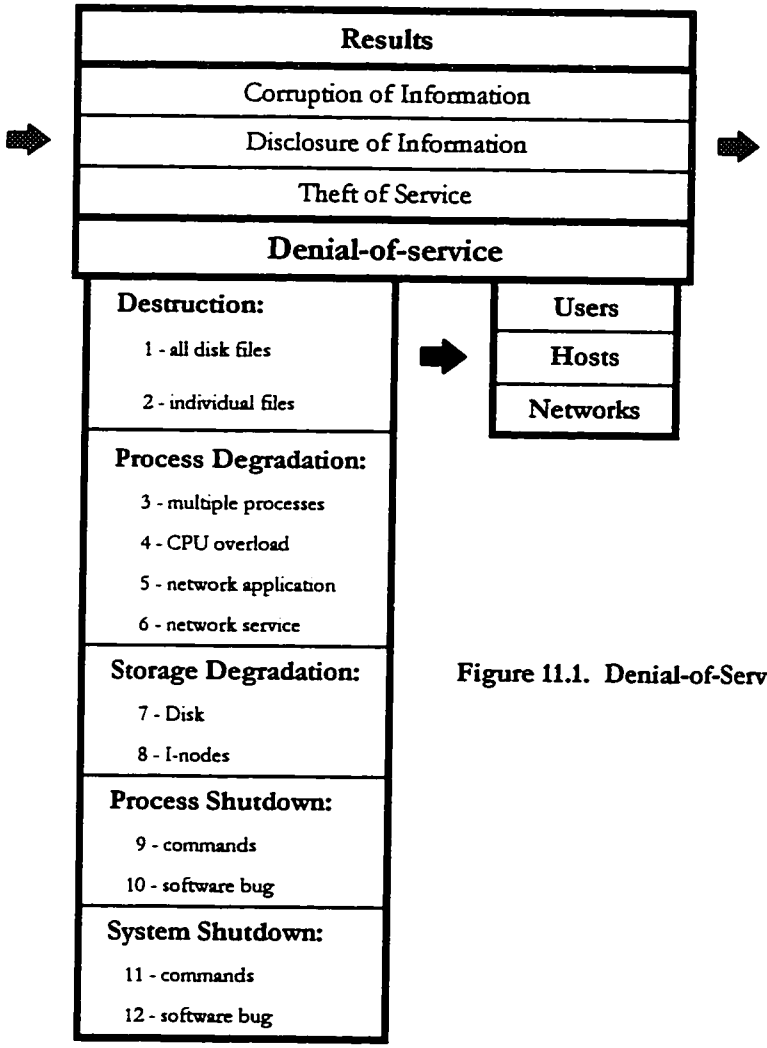


**Figure 11.1. Denial-of-Service Attack Methods**

Denial-of-service attacks over the Internet can be directed against three types of targets: a user, a host computer, or a network. This is shown in Figure 11.1, which expands a portion of the taxonomy developed in Chapter 6. Following the process in Figure 6.9, an attacker must begin a denial-of-service attack by using tools to exploit vulnerabilities and then either obtain unauthorized access to an appropriate process or group of processes, or to use a process in an unauthorized way. The attacker then completes the attack by using some method to destroy files, degrade processes, degrade storage capability, or cause a shutdown of a process or of the system.

This chapter presents a general discussion of these categories of denial-of-service attack. The frequency of specific methods of attack are discussed in Chapter 8 and in Appendix A.

**11.1.1 Destruction** - If an attacker obtains access to user, host, or network files, the attacker could delete or corrupt some or all of these files. The effect could be to deny the use of these files. At the user level, an attacker could delete some or all of the account's files, rendering the account unusable. At the host level, critical system files could be deleted. On Unix systems, this could be files such as the */etc/passwd* file, or files containing the system's programs. All files on the host's hard disk could also be removed, or the disk itself could be reformatted [GaS96:760]. This would make the host computer inaccessible or unusable to all users. At the network level, network files could be destroyed. The network or some of its services could then be degraded or unavailable.

Computer *viruses* (self-replicating, autonomous computer code fragments [RuG91:79]), or *worms* (self-replicating complete programs) often contain destructive payloads which corrupt or destroy some or all of a system's files. When a virus or worm operates in this manner, it would be causing denial-of-service.

Denial-of-service can be caused in a different way by the *flash* family of programs occasionally used on the Internet. These programs are designed to use the *talk* program to send control characters intended to cause changes in system terminal settings, which can cause the keyboard to lock, the screen to be unusable, or files to be corrupted [GaS96:333]. Electronic mail can also be used to send these control characters [Par90:545].

Another example of a method of denial-of-service through the destruction of files is found in some types of attacks against Usenet newsgroups or bulletin board systems. An example of an attack would be to delete postings by other users. Service to that user and the other users of that service would then be denied.

Not all cases of file destruction should be considered a denial-of-service attack. For example, an attacker could delete a user's data files with the intention of destroying the user's stored information. This would be different than removing the user account itself, which would deny service to the user. The distinction between these is exact, but its classification also requires some understanding or speculation about the attacker's intentions. If the attacker's objective is to destroy information, then this would be in the "corruption of information" category. If the attacker's intention is to prevent the use of computer or network capabilities, then this would be considered in "denial-of-service." This potential problem is discussed in Chapter 13, where the taxonomy's utility is evaluated.

**11.1.2 Process Degradation** - Instead of destroying files, denial-of-service could be accomplished through overloading processes on a host computer to such a point that the users' ability to use the resource is degraded either by reduced performance, or by the resource becoming unavailable. This can take place in two ways. First, an attacker could connect to a host across the Internet and then spawn *multiple processes* on the host to the point where the host could no longer support any new processes, either for an individual user, or for all the users on the target host computer. The targeted user, or users, would then not be able to run processes of their own [GaS96:761]. Programs that accomplish this are sometimes referred to as *fork bombs*. A second method would be to slow the host computer by spawning many processes that consume large amounts of central processing unit (CPU) time, causing a *CPU overload* [GaS96:764].

An attacker does not need to connect directly to a command interface on a host computer to cause a process degradation. An attacker could instead direct an attack against network processes. Figure 11.2 shows the layering for the primary Internet protocol suite, Transmission Control Protocol/Internet Protocol (TCP/IP) [Cer93:83].[1] In the classification shown in Figure 11.1, attacks against processes conceptualized at the application layer in a network protocol suite are classified as attacks directed at a *network application* and attacks against processes conceptualized to be at lower layers are considered directed at a *network service*.

| Target | Layer | Examples |
|---|---|---|
| Network Application | Application | HTTP, FTP, Telnet, SMTP (mail), Finger, X-Windows |
| Network Service | Transport | UDP, TCP, TP4, Routing |
| | Internet | ICMP, IP, CLNP, Ping |
| | Subnetwork | Ethernet, X.25, FDDI, Token Ring |
| | Link | HDLC, PPP, SLIP |
| | Physical | RS232, V.35, 10BaseT, fiber, etc. |

**Figure 11.2. Internet Protocol Layering Compared to Network Process Categories**

For both network services and network applications, the denial-of-service attack method is to send a flood of network requests to a server program (daemon) on a host computer.

> These requests can be initiated in a number of ways, many intentional.[2] The result of these floods can cause [a] system to be so busy servicing interrupt requests and network packets that it is unable to process regular tasks in a timely fashion [GaS96:775].

[1] Another common protocol suite is the seven-layer OSI protocol suite developed in Europe [Cer93:83]

[2] A software error can result in a flood of network requests which may result in a network service being overwhelmed and unavailable to a user. This would not be considered a denial-of-service *attack* because it was not an intentional act.

One type of network attack directed against network services is a *broadcast storm.* Although broadcast storms usually occur through faulty software or failing hardware, they can be used for intentional attack [GaS96:777]. Broadcast storms result when

> . . . a host receives a broadcast, decides it needs to be responded to, and then blindly sends the response back out to the destination address, resulting in another broadcast. A few hosts doing this, perhaps infinitely as they respond to the new broadcasts with more broadcasts, can cause the network to freeze up entirely [LyR93:452].

The *nuke* family of programs sometimes used on the Internet, is similar to a broadcast storm in that it accomplishes denial-of-service at the network service layer by overloading a system with Internet Control Message Protocol (ICMP) "Echo" or "Destination Unreachable" messages [GaS96:461]. These are commonly called *Ping floods*, or *ICMP bombs.*

In some cases, requests for network services only need to be initiated in order to cause denial-of-service. An attacker could send multiple requests to initiate a connection but then fail to respond to the network server, which would prevent completing the connection. The network server would then have multiple half-open connections waiting to time out, which would consume network resources [GaS96:778].

There are even some cases where a single packet could cause system problems and denial-of-service. This occurs when a process does not properly check for a packet to be of the correct form when it is received. In the case of the *ping* utility, an assumption is often inadvertently made by programmers implementing this utility that incoming packets will be small. In some instances, a large packet sent to the *ping* utility can cause systems to shut down (the so-called "ping of death").[3]

**11.1.3 Storage Degradation -** A similar, although distinguishable, method of attack is aimed at consuming disk storage capacity on the target host or network of hosts. Since a disk has finite capacity, if an attacker fills up a user's disk quota, or fills up the space available for all users, then the user's account or the entire host, will not be available for use until the *disk full* condition is changed [GaS96:764]. An attacker can either create too many files for the system, or a few files that are too large. The same is true for a network, where the files may be distributed across multiple computers.

An example of such an attack is "mail bombardment," or "mail spam." The attacker accomplishes this attack by either flooding a user, or group of users, with numerous, perhaps thousands, of electronic mail (e-mail) messages [ISV95:13], by flooding the user with very large messages, or by flooding the user having messages with large attachments. Any of these would

---

[3] As described by Dr. Thomas A. Longstaff, CERT®/CC.

quickly fill up a user's Mailbox, which would then deny the user access to e-mail, and perhaps all system services. Depending on how the system is configured, this could cause the system to run out of storage space and then stop processing for all users on the host or network. The attacker could also easily forge the "From:" block in these messages, which would disguise their origin.

A variation on this type of attack would be to create enough *empty* files on a disk or network file service to exceed the I-node capacity of the file system [GaS96:767]. I-nodes (index-nodes) are special tables associated with each file that list the attributes and disk addresses of the file. For small files, the I-nodes and all of the file are stored together. For larger files, the I-nodes contain addresses that point to other locations on the disk where other parts of the file are stored [Tan92:165]. If the supply of available I-nodes is exhausted, an *I-nodes full* condition, then the operating system cannot create a new file, even if disk space is available [GaS96:766].

Usenet newsgroups and bulletin board systems provide another possible way to degrade storage. In this case, an attacker makes numerous postings of material that is inappropriate or otherwise unwanted on one or more newsgroups or bulletin boards. These postings are commonly referred to as *spam*. Spam may result in more than just the irritation of the users. It takes up resources, makes systems slower to respond, and may stifle the use of these systems.

**11.1.4. Shutdowns** - The last two categories of denial-of-service attacks shown in Figure 11.1 are *process shutdown* and *system shutdown* attacks. In these types of attacks, the attacker aims at halting a process, or all processing, on a host or network. If the attacker has privileged access, this could be accomplished by issuing the appropriate commands to kill a process or shutdown the system completely. The *kill* command in Unix is an example of a command that could be used to terminate a process.

A complete system shutdown across a network may not be possible in some systems. On a Unix system, for example, a partial shutdown may be accomplished by running a program such as */etc/shutdown*, which brings the system to the single-user mode [Sob95:497]. This would, however, result in the loss of network access for all users, including the attacker. An alternative would be to use the appropriate command to terminate processes on the host. For example, if logged in as a Unix superuser, an attacker could issue a command such as *kill -9 0*, which would terminate all processes and bring the system down [Sob95:624].

As shown in Figure 11.1, process or system shutdown could be caused by exploiting a *software bug* that causes the process or system to halt. In this case, an attacker has knowledge of a "silver bullet" command, or set of commands, that will crash the process or system. Just as with software

bugs that are used to gain access, it is unlikely that such a command would be effective against all systems, but until the software bug is corrected, all systems of a certain type would be vulnerable.

## 11.2. History of Internet Denial-of-Service Attacks

**11.2.1. Numbers of Attacks** - The CERT®/CC has records of 104 denial-of-service incidents that took place on the Internet between 1989 and 1995. In addition, 39 other incident reports classified as either root-level or account-level break-ins also included denial-of-service attacks.[4] These 143 incidents represent only 3.3% of the CERT®/CC incident reports. Of these 143 incidents, six took place at Site A, the case study site (discussed in Chapter 9). Figure 11.3 shows the average number of sites per day involved in denial-of-service incidents recorded by the CERT®/CC (including Site A). Because there are so few incidents in the CERT®/CC records, the incidents shown in Figure 11.3 were averaged over quarters.[5]

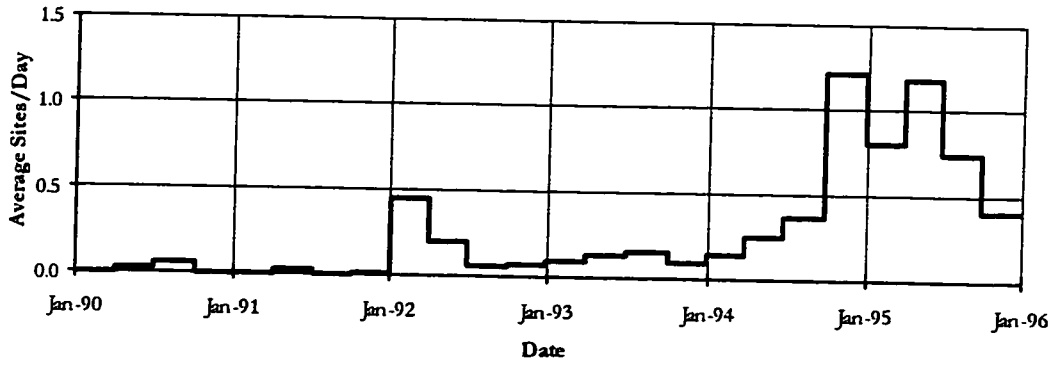


**Figure 11.3. Sites per Day Involved in Denial-of-service Attacks, Averaged Over Each Quarter, as Recorded in CERT®/CC Records**

A comparison to the size of the Internet is given in Figures 11.4 and 11.5. For Figure 11.4, the growth in Internet *domains* (discussed in Chapter 2) was used to determine the average sites per day per 100,000 Internet domains. If the rate of denial-of-service attacks matched the growth of Internet domains, we would expect to see a steady average. Instead, peaks occurred in 1990, 1992 and at the end of 1994. A simple linear least squares fit of the data in Figure 11.4 showed the slope to be positive, but not statistically different from zero ($\alpha = 5\%$).

---

[4] Recall that in Chapter 7, incidents were classified into one of six categories. If the incidents involved root- or account-level break-ins, *and* they mentioned denial-of-service attacks or methods, then they were classified as root- or account-level break-ins. If they did *not* involve root- or account-level break-ins, and they mentioned denial-of-service attacks or methods, they were classified into the denial-of-service category. In other words, actual *break-ins* took precedence over denial-of-service for an overall classification.

[5] Sites per day for denial-of-service incidents were calculated in the same manner as in Chapter 7. The number of days for each incident was divided by the incident's duration. The sites per day for all incidents in the category were added together for each day and then averaged over quarters.

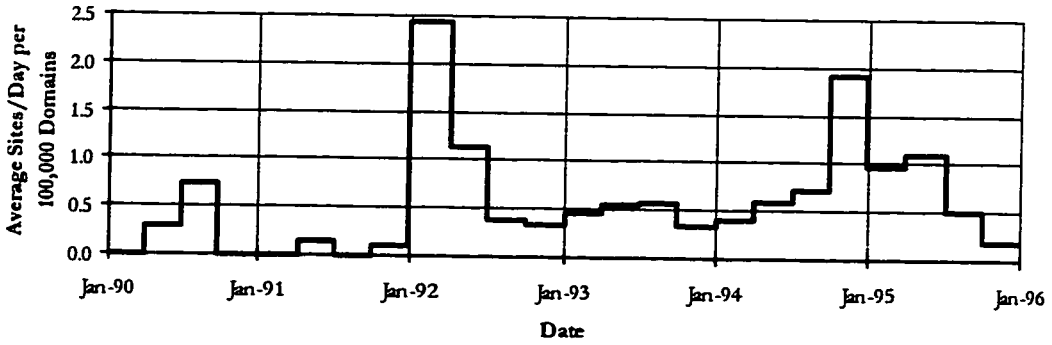


**Figure 11.4. Sites per Day Involved in Denial-of-service Attacks, per 100,000 Internet Domains Averaged Over Each Quarter, as Recorded in CERT®/CC Records [Lot92; Lot96]**

The pattern shown in Figure 11.4 may be influenced somewhat by the reduction in the number of Internet hosts per Internet domain after 1993, as shown in Chapter 2 (Figure 2.8). For Figure 11.5, the growth in Internet *hosts* (discussed in Chapter 2) was used to determine the average sites per day per 10,000,000 Internet hosts. Again, if the rate of denial-of-service attacks matched the growth of Internet hosts, we would expect to see a steady average. Instead, a large peak is shown in 1992, and smaller peaks are shown in 1990, and at the end of 1994. With these exceptions, however, the rate of denial-of-service reports to the CERT®/CC relative to the number of Internet hosts has been relatively constant, and presented this way, the decline in 1995 appears less significant.

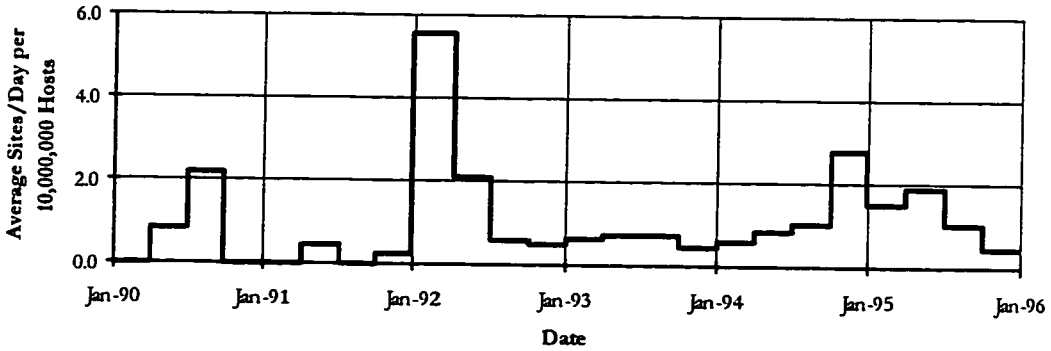


**Figure 11.5. Sites per Day Involved in Denial-of-service Attacks, per 10,000,000 Internet Hosts Averaged Over Each Quarter, as Recorded in CERT®/CC Records [Lot92; Lot96]**

The data from Figure 11.5 were fitted to a line using simple regression. The slope was found to be positive (0.13 sites/day/year/10,000,000 hosts), and statistically different from zero ($\alpha$ = 1%). This corresponds to an increase of around 50% per year ($R^2$ = 39.0%), which indicates denial-of-

service was becoming a greater problem for the Internet during this period. The sample size, however, was small, with the absolute numbers being only 143 incidents (3.3% of all incidents).[6]

**11.2.2. Methods of Attack** - Each of the 143 denial-of-service incidents in the CERT®/CC records used at least one of the methods in the categories of Figure 11.1. Five of these incidents included multiple methods of attack (a total of eight additional methods used were recorded). In addition, the Internet Worm of November, 1988, was an additional denial-of-service attack not recorded in the early CERT®/CC records. Figure 11.6 shows these 152 instances of a denial-of-service methods being used, classified according to attack method (Figure 11.1).

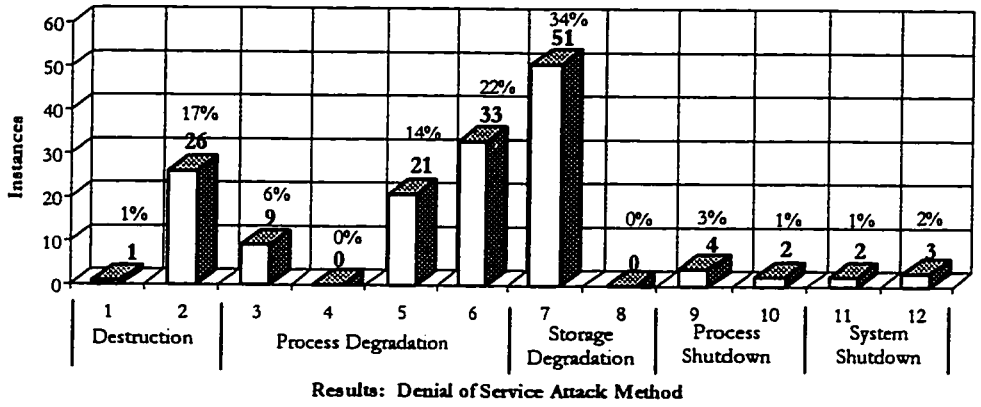


**Figure 11.6. Denial-of-service Attacks by Method, as Recorded in CERT®/CC Records**

| Destruction: | Process Degradation: | Storage Degradation: | Process Shutdown | System Shutdown: |
|---|---|---|---|---|
| 1. All disk files | 3. Multiple processes | 7. Disk full | 9. Commands | 11. Commands |
| 2. Critical files | 4. CPU overload | 8. I-nodes fill | 10. Software bug | 12. Software bug |
| | 5. Network application | | | |
| | 6. Network service | | | |

Aside from the overall low numbers of denial-of-service incidents, perhaps the most interesting aspect of CERT®/CC records of denial-of-service attacks can be seen in Figure 11.6: the small numbers of denial-of-service attacks resulting in the destruction of files. Even the 27 incidents shown were primarily minor attacks. First, the majority (15) of these incidents involved the use of variants of the *flash* program to send control characters to modify the files controlling the screen and keyboard of a host computer. The rest of the incidents involved the deletion of files on host computers, including the deletion of user accounts, the deletion of files on bulletin board systems, and one incident of the corruption of root name server files. Only one incident resulted in the deletion of all files on a host computer's hard drive. This was an incident where an intruder had

[6] As shown in Chapter 7, the growth rate was not statistically different from zero if none of the root or account break-in incidents are included.

broken into a computer at the root level and then found out he was being monitored. He removed all files on the hard drive before terminating his last connection.

More than 40% of denial-of-service instances in the CERT®/CC records were in the category of Process Degradation. Eight of the incidents were characterized by the intruder overloading a host computer with multiple processes – *fork bombs*. An additional incident, the Internet Worm, became a denial-of-service incident when copies of the worm on host computers spawned multiple copies, causing processing on these hosts to slow and usually terminate [ISV95:14]. The remaining process degradations were accomplished by repeated calling of network applications (finger, login, mail, IRC, talk and inetd), or with floods of ICMP and Ping messages (primarily *nuke* family programs).

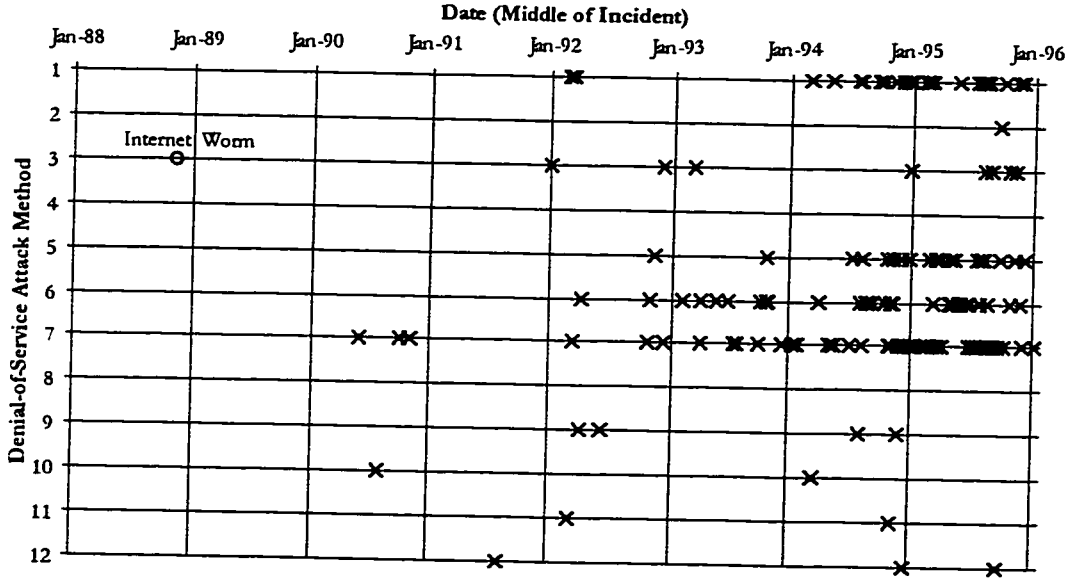


**Figure 11.7. Primary Category of Denial-of-service Attacks, as Recorded in CERT®/CC Records within the following categories (see Figure 11.1):**

| Destruction: | Process Degradation: | Storage Degradation: | Process Shutdown | System Shutdown: |
|---|---|---|---|---|
| 1. All disk files | 3. Multiple processes | 7. Disk full | 9. Commands | 11. Commands |
| 2. Critical files | 4. CPU overload | 8. I-nodes fill | 10. Software bug | 12. Software bug |
| | 5. Network application | | | |
| | 6. Network service | | | |

The largest single method used for denial-of-service attacks as recorded in CERT®/CC records was the use of mail spam to degrade storage capacity (49 incidents, 32% of instances). In another two incidents, this same result was achieved by using the file transfer protocol (FTP) to transfer large files to the host computer.

Finally, process or systems shutdown was achieved in 11 of the incidents. The methods used included terminating user connections (3 incidents IRC, 3 incidents telnet), commanding host

computer shutdown (2 incidents), and exploiting software bugs to cause shutdown (3 instances). There were no instances of attacks directed specifically at overloading the CPU processing capability (Method 4), or specifically at exceeding the I-node capacity (Method 8).

Figure 11.7 shows these 152 instances of denial-of-service methods, plotted by method over time. There is some indication in this figure of the peak in sites per day at the end of 1994. The peak in 1992 is less visible, but it occurred when the Internet was smaller and the incidents at this time involved more sites per incident.

**11.2.3. Additional Denial-of-service Attack Characteristics** - Two additional characteristics of denial-of-service attacks were shown in CERT®/CC records. First, the average number of sites involved in denial-of-service incidents is relatively low compared to root and account level break-ins. The mean number of sites involved in the 4,299 incidents reported to the CERT®/CC between 1989 and 1995 was 6.5. On the other hand, the average number of sites per incident in the 104 denial-of-service incidents in this population was 3.7. These were statistically different according to a two-sample t-test assuming unequal variances [$P(T \leq t)$ one-tail = 0.0007].[7]

In addition, 70% of these incidents involved only two sites: the attacking site and the target site. Only three of the incidents involved more than six sites. In fact, none of the denial-of-service incidents in the CERT®/CC records is of the order of magnitude of the Internet Worm, which involved 2,100 to 2,600 host computers, representing around 5% of the entire Internet at the time [RuG91:4].[8]

The other additional characteristic of CERT®/CC denial-of-service records is that a large number of the attackers were apparently identified. Although the CERT®/CC records do not confirm that it was "relatively easy to figure out who was responsible" for the attacks, as postulated by Ritchie [GaS96:759], the attacker was reported in more than 50% of the denial-of-service incidents. This is significantly higher than the other incidents reported to CERT®/CC.

Chapter 12 gives an estimate of the total rate of denial-of-service attacks on the Internet using the information from this chapter and Chapter 9.

---

[7] The distribution of the number of sites in an incident was lognormal. Because of the large sample size, assuming the distribution is normal may be satisfactory. The Wilcoxan Two-Sample test for independent samples, a non-parametric test, did *not* show the means to be statistically different.

[8] The number of hosts infected with the Internet Worm is generally believed to be 6,000. The actual number, however, appears to have been 2,100 to 2,600 [RuG91:4]. The number of *sites* involved, around 100 probably, makes this the largest known denial-of-service incident.

### 11.3. Summary of Denial-of-Service Incidents

The Internet Worm incident during the first week of November 1988, was a wide-spread denial-of-service attack. Since the Internet Worm, there has not been another large-scale denial-of-service incident on the Internet. On the other hand, the CERT®/CC records do not give any indication that Internet denial-of-service incidents could not become widespread.

A *denial-of-service attack* is considered to take place only when access to a computer or network resource is *intentionally* blocked or degraded as a result of malicious action taken by another user. These attacks don't necessarily damage data directly, or permanently (although they could), but they intentionally compromise the *availability* of the resources. An attacker carries out a denial-of-service attack by making a resource inoperative, by taking up so much of a shared resource that none of the resource is left for other users, or by degraded the resource so that it is less valuable to users. Those shared resources are reached through processes and can include other processes, shared files, disk space, percentage of CPU, modems, etc.

Denial-of-service attacks over the Internet can be directed against three types of targets: a user, a host computer, or a network. An attacker must begin a denial-of-service attack by using tools to exploit vulnerabilities and then either obtain unauthorized access to an appropriate process or group of processes, or to use a process in an unauthorized way. The attacker then completes the attack by using some method to destroy files, degrade processes, degrade storage capability, or cause a shutdown of a process or of the system.

Unlike other attacks reported to the CERT®/CC, denial-of-service incidents grew at a rate around 50% per year greater than the rate of growth of Internet hosts. This indicates that denial-of-service was becoming a greater problem for the Internet during this period, although the total number of denial-of-service incidents was small.

The largest single method used for denial-of-service attacks as recorded in CERT®/CC records was the use of mail spam to degrade storage capacity (49 incidents, 32% of instances). Another large category was process degradation (40% of the instances).

The average number of sites involved in denial-of-service incidents was found to be relatively low compared to root and account level break-ins. In addition, a large number of the attackers were apparently identified, compared to the average for all incidents.

*Chapter 12*

# Estimates of Total Internet Incident Activity

Estimates of total Internet incident activity vary widely. The actual number of incidents reported to the CERT®/CC can be considered the minimum estimate. For 1995, 1,168 actual incidents were reported to the CERT®/CC (Figure 7.3). The largest estimate found during this research for this same year was 900 million attacks [Coh95:40]. Even though the CERT®/CC estimate is of *incidents*, and this largest estimate is of *attacks*, this nearly six order of magnitude difference reflects how little is actually known about the total Internet activity.

Total Internet security activity could be measured by either the total Internet *attack* activity or the total Internet *incident* activity. This chapter examines simple estimates of Internet *attack* activity based primarily on projections from vulnerability studies by Defense Department organizations. The estimated number of attacks per year in 1995 ranged between 40,000 and 2.5 million based on these studies.

Estimates of total Internet *incident* activity were made by projecting data from Site A, and from estimating the percentage of incidents reported based on estimates of attacks per incident and the probability of an attack being reported. The estimated number of incidents per year in 1995 ranged between 1,200 and 22,800.

The final sections of this chapter show that a minimum of 96% of severe incidents (defined in Chapter 10) were reported to the CERT®/CC, and the probability of an above average incident (in terms of duration and number of sites) being reported was a minimum of 1 out of 2.6 (and nearly all of them may have been reported).

## 12.1. Relationship of Attacks, Incidents and Total Activity

As discussed in Chapter 1, there is a difference between an *attack* and an *incident*. An *attack* is a single unauthorized access attempt, or unauthorized use attempt, regardless of success. An *incident*, on the other hand, involves a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing. The CERT®/CC records were of incidents, which were composed of numerous attacks.

Since attacks make up incidents, total Internet security *activity* could be measured by either the total Internet *attack* activity or the total Internet *incident* activity. Unfortunately, very little has been known about either of these. Consequently, as was stated in Chapter 1, our knowledge about total Internet security activity prior to this research has been incomplete and primarily anecdotal.

### 12.2. Estimates of Total Internet Attack Activity

In order to estimate the number of *attacks*, some sample of Internet activity is required. This is primarily because *incidents* (not attacks) are generally reported. There are three ways to obtain a sample of attack activity: 1) a representative site or series of sites could be monitored for attack activity, 2) a representative site or series of sites could be requested to report all attack activity, and 3) representative sites could be attacked in some systematic manner to determine the rate of reporting. The results of such experiments could be compared to actual attack reports to determine the total number of attacks. These three approaches will be discussed in the following three sections.

**12.2.1. Monitoring Sites For Attack Activity** - The first approach to determining total Internet attack activity would be to monitor a site, or several representative sites, for attack activity, and then to use information about the size of the Internet to project this site activity to total Internet attack activity. It is likely that such monitoring has been conducted at numerous sites, but by personnel at that site only. This is the type of information that most sites would be reluctant to have become public and it is unlikely that sites would allow monitoring of their network by outside agencies. It is also technically difficult to monitor the activity at one site from another site. As such, this does not appear to be a viable option to obtaining sample attack data. In addition, the results from any such monitoring program do not appear to have been published.

**12.2.2. Reports of Attack Activity From Representative Sites** - Instead of monitoring attack activity, representative sites could monitor for attacks at their own sites and then report all attack activity either publicly, or to some agency in confidence, such as to the CERT®/CC. These data could then be used, along with information about the size of the Internet, to project this site activity to total Internet attack activity. A search of related literature has not indicated that this has taken place either spontaneously, nor as part of any scholarly research or program in this area.

Projections from the activity at a single site to the Internet as a whole would be highly dependent on the accuracy of the site information, and on how typical the site is. In other words, such a projection would be very sensitive to errors in the site information, and to assumptions about the size of the site compared to the size of the Internet.

One example of using the attack activity at a group of sites to estimate the total Internet attack activity was given by Cohen as follows:

> Several authors have reported that once detection was put in place, over one incident per day was detected against their computers attached to the Internet. Other people have placed detection systems on the Internet to detect attacks and have privately reported

similar figures. There are about 2.5 million computers on the Internet, so simple multiplication tells us that something like 900 million attacks per year take place on the Internet alone [Coh95:40].

This projection is in error for several reasons. First, the sites that reported an average of one attack per day were well-known, attractive sites. In this case, one of the sites was Bell Labs, as reported by Cheswick and Bellovin [ChB94]. The data on which the projection is based may, therefore, not be typical of Internet sites.

The second error is more serious. The reports of "one incident per day"[1] are on *sites*, and not *hosts*. As such, the projection should not be done to the host level, but to the site level. An approximation to the number of sites is the estimate of the number of *domains* as discussed in Chapter 2. As shown in Table 2.5, the number of domains on the Internet in July, 1995, was around 120,000. This would indicate around 44 million attacks per year in 1995, not 900 million. However, given that this projection is based on data from well-known sites, and that the number of sites is most likely less than the number of domains, this estimate is likely to still be too high. Better estimates of individual site attack activity, however, do not appear to be published, and logically, they are unlikely to appear without a research program in this area.

With its position in the Internet community, the CERT®/CC may be able to enlist the cooperation of representative sites on the Internet in order to gather these data in the future. This will be discussed further in Section 12.3.2.

**12.2.3. Vulnerability Studies** - A third approach to determining the rate of Internet attacks would be to estimate the rate of reporting through a program of attacks on Internet sites. Such a program is called a vulnerability study. The ratio of attacks to reports of these attacks during such a vulnerability study could be used, along with the total reports of attacks, to estimate the total Internet attack activity.

In general, however, such vulnerability studies would not be feasible. It would be against established rules and laws to attack sites without their consent. On the other hand, the reporting rate would likely be influenced if the site were notified of an attack ahead of time, which may make the results invalid. Such attacks have, however, been conducted against one group of hosts on the Internet: those belonging to the Department of Defense (DoD). In fact, because of these DoD studies, it appears the most common method used to estimate the number of attacks on the Internet is to project from vulnerability assessments.

---

[1] Cohen states these are one incident per day, but it should be one *attack* per day.

*12.2.3.1. DISA Vulnerability Studies* - In order to test the vulnerability of a system, several methods could be used, such as examining the software on a system to ensure it is properly configured, or has the correct versions, etc. Sometimes, a vulnerability assessment program involves attempted penetrations of a system. An example of this is the Vulnerability Analysis and Assessment Program of the Defense Information Systems Agency (DISA). Under this program, DISA personnel have attempted to penetrate computer systems at various military service and Defense agency sites via the Internet since the program's inception in 1992 [GAO96:19].

The results of DISA vulnerability assessments from 1992 through 1995 are depicted in Figure 12.1. Over this period, DISA conducted 38,000 attacks. Protection on the systems attacked blocked 35% of these attacks. Of the 24,700 successful attacks (65% of all attacks), almost all of them (23,712, 62.4% of all attacks, 96% of successful attacks) went undetected. Of the relatively small number that were detected (988, 2.6% of all attacks, 4% of successful attacks), three quarters were not reported after detection (721, 1.9% of all attacks, 73% of detected attacks). This means that only 267 of the 38,000 attacks (0.7% of all attacks, 27% of detected attacks) were reported. This is around 1 out of 140 attacks. Stated another way, given an incident that consists of one attack only, the probability the incident would be reported is around 0.7%, based on these data.

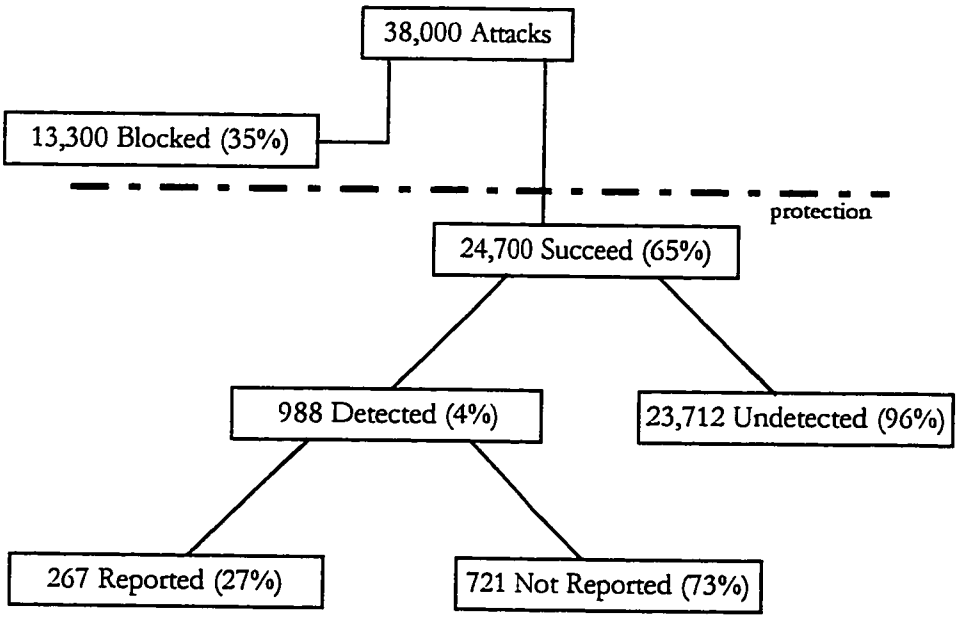


**Figure 12.1. Results of DISA Vulnerability Assessments, 1992 - 1995 [GAO96:20]**

According to the GAO, DISA estimates that DoD computers may have been attacked as many as 250,000 times during 1995 [GAO96:18]. Assuming the DoD represented 10% or less of the

Internet during that year (see Figure 2.6), this would correspond with 2.5 million Internet attacks. Unfortunately, it is not clear where the DISA estimate comes from. The DISA data suggests 1 out of 140 attacks were reported, and the GAO report indicates that around 500 attacks were reported in 1995 [GAO96:21]. This would suggest a lower figure, 70,000, for the number of attacks on DoD systems in 1995, and 700,000 for the number of attacks on the Internet as a whole.

The 500 attacks reported by DISA in 1995, however, actually appear to be *incidents*, and not just *attacks*. This suggests the actual number of attacks may be higher, depending on the number of attacks per incident. This points out the fundamental problem with using vulnerability assessments to estimate total Internet activity: the vulnerability studies show the reporting rate of *attacks*, while the reports from sites are generally of *incidents*. More specifically, it is generally unclear whether a report of attack activity at a site is a report of one attack, or a report of several related attacks (i.e., an incident).

***12.2.3.2. AFIWC Security Posture Studies*** - In a different study during 1995, the "security posture" of selected systems at 15 Air Force bases was evaluated by the Air Force Information Warfare Center (AFIWC), as part of their Computer Security Assistance Program (CSAP) [WhK96:slide19]. The results of their On-Line Survey during January, 1995 are shown in Figure 12.2. Of the 1,248 hosts attacked, 673 (54%) did not allow access. Access was gained at the root level on 291 hosts (23%), and to the account level on 284 hosts (23%). Of the 1,248 attacks, 156 were reported (13%), which means that around 1 out of every 8 attacks resulted in a report.

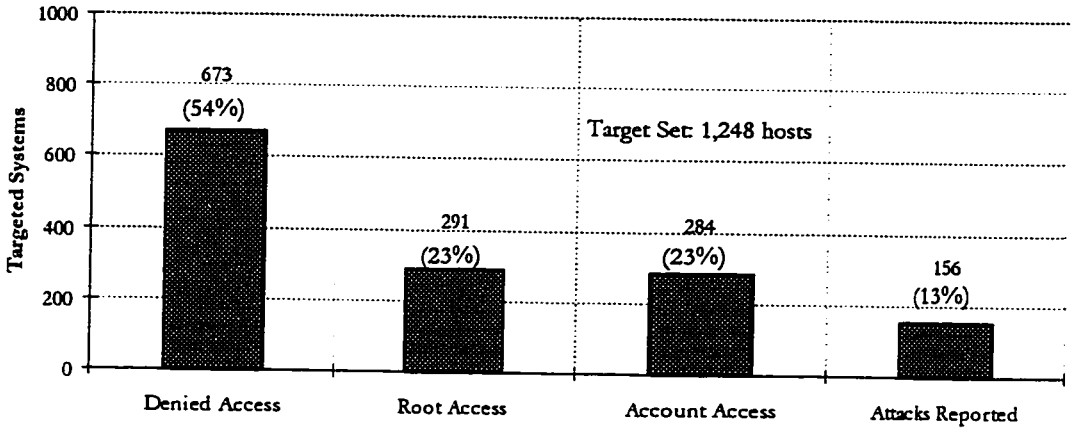


**Figure 12.2. On-Line Survey Results from 1,248 Hosts at 15 USAF Bases, Air Force Information Warfare Center, Jan 95 [WhK96:slide20]**

There are several potential reasons for the substantial difference between the DISA vulnerability assessment (1 out of 140 reported), and the AFWIC On-Line Survey (1 out of 8 reported). First, the AFWIC survey was over a small number of systems that could be similar in security posture,

while the DISA assessment was over a larger, and potentially less homogeneous, number of DoD systems. Second, the DISA assessments were conducted over a four year period (1992 - 1995), while the AFWIC survey was all in the month of January, 1995. The higher probability of an attack being reported in the AFWIC survey may, therefore, reflect improved security during 1995 compared to the other years.

The third possible reason the two surveys differed so greatly was that the methods of attack may have been different. This has the potential to make this difference very large. For example, the more widely-known an attack technique is, the more likely it is to be detected and reported. In addition, some techniques, such as *IP spoofing*, are very difficult to detect.

A fourth reason may be a difference in reporting requirements. If the sites selected for the AFWIC survey had established procedures requiring reports of attacks, then the population they surveyed may have been more likely to report an incident that was detected than the DISA sites. This may account for some of the difference. For example, in the DISA assessment, 1 out of 38 sites detected the DISA attacks, which is a rate nearly four times the rate of reporting. Perhaps this reflects less of a reporting requirement in the DISA study population.

Finally, the large difference between the AWFIC and DISA studies may reflect a difference in the motivation or purpose of the studies. The AFWIC program was instituted to aid individual sites in their security. In fact, the AFWIC team provided technical assistance to the sites attacked in January, 1995, in order to help site administrators improve site security. This effort was reflected in a significant improvement shown at these sites when they were surveyed again in April, 1995. In this later survey, only 2% of attacks were successful at the root level, 10% at the account level, and 25% of the attacks were detected and reported (1 out of 4). On the other hand, the DISA assessment data were used in Congressional Hearings, reported in a GAO Report [GAO96], and reported in the Press. It is conceivable that the greater the perceived threat from Internet attacks reported by DISA, the greater the funding for DISA. This is a potential conflict of interest with respect to the DISA assessments.

If the AFIWC estimate of the rate of reporting (12.5%) were used instead of the DISA rate of reporting (0.7%) for a simple projection of total Internet attacks per year, the value is considerably lower. Assuming the 500 attacks reported by DISA in 1995 is correct, the AFIWC estimate of total Internet attacks per year for 1995 would be

$$500 \ \textit{attacks reported} \times \frac{8 \ \textit{actual attacks}}{\textit{attack reported}} \times \frac{10 \ \textit{Internet sites}}{\textit{DoD Internet site}} \cong 40{,}000 \ \textit{attacks}$$

Again, if the 500 attacks were actually 500 *incidents* made up of multiple attacks, then the number of estimated attacks would be higher.

The conclusion we can draw from these two studies is that the rate of reporting of individual Internet attacks is likely to be somewhere between 1 in 8, and 1 in 140. Stated another way, the probability that a site will report an individual attack is likely to be between approximately 0.7% and 12%. The estimates of the total number of attacks is highly speculative primarily because it is based on an uncertain estimate of the number of incidents. More specifically, an estimate of the total number of Internet attacks projected from vulnerability studies depends on accurate reports of Internet attacks and not incidents. This is information that is generally not available. If the number of attacks is to be estimated from incident reports, then information about the number of attacks per incident would be required. This is discussed in Section 12.3.3.

Table 12.1 summarizes the estimates of total Internet attack activity discussed in this section.

| Source of Estimate | Estimate of Total Attacks per Year |
|---|---|
| Cohen [Coh95:40] | 900 million |
| Cohen (corrected for Internet Domains) | 44 million |
| DISA [GAO96:18] | 2.5 million |
| DISA (corrected for 500 reported attacks) | 700,000 |
| AFIWC (using estimated 500 reported attacks) [WhK96] | 40,000 |

**Table 12.1. Estimates of Total Internet Attacks per Year in 1995**

## 12.3. Estimates of Total Internet *Incident* Activity

Unlike attack activity, reports of Internet incidents are known to exist in various organizations. First, they probably exist at most Internet sites, because most of these sites probably keep records of security incidents involving that site. It is unlikely, however, that these reports would be publicly available for the same reasons that individual attacks would not be reported (discussed in the previous section). Second, some information has been reported publicly. As has been discussed in this dissertation, this information is limited and anecdotal in nature.

Finally, Internet response teams, particularly the CERT®/CC, are known to have reports of incidents (as reported in this dissertation). These reports could be used to estimate total Internet incident activity if an estimate could be made of the percentage of incidents reported to the

CERT®/CC. This could be done in three different ways: 1) a representative site or series of sites could be monitored for incident activity, 2) a representative site or series of sites could be requested to report all incident activity, and 3) estimates of the rate of reporting of *attacks*, and of the number of *attacks per incident*, could be used to estimate the percentage of incidents reported. The results of such estimates could be compared to actual incident reports to estimate the total number of Internet incidents. These three approaches will be discussed in the following three sections.

**12.3.1. Monitoring Sites For Incident Activity** - The first approach to determining total Internet incident activity would be to monitor a site, or several representative sites, for incident activity, and then to use information about the size of the Internet to project this site activity to total Internet incident activity. As with monitoring for individual attacks (discussed in Section 12.2.1), it is likely that such incident monitoring has been conducted at numerous sites, but by personnel at that site only. This is also the type of information that most sites would be reluctant to have become public, and it is unlikely that sites would allow monitoring of their network by outside agencies. It is also technically difficult to monitor incident activity at one site from another site. As such, this does not appear to be a viable option to obtaining sample incident data. In addition, the results from any such monitoring program do not appear to have been published.

**12.3.2. Reports of Incident Activity From Representative Sites** - Instead of monitoring incident activity, a representative site or series of sites could be requested to report all incident activity. As discussed in Chapter 9, Site A *did* report all such activity to the CERT®/CC. Estimates based on Site A activity are discussed in the following pages.

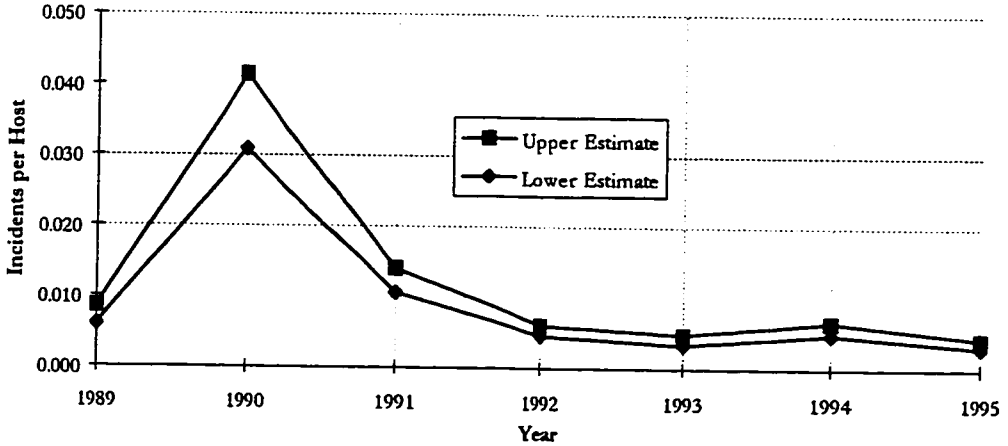


**Figure 12.3. Estimates of the Number of Incidents per Host at Site A**

In Chapter 9, Table 9.1 gives estimates of the number of hosts on the Site A network. Figure 9.1 shows the number of incidents at Site A. These data can be combined to give an estimate of the number of Internet incidents.

