CERT RESEARCH ANNUAL REPORT

2008

Software Engineering Institute | Carnegie Mellon

Software Engineering Institute
Carnegie Mellon

The primary goals of the CERT® Program are to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of attacks, accidents, or failures.

CERT is part of the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University. The SEI advances software engineering and related disciplines to ensure systems with predictable and improved quality, cost, and schedule.

This report describes how CERT research advanced the field of information and systems security during the 2008 fiscal year.

To download a PDF version of this annual report, go to http://www.cert.org/research/2008research-report.pdf

TABLE OF CONTENTS

CERT Research Vision

One of the challenges CERT has faced over the years is that attention to system security, particularly proactive security measures, was not a priority for the majority of users. I am excited to see that trend changing—vendors are doing a better job of incorporating security into their software and establishing practices for addressing vulnerabilities, home users are more knowledgeable about risks, and system administrators are implementing strategies at the network level to protect their systems. But the need to tackle tough research problems remains.

It is tempting to focus on isolated solutions to specific problems, but the span and interconnections of networked systems requires a more comprehensive approach. Our research reflects that approach in focusing on four principal objectives:

- Embed software and system assurance techniques in all aspects of the system development life cycle.
- Improve the effectiveness of the international intrusion analysis and response team community.
- Develop an international workforce skilled in secure cyber operations.
- Improve the survivability and resiliency of critical networked information systems.

At the software level, we are developing secure coding practices and methods for discovering vulnerabilities in software before they are exploited, and are introducing advanced technologies for malware analysis. At the system level, we are focusing on addressing security as an integral part of the development process. Our projects focused on network situational awareness allow system administrators to examine traffic on their networks to identify problems and trends. We are developing tools and techniques for organizations to implement security policies at the enterprise level, and our research into insider threats helps organizations understand one of the most serious risks they face. And the popularity and scope of our work in computer forensics continues to grow. We are also working with a variety of organizations around the world to understand shared problems and collaborate on solutions.

The sophistication of technology and attack methods continues to evolve rapidly, and we must develop mitigation strategies and solutions at the same pace. The need to maintain constant vigilance and awareness of the threat landscape is important, and organizations need to keep security awareness at the forefront. Security policies must be dynamic and adapted as necessary to address the evolution of the threats.

Striving to achieve these objectives requires our own best efforts, as well as cooperation and collaboration within the community we serve. In our third decade of work, we will continue to promote and rely on cooperation and collaboration within the security community. We welcome participation by organizations that share our belief that the networked environment of the future can provide safe and secure computing for all participants in the global information community.

Rich Pethia
Director, CERT
Software Engineering Institute
Carnegie Mellon University

Executive Summary

The work of the CERT Program at Carnegie Mellon University's Software Engineering Institute includes technologies and methods for

- eliminating security flaws and vulnerabilities in systems
- preventing intrusions from occurring
- identifying intrusions that have occurred
- preserving essential services when systems have been penetrated and compromised
- providing decision makers with information required for network defense

We recognize the importance of multiple strategies for prevention and detection of and recovery from cyber security attacks, and the CERT Program has been designed to address a broad spectrum of security technology research, development, and transfer.

In our research activities, the goal is to replace informal methods with precise software and security engineering. In our technology development work, we create software and security standards, technologies, and automation. In technology transfer, we work with clients to incorporate results into key acquisition and development projects. We also provide training and materials, such as books and articles, to support technology transfer.

While all these elements are necessary to achieve success, the focus of this report is on CERT's research work. Our research agenda is driven by the need to develop theoretical foundations and engineering methods to help ensure the security of critical systems and networks. We believe the projects described in this report are essential elements of this agenda. Abstracts are provided here for our major research projects, followed in the report by more detailed descriptions of the projects. Additional research activities, publications, and technical leadership activities are also described.

An Evaluation of Architectural Information Security Defenses

Many information security techniques have been proposed and implemented in the last three decades. However, there has been little empirical evaluation as to the effectiveness of these techniques in addressing modern attacks. This report describes research that enables evaluation of these architectural defenses from live-network data, allowing incorporation of real-world threats to the evaluation of these defenses without increasing the risk to the networks under observation. Security improvement decisions are often made on the basis of theoretical security gains or to match common practice, rather than on the basis of how much security improvement an investment may yield. This research describes a methodology for substantive evaluation of defenses against real-world threats, without increasing the risk on network operations.

An Insider Threat Risk Mitigation Framework

CERT's research into insider threat cases conducted since 2001 has gathered data about actual malicious insider incidents, including IT sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to the critical infrastructure of the United States. CERT's insider threat work, referred to as MERIT (Management and Education of the Risk of Insider Threat), uses the wealth of empirical data collected by CERT to convey the "big picture" of the insider threat problem—the complexity of the problem, relative degree of risk, and unintended consequences of policies, practices, technology, insider psychological issues, and organizational culture over time. As part of MERIT, this report describes our development of an Insider Threat Risk Mitigation Framework.

This framework merges technical, organizational, personnel, and business security and process issues into a single, actionable instrument that enables organizations to gain a better understanding and manage the risk of insider threat. The instrument will be structured to encompass all stakeholders in the fight against insider threat: management, information technology, human resources, legal, data owners, and physical security.

A Trojan by Any Other Name: Analysis of Malware Naming Conventions Across Vendors

The number of unique malicious files on the Internet is increasing exponentially. With the advent of polymorphic code that changes as it replicates, more malware analysts are focusing on studying behavioral traits and "familial" relationships between unique files. In this research, we extract families, variants, and behavior characteristics from published names from antivirus (AV) vendors. We also develop metrics to capture classification agreement across vendors that allows for aliasing of names. We analyze an archive of 6.4 million unique malicious files encountered by AV-test.org, an independent company that performs tests of AV software.

Computational Security Attribute Analysis

In the current state of practice, security properties of software systems are often assessed through labor-intensive human evaluation. These a priori evaluations can be of limited value in the dynamics of system operation, where threat environments can change quickly. This project focuses on automated analysis of the security properties of software. The goal is to develop foundations to help transform security engineering into more of a computational discipline.

Critical Infrastructure Cyber Risk Analysis

Every level of government and industry participates in risk analysis and management efforts to examine threats, vulnerabilities, countermeasures and protective programs, and consequences related to U.S. critical infrastructures. Coordinated or not, there is an overriding need to protect productive infrastructure activities and functions from harm that is understood by individual companies as well as the U.S. government. In the past, the traditional physical protections afforded critical sector-based functions and productivities have served well

to prime the risk analysis mindset, but cyber risk analysis presents a unique opportunity to examine risks based on both the physical and logical domain spaces. In 2008, we began to examine the structured process necessary to conduct, facilitate, and participate in a national-level critical infrastructure risk assessment. In 2009, we plan to codify distinct cyber risk components and improve analysis capabilities for projections of threat, vulnerability, and consequence.

Direct Response to Spam Email

Spam is a large and growing problem on the Internet. Traffic statistics vary in their estimates, but between 60% and 80% of the email on the Internet appears to be spam email. While many approaches have been identified for detection and reduction of spam, little work has been done on the operationally important issue of detecting individuals who respond to spam from within an organization. This report describes an initial approach to detection of spam responses, specifically emailed responses. Acting on spam email has been associated with numerous forms of damage, including installation of malware, financial compromises, disclosure of proprietary information, and identity theft. By determining when individuals in the organization are responding to spam email, the exposure to these forms of damage can be assessed. Identification of the individuals involved enables managerial and technical remediation to these forms of damage and improvement of the individual's behavior. The results of this research are currently an operational script to identify emailed response; in future the research will be generalized to non-email responses to spam.