Figure 12.3 shows an estimate of the number of incidents per host per year at Site A. The average incidents per host for the years 1992 through 1995 was 0.0048, and the range was 0.0033 to 0.0057. Figure 12.4 shows an estimate of the number of Internet incidents based on these Site A data and the number of Internet hosts (see Chapter 2). Using the total data at Site A, the estimate for 1989 through 1995 is that the total number of Internet incidents was between 46,000 and 62,000. In other words, based on the Site A data, an average of between 1 out of 14, and 1 out of 11 of the actual incidents on the Internet were reported to the CERT®/CC (see Table 12.2).

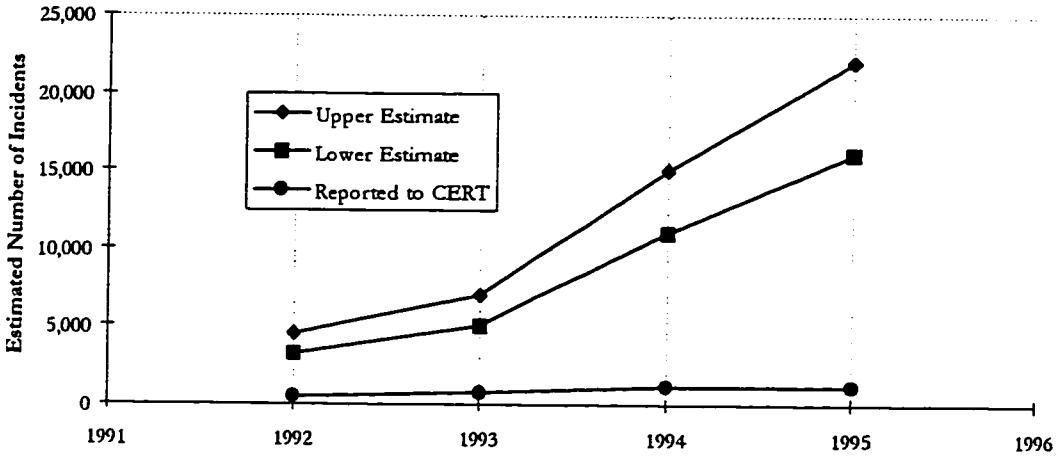


**Figure 12.4. Estimates of the Number of Internet Incidents based on Site A Data**

The number of incidents reported to the CERT®/CC are also plotted in Figure 12.4. This appears to show a decline in the percentage of incidents reported to the CERT®/CC over this period. This is also indicated in Table 12.2, which shows the ratio of the number of total Internet incidents to the number reported to the CERT®/CC over this period. There is, however, a significant difference between the Site A data and all of the data reported to the CERT®/CC which may explain this. These differences are shown in Table 12.3.

| Year | Lower Estimate | Upper Estimate |
|---|---|---|
| 1992 | 1 out of 9 | 1 out of 6 |
| 1993 | 1 out of 9 | 1 out of 7 |
| 1994 | 1 out of 12 | 1 out of 9 |
| 1995 | 1 out of 19 | 1 out of 14 |
| **Average** | 1 out of 14 | 1 out of 11 |

**Table 12.2. Estimate of the Ratio of Total Internet Incidents to Reported Incidents**

| | All Incidents (minus Site A) | | Site A Incidents | |
|---|---|---|---|---|
| | # of Incidents | % of Total | # of Incidents | % of Total |
| Total Incidents | 3,862 | 100.0% | 437 | 100.0% |
| Root break-ins | 1,159 | 30.0% | 30 | 6.9% |
| Account break-ins | 973 | 25.2% | 61 | 14.0% |
| Access attempts | 1,297 | 33.6% | 321 | 73.5% |
| Unauthorized Use Incidents | 433 | 11.2% | 25 | 5.7% |

**Table 12.3. All CERT®/CC Incidents Compared To Incidents at Site A (using a two-factor ANOVA, the occurrences for all incidents (minus Site A) and Site A incidents were determined to be statistically different [p = 0.011])**

If we make the assumption that Site A is representative of sites on the Internet, Table 12.3 may indicate that the more serious an incident is, the more likely it is to be reported to the CERT®/CC. This was evident in all three levels of access incidents. In the record of all incidents (minus Site A), the number of root break-ins exceeded the number of account break-ins (1,159 root break-ins compared to 973 account break-ins). At Site A, however, the number of root break-ins was only half that of account break-ins (30 root break-ins compared to 61 account break-ins). In terms of percentage, access attempts at Site A were reported at more than twice the rate of all incidents (73.5% access attempts at Site A, compared to 33.6% overall). This may account for the decline in the ratio of reports to total incidents that was indicated in Figure 12.4. In other words, the CERT®/CC may be receiving relatively less reports about attempts, but not necessarily less reports of successful attacks over time.

Because of its apparent diligence in reporting incidents to the CERT®/CC, Site A may report root break-ins to the CERT®/CC at a rate greater than that of other sites. Let us assume, however, that the rate of reporting root break-ins was approximately the same. Furthermore, let us assume the other levels were underreported to the extent that they actually took place in the approximate percentages reported by Site A. With these assumptions in mind, if all sites were as diligent in reporting as Site A, in terms of percentages, the approximate number of incidents that would have been 7% root break-ins, 14% account break-ins, 74% access attempts, and 5% unauthorized use incidents. This would correspond to around 1,200 root break-ins, 2,400 account break-ins, 12,700 access attempts, and 900 unauthorized access incidents, for a total of approximately 17,200 incidents. That would be around four times the 4,299 incidents actually reported to the CERT®/CC over the period of this research.

The reporting of 1 out of 4 incidents is a rate higher than the values given in Table 12.2. Table 12.4 shows that none of the estimates based on the Site A data falls within the ranges of Table 12.2.

The most suspicious assumption of Table 12.4 is the assumption that all root break-ins were reported. This is likely to be inaccurate because 1) not all root break-ins may be detected, either at Site A, or at all sites, and 2) not all incidents detected involving root break-ins may be reported. The data of Table 12.4 were, therefore, not considered to be a good estimate.

| Access | Estimated Incidents for 1989-95 | Estimated Reporting Rate |
|---|---|---|
| root break-ins | 1,200 | 1 out of 1 |
| account break-ins | 2,400 | 1 out of 2.5 |
| access attempts | 12,700 | 1 out of 8 |
| unauthorized use incidents | 900 | 1 out of 2 |
| **All Incidents** | 17,200 | 1 out of 4 |

**Table 12.4. Estimate of Incident Reporting Rates from Site A Data, Assuming All Root Break-ins Reported**

As discussed in Section 12.2.2, with its position in the Internet community, the CERT®/CC may be able to enlist the cooperation of representative sites on the Internet in order to generate these data in the future. The CERT®/CC is in a unique position within the Internet community. As such, the CERT®/CC should lead the development and implement a program to better estimate total Internet incident activity. Such a program should involve the voluntary reporting of all incident activity at representative Internet sites and should include coordination and/or participation from other response teams and related organizations, such as DISA and AFIWC. This is discussed in Chapter 14.

**12.3.3. Estimates of Attack Reporting Rate and Attacks per Incident** - Estimates of the rate of reporting of attacks, and of the number of attacks per incident, could be used to estimate the total number of Internet incidents as follows:

$$N_t \cong \frac{N_r}{P(I)} \cong \frac{N_r}{1 - [1 - P(A)]^{\alpha}} \qquad (12.1)$$

where $N_t$ = the total number of Internet incidents

$N_r$ = the number of Internet incidents reported

$P(I)$ = the probability (percentage) that an *incident* will be reported

$P(A)$ = the probability that an *attack* will be reported

$\alpha$ = the number of attacks per incident

*12.3.3.1. Estimates of Attack Reporting Rate* - Section 12.2.3 gave two estimates of the probability of an attack being reported [*P(A)*]. The first, from DISA vulnerability assessments, was 1 out of 140 (0.7%). The second, from the AFIWC survey, was 1 out of 8 (12.5%). These estimates will be used as an upper and lower estimate of the probability of an attack being reported.

*12.3.3.2. Estimates of Attacks per Incident Using All CERT®/CC Incidents* - The CERT®/CC data gives some limits on an estimate of the number of attacks per incident ($\alpha$). For a lower estimate, we could use the number of sites per incident. In this case, we assume that each site identified in the incident was attacked at least one time during the incident. Figure 12.5 shows the average number of sites per incident for the CERT®/CC incidents in each year of this research. Throughout this period, this average was around six sites per incident. Because of the large number of incidents in 1994 and 1995, the overall average was higher, at 6.54 sites per incident. We can then figure the lower limit of the attacks per incident as follows:

$$\frac{1\ attack}{site} \times \frac{6.54\ sites}{incident} \equiv \frac{6.54\ attacks}{incident}$$

If only the data from 1995 were used, the lower estimate would be 7.3 attacks per incident.

Even though this estimate is intended to be the *lower* estimate, it would be appropriate to round this figure up to 10. This is because, even though this estimate comes from incidents that were reported, there is most likely some *attacks* in each incident that went unreported..

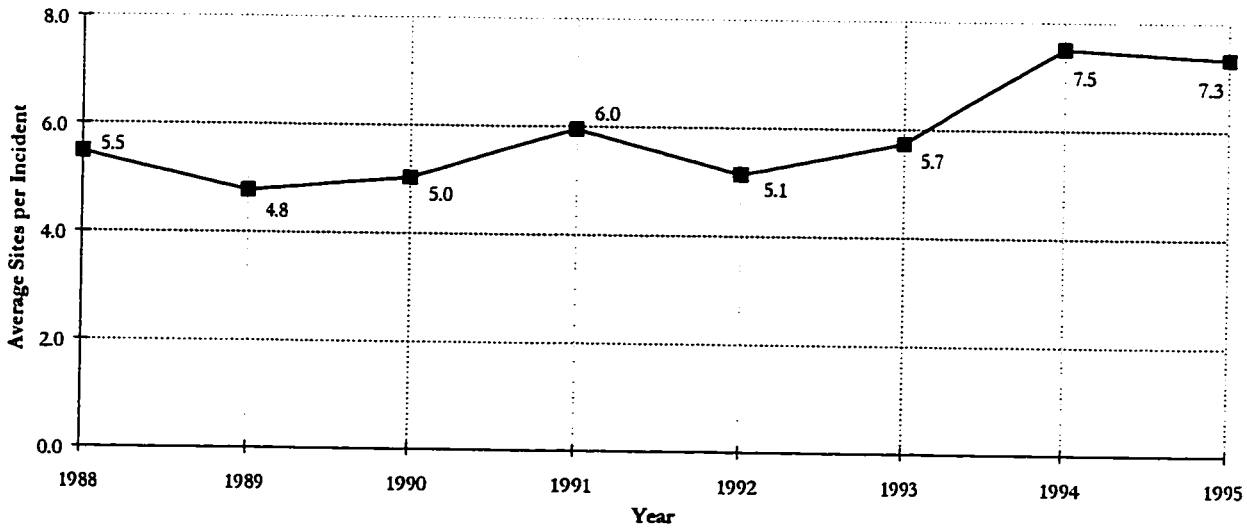


**Figure 12.5. Average Sites per Incident by Year**

Establishing an estimate of the upper limit of attacks per incident is more difficult. One way would be to assume *each* site was attacked once a day. Then, we could use the average duration of incidents in the entire CERT®/CC data set to make following estimate:

$$\frac{1\ attack}{day} \times \frac{165\ days}{site} \times \frac{654\ sites}{incident} \cong \frac{108\ attacks}{incident}$$

An attacker is capable of making multiple attacks on the same day. In addition, there could be multiple attackers in an incident. For example, a 1996 GAO report describes an incident at Rome Laboratory, New York [GAO96:22] involving two attackers. One attacker was from the U.K. and was arrested in May, 1994, and the other attacker was unidentified. According to the GAO report, these attackers made more than 150 intrusions during March and April, 1994. This is an average of 2.5 attacks per day. Using this average, the estimate of attacks per incident increases as follows:

$$\frac{2.5\ attacks}{day} \times \frac{165\ days}{site} \times \frac{654\ sites}{incident} \cong \frac{270\ attacks}{incident}$$

This particular incident was also recorded in the CERT®/CC records. It involved the use of sniffers and over 1,500 sites.

On any particular day, an attacker is capable of perhaps dozens of attacks.[2] They would have a tendency, however, to perform less attacks if they are successful. For example, an attacker would tend to take time exploring a computer after a successful attack. As stated earlier, there could also be multiple attackers. On the other hand, it would be unlikely that each attacker would be active on every day of an incident, and that all of the attackers would be equally active. Let us assume the following: 1) each attacker is capable, on average, of 5 attacks per day, 2) there were, on average, 3 attackers per incident, 3) each attacker was active, on average, 3 days each week, and 4) attackers were active half of the days the incident was open.

The first assumption was made by assuming that each attacker could perform a dozen or more attacks during a day, but would perform less if one or more attacks was successful. Regarding the second assumption, as was noted in Chapter 9, the CERT®/CC incident records contain very little information about the identity or numbers of attackers. Assuming that each incident had at least one attacker, the CERT®/CC records would appear to indicate the average number of attackers was a little more than one. Here we will assume the average is three attackers. The third assumption above is based upon a judgment that an attacker is not likely to be active every day. The last assumption comes from experience with the actual incidents in the CERT®/CC records. These records show that attacks came primarily during the early part of an incident. Part of the reason for this is that the CERT®/CC records were generally held open past the bulk of attacks in order to

[2] This is an estimate based on discussions with several people experienced in the field, such as LtCol Gregory B. White, US Air Force Academy, Department of Computer Science.

perform investigations, and administrative actions. In addition, as an incident progressed, sites took defensive measures which generally prevented some attacks.

Using these assumptions, the approximation for the number of attacks per incident is:

$$\frac{5\ attacks}{day \times attacker} \times \frac{3\ attackers}{site} \times \frac{3\ active\ days}{each\ 7\ days} \times \frac{1\ active\ day}{2\ total\ days} \times 16.5\ days \times \frac{6.54\ sites}{incident} \cong \frac{350\ attacks}{incident}$$

It should be noted that this estimate is sensitive to the assumed values. For example, if the average number of attackers involved in each incident is 5 instead of 3, the estimate of attackers per incident is nearly doubled to around 600.

Another way the upper limit to the number of attacks per incident could be estimated, is to give some consideration to the types of attacks. We would expect a similar answer, because the same data would be used, but it is interesting to note the distribution of data as shown in Table 12.5. The values in this table were determined by a judgment based on experience with the CERT®/CC records. Using the estimates shown in Table 12.5, this results in an estimate of the number of attacks per incident as being around 1,000. Again, this estimate is sensitive to the estimates of the other parameters. For example, if the ratio of active time to duration (active/duration) for root break-ins is increased from 0.50 to 0.75, this results in the overall estimate increasing to over 1,500 attacks per incident.

| | Average of data | | Incidents | | Estimates | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Type | Sites | Duration | Number | Percent | # of attackers | Active/ week | Active/ duration | Attacks/ day/attacker | Attacks/ incident |
| Root Break-in | 13.1 | 29.4 | 1,189 | 27.7% | 5 | 5 | 0.50 | 5 | 3,439 |
| Account Break-in | 5.96 | 16.6 | 1,034 | 24.1% | 3 | 3 | 0.50 | 4 | 254 |
| Access attempt | 2.54 | 9.48 | 1,618 | 37.6% | 2 | 2 | 0.25 | 10 | 34 |
| Denial-of-service | 3.68 | 7.1 | 104 | 2.4% | 2 | 4 | 0.25 | 3 | 22 |
| Corruption | 2.72 | 7.37 | 135 | 3.1% | 3 | 3 | 0.25 | 3 | 19 |
| Disclosure | 6.84 | 7.91 | 219 | 5.1% | 10 | 3 | 0.50 | 3 | 348 |
| Averages: | 6.54 | 16.5 | Weighted Averages: | | 3.5 | 3.2 | 0.39 | 6.4 | 1,044 |

**Table 12.5. Example Weighted Estimates of Attacks per Incident**

Using this last estimate (Table 12.5), we have an "order of magnitude" estimate of the number of attacks per incident as being between 10 and 1,000. My experience with the CERT®/CC records suggests that 100 attacks per incident might be a reasonable estimate of the mean.

The number of incidents reported to the CERT®/CC during 1995 was approximately 1,200. Based on the number of attacks per incident being between 10 and 1,000, we could use Equation 12.1 to estimate the number of *incidents* on the Internet. This showed that if we assume the probability of reporting an attack was 0.7% (DISA estimate), the estimated number of incidents per

year in 1995 is estimated to be between 1,200 and 17,350. This would correspond to an estimated number of *attacks* between 12,000 and 17.4 million. If we assume the probability of reporting an attack was 12.5% (AFIWC estimate), the estimated number of incidents per year in 1995 is estimated to be between 1,200 and 1,630. This would correspond to an estimated number of *attacks* between 12,000 and 1.6 million.

#### *12.3.3.3. Estimates of Attacks per Incident Using CERT®/CC Incidents by Type -*

In the previous section, the number of attacks per incident was estimated using all the CERT®/CC incidents together. As was discussed in Section 12.3.2, however, the likelihood that an Internet incident will be reported to the CERT®/CC is greater the more severe the incident. Chapter 7 also discussed measures of severity which included the level of access or type of unauthorized use, number of sites involved, duration, and number of messages to and from the CERT®/CC. These measures of severity give some indication of the number of attacks per incident. If estimates of the number of attacks per incident were made for each of the six categories of CERT®/CC incidents (see Table 12.6) were made, perhaps this would yield a better estimate of the upper limit of attacks per incident. This could be done with the following formula:

$$\frac{attacks}{incident} \equiv \frac{sites}{incident} \times days \times \frac{attacks}{day \times attacker} \times \frac{attackers}{site} \times \frac{active\ days}{each\ 7\ days} \times \frac{active\ days}{total\ days} \qquad (12.2)$$

| | Assumed Values | | | |
|---|---|---|---|---|
| Type | # of attackers | Active/ week | Active/ duration | Attacks/ day/attacker |
| Root Break-in | 5 | 5 | 0.50 | 5 |
| Account Break-in | 3 | 3 | 0.50 | 4 |
| Access attempt | 2 | 2 | 0.25 | 10 |
| Denial-of-service | 2 | 4 | 0.25 | 3 |
| Corruption | 3 | 3 | 0.25 | 3 |
| Disclosure | 10 | 3 | 0.50 | 3 |
| Averages: | 3.5 | 3.2 | 0.39 | 6.4 |

**Table 12.6. Assumed Values for an Estimate of the Number of Attacks for Each CERT®/CC Incident**

As noted in the previous section, the estimate of the number of attacks is very sensitive to the estimates of the other parameters. The estimated values of the parameters were as shown in Table 12.6 (taken from Table 12.5). Using these assumed values, Equation 12.2 was used to estimate the number of attacks for each of the incidents in the CERT®/CC data. The results are shown in Table 12.7, which shows an average number of attacks in an incident as being between 7 and 3,000. This is a wider range than was estimate in the previous section. Notice that the range depends strongly

on the type of incident, with a high range of between 13 and 10,220 for root break-ins, and a low range of between 3 and 24 for denial-of-service attacks.

The estimates in Table 12.7 can be used to estimate the total number of Internet incidents. In order to do this, the probability of an individual attack being reported must be assumed. Most likely, this probability is dependent on the severity of an incident. For example, a site administrator may not be inclined to report to the CERT®/CC attacks that were unsuccessful. On the other hand, this same site administrator might be highly likely to report an attack that resulted in a root break-in. Unfortunately, the only information available about the probability an attack will be reported are for overall averages and not for individual types of attack. These were presented in Section 12.2.3 (the DISA assessment of the probability of an individual attack being reported as 1/140 (0.7%), and the AFIWC study, with the probability of being reported as 1/8 (12.5%)).

| | Estimate Average Attacks/Incident | |
|---|---|---|
| Type | Lower Estimate | Upper Estimate |
| Root Break-in | 13 | 10,220 |
| Account Break-in | 6 | 377 |
| Access attempt | 4 | 31 |
| Denial-of-service | 3 | 24 |
| Corruption | 3 | 38 |
| Disclosure | 7 | 669 |
| Averages: | 7 | 2,967 |

**Table 12.7. Estimate Average Attacks/Incident Derived From Each CERT®/CC Incident Using Assumed Parameters**

We do, however, have information from Site A that may indicate a difference in the rate of reporting for each type of incident. Such an adjustment is given in Table 12.8. The middle column of this table shows the ratio of the percentage of all incidents in a type to the percentage of incidents in that type at Site A. This ratio was used to adjust the probability of report as shown.

| | % of Total | | | Probability of Report | |
|---|---|---|---|---|---|
| Type | All Incidents | Site A Incidents | Ratio | Low Estimate | High Estimate |
| Total Incidents | 100.0% | 100.0% | | 0.71% | 12.50% |
| Root break-ins | 27.7% | 6.9% | 4.0 | 2.87% | 50.18% |
| Account break-ins | 24.1% | 14.0% | 1.7 | 1.23% | 21.52% |
| Access attempts | 37.6% | 73.5% | 0.5 | 0.37% | 6.39% |
| Denial-of-Service Incidents | 5.1% | 3.0% | 1.7 | 1.21% | 21.25% |
| Corruption Incidents | 2.4% | 1.4% | 1.7 | 1.22% | 21.43% |
| Disclosure Incidents | 3.1% | 1.4% | 2.2 | 1.58% | 27.68% |

**Table 12.8. Adjustments to the Probability of Report, Based on Site A Information**

In Table 12.8, the low estimates of the probability of report were based on the DISA assessments, and the high estimates of the probability of report were based on the AFIWC survey.[3]

| | Average Probability of Report | | Estimated Total of Internet Incidents | |
|---|---|---|---|---|
| Type | Low Estimate | High Estimate | Low Estimate | High Estimate |
| Total Incidents | 48.0% | 83.6% | 6,597 | 16,603 |
| Root break-ins | 86.2% | 100.0% | 1,189 | 1,408 |
| Account break-ins | 54.4% | 95.6% | 1,096 | 2,137 |
| Access attempts | 14.6% | 62.3% | 3,745 | 12,099 |
| Denial-of-Service Incidents | 45.0% | 76.7% | 161 | 248 |
| Corruption Incidents | 45.8% | 81.6% | 186 | 312 |
| Disclosure incidents | 59.9% | 99.6% | 220 | 398 |

**Table 12.9. Estimates of the Average Percentage of Reports of Incidents and the Total Number of Internet Incidents Based on an AFWIC Estimated Average Probability of Report of Attack**

The results of using the higher estimated probabilities are given in Table 12.9. Overall, this process estimates the total number of Internet incidents for the period of this research to be between 6,600 and 16,600, and the total number of attacks to be between 53,000 and 133,000. Recalling that the total number of incidents in the CERT®/CC records was 4,299, experience with the CERT®/CC records seems to indicate these estimates are probably too low. Evidence for this was seen particularly in the fact that there were generally far more sites involved in an incident than sites that reported the incident.

| | Average Probability of Report | |
|---|---|---|
| Type | Low Estimate | High Estimate |
| Total Incidents | 1 out of 2.1 | 1 out of 1.2 |
| Root break-ins | 1 out of 1.2 | 1 out of 1.0 |
| Account break-ins | 1 out of 1.8 | 1 out of 1.1 |
| Access attempts | 1 out of 6.8 | 1 out of 1.6 |
| Denial-of-Service Incidents | 1 out of 2.2 | 1 out of 1.3 |
| Corruption Incidents | 1 out of 2.2 | 1 out of 1.2 |
| Disclosure incidents | 1 out of 1.7 | 1 out of 1.0 |

**Table 12.10. Estimates of the Average Probability of Report of an Incident Based on an AFWIC Estimated Average Probability of Report of Attack**

[3] These adjusted probabilities were used for generating the data described in the remaining part of this section. The same data were also generated without these probability adjustments. In the overall numbers, these adjustments made little difference. On the other hand, there were significant differences in the individual types. For example, when the probabilities were adjusted, the highest estimate of the number of root break-ins dropped from 55,000 to 14,000, while the highest estimate of the number of access attempts nearly doubled, from 105,000 to 202,000. These estimates appeared to make more sense when the adjusted probabilities were used.

This can be seen more clearly in Table 12.10 which shows the average probability of report in a different form. These probabilities suggest that most incidents were reported to the CERT®/CC during the period of this research, particularly root and account break-ins. Again, experience with the CERT®/CC records indicates this was probably not the case.

| | Average Probability of Report | | Estimated Total of Internet Incidents | |
|---|---|---|---|---|
| Type | Low Estimate | High Estimate | Low Estimate | High Estimate |
| Total Incidents | 7.4% | 46.3% | 59,528 | 260,000 |
| Root break-ins | 18.2% | 91.1% | 1,409 | 13,944 |
| Account break-ins | 6.0% | 54.4% | 4,497 | 30,515 |
| Access attempts | 0.9% | 10.8% | 49,402 | 201,536 |
| Denial-of-Service Incidents | 4.1% | 16.9% | 1,813 | 3,779 |
| Corruption Incidents | 3.3% | 17.3% | 1,847 | 4,732 |
| Disclosure incidents | 8.7% | 58.5% | 562 | 5,493 |

**Table 12.11. Estimates of the Average Probability of Report of an Incident and the Total Number of Internet Incidents Based on an DISA Estimated Average Probability of Report of Attack**

The results of using the lower estimated probabilities are given in Table 12.11. Overall, this process estimates the total number of Internet incidents to be between around 60,000 and 260,000, and the total number of attacks to be between 8.4 million and 36.4 million.

The lower estimate of the average probability of report in Table 12.12 (1 out of 13) is within the average range estimate from the Site A (see Table 12.2). The high estimate still seems unrealistic compared to CERT®/CC records. This may indicate that the number of sites was a poor choice for a lower limit of attacks per incident. On the other hand, this was a realistic choice because, if a site was identified as being involved in an incident, it was most likely attacked. The error is probably that, most likely, on average, sites were attacked more than once during an incident.

| | Average Probability of Report | |
|---|---|---|
| Type | Low Estimate | High Estimate |
| Total Incidents | 1 out of 13 | 1 out of 2.2 |
| Root break-ins | 1 out of 5.5 | 1 out of 1.1 |
| Account break-ins | 1 out of 17 | 1 out of 1.8 |
| Access attempts | 1 out of 108 | 1 out of 9.3 |
| Denial-of-Service Incidents | 1 out of 31 | 1 out of 5.8 |
| Corruption Incidents | 1 out of 12 | 1 out of 1.7 |
| Disclosure incidents | 1 out of 25 | 1 out of 5.9 |

**Table 12.12. Estimates of the Average Probability of Report of an Incident Based on an DISA Estimated Average Probability of Report of Attack**

**12.3.4. Summary of Incident Estimates** - Table 12.13 summarizes the estimates of total Internet incident activity made in this section. These estimates are for one year in 1995.

| Estimates of Total Internet Incidents per Year in 1995 | | |
|---|---|---|
| **Source** | **Low Estimate** | **High Estimate** |
| Based on Incidents per Host estimates at Site A | 16,800 | 22,800 |
| Based on attacks per incident 10 to 1,000, and DISA probability | 1,200 | 17,350 |
| Based on attacks per incident 10 to 1,000, and AFIWC probability | 1,200 | 1,630 |
| Based on DISA probability (Table 12.11) | 2,500 | 15,800 |
| Based on AFIWC probability (Table 12.9) | 1,400 | 2,400 |

**Table 12.13. Summary of Estimates of Total Internet Incident Activity**

## 12.4. Severe and Above Average Incidents

The 22 incidents identified in Chapter 10 as being the most severe in the CERT®/CC records were given the same analysis as was done for all incidents in the last section. Using the DISA probability of reporting an attack, the probability of any incident meeting the Chapter 10 criteria *not* being reported to the CERT®/CC was between 0% and 4%. Using the AFIWC probability of reporting an attack, the probability of any incident meeting Chapter 10 criteria *not* being reported to the CERT®/CC was essentially zero. This confirms the impression the reports themselves give: that it is hard to conceive that a severe incident would not be reported to the CERT®/CC.

There were 394 incidents in the CERT®/CC records (9.2%) that were above average both in terms of duration (above 16.5 days) and number of sites (above 6.5). When these incidents were isolated and analyzed in the same manner as the previous section, it yielded the results of Table 12.14. If we assume the DISA probability of report, then a minimum of around 1 out of 2.6 of the above average incidents were reported to the CERT®/CC (and nearly all of them may have been reported). If we assume the AFIWC probability, then it was estimated that less than 4% of these incidents were not reported to the CERT®/CC (and nearly all of them may have been reported).

| | **Probability of Report ~ 1/140** | | **Probability of Report ~ 1/8** | |
|---|---|---|---|---|
| | **Low Estimate** | **High Estimate** | **Low Estimate** | **High Estimate** |
| Probability of Incident Report | 38.5% | 99.3% | 96.5% | 100.0% |
| Rate of Incident Reports | 1 out of 2.60 | 1 out of 1.01 | 1 out of 1.03 | 1 out of 1.00 |
| Total Internet Incidents | 397 | 1,866 | 394 | 415 |

**Table 12.14. Estimates of the Probability of Incident Report, Rate of Incident Reports, and Total Internet incidents for Incidents with Above Average Duration and Number of Sites**

Estimates of attacks per incident, and therefore, estimates of total Internet incident activity, could be improved with better information about the average number of attackers per incident, and their typical activity. Estimates of average number of attackers per incident, and their typical activity, should be made by personnel from DISA, AFIWC, CERT®/CC and other response teams, in order to improve estimates of total Internet incident activity. This is discussed in Chapter 14.

### 12.5. Estimated Number of Internet Denial-of-service Incidents

Tables 12.9 and 12.11 estimate that there were between approximately 160 and 3,800 denial-of-service incidents on the Internet between 1989 and 1995. There was, however, only one denial-of-service incident in the CERT®/CC records that was in the 394 above average incidents identified in the previous section. This incident involved 21 sites.

There is general acknowledgment that the Internet is relatively defenseless against denial-of-service attacks [GaS96:759]. The small numbers of denial-of-service incidents, and their relatively small size, however, do not completely confirm this vulnerability. On the one hand, the records indicate that denial-of-service vulnerabilities have not been mitigated over this period. The same methods of attack used in the early incidents appear to be successful in the later incidents also. All of the incidents, however, were localized and small in scale.

The CERT®/CC record of denial-of-service incidents show no large-scale incidents whatsoever. The only large-scale denial-of-service incident known to have occurred on the Internet remains the Internet Worm of 1988. This is an interesting finding. The CERT®/CC was established in response to a large-scale denial-of-service attack, and yet, no other large-scale denial-of-service attack is known to have occurred.

CERT®/CC records give no indication of why large-scale denial-of-service attacks do not occur on the Internet. Either potential attackers have not had enough motivation, or the Internet is not vulnerable to large-scale denial-of-service attack.[4]

### 12.6. Summary of the Estimates of Total Internet Incident Activity

Since attacks make up incidents, total Internet security *activity* could be measured by either the total Internet *attack* activity or the total Internet *incident* activity. In order to estimate the number of *attacks*, some sample of Internet activity is required. Vulnerability studies by Defense Department agencies can be used for such an estimate. A vulnerability analysis by the Defense Information Systems Agency (DISA) showed that the probability of an individual attack being reported was

[4] Conversations with Dr. Thomas A. Longstaff, CERT®/CC, indicate that denial-of-service incidents during 1996 and 1997 may indicate increases in frequency and severity. These were not, however, evident in the period of this research.

around 1 out of 140 (0.7%). In a different study, the Air Force Information Warfare Center (AFIWC) estimated this probability to be 1 out of 8 (12.5%). Table 12.15 summarizes the estimates of total Internet attack activity based on these studies.

| Source of Estimate | Estimate of Total Attacks per Year |
|---|---|
| DISA [GAO96:18] | 2.5 million |
| DISA (corrected for 500 reported attacks) | 700,000 |
| AFIWC (using estimated 500 reported attacks) [WhK96] | 40,000 |

**Table 12.15. Estimates of Total Internet Attacks per Year in 1995**

Site A was used to estimate total Internet incident activity based on estimates of incidents per host at this site. This was the only site reporting all incident activity to the CERT®/CC. Because of its position in the Internet community, the CERT®/CC may be able to enlist the cooperation of other representative sites on the Internet in order to generate these data in the future. As such, the CERT®/CC should lead the development and implementation of a program to better estimate total Internet incident activity. Such a program should involve the voluntary reporting of all incident activity at representative Internet sites and should include coordination and/or participation from other response teams and related organizations, such as DISA and AFIWC.

Estimates of the rate of reporting of attacks, and of the number of attacks per incident, could be used to estimate the total number of Internet incidents as follows:

$$N_t \cong \frac{N_r}{P(I)} \cong \frac{N_r}{1 - [1 - P(A)]^{\alpha}} \qquad (12.1)$$

where $N_t$ = the total number of Internet incidents

$N_r$ = the number of Internet incidents reported

$P(I)$ = the probability (percentage) that an *incident* will be reported

$P(A)$ = the probability that an *attack* will be reported

$\alpha$ = the number of attacks per incident

The DISA and AFIWC studies gave low and high estimates of the probability of an attack being reported [$P(A)$]. The number of attacks per incident was estimated to be between 10 and 1,000 when all CERT®/CC data was considered together. Better estimates were obtained when the types

of incidents were considered separately. Table 12.16 summarizes the estimates of total Internet incident activity made by estimating attacks per incident, or from Site A projections. These estimates are for one year in 1995.

| Estimates of Total Internet Incidents per Year in 1995 | | |
|---|---|---|
| **Source** | **Low Estimate** | **High Estimate** |
| Based on Incidents per Host estimates at Site A | 16,800 | 22,800 |
| Based on attacks per incident 10 to 1,000, and DISA probability | 1,200 | 17,350 |
| Based on attacks per incident 10 to 1,000, and AFIWC probability | 1,200 | 1,630 |
| Based on DISA probability (Table 12.11) | 2,500 | 15,800 |
| Based on AFIWC probability (Table 12.9) | 1,400 | 2,400 |

**Table 12.16. Summary of Estimates of Total Internet Incident Activity**

Using the DISA probability of reporting an attack, the probability of any severe incident meeting the Chapter 10 criteria *not* being reported to the CERT®/CC was between 0% and 4%. Using the AFIWC probability of reporting an attack, the probability of any severe incident meeting the Chapter 10 criteria *not* being reported to the CERT®/CC was essentially zero. This confirms the impression the reports themselves give: that it is hard to conceive that a severe incident would not be reported to the CERT®/CC.

There were 394 incidents in the CERT®/CC records (9.2%) that were above average both in terms of duration (above 16.5 days) and in terms of the number of sites (above 6.5). When these incidents were isolated and analyzed, it showed that if we assume the DISA probability of report, then a minimum of around 1 out of 2.6 of the above average incidents were reported to the CERT®/CC (and nearly all of them may have been reported). If we assume the AFIWC probability, then it was estimated that less than 4% of these incidents were not reported to the CERT®/CC (and nearly all of them may have been reported).

Estimates of attacks per incident, and therefore, estimates of total Internet incident activity, could be improved with better information about the average number of attackers per incident, and their typical activity. Estimates of average number of attackers per incident, and their typical activity, should be made by personnel from DISA, AFIWC, CERT®/CC and other response teams, in order to improve estimates of total Internet incident activity.

*Chapter 13*

# The Utility of the Taxonomy of Computer and Network Attacks

In Chapter 6, a taxonomy was developed for classifying computer and network attacks. This taxonomy was used in subsequent chapters to classify and analyze the Internet incidents reported to the CERT®/CC from 1998 to 1995. This chapter presents a brief critique of the taxonomy based on this experience. This is followed by a discussion of how incidents can be classified by using this taxonomy and other data from the incidents.

## 13.1. Review of the Characteristics of Satisfactory Taxonomies

A taxonomy is an approximation of reality that is used to gain greater understanding in a field of study. Because it is an approximation, it will fall short in some characteristics. This may be particularly the case when the characteristics of the data being classified are imprecise and uncertain, as was the data for this study. Nevertheless, classification is an important and necessary process for systematic study.

As presented in Chapter 6, a taxonomy should have classification categories with the following characteristics [Amo94:34]:

1) mutually exclusive - classifying in one category excludes all others because categories do not overlap,
2) exhaustive - taken together, the categories include all possibilities,
3) unambiguous - clear and precise so that classification is not uncertain, regardless of who is classifying,
4) repeatable - repeated applications result in the same classification, regardless of who is classifying,
5) accepted - logical and intuitive so that they could become generally approved,
6) useful - can be used to gain insight into the field of inquiry.

These characteristics can be used to evaluate possible taxonomies. This will be done in the remaining sections of this chapter.

## 13.2. Evaluation of the taxonomy relative to the taxonomy criteria

The following sections compare the taxonomy to each of the desired characteristics using the experience of applying the taxonomy in this research. It should be emphasized, however, that there is a difference between classifying an *incident* and an *attack*. The CERT®/CC records were of *incidents*, which were composed of numerous *attacks* (a distinction made in Chapters 1, 6, 7 and 12). This taxonomy only produces a single classification for single attacks. The remainder of this section evaluates the taxonomy for classifying attacks. Section 13.3 discusses using this taxonomy, along with other criteria, to classify an incident. This is more difficult since an incident can be made up of multiple attacks.

**13.2.1. Categories that are Mutually Exclusive** - The categories of a taxonomy should be such that classification into one category excludes classification into all others, because the taxonomy categories do not overlap. Care was taken in developing the categories of this taxonomy to ensure they were mutually exclusive (see Figure 6.9). In general, in applying the taxonomy for this research, there were few instances when a single classification was not directly determined.

There were, however, two problems noted with respect to the categories being mutually exclusive. The first problem was that sometimes, when there was limited information, the determination of a single category was difficult. The second problem was that sometimes, one attack could theoretically be in two categories.

An example of the first problem came in the vulnerability categories. Generally, the CERT®/CC records reported vulnerabilities in terms of software processes or programs. An example is the keyword *sendmail.* This key word indicated a vulnerability in sendmail was exploited, but it did not indicate whether this vulnerability resulted from an implementation, design or configuration error. More information would generally point to one category, although sometimes there could be a disagreement when there was not general acceptance of the definition of terms. This problem will be discussed in Section 13.2.5.

The second problem noted with the categories being mutually exclusive was that one attack could theoretically be classified into two categories. This was particularly the case when differentiating between results and objectives. In these cases, the problem was that one attack could have multiple results, or accomplish multiple objectives. This was generally not a problem for the application of the taxonomy for this research, but then there were also few data in the CERT®/CC records about results and objectives (see Chapters 7 and 8).

An example of a possible problem with objectives not being mutually exclusive might be in the destruction of files by one company on a rival company's computer system. In this case, *damage* was caused, and *financial gain* may be achieved (two possible objectives). On closer examination, however, the categories are found to be mutually exclusive. In this example, the objective should be classified as being financial gain. The damage to files should be classified in the *corruption of files* category of *Results*, which leads the attacker to the *objective* of *financial gain.*

The greatest potential classification problem was with denial-of-service attacks. For example, if selected files in a user's account are deleted, then an argument could be made that both *corruption of files* and *denial-of-service* resulted (two results). In the application of the taxonomy for this research, an incident like this was classified in the corruption of information category. On the other hand, if

the only files deleted were systems programs or files, such as the system's password file, the system's *login* program, or a user's account, then this incident was classified in the denial-of-service category.

A more serious problem occurs if an attacker deleted *all* files on a system. In this case, there are clearly two results: destruction of data files (corruption of information), and destruction of system files (denial-of-service). Even knowing the attacker's motivation may not help to classify such an attack. The attacker's motivation may include *both* results ("I'm going to get the company that fired me by destroying all their records and shutting down their system so nobody can use it....."). This ambiguity concerning denial-of-service results was not a problem for this research, because it was generally obvious what category the attack should be classified in. On the other hand, the experience with this research showed that it could be a problem. This problem could be mitigated with more information, which would make the classifications easier.

One final example of possible problems with categories being mutually exclusive was seen in the tools category (see Figure 6.9). With the exception of the data tap category, each of the tool categories may contain the other tool categories within them. For example, toolkits contain scripts, programs, and sometimes autonomous agents. So when a toolkit is used, the scripts and programs category is also included. User commands also must be used for the initiation of scripts, programs, autonomous agents, toolkits and distributed tools. In other words, there is an order to the categories in the tools block, from the simple user command category to the more sophisticated distributed tools category (the last category, data taps, is not related to the other categories). This is unlike the other blocks of the taxonomy.[1] What made these categories in the tools block mutually exclusive when applied to the CERT®/CC records was that attacks were classified according to the *highest* category of tool used.

**13.2.2. Categories that are Exhaustive -** Taken together, the categories in a taxonomy should include all possibilities. In terms of the taxonomy developed for this research, all paths connecting attackers with objectives (see Figure 6.9) should be included. During the classification of the data for this research, there was no instance when a category could not be found for the data.

With respect to the classification of the CERT®/CC data, the *attackers* and *objectives* blocks were exhaustive. There were such few data in these blocks, however, that there remains a question as to whether more categories would be necessary when classifying a larger data set. One question did

[1] The exception to this is the ordered list for describing the level of unauthorized *access* obtained by an intruder. In this case, the *highest* level of access obtained (root, account or attempt) was used to give a classification.

arise for those instances when *former employees* were identified in the records as attackers. The categories in the attackers block were established according the *motivations* of the attackers and not who there are. For this research, former employees were classified as *vandals*. More questions may arise when attackers from a larger data set are classified.

Another group of incidents that may lead to further refinements of categories in the taxonomy is *internal* attackers, where an attacker is located within the organization being attacked. The CERT®/CC incidents primarily involved *external* attackers, where the attackers were outside the organization being attacked. As such, the taxonomy is largely untested against incidents involving internal attackers.

There were two adjustments made to the taxonomy during the research to add categories. The first instance was to add the *data in transit* category to the access block of the taxonomy. Originally, data in transit was considered to be in the *files* category, but it made more logical sense to separate it out because the data are in different forms when they are in a file or in transit across a network. In addition, the methods used for attack against files and data in transit may be different, which makes it important to have separate categories in the taxonomy.

The second adjustment made to the taxonomy was to add the *distributed tool* and *data tap* categories to the tools block. As noted in Chapter 8, there were no instances of the use of these tools being recorded in the CERT®/CC records during the period of this research. The categories were added, however, to make sure the tools block was exhaustive.[2] In the case of distributed tools, this was because of incidents recorded at the CERT®/CC in 1996 and 1997, after the period of this research. The data tap category is based on theoretical attacks that have not been recorded in any CERT®/CC incidents.

This experience is an example of what we should expect, over time, regarding any taxonomy of computer and network attacks: the need will arise to add new categories. If nothing else, attackers will try new tools that may not be able to be classified into the current tools category. Greater understanding of attackers and their methods, however, may also make changes to other categories.

**13.2.3. Categories that are Unambiguous** - Categories in a taxonomy should be clear and precise so that classification is certain, regardless of who is classifying. Only one person did classifications for this research. As such, no determination was made as to whether classifications

[2] The suggestion to add the distributed tool category came from Dr. Thomas A. Longstaff at the CERT®/CC as a result of intruder activity appearing in the CERT®/CC records after 1995. The data tap category was the result of trying to help one of my students conceptualize how law enforcement could conduct searches on networks.

using the taxonomy were unambiguous. On the other hand, there were some difficulties in making classifications due to ambiguity. This was primarily the result of the lack of information. A typical example of this was a narrative description of an attack that did not contain enough information to classify the incident. If the classifications of attacks were done with more information available, such as by CERT®/CC personnel during an incident, ambiguity would be reduced. This is one course of action discussed in Chapter 14.

**13.2.4. Categories that are Repeatable** - Repeated applications of a taxonomy should result in the same classification, regardless of who is classifying. For this research, classifications of data were made only one time. As such, no determination was made as to whether classifications using the taxonomy were repeatable. On the other hand, it is likely that some of the classifications are, in fact, *not* repeatable because of incomplete information as described in the previous section. This is because, the greater the uncertainty when making a classification, the greater the chance for error or for disagreement in a classification.

**13.2.5. Categories that are Accepted** - The categories of a taxonomy should be logical and intuitive so that they could become generally approved. The taxonomy developed for this research was based upon a logical process that was intended to be intuitive. How logical and intuitive the taxonomy is could be investigated by having the taxonomy evaluated by others, such as during use by response personnel, as recommended in Chapter 14.

One of the ways the taxonomy was designed to be widely accepted was in the use of simple and accepted terms for the classifications. Terms that were widely used, but which had controversial definitions were intentionally avoided. For example, the term *computer virus* is widely used, but there is no accepted definition. One set of terms that has some problems with accepted definitions that were necessary to include in the taxonomy were the three categories of vulnerabilities. An example of the problem with these terms is when a program such as *sendmail* is targeted with a *mail spam* attack (repeated mailings). If this causes a system's storage capacity to be exceeded, then service may be denied to users. Some would view the failure to check for too many messages as an *implementation* vulnerability because the person that implemented the *sendmail* code did not include the proper checks. On the other hand, others may view this as a vulnerability resulting from an improper *design* if its inclusion was not part of the design.

Such problems were not seen in the application of this taxonomy to the CERT®/CC records. They can be avoided in the future by having good information about what is being classified, and by the use of specific definitions for the terms describing each category. As was noted earlier, not

enough information was generally available for classification into the three categories of vulnerabilities, so, for this category of the access block, its application is largely untested. For other categories, however, no problems were indicated concerning the acceptance or the intuitive nature of any of the terms.

**13.2.6. Categories that are Useful** - The final characteristic of a satisfactory taxonomy is that it can be used to gain insight into the field of inquiry. The conclusions from this research were largely drawn from analyzing data that had been classified using the taxonomy of attacks presented in Chapter 6. This showed the usefulness of the taxonomy because the analysis could not have been conducted without such a taxonomy for classification. As discussed in Chapter 6, previous taxonomies were inadequate for this classification because they did not meet the criteria for a satisfactory taxonomy.

As discussed in Chapter 6 (Section 6.2), the taxonomy is also potentially useful because it can organize thinking about computer and network security. The taxonomy emphasizes that, in order to be successful, an attacker must find one or more paths that connect the attackers to their objective. As the formal definition presented in Chapter 5 indicates, computer security is preventing attackers from achieving objectives by preventing them from making any complete connections through the process depicted in the taxonomy. More specifically, computer security efforts are aimed at the six blocks of the taxonomy. This is potentially useful because it helps direct policies and programs against specific targets or events in the attack process. Section 6.4.5 discussed how this might be done for each of the six blocks of the taxonomy.

### 13.3. Classifications of Incidents

Classification of incidents is more difficult than the classification of attacks. First of all, incidents can be made up of multiple attacks. But it is more complicated than that. These multiple attacks could not only be classified differently, but could also involve multiple attackers who are attacking multiple targets. As has been stated previously, what distinguishes one incident from another is the *distinctiveness* of the attackers, and the degree of *similarity* of sites, techniques, and timing. It does not mean that attackers, sites, techniques and timing are *identical.*

As such, the determination of the scope and characteristics of an incident, and then its classification must be accomplished in an atmosphere of uncertainty. Nevertheless, as has been discussed in this dissertation, it is important to do so. Indeed, this is routinely done by CERT®/CC personnel, and it was done for this research. However, for both the CERT®/CC and myself, this

process was informal and uncertain, particularly with respect to determining the *scope* of the incidents. For CERT®/CC personnel, this involved meetings where information was exchanged and then correlated. In the early years of the CERT®/CC, these were often chance encounters "around the coffee pot." In more recent years, information exchange took place in periodic meetings. For this research, this judgment of CERT®/CC personnel was combined with comparisons between the records to determine the scope of each incident.

This ad hoc process will not scale up as the Internet grows exponentially. A more formal process is required. In addition, unless more personnel can be assigned to incidents response, automated software tools will be necessary for the more routine incidents, leaving personnel free to determine the scope of only those incidents with the greatest uncertainty.

The following sections will discuss first, how incidents classification was done at the CERT®/CC, second, how it was done for this research, and third, how incident classification should be accomplished as a result of this research. The three steps for full classification of an incident are 1) determine the scope, 2) determine the characteristics, and 3) determine the classifications. Development of a more formal process to determine the scope of incidents, and software tools to automate part of that process are discussed in Chapter 15.

**13.3.1 Classifications at the CERT®/CC during the period of research** - The process of classification of incidents at the CERT®/CC during the period of this research was described briefly in Chapter 4. As noted there, after December, 1993, the process included summaries, and after the summer of 1994, the summary records were relatively complete records of the incidents. These summary files represented classifications of the incidents. As Chapter 4 indicates, these summaries contained the following:

1. A file identification consisting of the key letters CERT®#, INFO#, or VUL# followed by a randomly generated, but unique, number,
2. Reporting date,
3. Notes and excerpts from e-mail and other files sent to the CERT®/CC,
4. An identification number for each excerpt that could be used to retrieve the original file,
5. List of sites involved,
6. Lists of keywords describing attacker activity in various categories.

The last item, the lists of keywords, was related to the classifications of the taxonomy for this research in Chapters 7 and 8.

CERT®/CC action was initiated when the incident activity, information request, or vulnerability information was reported. If it was deemed appropriate, a CERT®, INFO, or VUL number was assigned, which then automatically resulted in a summary file being opened. As stated in Chapter 4, the correspondence between incidents and summaries was not one-to-one. Some of the summaries initially opened by the CERT®/CC later proved to be related to each other. Once CERT®/CC personnel determined that two or more summaries were related, the usual course of action was to indicate this relationship in the summaries, but to keep all the summaries open. As such, the number of summaries in the CERT®/CC records was greater than the number of actual incidents. Occasionally, a summary was closed and the information from that summary was copied to a related summary.

CERT®/CC personnel did not classify the attacks within each incident. Instead, they recorded keywords as described in Chapters 4, 7 and 8. This process was not consistent for several reasons. First, different terms were used in different incidents to describe the same type of attack. Second, while most of the summaries contained at least one key word that described the level of access obtained by the attacker, many of the summaries contained few, if any, other keywords. This meant the CERT®/CC summaries often did not contain complete details of the incidents.

**13.3.2. Classification of Incidents for this Research** - In order to gather data about incidents during the period of this research, the incidents had to be created from the CERT®/CC summaries. As described in Chapter 4, this was a difficult and time-consuming process, particularly since this was done after the incidents were closed. As stated in that chapter, the summary records were searched first by reading the summary, and then Unix search tools, such as the *grep* utility, were used to relate key words and phrases to the incidents already created. The four types of key words and phrases were:

1) Notes by CERT®/CC personnel indicating a relationship with other summaries,
2) Site names,
3) Keywords from the categories of the taxonomy (tools, vulnerabilities, access level, etc.),
4) Unique words, phrases or letters.

As stated in Chapter 4, the first of these categories, the judgment of CERT®/CC personnel, was given strong weight in determining the scope of an incident. Experience with this research found that, when searching with the Unix utilities, site names was the best category of words or phrases to use. However, unique words or phrases were a particularly good way to reduce uncertainty. An example of this was given in Chapter 10 where the "Dutch hacker" incident was described (Section

10.2.1). In this incident, the intruders often installed a backdoor process operating on socket 87. Therefore, the keywords "socket 87" or "87 socket" were definite indications of a relationship when they were found in the CERT®/CC records.

Once the incident records were reconstructed, the keywords in the records were used to determine the following:

1) an overall classification of the incident according to either the highest level of access the intruder obtained (root, account, or attempt), or the type of unauthorized use (denial-of-service, disclosure of information, or corruption of information)
2) the presence of keywords from the other categories of the taxonomy, including attackers, tools, vulnerabilities, results and objectives

There were several difficulties with this approach. First, as discussed in Chapter 8, numerous categories in the taxonomy (Figure 6.9) had little information in the CERT®/CC records, and, as noted above, the use of various terms was inconsistent. Second, inaccuracies were introduced because the classification was done by someone who had not participated in the response to the incident (me) *after* the incident was closed . Finally, this process was very labor intensive, making it essentially unrepeatable.

**13.3.3. Recommended Process for Classifying Incidents** - The following sections outline a recommendation for a process to classifying incidents, based on experience with this research.

***13.3.3.1. Determining Incident Scope*** - In the short term, the process of determining the scope of an incident could be improved by taking two steps. First, only one incident summary should be maintained for each incident, open or closed. When a relationship is found between two summaries indicating they are part of one incident, they should be combined under one summary. Unfortunately, it would be difficult to discontinue the use of a particular CERT® number, because CERT® numbers are used in communications with the affected sites. One possible approach would be to have each incident summary identified with an incident number for *internal CERT®/CC use only*. The CERT® numbers would continue to be used in communications with affected sites, but related records would be stored within one summary file under the separate incident number.

***13.3.3.2. Determining Incident Characteristics*** - The process of searching records for keywords in order to determine the scope of an incident will work more effectively if a standard set of keywords and phrases is recorded in each summary. Recording these incident characteristics during an incident will make the information more timely and accurate. Experience during this research suggests several fields of data are useful to record. These fields are grouped in the following categories: time and duration, sites, workload, attacks, and responses.

A) Time and Duration:

1) ***Reporting Date*** - the date the incident was reported to the CERT®/CC
2) ***Starting Date*** - the earliest date of known intruder activity
3) ***Ending Date*** - the latest date of known intruder activity (note, this is not the date the incident was closed, which is an administrative action unrelated to intruder activity)

B) Sites:

4) ***Number of Reporting Sites*** - the total number of sites reporting the incident
5) ***Reporting Sites*** - the site names of each site that reported the incident
6) ***Number of Other Sites*** - the total number of sites involved, but not reporting the incident
7) ***Other Sites*** - the site names of other sites involved, but not reporting the incident

C) Response Workload:

8) ***Number of Messages*** - the number of messages to/from the CERT®/CC (or some other appropriate measures of CERT®/CC workload with respect to the incident)

D) Attack Activity:

9) ***Attackers*** - keywords identifying attackers and their categories (from Figure 6.9)
10) ***Tools*** - keywords identifying tools and their categories (from Figure 6.9)
11) ***Vulnerabilities*** - keywords identifying vulnerabilities and their categories (from Figure 6.9)
12) ***Level*** - keywords identifying the types of unauthorized access or unauthorized use, and the *highest* level achieved by the attackers (from Figure 6.9)
13) ***Results*** - keywords identifying results and their categories (from Figure 6.9)
14) ***Objectives*** - keywords identifying objectives and their categories (from Figure 6.9)

E) Response to Attacks:

15) ***Corrective Actions*** - keywords identifying corrective actions taken at the sites involved, which could be categorized as internal actions (restrict hardware/software, configure hardware/software, upgrade system, or preventive measures), external actions (actions against intruders, or law enforcement), or other appropriate categories

Experience with recording of these data will probably show that these categories should be modified or additional categories should be added. It is important, however, for the data that is recorded and the keywords that are used, to be defined, systematic and consistent. New keywords should only be added when intruder activity cannot be described by the existing set of keywords, and only when accompanied by a detailed description of the keyword.

***13.3.3.3. Classification of Incidents*** - Implicitly, CERT®/CC assigned an overall classification to each incident according to the *highest* level of access obtained by any intruder (root, account or access) for the unauthorized *access* incidents (90% of all incidents). For unauthorized *use* incidents,

general or average intruder activity was used to determine a category for the incident (denial-of-service, corruption of information, disclosure of information). This process was also followed for this research and was found to be a satisfactory overall classification for an incident. It is recommended this process be continued. Such a classification was useful in determining overall activity.

The frequency of occurrence of activity in the various categories of the taxonomy could be determined from the keywords describing the incident. This was done for this research (Chapter 8), and should be improved as these data are recorded more systematically.

### 13.4. Summary of the Utility of the Taxonomy of Computer and Network Attacks

The taxonomy developed for the classification of attacks was found to be satisfactory for classifying the CERT®/CC records. It should be expected, however, that a satisfactory taxonomy would be limited in some of the desired characteristics. This was found in this research also.

In general, in applying the taxonomy for this research to the CERT®/CC incidents, there were few instances when a single classification was not directly determined; an indication that taxonomy categories were mutually exclusive. Two problems were noted. First, when there was limited information, there was sometimes difficulty in assigning an attack to a single category. Second, one attack could sometimes, theoretically, be in two categories.

During the classification of the data for this research, there was no instance when a category could not be found for some data, which was an indication that the taxonomy categories were exhaustive. Two adjustments to the taxonomy were made during the research to ensure that the categories were theoretically exhaustive. First, the *data in transit* category was added to the access block. Second, the *distributed tool* and *data tap* categories were added to the tools block.

The criteria that the categories to be unambiguous, that the classifications to be repeatable, and that the terms to be intuitive and acceptable could not be tested with the data used in this research, because classifications were made once by one person. Additional testing by the CERT®/CC, other response teams, and other researchers, could be an opportunity for such an evaluation.

The conclusions from this research were largely drawn from analyzing data that had been classified using the taxonomy of attacks. The analysis could not have been conducted without such a taxonomy for classification. The taxonomy is also potentially useful because it can organize thinking about computer and network security to emphasize that, in order to be successful, an attacker must find one or more paths that connect the attackers to their objective. Computer security efforts can be aimed at the six blocks of the taxonomy.

The process of determining the scope of an incident could be improved by maintaining only one internal incident summary for each incident, open or closed, and by using a formal process of searching records for keywords and phrases, in addition to other methods to collapse attacks into incidents.

A standard set of keywords and phrases that are defined, systematic and consistent, should be recorded in each summary. New keywords should only be added when intruder activity cannot be described by the existing set of keywords, and only when accompanied by a detailed description of the keyword. Suggested fields of information to record are reporting date, starting date, ending date, number of reporting sites, reporting sites, number of other sites, other sites, number of messages, attackers, tools, vulnerabilities, level, results, objectives, and corrective actions. Experience with recording of these data will probably show that these categories should be modified or additional categories should be added. It is important, however, for the data that is recorded and the keywords that are used, to be defined, systematic and consistent.

An overall classification should be given to each incident according to the worst level of unauthorized access or unauthorized use. The frequency of occurrence of activity in the various categories of the taxonomy could be determined from the keywords describing the incident.

*Chapter 14*

# Policy Implications and Recommendations

This chapter presents policy implications of this research and recommended actions for Internet users, suppliers, response teams and the U.S. government. This includes an estimate of the likelihood an Internet domain or host will be involved in an incident. This chapter also presents an analysis of the information policies of the U.S. government and Internet incident response teams, and recommends changes to these policies.

## 14.1. General Implications of This Research

Security is a problem on the Internet. The thousands of successful break-ins described in this research are a testimony to that. Numerous authors -- scholars and sensationalists alike -- go even farther by describing the Internet as a dangerous place in terms of security.

But just how much of a problem does this research say security really is on the Internet? As stated in Chapter 1, the answer to this question is important for two reasons. First, with information about Internet security problems, we could determine to what extent, and in what areas, government programs and policies should be instituted to protect the Internet. Second, trends over time could indicate the effectiveness of these policies and programs.

Because it shows the state of security on the Internet, this research is also important for Internet users, suppliers, and response teams. It provides all of these Internet participants indications of what they should and should not be doing on the Internet because of potential security problems. It can also indicate whether increased user awareness, more secure software and hardware, improved security tools, and increased incident response capacity, lead to desired changes in incident trends.

What this research shows is a mixed message. On the positive side, this research clearly shows that the state of Internet security is not as bad as some authors have proposed. Both in terms of the absolute numbers of incidents, and in the growth of these incidents, the numbers are lower than reported in popular literature and in the Press. More importantly, response teams and researchers are not as unaware of Internet security activity as some authors have argued. As shown in Chapter 12, the most serious incidents on the Internet *are* reported and successfully dealt with. In addition, none of the incidents were tremendously destructive.[1] In fact, very few instances were

[1] In terms of financial impact, files lost, and time spent by personnel, some incidents were quite destructive locally. In general, however, most incidents were not destructive, and if they were destructive, the destruction was relatively limited and confined.

recorded of destructive attacks. Most attacks were in the category of a nuisance (although some were a *big* nuisance), and not something more destructive or harmful.

Nevertheless, on the negative side, security incidents were clearly not dropping to zero. As shown in Chapter 7, the rate of growth of Internet incidents was less than the growth of Internet hosts by 7%. But, stated another way, this means that the growth of Internet incidents in absolute terms was nearly at the *same* pace as the growth of the Internet. If these trends were to continue indefinitely, the number of Internet incidents may eventually drop in absolute terms, but clearly *not for a very long time.*[2]

To put this in perspective, we can use the estimates of total Internet incident activity in Chapter 12 to see how likely we are to be involved in an Internet incident. In Table 12.13, the number of total Internet incidents per year for 1995 was estimated to be between 1,200 and 22,800. The average number of sites per incident was 6.5, which means an estimate of the number of sites involved in an incident per year is between 7,800 and 148,000.[3] In July, 1995, the number of Internet domains was estimated to be around 120,000, and the number of Internet hosts to be around 6.64 million. This yields the very rough estimates in Table 14.1.

| | Low Estimate | High Estimate |
|---|---|---|
| **Individual Domain Involved** | 1 time in 15 years | 1 time in 0.8 years |
| **Individual Host Involved** | 1 time in 850 years | 1 time in 45 years |

**Table 14.1. Estimated Rate that an Internet Domain or Host was Involved in an Incident in 1995**

This table shows that, according to these estimates, a typical Internet domain is involved in *no more* than around *one incident per year.* In terms of hosts, the estimates of Table 14.1 show that a typical Internet host is involved in *no more* than around *one incident in every 45 years.* The CERT®/CC records show that some sites and hosts are apparently more attractive because they were involved in many incidents each year. This means that for the average, less attractive, domains and hosts, the probability of being involved in an incident is even lower.

In addition, as shown by this research, many of the Internet incidents are minor and often do not involve successful break-ins. As such, the rate at which domains and hosts are involved in

[2] This, of course, raises the question of just how long, based on this research. If the growth rate in Internet incidents remains relatively constant at only 7% less than the Internet growth rate, the number of incidents would stop growing near the time the Internet stops growing. I am not aware of any predictions of when the Internet will stop growing.

[3] The actual number of sites involved each year in incidents will probably be lower than these figures because some sites are involved in more than one incident, but the high estimate shown here will yield the *highest* estimates of the chances of being involved in an incident, which is what I am trying to estimate.

*serious* incidents is even lower. For example, at Site A only 7% of incidents involved root break-ins. If this were similar throughout the Internet, then the *maximum* rate that any one domain would be involved in a root break-in would be around once in 10 years (instead of once in 0.8 years), and any individual host around once in 540 years (instead of once in 45 years).

These rates of occurrence are similar to other risks that we take reasonable precautions for. The following are several examples:

- We may purchase flood insurance for the possibility of flooding that occurs, on average, only once in 100 years, or once in 500 years.
- The mean time between failure (MTBF) of new hard drives ranges between 300,000 and 1,000,000 hours [Pik97]. If a drive is used continuously, failures could be expected to occur from between once in 34 years to once in 114 years. For such an event, it is prudent for users to make backups of important hard disk files.
- In 1994, the U.S. Census Bureau estimated there were around 54,000 convenience stores in the U.S. [USB96:Chart No. 1263]. During that same year, there were around 32,000 robberies at convenience stores [USB96:Chart No. 318]. This means that the average convenience store is robbed around once every year and a half. Convenience store owners and employees can take reasonable precautions to reduce the risks through actions such as limiting the cash available at night, placing the cashier within a bullet resistant structure, etc.
- In 1993, there were around 16.3 deaths in motor vehicle accidents per 100,000 people (a rate corresponding to once in 6,250 years for an individual) [USB96:Chart No. 138]. As a precaution, drivers and passengers can use seat belts, drive in cars with airbags, and drivers can drive at safe speeds.
- In 1994, there were around 16.6 deaths due to breast cancer per 100,000 people (once in 6,224 years) [USB96:Chart No. 129]. As a precaution, women examine themselves and have regular breast cancer screenings, depending on their age.
- The City of New York, with a 1994 population of more than 7.3 million, has around 800,000 buildings [NYC97b]. In 1995, there were 30,294 known structural fires, of which 3,666 were determined to be serious [NYC97a]. This means that each building in New York City has a serious structural fire an average of once every 220 years. There were also 2.5 deaths per 100,000 population due to fire (once in 40,000 years). Due to these risks, in 1995, the Fire Department of the City of New York employed more than 12,000 people and had a budget of $142.6 million.

Table 14.2 compares these examples with the Internet security risks. The conclusion we can draw from this is that there is a steady, but relatively small, level of Internet security incidents. Internet users should take reasonable security precautions, just as they would take for other risks in their lives. In addition, Internet suppliers should produce and distribute products that provide users with reasonable security, and the U.S. government and Internet response teams should institute programs and procedures to mitigate Internet security problems.

| Risk | Estimated Rate Risk Occurs |
|---|---|
| Root Break-In, Internet Domain | 1 out of 10 years |
| Root Break-In, Internet Host | 1 out of 540 years |
| Convenience Store Robbery | 1 out of 1.5 years |
| Hard Disk Failure | 1 out of 75 years |
| 100 Year Flood | 1 out of 100 years |
| Serious Structural Fire, NY City | 1 out of 220 years |
| Death Due to Breast Cancer | 1 out of 6,224 years |
| Death in Motor Vehicle | 1 out of 6,250 years |
| Death Due to Fire, NY City | 1 out of 40,000 years |

**Table 14.2. Comparison of Estimated Rates That Risks Occur**

The following sections discuss these implications in more detail.

### 14.2. Implications for Internet Users

This year you will most likely *not* be the victim of a violent crime, have your house robbed, or your car stolen. But you might. Because of this, you are likely to take reasonable precautions to protect yourself and your property.

This research shows the same is true of the Internet. Unlike what some authors have proposed,[4] if you are an Internet user, this year you are most likely *not* going to be the victim of an Internet attack. But you might. Because of this, you should take reasonable precautions to protect the files on your computer, and to protect your data as it transits the Internet.

Two analogies illustrate this point. Take, for example, convenience stores. They get robbed sometimes. This could clearly be prevented with a "fortress" security system of physical barriers and armed guards. But then how convenient would that store be to shop in? Instead of ensuring *no* risk of robbery, the convenience store owner typically takes reasonable precautions against robbery in order reduce that risk, but accepts some risk in order to ensure the store is still convenient to shoppers.

An Internet user can be perfectly secure from Internet attack by simply disconnecting from the Internet. But then, this user would no longer be an Internet user. Instead of taking this no risk strategy, it is probably more appropriate to take reasonable precautions and accept a level of risk that depends on that user's individual needs.

---

[4] See, for example, the quote from Winn Schwartau at the beginning of Chapter 1.

A second analogy is the mail system. We view the mail system as generally being secure enough to send a personal letter, or to send a check to pay a bill. On the other hand, most people do not send cash or valuables through the mail unless special precautions are taken. We also don't usually send sensitive personal information on a post card, and instead, we enclose it in an envelope. Sometimes a letter is lost, but not often.

In some ways, the Internet is a less secure system than the U.S. Postal Service ("snail mail" in the computer vernacular). E-mail is sent across the Internet in clear text that could be read by other users. On the other hand, Internet e-mail is usually a lot quicker, and perhaps more convenient and inexpensive. As such, users may be willing to accept the higher security risk when using the Internet in order to have the capabilities.

Prudent users of the Internet, however, should take precautions in two ways. First, they should take reasonable precautions to protect their files stored on their local computer or stored on the network. And second, they should take reasonable precautions to protect their data in transit on the Internet. For each user of the Internet, the *reasonable* level of precautions may be different, and it depends on that user's needs.

**14.2.1. Basic Precautions All Users Should Take to Protect Files -** There are three basic precautions that all Internet users should take. The first precaution is to back up important files. This will not prevent an incident, but it may reduce the impact if a user is involved an incident. Which files should be backed up can easily be determined if a user imagines losing the original files. For example, if a user's files are stored on the local hard drive, what would the user lose that is important if the hard drive files were lost? Software can usually be reloaded, but a user's personal files may be lost permanently if they are not stored elsewhere. How many backups a user should make and where they should be stored depends on how important the files are. The files for this dissertation were an extreme example, but I was determined not to lose any of the files, so I backed up all files to hard drives on four different computer systems (in different locations) and three sets of floppy disks. For most users, one backup to floppy disks or to a hard drive on a separate computer is probably sufficient.

The second security precaution that all users should take is to have a good password for the access controls to their network. Unlike backing up files, this action may prevent an incident. This research showed that 22% of all incidents in the CERT®/CC records involved problems with passwords. Good passwords have the following characteristics: 1) eight or more characters, 2) both uppercase and lowercase letters, 3) punctuation or other special characters, 4) easily

remembered (no need to write down), and 5) can be typed quickly [RuG91:61; GaS96:63]]. Having a good password will help protect a user from having his account and files accessed under most conditions. What it will not protect against is an intruder who gains access to the root level on the computer system, which would allow bypassing the account access controls. As shown in this research, however, this does not happen often.

A good password can also be compromised if it is sent over the Internet in the clear, which may allow it to be read by sniffer software. One precaution that a user can take to minimize this problem is to change passwords periodically. This research shows, however, that this is unlikely to do much good. This is because of a combination of the low likelihood of a user's password being sniffed, and that actual incidents are of short duration.

The likelihood that a user's password is going to be sniffed is low for several reasons. First, many users do not send their password over the Internet in the clear because they do not sign into systems over the Internet (they only sign in locally). Second, as Chapter 8 indicated, even though passwords were identified as a problem in 22% of all incidents, only 245 incident records mentioned sniffers specifically (5.7%). As was discussed earlier in this chapter, a typical Internet domain is involved in an incident no more than around once a year. On the other hand, the rate at which a typical domain is involved in an incident where a sniffer is used is probably significantly less. Using this criteria, users could safely go years without changing passwords.

If, however, a user's password *is* sniffed from the network, then any resulting problems will occur in a relatively short period of time. The average duration of incidents involving root or account break-ins was 23.4 days, for incidents recording password problems, 8.6 days, and incidents recording sniffer use, 17.3 days. Using these figures, a user should change passwords every few days so that *if* the password is compromised, any resulting problems will be minimized. But then, as stated above, the incidents don't happen very often.

Some site administrators require users to change passwords every few months. As was discussed above, this is too long a period to reduce problems if a password is actually sniffed, and it is too frequent based on the probability of an incident taking place at any particular site. This research seems to indicate that changing passwords every few months is generally not appropriate. Instead, site administrators should probably ask users to change passwords only if their site is compromised, or if the site administrator determines the user has a weak password (such as through the use of a password cracking program). One caveat is that users who frequently sign in over the

Internet (send their password in the clear over the Internet) should consider changing their password frequently.

A third precaution that all users should take is to ensure that permissions on files that can be accessed by others are set properly. An example of files that could be accessed by others are files in a Unix account. The Unix operating system maintains a set of permissions on each file that establishes permission to read, write, or execute the file by the file owner, a group of users, or all users. If a user does not want other users to read his files, then the permissions for each file must be set to prevent this. This is not just a concern for Unix users. As operating systems become more network capable, such as Windows NT, the same capabilities and concerns arise.

**14.2.2. Advanced Precautions to Protect Files** - Users may elect to take further precautions for files that are particularly sensitive. If the concern is unauthorized disclosure, files could be encrypted.[5] Another alternative is to store files off-line from the network.

**14.2.3. Precautions to Protect Data in Transit** - Almost all Internet traffic is sent "in the clear." This means that it can be read by software on any host computer through which the network packets are routed. This should be of little concern to most Internet users because most of the packets traveling on the Internet contain data that is not sensitive from the user's viewpoint, and is not of interest to Internet attackers. Three types of information traveling across net that *are* sensitive to users, and of interest to Internet attackers, are discussed in the following paragraphs.

The first type of sensitive information traveling across the Internet is user name, password, and IP address combinations. These data are the primary targets of sniffer programs operated by Internet attackers. These are read by the sniffer program and typically recorded in a file intended to be retrieved later by the attacker. These combinations can then be used to break into the user's account. A solution to this problem is to have these data sent across the Internet in a secure manner, such as by encrypting them first. Currently, an individual user cannot do anything about this, except, as noted above, to change passwords frequently. What is required is for suppliers to provide a more secure procedure for logging in across the network, as discussed in the next section.

The two other types of sensitive information traveling across the Internet are sensitive user identifications, and files sensitive to the user. Users should take one of two precautions, either encrypt the information or don't send it across the Internet. Examples of sensitive user

---

[5] The CERT®/CC records show no instance when even very simple encryption was broken. This, of course, does not indicate that encryption is an effective method of protecting files, just that there is no indication that it is *not* an effective method.

identifications are social security number, address, phone number, personal data, and perhaps most sensitive of all, credit card numbers. In general, none of these data should be sent across the Internet unless they are encrypted at the source (prior to being sent across the Internet).

An example of a file that would possibly be sensitive to the user is e-mail containing personal information or sensitive business information. If a user wants to ensure this information is kept confidential, then it must either be encrypted, or sent some other way (such as through the U.S. mail). Pretty Good Privacy (PGP) is an e-mail encryption program available on the Internet that can provide encrypted e-mail.

**14.2.4. Additional Considerations for Commercial Internet Users** - A commercial Internet user may have more security concerns than individual users, because commercial users may have more connections to the Internet, and may have more assets exposed to the Internet. Commercial users should conduct some form of risk analysis to determine the cost effective level of security they should have.[6]

**14.2.5. Summary of the Implications for Internet Users** - This research shows that Internet users are not likely to be the victim of an Internet attack. They should, however, take reasonable precautions to protect the files on their computers, and to protect data as it transits the Internet. For each user of the Internet, the *reasonable* level of precautions may be different, and it depends on that user's needs.

All Internet users should take the following basic security precautions:

1. Back up important files.
2. Use a good password for network access controls.
3. Ensure permissions are set properly on files that can be accessed by others.
4. Encrypt, or store off-line, files that are particularly sensitive.
5. Do not send sensitive user identifications, such as a social security number, address, phone number, personal data, or credit card number across the Internet unless it is encrypted at the source (prior to being sent across the Internet).
6. Use an encryption program, such as Pretty Good Privacy (PGP), if you want e-mail to be private.[7]

---

[6] Risk-based characterization of network vulnerability is currently being researched at the Sandia National Laboratories in Albuquerque, NM. For information, contact Laura Painton at 505-844-8093 or lapaint@sandia.gov.

[7] As was noted in Chapter 8, there were very few references to viruses in the CERT®/CC records. As such, this research did not indicate that virus protection was required. This research did not, however, examine problems *within* local area networks. Viruses can be a considerable problem within LANs, particularly for LANs with personal computers (PCs and MacIntoshes). As such, an additional precaution that users on LANs with PCs and MacIntoshes should take is to use virus protection software that is frequently updated.

An additional recommendation for commercial Internet users is as follows:

7. Conduct some form of risk analysis to determine the cost effective level of security.

There was no indication in this research that these simple precautions would not be effective in preventing most Internet attacks.

### 14.3. Implications for Internet Suppliers

Internet suppliers include both commercial vendors that supply hardware and software used to access the Internet, and organizations such as the Internet Society and its member organizations that help establish standards for Internet protocols. As noted in the previous sections, this research gave no indication that simple precautions would not be effective in preventing most Internet security problems. Suppliers of Internet products should ensure their protocols and products conveniently provide Internet users with capability to take these simple precautions as described it the previous section.

The CERT®/CC incident records clearly indicate specific problem areas with respect to Internet security that should be corrected by Internet suppliers. These problems are as follows:

**14.3.1. Password Problems** - Two significant problems related to passwords were indicated in the CERT®/CC records. First, user name, password and IP address combinations are sometimes sent in the clear across the Internet. Packet sniffers may be used by Internet attackers to read these combinations. Internet suppliers should provide protocols and software that encrypt these data at the source, or provide alternative systems that do not require passwords to be sent in the clear across the Internet.

The second password problem that continues to be a concern is access to password files for password cracking. CERT®/CC records shows that, though this problem was declining among severe incidents, it continued to be a problem for smaller incidents. Internet suppliers should provide protocols and software that prevent access to files of encrypted passwords, or provide an alternative system that does not require encrypted passwords to be stored in files on systems accessible across the Internet.

**14.3.2. Shipping Software in an Insecure State** - There are repeated examples, in the CERT®/CC records, of Internet attacks that successfully took advantage of software that was shipped to users in an insecure state. This includes default passwords for system accounts, default permissions on files, and a default trusted-host configuration. Suppliers of systems should discontinue this practice. Software should always be shipped in a secure state.

**14.3.3. Additional Actions Suppliers Should Take** - The CERT®/CC records for the period of this research showed that denial-of-service attacks were a small problem. However, the rate of growth of these incidents was greater than the rate of growth of Internet hosts. In addition, other than the small number of incidents, there was no indication that users on networks and hosts connected to the Internet could successfully prevent denial-of-service attacks. This is an area where further investigation is warranted. Internet suppliers should develop protocols and programs with reasonable protections against denial-of-service attacks.

An additional area that Internet suppliers should investigate is user privacy. Development of protocols and programs that provide reasonable privacy for such user programs as e-mail should be accelerated to provide this capability in the near term.

**14.3.4. Summary of Implications for Suppliers** - CERT®/CC incident records clearly indicate specific problem areas with respect to Internet security that should be corrected by Internet suppliers. The recommended corrections are as follows:

1. Provide protocols and software that encrypt user name, password and IP address combinations at the source, or provide an alternative to system that does not require passwords to be sent in the clear across the Internet.
2. Provide protocols and software that prevent access to files of encrypted passwords, or provide an alternative system that does not require encrypted passwords to be stored in files on systems accessible across the Internet.
3. Deliver systems to customers in a secure state.
4. Develop protocols and programs with reasonable protections against denial-of-service attacks.
5. Accelerate development of protocols and programs that provide reasonable privacy for such user programs as e-mail.

### 14.4. Implications for the Government

This research has shown that there are security problems on the Internet. But just the existence of problems does not necessarily justify government intervention. If the free market provides the necessary solutions, then government intervention is not required, or desirable. In fact, in some circumstances, government intervention may make matters worse.

Although information about the actual state of Internet security has been limited, the government already intervenes in four ways. First, the government provides incident response through funding of the CERT®/CC and other agencies in the Department of Defense (DoD), such as AFCERT, ASSIST, DISA, and NAVCIRT (see Chapter 3). Second, through the CERT®/CC, other response teams, and other agencies, such as the National Institute of Standards and

Technology (NIST), and the National Security Agency (NSA), the government controls information related to Internet security. Third, the government affects Internet security through the rules and regulations of such agencies as NIST, NSA and DoD. And finally, the government influences research and development through funding and participation in such organizations as the Internet Society.

With improved information about the state of Internet security, we may be able determine whether these interventions have been effective. Potentially, we could also determine to what extent, and in what areas, government programs and policies should be changed to improve the security of the Internet. Trends over time could possibly be used to determine the effectiveness of current and future policies and resources.

Most of the current government interventions concern providing or controlling information. This is the most common and basic method of government intervention. The next section presents the theoretical justification for government intervention in providing information to the Internet community. This is followed by a discussion of what government policies should be, based on the results of this research.

**14.4.1. The Government's Role in Providing Information** - The key insight into the operation of free markets is attributed to Adam Smith, the author of the *Wealth of Nations*. He postulated that "if an exchange between two parties is voluntary, it will not take place unless both believe they will benefit from it [Fri78:13]." The "belief" of the parties that leads to a voluntary transaction between them is based on their information about the transaction. The primary signaling mechanism providing information in such free market transactions is the price system.

Prices send information between customers and suppliers about the value of goods and services. If there is unhindered flow of information to both customers and suppliers, then this price mechanism helps enable efficient market outcomes. However, if customers and suppliers do not have the same information about prices, quality, and other aspects of goods and services, the result may be an inefficient outcome -- a market failure -- due to *asymmetric information* [McB96:611].

> For the price system to perform its signaling function perfectly, information must be costlessly shared among all individuals . . . Obviously, perfection is rarely achieved. The critical issue will be how consequential the asymmetries in information are [StZ78:298].

The market for computer security, just like other markets, is based on the flow of information about suppliers, customers, products and services. The sources of information include customers and suppliers, but also other organizations which have information about computer security. These other organizations include the press, educational institutions, governmental organizations, sites on

the World Wide Web, and attackers. If there are consequential differences in information available to suppliers and customers, the market can become inefficient. An example might be if suppliers are aware of security problems in hardware and software, but customers are not, then customers may purchase more insecure products than they would if they had known of the security problems.

In summary, if information is not shared costlessly among all prospective participants in a market, then the market will have asymmetries of information that may lead to inefficient outcomes [StZ78:321]. Under this condition, the government may be required to intervene.

**14.4.2. Government Information Policies and the Computer Security Market** - During the history of the Internet, the government has maintained a very high level of confidentiality regarding Internet security. This policy has been controversial, because it has resulted in an asymmetry of information, where information about security incidents and vulnerabilities may be known by attackers, suppliers, government agencies, and response personnel significantly better than it is known by the average user of the Internet. It is possible that users would make different purchasing decisions if they had more information about Internet security problems and incidents. It is also possible that suppliers would offer products and services with greater security if more information was available, particularly to their ultimate customers, Internet users.

On the other hand, this high level of confidentiality may have several beneficial effects. First, it may protect individual sites from adverse publicity that may result if security problems or incidents at that site were made public. Second, it may protect individual sites from further attacks. This is because, as the CERT®/CC records show, attackers spread information about site insecurities, which may then be used by other attackers. Withholding information may help prevent this. Third, withholding information may result in attackers having more difficulties finding insecurities to exploit. Finally, and perhaps most importantly, strict rules of confidentiality may result in more reports of incidents being given to government agencies, such as the CERT®/CC.

The net benefit of the effects resulting from the government's confidentiality policy is difficult to determine and the subject of debate. Some view the government policies as too restrictive because they leave attackers more informed than users and site administrators [ShM96:116]. Others, such as CERT®/CC personnel, maintain that stricter confidentiality results in more security. The issue of what information should be released to the public is discussed in Section 14.4.4.

**14.4.3. Funding of Incident Response Supported by This Research** - This research does not provide any conclusive evidence that current government interventions in support of Internet security should be changed in any significant way. On the other hand, this research shows the value

of obtaining more information about Internet activity, of promoting Internet security, and of funding incident response teams, particularly the CERT®/CC.

As stated before, information about Internet security activity provides information for the setting of national policy. Problems that arise can be targeted for policies and programs. Without information, this simply cannot be done properly. Funding of incident response teams, particularly the CERT®/CC, was shown to be important by this research. As this research has shown, most of the significant security activity gets reported to the CERT®/CC. In addition, the CERT®/CC is the single point where information about Internet security incidents is gathered.

Because of these reasons, the CERT®/CC, and to a lessor extent, other response teams, act as our "eyes" to see into the Internet security world. This research supports the view that the CERT®/CC is our only real source for comprehensive and timely information on Internet security incidents in four important areas. First, their records show the state of the art in *practical* Internet intrusion techniques. Many authors present information about what attacks are *possible* on the Internet, but the CERT®/CC records show what attackers have found actually works. Second, CERT®/CC personnel and their records can provide information about security problems which can focus government actions. Third, these records can be used to determine the result of those actions. And fourth, CERT®/CC response personnel could provide warning of significant security events. They currently provide this to the Internet community through CERT® advisories. They could also, however, provide more detailed information to government intelligence and law enforcement agencies that could focus their attention on developing problems.

A recent Defense Science Board (DSB) Report confirmed a national security need for warning of significant Internet events as follows:

> The essence of tactical warning is monitoring, detection of incidents, and reporting of the incidents. Monitoring and detection of infrastructure disruptions, intrusions, and attacks are also an integral part of the information warfare (defense) process. Providing an effective monitoring and detection capability will require some policy initiatives, some legal clarification, and an ambitious research and development program . . . . All intrusions and incidents should be reported so that patterns of activity can be established to aid in strategic indications and warning. The FCC requirement to report telephone outages of specified duration affecting more than a specified number of customers serves as a model in this regard [DSB96:55]

This research shows that requiring the reporting of all intrusions and incidents may not be necessary because most significant incidents are already reported. For the CERT®/CC to be

effective in providing tactical warning, however, the information they provide will have to be accurate and timely.

Two additional recommendations of the DSB are to:

> 9b. Develop techniques and tools for modeling, monitoring, and management of large-scale distributed/networked systems.
>
> 9c. Develop tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks [DSB96:16].

These are additional capabilities that can be provided by the CERT®/CC and, to a lessor extent, by other response teams (see Chapter 3 for a list of other response teams).

The DSB recommends the establishment of two centers for Information Warfare - Defense (IW-D). They recommend the first be located at the National Security Agency (NSA), with Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA) support. This center would provide *strategic* indications and warning, current intelligence and threat assessments [DSB96:12]:

> There may, in fact, be a need to form a National Center for Indications and Warning. This center would gather and analyze monitoring data continuously. The data would be derived from commercial infrastructure systems as well as government. The center could be charged with searching for and detecting early signs and precursors of a wide scale, coordinated attack and with providing warnings to U.S. government and private sector organizations [DSB96:63].

The second center would be located at the Defense Information Systems Agency (DISA), with National Communications System (NCS), NSA and DIA support. This second center would provide *tactical* indications and warning [DSB96:13].[8]

It is unlikely an operations center at DISA or NSA would receive much timely information directly from the Internet community. This is because most of the Internet is not within the area of control or responsibility of the DoD or NSA. In addition, monitoring of Internet activity *within* the U.S. may be completely outside the responsibility and authority of the DoD and NSA. As such, either this responsibility should be given to the CERT®/CC (or similar organization), or these operations centers should establish strong and timely liaison with the CERT®/CC and, to a lessor extent, other response teams.

In summary, because there is this growing need for information on Internet security incidents, and because the CERT®/CC is our only real source for comprehensive and timely information on Internet security incidents, this research supports continued funding of the CERT®/CC. More specifically, the research supports *increased* funding for the CERT®/CC, because of its capability to

---

[8] The difference between what is *strategic* and what is *tactical* is not clearly defined. In general, *strategic* is greater in scope and longer in duration than *tactical*.

provide timely strategic and tactical indications and warning, and because of the increase in total Internet security activity.

**14.4.4. Other Government Policies Supported by This Research** - This research supports government policies in two additional areas. First, the government should encourage Internet users to take the security precautions summarized in Section 14.2.5. Internet suppliers should also be encouraged to improve Internet security through the steps summarized in Section 14.3.4.

Second, this research shows that the government should take reasonable precautions to protect government data (just as other users). In addition, some government data is too sensitive to be available on the Internet, unless special precautions are taken. Stated another way, government employees should be required to take the same reasonable security precautions as other Internet users (summarized in Section 14.2.5).

## 14.5. Implications for Response Teams

The business of Internet incident response teams is *information.* They gather information relevant to Internet security, study that information, and selectively release information to the Internet community. This section presents an analysis of response team information policies based on theory and experience with this research. This analysis specifically examines the confidentiality policy of the CERT®/CC, but it is also generally applicable to other response teams. It begins with a discussion of the objectives of incident response, examines alternatives, and recommends changes to information release policies.[9]

**14.5.1. Objectives of Incident Response** - As discussed in Chapter 3, the CERT®/CC, and other response teams, provide products and services to the Internet in three areas: operations, education and training, and research and development. These are information producing activities in keeping with the three aspects of the CERT®/CC's charter, which is stated as follows (repeated from Chapter 3):

> The CERT® charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems [CER96:1].

The underlying motivation for the CERT®/CC charter, and the charter of other response teams, is to improve the security of the Internet. That is also the first objective of this research – to

[9] The theory follows the framework for analysis recommended by Stokey and Zeckhauser: establishing the context, laying out alternatives, predicting the consequences, valuing the outcomes, and making a choice [StZ78:5-6,320-329].

provide the suppliers and customers in the Internet community with more information about the history of Internet security incidents, security of Internet-related products and services will improve. Other objectives are also important. These objectives can be summed up as follows:

**Objective #1** - Improve the security of Internet products and services

**Objective #2** - Protect Internet sites from adverse publicity

**Objective #3** - Protect Internet sites from attacks

**Objective #4** - Gather information about Internet security problems and incidents

These are conflicting objectives. For example, if our only objective was the first one, to improve the security of Internet products and services, we would consider a policy of full disclosure of all incident response information. The intention would be to put pressure on Internet suppliers to improve the security of their products and services. This would likely, however, also result in undesirable outcomes, such as adverse publicity for sites identified, an increase in attacks at sites identified as being vulnerable, and increased reluctance to report vulnerabilities and incidents. Other conflicts emerge if different objective are emphasized.

Maintaining sources of information clearly has to be the most important of these objectives. If incident response personnel lose their sources of information, then they will have no information to use to improve Internet products and security, and to protect Internet sites from attack, except what information they can generate themselves.

These objectives will be used to value the alternative courses of action discussed in the next section in order to develop recommendations.

**14.5.2. Possible Alternative Courses of Action** - Providing information is a common approach used by the government to improve the working of a market [StZ78:310], as discussed in Section 14.4.1. As discussed, operation of the CERT®/CC is one measure the government is already taking to improve the operation of the Internet market by supplying information. The following analysis determined whether the amount and form of the information released by the CERT®/CC should be increased.[10] The information kept confidential by the CERT®/CC generally falls into three categories which will be treated as being mutually exclusive: site names, incident activity, and vulnerabilities. In the following sections, alternative courses of action will be presented in each of these categories. After a description of each alternative, predictions will be given of possible outcomes from the adoption of each alternative.

[10] No evidence could be found in the CERT®/CC records, or in publications, proposing the CERT®/CC release *less* information, so this alternative was not considered.

*14.5.2.1. Disclosure of Site Names* - Throughout the CERT®/CC records, actual site names were recorded. These included sites that reported incidents, other sites that were involved incidents but that were not aware of or did not report such involvement, and sites that were involved in incident response. Of course, the simple revealing of a site name is not sensitive. The Internet Domain Name System (DNS) generally makes site names publicly available. The specific restricted information is the association of a site name with either a vulnerability or with an incident.

CERT®/CC policy has been for there to be no association of site names with vulnerabilities or incidents. Not only did this mean that no site name associations were publicly released, but that site names were not revealed to other sites involved in the same incidents, unless a site specifically authorized the disclosure.[11] Possible alternatives to this policy are as follows:

*14.5.2.1.1. Alternative 1.1 - Full Disclosure of Site Names* - adoption of this alternative would eliminate all restrictions on the disclosure of site names. How this might actually be accomplished is open to speculation. One possibility would be to periodically release lists of sites with known vulnerabilities, and sites involved in known incidents.

The primary reason to adopt such an approach would be to put pressure on site administrators and Internet suppliers to improve site security and to improve the security of products and services. It is likely that system administrators of sites on the Internet would react to adverse publicity by securing their sites. This may be particularly true with sites that were vulnerable, but had not yet been attacked. This is because the public disclosure of the vulnerability may lead to attacks, since attackers would now have the information. Other things being equal, these attacks (or the potential for them) may pressure site administrators and, in turn, Internet suppliers. This may result in Internet suppliers providing products and services with improved security.

It is unlikely, however, that "other things" would be equal. Sites are very reluctant to reveal vulnerabilities or their involvement in incidents. Evidence of this can be seen in the very small number of incidents on the Internet that have been publicly reported. If sites were willing to be publicly identified, more information would have been publicly released. Under this policy, however, reporting vulnerabilities or incidents to a response team would be essentially equivalent to releasing the information publicly, since that is what the response team would do. The likely result of this policy would, therefore, be a reduction in information reported to response teams, and because of that, there would likely be little information for response teams to release publicly.

---

[11] CERT®/CC personnel would "neither confirm nor deny" the involvement of a site without authorization specifically from that site.

The final problem with this alternative would be the real possibility of response teams being held responsible for damage that resulted from attacks following disclosure of site information, unless there were special laws that protected the response teams from such liability.

In summary, the primary result of full disclosure of site names with known vulnerabilities and known incidents would be a reduction in the information available to the response teams. Those sites that were publicly identified, however, would be more likely to take increased security precautions. The larger effect would logically be the first because, if a response team has little information reported to it, then there will be few sites that are publicly reported. In other words, since response teams rely on *voluntary* disclosure from sites,[12] the benefits of full disclosure would likely be overwhelmed by the cost due to the loss of information.

***14.5.2.1.2. Alternative 1.2 - Partial Disclosure of Site Names*** - An alternative to full disclosure of site names would be to disclose only some site names. Using this proposal, response teams could establish, for example, that site names would not be reported unless the sites did not correct known vulnerabilities, take steps to secure their sites, or cooperate in incident response. This would provide sites an incentive to take timely corrective actions in order to avoid publicity. Liability problems for response teams would be reduced, as well as the amount of attacks that would result from the public disclosure. Other things being equal, this would result in greater security. The incentives for quick action by site administrators would, perhaps, be less than if Alternative 1.1 were chosen, because there would be less adverse publicity.

This proposal, however, also suffers from the same problem that the first proposal does: there would be less information flowing to response teams because of the threat of disclosure. The benefits of partial disclosure would likely be overwhelmed by the loss of information.

***14.5.2.1.3. Alternative 1.3 - Delayed Disclosure of Site Names*** - A second alternative to full disclosure of site names would be to disclose site names only after some period of time. After that period of time, either all site names would be disclosed, or only some subset. For example, response teams could establish that site names would not be reported unless the sites did not correct known vulnerabilities, take steps to secure their sites, or cooperate in incident response. This would provide sites the incentive to correct vulnerabilities and secure sites in a timely manner. Again, other things being equal, this may result in greater security. As with Alternative 1.2, the

[12] Two variants on this alternative involved greater changes and were considered unacceptable: *mandatory* reporting of vulnerabilities and incidents (unenforceable and a detriment to the Internet market), and active investigation of vulnerabilities and incidents by response teams (beyond their capability).

incentives for quick action by site administrators may be less because there would be less adverse publicity. On the other hand, this may be partially offset by the incentive to move quickly.

This proposal, however, also suffers from the same problem that the first two proposals do: there may be reduced information flowing to response teams because of the threat of disclosure. The benefits of delayed disclosure would likely be overwhelmed by the cost due to the loss of information.

***14.5.2.1.4. Alternative 1.4 - No Disclosure of Site Names*** - The fourth alternative is disclosure of site names only with specific authorization from the sites involved. The disclosures would only be to other sites involved in incidents. There would be no disclosure of sites with known vulnerabilities. This alternative represents the status quo.

This alternative should provide sites the least problems with reporting. If strictly adhered to, these confidentiality requirements should minimize concerns about adverse publicity and the possibilities for continued or increased attacks. Response teams could maximize the information they receive, although there would be less pressure on sites to increase security (other things being equal).

***14.5.2.1.5. Recommended Alternative for the Disclosure of Site Names*** - As stated earlier, gathering basic information about Internet security problems and incidents (objective #4) is key to fulfilling the charter of the CERT®/CC and other response teams. Alternative 1.4 should provide the most information to response teams. In addition, because of the loss of information, it is unclear that any of the other alternatives would result in increased security. They would also expose sites to adverse publicity and the potential for increased attacks. Therefore, it is recommended that there be no disclosure of sites names that appear in response team records or are otherwise reported to response teams (the status quo).

***14.5.2.2. Disclosure of Incident Activity*** - This research has involved the disclosure of incident activity during the period from the formation of the CERT®/CC in 1988 to the end of 1995. The records themselves, however, were not disclosed, but rather a summary of data extracted from the incident records, along with a classification and analysis of these data. This is the first time such data have been released by the CERT®/CC or any other response team. This in itself was a change in policy. In the past, the CERT®/CC has generally released no information about actual incidents, except to the sites involved. Even when this information was released to these sites, it was limited only to information of concern specifically to that one site. Among the participants, only incident response teams were generally able to see the actual scope of the

incidents. The exception to this was twelve CERT® advisories which give some information about specific incidents.[13]

The possible alternatives to this policy of limited disclosure of incident activity are discussed below. Disclosure of site names was treated as a separate issue in the previous section. As such, each of the alternatives below assumes that whatever material is released, it will not contain site names. The possible alternatives are as follows:

***14.5.2.2.1. Alternative 2.1 - Disclosure of Incident Summaries*** - As described in Chapter 4, incidents reported to the CERT®/CC were tracked in summary files kept on-line at the CERT®/CC. Once a week, closed incident records were removed from the on-line file and archived, and a copy of all open summaries was archived in a separate file. A similar process is probably used by other response teams. Adoption of this alternative would involve the releasing of these summaries on a periodic basis, perhaps weekly as they are archived.

All of these files, however, would have to have all site names removed. Experience with the files for this research showed that removing most of these site names is relatively easy, but *completely* removing references to site names is a difficult process. This is because the site names are not always accurately recorded, and they can be embedded anywhere in the records.

Assuming the files could be sanitized of site information on a regular basis, this research has also shown that the files would be of limited use. In order to determine the extent of an incident, other CERT®/CC files had to be searched for relationships. This same process would have to be done to form incidents out of the summary files if they were publicly released (the same process may have to be done with the records of other response teams).

This entire process makes this alternative impractical and of limited value. Any imperfections in removing the site names could also result in problems with liability and with sites becoming reluctant to provide information to response teams.

***14.5.2.2.2. Alternative 2.2 - Creation and Disclosure of Incident Files*** - A second alternative would be for response personnel to combine summaries together to form the incidents, as was done for the incidents studied in this research. This would eliminate the need for others to piece together the incidents. Instead, this would be done by personnel who have the most knowledge about an incident and would, therefore, be able to accomplish this task.

While this would be an improvement over the first alternative, it would also have similar problems. Site names would have to be eliminated from the files to be released, and any

[13] CERT® Advisories 89:03, 89:04, 90:02, 90:11, 91:04, 91:18, 92:03,92:14, 93:10, 94:01, 95:01, 95:18.

imperfections in removing the site names could result in problems with liability and with sites becoming reluctant to provide information to response teams. It would likely also have limited value in terms of the objectives for this analysis. This entire process makes this alternative impractical and of limited value.

***14.5.2.2.3. Alternative 2.3 - Development and Disclosure of Incident Data based on Incident Summaries*** - An alternative to the release of summary files would be to follow the data development process of this research further and develop and release data summary files and statistics. Response personnel would group the summary files together into incidents, extract data from these incidents (see Section 4.3), eliminate sites names, and then use a classification scheme, such as the taxonomy developed for this research, to classify, analyze and summarize these data. The files of extracted data as well as the data analysis would be released to the public.