Foreign Cyber Influence Analysis

Nations require an ability to determine the degree to which they depend on and are influenced by foreign partnerships, investments, and operations. However, in terms of effects to ongoing national critical infrastructure protection efforts, many foreign influence situations are examined only at the point of supply chain onset or investment. In 2008, our work examined cases of influence tied to investment in U.S. critical infrastructures, using what-if scenarios and projections of near-term consequences to industry, government, and essential paradigms such as national security. In 2009, we plan to examine and document the analysis requirements for more longitudinal, holistic trends and patterns, which can be used to detect emerging behaviors and emergent properties.

Function Extraction Technology for Software Assurance

CERT recognizes the importance of software assurance to national defense. Software assurance depends on knowing and verifying the complete behavior of software, because behavior that is not known can contain errors, vulnerabilities, and malicious content. To help address this need, CERT is evolving and transitioning the emerging technology of function extraction (FX). The goal is to compute the behavior of software with mathematical precision to the maximum extent possible. Computation of the behavior of malicious code is a particular focus, to help analysts quickly determine intruder objectives and develop countermeasures.

Identifying Port-Specific Network Behavior

A port is an integer value between 0 and 65535 that represents a logical connection place for TCP and UDP communications. Increasing trends in traffic volume on specific ports may indicate new interest in a vulnerability associated with that port, and this activity can precede Internet-wide attacks. Port-specific behavior can also arise from stealthy applications that migrate to different ports in order to evade firewalls. In this analysis, we use a method based on statistical outlier detection and time series analysis to determine unusual port-specific network behavior. We apply the method to the hourly count of incoming records for a large network over a period of three weeks.

Making Business-Based Security Investment Decisions – A Dashboard Approach

The Security Investment Decision Dashboard is one approach for selecting security investments using business-based criteria. The approach and supporting tool define seven decision criteria categories, each supported by three or more indicators. Categories and indicators are ranked and applied to a series of investments. Individual investment scores are presented for discussion and evaluation by decision makers. The Dashboard can be used to rationalize and prioritize any class of security investments including security governance, operational resilience, and software assurance.

Process Improvement in Managing Operational Resiliency Using the CERT Resiliency Engineering Framework

Operational resiliency is an emergent property of organizations that are effectively managing operational risk activities such as security, business continuity, and IT operations. Many organizations are managing these activities in a compartmentalized and ad hoc manner and are often overly reliant on a small number of knowledgeable heroes. Research at CERT is applying process maturity concepts to operational risk management activities. A process approach can be used in organizations to implement, mature, and continuously improve these risk management activities so that they become ingrained into the organization's culture, governance, and strategy. This acculturation of the resiliency process prepares the organization to confidently respond in times of crisis or threat and reduces its reliance on heroics and discrete reactions. The CERT Resiliency Engineering Framework codifies this process maturity approach for the implementation, management, and continuous improvement of operational resiliency activities. This article describes the process maturity features implemented in the framework, explains how the framework provides usable guidance for maturing an organization's processes, and distinguishes this maturity approach from others.

PySiLK – A Language for Scripted Flow Manipulation

The System for internet-Level Knowledge (SiLK) analysis programs are powerful tools for the analysis of network flow data. As flexible as these tools are, they are designed to do specific types of analyses. The programmers of these tools cannot predict all possible types of analysis. Consequently, users will always find features that they wish the current tools had implemented and will come up with ideas for completely new tools for new types of analysis. By enabling easer tool modification, PySiLK enables both more efficient customization of analysis to meet user needs and more rapid creation of new analysis methods to meet emerging needs. This report describes the evolution and implementation of PySiLK and several of the enabled analytical results.

Secure Coding Initiative

The Secure Coding Initiative (SCI) was established to work with software developers and software development organizations to eliminate vulnerabilities resulting from coding errors before they are deployed. The SCI is building a comprehensive approach to secure software development in the C, C++, and Java programming languages. The goal of this effort is reduce the number of vulnerabilities deployed in operational software by preventing their introduction or discovering and eliminating security flaws during implementation and test. Specific projects include the development and extension of secure coding standards, static analysis tools, application certification processes, and education and professional training courses.

SQUARE: Requirements Engineering for Improved System Security

Through the SQUARE project, CERT researchers have developed an end-to-end process for security requirements engineering to help organizations build security into the early stages of the production life cycle. The SQUARE methodology consists of nine steps that generate a final deliverable of categorized and prioritized security requirements. The process has been baselined and transition to real-world clients has shown that the methodology can be incorporated into industry practice. A prototype tool and educational and training materials have been developed for SQUARE.

STAR*Lab: A Software Development Laboratory for Security Technology Automation and Research

STAR*Lab is an internal software development capability that CERT employs to create theory-based prototype automation that addresses challenge problems in security engineering and software assurance. STAR*Lab is currently engaged in evolution and transition of function extraction technology for computing the behavior of software, with focus on malicious code analysis, and is ready to expand the technology in pilot projects for correctness verification, computational analysis of security attributes, and component composition in network systems.

Support for Automated Software Correctness Verification

In the current state of practice, no practical support exists for automated, large-scale correctness verification of software with respect to intended behavior. As a result, much time and energy is devoted to inspection and testing activities that can provide only limited evidence of correctness. The objective of this project is to develop a proof-of-concept prototype of a function verification system that will help analyze the correctness of programs.

Support for Component Integration in Network Systems

Modern systems are characterized by large-scale heterogeneous networks with many components that must be correctly integrated to achieve mission objectives. System integration today is a complex, labor-intensive process that can take months or even years for large systems. The objective of this project is to develop a proof-of-concept prototype of a component composition system that will help determine the net effect of combining components in network architectures for faster integration.

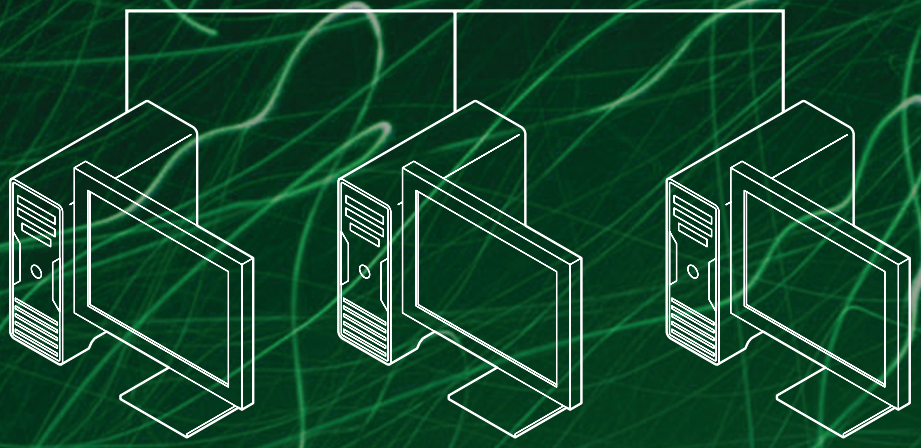
System of Systems Assurance Framework

The System of Systems Assurance Framework (SoSAF) was developed to provide a structured view of people, process, and technology, to help organizations characterize the complexity of multi-system and multi-organizational business processes. Assurance gaps arise when assumptions and decisions within one component are inconsistent with those of another. The complexity as systems are connected into systems of systems is an aggregate of technology, scale, scope, operational, and organizational issues. This research effort has expanded to address the need for analytical capability of services such as components of a service-oriented architecture and the integration of these shared services with organizational mission. Through the analysis of business (mission) threads in end-to-end workflows and the identification of potential stresses that could limit completion of the workflows, the interrelations among people, processes, and technology are analyzed to identify critical patterns for simplification, support for assurance, and reduction in mission failure.