There are two primary advantages to this alternative. Incident activity data would be released to the public in a useful, summary form and, the elimination of site names would be easier and more accurate. On the other hand, this research has shown this process to be difficult and time consuming. The next alternative addresses this concern.

***14.5.2.2.4. Alternative 2.4 - Development and Disclosure of Incident Data based on a Taxonomy*** - This alternative would involve the release of information that is similar to Alternative 2.3, but the information would be generated in a different manner.

By way of background, the research for this dissertation involved the examination and classification of incident records well after the incidents were closed. The information available for the process of constructing incident records, data extraction, and classification was limited to what was written into the summary files. During an incident, however, response personnel generally are more knowledgeable about the characteristics of the incident. More importantly, if information is missing, response personnel could take steps during the incident to acquire that information. For example, if an incident summary shows evidence of an intruder attempting access at a site, but no information about the level of success, response personnel could ask the site for more information about whether the attacks were successful at the root or account level. While response personnel may not always be able to obtain that information, they would be more successful than anyone either not involved in the incident, or attempting to determine this information after the incident was closed.

As such, this alternative proposes to have response personnel extract data and classify an incident while the incident is still open. Response personnel could gather data as recommended in

Chapter 13. Sites involved would be sanitized, as was done in this research, so that the actual site names are not revealed.

Recording of these data should be simple for response personnel, since they should have the information readily available. The use of an agreed-upon classification scheme (taxonomy) would be necessary. A possibility would be to use the taxonomy developed for this research. A better approach, and one advocated here, would be to use this taxonomy on an experimental basis over some period of time, with the intention of making practical improvements to the taxonomy. The goal would be to develop an accepted and simple scheme for data extraction and classification. The files of recorded data, as well as an analysis of these data would be released to the public.

This alternative has a positive outcome with respect to all of the objectives identified in Section 14.5.1, with significantly less work required by response personnel than other alternatives. Release of these data would provide more information to suppliers and customers, which may result in improvement in the security of Internet sites, products, and services. Individual sites would be protected from adverse publicity and further attacks. The release of these data may also make sites more likely to report information to response teams, because they would see the value in helping the data response teams release to be more complete and accurate.

***14.5.2.2.5. Alternative 2.5 - Limited Disclosure of Incident Activity*** - The final alternative considered was to make no change in current official policy. Under this alternative, the only incident activity information released would be high-level summary information released in CERT® advisories, and limited information to the sites involved in an incident. In light of the release of the information in this dissertation, it appears that CERT®/CC personnel are in favor of releasing more incident activity information, which achieves more of the objectives than this alternative.

***14.5.2.2.6. Recommended Alternative for the Disclosure of Incident Activity*** - Development and disclosure of incident data based on a taxonomy (Alternative 2.4), has a positive outcome with respect to all of the objectives. It achieves this with less work than other alternatives, and is, therefore, the preferred choice. Under this alternative, response personnel would take steps during the incident to extract data, eliminate site references, and classify the incident using the categories of a taxonomy. The files of recorded data, as well as any analysis of these data, would be released to the public.

A suggested approach to implementation would be to first develop and implement a program at the CERT®/CC. This would be followed by development and implementation at other response teams. A suggested schedule is as follows:

1. *Methodology development at the CERT®/CC* - During this period, CERT®/CC personnel would build on this current research, particularly the taxonomy, to develop a process for data extraction, classification, analysis and public release.

2. *Trial implementation at the CERT®/CC* - The process for data extraction, classification, analysis and public release should initially be fully implemented at the CERT®/CC for all incidents. During this trial period, CERT®/CC personnel would evaluate the process and the data generated, and implement improvements.

3. *Methodology development with other response teams* - After the trial period at the CERT®/CC, other FIRST response teams should be brought into the program. CERT®/CC personnel should meet with members of these other response teams and aid in the development of programs for their teams. Processes should also be developed for coordinating, sharing, reconciling, and analyzing information across the teams.

4. *Trial implementation at other response teams* - Another trial period should follow, this time involving CERT®/CC and other response teams. During this trial period, all teams would evaluate the process and the data generated, and coordinate and implement improvements.

5. *Public release and formalization* - After the development and trial periods are satisfactorily completed, other response teams, law enforcement agencies, and possibly other groups, should be encouraged to join this data generation and release process.

The end result of such an implementation would be the release of information that response teams, law enforcement agencies, analysts, policy makers, customers, and suppliers could use to improve the security of the Internet. For example, one possible use for a policy maker would be to see the results of policy changes. In this case, a policy change could be implemented and then the results could be tracked in the incident activity data.

***14.5.2.3. Disclosure of Vulnerabilities*** - The disclosure of vulnerabilities is the most controversial of the three areas of information that might be released by response teams. There is general agreement that site names should not be released, and there should be general agreement on the release of more information about incident activity. Disclosure of vulnerabilities is more difficult to agree on. If both the existence and the technical details of all vulnerabilities were fully disclosed, this would undoubtedly result in suppliers making a greater effort to secure their products. This would be because more attackers would probably be exploiting these vulnerabilities. As to whether this would lead to more or less security is unclear (and hotly debated).

There is certainly an asymmetry of information between attackers, response personnel, suppliers and customers when it comes to vulnerabilities. But just the existence of an asymmetry does not mean that policies should be implemented to change that asymmetry. A policy change could end up being detrimental to Internet security.

One possible alternative would be to have a layered and timed disclosure of vulnerabilities. In this case, only suppliers and others who could "repair" vulnerabilities would initially have full disclosure to them. After a "work-around" or patch were available, partial disclosure would be given to sites so their vulnerabilities could be eliminated. After some period of time, full disclosure would be made to put pressure on sites and suppliers to repair their vulnerabilities and to supply more secure products and services.

This research did not provide more information or greater insight into the possible disclosure of vulnerabilities. The research was of incident activity and not specifically vulnerabilities. These data could potentially be used for such studies, particularly if it were more complete (such as would be the case if Alternative 2.4 were implemented). For example, this research did not compare the disclosure of a vulnerability compared to its exploitation in Internet incidents (research recommended in Chapter 15). As such, it is recommended that response teams reexamine their policies toward the release of vulnerability information with the objective of seeing the degree to which more disclosure would benefit the Internet community.

***14.5.3. Other Implications for Response Teams*** - As was shown by this research, response teams get information on only part of the incidents that take place on the Internet. Total Internet activity can be estimated in several ways as discussed in Chapter 12. These estimates can be improved through a program involving voluntary reporting of incident activity at selected Internet sites as recommended in Section 12.3.2.

Response personnel should also evaluate the taxonomy for computer and network attacks developed for this research as discussed in Chapter 13.

### 14.6. Implications for the CERT®/CC

Previous sections and chapters have discussed several recommendations for actions by the CERT®/CC. These recommendations are summarized in this section. One recommendation that has not been discussed previously is for the CERT®/CC to publicly release the summary data set from this research. The data set developed for this research yielded valuable information about the state of Internet security. The analysis presented in this dissertation, however, is only a small part of what could potentially be done with the data. This is discussed further in Chapter 15. In order

to allow other researchers to use these data, it is recommended that the CERT®/CC make this data set available on line at www.cert.org.

A summary of the recommendations for the CERT®/CC from this research is as follows:

1. Maintain only one internal incident summary for each incident, open or closed.
2. Record a standard set of keywords and phrases that are defined, systematic and consistent, in each summary, such as reporting date, starting date, ending date, number of reporting sites, reporting sites, number of other sites, other sites, number of messages, attackers, tools, vulnerabilities, level, results, objectives, and corrective actions.
3. Classify each incident according to the worst level of unauthorized access or use.
4. Post the data set used in this research on line at www.cert.org.
5. Evaluate the taxonomy for computer and network attacks.
6. Develop and implement a program to better estimate total Internet incident activity. Such a program should involve the voluntary reporting of all incident activity at representative Internet sites. This program should include coordination and/or participation from other response teams and related organizations, such as DISA and AFIWC.
7. Estimate average number of attackers per incident, and their typical activity, in cooperation with personnel from DISA, AFIWC, and other response teams, in order to improve estimates of total Internet incident activity.
8. Do not disclose sites names that appear in the CERT®/CC records or are otherwise reported to the CERT®/CC (this is the status quo).
9. Disclose incident data based on a taxonomy. Suggested steps are as follows:
    1. *Methodology development at the CERT®/CC*
    2. *Trial implementation at the CERT®/CC*
    3. *Methodology development with other response teams*
    4. *Trial implementation at other response teams*
    5. *Public release and formalization*
10. Reexamine policies toward the release of vulnerability information with the objective of seeing the degree to which more disclosure would benefit the Internet community.

### 14.7. Summary of Policy Implications and Recommendations

This research clearly shows that the state of Internet security is not as bad as some authors have proposed. Both in terms of the absolute numbers of incidents, and in the growth of these incidents, the numbers are lower than popularly thought. In addition, most attacks were in the category of a nuisance (although some were a *big* nuisance), and not something more destructive or harmful.

Internet security incidents were, however, clearly not dropping to zero. The growth of Internet incidents in absolute terms was nearly at the same pace as the growth of the Internet.

Table 14.3 shows that, according to estimates from this research, a typical Internet domain is involved in *no more* than around *one incident per year*. In terms of hosts, the estimates of Table 14.3 show that a typical Internet host is involved in *no more* than around *one incident in every 45 years*. At the same time, however, it should be noted that some sites and hosts are more attractive to attack and may be involved in many incidents each year.

| | Low Estimate | High Estimate |
|---|---|---|
| **Individual Domain Involved** | 1 time in 15 years | 1 time in 0.8 years |
| **Individual Host Involved** | 1 time in 850 years | 1 time in 45 years |

**Table 14.3. Estimated Rate that an Internet Domain or Host was Involved in an Incident in 1995**

Given this steady but relatively small level of Internet security incidents, the average Internet user is not likely to be the victim of an Internet attack. Internet users should, however, take reasonable precautions to protect their files and data in transits on the Internet.

**Recommendations for all Internet users are as follows:**

1. Back up important files.
2. Use a good password for network access controls.
3. Ensure permissions are set properly on files that can be accessed by others.
4. Encrypt, or store off-line, files that are particularly sensitive.
5. Do not send sensitive user identifications, such as a social security number, address, phone number, personal data, or credit card number across the Internet unless it is encrypted at the source (prior to being sent across the Internet).
6. Use an encryption program, such as Pretty Good Privacy (PGP), if you want e-mail to be private.

**An additional recommendation for commercial Internet users is as follows:**

7. Conduct some form of risk analysis to determine the cost effective level of security.

**Recommendations for Internet suppliers are as follows:**

1. Provide protocols and software that encrypt user name, password and IP address combinations at the source, or provide an alternative to system that does not require passwords to be sent in the clear across the Internet.
2. Provide protocols and software that prevent access to files of encrypted passwords, or provide an alternative system that does not require encrypted passwords to be stored in files on systems accessible across the Internet.

3. Deliver systems to customers in a secure state.
4. Develop protocols and programs with reasonable protections against denial-of-service attacks.
5. Accelerate development of protocols and programs that provide reasonable privacy for such user programs as e-mail.

**Recommendations for the U.S. government are as follows:**

1. Increase funding for incident response, particularly the CERT®/CC.
2. Encourage Internet users to take simple security precautions.
3. Encourage Internet suppliers to improve Internet security.
4. Require government employees to take reasonable security precautions to protect sensitive data.

**Recommendations for Internet response teams are as follows:**

1. Do not disclose sites names reported to response teams (the status quo).
2. Disclose incident data based on a taxonomy.
3. Reexamine policies on the release of vulnerability information with the objective of seeing the degree to which more disclosure would benefit the Internet community.
4. Evaluate the taxonomy for computer and network attacks developed for this research.

**Recommendations for the CERT®/CC are as follows:**

1. Maintain only one internal incident summary for each incident, open or closed.
2. Record a standard set of keywords and phrases that are defined, systematic and consistent, in each summary, such as reporting date, starting date, ending date, number of reporting sites, reporting sites, number of other sites, other sites, number of messages, attackers, tools, vulnerabilities, level, results, objectives, and corrective actions.
3. Classify each incident according to the worst level of unauthorized access or use.
4. Post the data set used in this research on line at www.cert.org.
5. Evaluate the taxonomy for computer and network attacks developed for this research.
6. Develop and implement a program to better estimate total Internet incident activity. Such a program should involve the voluntary reporting of all incident activity at representative Internet sites. This program should include coordination and/or participation from other response teams and related organizations, such as DISA and AFIWC.
7. Estimate average number of attackers per incident, and their typical activity, in cooperation with personnel from DISA, AFIWC, and other response teams, in order to improve estimates of total Internet incident activity.
8. Do not disclose sites names that appear in the CERT®/CC records or are otherwise reported to the CERT®/CC (this is the status quo).

9. Disclose incident data based on a taxonomy. Suggested steps are as follows:
    1. *Methodology development at the CERT®/CC*
    2. *Trial implementation at the CERT®/CC*
    3. *Methodology development with other response teams*
    4. *Trial implementation at other response teams*
    5. *Public release and formalization*
10. Reexamine policies toward the release of vulnerability information with the objective of seeing the degree to which more disclosure would benefit the Internet community.

*Chapter 15*

# Future Research

This dissertation presents only a preliminary analysis of the data derived from the CERT®/CC incident records during 1989 to 1995. In the last chapter, it was recommended that the CERT®/CC make the summary data set available on-line at cert.org for use by other researchers. Possible research opportunities with this data set are as follows:

1. **Trends in the data over time** - Since the data set has historical information of Internet incidents over a seven-year period, there are many research opportunities involving an analysis of the trends in the data over time. This dissertation examined overall trends, such as root-level break-ins or denial-of-service attacks. These data could be analyzed in greater detail. For example, 22% of incidents reported problems with passwords. Did the type of problems change over time? It appears that they did, but this level of analysis was beyond the scope of this dissertation. Another example is the types of sites involved in incidents. There appears to be an increase in the percentage of commercial sites involved over time. Does this correspond to the increase in the percentage of Internet sites in the *.com* and *.net* domains, or is the trend different? Further research into trends in the data over time could yield additional interesting insights into Internet security.

2. **Comparison of Incident trends to other events** - CERT®/CC personnel speculate that the release of information about Internet security problems, such as in a CERT® advisory, influences incident activity. Dr. Dorothy Denning from Georgetown University suggested that law enforcement activities, such as "hacker crackdowns" may also influence the rate of Internet security activity.[1] Perhaps the rate that activity is recorded at the CERT®/CC is influenced by funding for incident response, or manning at the CERT®/CC. I have speculated that the World Wide Web growth after 1993 may be responsible for a decline in activity because Internet hackers now have more interesting things to do on the Internet than break into computers. Perhaps the activity was influenced by historical events such as Presidential elections, the weather, the economy, etc. These types of comparisons between Incident trends and other events remain unexplored.

3. **Implications of trends in the types of hosts (operating systems) on the Internet** - In the early days of the Internet, most hosts on the Internet used the Unix operating system. Over time, many hosts were added to the Internet that used operating systems that were not Internet attackable, such as DOS or Windows 3.1. Newer operating systems such as Windows 95 and

[1] Dr. Denning suggested I explore this relationship in the data when we met at a workshop at SAIC in 1996, but I was unable to investigate it.

Windows NT are more vulnerable. What are the implications of these trends? Should we expect increased problems as operating systems become capable of more integration on the Internet?

The findings of this research could be validated or extended through additional data. This could be accomplished as follows:

**4. Validation and extension through 1996 and 1997 CERT®/CC data** - This research included CERT®/CC records through 1995. It is recommended that CERT®/CC personnel generate summary data for release (see Chapter 13), probably beginning in 1998. As such, the records from 1996 and 1997 will remain unexplored. Extracting data from these records would provide a more complete picture.

**5. Validation and extension through data from other response teams** - Although other response teams have smaller constituencies, their data could provide additional valuable data.

Experience during this research has also indicated there are important areas of related research that remain largely unexplored. Among these are:

**6. Development of a heuristic for determining the scope of an incident** - As described in Chapter 13, an ad hoc process was used to determine the scope of an Internet incident both by the CERT®/CC, and for this research. This ad hoc process will not scale up as the Internet grows exponentially. Automated software tools will be necessary. This will probably require some capabilities in the field of artificial intelligence, particularly those capabilities for analyzing the content of text.

**7. Refinements of the taxonomy** - Use and evaluation of the proposed taxonomy by the CERT®/CC and other response teams was recommended in Chapter 14. Further research into the utility and validity of the taxonomy is recommended. One particular area of investigation would be to examine relationships between the categories of the taxonomy. Do certain tools pair up with certain types of access, results or objectives?

**8. Research into behavior of attackers** - As noted in Chapter 12, very little is known about the behavior of actual attackers. This is an open area of research that could significantly increase our understanding of Internet security attacks and incidents.

**9. Better sampling of Internet activity** - This research indicated that an accurate estimate of total Internet activity must be based on some sampling of the Internet. For this research, only two types of samples were available: the reports from Site A, and the DISA and AFIWC studies of the rate of reporting of attacks at DoD sites. Perhaps more rigorous and beneficial methods of sampling Internet security activity could be developed and implemented.

*Chapter 16*

# Conclusions and Recommendations

This research analyzed trends in Internet security through an investigation of 4,299 security-related incidents on the Internet reported to the CERT® Coordination Center (CERT®/CC) from 1989 to 1995. In 1988, the Defense Advanced Research Projects Agency (DARPA), established the CERT®/CC at CMU's Software Engineering Institute (SEI), in order to provide the Internet community a single organization to coordinate responses to security incidents on the Internet.

## 16.1. Contributions of this Research

Prior to this research, our knowledge of security problems on the Internet was limited and primarily anecdotal. This information could not effectively be used to determine what government policies and programs should be, or to determine the effectiveness of current policies and programs. This research brings us toward improved Internet security through:

1) development of a taxonomy for the classification of Internet attacks and Internet incidents
2) organization, classification (using the taxonomy), and analysis of the records available at the CERT®/CC concerning Internet security incidents
3) development of recommendations to improve Internet security and to gather and distribute useful information concerning Internet security

## 16.2. A Taxonomy of Computer and Network Attacks

A taxonomy of computer and network attacks was developed for this research in order to classify Internet security incidents. The taxonomy is based on a process viewpoint where an *attacker* attempts to link to ultimate *objectives*. This link is established through an operational sequence of *tools*, *access*, and *results*.

An *attack* is a single unauthorized access attempt, or unauthorized use attempt, regardless of success. An *incident*, on the other hand, involves a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing. The taxonomy developed for this research was to classify *attacks*. This taxonomy was used to in this research to classify attacks within Internet *incidents*. These incidents were also classified using other measures of severity.

The taxonomy developed for this research was found to be satisfactory.

## 16.3. Classification of Internet Incidents and Internet Activity

A total of 4,567 incidents over this 7 year period were reconstructed from the CERT®/CC records. This included 268 false alarms (5.9%), and 4,299 actual incidents (94.1%). Most of the

CERT®/CC incidents (89.3%) were unauthorized access incidents, which were further classified into their degree of success in obtaining access: *root break-in* (27.7%), *account break-in* (24.1%), and *access attempts* (37.6%). Relative to the growth in Internet hosts, each of these access categories was found to be *decreasing* over the period of this research: root-level break-ins at a rate around 19% less than the increase in Internet hosts, account-level break-ins at a rate around 11% less, and access attempts at a rate around 17% less.

Of the 4,299 actual incidents reported to the CERT®/CC, 458 (10.7%) were classified as unauthorized use incidents. These were further classified into *denial-of-service attacks* (2.4%), *corruption of information incidents* (3.1%), and *disclosure of information incidents* (5.1%). The growth in total unauthorized use incidents was around 9% per year greater than the growth in Internet hosts.

An alternative method of presenting the CERT®/CC incident information was developed for this research. For each incident, the average sites per day were calculated using the starting date, ending date and the total number of sites involved. These were then combined through the use of a custom computer program to find the total average sites per day for each classification of attack. The slope of the growth in all sites per day for all incidents, and for root- and account-level break-ins were both around 7% *less* than the growth rate in the number of Internet hosts.

### 16.4. Tools and Vulnerabilities

Recording of the use of tools and vulnerabilities in the CERT®/CC records was not systematic or complete. As a result, this information is incomplete. Some valuable information, however, can be obtained by determining the relative frequency that various tools and vulnerabilities appear in the CERT®/CC incident records.

A total of 778 incidents (18.1% of all incidents) reported the use of some tool. From these records, the largest category of tools was scripts or programs (15.4%). These consisted primarily of *Trojan horses* (10.5%) and *sniffers* (5.7%). The two general categories of toolkits were tools designed to exploit privileged or root access (1.2%), and *scanners* (2.6%). These tools appeared relatively late in the CERT®/CC records. The CERT®/CC records contain very few references to autonomous agents such as *worms*, and *viruses*.

Nearly half of the incidents in the CERT®/CC records mention specific vulnerabilities (45.3%). The most frequently recorded vulnerability involved various problems with passwords (21.8%). Most of the password vulnerabilities were in three categories: *password files*, which indicated that a password file had been copied (13.8%), *password cracking*, generally indicating that passwords had

been determined by the operation of a password cracking tool (10.4%), and *weak passwords*, which could easily be guessed (3.6%).

The reputation of *sendmail* and other mail transfer agents for being "plagued with security problems" was confirmed in the CERT®/CC incident records, which contain numerous references to *sendmail* (10.4%), *SMTP* (0.4%) and *mail* (7.7%). Problems with implementation of trusted hosts (such as *hosts.equiv* or *.rhosts* files) was recorded in a significant number of incidents (5.8%), as was *configuration* (5.7%), *TFTP* (5.5%), *NIS* and *YP* (4.0%), *FTP* (4.0%), and *NFS* (3.2%).

### 16.5. Severe Incidents

A criteria was developed for this research in order to identify the most severe incidents in the CERT®/CC records. The criteria were as follows: ≥ 79 days duration, ≥ 62 sites, and ≥ 87 messages. These criteria selected 22 incidents with an average of 203 days duration, which involved an average of 169 sites, and contained an average of 466 messages in the CERT®/CC record.

There were two predominant trends seen in the 22 severe incidents. First, the sophistication of intruder techniques progressed from simple user commands, scripts and password cracking, through the use of tools such as sniffers (1993) and toolkits (1994), and finally to intricate techniques that fool the basic operation of the Internet Protocol (1995). The second trend was that intruders became increasingly difficult to locate and identify. In the early incidents, the attackers tended to be a few individuals confined to a specific location or group of locations, and as a consequence, tended to be easily identifiable. As intruder tools became more sophisticated and the size of the Internet grew, the severe incidents involved more attackers operating in many different locations. The newest and most sophisticated techniques allowed the attackers to obtain nearly total obscurity.

For these 22 incidents, a three-phase process of attack was consistently used: 1) gain access to an account on the target system, 2) exploit vulnerabilities to gain privileged (root) access on that system, and 3) use this privileged access to attack other systems across the network.

### 16.6. Denial-of-Service Incidents

Since the Internet Worm during the first week of November 1988, there has not been another large-scale denial-of-service incident on the Internet. On the other hand, the CERT®/CC records do not give any indication that Internet denial-of-service incidents could not become widespread. Unlike other attacks reported to the CERT®/CC, denial-of-service incidents grew at a rate around 50% per year greater than the rate of growth of Internet hosts.

## 16.7. Estimates of Total Internet Incident Activity

Table 16.1 summarizes the estimates of total Internet incident activity based on this research. These estimates are for one year in 1995.

| Estimates of Total Internet Incidents per Year in 1995 | | |
|---|---|---|
| **Source** | **Low Estimate** | **High Estimate** |
| Based on Incidents per Host estimates at Site A | 16,800 | 22,800 |
| Based on attacks per incident 10 to 1,000, and DISA probability | 1,200 | 17,350 |
| Based on attacks per incident 10 to 1,000, and AFIWC probability | 1,200 | 1,630 |
| Based on DISA probability (Table 12.11) | 2,500 | 15,800 |
| Based on AFIWC probability (Table 12.9) | 1,400 | 2,400 |

**Table 16.1. Summary of Estimates of Total Internet Incident Activity**

Using the DISA probability of reporting an attack, the probability of any severe incident meeting the severe incident criteria *not* being reported to the CERT®/CC was between 0% and 4%. Using the AFIWC probability of reporting an attack, the probability of any severe incident meeting the severe incident criteria *not* being reported to the CERT®/CC was essentially zero. This confirms the impression the reports themselves give: that it is hard to conceive that a severe incident would not be reported to the CERT®/CC.

There were 394 incidents in the CERT®/CC records (9.2%) that were above average both in terms of duration (above 16.5 days) and in terms of the number of sites (above 6.5). When these incidents were isolated and analyzed, it showed that if we assume the DISA probability of report, then a minimum of around 1 out of 2.6 of the above average incidents were reported to the CERT®/CC (and nearly all of them may have been reported). If we assume the AFIWC probability, then it was estimated that less than 4% of these incidents were *not* reported to the CERT®/CC (and nearly all of them may have been reported).

## 16.8. Policy Implications and Recommendations

This research clearly showed that the state of Internet security is not as bad as some authors have proposed. Both in terms of the absolute numbers of incidents, and in the growth of these incidents, the numbers are lower than popularly thought. In addition, most attacks were in the category of a nuisance (although some were a *big* nuisance), and not something more destructive or harmful.

Internet security incidents were, however, clearly not dropping to zero. The growth of Internet incidents in absolute terms was nearly at the same pace as the growth of the Internet.

According to estimates from this research, a typical Internet domain is involved in *no more* than around *one incident per year*, as shown in Table 16.2. A typical Internet host is involved in *no more* than around *one incident in every 45 years*. At the same time, however, it should be noted that some sites and hosts are more attractive to attack and may be involved in many incidents each year.

| | Low Estimate | High Estimate |
|---|---|---|
| **Individual Domain Involved** | 1 time in 15 years | 1 time in 0.8 years |
| **Individual Host Involved** | 1 time in 850 years | 1 time in 45 years |

**Table 16.2. Estimated Rate that an Internet Domain or Host was Involved in an Incident in 1995**

Table 16.3 compares the risk of root-level break-ins to other typical risks.

| Risk | Estimated Rate Risk Occurs |
|---|---|
| Root Break-In, Internet Domain | 1 out of 10 years |
| Root Break-In, Internet Host | 1 out of 540 years |
| Convenience Store Robbery | 1 out of 1.5 years |
| Hard Disk Failure | 1 out of 75 years |
| 100 Year Flood | 1 out of 100 years |
| Serious Structural Fire, NY City | 1 out of 220 years |
| Death Due to Breast Cancer | 1 out of 6,224 years |
| Death in Motor Vehicle | 1 out of 6,250 years |
| Death Due to Fire, NY City | 1 out of 40,000 years |

**Table 16.3. Comparison of Estimated Rates That Risks Occur**

Given this steady but relatively small level of Internet security incidents, the average Internet user is not likely to be the victim of an Internet attack. Internet users should, however, take reasonable precautions to protect their files and data in transits on the Internet.

**Recommendations for all Internet users are as follows:**

1. Back up important files.
2. Use a good password for network access controls.
3. Ensure permissions are set properly on files that can be accessed by others.
4. Encrypt, or store off-line, files that are particularly sensitive.

5. Do not send sensitive user identifications, such as a social security number, address, phone number, personal data, or credit card number across the Internet unless it is encrypted at the source (prior to being sent across the Internet).
6. Use an encryption program, such as Pretty Good Privacy (PGP), if you want e-mail to be private.

**An additional recommendation for commercial Internet users is as follows:**

7. Conduct some form of risk analysis to determine the cost effective level of security.

Additional recommendations for Internet suppliers, the U.S. government, and response teams are as follows:

**Recommendations for Internet suppliers are as follows:**

1. Provide protocols and software that encrypt user name, password and IP address combinations at the source, or provide an alternative to system that does not require passwords to be sent in the clear across the Internet.
2. Provide protocols and software that prevent access to files of encrypted passwords, or provide an alternative system that does not require encrypted passwords to be stored in files on systems accessible across the Internet.
3. Deliver systems to customers in a secure state.
4. Develop protocols and programs with reasonable protections against denial-of-service attacks.
5. Accelerate development of protocols and programs that provide reasonable privacy for such user programs as e-mail.

**Recommendations for the U.S. government are as follows:**

1. Increase funding for incident response, particularly the CERT®/CC.
2. Encourage Internet users to take simple security precautions.
3. Encourage Internet suppliers to improve Internet security.
4. Require government employees to take reasonable security precautions to protect sensitive data.

**Recommendations for Internet response teams are as follows:**

1. Do not disclose sites names reported to response teams (the status quo).
2. Disclose incident data based on a taxonomy.
3. Reexamine policies on the release of vulnerability information with the objective of seeing the degree to which more disclosure would benefit the Internet community.
4. Evaluate the taxonomy for computer and network attacks developed for this research.

**Recommendations for the CERT®/CC are as follows:**

1. Maintain only one internal incident summary for each incident, open or closed.
2. Record a standard set of keywords and phrases that are defined, systematic and consistent, in each summary, such as reporting date, starting date, ending date, number of reporting sites, reporting sites, number of other sites, other sites, number of messages, attackers, tools, vulnerabilities, level, results, objectives, and corrective actions.
3. Classify each incident according to the worst level of unauthorized access or use.
4. Post the data set used in this research on line at www.cert.org.
5. Evaluate the taxonomy for computer and network attacks developed for this research.
6. Develop and implement a program to better estimate total Internet incident activity. Such a program should involve the voluntary reporting of all incident activity at representative Internet sites. This program should include coordination and/or participation from other response teams and related organizations, such as DISA and AFIWC.
7. Estimate average number of attackers per incident, and their typical activity, in cooperation with personnel from DISA, AFIWC, and other response teams, in order to improve estimates of total Internet incident activity.
8. Do not disclose sites names that appear in the CERT®/CC records or are otherwise reported to the CERT®/CC (this is the status quo).
9. Disclose incident data based on a taxonomy. Suggested steps are as follows:
    1. *Methodology development at the CERT®/CC*
    2. *Trial implementation at the CERT®/CC*
    3. *Methodology development with other response teams*
    4. *Trial implementation at other response teams*
    5. *Public release and formalization*
10. Reexamine policies toward the release of vulnerability information with the objective of seeing the degree to which more disclosure would benefit the Internet community.

### 16.9. Future Research

This dissertation presents only a preliminary analysis of the data derived from the CERT®/CC incident records during 1988 to 1995. It was recommended that the CERT®/CC make the summary data set available on-line at www.cert.org for use by other researchers. Possible research opportunities with this data set are as follows:

1. Analysis of trends in the data over time
2. Comparison of Incident trends to other events
3. Implications of trends in the types of hosts (operating systems) on the Internet

The findings of this research could be validated or extended through additional data. This could be accomplished as follows:

4. Validation and extension through 1996 and 1997 CERT®/CC data
5. Validation and extension through data from other response teams

Experience during this research has also indicated there are important areas of related research that remain largely unexplored. Among these are:

6. Development of a heuristic for determining the scope of an incident
7. Refinements of the taxonomy
8. Research into behavior of attackers
9. Better sampling of Internet activity

## *References*


[ABH96] Derek Atkins, Paul Buis, Chris Hare, Robert Kelley, Carey Nachenberg, Anthony B. Nelson, Paul Phillips, Tim Ritchey, and William Steen, *Internet Security Professional Reference*, New Riders Publishing, IN, 1996.

[Amo94] Edward G. Amoroso, *Fundamentals of Computer Security Technology*, Prentice-Hall PTR, Upper Saddle River, NJ, 1994.

[Bel89] Steve Bellovin, "Security Problems in the TCP/IP Protocol Suite," *Computer Communications Review*, vol. 19, no. 2, April, 1989, pp. 32-48.

[Cer93] Vinton G. Cerf, "Core Protocols," in *Internet System Handbook*, Daniel C. Lynch, and Marshall T. Rose, editors, Addison-Wesley Publishing Company, Inc., Greenwich, CT, 1993, pp. 79-155.

[CER92] *Computer Emergency Response Team Coordination Center*, brochure available from the CERT®/CC, Carnegie Mellon University, Pittsburgh, PA, 1992.

[CER96] *The CERT® Coordination Center FAQ*, available on the World Wide Web at *www.cert.org*, November, 1996.

[ChB94] William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley Publishing Company, Reading, MA, 1994.

[Coh95] Frederick B. Cohen, *Protection and Security on the Information Superhighway*, John Wiley & Sons, New York, 1995.

[DSB96] Defense Science Board, *Report of the Defense Science Board Task Force On Information Warfare - Defense (IW-D)*, Office of the Under Secretary of Defense for Acquisition and Technology, Washington, DC, November, 1996.

[FIR96] Forum of Incident Response Teams, *FIRST Team Contact Information*, available on the World Wide Web at *www.first.org*, November, 1996.

[Fri78] Milton and Rose Friedman, *Free to Choose: A Personal Statement*, Harcourt Brace Jovanovich, New York, 1978.

[GAO96] . . . . . ., *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD-96-84, Government Accounting Office, Washington, DC, May, 1996.

[GaS96] Simson Garfinkel and Gene Spafford, *Practical UNIX and Internet Security: Second Edition*, O'Reilly & Associates, Inc., 1996.

[Gil92] Daniel Gilly, *Unix in a Nutshell, System V Edition*, O'Reilly and Associates, Inc., Sebastopol, CA, 1992.

[Gra96] Matthew Gray, *Web Growth Summary*, published by the Massachusetts Institute of Technology and available at *http://www.mit.edu:8001/people/mkgray/net* on the Internet, June, 1996.

[Gue93] Gary L. Guertner, editor, Introduction to *The Search for Strategy: Politics and Strategic Vision*, Greenwood Press, Westport, CT, 1993.

[HoR91] P. Holbrook, and J. Reynolds, editors, *Site Security Handbook*, RFC 1244, available on the Internet from the Internet Engineering Task Force (IETF), and at numerous other sites.

[Hug95] Larry J. Hughes, Jr., *Actually Useful Internet Security Techniques*, New Riders Publishing, Indianapolis, IN, 1995.

[ISV95] David Icove, Karl Seger and William VonStorch, *Computer Crime: A Crimefighter's Handbook*, O'Reilly & Associates, Inc., Sebastopol, CA, 1995.

[Kum95] Sandeep Kumar, *Classification and Detection of Computer Intrusions*, Ph.D. Dissertation, Computer Sciences Department, Purdue University, Lafayette, IN, August, 1995.

[LaL96] Kurt F. Lauckner and Mildred D. Lintner, *Computers Inside and Out, Fifth Edition*, Pippin Publishing Ltd., Ann Arbor, MI, 1996.

[Lan81] Carl E. Landwehr, "Formal Models for Computer Security," *Computing Surveys*, Vol. 13, No. 3, September, 1981, pp. 247-278.

[LBM94] Carl E. Landwehr, Alan R. Bull, John P. McDermott, and William S. Choi, "A Taxonomy of Computer Security Flaws," *ACM Computing Surveys*, Vol. 26, No. 3, September, 1994, pp. 211-254.

[Lot92] Mark Lottor, *Internet Growth (1981-1991), Request for Comments 1296*, SRI International, Network Information Systems Center, January, 1992. Available on the Internet at *http://www.nw.com/zone/rfc1296.txt*.

[Lot96] Mark Lottor, *Internet Domain Survey, July, 1996*, produced by Network Wizards and published at *http://www.nw.com/zone/WWW* on the Internet.

[Lyn93] Daniel C. Lynch, "Historical Evolution," in *Internet System Handbook*, Daniel C. Lynch, and Marshall T. Rose, editors, Addison-Wesley Publishing Company, Inc., Greenwich, CT, 1993, pp. 3-14.

[LyR93] Daniel C. Lynch, and Marshall T. Rose, editors, *Internet System Handbook*, Addison-Wesley Publishing Company, Inc., Greenwich, CT, 1993.

[Mar91] John Markhoff, Dutch Computer Intruders Tap U.S. Files With Impunity," *New York Times*, April 21, 1991, p.A-1.

[McB96] Campbell R. McConnell, and Stanley L. Brue, *Economics: Principles, Problems, and Policies, 13th Edition*, McGraw-Hill, Inc., New York, 1996

[McK82] McKelvey, Bill, *Organization Systematics: Taxonomy, Evolution, Classification*, University of California Press, Berkeley, CA, 1982.

[Mer95] ....., *NSFNET Statistics*, produced by Merit Network Information Center Services, October 29, 1995, and published at *http://nic.merit.edu/nsfnet/statistics* on the Internet.

[Moc93] Paul V. Mockapetris, "Directory Services," in *Internet System Handbook*, Daniel C. Lynch, and Marshall T. Rose, editors, Addison-Wesley Publishing Company, Inc., Greenwich, CT, 1993, pp. 469-491.

[NYCa] Fire Department, City of New York, *Facts About the FDNY*, World Wide Web Site, *http://www.ci.nyc.ny.us/html/fdny/html/facts.html*, April, 1997.

[NYCb] Department of Buildings, New York City, *Home Page*, World Wide Web Site, *http://www.ci.nyc.ny.us/html/dob/html/dobabout.html*, April, 1997.

[NeP89] Peter Neumann and Donald Parker, "A Summary of Computer Misuse Techniques," *Proceedings of the 12th National Computer Security Conference*, 1989.

[Par90] Donald B. Parker, "The Trojan Horse Virus and Other Crimoids," in *Computers Under Attack: Intruders, Worms, and Viruses*, Peter J. Denning, editor, ACM Press, New York, NY, 1990, pp. 544-554.

[Per93] Radia Perlman, "Routing Protocols," in *Internet System Handbook*, Daniel C. Lynch, and Marshall T. Rose, editors, Addison-Wesley Publishing Company, Inc., Greenwich, CT, 1993, p. 180.

[PeW84] T. Perry and P. Wallich, "Can Computer Crime Be Stopped?," *IEEE Spectrum*, Vol. 21, No. 5.

[Pik97] Frank Pikelner, *Hard Drive Specs*, World Wide Web Site, *http://www.ariel.cs.yorku.ca/~frank/hd-specs.html*, April, 1997.

[RuG91] Deborah Russell and G. T. Gangemi, Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991.

[Sch94] Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, Thunder's Mouth Press, New York, NY, 1994.

[SHF90] Eugene H. Spafford, Kathleen A. Heaphy, and David J. Ferbrache, "A Computer Virus Primer," in *Computers Under Attack: Intruders, Worms, and Viruses*, Peter J. Denning, editor, ACM Press, New York, NY, 1990, pp. 316-355.

[ShM96] Tsutomu Shimomura and John Markoff, *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – By the Man Who Did It*, Hyperion, New York, NY, 1996.

[Sob95] Mark G. Sobell, *A Practical Guide to the UNIX System*, The Benjamin Cummings Publishing Company, Inc., Redwood City, CA, 1995.

[Sta91] "Dutch Hackers Hit Stanford," *Stanford Daily*, April 24, 1991.

[Sta95] William Stallings, *Network and Internetwork Security Principles and Practice*, Prentice Hall, Englewood Cliffs, NJ, 1995.

[StZ78] Edith Stokey and Richard Zeckhauser, *A Primer for Policy Analysis*, W. W. Norton & Company, Inc., New York, NY, 1978.

[Tan92] Andrew S. Tanenbaum, *Modern Operating Systems*, Prentice Hall, Englewood Cliffs, NJ, 1992.

[Til96] Ed Tiley, *Personal Computer Security*, IDG Books Worldwide, Inc., Foster City, CA, 1996.

[TsM96] Tsutomo Shimomura and John Markoff, *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – By the Man Who Did It*, Hyperion, New York, NY, 1996.

[USB96] U.S. Bureau of the Census, *Statistical Abstract of the United States: 1996 (116th Edition)*, Washington, DC, 1996.

[WhK96] Richard White and Greg Kincaid, *Information Warfare: An Overview of AFIWC Operations*, version 2.3, briefing at the USAF Academy, CO, February, 1996.

## *Appendix A*

## Summary of Methods of Operation

The following pages summarizes the methods of operations listed in the CERT®/CC records. Table A.1 presents the data in tabular form. This table shows the following for each category:

1. First report - The reporting date of the earliest incident where the method was recorded.
2. Mean Report - The mean reporting date for all incidents where the method was recorded.
3. Last Report - The reporting date of the last incident where the method was recorded.
4. Incidents - The total number of incidents reporting the method.
5. Delta - The difference between the Mean Reporting Dates for the incidents reporting the method and the Mean Reporting Date for all incidents.

This same data are plotted in Figures A.1 to A.41.

The methods of operation are indicated by keywords that were recorded in the CERT®/CC records. These keywords were classified within the taxonomy presented in Figure 3.6 of Chapter 3. This represents the organization of the data in Table A.1. This is also the organization of the Figures as follows:

*Attackers* - Figure A.1. *Access* - Figures A.9 to A.37. *Objectives* - Figure A.41.

*Tools* - Figures A.2. to A.8. *Results* - Figures A.39 to A.40

| Figure A.1. Methods of Operation | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| all | 1-Oct-88 | 24-Oct-93 | 30-Dec-95 | 4299 | 0 |
| Attackers | 14-Oct-89 | 19-Feb-93 | 15-Oct-95 | 35 | -246.9 |
| hackers | 14-Oct-89 | 29-May-92 | 6-Jul-95 | 18 | -513.1 |
| "carlos" | 14-Oct-89 | 14-Oct-89 | 14-Oct-89 | 1 | -1471.4 |
| Australian hackers | 21-Dec-89 | 21-Dec-89 | 21-Dec-89 | 1 | -1403.4 |
| "sw" cracker | 1-Mar-90 | 1-Mar-90 | 1-Mar-90 | 1 | -1333.4 |
| "lori" | 29-Mar-90 | 29-Mar-90 | 29-Mar-90 | 1 | -1305.4 |
| Dutch hackers | 1-Apr-90 | 1-Apr-90 | 1-Apr-90 | 1 | -1302.4 |
| "code blue" | 12-Jul-90 | 12-Jul-90 | 12-Jul-90 | 1 | -1200.4 |
| "majr" | 4-Mar-91 | 4-Mar-91 | 4-Mar-91 | 1 | -965.4 |
| "grok" | 24-Mar-92 | 24-Mar-92 | 24-Mar-92 | 1 | -579.4 |
| Portland hacker | 24-Feb-92 | 11-May-92 | 11-May-92 | 2 | -531.4 |
| "crackerhack" | 4-Nov-92 | 4-Nov-92 | 4-Nov-92 | 1 | -354.4 |
| Danish hackers | 12-Aug-93 | 12-Aug-93 | 12-Aug-93 | 1 | -73.4 |
| "prog" | 24-Nov-93 | 24-Nov-93 | 24-Nov-93 | 1 | 30.6 |
| Mitnick | 11-Jun-93 | 20-May-94 | 3-Jan-95 | 3 | 208.3 |
| "cracker buster" | 18-Apr-95 | 18-Apr-95 | 18-Apr-95 | 1 | 540.6 |
| "olga" | 6-Jul-95 | 16-Jun-95 | 6-Jul-95 | 1 | 599.6 |
| vandals - former employee | 19-Dec-90 | 28-Nov-93 | 15-Oct-95 | 17 | 34.9 |
| Tools | 4-Dec-88 | 28-Mar-94 | 24-Dec-95 | 778 | 155.2 |
| User command | 14-Apr-93 | 10-May-93 | 25-Jun-93 | 3 | -167.4 |
| Script or Program | 4-Dec-88 | 10-Feb-94 | 24-Dec-95 | 661 | 109.0 |
| to get root | 13-Sep-90 | 28-Jun-94 | 20-Dec-95 | 59 | 247.2 |
| moron program | 13-Sep-90 | 13-Sep-90 | 13-Sep-90 | 1 | -1137.4 |
| scr script | 10-Nov-92 | 10-Nov-92 | 10-Nov-92 | 1 | -348.4 |
| chesstool | 24-Sep-93 | 24-Sep-93 | 24-Sep-93 | 1 | -30.4 |
| gimme | 15-Jun-92 | 24-Dec-93 | 23-Jul-95 | 12 | 61.4 |
| getroot | 14-Jul-94 | 14-Jul-94 | 14-Jul-94 | 1 | 262.6 |
| chasin | 2-Nov-93 | 4-Sep-94 | 20-Dec-95 | 44 | 315 |
| froot | 28-May-95 | 28-May-95 | 28-May-95 | 1 | 580.6 |
| exploitation script | 25-Jul-95 | 14-Sep-95 | 5-Nov-95 | 2 | 690.1 |
| keystroke logging | 10-Mar-93 | 6-Jun-93 | 2-Sep-93 | 2 | -140.4 |
| logic bomb | 27-Feb-92 | 27-Feb-92 | 27-Feb-92 | 1 | -605.4 |
| DOS tools | 4-Jan-92 | 9-Sep-94 | 6-Dec-95 | 29 | 319.7 |
| crashme | 4-Jan-92 | 4-Jan-92 | 4-Jan-92 | 1 | -659.4 |
| lab program to crash system | 9-Mar-93 | 9-Mar-93 | 9-Mar-93 | 1 | -229.4 |
| nuke (icmp) | 13-Oct-92 | 10-Aug-94 | 6-Dec-95 | 13 | 289.7 |
| flash, ANSI escape sequences | 3-May-94 | 1-Jan-95 | 3-May-95 | 14 | 434.1 |
| pmcrash | 25-Sep-95 | 25-Sep-95 | 25-Sep-95 | 1 | 700.6 |
| password cracking | 14-Jan-92 | 15-Feb-94 | 19-Dec-95 | 52 | 113.6 |
| sniffer | 7-Sep-90 | 25-Oct-94 | 8-Dec-95 | 245 | 365.7 |
| dev/nit | 30-Aug-93 | 30-Aug-93 | 30-Aug-93 | 1 | -55.4 |
| ari | 27-Jan-94 | 27-Jan-94 | 27-Jan-94 | 1 | 94.6 |
| ari.nit | 12-Jan-94 | 25-Feb-94 | 2-May-94 | 1 | 123.9 |
| sniffer | 7-Sep-90 | 25-Oct-94 | 8-Dec-95 | 245 | 365.7 |
| tap | 3-May-95 | 3-May-95 | 3-May-95 | 1 | 555.6 |