Understanding Anycast Routing Behavior

The network behavior of DNS root servers, IP version 6 tunnel brokers, and the AS112 project is not widely understood because they use a mechanism known as *anycast*. Anycast is an addressing and routing technique that allows a global destination IP address to represent any number of devices, anywhere on the Internet, without any indication of the home network of the device. This report discusses anycast routing behavior and a method that uses active traceroute probing to identify devices on the Internet.

An Evaluation of Architectural Information Security Defenses



Timothy Shimeall

An Evaluation of Architectural Information Security Defenses

Problem Addressed

Many information security techniques have been proposed and implemented in the last three decades. However, there has been little empirical evaluation as to the effectiveness of these techniques in addressing modern attacks. What evaluation has been done has largely been in controlled environments using artificially generated network operations, with results that have been called into question [1]. Even more problematic is the evaluation of network architecture choices from the point of view of information security. These choices, which affect the flow of network traffic, offer the opportunity for increased network performance and connectivity, but also offer differing exposure to information security threats. To deal with these threats, defenses such as firewalls, honeynets, intrusion prevention systems, and tarpits have been proposed and implemented. This report describes research that enables evaluation of these architectural defenses from live-network data, allowing incorporation of real-world threats to the evaluation of these defenses without increasing the risk to the networks under observation.

Benefits

Decision makers wishing to improve the security of their networks have many choices but little objective data on the performance or expected improvement from each option. Therefore, decisions are often made on the basis of theoretical security gains or to match common practice rather than on the basis of how much security improvement an investment may yield. This research will change that dynamic, offering substantive evaluation of defenses against real-world threats.

Research Approach

One approach to this problem would be to interview network administrators, determine their security architectures, and then observe the network reactions to real-world security threats. However, organizations have an understandable reluctance to disclose details of their security practices, and it is difficult to scale the human-intensive approach of interviewing the operators of each individual network across large address spaces. The approach taken in this research starts from analysis of network architectures. Figure 1 shows a sample network architecture. Differing architectures will have different traffic characteristics, permitting recognition of the architecture from the traffic to and from the network.

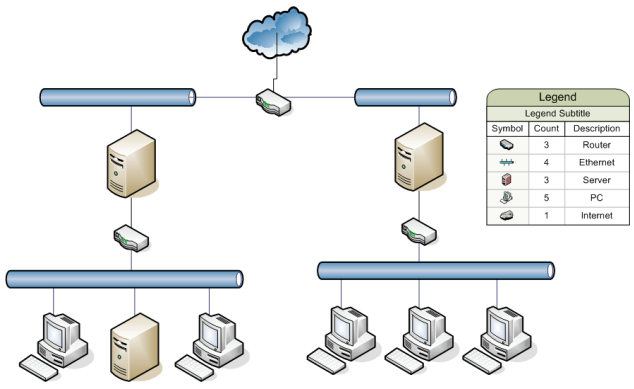


Figure 1: Sample Network Architecture

As a population of different network architectures is identified, behavioral observation of the responses to network attack is facilitated. This allows us to identify network characteristics that respond better or worse to various forms of vulnerability and exploitation. Measurement of the impact of these characteristics by the network will lead to objective understanding of the effectiveness of the architectural defenses on networks.

2008 Accomplishments

During FY2008, an initial catalogue of network architectures and their recognition characteristics was constructed. While the recognition characteristics were expressed informally, they were expressed in detail. Also, an initial analysis of the role of architectural defenses in improving network security was developed and carried to a level where traffic characteristics of network defense could be identified.

Finally, during FY2008, theoretic investigations of the differences in attack response due to network architectures were performed, to lay a basis for follow-on quantitative work.

2009 Plans

During FY2009, the research will formalize the network identification characteristics into operational models of architecture recognition. These models will be evaluated using anonymized data derived from public network flow data archives. As they mature, the models will be transitioned to better inform large-scale network operations as to the variety of architectures under their purview. Also during FY2009, models of attack response (indications as to whether a given network attack had been successful) will be developed, incorporating work described elsewhere in the *2008 CERT Research Annual Report* (e.g., botnet beaconing [2] and spam response [3]). These two efforts will then be fused to provide quantitative results for network architectural defense evaluation.

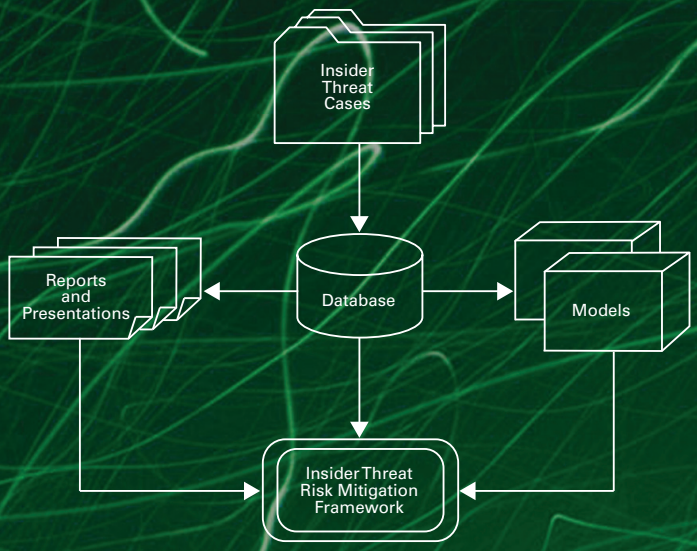
References

[1] McHugh, J. "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory." *ACM Trans. Inf. Syst. Secur. 3*, 4 (2000): 262–294.

[2] Krystosek, P. "Detecting Network Beacons," *2008 CERT Research Annual Report.*

[3] Shimeall, T. "Direct Response to Spam Email," *2008 CERT Research Annual Report.*

An Insider Threat Risk Management Framework



Dawn Cappelli

Andrew Moore

Randall Trzeciak

An Insider Threat Risk Mitigation Framework

Problem Addressed

An identity theft ring composed of six individuals stole identities of at least 25 people and used the identities to defraud 10 financial institutions and 25 retailers in multiple states a total of $335,000 over a four year time period. The ringleader carefully recruited participants, each with a specific role in the scheme. Two conspirators were recruited because they held positions in financial institutions with access to confidential customer data. A loan officer at a mortgage company stole personal and financial information of customers applying for a mortgage with her company, and an employee at an escrow firm stole financial information of her company's clients. The information was used by two members of the crime ring with equipment to create counterfeit driver's licenses. The remaining conspirators used the licenses to open new credit accounts with banks and retailers, purchased goods and services with the new accounts, and drained the cash from existing checking and savings accounts of the victims.

CERT's research into insider threat cases like these conducted since 2001 has gathered data about actual malicious insider incidents, including IT sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to the critical infrastructure of the United States.[1] Consequences of malicious insider incidents include financial losses, operational impacts, damage to reputation, and harm to individuals. The actions of a single insider have caused damage to organizations ranging from a few lost staff hours to negative publicity and financial damage so extensive that businesses have been forced to lay off employees and even go out of business. Furthermore, insider incidents can have repercussions extending beyond the affected organization, disrupting operations or services critical to a specific sector, or resulting in issuance of fraudulent identities that create serious risks to public safety and national security.

CERT's insider threat work, referred to as MERIT (Management and Education of the Risk of Insider Threat), uses the wealth of empirical data collected by CERT to convey the big picture of the insider threat problem—the complexity of the problem, relative degree of risk, and unintended consequences of policies, practices, technology, insider psychological issues, and organizational culture over time[2] [1,2]. As part of MERIT, we are developing an Insider Threat Risk Mitigation Framework that enables organizations to gain a better understanding and manage the risk of insider threat. It will merge technical, organizational, personnel, and business security and process issues into a single, actionable framework. As in our past projects, the project team includes psychological and technical expertise. The instrument will be structured to encompass all stakeholders in the fight against insider threat: management, information technology, human resources, legal, data owners, and physical security.