**Table A.1. Methods of Operation (Continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| Trojan horse | 4-Dec-88 | 21-Nov-93 | 24-Dec-95 | 450 | 28.3 |
| trojan | 3-Sep-90 | 19-Jun-94 | 7-Dec-95 | 30 | 238.3 |
| trojan rcp | 30-Oct-89 | 30-Oct-89 | 30-Oct-89 | 1 | -1455.4 |
| trojan image | 31-Oct-90 | 31-Oct-90 | 31-Oct-90 | 1 | -1089.4 |
| trojan xnetd | 15-Jun-91 | 15-Jun-91 | 15-Jun-91 | 1 | -862.4 |
| trojan sysman | 18-Jan-90 | 9-Sep-91 | 4-Mar-93 | 3 | -775.7 |
| trojan uucp | 17-Jan-92 | 29-Feb-92 | 13-Apr-92 | 2 | -602.9 |
| trojan game | 7-Apr-92 | 7-Apr-92 | 7-Apr-92 | 1 | -565.4 |
| trojan sendmail | 16-Jul-92 | 16-Jul-92 | 16-Jul-92 | 1 | -465.4 |
| trojan pkzip | 12-Aug-92 | 12-Aug-92 | 12-Aug-92 | 1 | -438.4 |
| trojan keyenvoy | 1-Jan-93 | 1-Jan-93 | 1-Jan-93 | 1 | -296.3 |
| trojan telnet | 5-Dec-88 | 31-Mar-93 | 6-Dec-95 | 70 | -207.3 |
| trojan lpr | 2-Apr-93 | 2-Apr-93 | 2-Apr-93 | 1 | -205.4 |
| trojan sh | 24-May-93 | 24-May-93 | 24-May-93 | 1 | -153.4 |
| trojan ftp | 12-Aug-92 | 31-May-93 | 11-Nov-93 | 3 | -146.1 |
| trojan rsh | 16-Mar-92 | 25-Jun-93 | 28-Sep-95 | 5 | -121.0 |
| trojan sync | 11-May-92 | 17-Jul-93 | 23-Sep-94 | 2 | -98.9 |
| trojan lpd | 12-Feb-92 | 3-Sep-93 | 27-Mar-95 | 2 | -50.9 |
| trojan crontab | 18-Feb-93 | 25-Sep-93 | 2-May-94 | 2 | -29.4 |
| trojan named | 27-Oct-93 | 27-Oct-93 | 27-Oct-93 | 1 | 2.6 |
| trojan login | 4-Dec-88 | 31-Oct-93 | 8-Dec-95 | 251 | 7.5 |
| trojan libc | 17-Aug-92 | 28-Dec-93 | 6-May-95 | 7 | 65.3 |
| trojan wu-ftpd | 4-Feb-94 | 4-Feb-94 | 4-Feb-94 | 1 | 102.6 |
| trojan shutdown | 2-Mar-94 | 2-Mar-94 | 2-Mar-94 | 1 | 128.6 |
| trojan attempt | 22-May-94 | 22-May-94 | 22-May-94 | 1 | 209.6 |
| trojan su | 23-Mar-93 | 11-Jun-94 | 15-Mar-95 | 4 | 229.9 |
| trojan tcp-wrapper | 14-Jun-94 | 14-Jun-94 | 14-Jun-94 | 1 | 232.6 |
| trojan csh | 6-May-94 | 5-Sep-94 | 6-Jan-95 | 2 | 316.1 |
| trojan mail | 14-Sep-94 | 14-Sep-94 | 14-Sep-94 | 1 | 324.6 |
| trojan time | 30-Dec-93 | 14-Sep-94 | 10-Oct-95 | 4 | 324.9 |
| trojan ps | 23-Jul-92 | 27-Sep-94 | 8-Dec-95 | 53 | 338.4 |
| trojan rexecd | 20-Nov-92 | 11-Oct-94 | 26-Oct-95 | 6 | 352.1 |
| trojan defunct, trapdoor | 23-Sep-94 | 15-Dec-94 | 7-Feb-95 | 3 | 416.6 |
| trojan ifconfig | 11-Mar-94 | 17-Dec-94 | 10-Oct-95 | 17 | 418.7 |
| trojan ping | 19-Dec-94 | 19-Dec-94 | 19-Dec-94 | 1 | 420.6 |
| trojan loadmodule | 3-Jan-95 | 3-Jan-95 | 3-Jan-95 | 1 | 435.6 |
| trojan ls | 7-Feb-94 | 4-Jan-95 | 10-Oct-95 | 21 | 437.3 |
| trojan netstat | 14-Feb-94 | 7-Jan-95 | 10-Oct-95 | 10 | 439.8 |
| trojan finger | 9-Nov-94 | 8-Jan-95 | 15-Mar-95 | 6 | 441.4 |
| trojan find | 23-Jan-95 | 23-Jan-95 | 23-Jan-95 | 1 | 455.6 |
| trojan inet | 2-Mar-94 | 23-Jan-95 | 12-Dec-95 | 8 | 455.7 |
| trojan es | 26-Jan-95 | 26-Jan-95 | 26-Jan-95 | 1 | 458.6 |
| trojan syslog | 24-Feb-95 | 24-Feb-95 | 24-Feb-95 | 1 | 487.6 |
| trojan irc | 28-Jan-94 | 9-Mar-95 | 7-Dec-95 | 16 | 501.2 |
| trojan df | 30-Mar-95 | 30-Mar-95 | 30-Mar-95 | 1 | 521.6 |
| trojan du | 23-Jan-95 | 15-Apr-95 | 8-Dec-95 | 10 | 538.2 |
| trojan httpd | 24-May-95 | 24-May-95 | 24-May-95 | 1 | 576.6 |
| toolkit | 24-Jun-92 | 3-Feb-95 | 24-Dec-95 | 185 | 466.6 |
| to get root | 24-Jun-92 | 19-Feb-95 | 8-Dec-95 | 77 | 482.6 |
| limbo kit - to install trojans | 24-Jun-92 | 24-Jun-92 | 24-Jun-92 | 1 | -487.4 |
| toolkit - unspecified | 25-May-93 | 22-Oct-94 | 18-Sep-95 | 8 | 363.5 |
| rootkit | 30-Jan-94 | 15-Mar-95 | 8-Dec-95 | 68 | 506.9 |
| scanners | 24-Feb-93 | 26-Jan-95 | 24-Dec-95 | 111 | 459.2 |
| iss attempt, attack, scans | 24-Feb-93 | 2-Jan-95 | 24-Dec-95 | 93 | 434.8 |
| satan attempt, attack, scans | 14-Sep-94 | 7-Jun-95 | 10-Oct-95 | 21 | 590.9 |

| Table A.1. Methods of Operation (Continued) | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| autonomous agent | 4-Dec-88 | 24-Jan-94 | 24-Dec-95 | 567 | 91.6 |
| viruses | 14-May-91 | 20-Feb-94 | 20-May-95 | 5 | 119.0 |
| choosegirl.game | 14-May-91 | 14-May-91 | 14-May-91 | 1 | -894.4 |
| viruses | 1-Jul-93 | 5-Sep-94 | 20-May-95 | 3 | 315.9 |
| virus in mail | 19-Apr-95 | 19-Apr-95 | 19-Apr-95 | 1 | 541.6 |
| worm | 2-Nov-88 | 2-Jan-91 | 12-Jan-93 | 2 | -1026.4 |
| worm | 22-Dec-88 | 22-Dec-88 | 22-Dec-88 | 1 | -1767.4 |
| worm rumor | 12-Jan-93 | 12-Jan-93 | 12-Jan-93 | 1 | -285.4 |
| Access | 1-Oct-88 | 13-Oct-93 | 30-Dec-95 | 4078 | -11.0 |
| vulnerability | 1-Oct-88 | 15-Dec-93 | 30-Dec-95 | 1948 | 52.4 |
| autofinder | 2-Apr-90 | 2-Apr-90 | 2-Apr-90 | 1 | -1301.4 |
| autoreply | 5-Mar-94 | 10-Oct-94 | 27-Nov-95 | 13 | 350.7 |
| bin/shell | 29-Jun-90 | 12-Jan-93 | 23-Oct-95 | 15 | -285.1 |
| etc/alias | 29-Jun-90 | 29-Jun-90 | 29-Jun-90 | 1 | -1213.4 |
| unset | 17-Oct-91 | 17-Oct-91 | 17-Oct-91 | 1 | -738.4 |
| bin | 28-Feb-91 | 15-Jan-93 | 22-Aug-95 | 10 | -282.1 |
| alias | 3-Aug-93 | 3-Aug-93 | 3-Aug-93 | 1 | -82.4 |
| ksh | 10-Aug-94 | 10-Aug-94 | 10-Aug-94 | 2 | 289.6 |
| bugs | 2-Aug-90 | 30-Jul-93 | 25-Jun-95 | 4 | -85.6 |
| software bug | 2-Aug-90 | 11-Dec-92 | 22-Mar-94 | 3 | -317.1 |
| cisco bug | 25-Jun-95 | 25-Jun-95 | 25-Jun-95 | 1 | 608.6 |
| chfn/chsh | 1-Apr-90 | 4-Jan-93 | 10-Oct-95 | 2 | -293.4 |
| chsh/chfn | 1-Apr-90 | 1-Apr-90 | 1-Apr-90 | 1 | -1302.4 |
| chfn | 10-Oct-95 | 10-Oct-95 | 10-Oct-95 | 1 | 715.6 |
| configuration | 5-Dec-88 | 6-Feb-93 | 28-Dec-95 | 244 | -259.9 |
| open server | 5-Dec-88 | 28-Jan-92 | 22-Aug-95 | 96 | -634.5 |
| misconfiguration | 8-Jan-93 | 8-Jan-93 | 8-Jan-93 | 1 | -289.4 |
| configuration | 5-Dec-88 | 24-Sep-93 | 28-Dec-95 | 158 | -30.4 |
| weak sysadmin | 18-Sep-95 | 18-Sep-95 | 18-Sep-95 | 1 | 693.6 |
| crontab | 5-Feb-90 | 3-Aug-93 | 2-May-95 | 4 | -81.9 |
| decode, uudecode | 15-Mar-90 | 6-Jul-93 | 17-Nov-95 | 16 | -110.0 |
| uudecode | 15-Mar-90 | 2-Jun-92 | 14-Sep-94 | 4 | -509.1 |
| decode | 24-Sep-91 | 16-Nov-93 | 17-Nov-95 | 12 | 23.1 |
| dev | 20-Dec-91 | 2-Sep-93 | 18-May-95 | 2 | -51.9 |
| dev/tty | 18-May-95 | 18-May-95 | 18-May-95 | 1 | 570.6 |
| dev | 20-Dec-91 | 20-Dec-91 | 20-Dec-91 | 1 | -674.4 |
| dns | 14-Jun-92 | 10-Jan-94 | 5-Jun-95 | 5 | 78.4 |
| dns server | 14-Jun-92 | 14-Jun-92 | 14-Jun-92 | 1 | -497.4 |
| dns | 14-Aug-92 | 14-Aug-92 | 14-Aug-92 | 1 | -436.4 |
| root nameserver corruption | 19-Jul-94 | 19-Jul-94 | 19-Jul-94 | 1 | 267.6 |
| dns fraud | 6-Feb-95 | 6-Feb-95 | 6-Feb-95 | 1 | 469.6 |
| backup dns address | 5-Jun-95 | 5-Jun-95 | 5-Jun-95 | 1 | 588.6 |
| domain | 24-Aug-95 | 24-Aug-95 | 24-Aug-95 | 1 | 668.6 |
| dump | 7-Jul-94 | 24-Jul-94 | 10-Aug-94 | 2 | 272.6 |
| emacs | 30-Nov-92 | 30-Nov-92 | 30-Nov-92 | 1 | -328.4 |

**Table A.1. Methods of Operation (Continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| expreserve | 2-Sep-90 | 24-Sep-93 | 16-Jun-95 | 19 | -29.6 |
| finger | 4-Apr-91 | 15-Aug-94 | 14-Dec-95 | 28 | 295.1 |
| finger bombs | 7-Nov-92 | 7-Nov-92 | 7-Nov-92 | 1 | -351.4 |
| repeated fingers | 1-Feb-93 | 1-Feb-93 | 1-Feb-93 | 1 | -265.4 |
| finger storms | 20-Jan-94 | 20-Jan-94 | 20-Jan-94 | 1 | 87.6 |
| finger attempt | 4-Apr-91 | 29-Sep-94 | 10-Nov-95 | 14 | 339.6 |
| finger attack | 24-Oct-94 | 24-Oct-94 | 24-Oct-94 | 1 | 364.6 |
| finger | 25-Jul-91 | 26-Oct-94 | 14-Dec-95 | 10 | 367.2 |
| fork | 27-Oct-95 | 4-Nov-95 | 13-Nov-95 | 2 | 741.1 |
| forward | 15-Mar-90 | 20-Oct-92 | 13-Jan-95 | 6 | -369.4 |
| fparel | 16-Feb-93 | 16-Feb-93 | 16-Feb-93 | 1 | -250.4 |
| ftp | 1-Oct-88 | 7-Mar-93 | 24-Dec-95 | 170 | -230.7 |
| ftp attempts | 20-Mar-90 | 3-Jan-93 | 23-Nov-95 | 98 | -294.3 |
| ftp | 1-Oct-88 | 8-Mar-93 | 6-Dec-95 | 57 | -230.1 |
| anon ftp | 17-Jul-91 | 29-Apr-93 | 6-Apr-94 | 3 | -177.7 |
| ftpd | 17-Jul-91 | 29-Apr-93 | 6-Apr-94 | 3 | -177.7 |
| wuarchive ftp | 1-Mar-93 | 21-Feb-94 | 10-Oct-94 | 3 | 119.6 |
| unauthorized ftp | 27-May-94 | 27-May-94 | 27-May-94 | 1 | 214.6 |
| ftp bug | 19-Jun-92 | 4-Jul-94 | 24-Dec-95 | 4 | 253.4 |
| ftp configuration | 14-Dec-94 | 14-Dec-94 | 14-Dec-94 | 1 | 415.6 |
| ftp attacks | 10-Jul-94 | 23-Dec-94 | 16-Nov-95 | 3 | 424.9 |
| gopher | 14-Dec-92 | 18-Mar-94 | 27-Jan-95 | 9 | 145.0 |
| gopher, "more" | 14-Dec-92 | 5-Jan-94 | 27-Jan-95 | 2 | 72.6 |
| gopher abuse | 30-Jan-94 | 30-Jan-94 | 30-Jan-94 | 1 | 97.6 |
| gopher | 12-Aug-93 | 29-May-94 | 27-Jan-95 | 7 | 217.5 |
| history | 24-May-93 | 24-May-93 | 24-May-93 | 1 | -153.4 |
| http | 14-Sep-94 | 10-Jun-95 | 28-Dec-95 | 7 | 594.5 |
| http, http attempt | 14-Sep-94 | 23-Apr-95 | 28-Dec-95 | 5 | 546.0 |
| web bots | 27-Dec-95 | 27-Dec-95 | 27-Dec-95 | 1 | 793.6 |
| web abuse | 24-Jul-95 | 24-Jul-95 | 24-Jul-95 | 1 | 637.6 |
| icmp | 24-Mar-92 | 9-Jun-94 | 26-Dec-95 | 33 | 228.3 |
| icmp packet storm | 24-Mar-92 | 21-Feb-93 | 1-Nov-94 | 3 | -245.4 |
| icmp packet spoofing | 24-Feb-93 | 24-Feb-93 | 24-Feb-93 | 1 | -242.4 |
| icmp bomb | 13-Oct-92 | 4-Mar-94 | 6-Dec-95 | 12 | 130.9 |
| icmp | 22-Apr-92 | 2-Apr-94 | 31-Oct-95 | 6 | 159.8 |
| icmp attack | 13-May-93 | 12-Nov-94 | 23-Nov-95 | 9 | 384.0 |
| icmp attempts | 6-Apr-95 | 28-Jul-95 | 26-Dec-95 | 5 | 642.2 |
| ident | 3-Jul-95 | 3-Jul-95 | 3-Jul-95 | 1 | 616.6 |
| inetd | 21-Aug-93 | 3-May-94 | 14-Jan-95 | 2 | 191.1 |
| install | 5-Dec-88 | 5-Dec-88 | 5-Dec-88 | 1 | -1784.4 |
| kernal | 4-May-95 | 4-May-95 | 4-May-95 | 1 | 556.6 |
| libc | 13-Apr-92 | 23-Oct-93 | 28-Jun-95 | 6 | -0.9 |
| shared library | 13-Apr-92 | 23-Jun-93 | 21-Mar-94 | 5 | -123.4 |
| libc | 28-Jun-95 | 28-Jun-95 | 28-Jun-95 | 1 | 611.6 |
| loadmodule | 4-Apr-93 | 25-Nov-94 | 23-Nov-95 | 41 | 396.7 |

**Table A.1. Methods of Operation (Continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| irc | 12-Mar-91 | 16-Jun-94 | 23-Dec-95 | 72 | 234.9 |
| irc | 12-Mar-91 | 15-Apr-93 | 10-Oct-95 | 35 | -191.5 |
| botkillers | 1-Mar-94 | 1-Mar-94 | 1-Mar-94 | 3 | 127.6 |
| irc threats | 22-May-94 | 22-May-94 | 22-May-94 | 1 | 209.6 |
| irc flooding | 14-Sep-94 | 14-Sep-94 | 14-Sep-94 | 1 | 324.6 |
| irc abuse | 14-Jan-92 | 15-Nov-94 | 23-Dec-95 | 6 | 386.8 |
| irc bombs | 27-Dec-94 | 27-Dec-94 | 27-Dec-94 | 3 | 428.6 |
| irc bots | 27-Dec-94 | 19-Mar-95 | 7-Jun-95 | 1 | 510.9 |
| irc posting | 20-Feb-95 | 4-Apr-95 | 27-May-95 | 1 | 526.9 |
| irc script | 7-Mar-95 | 8-Apr-95 | 26-Apr-95 | 2 | 530.9 |
| irc help | 15-Apr-95 | 22-May-95 | 28-Jun-95 | 1 | 574.6 |
| login | 23-May-94 | 4-Jan-95 | 23-Oct-95 | 4 | 437.4 |
| bin/login | 23-May-94 | 19-Jul-94 | 15-Sep-94 | 2 | 268.1 |
| login -f | 21-Feb-95 | 21-Feb-95 | 21-Feb-95 | 1 | 484.6 |
| klogin | 23-Oct-95 | 23-Oct-95 | 23-Oct-95 | 1 | 728.6 |
| lp | 15-Apr-91 | 8-Aug-94 | 17-Dec-95 | 25 | 288.2 |
| lpd, lpd attack | 15-Apr-91 | 18-Sep-93 | 11-Apr-95 | 9 | -36.3 |
| lpr | 12-Oct-93 | 27-Jul-94 | 8-Dec-94 | 4 | 275.9 |
| lp | 31-May-91 | 13-Apr-95 | 17-Dec-95 | 12 | 535.6 |
| mail | 14-Nov-89 | 26-Jun-94 | 28-Dec-95 | 333 | 245.2 |
| massmail | 5-Mar-92 | 5-Mar-92 | 5-Mar-92 | 1 | -598.4 |
| secretmail | 7-Apr-92 | 17-Oct-92 | 20-Sep-93 | 3 | -372.4 |
| mail attempt | 8-Mar-93 | 8-Mar-93 | 8-Mar-93 | 1 | -230.4 |
| mail spoofing | 14-Nov-89 | 18-Apr-94 | 28-Dec-95 | 210 | 176.3 |
| mail bombs | 5-Oct-90 | 19-Aug-94 | 11-Dec-95 | 44 | 299.2 |
| mail fraud | 29-Nov-94 | 29-Nov-94 | 29-Nov-94 | 1 | 400.6 |
| mailrace | 23-Mar-94 | 18-Dec-94 | 28-Sep-95 | 36 | 420.4 |
| binmail | 23-Mar-94 | 21-Dec-94 | 13-Dec-95 | 39 | 423.3 |
| modify mail alias | 10-Jan-95 | 10-Jan-95 | 10-Jan-95 | 1 | 442.6 |
| mail abuse | 30-Jan-92 | 23-Feb-95 | 11-Dec-95 | 28 | 487.0 |
| anon mail | 10-Apr-95 | 10-Apr-95 | 10-Apr-95 | 1 | 532.6 |
| mail subscriptions | 5-Jan-95 | 7-Aug-95 | 28-Dec-95 | 4 | 652.1 |
| mail spam | 27-Sep-95 | 27-Sep-95 | 27-Sep-95 | 1 | 702.6 |
| majordomo | 14-Jun-94 | 22-Mar-95 | 28-Dec-95 | 2 | 513.6 |
| mem | 18-Jul-90 | 17-Apr-93 | 1-May-95 | 3 | -190.1 |
| dev/mem | 18-Jul-90 | 18-Jul-90 | 18-Jul-90 | 1 | -1194.4 |
| kmem | 3-Jan-94 | 1-Sep-94 | 1-May-95 | 2 | 312.1 |
| modload | 30-Jan-94 | 16-Feb-94 | 28-Feb-94 | 3 | 115.3 |
| motd | 3-Feb-92 | 5-Jun-92 | 21-Jan-93 | 3 | -505.7 |
| motd | 21-Feb-92 | 21-Feb-92 | 21-Feb-92 | 1 | -611.4 |
| etc/motd | 3-Feb-92 | 28-Jul-92 | 21-Jan-93 | 2 | -452.9 |
| mouse | 23-Sep-94 | 2-Apr-95 | 11-Oct-95 | 2 | 524.6 |
| mult | 14-Jun-92 | 1-Jul-93 | 20-May-94 | 10 | -114.8 |
| mult/div bug | 15-Aug-93 | 5-Jan-94 | 20-May-94 | 4 | -827.1 |
| mult bug | 14-Jun-92 | 26-Feb-93 | 5-Oct-93 | 6 | -239.9 |
| news | 22-Feb-93 | 25-Jan-94 | 4-Nov-94 | 3 | 93.3 |
| usr/lib/news/sys | 22-Feb-93 | 22-Feb-93 | 22-Feb-93 | 1 | -244.4 |
| long newsgroup name | 22-Mar-94 | 22-Mar-94 | 22-Mar-94 | 1 | 148.6 |
| newsh | 4-Nov-94 | 4-Nov-94 | 4-Nov-94 | 1 | 375.6 |

**Table A.1. Methods of Operation (Continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| nis | 4-May-90 | 29-Jun-94 | 19-Dec-95 | 103 | 248.0 |
| getpwname | 4-May-90 | 4-May-90 | 4-May-90 | 1 | -1269.4 |
| clients | 24-Feb-92 | 24-Feb-92 | 24-Feb-92 | 1 | -608.4 |
| nis attack | 15-Apr-92 | 16-May-94 | 20-Nov-95 | 39 | 203.9 |
| nis | 17-Jun-92 | 20-Jul-94 | 19-Dec-95 | 35 | 268.7 |
| nis attempt | 22-Dec-92 | 1-Nov-94 | 25-Oct-95 | 27 | 372.8 |
| nfs | 20-Sep-90 | 10-Jun-94 | 20-Dec-95 | 138 | 229.5 |
| nfs exports, exports | 24-Jan-92 | 25-Apr-92 | 27-Jul-92 | 2 | -546.9 |
| nfssnoops | 12-Aug-93 | 12-Aug-93 | 12-Aug-93 | 1 | -73.4 |
| showmount | 7-Nov-91 | 7-Jan-94 | 6-Apr-95 | 6 | 75.1 |
| mountd probes | 7-Feb-94 | 7-Feb-94 | 7-Feb-94 | 1 | 105.6 |
| mount | 16-Aug-93 | 16-Feb-94 | 23-Jun-94 | 4 | 114.6 |
| expsh | 25-Mar-94 | 25-Mar-94 | 25-Mar-94 | 1 | 151.6 |
| nfs mount attempts | 30-Jul-92 | 30-May-94 | 10-Oct-95 | 12 | 217.8 |
| mountd attempts | 14-Feb-94 | 5-Jun-94 | 27-Oct-94 | 5 | 224.4 |
| nfs attempts | 20-Sep-90 | 7-Jun-94 | 14-Sep-95 | 34 | 226.2 |
| nfs attack | 2-Jun-92 | 15-Jun-94 | 20-Dec-95 | 30 | 234.2 |
| automounter attempts | 22-Jun-94 | 22-Jun-94 | 22-Jun-94 | 1 | 240.6 |
| nfs mount attempts | 7-Jul-92 | 27-Jun-94 | 4-Jun-95 | 4 | 246.4 |
| nfs | 17-Jul-91 | 8-Aug-94 | 28-Nov-95 | 32 | 288.5 |
| mountd | 24-Feb-92 | 25-Oct-94 | 14-Sep-95 | 12 | 366.0 |
| nfs bug | 17-Aug-94 | 14-Nov-94 | 28-Feb-95 | 4 | 386.1 |
| netfind | 13-Apr-92 | 13-Apr-92 | 13-Apr-92 | 1 | -559.4 |
| nntp | 22-Oct-94 | 11-Nov-94 | 1-Dec-94 | 2 | 382.6 |
| ping | 1-Oct-88 | 10-Oct-93 | 31-Oct-95 | 14 | -14.2 |
| ping attack | 29-Jul-91 | 29-Jul-91 | 29-Jul-91 | 1 | -818.4 |
| ping | 1-Oct-88 | 13-Nov-93 | 31-Oct-95 | 9 | 19.6 |
| ping flood | 4-Feb-93 | 15-Dec-93 | 11-Nov-94 | 3 | 52.3 |
| ping bombs | 7-Aug-94 | 7-Aug-94 | 7-Aug-94 | 1 | 286.6 |
| pipe | 19-May-95 | 19-May-95 | 19-May-95 | 1 | 571.6 |
| portmap | 13-Nov-90 | 22-Dec-94 | 13-Dec-95 | 44 | 424.5 |
| portmapper | 13-Nov-90 | 23-Aug-93 | 8-Aug-94 | 9 | -62.3 |
| scans | 4-Nov-94 | 26-Mar-95 | 23-Aug-95 | 4 | 518.1 |
| potrmap | 14-Jun-94 | 28-Mar-95 | 13-Dec-95 | 20 | 519.8 |
| portmap attempts | 10-Aug-94 | 16-Apr-95 | 21-Nov-95 | 4 | 538.6 |
| port scan | 6-Apr-95 | 14-Aug-95 | 4-Dec-95 | 7 | 659.2 |
| ps | 6-Sep-95 | 6-Sep-95 | 6-Sep-95 | 1 | 681.6 |
| rcp | 29-Jun-89 | 29-Jun-89 | 29-Jun-89 | 1 | -1578.4 |
| rdist | 8-Nov-91 | 23-Nov-93 | 27-Nov-95 | 81 | 30.1 |
| rdist | 8-Nov-91 | 15-Nov-93 | 27-Nov-95 | 77 | 22.3 |
| rdist attempt | 15-Jul-93 | 3-Apr-94 | 22-Dec-94 | 2 | 161.1 |
| rdist attack | 12-Oct-93 | 2-May-94 | 21-Nov-94 | 2 | 190.1 |
| rexd | 13-Mar-92 | 16-Dec-93 | 31-Jan-95 | 8 | 53.1 |
| rexd | 13-Mar-92 | 24-Aug-93 | 2-Aug-94 | 6 | -60.6 |
| rexd attack | 14-Sep-94 | 14-Sep-94 | 14-Sep-94 | 1 | 324.6 |
| rexd attempt | 31-Jan-95 | 31-Jan-95 | 31-Jan-95 | 1 | 463.6 |

**Table A.1. Methods of Operation (Continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| rexec | 31-Jan-95 | 7-Jul-95 | 22-Oct-95 | 7 | 620.9 |
| exec attempts | 31-Jan-95 | 31-Jan-95 | 31-Jan-95 | 1 | 463.6 |
| exec | 19-Jun-95 | 19-Jun-95 | 19-Jun-95 | 1 | 602.6 |
| site exec | 4-Jul-95 | 4-Jul-95 | 4-Jul-95 | 1 | 617.6 |
| rexec | 24-Apr-95 | 21-Jul-95 | 18-Oct-95 | 2 | 635.1 |
| rexec attempts | 20-Aug-95 | 20-Sep-95 | 22-Oct-95 | 2 | 696.1 |
| rwall | 14-Mar-90 | 17-Aug-93 | 11-Jan-95 | 5 | -68.2 |
| rwall | 14-Mar-90 | 25-Mar-93 | 11-Jan-95 | 3 | -212.7 |
| rwall spoofing | 21-Feb-94 | 21-Feb-94 | 21-Feb-94 | 1 | 119.6 |
| rwalld | 20-Apr-94 | 20-Apr-94 | 20-Apr-94 | 1 | 177.6 |
| rpc | 25-Jul-91 | 16-Aug-94 | 13-Dec-95 | 35 | 295.9 |
| rpc getport | 12-Mar-93 | 12-Mar-93 | 12-Mar-93 | 1 | -226.4 |
| rpc mountd attack | 28-May-92 | 17-Apr-93 | 26-Apr-94 | 3 | -190.4 |
| sunrpc | 25-Jul-91 | 7-Oct-93 | 21-Dec-94 | 4 | -16.6 |
| rpc rusers connections | 29-Dec-93 | 29-Dec-93 | 29-Dec-93 | 1 | 65.6 |
| rpc info | 16-Aug-93 | 23-May-94 | 28-Feb-95 | 1 | 211.1 |
| rpc toolkit | 30-Jun-94 | 30-Jun-94 | 30-Jun-94 | 1 | 248.6 |
| rpc probes | 16-Jul-94 | 16-Jul-94 | 16-Jul-94 | 1 | 264.6 |
| rpc | 2-Mar-94 | 1-Jan-95 | 6-Dec-95 | 15 | 434.1 |
| rpc attempt | 12-Mar-93 | 2-Jan-95 | 13-Dec-95 | 7 | 434.6 |
| rpc scans | 8-Jan-95 | 8-Jan-95 | 8-Jan-95 | 1 | 440.6 |
| rsh/rlogin | 26-Mar-90 | 19-Sep-94 | 19-Dec-95 | 40 | 329.8 |
| rlogin attack | 18-Feb-93 | 18-Feb-93 | 18-Feb-93 | 1 | -248.4 |
| rsh/login attack | 26-Feb-93 | 26-Feb-93 | 26-Feb-93 | 1 | -240.4 |
| rlogin connections | 14-Sep-94 | 14-Sep-94 | 14-Sep-94 | 1 | 324.6 |
| rlogin | 26-Mar-90 | 27-Sep-94 | 30-Nov-95 | 26 | 338.4 |
| rsh/login | 25-Jul-94 | 15-Oct-94 | 6-Jan-95 | 2 | 356.1 |
| rsh attempt | 29-Jun-92 | 7-Feb-95 | 19-Dec-95 | 7 | 470.6 |
| rsh | 22-Jun-94 | 11-Jun-95 | 24-Oct-95 | 5 | 595.2 |
| sendmail | 1-Sep-89 | 25-Jul-94 | 26-Dec-95 | 447 | 274.3 |
| sendmail | 5-Dec-88 | 8-May-94 | 16-Dec-95 | 157 | 196.5 |
| sendmail debug | 24-Jul-89 | 22-Jul-94 | 10-Dec-95 | 34 | 271.0 |
| sendmail attacks | 1-Apr-90 | 12-Aug-94 | 26-Dec-95 | 51 | 291.6 |
| sendmail attempt | 15-Mar-90 | 15-Sep-94 | 20-Dec-95 | 238 | 326.3 |
| wiz | 6-Jun-94 | 8-Aug-95 | 4-Dec-95 | 18 | 652.9 |
| shutdown | 9-Mar-92 | 4-Aug-92 | 30-Dec-92 | 2 | -446.4 |
| smtp | 15-Feb-90 | 22-Apr-94 | 25-Aug-95 | 15 | 180.3 |
| mconnect | 15-Feb-90 | 15-Feb-90 | 15-Feb-90 | 1 | -1347.4 |
| smtp port | 16-Jan-94 | 16-Jan-94 | 16-Jan-94 | 1 | 83.6 |
| smtp attack | 2-May-94 | 2-May-94 | 2-May-94 | 1 | 189.6 |
| smtp | 25-Jul-91 | 28-May-94 | 7-Aug-95 | 5 | 216.0 |
| smtp attempt | 9-Jun-94 | 13-Nov-94 | 25-Aug-95 | 7 | 385.5 |
| snmp | 2-Sep-93 | 2-Oct-94 | 9-Sep-95 | 5 | 342.8 |
| cmp attack | 2-Sep-93 | 2-Sep-93 | 2-Sep-93 | 1 | -52.4 |
| snmp | 20-May-94 | 5-Jan-95 | 23-Aug-95 | 2 | 437.6 |
| snmp attempt | 19-May-94 | 13-Jan-95 | 9-Sep-95 | 2 | 445.6 |
| suid | 17-Aug-94 | 17-Aug-94 | 17-Aug-94 | 1 | 296.6 |
| syslog | 12-Nov-95 | 12-Nov-95 | 12-Nov-95 | 1 | 748.6 |

| Table A.1. Methods of Operation (Continued) | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| source hiding | 29-Aug-91 | 19-Aug-94 | 27-Dec-95 | 36 | 298.7 |
| source spoofing, attempts | 29-Aug-91 | 7-Mar-94 | 27-Dec-95 | 14 | 134.2 |
| source route spoofing | 15-Jul-94 | 15-Jul-94 | 15-Jul-94 | 1 | 263.6 |
| dns spoofing | 26-Sep-93 | 3-Aug-94 | 2-May-95 | 4 | 283.1 |
| tsutomo attack, tsutomo | 21-Mar-94 | 2-Oct-94 | 13-Jan-95 | 3 | 342.9 |
| ip spoofing | 5-Jun-92 | 17-Oct-94 | 10-Oct-95 | 9 | 358.4 |
| ip spoofing attempt | 3-Feb-95 | 25-Jul-95 | 20-Nov-95 | 7 | 638.7 |
| talk | 7-Apr-92 | 1-Nov-94 | 18-Oct-95 | 19 | 373.1 |
| talk abuse | 7-Apr-92 | 7-Apr-92 | 7-Apr-92 | 1 | -565.4 |
| talk request | 29-Dec-92 | 12-Apr-94 | 25-Jul-95 | 2 | 169.6 |
| talk attack | 27-Sep-94 | 13-Nov-94 | 31-Dec-94 | 2 | 385.1 |
| talk attempts | 20-Dec-94 | 20-Dec-94 | 20-Dec-94 | 1 | 421.6 |
| talk | 1-Nov-94 | 23-Dec-94 | 14-Feb-95 | 2 | 425.1 |
| talk bombs | 3-May-94 | 24-Dec-94 | 16-Aug-95 | 2 | 425.6 |
| talk flood | 24-Jul-94 | 27-Feb-95 | 18-Oct-95 | 9 | 491.3 |
| tcp | 17-Mar-94 | 11-Oct-94 | 19-Jun-95 | 4 | 352.4 |
| tcp ports | 12-Jul-94 | 12-Jul-94 | 12-Jul-94 | 1 | 260.6 |
| tcp packets bombs | 1-Dec-94 | 1-Dec-94 | 1-Dec-94 | 1 | 402.6 |
| tcp | 17-Mar-94 | 1-Nov-94 | 19-Jun-95 | 2 | 373.1 |
| telnet | 1-Sep-89 | 14-Jul-93 | 20-Dec-95 | 32 | -102.2 |
| 87 socket | 1-Apr-90 | 1-Apr-90 | 1-Apr-90 | 1 | -1302.4 |
| public telnet | 3-Sep-90 | 3-Sep-90 | 3-Sep-90 | 1 | -1147.4 |
| telnet | 1-Sep-89 | 24-Feb-93 | 20-Dec-95 | 14 | -241.6 |
| telnet attack | 26-Feb-93 | 14-Jul-93 | 10-Jul-94 | 6 | -102.1 |
| telnet bug | 11-Sep-93 | 11-Sep-93 | 11-Sep-93 | 1 | -43.4 |
| socket 7002 | 10-Jul-94 | 10-Jul-94 | 10-Jul-94 | 1 | 258.6 |
| telnet connections | 14-Sep-94 | 14-Sep-94 | 14-Sep-94 | 1 | 324.6 |
| port 25 | 22-Jul-92 | 18-Sep-94 | 4-Nov-95 | 3 | 328.6 |
| telnet attempts | 19-Sep-94 | 19-Sep-94 | 19-Sep-94 | 1 | 329.6 |
| telnet probes | 7-Dec-94 | 7-Dec-94 | 7-Dec-94 | 1 | 408.6 |
| port 167 | 4-May-95 | 4-May-95 | 4-May-95 | 1 | 556.6 |
| port 222 | 18-Aug-95 | 18-Aug-95 | 18-Aug-95 | 1 | 662.6 |
| telnet hijacking | 4-Sep-95 | 4-Sep-95 | 4-Sep-95 | 1 | 679.6 |
| time | 14-Jun-94 | 12-Aug-94 | 23-Sep-94 | 3 | 292.3 |
| time | 14-Jun-94 | 23-Jul-94 | 31-Aug-94 | 2 | 271.6 |
| bin/time | 23-Sep-94 | 23-Sep-94 | 23-Sep-94 | 1 | 333.6 |
| tftp | 1-Oct-88 | 5-Dec-92 | 25-Nov-95 | 238 | -322.7 |
| tftp attacks | 24-Jul-89 | 7-Oct-92 | 25-Nov-95 | 64 | -381.5 |
| tftp attempts | 5-Nov-89 | 14-Dec-92 | 22-Sep-95 | 143 | -313.8 |
| tftp | 1-Oct-88 | 9-Feb-93 | 17-Nov-95 | 30 | -256.9 |
| automated tftp | 15-May-94 | 15-May-94 | 15-May-94 | 1 | 202.6 |
| traceroute | 27-May-95 | 27-May-95 | 27-May-95 | 1 | 579.6 |
| trusted hosts | 5-Dec-88 | 4-Jul-93 | 24-Dec-95 | 249 | -112.2 |
| etc.hosts | 16-Feb-90 | 29-Sep-91 | 11-May-93 | 2 | -756.4 |
| gethost | 5-Nov-91 | 5-Nov-91 | 5-Nov-91 | 1 | -719.4 |
| show hosts | 2-Oct-92 | 2-Oct-92 | 2-Oct-92 | 1 | -387.4 |
| hosts.equiv | 1-Sep-89 | 28-Oct-92 | 28-Sep-95 | 52 | -361.3 |
| .rhosts, .rhost attempt | 5-Dec-88 | 16-Aug-93 | 24-Dec-95 | 210 | -68.8 |
| trusted hosts attack | 21-Mar-94 | 5-Nov-94 | 6-Feb-95 | 5 | 377.4 |
| hosts.allow | 15-Aug-95 | 15-Aug-95 | 15-Aug-95 | 1 | 659.6 |
| utmp | 27-Jan-95 | 27-Jan-95 | 27-Jan-95 | 1 | 459.6 |

**Table A.1. Methods of Operation (Continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| udp | 23-May-94 | 11-Mar-95 | 22-Oct-95 | 8 | 503.5 |
| udp | 23-May-94 | 16-Feb-95 | 22-Oct-95 | 4 | 479.6 |
| udp attempts | 18-Jan-95 | 4-Apr-95 | 23-Jun-95 | 4 | 527.4 |
| uucp | 27-Sep-90 | 9-Dec-92 | 23-Oct-95 | 9 | -319.3 |
| uucp attempt | 27-Sep-90 | 11-Aug-91 | 24-Jun-92 | 2 | -805.4 |
| uucp | 20-Aug-91 | 27-Apr-93 | 23-Oct-95 | 7 | -180.4 |
| windows nt | 21-Dec-95 | 24-Dec-95 | 30-Dec-95 | 3 | 790.6 |
| x | 13-Jan-91 | 26-Dec-93 | 23-Nov-95 | 11 | 62.6 |
| x file | 13-Jan-91 | 13-Jan-91 | 13-Jan-91 | 1 | -1015.4 |
| X11R5 bug | 20-May-92 | 20-May-92 | 20-May-92 | 1 | -522.4 |
| x11 attack | 13-Aug-93 | 16-Aug-93 | 19-Aug-93 | 2 | -69.4 |
| xterm | 5-Jan-94 | 25-Jan-94 | 15-Feb-94 | 2 | 93.1 |
| xtrek | 25-Mar-94 | 25-Mar-94 | 25-Mar-94 | 1 | 151.6 |
| xcat | 11-Apr-94 | 11-Apr-94 | 11-Apr-94 | 1 | 168.6 |
| x attack | 13-Apr-95 | 13-Apr-95 | 13-Apr-95 | 1 | 535.6 |
| xkey | 11-May-95 | 11-May-95 | 11-May-95 | 1 | 563.6 |
| x | 23-Nov-95 | 23-Nov-95 | 23-Nov-95 | 1 | 759.6 |
| yp | 9-Mar-92 | 27-Jan-94 | 19-Dec-95 | 69 | 94.8 |
| yppasswd | 9-Mar-92 | 21-Jun-92 | 4-Oct-92 | 2 | -489.9 |
| ypxfer | 4-Nov-92 | 4-Nov-92 | 4-Nov-92 | 1 | -354.4 |
| yp | 3-Jul-92 | 21-Sep-93 | 8-Jan-95 | 18 | -32.6 |
| ypsnarf | 6-Oct-92 | 12-Oct-93 | 23-Sep-94 | 8 | -12.3 |
| yp attempt | 24-Sep-93 | 31-Oct-93 | 8-Dec-93 | 2 | 7.1 |
| ypserv, ypserv attack | 22-Apr-93 | 26-Mar-94 | 12-Dec-94 | 17 | 153.1 |
| ypcat | 17-May-93 | 20-May-94 | 8-Dec-95 | 5 | 207.8 |
| ypx, ypx attempts | 19-Jun-92 | 28-Jul-94 | 19-Dec-95 | 15 | 277.0 |
| ypbind | 10-Oct-94 | 10-Oct-94 | 10-Oct-94 | 1 | 350.6 |
| ypbreak | 14-Oct-94 | 14-Oct-94 | 14-Oct-94 | 1 | 354.6 |
| misc/unknown | 20-Sep-89 | 8-Nov-93 | 8-Dec-95 | 26 | 15.3 |
| prompter | 20-Sep-89 | 20-Sep-89 | 20-Sep-89 | 1 | -1495.4 |
| analimddmp | 19-Dec-90 | 19-Dec-90 | 19-Dec-90 | 1 | -1040.4 |
| hhstore | 15-Apr-91 | 15-Apr-91 | 15-Apr-91 | 1 | -923.4 |
| rightslist.dat | 17-Apr-92 | 9-May-92 | 1-Jun-92 | 2 | -532.9 |
| dynamic linking | 20-May-92 | 20-May-92 | 20-May-92 | 1 | -522.4 |
| sysuaf | 1-Jun-92 | 1-Jun-92 | 1-Jun-92 | 1 | -510.4 |
| KVMsnf | 13-Jul-92 | 13-Jul-92 | 13-Jul-92 | 1 | -468.4 |
| systest | 29-Jul-92 | 29-Jul-92 | 29-Jul-92 | 1 | -452.4 |
| private/etc | 26-Feb-93 | 26-Feb-93 | 26-Feb-93 | 1 | -240.4 |
| internet discovery application | 19-May-93 | 19-May-93 | 19-May-93 | 1 | -158.4 |
| .runner | 3-Aug-93 | 3-Aug-93 | 3-Aug-93 | 1 | -82.4 |
| echo | 6-Apr-94 | 6-Apr-94 | 6-Apr-94 | 1 | 163.6 |
| prc | 17-May-94 | 17-May-94 | 17-May-94 | 1 | 204.6 |
| neil.bug | 17-May-94 | 17-May-94 | 17-May-94 | 1 | 204.6 |
| aup abuse | 18-May-94 | 18-May-94 | 18-May-94 | 1 | 205.6 |
| watch | 23-Mar-93 | 1-Jul-94 | 10-Oct-95 | 2 | 250.1 |
| inn bug attempt | 5-Jul-94 | 5-Jul-94 | 5-Jul-94 | 1 | 253.6 |
| simlink attempt | 11-Oct-94 | 11-Oct-94 | 11-Oct-94 | 1 | 351.6 |
| selection service | 6-May-95 | 6-May-95 | 6-May-95 | 1 | 558.6 |
| ropt | 4-Sep-95 | 10-Oct-95 | 21-Nov-95 | 3 | 716.3 |
| popper | 23-Oct-95 | 23-Oct-95 | 23-Oct-95 | 1 | 728.6 |
| rbone | 17-Nov-95 | 17-Nov-95 | 17-Nov-95 | 1 | 753.6 |
| tprof | 8-Dec-95 | 8-Dec-95 | 8-Dec-95 | 1 | 774.6 |

**Table A.1. Methods of Operation (Continued)**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| password vulnerability | 1-Oct-88 | 15-Jun-93 | 28-Dec-95 | 938 | -131.1 |
| password cracking | 20-Sep-89 | 20-Sep-89 | 20-Sep-89 | 1 | -1495.4 |
| password change | 22-Feb-91 | 30-Aug-92 | 1-Nov-94 | 22 | -420.1 |
| weak password(s) | 5-Dec-88 | 25-Nov-92 | 22-Dec-95 | 156 | -332.5 |
| no password(s) | 5-Dec-88 | 7-Mar-93 | 21-Dec-95 | 61 | -231.4 |
| password cracking | 1-Oct-88 | 10-Jun-93 | 28-Dec-95 | 448 | -136.4 |
| shared password | 10-Jun-91 | 11-Jul-93 | 13-Aug-95 | 11 | -104.6 |
| password file | 4-Dec-88 | 22-Jul-93 | 26-Dec-95 | 592 | -93.6 |
| default passwords | 22-Feb-93 | 10-Dec-93 | 27-Sep-94 | 2 | 46.6 |
| stolen password | 6-Aug-93 | 7-Feb-94 | 9-Aug-94 | 3 | 105.6 |
| cracked password | 10-Feb-94 | 5-Mar-94 | 29-Mar-94 | 2 | 132.1 |
| password(s) | 7-Jul-93 | 16-Mar-94 | 23-Nov-94 | 2 | 142.6 |
| captured password | 8-Apr-94 | 8-Apr-94 | 8-Apr-94 | 1 | 165.6 |
| shared account | 16-Feb-90 | 10-May-94 | 13-Dec-95 | 19 | 197.8 |
| eeprom password | 4-Jul-94 | 4-Jul-94 | 4-Jul-94 | 1 | 252.6 |
| password -f | 20-May-94 | 6-Dec-94 | 16-Sep-95 | 3 | 407.9 |
| passwdrace | 14-Sep-95 | 14-Sep-95 | 14-Sep-95 | 1 | 689.6 |
| access level | 1-Oct-88 | 19-Sep-93 | 30-Dec-95 | 3406 | -34.8 |
| student research project | 3-Dec-90 | 3-Dec-90 | 3-Dec-90 | 1 | -1056.4 |
| login attempts | 27-Jan-89 | 16-Jun-93 | 24-Dec-95 | 1080 | -130.1 |
| account breakin | 7-Dec-88 | 29-Jul-93 | 30-Dec-95 | 864 | -87.2 |
| probes | 1-Sep-93 | 1-Sep-93 | 1-Sep-93 | 1 | -53.4 |
| breakin | 23-Aug-90 | 16-Oct-93 | 21-Dec-95 | 187 | -7.9 |
| root breakin | 1-Oct-88 | 11-Dec-93 | 26-Dec-95 | 1188 | 48.0 |
| misuse | 1-Jul-93 | 31-Dec-93 | 15-Jul-94 | 6 | 67.8 |
| infrastructure attack | 1-Feb-94 | 2-Feb-94 | 3-Feb-94 | 2 | 100.6 |
| attempts | 26-May-92 | 26-Feb-94 | 7-Dec-95 | 31 | 124.7 |
| prank call | 17-Mar-94 | 17-Mar-94 | 17-Mar-94 | 1 | 143.6 |
| bbs, hacker bbs | 6-Mar-94 | 24-Mar-94 | 12-Apr-94 | 2 | 151.1 |
| router attack | 4-Mar-94 | 14-Jul-94 | 23-Nov-94 | 2 | 262.6 |
| dos attack, attempt, dos threat | 1-Jun-90 | 19-Aug-94 | 28-Dec-95 | 143 | 298.9 |
| account misuse | 23-Sep-94 | 23-Sep-94 | 23-Sep-94 | 1 | 333.6 |
| listservers | 14-Jun-95 | 14-Jun-95 | 14-Jun-95 | 1 | 597.6 |
| bbs posting | 27-May-95 | 31-Aug-95 | 5-Dec-95 | 2 | 675.6 |
| type of account | 5-Dec-88 | 22-Jul-93 | 24-Dec-95 | 223 | -94.4 |
| parity account | 31-Jan-90 | 31-Jan-90 | 31-Jan-90 | 1 | -1362.4 |
| demo account | 28-May-90 | 28-May-90 | 28-May-90 | 1 | -1245.4 |
| guest account | 25-Aug-89 | 15-Jun-91 | 13-Nov-95 | 35 | -861.5 |
| sync, sync account | 5-Dec-88 | 21-May-92 | 24-Dec-95 | 38 | -520.9 |
| field account, field | 7-Dec-90 | 10-Aug-92 | 15-Apr-94 | 2 | -439.9 |
| me account | 26-Feb-93 | 10-Apr-93 | 24-May-93 | 2 | -196.9 |
| system account | 5-Dec-88 | 23-Jun-93 | 21-Dec-95 | 53 | -123.0 |
| lp account | 13-Jun-93 | 29-Jan-94 | 25-May-94 | 3 | 97.3 |
| bin account | 25-May-94 | 25-May-94 | 25-May-94 | 1 | 212.6 |
| user account | 1-Apr-90 | 6-Jul-94 | 20-Dec-95 | 121 | 254.7 |
| uucp account | 21-Dec-94 | 21-Dec-94 | 21-Dec-94 | 1 | 422.6 |
| nobody | 27-Oct-95 | 27-Oct-95 | 27-Oct-95 | 1 | 732.6 |
| results | 2-Aug-89 | 5-May-94 | 26-Dec-95 | 419 | 193.2 |
| corruption of information | 2-Aug-89 | 3-Jan-94 | 26-Dec-95 | 170 | 71.2 |
| rm -rf | 1-Apr-90 | 1-Apr-90 | 1-Apr-90 | 1 | -1302.4 |
| shared files deleted | 9-Mar-92 | 9-Mar-92 | 9-Mar-92 | 1 | -594.4 |
| systems files deleted | 11-Feb-92 | 25-Apr-93 | 14-Sep-94 | 3 | -182.1 |
| suspicious files | 10-Sep-93 | 10-Sep-93 | 10-Sep-93 | 1 | -44.4 |
| files deleted | 21-Dec-89 | 7-Dec-93 | 13-Dec-95 | 71 | 44.1 |