Research Approach

Figure 1 depicts our data-centered research approach to developing the MERIT Insider Threat Risk Mitigation Framework. It is based on the collection of real insider threat compromises that have been prosecuted in the United States. Starting in 2002, we collaborated with U.S. Secret Service (USSS) behavioral psychologists to collect approximately 150 actual insider threat cases that occurred in U.S. critical infrastructure sectors between 1996 and 2002, and examined them from both a technical and a behavioral perspective. Over the past three years, Carnegie Mellon's CyLab[3] funded us to update our case library with more recent cases. One hundred additional cases were collected and coded in our insider threat database, bringing the case library to a total of nearly 250 cases.

Our data collection process has been guided by the development of codebooks that detail behavioral, organizational, and technical aspects of the cases. CERT staff collects information from court documents, media reports, and interviews with convicted insiders, victim organizations, investigators, and prosecutors. All data regarding insider motivation, planning, technical preparatory actions, technical details of the incident, detection, and more is stored in a database management system.

This approach facilitates ongoing, evolving analysis for multiple purposes. For instance, we have published reports detailing motive, planning behaviors, technical actions, and detection of insider threats. Three reports have been published describing insider incidents in critical infrastructure sectors in the United States: the banking and finance sector, the information technology and telecommunications sector, and the government sector.

One report analyzed insider IT sabotage attacks across all critical infrastructure sectors. We produce regular updates to the *Common Sense Guide to Prevention and Detection of Insider Threats* [3], which describes practices that organizations can adopt to mitigate the risk of the insider compromises that we've seen in the cases collected.

We also develop models that describe the insider threat problem as it evolves over time by conducting a series of meetings involving a group of domain experts. Our approach to group modeling is based on the system dynamics methodology. System dynamics is a method for modeling and analyzing the holistic behavior of complex problems as they evolve over time. Group model building involves bringing

1 "Insiders" include current and former employees, contractors, and other business partners who have or had authorized access to their organization's systems, data, and networks. Insiders are familiar with internal policies, procedures, and technology and can exploit that knowledge to facilitate attacks and even collude with external attackers.

2 CERT/CyLab's insider threat research is published on http://www.cert.org/insider_threat. Early research was funded by the USSS and the Department of Homeland Security, Office of Science and Technology. Our current work, including MERIT, was funded by Carnegie Mellon University CyLab.

3 http://www.cylab.cmu.edu/

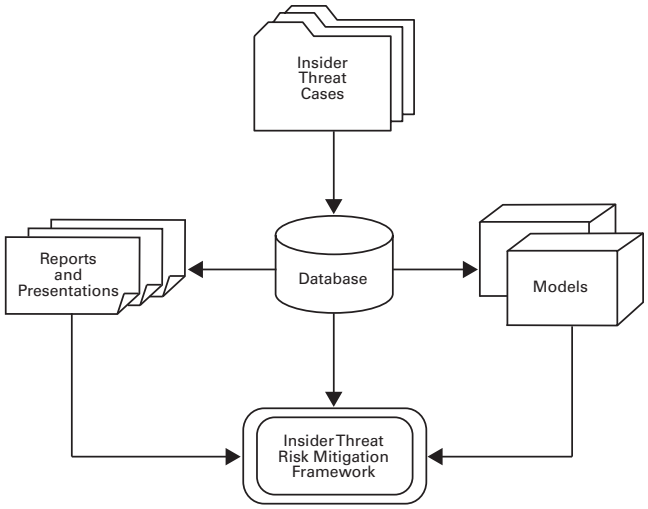


Figure 1: Origins of the MERIT Insider Threat Risk Mitigation Framework

together individuals with a range of domain expertise to build dynamic theory based on case study research. Over the years, we've brought together behavioral scientists, psychologists, and historians to complement CERT's technical understanding of the problem to build system dynamics models that capture the nature of the insider threat problem and how it evolves over time [3].

Results documented in our reports and insights gained through our modeling efforts are used to develop and inform the MERIT Insider Threat Risk Mitigation Framework. Applying the framework will help organizations to evaluate the controls they have in place to prevent the actions that have been exploited by insiders in the cases we have reviewed. The framework is broadly scoped to address technical, organizational, personnel, security, and process issues.

Expected Benefits

The ultimate effect of business policy and technical decisions on insider threat risks is complex and often counterintuitive, and can result in significant losses and operational impacts due to insider cyber attack. This work identifies and validates policies, practices, and technologies—helping decision makers better understand insider threat risks and the effects of decisions on the promotion or mitigation of those risks. The results of our work will empower organizations to develop comprehensive, efficient, and justifiable defenses against insider threats along with the organizational understanding and support needed to maintain a strong security posture over time. Broad application of concepts developed will enable organizations across the U.S. and abroad to significantly reduce their risk and losses due to insider attacks. The capability that will result from this work promotes the security, survivability, and resiliency of all government, military, and commercial critical systems. The ultimate beneficiaries will be organizational stakeholders and, where the U.S. critical infrastructures are better protected, the general public.

2008 Accomplishments

A crucial step in creating the framework was to capture in our database specific vulnerabilities or areas of concern that were exploited in each case, including technical vulnerabilities, exploits that were facilitated by oversights in business processes, human resources functions, organizational policies and practices, and legal issues. More than 1,300 detailed vulnerabilities/exploits were identified and organized into over 100 categories to be addressed in the framework.

We used those categories to create an insider threat taxonomy, which was transformed into a series of detailed questions that forms the basis of the assessment instrument. The questions were organized into a set of workbooks. Each workbook targets a specific audience within an organization, e.g., information technology, human resources, data owners, management, physical security, software engineering, and legal.

Much of our effort in previous years has focused on the area of insider IT sabotage [4] and espionage against the U.S. [1]. Our effort over the last year has focused on analyzing cases of insider theft and insider fraud to identify patterns of insider behavior, organizational events or conditions, and technical issues across the cases. The initial analysis of 87 theft cases and 49 fraud cases revealed an unexpected finding: the patterns identified actually separated the crimes into two different classes than originally expected:

- Theft or modification of information for financial gain – This class includes cases where insiders used their access to steal information that they sold to outsiders or to modify information for financial gain for themselves or others. Insiders in this class were generally current employees in relatively low-level positions, with a fairly equal split among male and female perpetrators. Insiders stole personally identifiable information or customer information, or modified data. The majority of crimes were committed during normal working hours using authorized access.
- Theft of information for business advantage – This class includes cases where insiders used their access to organization systems to obtain information that they used for their own personal business advantage, such as obtaining a new job or starting their own business. This class includes cases of "industrial espionage," although we found that insiders did not attempt to sell trade secrets for financial gain but instead stole trade secrets to take to a new job or to give to a non-U.S. government or a non-U.S. based organization. Insiders in this class were all men, most in technical positions, but some in sales. The majority of the insiders stole intellectual property and customer information during normal working hours, most using authorized access. Those who did not use authorized access were all former employees.

There are some interesting differences between the two classes of theft that influence how they are detected. When financial gain is the specific motive, crimes tend to involve theft of small amounts of data (e.g., social security numbers), repeatedly, over long periods of time. When business advantage is the motive, crimes tend to involve much larger amounts of data (e.g., proprietary source code) and often occur within three weeks of the insider's resignation. Both types of crime have a high rate of collusion with both insiders and outsiders. This behavior, if detected, provides an opportunity for an organization to identify a higher risk of insider theft and act on those foresights.