**Table A.1. Methods of Operation (Continued)**

| | First Report | Last Report | Mean Report | Incidents | Delta |
|---|---|---|---|---|---|
| corruption of information (continued) | 2-Aug-89 | 3-Jan-94 | 26-Dec-95 | 170 | 71.2 |
| modify logs, deleted logs | 2-Aug-89 | 28-Jan-94 | 26-Dec-95 | 103 | 95.8 |
| all files deleted | 23-Mar-93 | 9-Mar-94 | 24-Feb-95 | 2 | 136.1 |
| gopher files replaced | 14-Jun-94 | 14-Jun-94 | 14-Jun-94 | 1 | 232.6 |
| files | 18-Jan-95 | 18-Jan-95 | 18-Jan-95 | 1 | 450.6 |
| cert.org summary cancel attempt | 27-Jul-95 | 27-Jul-95 | 27-Jul-95 | 1 | 640.6 |
| remove netnews messages | 31-Jul-95 | 31-Jul-95 | 31-Jul-95 | 2 | 644.6 |
| forge | 12-Nov-95 | 12-Nov-95 | 12-Nov-95 | 1 | 748.6 |
| disclosure of information | 1-Apr-90 | 20-Jul-94 | 22-Dec-95 | 252 | 269.5 |
| credit report (stolen) | 9-Dec-91 | 9-Jan-92 | 9-Feb-92 | 2 | -654.4 |
| info on bbs | 17-Aug-92 | 17-Aug-92 | 17-Aug-92 | 1 | -433.4 |
| disclosure issue | 24-Feb-93 | 24-Feb-93 | 24-Feb-93 | 1 | -242.4 |
| software piracy | 1-Apr-90 | 28-Jul-94 | 22-Dec-95 | 221 | 276.6 |
| credit report on irc | 4-Sep-94 | 4-Sep-94 | 4-Sep-94 | 1 | 314.6 |
| logs sent around net | 21-Sep-94 | 21-Sep-94 | 21-Sep-94 | 1 | 331.6 |
| warez | 17-Jun-92 | 13-Nov-94 | 22-Dec-95 | 73 | 385.3 |
| alt.2600 posting | 4-Mar-95 | 22-Mar-95 | 18-Apr-95 | 3 | 513.9 |
| copied files | 16-Mar-95 | 16-Jun-95 | 17-Sep-95 | 2 | 600.1 |
| theft of service | 6-Dec-88 | 29-Mar-94 | 22-Dec-95 | 290 | 155.9 |
| bogus newsgroup | 24-Sep-91 | 24-Sep-91 | 24-Sep-91 | 2 | -761.4 |
| 800# abuse | 21-Jun-90 | 10-Oct-91 | 22-Apr-94 | 3 | -745.4 |
| high phone bill | 18-Sep-92 | 18-Sep-92 | 18-Sep-92 | 1 | -401.4 |
| illegal bbs | 5-Dec-92 | 5-Dec-92 | 5-Dec-92 | 1 | -323.4 |
| unauthorized gateway use | 3-Feb-93 | 3-Feb-93 | 3-Feb-93 | 1 | -263.4 |
| mud | 25-Jul-91 | 16-Mar-93 | 28-Nov-94 | 4 | -221.9 |
| fidonet abuse | 12-Jul-93 | 12-Jul-93 | 12-Jul-93 | 1 | -104.4 |
| chain letter | 6-Dec-88 | 5-Nov-93 | 26-Jul-95 | 14 | 12.3 |
| bbs abuse | 26-Apr-94 | 26-Apr-94 | 26-Apr-94 | 1 | 183.6 |
| ftp abuse, anon ftp abuse | 7-Mar-90 | 5-May-94 | 22-Dec-95 | 263 | 193.2 |
| account added | 23-Aug-94 | 23-Aug-94 | 23-Aug-94 | 1 | 302.6 |
| denial of service | 10-Mar-90 | 17-Mar-94 | 15-Oct-95 | 6 | 144.1 |
| deleted accounts | 10-Mar-90 | 9-Mar-93 | 15-Oct-95 | 3 | -229.1 |
| halt system | 14-Sep-94 | 14-Sep-94 | 14-Sep-94 | 1 | 324.6 |
| system crash | 5-May-95 | 30-Jun-95 | 25-Aug-95 | 2 | 613.6 |
| objectives | 17-Apr-91 | 13-Mar-94 | 16-Nov-95 | 56 | 140.2 |
| financial gain | 17-Apr-91 | 15-Mar-94 | 16-Nov-95 | 44 | 141.7 |
| industrial sabatoge | 12-Nov-92 | 12-Nov-92 | 12-Nov-92 | 1 | -346.4 |
| extorsion threat | 2-Dec-92 | 31-Mar-93 | 29-Jul-93 | 2 | -206.9 |
| scam | 22-Feb-93 | 28-Sep-93 | 21-Jan-94 | 3 | -26.4 |
| fraud | 11-Jul-93 | 2-Nov-93 | 1-Jun-94 | 3 | 8.9 |
| credit card fraud | 17-Apr-91 | 24-Nov-93 | 16-Nov-95 | 27 | 30.6 |
| industrial espionage | 25-Jul-94 | 25-Jul-94 | 25-Jul-94 | 1 | 273.6 |
| embezzlement | 29-Nov-94 | 29-Nov-94 | 29-Nov-94 | 1 | 400.6 |
| isp rivalry, isp | 20-Jun-95 | 5-Jul-95 | 27-Jul-95 | 6 | 619.3 |
| damage | 7-Oct-93 | 7-Jan-95 | 9-Nov-95 | 12 | 439.9 |
| harassment | 7-Oct-93 | 7-Oct-93 | 7-Oct-93 | 1 | -17.4 |
| damage | 30-Jun-94 | 30-Jun-94 | 30-Jun-94 | 1 | 248.6 |
| threat | 10-Jan-94 | 26-Jan-95 | 8-Nov-95 | 8 | 458.9 |
| arson threat | 17-Jul-95 | 17-Jul-95 | 17-Jul-95 | 1 | 630.6 |
| feud | 9-Nov-95 | 9-Nov-95 | 9-Nov-95 | 1 | 745.6 |

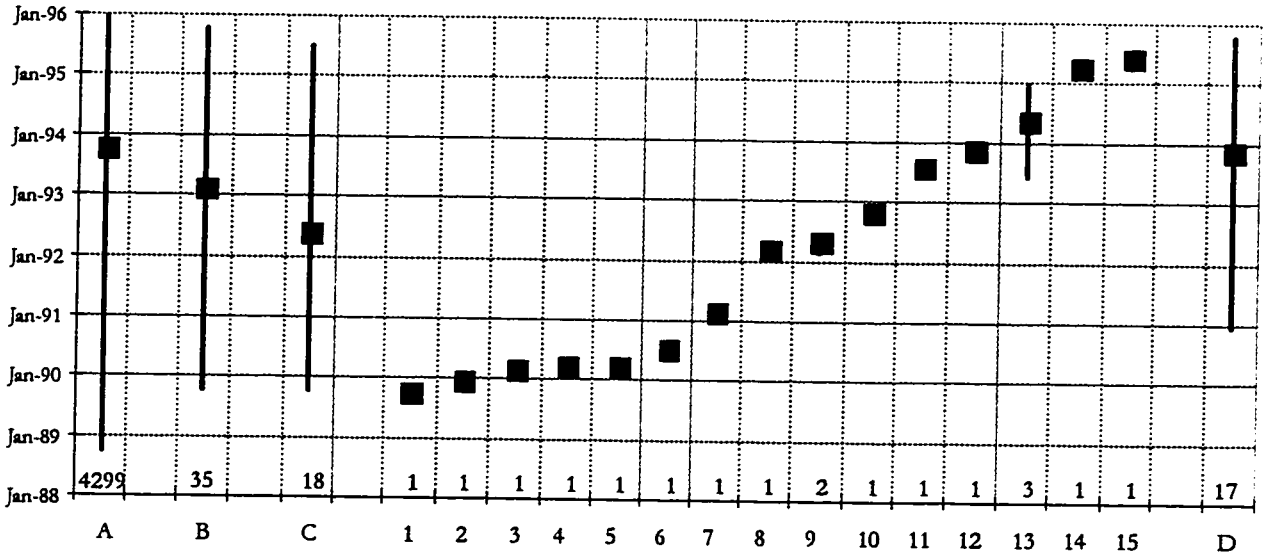


**Figure A.1. Range and Mean Incident Start for Methods of Operation - Attackers**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 3 - "sw" cracker | 8 - "grok" | 13 - Mitnick |
| B - All Attackers | 4 - "lori" | 9 - Portland hacker | 14 - "cracker buster" |
| C - All Hackers | 5 - Dutch hackers | 10 - "crackerhack" | 15 - "olga" |
| 1 - "Carlos" | 6 - "code blue" | 11 - Danish hackers | D - All Vandals - Former Employees |
| 2 - Australian hackers | 7 - "majr" | 12 - "prog" | |

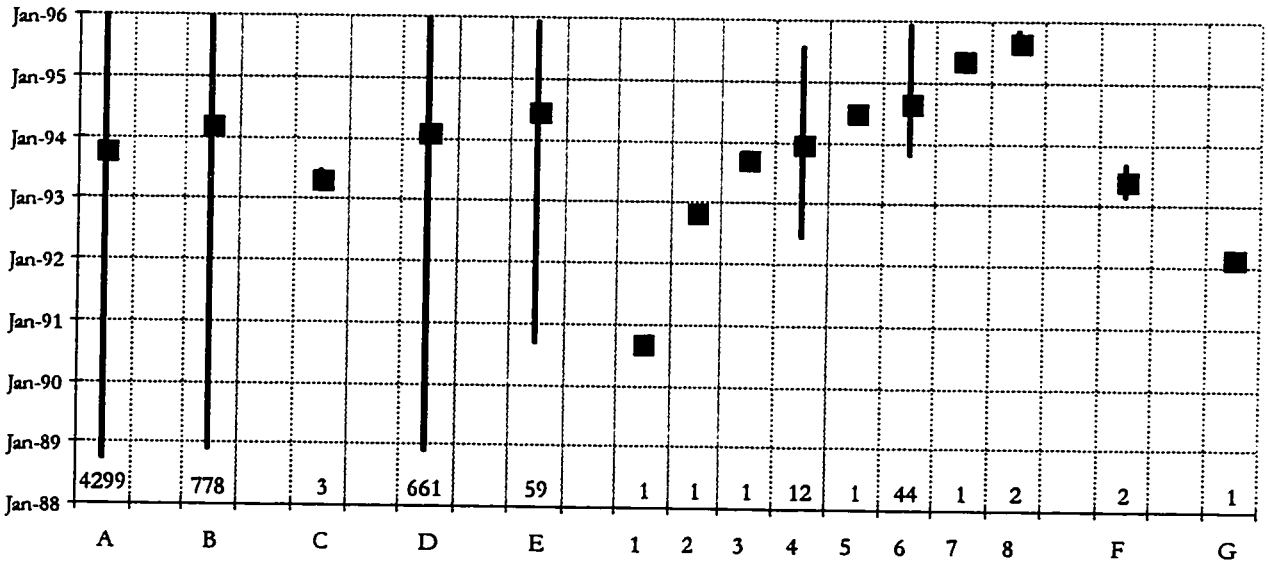


**Figure A.2. Range and Mean Incident Start for Methods of Operation - Tools - Part 1**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | E - To get root | 4 - *gimme* | 8 - *exploitation* script |
| B - All Tools | 1 - *moron* program | 5 - *getroot* | F - Keystroke logging |
| C - All User commands | 2 - *scr* script | 6 - *chasin* | G - Logic bomb |
| D - All Scripts or Programs | 3 - *chesstool* | 7 - *froot* | |

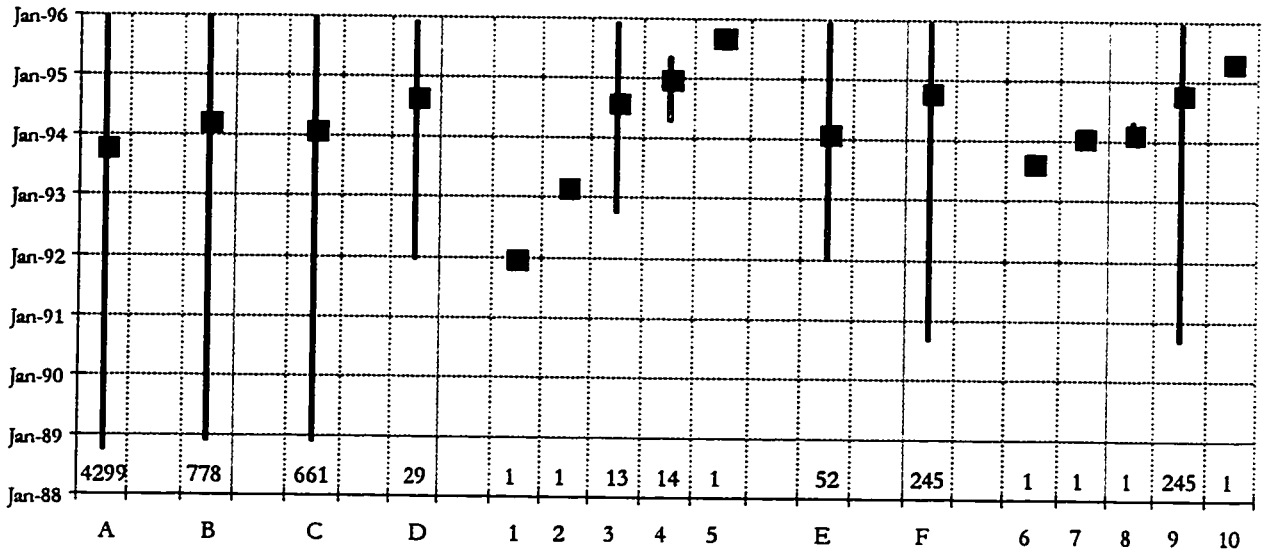


**Figure A.3. Range and Mean Incident Start for Methods of Operation - Tools - Part 2**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Tools**
**C - All Scripts or Programs**
**D - All DOS Tools**
**1 - *crashme***
**2 - *lab* program to crash system**
**3 - *nuke* program (icmp)**
**4 - *flash* program, ANSI escape sequences**
**5 - *pmcrash* program**
**E - *Crack* password**
**6 - dev/nit**
**7 - ari**
**8 - ari.nit**
**9 - sniffer**
**10 - tap**

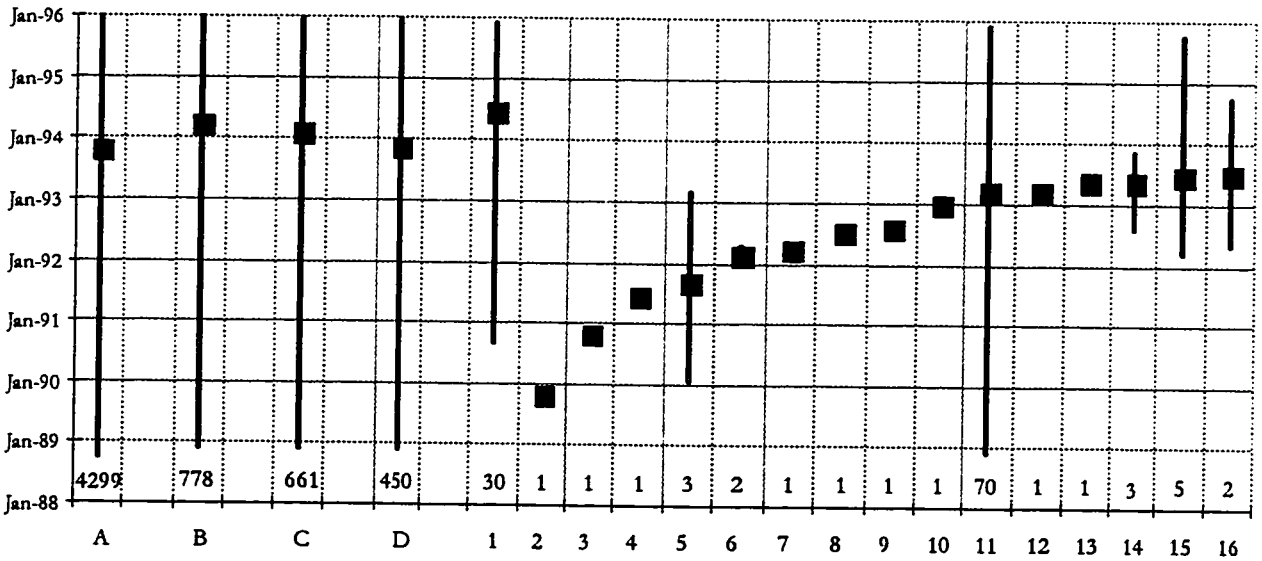


**Figure A.4. Range and Mean Incident Start for Methods of Operation - Tools - Part 3**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Tools**
**C - All Scripts or Programs**
**D - All Trojan Horses**
**1 - Trojan, unspecified**
**2 - trojan rcp**
**3 - trojan image**
**4 - trojan xnetd**
**5 - trojan sysman**
**6 - trojan uucp**
**7 - trojan game**
**8 - trojan sendmail**
**9 - trojan pkzip**
**10 - trojan keyenvoy**
**11 - trojan telnet**
**12 - trojan lpr**
**13 - trojan sh**
**14 - trojan ftp**
**15 - trojan rsh**
**16 - trojan sync**

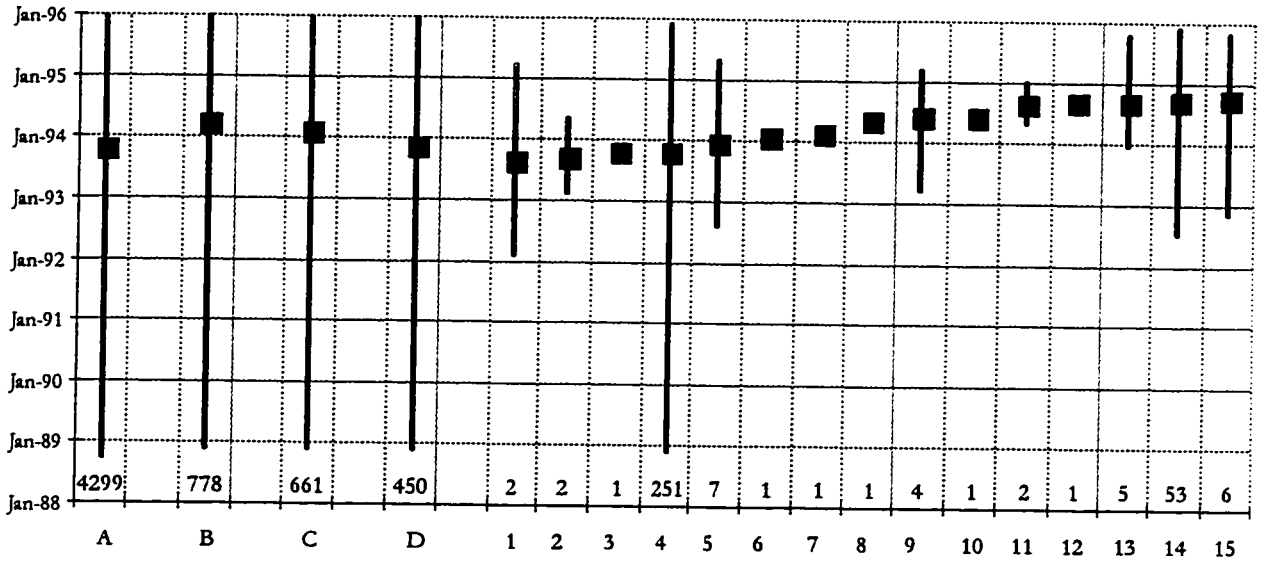


**Figure A.5. Range and Mean Incident Start for Methods of Operation - Tools - Part 4**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - Trojan crontab | 7 - Trojan shutdown | 12 - Trojan mail |
| B - All Tools | 3 - Trojan named | 8 - Trojan attempt | 13 - Trojan time |
| C - All Scripts or Programs | 4 - Trojan login | 9 - Trojan su | 14 - Trojan ps |
| D - All Trojan Horses | 5 - Trojan libc | 10 - Trojan tcp-wrapper | 15 - Trojan rexecd |
| 1 - Trojan lpd | 6 - Trojan wu-ftpd | 11 - Trojan csh | |

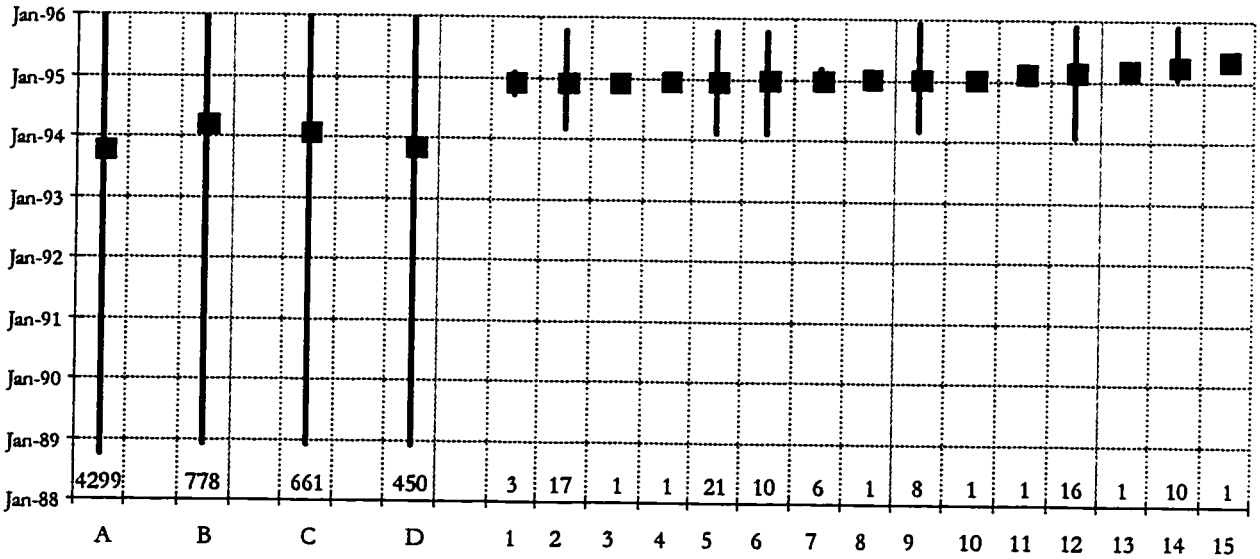


**Figure A.6. Range and Mean Incident Start for Methods of Operation - Tools - Part 5**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - Trojan ifconfig | 7 - Trojan finger | 12 - Trojan irc |
| B - All Tools | 3 - Trojan ping | 8 - Trojan find | 13 - Trojan df |
| C - All Script or Programs | 4 - Trojan loadmodule | 9 - Trojan inet | 14 - Trojan du |
| D - All Trojan Horses | 5 - Trojan ls | 10 - Trojan es | 15 - Trojan httpd |
| 1 - Trojan defunct, trapdoor | 6 - Trojan netstat | 11 - Trojan syslog | |

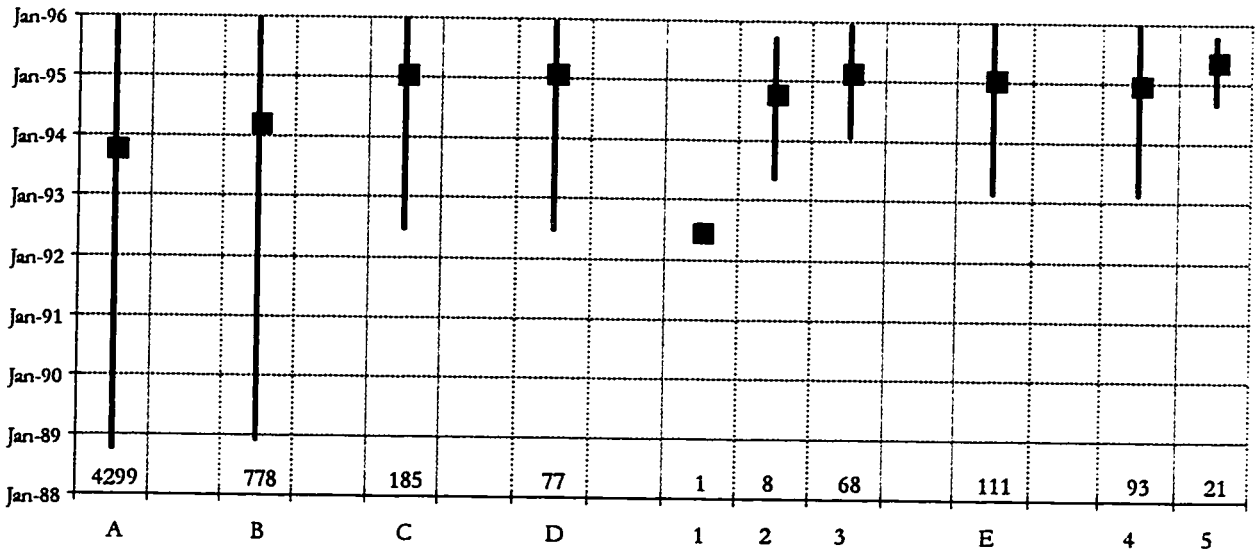


**Figure A.7. Range and Mean Incident Start for Methods of Operation - Tools - Part 6**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **D - To get root** | **3 -*rootkit*** | **4 - *ISS* attempt, attack, scans** |
| **B - All Tools** | **1 - *limbo* kit to install Trojans** | **E - All scanners** | **5 - *SATAN* attempt, attack, scans** |
| **C - All Toolkits** | **2 - toolkit - unspecified** | | |

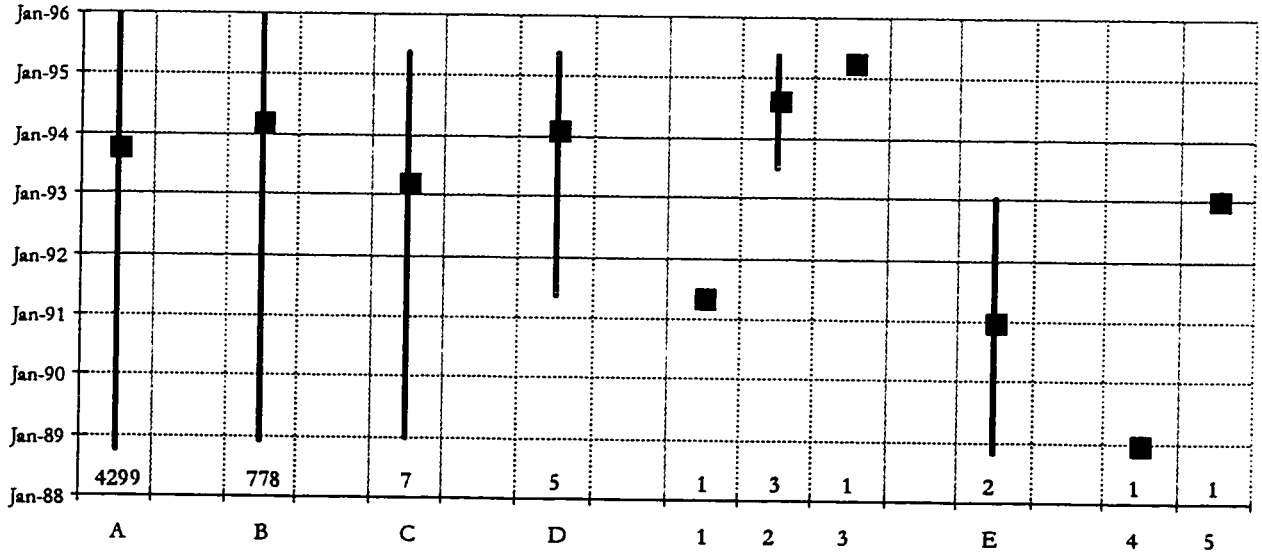


**Figure A.8. Range and Mean Incident Start for Methods of Operation - Tools - Part 7**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **D - All viruses** | **3 -Virus in mail** | **4 - Worm** |
| **B - All Tools** | **1 - *choosegirl*.game** | **E - All Worms** | **5 - Worm rumor** |
| **C - All Autonomous Agents** | **2 - viruses** | | |

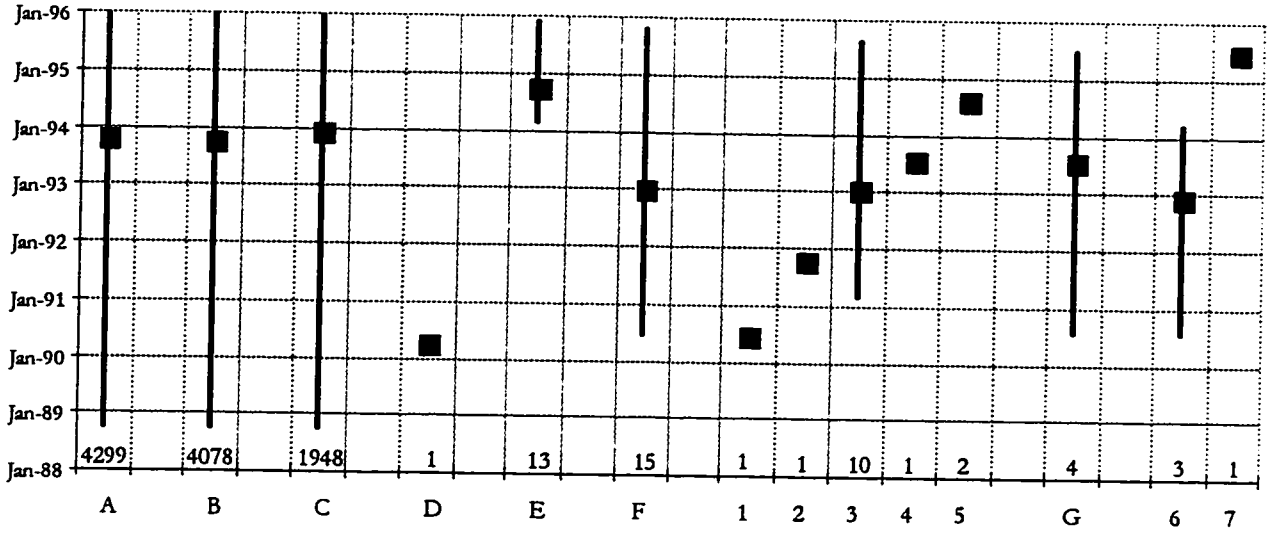


**Figure A.9. Range and Mean Incident Start for Methods of Operation - Access - Part 1**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **E - All autoreply** | **3 - bin** | **G - All bugs** |
| **B - All Access** | **F - All bin, shell** | **4 - alias** | **6 - software bug** |
| **C - All Vulnerabilities** | **1 - /etc/alias** | **5 - ksh** | **7 - Cisco bug** |
| **D - All autofinder** | **2 - unset** | | |

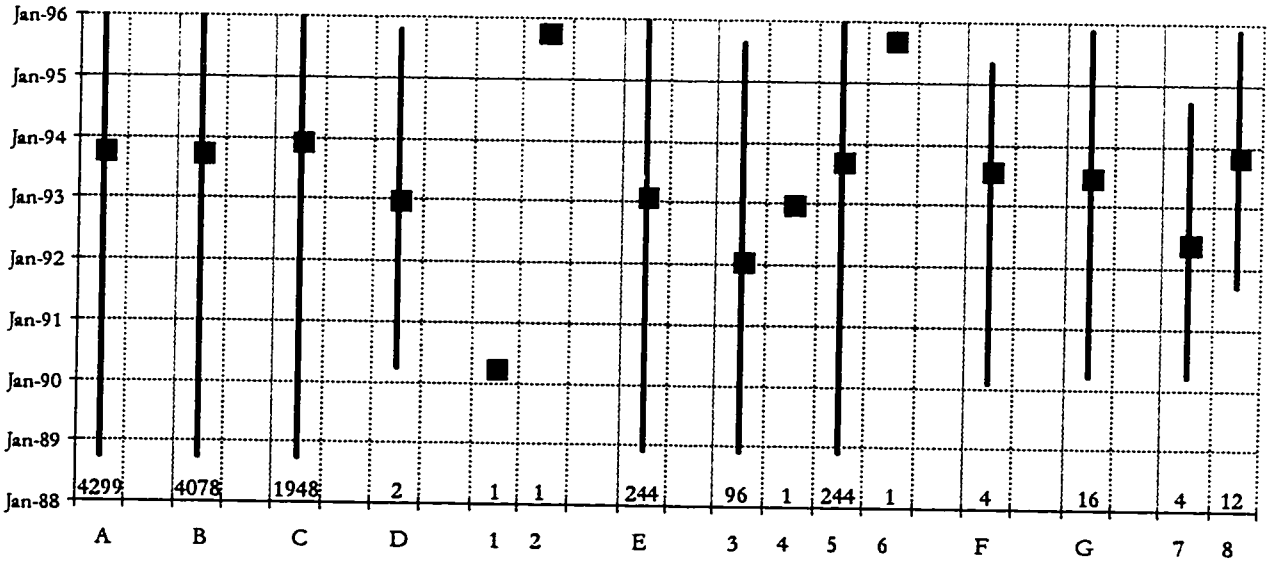


**Figure A.10. Range and Mean Incident Start for Methods of Operation - Access - Part 2**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **1 - chfn/chsh** | **4 - misconfiguration** | **G - All decode. uudecode** |
| **B - All Access** | **2 - chfn** | **5 - configuration** | **7 - uudecode** |
| **C - All Vulnerabilities** | **E - All configuration** | **6 - weak sysadmin** | **8 - decode** |
| **D - All chfn/chsh** | **3 - open server** | **F - All crontab** | |

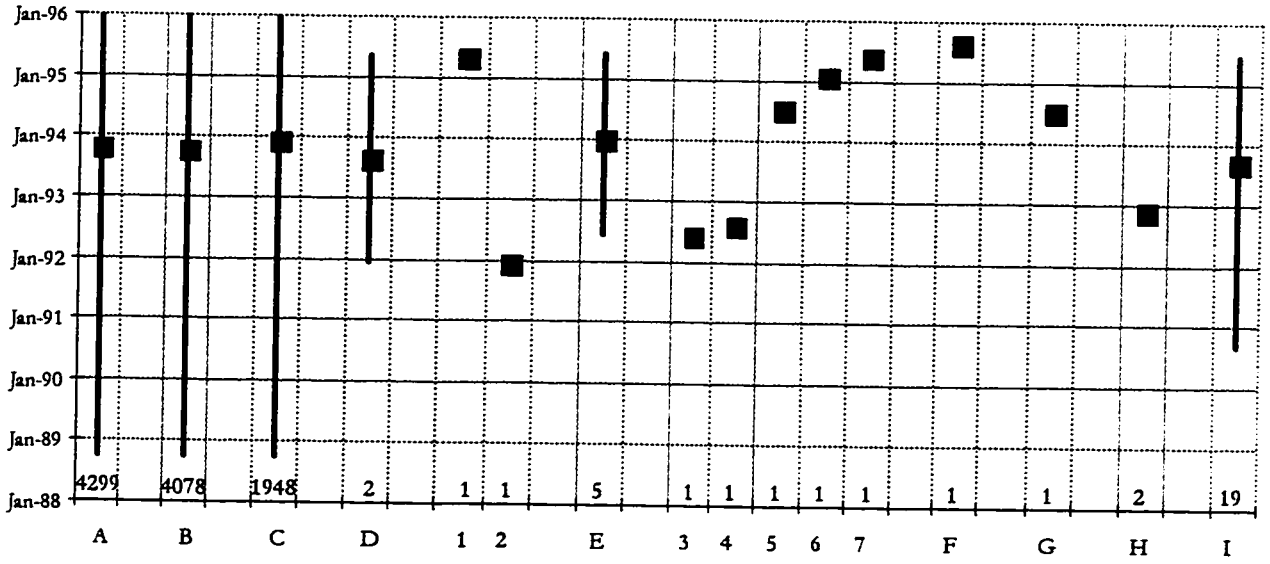


**Figure A.11. Range and Mean Incident Start for Methods of Operation - Access - Part 3**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - dev/tty | 4 - dns | F - domain |
| B - All Access | 2 - dev | 5 - root nameserver corruption | G - dump |
| C - All Vulnerabilities | E - All dns | 6 - dns fraud | H - emacs |
| D - All dev | 3 - dns server | 7 - backup dns address | I - expreserve |

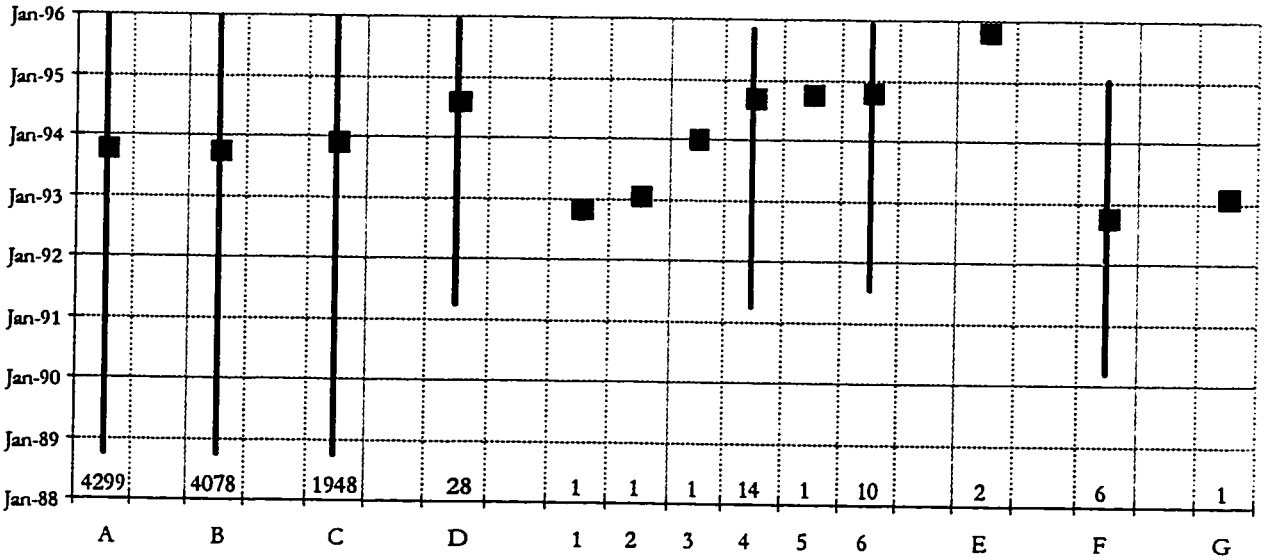


**Figure A.12. Range and Mean Incident Start for Methods of Operation - Access - Part 4**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - finger bombs | 4 - finger attempt | E - fork |
| B - All Access | 2 - repeated fingers | 5 - finger attack | F - .forward |
| C - All Vulnerabilities | 3 - finger storms | 6 - finger | G - fparel |
| D - All finger | | | |

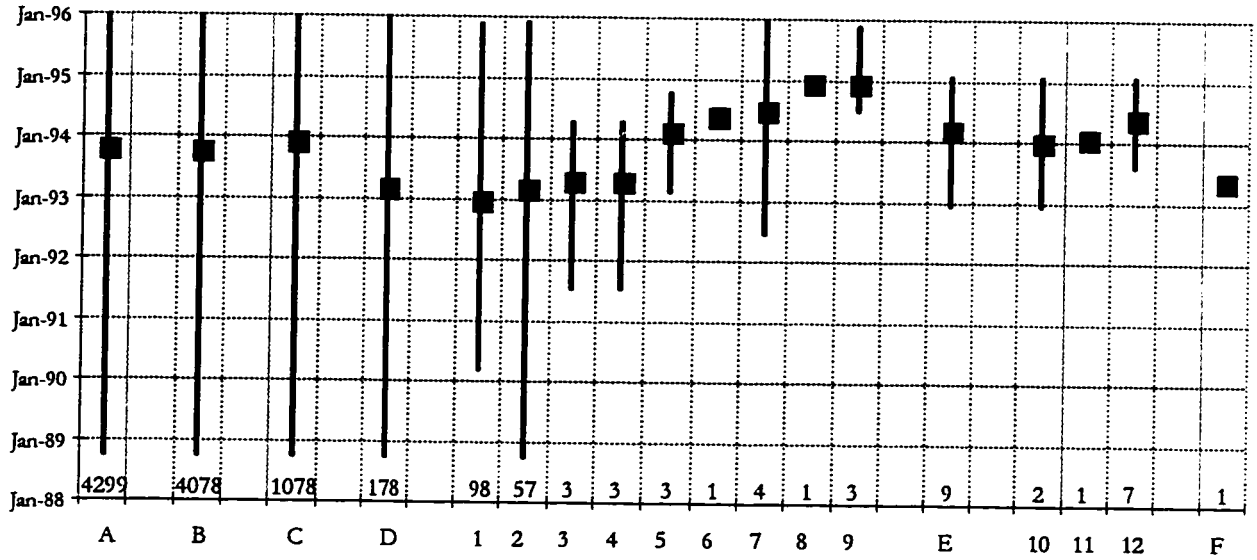


**Figure A.13. Range and Mean Incident Start for Methods of Operation - Access - Part 5**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - ftp | 7 - ftp bug | 10 - gopher "more" |
| B - All Access | 3 - anon ftp | 8 - ftp configuration | 11 - gopher abuse |
| C - All Vulnerabilities | 4 - ftpd | 9 - ftp attacks | 12 - gopher |
| D - All ftp | 5 - wuarchive ftp | E - All gopher | F - All history |
| 1 - ftp attempts | 6 - unauthorized ftp | | |

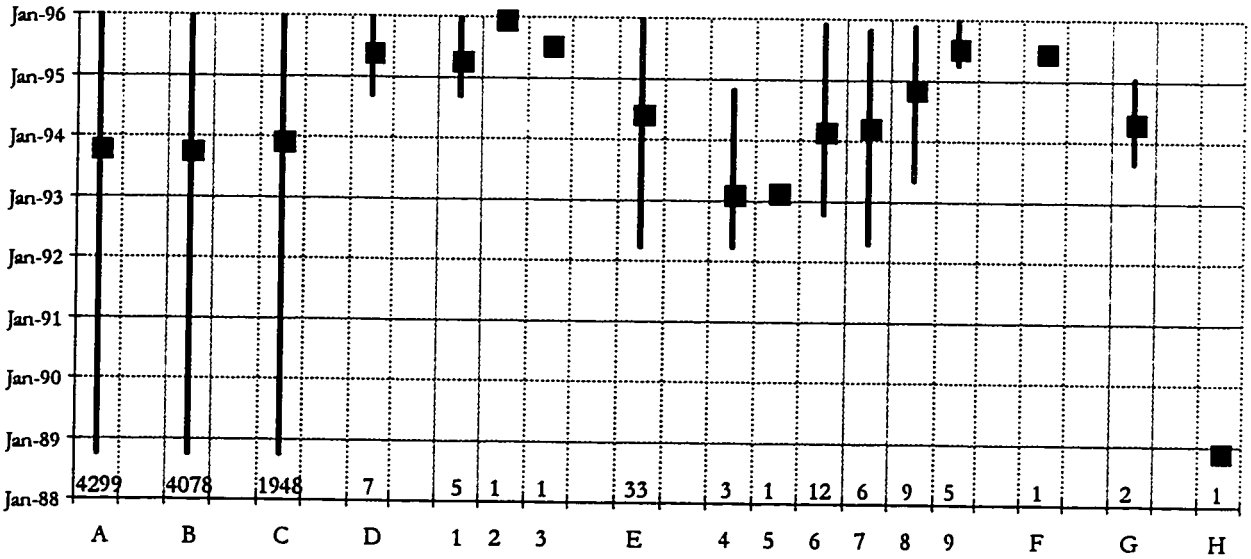


**Figure A.14. Range and Mean Incident Start for Methods of Operation - Access - Part 6**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - web bots | 5 - icmp packet spoofing | 9 -icmp attempts |
| B - All Access | 3 - web abuse | 6 - icmp bomb | F - .ident |
| C - All Vulnerabilities | E - All icmp | 7 - icmp | G - inetd |
| D - All http | 4 - icmp packet storm | 8 - icmp attack | H - install |
| 1 - http, http attempt | | | |

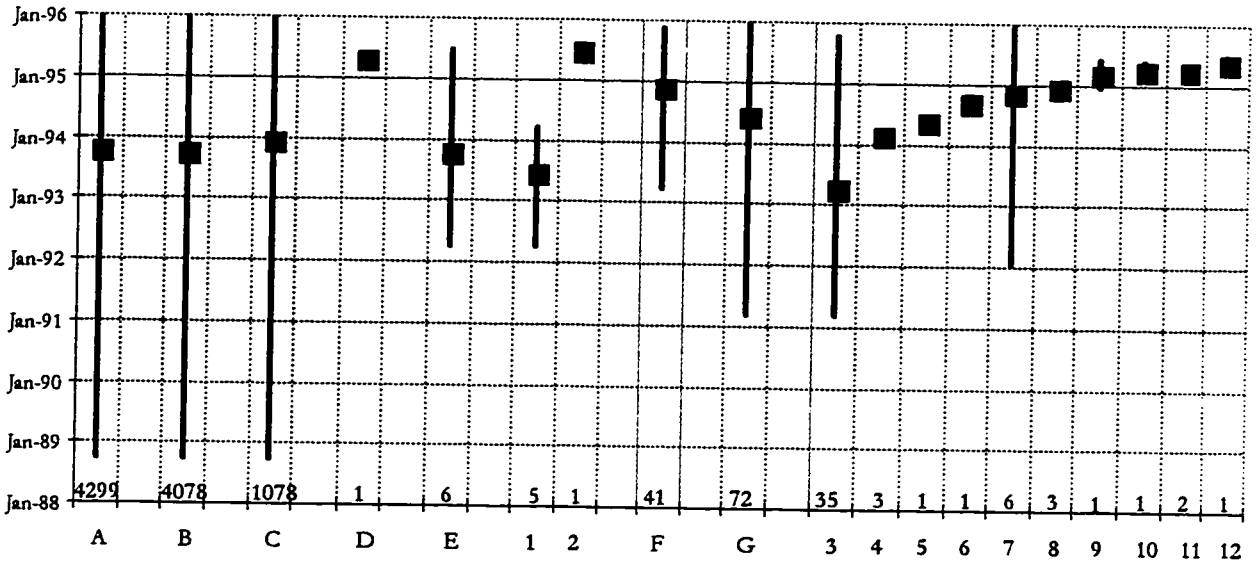


**Figure A.15. Range and Mean Incident Start for Methods of Operation - Access - Part 7**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - shared library | 4 - botkillers | 9 -irc bots |
| B - All Access | 2 - libc | 5 - irc threats | 10 - irc posting |
| C - All Vulnerabilities | F - All loadmodule | 6 - irc flooding | 11 - irc script |
| D - All kernal | G - All irc | 7 - irc abuse | 12 - irc help |
| E - All libc | 3 - irc | 8 - irc bombs | |

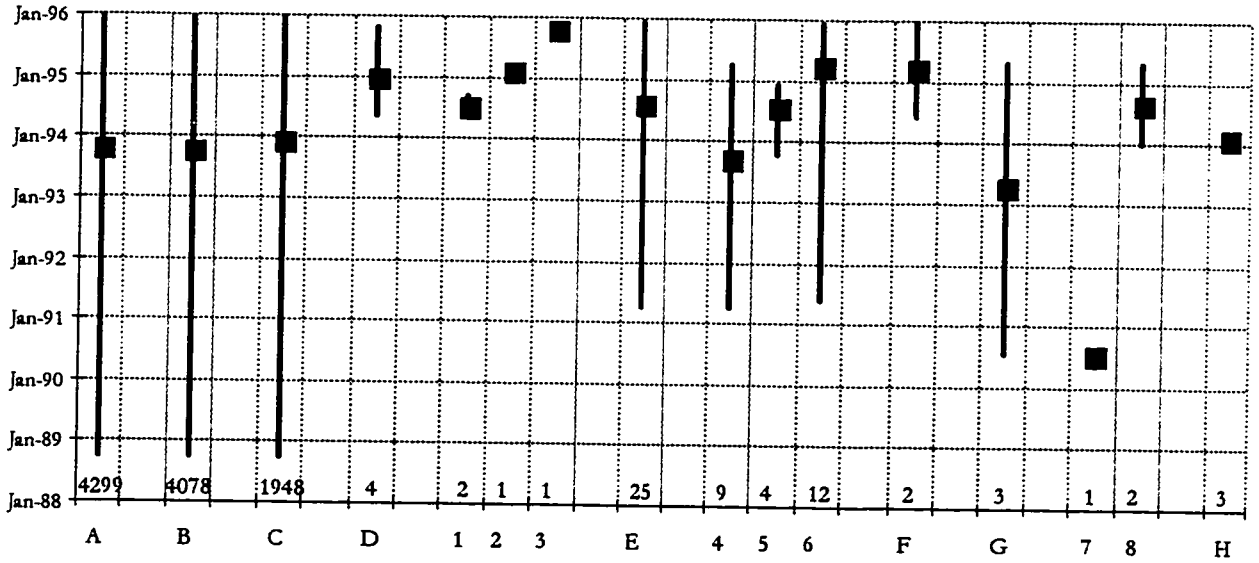


**Figure A.16. Range and Mean Incident Start for Methods of Operation - Access - Part 8**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - /bin/login | 4 - lpd, lpd attack | G - All mem |
| B - All Access | 2 - login -f | 5 - lpr | 7 - /dev/mem |
| C - All Vulnerabilities | 3 - klogin | 6 - lp | 8 - kmem |
| D - All login | E - All lp | F - All majordomo | H - All modload |