We compiled statistics that will inform organizations on cost-effective defenses to the insider threat. While our findings are too numerous to describe in full detail here, we will provide one example of a cost-effective defense. A striking finding is that in over two-thirds of the cases of theft for financial gain, the insider was recruited to steal by someone outside the organization. In many of these cases, the insider was taking most of the risk, while receiving relatively small financial compensation. Often the outsider was a relative of the insider or an acquaintance who realized the value of exploiting the insider's access to information. This suggests that organizations should educate employees on their responsibilities for protecting the information with which they are entrusted and the possibility that unscrupulous individuals will try to take advantage of their access to that information.

2009 Plans

We plan to apply the Insider Threat Risk Mitigation Framework within particular organizations interested in better understanding and mitigating their own insider threat risk. The workbooks will be used to assess organizational vulnerability to insider threats via a series of face to face interviews with members from across the organizations. We provide organizations with a confidential report on the findings of the assessment and suggestions for improvement. We are also seeking opportunities for collaboration with organizations, such as review of the instrument and confidential sharing of insider cases and/or best practice information for inclusion in the instrument.

The Insider Threat Risk Mitigation Framework provides an excellent opportunity for organizations to work more closely with CERT to understand the significance of the insider threat for their particular environment based on empirical evidence. As with all of our insider threat research, all collaborations will remain confidential and no references will ever be made to any organizations and/or individuals.

References

[1] Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. "The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures" in *Insider Attack and Cyber Security: Beyond the Hacker,* eds. Stolfo, S.J., et al., Springer Science + Business Media, LLC, 2008. Also published as an SEI technical report, CMU/SEI-2008-TR-009. http://www.cert.org/archive/pdf/08tr009.pdf

[2] Greitzer, F., Moore, A. P., Cappelli, D. M., Andrews, D., Carroll, L., & Hull, T. "Combating the Insider Cyber Threat". *IEEE Security & Privacy* (Jan./Feb. 2008): 61–64. http://www.cert.org/archive/pdf/combatthreat0408.pdf

[3] Cappelli, D. M., Moore, A. P., Shimeall, T. J., & Trzeciak, R. J. *Common Sense Guide to Prevention and Detection of Insider Threats: 3rd Edition.* Report of Carnegie Mellon University, CyLab, and the Internet Security Alliance, Sept. 2008 (update of earlier editions). http://www.cert.org/archive /pdf/CSG-V3.pdf

[4] Moore, A. P., Cappelli, D. M., Joseph, H., Shaw, E. D., & Trzeciak, R. F. "An Experience Using System Dynamics Modeling to Facilitate an Insider Threat Workshop." *Proceedings of the 25th International Conference of the System Dynamics Society.* July 2007. http://www.systemdynamics. org/conferences/2007 /proceed/papers/MOORE349.pdf

[5] Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., & Trzeciak, R. F. *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis* (CMU/SEI-2006-TR-026). Software Engineering Institute, Carnegie Mellon University, 2006. http://www.cert.org/archive/pdf /06tr026.pdf

A Trojan by Any Other Name: Analysis of Malware Naming Conventions Across Vendors

Rhiannon Weaver

Matt Sisk

A Trojan by Any Other Name: Analysis of Malware Naming Conventions Across Vendors

Problem Addressed

The number of unique malicious files on the Internet is increasing exponentially. In the past, malware analysts have catalogued malicious files keyed by a unique hash of the bytes in the file. But new hacker trends are making organization by unique file difficult. For example, polymorphic viruses [1] change as they replicate, and a single "outbreak" can result in thousands of unique individual files. Similar file structures do not translate to similar hash values, so relational information between files is lost. This makes it difficult to study trends in behavioral threats and attribution solely using hashes.

One way to better understand trends in the population is to categorize malware into families and variants and to look at behavioral traits. This imposes some structure and relationships on the ever-growing number of unique files. But categorization can be an expensive task, and it is also subject to interpretation. Much antivirus (AV) software includes behavioral information, as well as classifications of a family or variant, in the name returned to the user when a malicious file is recognized. But it is not always clear how internally consistent these naming conventions are, or how comparable names are across different vendors.

Research Approach

The research approach consists of two steps:

- internal name analysis
- cross-vendor agreement

In internal name analysis, we analyze return strings within each vendor, compiling canonical descriptions indicating malware behavior, targeted platform or propagation medium, family, and variant (if present) associated with each file. In cross-vendor agreement, we introduce a metric to compare consistency in family names across vendors, allowing for aliasing of names across vendors.

Two AV vendors, A and B, agree on a family classification when the set of files that A assigns to its internal family M is the same set of files that B assigns to an internal family N. This definition allows for aliasing; A and B may choose different names to assign to a collection of files, but the collection has the same elements across both vendors. On the other hand, the overlap could be imperfect. Suppose A assigns name M to a set of files, and B assigns name N to 80% of those files but different names to the other 20%. A and B agree, but not fully.

For each set of names in A, the *modal proportion* of B's names is the proportion associated with the most popular name in B for the elements of the set (0.80 in the example). The *average modal proportion*, AMP(A, B), is the average of B's modal percent across all unique family sets in A, weighted by the size of the set. As a metric, AMP(A, B) ranges from 0 to 1, with 0 indicating disagreement and 1 indicating agreement. It is also asymmetric: in general, AMP(A, B) is not equal to AMP(B, A).

Both AMP(A,B) and AMP(B,A) should be high to indicate strong agreement. As a clarifying example, consider the situation where A classifies files into many families, but B simply assigns every file the same name (for example, "generic virus"). In that case AMP(A, B) is equal to 1, which would indicate high agreement. But B is penalized in reverse, as AMP(B, A) is equal only to the size of A's largest set divided by the total number of files being compared. On the other hand, suppose B assigns every file a different family name. Then AMP(B, A) is equal to 1, but AMP(A, B) is equal to the number of unique family names in A divided by the total number of files being compared.

In practice, we use a Monte Carlo method for calculating a baseline level of disagreement for AMP, under the assumption that two vendors assign their names arbitrarily among available files.

Benefits

The names and categorizations that a vendor returns, in addition to a simple classification of a file as "safe" or "unsafe," reveal insights into the vendor's analysis of the file. Names reflect behavioral and relational traits that can be extracted even if the original file is not shared, or if it is not analyzed in-house. This information can be used to leverage vendor analysis in building relationships among unique files in a large corpus or catalogue, giving a coarse-grained, scalable labeling method for files that may otherwise have little associated information.

Agreement metrics also provide an outsider's view of inter-relationships in the vendor community. Vendors share information and methods among each other, and this dependence has implications for applications such as CloudAV [2] that rely on "majority vote" techniques for classification and analysis. Agreement metrics are a principled method for quantifying the extent of this co-operation among vendors. Finally, as more detailed and accurate categorizations arise, we can use agreement metrics to measure and rank vendors against a trusted standard.

2008 Accomplishments

In 2008, we implemented a system that analyzes AV vendor return strings and builds a common dictionary of platforms, operating systems, and behavioral traits across vendors. The system facilitates parsing of a rule set for name structures within a vendor by allowing an analyst to easily sort through common patterns and set any vendor-specific rules. Modular development allows easy integration of new vendors and new rules. Descriptive traits, as well as potential family names and variant names, are extracted automatically and summarized in a comma delimited file.

We applied internal name analysis and cross-vendor family agreement to eight AV vendors: Avast, AVG, BitDefender, ClamAV, Fortinet, FProt, Kaspersky, McAfee, Sophos, and Virusbuster. Vendors were compared based on results gathered from an archive of 6.4 million unique malicious files encountered by AV-test.org, an independent company that performs tests of AV software, from its inception through September of 2007.

An example of the breakdown of family names and traits observed for files classified by Kaspersky is shown in Figure 1. Table 1 shows the results of the cross-vendor agreement metric AMP(A, B) for the vendors. Baseline values (not pictured) were all considerably lower than observed values, indicating a general trend of agreement and principled name assignment among all vendors. Though F-Prot has the highest column totals across vendors, its row totals are low, suggesting that F-Prot uses a generally coarser naming scheme than other vendors. Kaspersky and BitDefender (blue shaded squares) appear to be the only two vendors that share high affinity (greater than 2/3 AMP) in both directions.