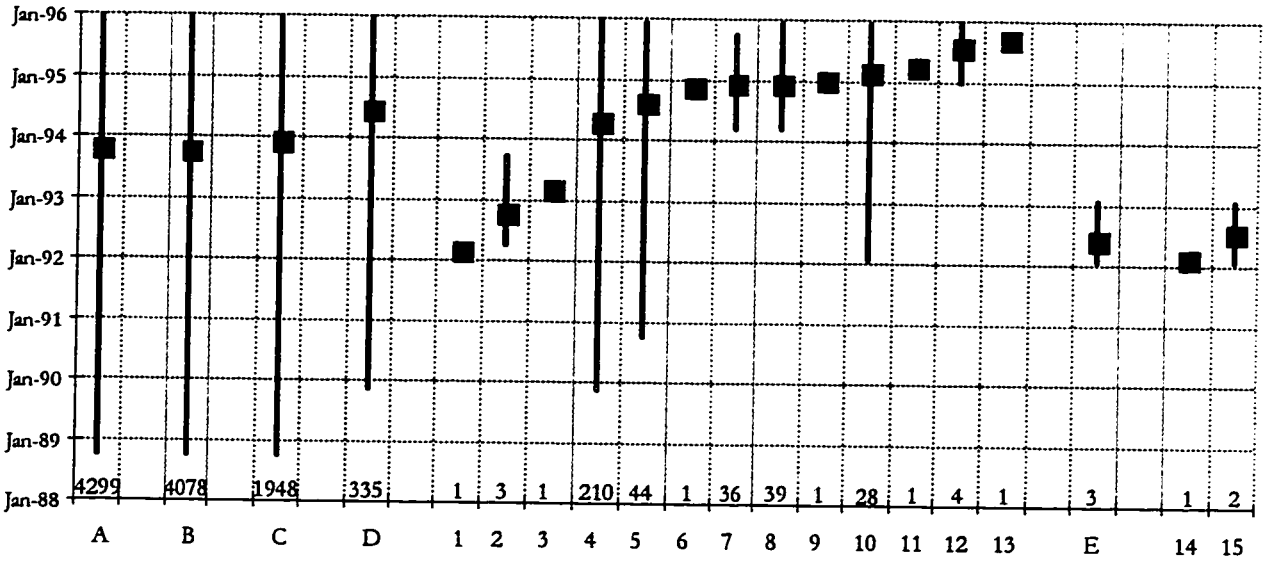


**Figure A.17. Range and Mean Incident Start for Methods of Operation - Access - Part 9**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - secretmail | 7 - mailrace | 12 - mail subscriptions |
| B - All Access | 3 - mail attempt | 8 - binmail | 13 - mail spam |
| C - All Vulnerabilities | 4 - mail spoofing | 9 - modify mail alias | E - All motd |
| D - All mail | 5 - mail bombs | 10 - mail abuse | 14 - motd |
| 1 - massmail | 6 - mail fraud | 11 - anon mail | 15 - /etc/motd |

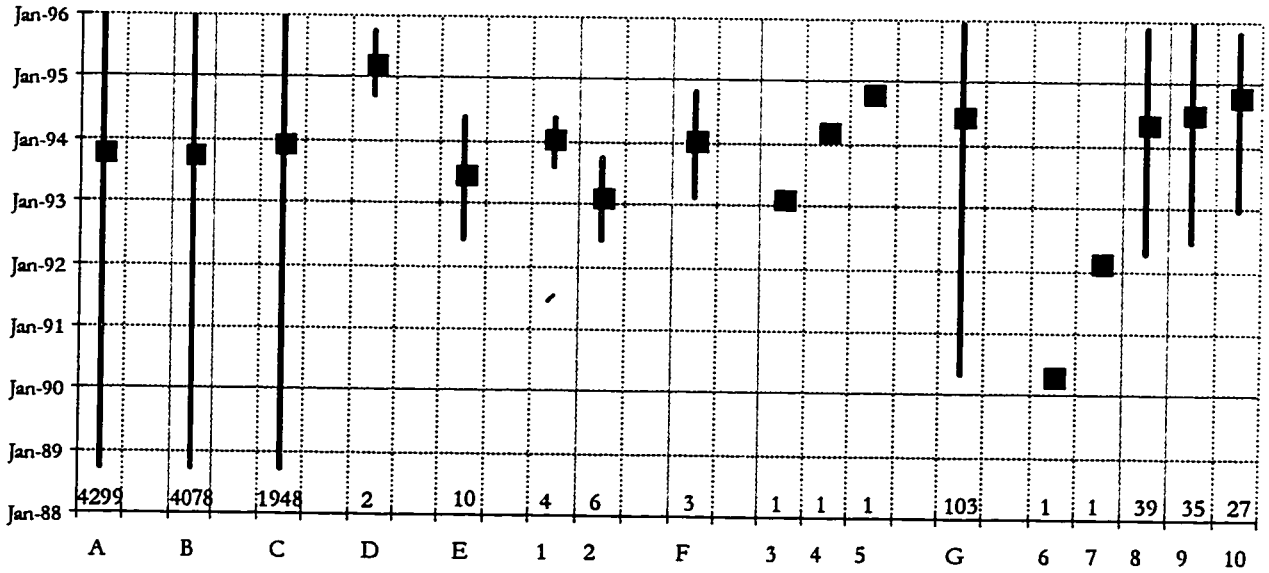


**Figure A.18. Range and Mean Incident Start for Methods of Operation - Access - Part 10**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - mult/div bug | 4 - long newsgroup name | 7 - clients |
| B - All Access | 2 - mult bug | 5 - newsh | 8 - nis attack |
| C - All Vulnerabilities | F - All news | G - All nis | 9 - nis |
| D - All mouse | 3 - /usr/lib/news/sys | 6 - getpwname | 10 - nis attempt |
| E - All mult | | | |

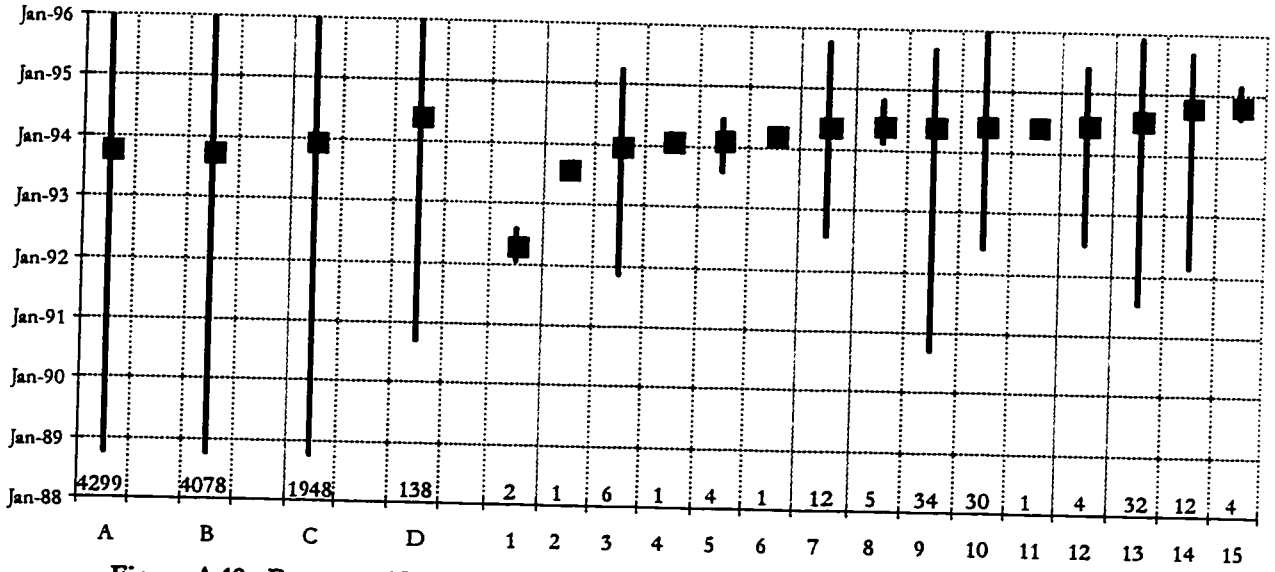


**Figure A.19. Range and Mean Incident Start for Methods of Operation - Access - Part 11**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Access**
**C - All Vulnerabilities**
**D - All nfs**
**1 - nfs exports, exports**
**2 - nfssnoops**
**3 - showmount**
**4 - mountd probes**
**5 - mount**
**6 - expsh**
**7 - nfs mount attempts**
**8 - mountd attempts**
**9 - nfs attempts**
**10 - nfs attack**
**11 - automounter attempts**
**12 - nfs mount attempts**
**13 - nfs**
**14 - mountd**
**15 - nfs bug**

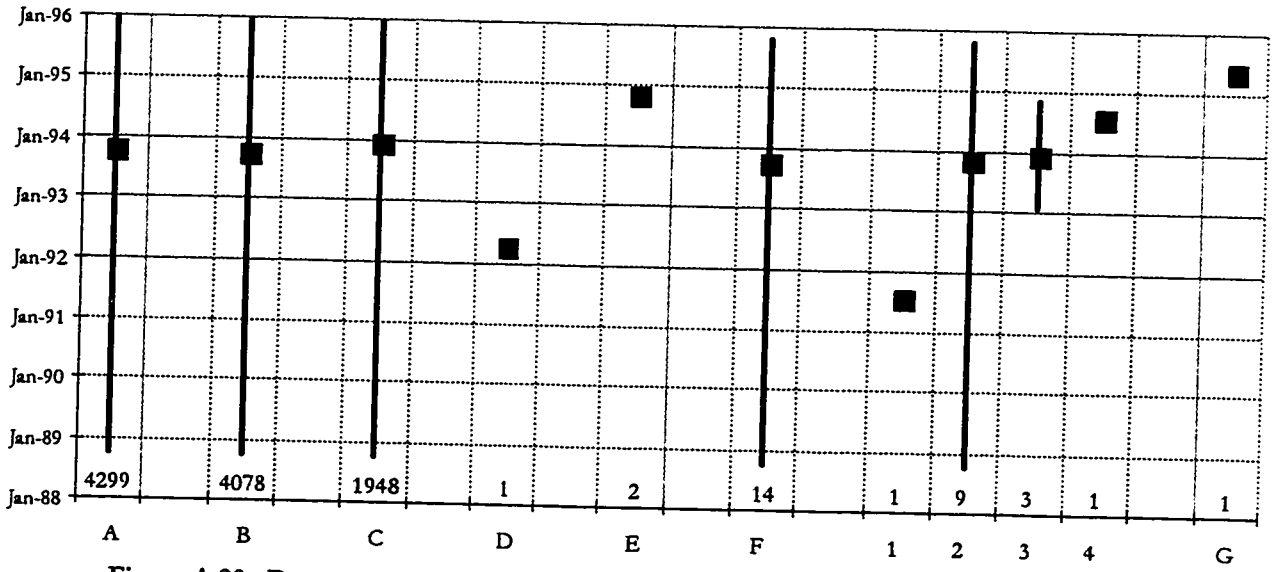


**Figure A.20. Range and Mean Incident Start for Methods of Operation - Access - Part 12**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Access**
**C - All Vulnerabilities**
**D - All netfind**
**E - All nntp**
**F - All ping**
**1 - ping attack**
**2 - ping**
**3 - ping flood**
**4 - ping bombs**
**G - All pipe**

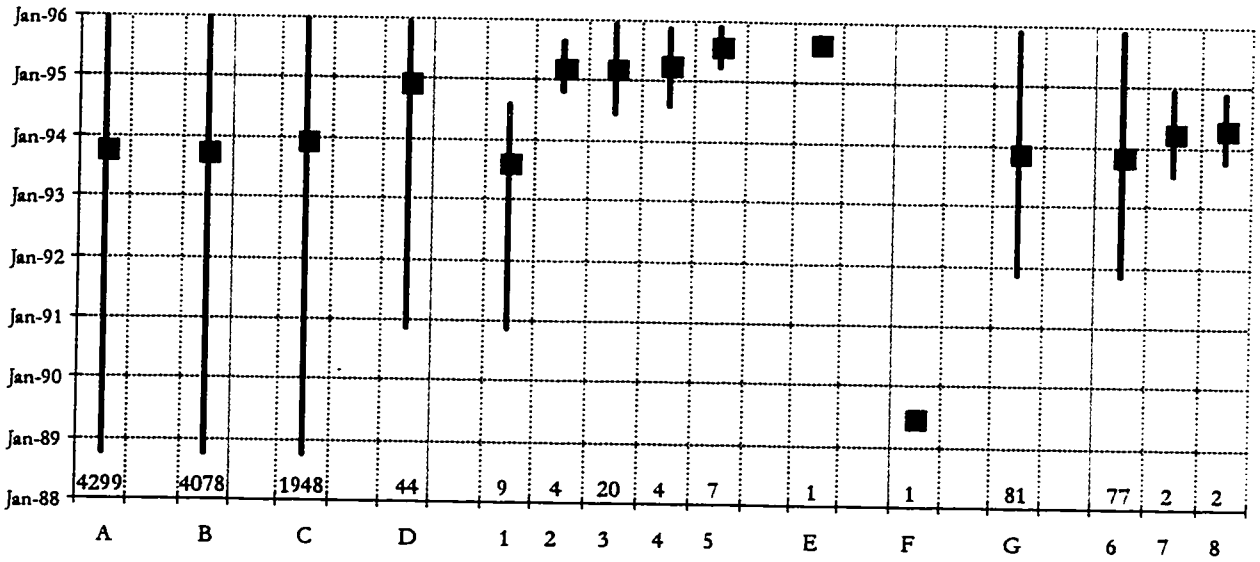


**Figure A.21. Range and Mean Incident Start for Methods of Operation - Access - Part 13**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - portmapper | 5 - port scan | 6 - rdist |
| B - All Access | 2 - scans | E - All ps | 7 - rdist attempt |
| C - All Vulnerabilities | 3 - portmap | F - All rcp | 8 - rdist attack |
| D - All portmap | 4 - portmap scans | G - All rdist | |

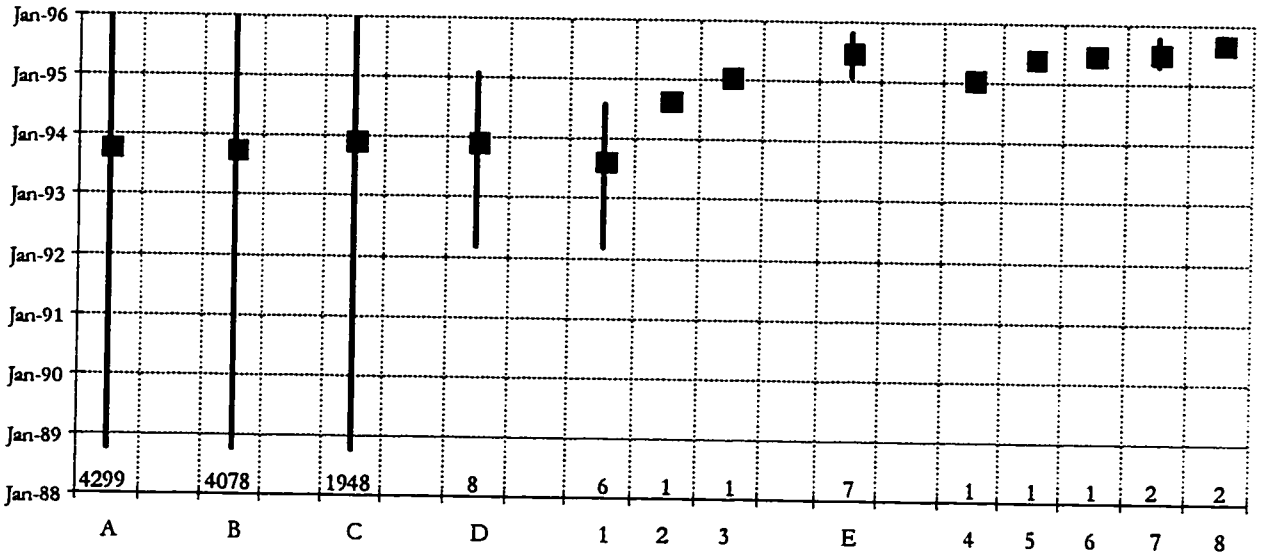


**Figure A.22. Range and Mean Incident Start for Methods of Operation - Access - Part 14**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - rexd | E - rexec | 6 - site exec |
| B - All Access | 2 - rexd attack | 4 - exec attempts | 7 - rexec |
| C - All Vulnerabilities | 3 - rexd attempt | 5 - exec | 8 - rexec attempts |
| D - All rexd | | | |

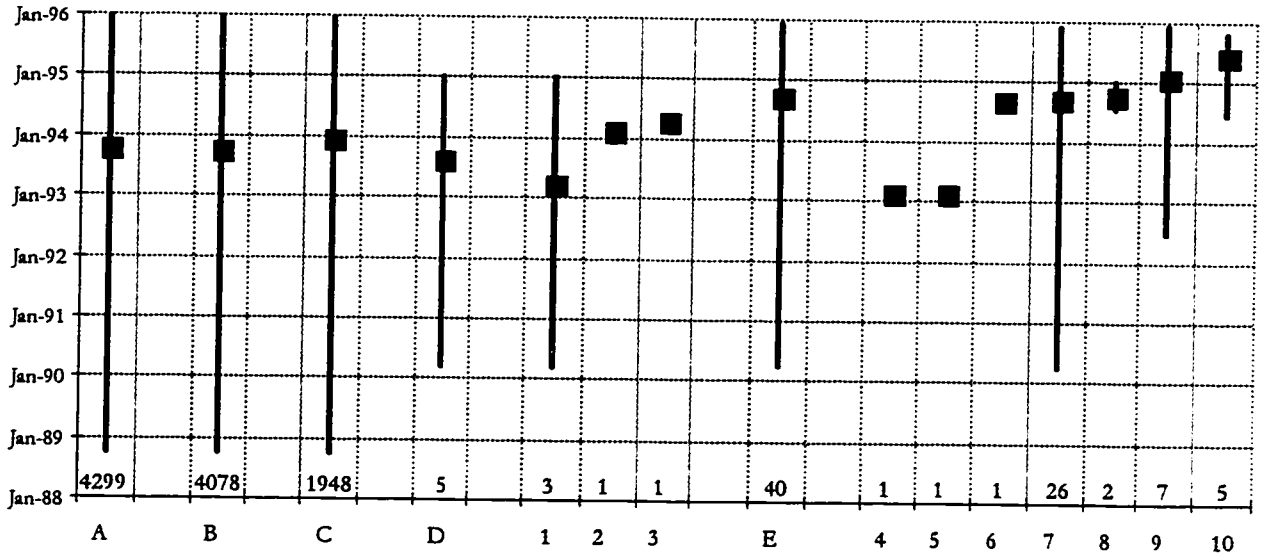


**Figure A.23. Range and Mean Incident Start for Methods of Operation - Access - Part 15**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **1 - rwall** | **4 - rlogin attack** | **8 - rsh/login** |
| **B - All Access** | **2 - rwall spoofing** | **5 - rsh/login attack** | **9 - rsh attempt** |
| **C - All Vulnerabilities** | **3 - rwalld** | **6 - rlogin connections** | **10 - rsh** |
| **D - All rwall** | **E - rsh/rlogin** | **7 - rlogin** | |

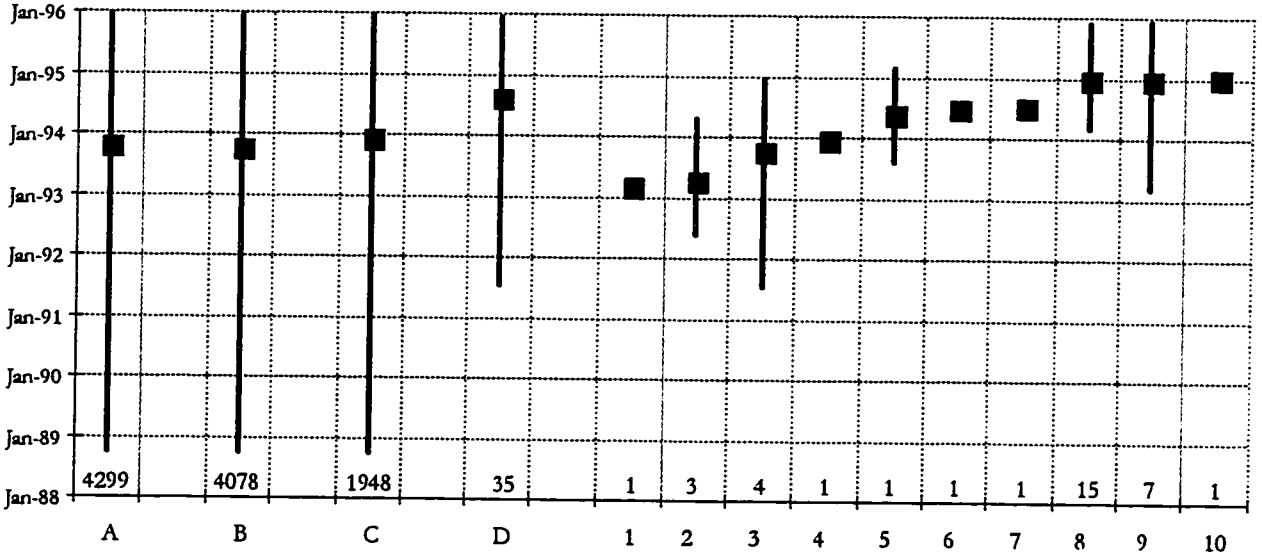


**Figure A.24. Range and Mean Incident Start for Methods of Operation - Access - Part 16**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **1 - rpc getport** | **5 - rpc info** | **8 - rpc** |
| **B - All Access** | **2 - rpc mountd attack** | **6 - rpc toolkit** | **9 - rpc attempt** |
| **C - All Vulnerabilities** | **3 - sunrpc** | **7 - rpc probes** | **10 - rpc scans** |
| **D - All rpc** | **4 - rpc rusers connections** | | |

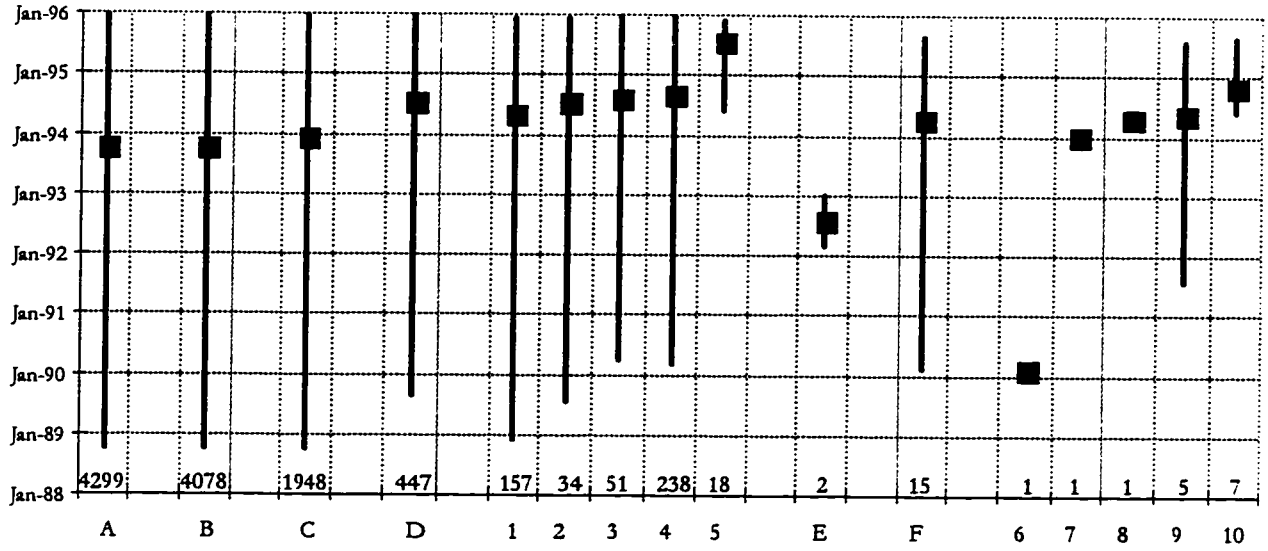


**Figure A.25. Range and Mean Incident Start for Methods of Operation - Access - Part 17**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **1 - sendmail** | **5 - *wiz*** | **7 - smtp port** |
| **B - All Access** | **2 - sendmail debug** | **E - All shutdown** | **8 - smtp attack** |
| **C - All Vulnerabilities** | **3 - sendmail attacks** | **F - All smtp** | **9 - smtp** |
| **D - All sendmail** | **4 - sendmail attempt** | **6 - mconnect** | **10 - smtp attempt** |

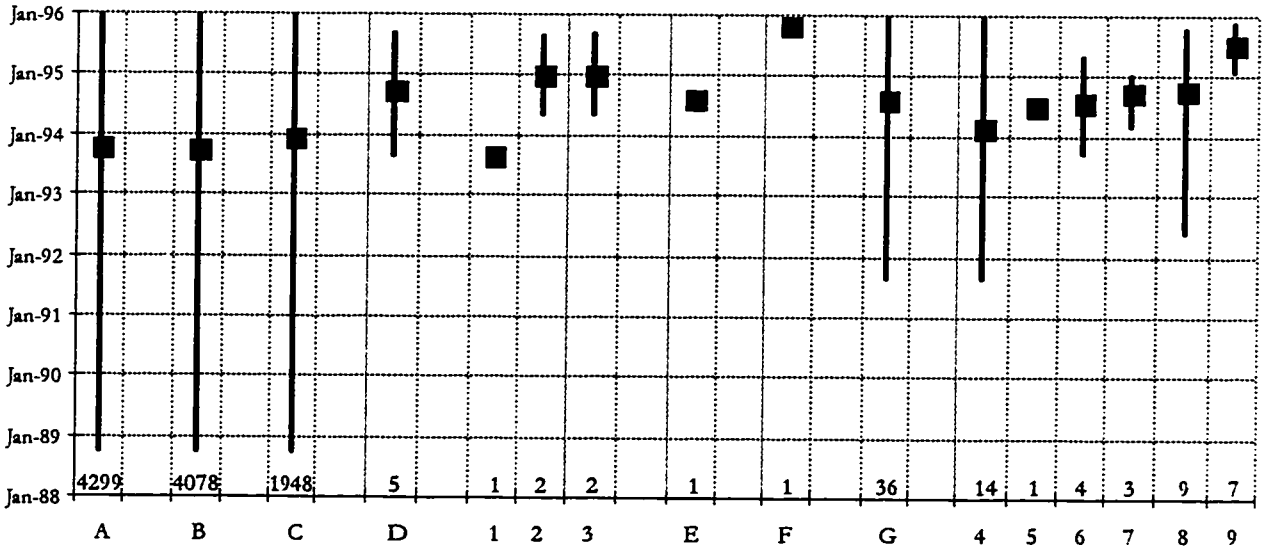


**Figure A.26. Range and Mean Incident Start for Methods of Operation - Access - Part 18**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **1 - snmp attack** | **F - All syslog** | **7 - dns spoofing** |
| **B - All Access** | **2 - snmp** | **G - All source hiding** | **8 - tsutomo attack, tsutomo** |
| **C - All Vulnerabilities** | **3 - snmp attempt** | **5 - source spoofing, attempts** | **9 - IP spoofing** |
| **D - All snmp** | **E - All suid** | **6 - source route spoofing** | **10 - IP spoofing attempt** |

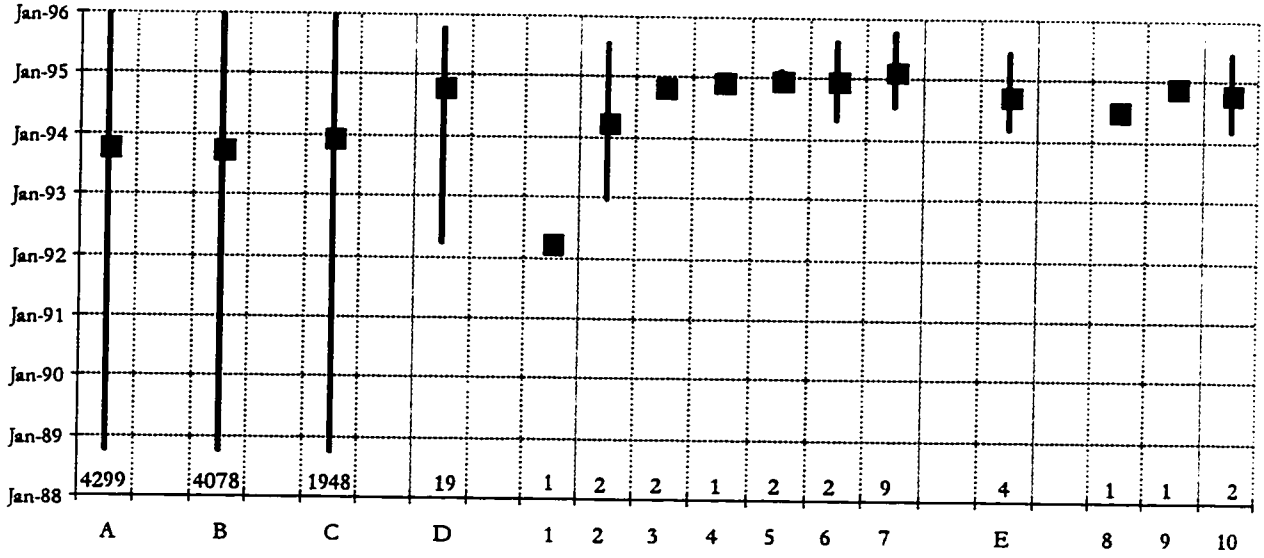


**Figure A.27. Range and Mean Incident Start for Methods of Operation - Access - Part 19**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - talk abuse | 5 - talk | 8 - tcp ports |
| B - All Access | 2 - talk request | 6 - talk bombs | 9 - tcp packet bombs |
| C - All Vulnerabilities | 3 - talk attack | 7 - talk flood | 10 - tcp |
| D - All talk | 4 - talk attempts | E - All tcp | |

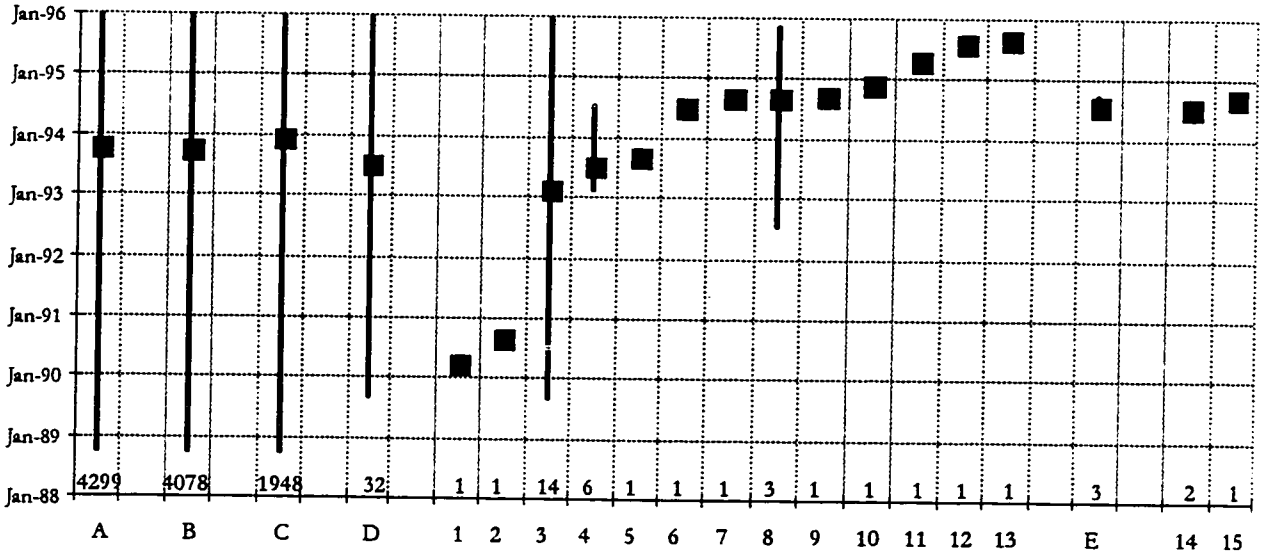


**Figure A.28. Range and Mean Incident Start for Methods of Operation - Access - Part 20**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - public telnet | 7 - telnet connections | 12 - port 222 |
| B - All Access | 3 - telnet | 8 - port 25 | 13 - telnet hijacking |
| C - All Vulnerabilities | 4 - telnet attack | 9 - telnet attempts | E - All time |
| D - All telnet | 5 - telnet bug | 10 - telnet probes | 14 - time |
| 1 - 87 socket | 6 - socket 7002 | 11 - port 167 | 15 - /bin/time |

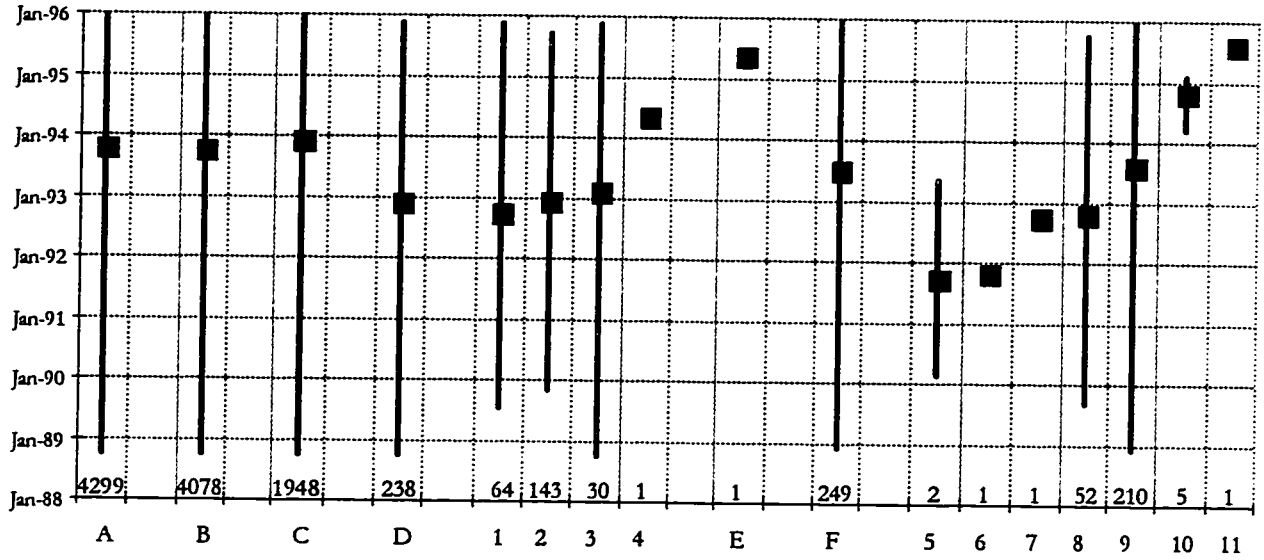


**Figure A.29. Range and Mean Incident Start for Methods of Operation - Access - Part 21**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Access**
**C - All Vulnerabilities**
**D - All tftp**
**1 - tftp attacks**
**2 - tftp attempts**
**3 - tftp**
**4 - automated tftp**
**E - All traceroutes**
**F - All trusted hosts**
**5 - /etc/hosts**
**6 - gethost**
**7 - show hosts**
**8 - hosts.equiv**
**9 - .rhosts, .rhost attempt**
**10 - trusted hosts attack**
**11 - hosts.allow**

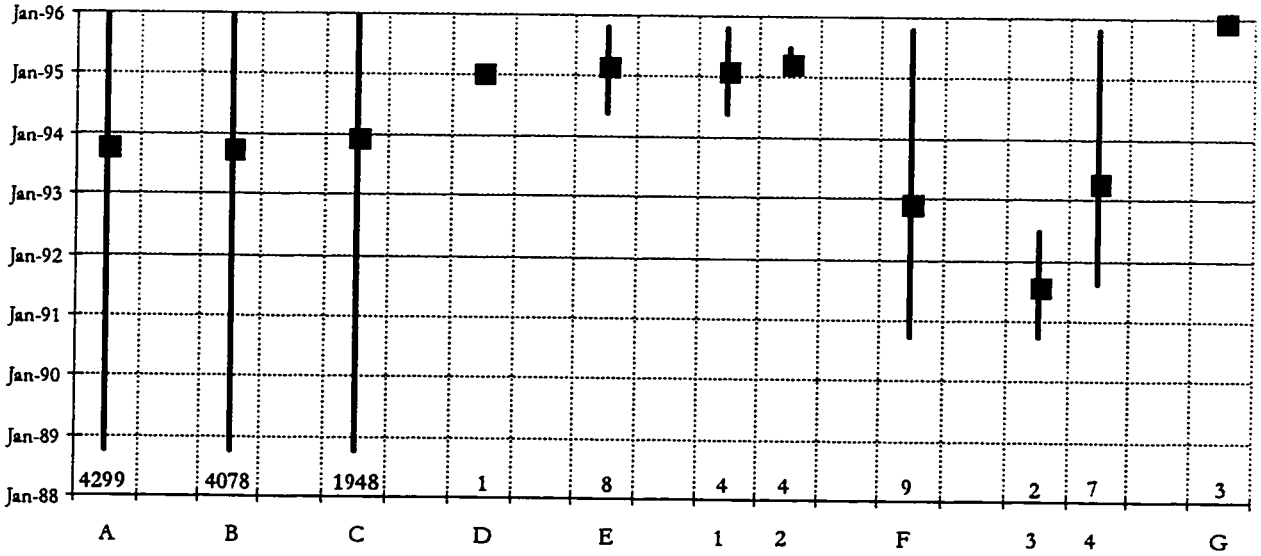


**Figure A.30. Range and Mean Incident Start for Methods of Operation - Access - Part 22**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Access**
**C - All Vulnerabilities**
**D - All utmp**
**E - All udp**
**1 - udp**
**2 - udp attempts**
**F - All uucp**
**3 - uucp attempts**
**4 - uucp**
**G - All Windows NT**

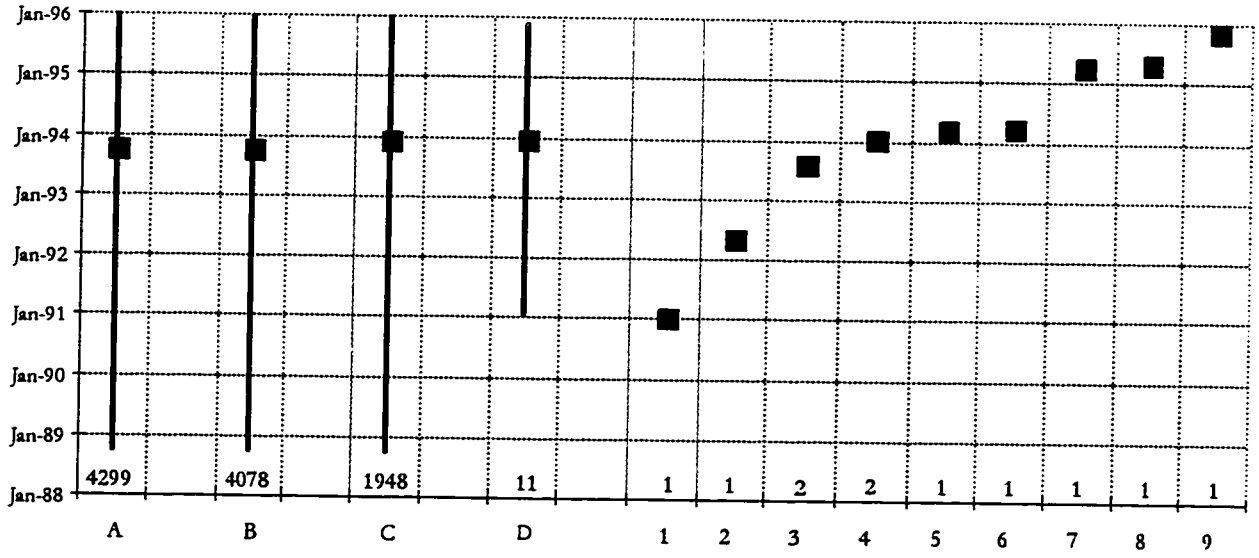


**Figure A.31. Range and Mean Incident Start for Methods of Operation - Access - Part 23**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **1 - x file** | **4 - xterm** | **7 - x attack** |
| **B - All Access** | **2 - X11R5 bug** | **5 - xtrek** | **8 - xkey** |
| **C - All Vulnerabilities** | **3 - x11 attack** | **6 - xcats** | **9 - x** |
| **D - All x** | | | |

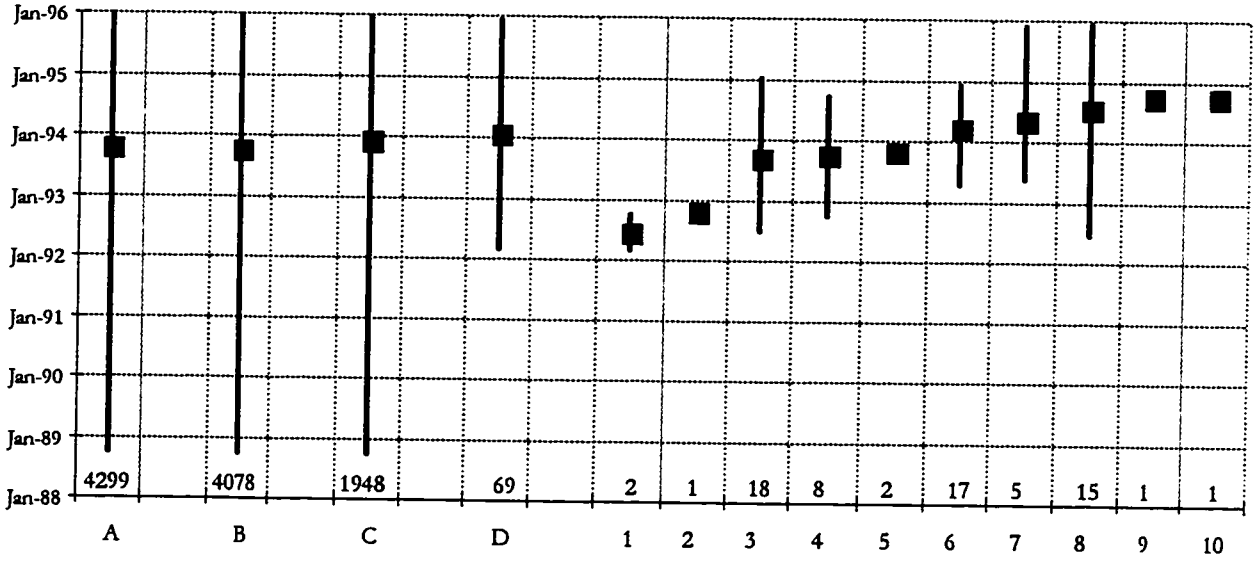


**Figure A.32. Range and Mean Incident Start for Methods of Operation - Access - Part 24**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **1 - yppasswd** | **5 - yp attempt** | **8 - ypx, ypx attempts** |
| **B - All Access** | **2 - ypxfer** | **6 - ypserv, ypserv attack** | **9 - ypbind** |
| **C - All Vulnerabilities** | **3 - yp** | **7 - ypcat** | **10 - ypbreak** |
| **D - All yp** | **4 - ypsnarf** | | |

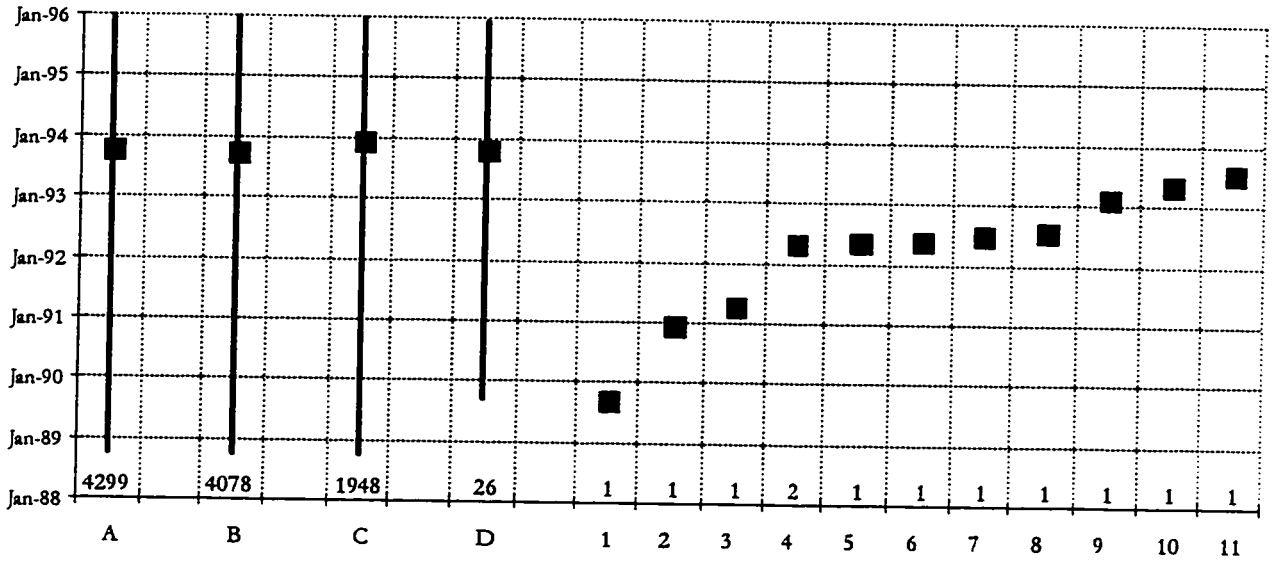


**Figure A.33. Range and Mean Incident Start for Methods of Operation - Access - Part 25**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - prompter | 5 - dynamic linking | 9 - private/etc |
| B - All Access | 2 - analimddmp | 6 - sysuaf | 10 - internet discovery application |
| C - All Vulnerabilities | 3 - hhstore | 7 - KVMsnf | 11 - .runner |
| D - All misc/unknown | 4 - rightslist.dat | 8 - systest | |

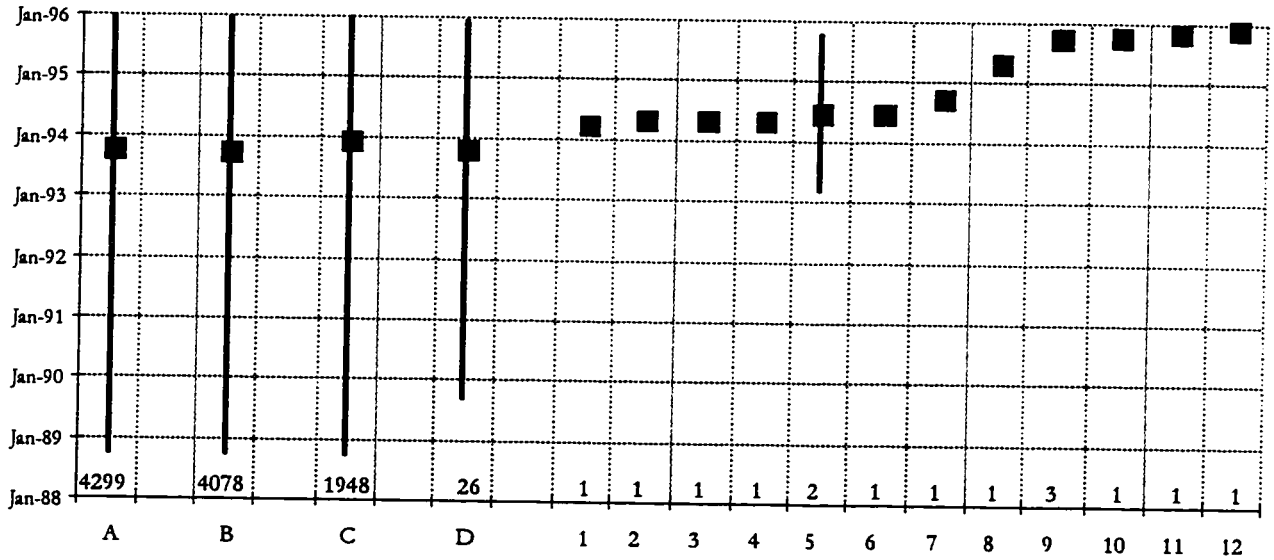


**Figure A.34. Range and Mean Incident Start for Methods of Operation - Access - Part 26**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 1 - echo | 5 - watch | 9 - ropt |
| B - All Access | 2 - prc | 6 - inn bug attempt | 10 - popper |
| C - All Vulnerabilities | 3 - neil.bug | 7 - simlink service | 11 - .rbone |
| D - All misc/unknown | 4 - aup abuse | 8 - selection service | 12 - tprof |

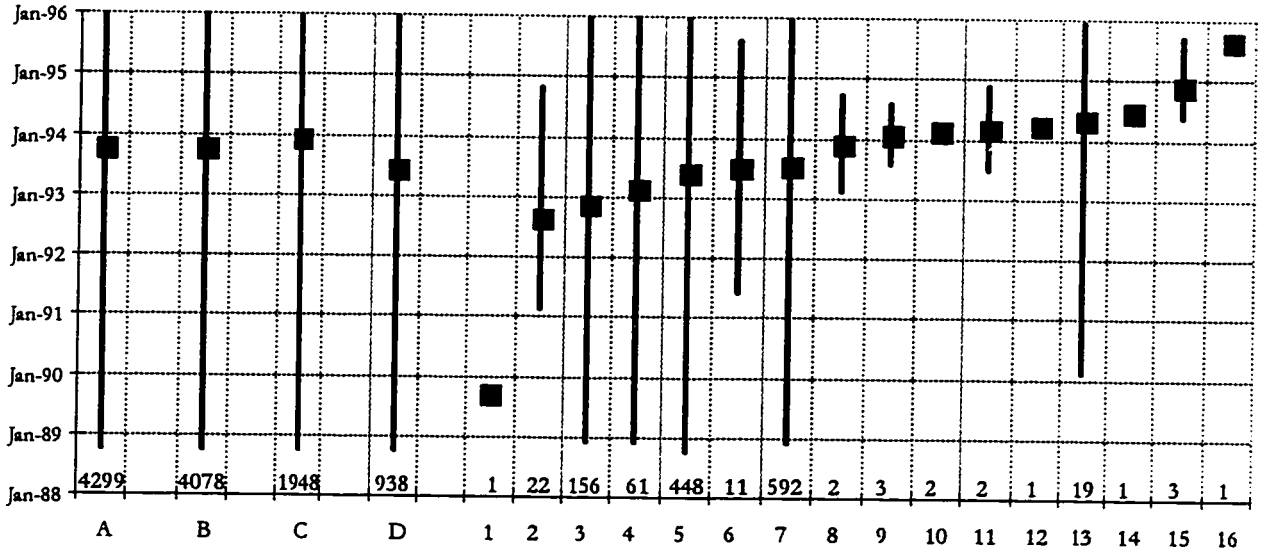


**Figure A.35. Range and Mean Incident Start for Methods of Operation - Access - Part 27**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - password change | 7 - password file | 12 - captured password |
| B - All Access | 3 - weak password(s) | 8 - default passwords | 13 - shared account |
| C - All Vulnerabilities | 4 - no password(s) | 9 - stolen password | 14 - eeprom password |
| D - All Passwords | 5 - password cracking | 10 - cracked password | 15 - password -f |
| 1 - password guessing | 6 - shared password | 11 - password(s) | 16 - passwdrace |