2009 Plans

We plan to use vendor agreement metrics to drive inference both for malicious code and for comparisons between AV vendors. For malware analysis, we are currently using descriptors such as family, variant, and behavior as predictors in a model that estimates the population size, average lifetime, and relative risk of detection and remediation for malicious files with certain traits. Agreement metrics will be used to represent a level of confidence in the value for each predictor and to reflect this confidence in the analysis using a weight. We also plan to compare external vendor naming conventions with new methods developed internally for CERT's malware catalogue, for the purpose of ranking vendors against expert analysis.

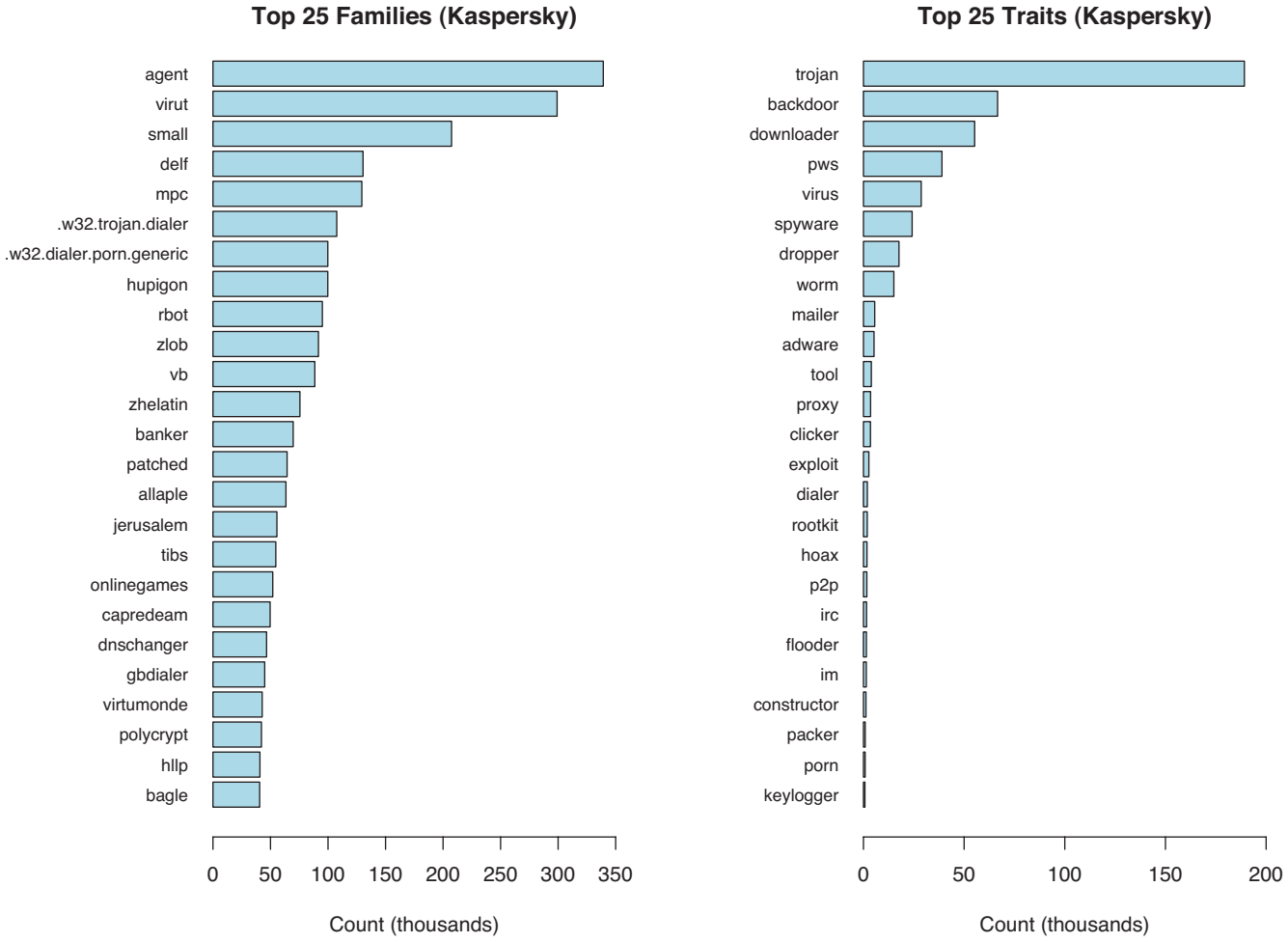


Figure 1: Breakdown of top 25 family names and traits catalogued for 5.9 million unique files recognized as malicious by the Kaspersky AV vendor. Family names are uniquely assigned; the top 25 names account for 40% of unique files recognized by Kaspersky. Traits are not exclusive; a file can be classified with any subset of names (e.g., "trojan.downloader.AZ"), or with none at all. In two cases, the classification system chose a family name based on traits ("w32.trojan.dialer" and "w32.dialer.porn.generic").

Vendor Agreement Using Average Modal Percentage (AMP) for Eight AV Vendors

AMP(Row,Col)	Avast	AVG	BitDefender	ClamAV	Fortinet	FProt	Kaspersky	McAfee	Sophos	Virusbuster
Avast	1.000	0.578	0.517	0.639	0.496	0.758	0.576	0.574	0.545	0.654
AVG	0.485	1.000	0.473	0.617	0.481	0.759	0.504	0.536	0.503	0.631
BitDefender	0.589	0.655	1.000	0.677	0.584	0.791	0.712	0.655	0.603	0.718
ClamAV	0.453	0.519	0.432	1.000	0.456	0.746	0.469	0.487	0.483	0.620
Fortinet	0.564	0.656	0.570	0.687	1.000	0.786	0.649	0.619	0.613	0.726
FProt	0.320	0.379	0.288	0.505	0.338	1.000	0.307	0.377	0.415	0.537
Kaspersky	0.617	0.687	0.678	0.677	0.611	0.788	1.000	0.668	0.633	0.722
McAfee	0.539	0.616	0.543	0.647	0.533	0.776	0.585	1.000	0.571	0.681
Sophos	0.559	0.624	0.556	0.678	0.560	0.788	0.610	0.636	1.000	0.726
Virusbuster	0.526	0.609	0.533	0.674	0.532	0.778	0.583	0.589	0.592	1.000

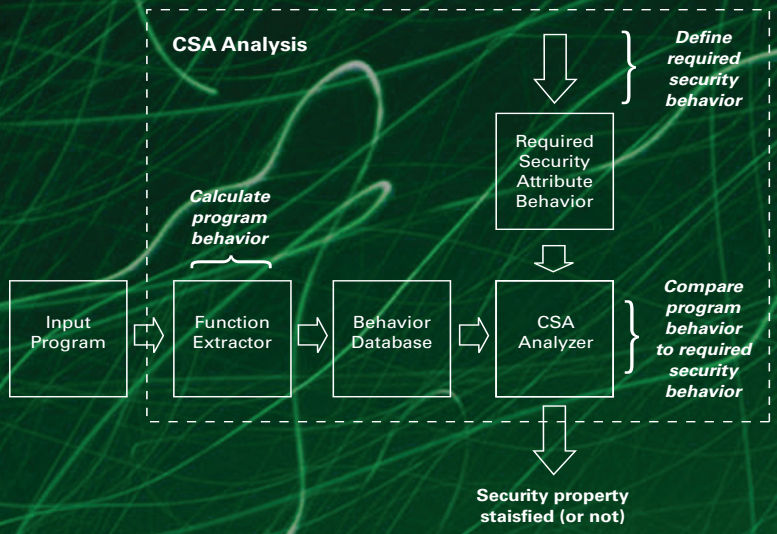
Table 1: AMP(A,B) calculated for eight AV vendors. The highest level of agreement appears between Kaspersky and BitDefender. Though FProt has high values per column, it is penalized per row, suggesting that FProt's naming scheme is generally coarser than its competitors.

References

[1] Stepan, A. "Defeating Polymorphism: Beyond Emulation." Microsoft Corporation white paper, 2005. http://downloads.microsoft.com

[2] Oberheide, J., Cooke, E., & Jahanian, F. "CloudAV: N-Version Antivirus in the Network Cloud." *Proceedings of the 17th USENIX Security Symposium,* 2008. http://www.eecs.umich.edu/fjgroup/pubs/cloudav-usenix08.pdf

Computational Security Attribute Analysis



Gwendolyn Walton

Luanne Burns

Computational Security Attribute Analysis

Problem Addressed

Security strategies must be sufficiently dynamic to keep pace with organizational and technical change. However, in the current state of practice, security properties of software systems are often assessed through labor-intensive human evaluation. The results can be of limited value in the dynamics of system operation, where threat environments and security attributes can change quickly. The Computational Security Attributes project takes a fundamentally different approach, focusing on the question "What can be computed with respect to security attributes?" to develop theory-based foundations for defining and computing attribute values with mathematical precision [1].

The ultimate goal of the project is to provide foundations to help transform security engineering into a theory-based computational discipline. Achieving this goal will require development of mathematical foundations and corresponding automation to permit both evaluation and improvement of security attributes of software during development and real-time evaluation of security performance during operation.

Research Approach

The problem of determining the security properties of programs comes down in large measure to the question of how they behave when invoked with stimuli intended to cause harmful outcomes. Thus, the first step in security analysis is to understand program behavior at a level of completeness and correctness that is often impractical with current technology. The emergence of function extraction (FX) technology, unavailable to previous researchers, provides the basis for this critical first step by computing the functional behavior of programs as a starting point for security analysis. The foundations of FX treat programs as rules for mathematical functions or relations that can be computed from program logic. These foundations can be generalized to accommodate what are often termed "non-functional" properties, in this case security properties, but which in reality exhibit functional characteristics amenable to computational approaches [2,3].

Automated evaluation of software security attributes consists of three major steps:

1. Specify security attributes in terms of required functional behavior for the operational environment of the software.
2. Apply FX technology to the software to compute a behavior database that specifies its as-built functional behavior.
3. Perform computational analysis to verify that the behavior is correct with respect to required security attribute behavior.

Figure 1 depicts the interaction of steps in this process.

The properties analyzed in the project include authentication, authorization, non-repudiation, confidentiality, privacy, and integrity.

Expected Benefits

There are several advantages to this approach:

- A rigorous method is used to specify security attributes in terms of the actual behavior of code during execution.
- The security properties of code can be checked through analysis of computed behavior.

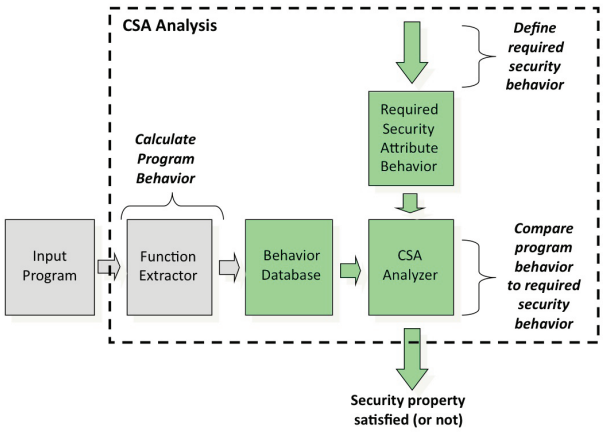


Figure 1: Automation Support for Evaluation of Software Security Attributes

- The specified security behaviors provide requirements for security architecture.
- Vulnerabilities can be better understood, making it easier to address evolution of code and its usage environment.
- The use of constraints provides a mechanism for explicitly defining all assumptions.

Computational security attribute technology can address specification of security attributes of software systems before they are built, specification and evaluation of security attributes of acquired software, verification of as-built security attributes of software, and real-time evaluation of security attributes during system operation.

2008 Accomplishments

The evolving FX system was employed to demonstrate detection of security attribute violations involving the presence of malware hidden in large bodies of software. Resulting behavior databases revealed both legitimate functionality and malicious intent that violated security attributes.

2009 Plans

Interested organizations are invited to sponsor development of engineering tools for computational evaluation of security attributes.

References

[1] Linger, R., Pleszkoch, M., Walton, G., & Hevner, A. *Flow-Service-Quality (FSQ) Engineering: Foundations for Network System Analysis and Development* (CMU/SEI-2002-TN-019). Software Engineering Institute, Carnegie Mellon University, 2002. http://www.sei.cmu.edu/publications/documents/02.reports/02tn019.html

[2] Walton, G., Longstaff, T., & Linger, R. *Technology Foundations for Computational Evaluation of Software Security Attributes* (CMU/SEI-2006-TR-021). Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu/publications/documents/06.reports/06tr021.html

[3] Walton, G., Longstaff, T., & Linger, R. "Computational Security Attributes." *Proceedings of Hawaii International Conference on System Sciences (HICSS-42)*. IEEE Computer Society Press, 2009.

Critical Infrastructure Cyber Risk Analysis

Bradford Wilke

Critical Infrastructure Cyber Risk Analysis

Problem Addressed

In many nations, the protection of critical infrastructures (CI) is an essential objective. These infrastructures are recognized as the engine by which a nation converts assets, whether raw materials, technologies, or ideas, into valuable commodities and services. When parts of the engine are threatened, whether banks and financial markets, manufacturing, information and communications technology, government, public health and healthcare, or energy, a nation feels real effects in terms of public safety, psychology, and economic impacts. In the U.S., the Executive branch of government has recognized critical infrastructure protection as a national imperative for more than 10 years [1,2].

Critical infrastructure protection (CIP) calls for "all-hazard" containment and risk management. In the digital age, this requirement includes the protection of information and communications technology (ICT, but also referred to as "cyber" technology) [3]. While ICTs are intrinsic to most political and societal functions, the emergence of cyber issues as a new element of infrastructure protection has made risk analysis more challenging. CIP risk analysis involves the computation of threats, vulnerabilities, assets, and consequences, but most risk practitioners' framing for the cyber element is at a lower level of understanding when compared to treatment of physical security elements.

Difficulties in articulating risk arise in at least three places:

1. generation of accurate, meaningful, cyber-focused risk scenarios and conditions
2. identification of cyber hazards in the same context as physical impacts and magnitudes of harm
3. promotion of cyber controls for CIP

For all three areas, the addition of the cyber element improves overall risk management but at the same time creates challenges for risk analysis. The cyber element (cyber security, cyber threats, cyber vulnerabilities, etc.) expands the risk environment, but it also makes risk analysis more challenging. For example, while physical threats (man-made acts and natural disasters) are easy to understand when examining potential consequences, cyber threats are often too complex for consequence analysis. Attacks on information systems are often not completed in one step, and the probability of success of cyber attacks is rarely known.

Another problem is that CI operators rarely know the total number of weaknesses and vulnerability in their IT and process control systems. Since CIP risk analysis depends on complete information, any inaccuracies in determining where business processes can fail or become exploitable when attacked create potential false negatives. This missing information translates into an incomplete picture of system risk and potentially wastes resources mitigating risks of lesser urgency or priority.