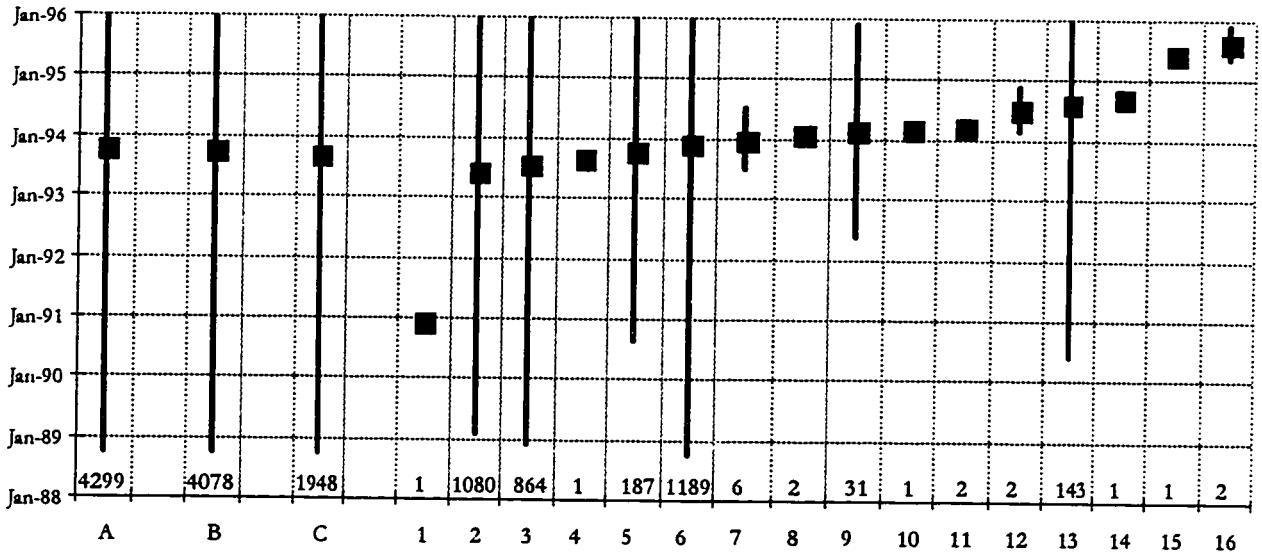


**Figure A.36. Range and Mean Incident Start for Methods of Operation - Access - Part 28**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 3 - account break-in | 8 - infrastructure attack | 13 - dos attack, dos attempt, |
| B - All Access | 4 - probes | 9 - attempts | dos threat |
| C - All Access level | 5 - break-in | 10 - prank call | 14 - account misuse |
| 1 - student research project | 6 - root break-in | 11 - bbs, hacker bbs | 15 - listservers |
| 2 - login attempts | 7 - misuse | 12 - router attack | 16 - bbs posting |

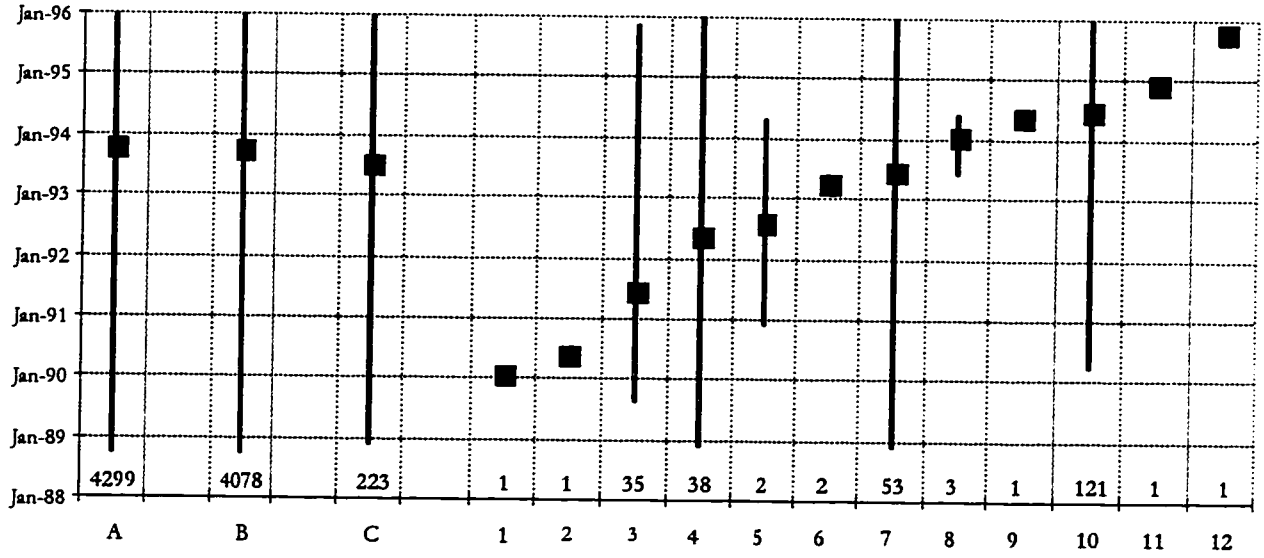


**Figure A.37. Range and Mean Incident Start for Methods of Operation - Access - Part 29**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - demo account | 6 - me account | 10 - user account |
| B - All Access | 3 - guest account | 7 - system account | 11 - uucp account |
| C - All Type of account | 4 - sync, sync account | 8 - lp account | 12 - nobody account |
| 1 - parity account | 5 - field, field account | 9 - bin account | |

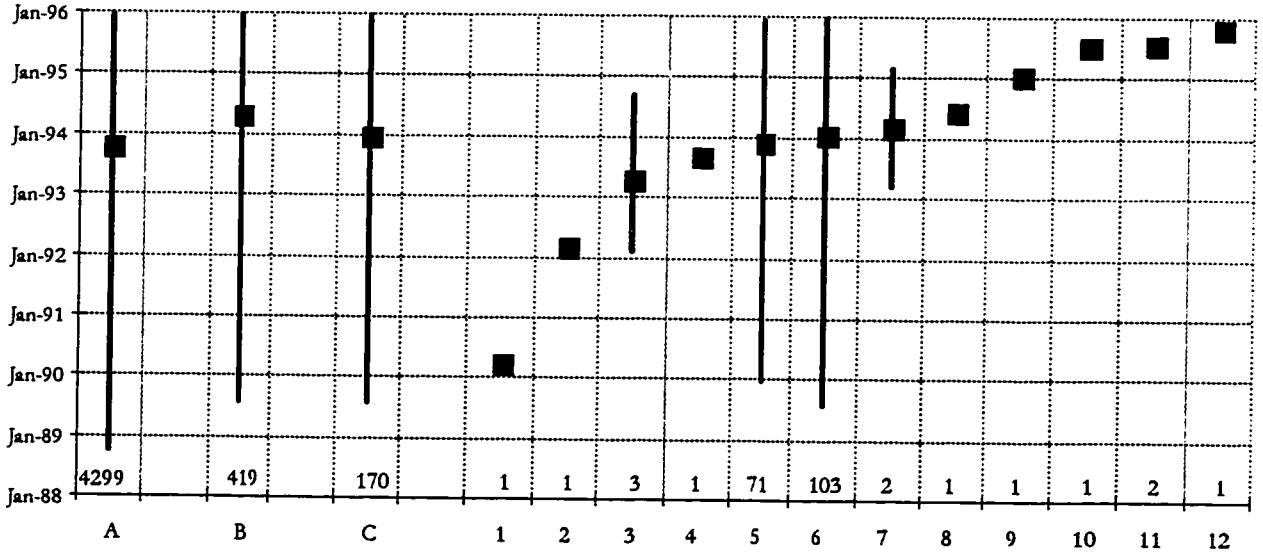


**Figure A.38. Range and Mean Incident Start for Methods of Operation - Results - Part 1**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| A - All Incidents | 2 - shared files deleted | 7 - all files deleted | 11 - remove netnews |
| B - All Results | 3 - system files deleted | 8 - gopher files deleted | messages |
| C - All Corruption of | 4 - suspicious files | 9 - files | 12 - forge |
| Information | 5 - files deleted | 10 - cert.org summary | |
| 1 - rm -rf | 6 - modify, delete logs | cancel attempt | |

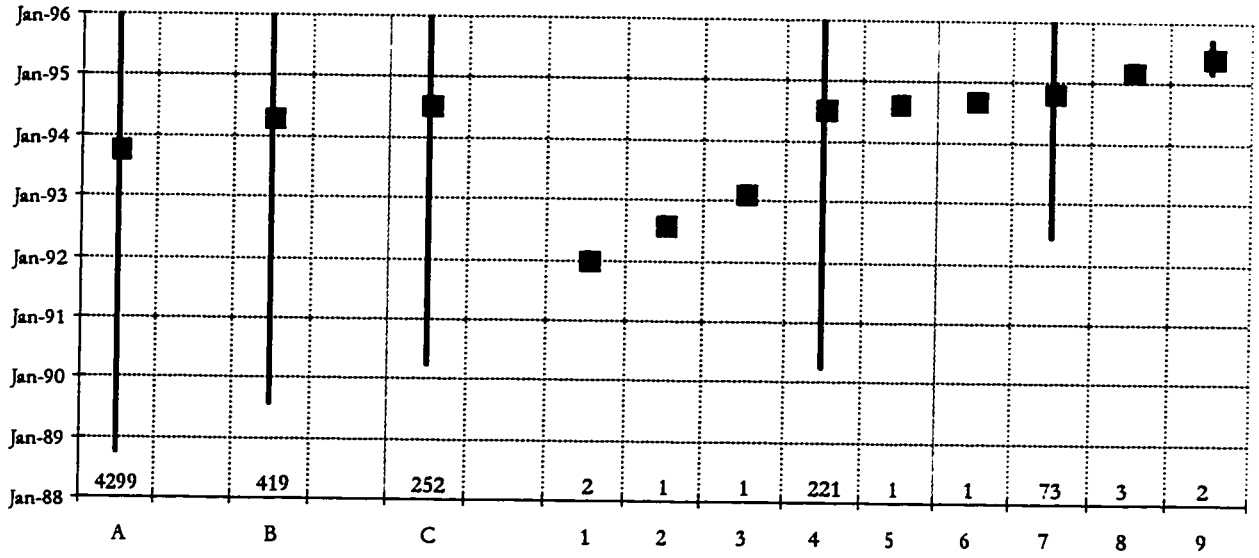


**Figure A.39. Range and Mean Incident Start for Methods of Operation - Results - Part 2**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **1 - credit report (stolen)** | **4 - software piracy** | **7 - warez** |
| **B - All Results** | **2 - info on bbs** | **5 - credit report on irc** | **8 - alt.2600 posting** |
| **C - All Disclosure of Information** | **3 - disclosure issue** | **6 - logs sent around net** | **9 - copied files** |

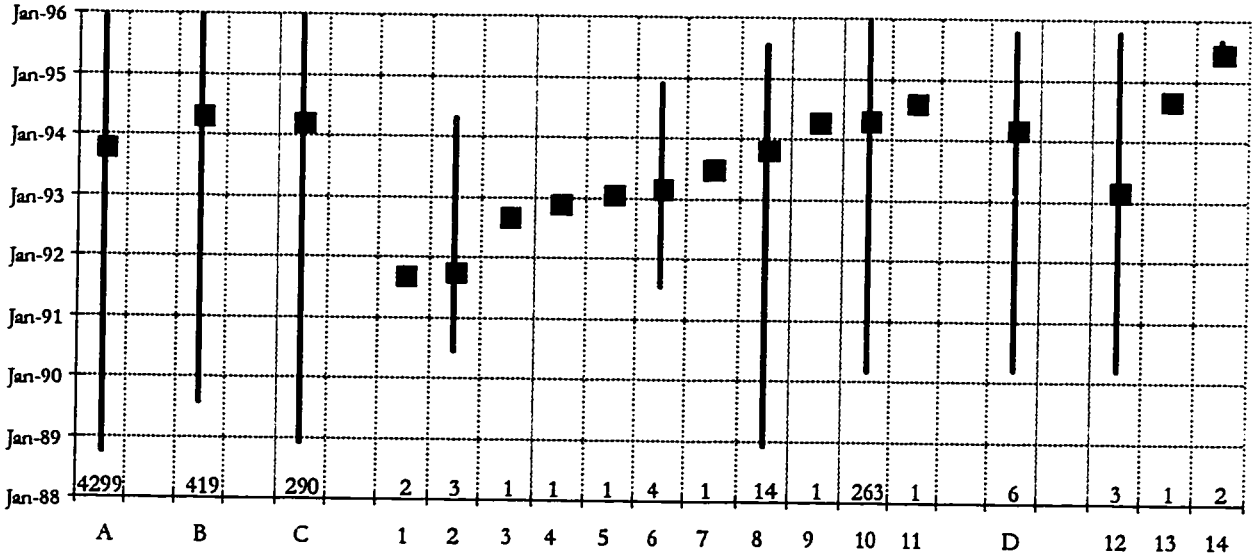


**Figure A.40. Range and Mean Incident Start for Methods of Operation - Results - Part 3**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

| | | | |
|---|---|---|---|
| **A - All Incidents** | **3 - high phone bill** | **8 - chain letter** | **D - All denial of service** |
| **B - All Results** | **4 - illegal bbs** | **9 - bbs abuse** | **12 - deleted accounts** |
| **C - All theft of service** | **5 - unauthorized gateway use** | **10 - ftp abuse** | **13 - halt system** |
| **1 - bogus newsgroup** | **6 - MUD** | **11 - account added** | **14 - system crash** |
| **2 - 800# abuse** | **7 - fidonet abuse** | | |

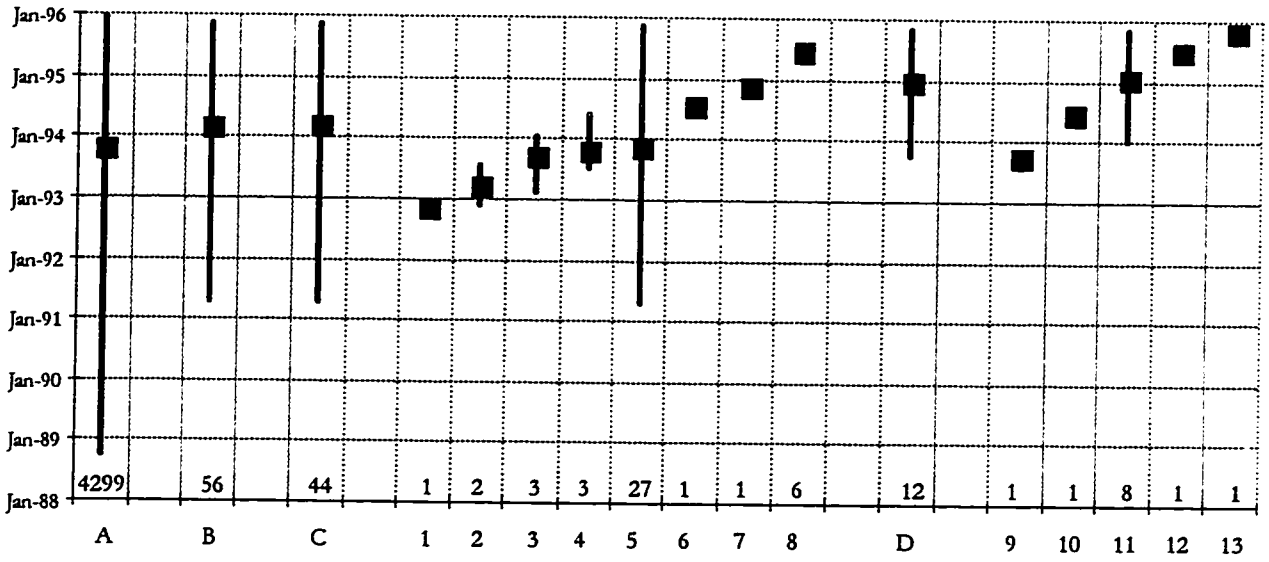


**Figure A.41. Range and Mean Incident Start for Methods of Operation - Objectives**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific methods of operation or groups as follows:

**A - All Incidents**
**B - All Objectives**
**C - All financial gain**
**1 - industrial sabotage**
**2 - extorsion threat**
**3 - scam**
**4 - fraud**
**5 - credit card fraud**
**6 - industrial espionage**
**7 - embezzlement**
**8 - isp, isp rivalry**
**D - All damage**
**9 - harassment**
**10 - damage**
**11 - threat**
**12 - arson threat**
**13 - feud**

## *Appendix B*

### Summary of Corrective Actions

The following pages summaries the corrective actions listed in the CERT®/CC records. Table B.1 presents the data in tabular form. This table shows the following for each category:

1. First report - The reporting date of the earliest incident where the action was recorded.
2. Mean Report - The mean reporting date for all incidents where the action was recorded.
3. Last Report - The reporting date of the last incident where the action was recorded.
4. Incidents - The total number of incidents reporting the action.
5. Delta - The difference between the Mean Reporting Dates for the incidents reporting the action and the Mean Reporting Date for all incidents.

This same data is plotted in Figures B.1 to B.6. The first four of these Figures present the internal corrective actions, and the external corrective actions are presented in the last two Figures.

Of the 4,299 incidents, 1.5% (63) of the incident reports recorded no corrective actions. The remaining 98.5% (4,236) of the incident reports record as a minimum some indication that one of more sites involved were notified. This corrective action (notifying sites) is not listed in Table B.1 or in the Figures after that. The Table and Figures show the other corrective actions that are recorded in 1,388 (32.3%) if the incidents in the CERT®/CC records.

**Table B.1 Corrective Actions**

| | First Report | Mean Report | Last Report | Incidents | Delta |
|---|---|---|---|---|---|
| all | 1-Oct-88 | 24-Oct-93 | 30-Dec-95 | 4299 | 0.0 |
| All Corrective Actions | 1-Oct-88 | 10-Oct-93 | 30-Dec-95 | 1388 | -13.9 |
| Internal Actions | 30-Nov-88 | 4-Oct-93 | 30-Dec-95 | 1137 | -20.3 |
| Restrict System Hardware/Software | 5-Dec-88 | 30-Dec-93 | 30-Dec-95 | 674 | 66.6 |
| disable tftp | 22-Jun-93 | 22-Jun-93 | 22-Jun-93 | 1 | -124.4 |
| disable ftp | 1-Jul-93 | 28-Jul-93 | 25-Aug-93 | 2 | -87.9 |
| wrapper | 12-Aug-93 | 12-Aug-93 | 12-Aug-93 | 1 | -73.4 |
| close account(s) | 1-Sep-89 | 29-Oct-93 | 28-Dec-95 | 460 | 5.1 |
| firewall | 1-Apr-90 | 4-Dec-93 | 10-Oct-95 | 4 | 40.9 |
| disconnect | 5-Dec-88 | 5-Jan-94 | 24-Dec-95 | 124 | 72.8 |
| filter | 1-Apr-90 | 31-Aug-94 | 30-Dec-95 | 162 | 310.6 |
| restrict logins | 25-Nov-94 | 19-Dec-94 | 12-Jan-95 | 2 | 420.6 |
| delete .rhosts | 22-Jul-94 | 12-Mar-95 | 31-Oct-95 | 2 | 503.6 |
| Configure System Hardware/Software | 30-Nov-89 | 8-Jun-93 | 24-Dec-95 | 447 | -137.5 |
| restrict server | 27-Aug-90 | 3-Apr-92 | 21-Feb-95 | 38 | -568.6 |
| change permissions | 19-May-92 | 19-May-92 | 19-May-92 | 1 | -523.4 |
| secure server/router | 5-Dec-88 | 16-May-93 | 13-Dec-95 | 140 | -160.8 |
| change password(s) | 22-Aug-89 | 23-Jul-93 | 24-Dec-95 | 310 | -92.5 |
| change configuration | 10-Aug-95 | 17-Sep-95 | 26-Oct-95 | 2 | 693.1 |
| Upgrade System Hardware/Software | 30-Nov-88 | 11-Oct-93 | 28-Dec-95 | 367 | -13.0 |
| add traps | 1-Apr-90 | 24-May-91 | 16-Jul-92 | 2 | -883.9 |
| patch | 30-Nov-88 | 10-Aug-93 | 28-Dec-95 | 200 | -74.5 |
| upgrade software | 20-Sep-89 | 13-Dec-93 | 20-Dec-95 | 81 | 50.1 |
| reload software/system | 30-Oct-89 | 18-Jan-94 | 20-Dec-95 | 161 | 86.0 |
| Preventive Measures | 5-Dec-88 | 22-Mar-93 | 19-Dec-95 | 245 | -215.9 |
| spy | 29-Jan-91 | 29-Jan-91 | 1-Jan-91 | 1 | -999.4 |
| checklist | 5-Dec-88 | 17-Mar-92 | 7-Dec-94 | 4 | -586.1 |
| increase monitoring | 1-Sep-89 | 28-Oct-92 | 19-Dec-95 | 143 | -360.6 |
| cops | 1-Apr-90 | 3-Jun-93 | 6-Aug-95 | 75 | -142.7 |
| crack | 18-Oct-89 | 31-Dec-93 | 20-Oct-95 | 28 | 68.3 |
| tripwire | 19-Sep-92 | 5-Aug-94 | 25-Oct-95 | 26 | 285.1 |
| publish reports | 2-May-95 | 2-May-95 | 2-May-95 | 1 | 554.6 |
| talk to all users | 26-Jul-95 | 22-Aug-95 | 19-Sep-95 | 2 | 667.1 |
| Miscellaneous Measures | | | | | |
| delete worm | 22-Dec-88 | 22-Dec-88 | 22-Dec-88 | 1 | -1767.4 |
| refer to assist | 23-Aug-93 | 23-Aug-93 | 23-Aug-93 | 1 | -62.4 |
| External Actions | 1-Oct-88 | 23-Oct-93 | 30-Dec-95 | 478 | -0.9 |
| Take Action Against Intruder | 5-Dec-88 | 14-Nov-93 | 30-Dec-95 | 295 | 20.7 |
| arrest | 1-Nov-89 | 9-Apr-93 | 7-Dec-95 | 27 | -197.6 |
| talk to intruder(s) | 5-Dec-88 | 2-Dec-93 | 30-Dec-95 | 273 | 39.2 |
| punish | 11-Apr-91 | 20-Nov-94 | 19-Dec-95 | 23 | 392.1 |
| Law Enforcement | 1-Oct-88 | 30-Aug-93 | 28-Dec-95 | 237 | -55.4 |
| trace | 1-Apr-90 | 1-Apr-90 | 1-Apr-90 | 1 | -1302.4 |
| investigate | 27-Jun-90 | 27-Jun-90 | 27-Jun-90 | 1 | -1215.4 |
| secret service | 1-Oct-88 | 30-Sep-92 | 18-Apr-95 | 19 | -389.2 |
| law enforcement | 1-Oct-88 | 24-Dec-92 | 7-Mar-95 | 3 | -304.1 |
| police | 29-Jun-89 | 30-Aug-93 | 28-Dec-95 | 141 | -55.4 |
| fbi | 2-Oct-89 | 20-Sep-93 | 6-Dec-95 | 110 | -33.9 |

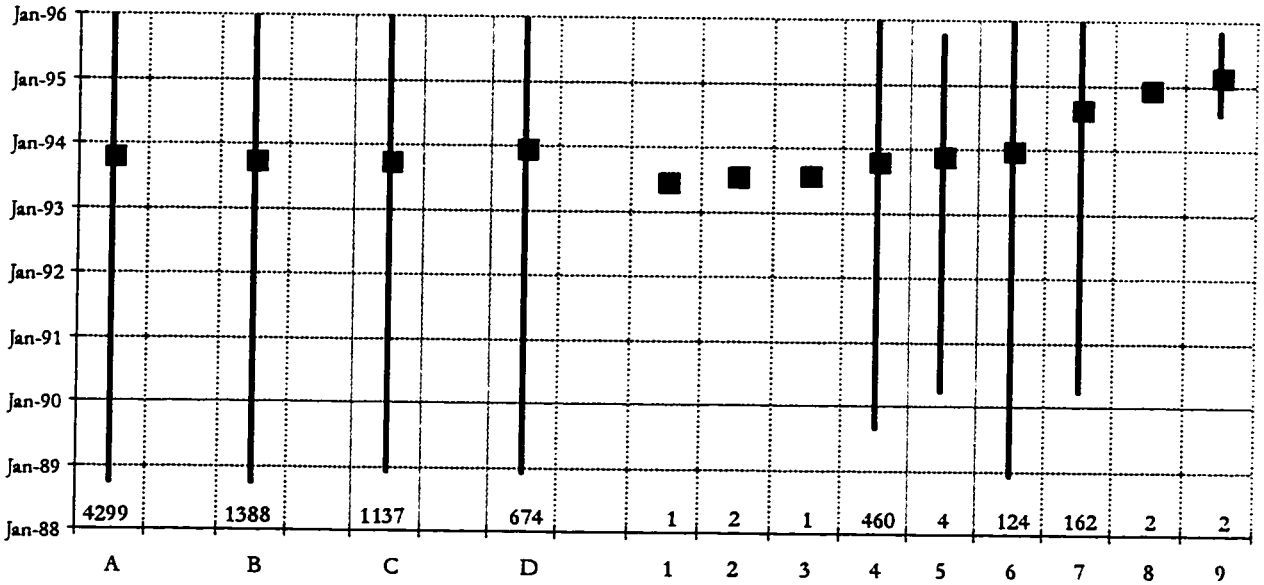


**Figure B.1. Range and Mean Incident Reporting Dates for Corrective Actions - Restrict System Hardware/Software**
Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific corrective actions or groups as follows:

A - All Incidents
B - All Corrective Actions
C - All Internal Actions
D - All Restrict Hardware/Software Actions
1 - Disable TFTP
2 - Disable FTP
3 - Install TCP wrapper
4 - Close account(s)
5 - Install firewall
6 - Disconnect from Internet
7 - Filter network traffic
8 - Restrict logins
9 - Delete .rhost file(s)

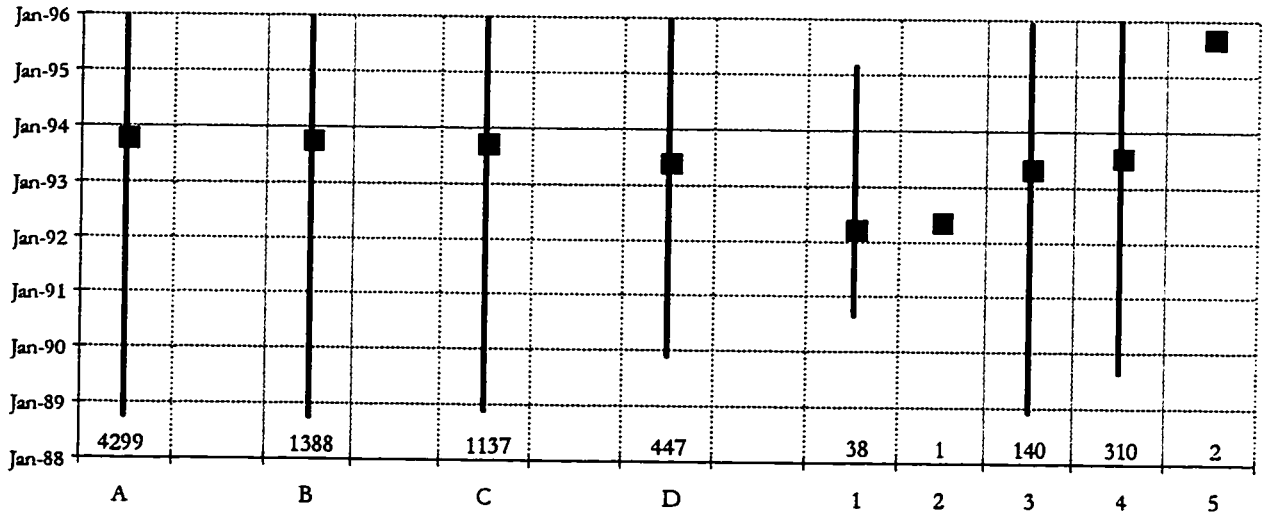


**Figure B.2. Range and Mean Incident Reporting Dates for Corrective Actions - Configure System Hardware/Software**
Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific corrective actions or groups as follows:

A - All Incidents
B - All Corrective Actions
C - All Internal Actions
D - All Restrict Hardware/Software Actions
1 - Restrict server
2 - Change permissions
3 - Secure server/router
4 - Change password(s)
5 - Change configuration

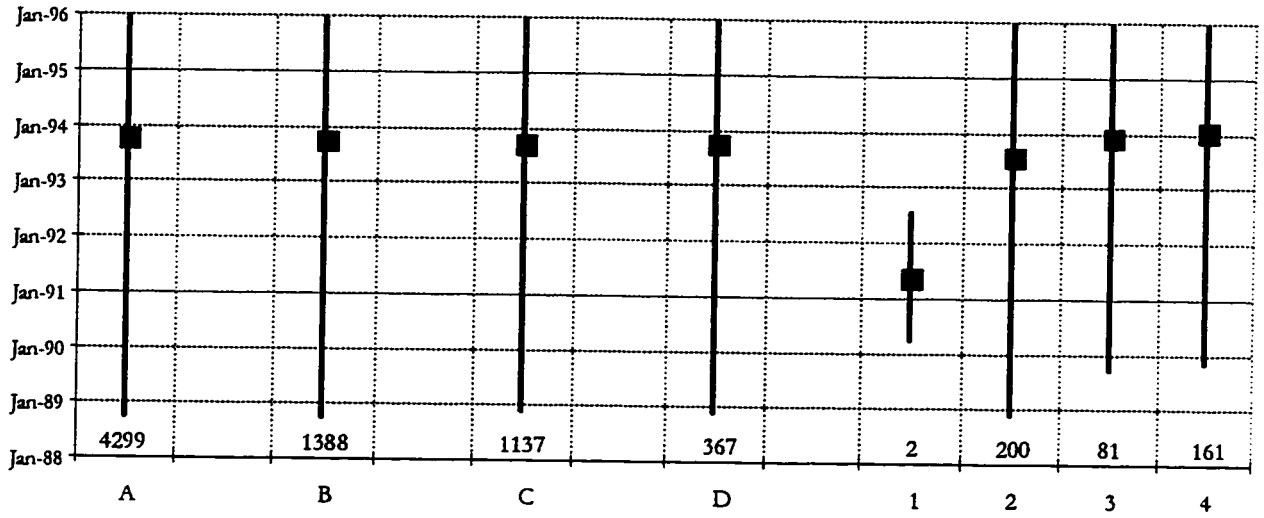


**Figure B.3. Range and Mean Incident Reporting Dates for Corrective Actions - Upgrade System Hardware/Software**
Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific corrective actions or groups as follows:

**A - All Incidents**
**B - All Corrective Actions**
**C - All Internal Actions**
**D - All Restrict Hardware/Software Actions**
**1 - Add traps**
**2 - Patch software**
**3 - Upgrade software**
**4 - Reload software/router**

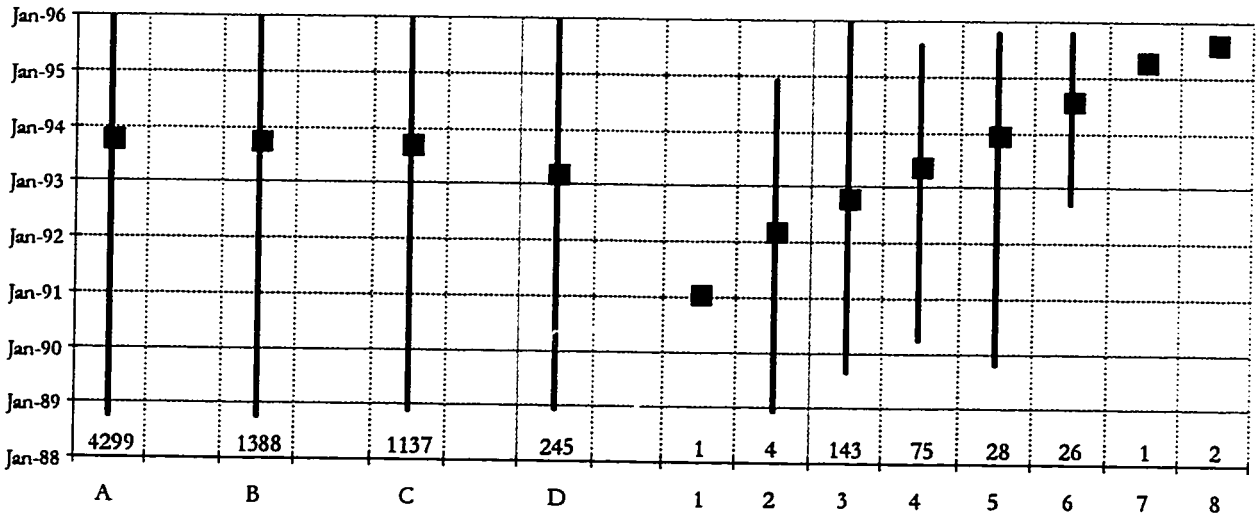


**Figure B.4. Range and Mean Incident Reporting Dates for Corrective Actions - Preventive Measures**
Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific corrective actions or groups as follows:

**A - All Incidents**
**B - All Corrective Actions**
**C - All Internal Actions**
**D - All Restrict Hardware/Software Actions**
**1 - Spy**
**2 - Checklist**
**3 - Increasing monitoring**
**4 - Cops**
**5 - Crack**
**6 - Tripwire**
**7 - Publish reports**
**8 - Talk to all users**

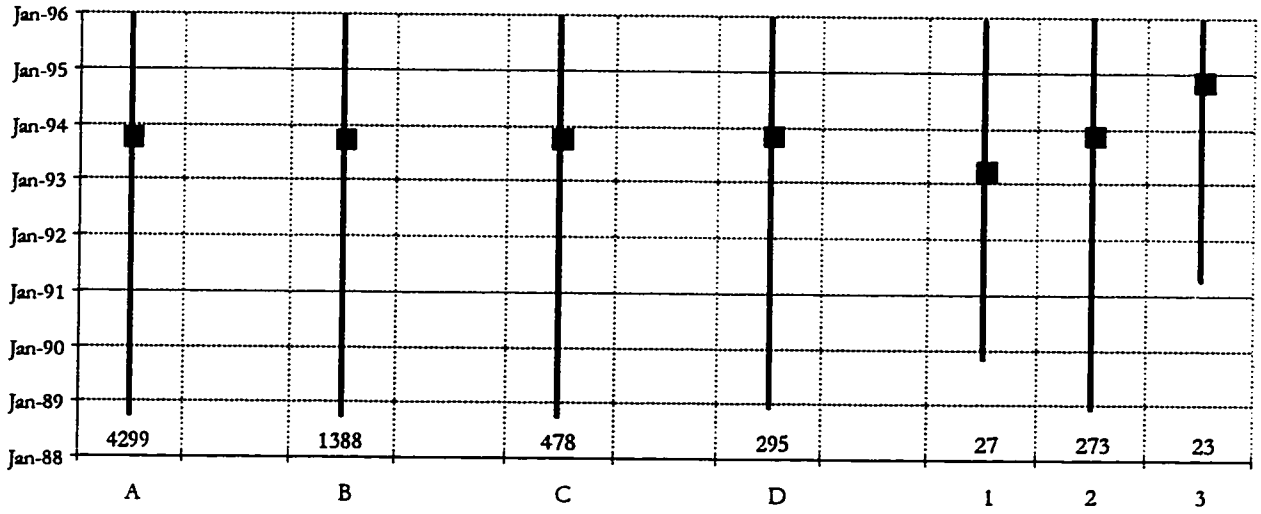


**Figure B.5. Range and Mean Incident Reporting Dates for Corrective Actions - Take Action Against Intruder**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific corrective actions or groups as follows:

**A - All Incidents**
**B - All Corrective Actions**
**C - All External Actions**
**D - All Actions Against Intruder**
**1 - Arrest**
**2 - Talk to intruder(s)**
**3 - Punish**

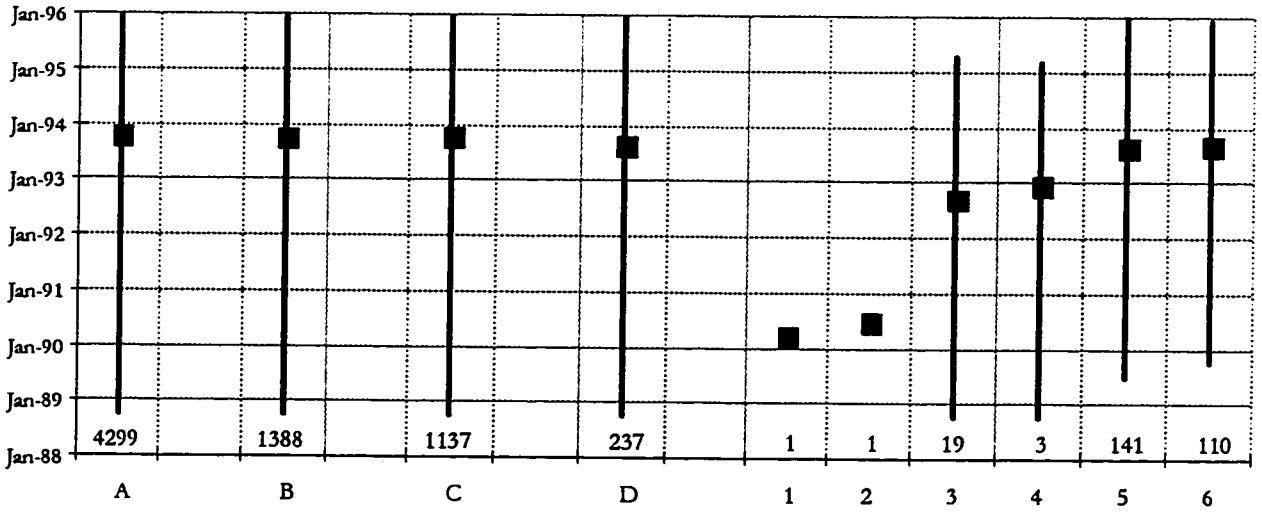


**Figure B.6. Range and Mean Incident Reporting Dates for Corrective Actions - Law Enforcement**

Large black squares indicate the mean reporting date of the incidents in that category. The first and last reporting dates are indicated by the vertical line. The number of incident records which record the particular corrective action are given by the numbers at the bottom of each column in the chart. The letters and numbers at the bottom of the chart indicate the specific corrective actions or groups as follows:

**A - All Incidents**
**B - All Corrective Actions**
**C - All External Actions**
**D - All Law Enforcement Actions**
**1 - Trace**
**2 - Investigate**
**3 - Secret Service**
**4 - Other law enforcement**
**5 - Police**
**6 - FBI**

## *Glossary of Terms*

**access** - establish a connection to a process, file or data in transit, or to read from or write to a file

**AFIWC** - the Air Force Information Warfare Center at Kelly Air Force Base, San Antonio, TX

**ANOVA** - analysis of variance

**ARPA** - the Advanced Research Projects Agency - the Defense Department's research agency that funded, through their Information Processing Techniques Office (IPTO), the development of the original Internet (at one time also known as DARPA)

**ARPAnet** - the name of the original Internet funded by ARPA

**attack** - a single unauthorized access attempt, or unauthorized use attempt, regardless of success

**authenticity** - the principle that ensures that a message is received in exactly the same form in which it is sent

**autonomous agents** - a program or program fragment which operates independently from the user to exploit vulnerabilities

**availability** - the computers, networks and files are all working and available for use

**back door** - an element in a system that allows access by bypassing access controls

**backup theft** - theft of the backup copy of data stored on a computer

**bribes** - paying for unauthorized access to information

**call forwarding fakery** - use of call forwarding to defeat systems using dial back for security

**CERT®/CC** - CERT® Coordination Center, formerly known as the Computer Emergency Response Team Coordination Center

**CIA** - Central Intelligence Agency

**CMU** - Carnegie Mellon University

**combined attacks** - combining multiple attack methods together

**computer security** - preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks

**computer virus** - see "virus" below

**confidentiality** - (secrecy) the principle that keeps information from being disclosed to anyone not authorized to access it

**corporate raiders** - employees of one company who break into computers of competitors for financial gain

**CA - corrective action** - a field in the CERT®/CC data for this incident which was used to record keywords as to the corrective actions taken in the incident

**corruption of information** - any unauthorized alteration of files stored on a host computer or data in transit across a network

**covert channel** - a communications channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy

**crack** - a common password cracking program

**cyberspace** - a popular term for the "world" of computers and networks including the Internet

**DARPA** - see "ARPA"

**data aggregation** - combining seemingly innocuous data to get confidential information

**database** - a large collection of data organized for rapid search and retrieval

**data diddling** - altering of data in an unauthorized manner before, during, or after input into a computer system

**data in transit** - packets of data that are being transmitted across a network

**data tap** - a device external to a network that can "listen" to the traffic on that network

**degradation of service** - see "denial-of-service"

**denial-of-service** - the intentional degradation or blocking of computer or network resources

**DIA** - Defense Intelligence Agency

**DISA** - Defense Information Systems Agency

**disclosure of information** -the dissemination of information to anyone who is not authorized to access that information

**distributed tool** - tools that are distributed to multiple hosts, which are then coordinated to perform an attack on a target host simultaneously after some delay

**DNS** - Domain Name System - Internet system which relates domain names and IP addresses

**domain** - a name associated with an organization, or part of an organization, to help identify systems uniquely; also a sub-tree under a location in a domain name tree (DNS)

**domain name** - a group of labels (words or letters), separated by dots (periods) that identify a host computer on the Internet

**DSB** - Defense Science Board

**dumpster diving** - searching for access codes or other sensitive information in the trash

**eavesdropping on emanations** - listening to electromagnetic signals surrounding computer and network equipment (see "Van Eck radiation")

**e-mail** - electronic mail

**e-mail overflow** - use of e-mail to flood computers with information to deny service

**e-mail spoofing** - sending e-mail with false information, such as the "from" block

**excess privileges** - obtaining capability on a system beyond that authorized

**false update disks** - sending a user or systems administrator a fake software update disk

**fictitious people** - taking on false identities

**file** - a collection of records or data designated by name and considered as a unit by the user

**FIRST** - The Forum of Incident Response and Security Teams

**FTP** - file transfer protocol - a program to transfer files between computers on a network

**GAO** - Government Accounting Office

**get a job** - defeating security by obtaining a job allowing access to privileged information or systems

**hacker** - an individual who breaks into computers primarily for the challenge and status of obtaining access

**hang-up hooking** - taking advantage of a modem that does not automatically hang up

**harassment** - using computer methods to slander or bother someone

**host** - a computer that communicates across the Internet

**human engineering** - see "social engineering"

**illegal value insertion** - using values out of limits to take advantage of software vulnerabilities

**incident** - a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing

**induced stress failures** - stressing a system to the point is begins to make errors

**infrastructure interference** - sending false signals to a satellite or microwave system

**infrastructure observation** - listening to traffic on a microwave link

**input overflow** - taking advantage of software errors that do not properly check input bounds

**integrity** - protection against forgery or tampering

**Internet** - the world's largest collection of networks that reaches universities, government agencies, commercial enterprises, and military installations; It generally uses the TCP/IP protocol suite

**internetwork** - a network of networks which has established methods of communication

**invalid values on calls** - unanticipated requests for service resulting in violations of protection

**IP address** - Internet Protocol address - a 32 bit number which serves as an address for a host on the Internet

**IP spoofing** - a method of attack in which an attacker forges the addresses on data packets sent over the Internet so they appear to be coming from inside a network within which computers trust each other

**IPTO** - Information Processing Techniques Office of the ARPA which funded the initial development of the Internet

**LAN** - local area network - a network connecting computers within a localized area such as a single building, department or site

**leakage** - when information ends up where it should not be

**listserver** - an e-mail "exploder" that sends a copy of incoming e-mail to each user on a list

**logic bombs** - a program, or portion of a program that triggers when a certain logical event occurs

**login spoofing** - simulation of a login program in order obtain passwords

**mail spam** - unauthorized or repetitive mailings that cause denial-of-service

**masquerading** - when one person uses the identity of another to gain access to a computer

**MO** - method of operation - a field in the CERT®/CC data for this incident which was used to record keywords as to the severity of an incident, and tools, and vulnerabilities used for attack

**NCS** - National Communications System

**network services attacks** - attacks against insecure network services

**NSA** - National Security Agency

**on-line** - connected to the computer network, commonly the Internet

**open microphone listening** - listening to a microphone that is open on the network

**packet insertion** - inserting a forged packet that appears from a different source; see "IP spoofing"

**password sniffing** - the use of a sniffer to "listen" for a password being sent across a network unencrypted

**packet watching** - see "sniffer"

**password guessing** - trying different guesses of passwords to defeat access controls

**PBX bugging** - exploiting flaws in a telephone system in order to listen to conversations when the phone is hung up

**process** - a program operating on a computer; an execution of a command on a Unix system

**process bypassing** - bypassing the normal controls on a business process, such as inventory control

**professional criminals** - individuals who break into computers for personal financial gain

**protection limit poking** - checking system protections for flaws

**root** - the name of the superuser on a Unix system; also, the ancestor of all files on a Unix system

**rootkit** - an Internet toolkit containing a sniffer and Trojan horse programs to hide activity and provide backdoors for later use

**salami technique** - the process of secretly and repetitively slicing away tiny amounts of money in a way that is unlikely to be noticed

**scanning** - running a program that tries a set of sequentially changing numbers

**script** - a series of commands entered into a file which can be executed by an operating system shell, such as a Unix shell

**SEI** - Software Engineering Institute at CMU (where the CERT®/CC is located)

**semaphore** - a switch in an operating system program

**sendmail** - the Unix program implementing the Internet standard for e-mail, the Simple Mail Transfer Protocol (SMTP)

**session hijacking** - taking over an authorized user's terminal session

**shell** - a command interpreter in a system such as Unix

**shoulder surfing** - watching someone enter a password or identification number

**site** - the organizational level used to track incidents for this research, and where the CERT®/CC could expect to be working with the site administrator or other authority with responsibility for the computers and networks at that site

**site name** - the domain name for the organization involved in an incident (a site)

**sniffer** - a program to monitor all data sent over a network and silently record some data

**social engineering** - the process of gaining privileged information by skillful lying, usually over a telephone

**software piracy** - unauthorized copying of copyrighted software

**spies** - individuals who break into computers primarily for information which can be used for political gain

**superuser** - a privileged user who has access to anything any other user has access to, plus all system files and processes

**sympathetic vibration** - the use of packet feedback mechanisms in network protocols to cause a network overload

**taxonomy** - agreed upon terminologies and principles of classification in a field of inquiry

**TCP/IP** - Transmission Control Protocol/Internet Protocol - the suite of protocols establishing the principle method of communication on the Internet

**telnet** - a program to connect to and remotely operate a computer over a network

**terrorist** - an individual who breaks into computers primarily to cause fear which will aid in achieving political gain

**TFTP** - trivial file transfer protocol - a program for transferring files between computers on a network

**theft of service** - the unauthorized use of computer or network services without degrading the service to other users

**time bomb** - a logic bomb who's condition is based on time

**timing attacks** - attacks that take advantage of the timing of computer processes and operations

**toll fraud networks** - networks of people shoulder surfing for information that is quickly distributed

**toolkit** - a software package contains scripts, programs, or autonomous agents that exploit vulnerabilities

**traffic analysis** - collection and analysis of information, particularly through the analysis of message characteristics

**trap door** - see "back doors"

**Trojan horse** - a program that performs like a real program a user may wish to run, but also performs unauthorized actions

**tunneling** - use of one data transfer method to carry data for another method

**Unix** - an operating system developed by Ken Thompson and Dennis Ritchie in 1969; it is the predominant operating system for high-performance microprocessors

**use or condition bombs** - see "logic bomb"

**vandals** - individuals who break into computers primarily to cause damage

**Van Eck radiation** - electronic emanations surrounding a computer, particularly the monitor

**video viewing** - monitoring video signals on a network

**virus** - a segment of computer code that will copy its code into one or more larger "host" programs when it is activated; it also may perform other unauthorized actions at that time

**vulnerability** - a flaw in a computer or network allowing unauthorized use or unauthorized access

**Web site** - a set of files on a host computer that can be linked to over the Internet using special client software known as a Web browser

**wiretapping** - physically picking up data flowing across a network from outside the network

**worm** - an independent program that can travel from host to host across a network

**ZONE** - Zealot of Name Edification - a program for recording domain names and IP addresses on the Internet