A third problem is that the presence of vulnerability often extends beyond IT and process control systems into the infrastructure of cyber security systems and physical security controls. CIP risk analysis is not currently structured to understand both business process vulnerability and the impact of security systems that become a weak point themselves. The resulting complication means that the most likely method of attack may be overlooked because security controls are expected to perform as designed.

If risk analysis were restricted to one cyber element, such as threat, there might be a clearer path to risk mitigation. But it would also mean that risk profiles would be incomplete and identify only simplistic, "low hanging fruit" solutions. Thus cyber treatment remains multi-faceted; it is an aspect of threat, vulnerability, asset definition, and even consequence, and it is both the actor and the means to create harm.

As with misunderstanding cyber context, the convergence of cyber and physical hazards in risk analysis of CI often gets confusing. When faced with cyber and physical hazards, risk scenarios often are constructed into too complex a story. For example, if the avenue of attack is both cyber and physical, a scenario can become far reaching and implausible. Allowing cyber and physical to become concurrent threats, vulnerabilities, and even assets is too complex for risk analysis. Physical threats to cyber systems can certainly cause cyber problems, but these must be separated from scenarios where cyber threats to cyber systems can cause physical problems. When physical and cyber risks are formulated in a circular manner, comprehension of the risk at hand is lost. Risk scenarios are a core element of risk analysis, and cyber and physical elements need to have clear and independent treatment.

There is one additional impediment to cyber risk analysis of CI from the field of information security itself. Performing information security is not the same as performing cyber security of critical infrastructure protection, but the two are often relegated as one discipline. The two fields are interconnected, but they require distinct considerations for risk analysis and very different levels of risk mitigation. For example, enterprise-level information security often benefits from community capabilities (such as research and vendor offering of vulnerability and threat information), while CI operations demand it. The most common problem this presents is that risk analysis considers information security controls and not other disciplines and practices associated with continuity, service reliability, and performance. Thus, cyber risk analysis of CI requires more than information security can provide alone, but the analysis does not consider this additional context.

Research Approach

CERT researchers have been very active within multiple levels of government and industry as these parties conduct risk analysis of CI. Our research approach has focused on management efforts to examine threats, vulnerabilities, countermeasures and protective programs, and consequences related to U.S. critical infrastructures. CERT research is engaged to understand specific strategic and operational requirements in order

to protect our productive infrastructure activities and functions from unacceptable loss and harm.

In the recent past, our research approach focused on traditional physical protections afforded sector-based functions (i.e., providing clean water, delivering electricity) and other productivities, which well served to prime the risk analysis process. Our evolution to incorporate cyber elements into CI risk analysis presents a unique opportunity to examine risks based on both the physical and logical domain spaces. Carefully crafted and applied, cyber dimensions of risk analysis present opportunities to address complex business challenges for CI, such as global supply chain management, software and systems assurance, security control selection and validation, and compliance justification.

CERT actively participates in nationally focused risk assessments of CI, considering threats from terrorist acts, cyber criminals, and insider threat actors. We have successfully included cyber security as an element of the risk assessment in contexts of asset description, threat actors (means and motives), vulnerability (opportunities), and negative outcomes. At the same time, we recognize that the formal adoption of cyber risk analysis is impeded by the lack of credible extensions to existing risk taxonomy. This typifies the problem where CI practitioners embrace physical elements in analysis over cyber elements. A taxonomy that converges cyber and physical elements would be more purposeful and provide a more robust risk analysis.

CERT works closely with U.S. government partners who serve as sector specific agency (SSA) leads for CI sectors, such as Information Technology and Energy. Through these partnerships, we meet with industry participants and consortia to expand our case study and evolve CI risk methodology.

We also recognize that to understand what changes we can make in risk analysis, we need an accurate picture of what is currently being done to approximate and calculate risk. In multi-sector CI risk assessments, CERT staff members have been able to capture invaluable traits and characteristics—such as the differing rates at which specific communities are able to grasp, inculcate, and formalize cyber risk information and use it to adjust protections for CI.

Benefits

The goal of CIP in the U.S. is to create a stabilizing effect for national security, public safety, economy, and psychology. National-level risks are managed to avoid catastrophic harm, distrust, and financial ruin. At the same time, the overwhelming majority of CI is not owned or operated by the government and requires a working partnership with industry. As simplistic as this concept sounds, risk analysis for CI must balance the need to manage shared risks against industry drivers such as profitability and stakeholder satisfactions.

The work of the CERT program is focused on striking a balance between the needs of CI owners and operators and the risk management goals and priorities of the U.S. government. We believe a common goal exists where the level of cyber security needed to mitigate shared risks to CI and still achieve specific business performances focuses appropriately on identifiable risk externalities. Because enterprises are often exposed to common risk factors, such as criminal activities and system and network vulnerabilities, the mitigation efforts (i.e., information sharing and analysis) that must happen across communities means the cost of countermeasures and implementations is somewhat shared and the benefit derived by all. Take for example the partnerships between industry and government to share timely threat and vulnerability information, analyze attacker trends and emerging behaviors, and enumerate CI dependency and interdependency. No one entity possesses both the full extent of the risk picture for CIP and the cyber security solutions. These solutions require thoughtful, earnest collaboration.

2008 Accomplishments

In 2008, CERT researchers began to examine a number of structured processes in-place to conduct, facilitate, and participate in a national-level CI risk assessment.

Sector-Oriented Accomplishments

At a policy level, in conjunction with the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) and other Sector Specific Agencies, CERT staff participated in and facilitated cyber vulnerability and consequence portions of a national risk assessment. CERT staff also participated as cyber risk analysts and SMEs across a number of CI sectors, including energy, transportation, chemical, emergency services, information technology, and public health and healthcare.

Also in 2008, CERT staff evaluated risk management strategies in the energy subsector related to operation of the Bulk Electricity System (or power grid). While formal risk assessment results are not widely available for a number of other subsectors, by examining the formula and treatment of cyber risk of one sector, expected results and the quality of such results to CIP can be accurately projected to others.

CI Technology-Oriented Accomplishments

At a lower level, CERT staff members have been instrumental in evaluating next-generation technologies planned to secure and operate CI and in reviewing R&D projects aimed at improving CI resilience. Exposure to such technological improvements has created an opportunity to catalog and preempt mistakes for cyber treatment within risk analysis of CI.

2009 Plans

In 2009, we plan to codify distinct cyber risk analysis components and improve capabilities for projecting threats, vulnerabilities, and consequences to CI (see Figure 1).

In addition, CERT plans to undertake specific research and development efforts to introduce a common risk management framework for CIP. With global supply chains and interconnected information and communications infrastructures, the degree to which cyber risks permeate the interdependency of CI must be studied.

Another clear area of work is to develop, pilot, and transition an internationally usable set of national cyber security readiness indicators and a self-assessment tool. This research would be done as an update to work based on previous attempts by the International Telecommunications Union (ITU-D) cyber security directorate to produce a nationally focused self-assessment tool against cyber security best practices.

In addition, through our partnership with DHS, we plan to mature an interagency relationship and harmonize certain physical and cyber security initiatives across government leadership in CIP. CERT staff members plan to actively facilitate cyber security risk assessments of CI facilities in the U.S. (such as chemical plant and electricity generation and delivery facilities). Each opportunity allows for expanded capture of requirements for industry-based information sharing and analysis activities.

Finally, in support of U.S. government goals to identify and protect infrastructures that are deemed most critical, CERT plans to support a number of government and industry initiatives targeted at identifying risks within CI and implementing protective measures. CERT plans to continue its participation and facilitation as cyber subject matter expert in the development and review of artifacts and results produced by national CI risk assessments.

References

[1] Presidential Decision Directive 63 (PDD-63), "Critical Infrastructure Protection." The White House, May 1998.

[2] Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection." The White House, December 2003.

[3] "The National Strategy to Secure Cyberspace." The White House, February 2003. http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

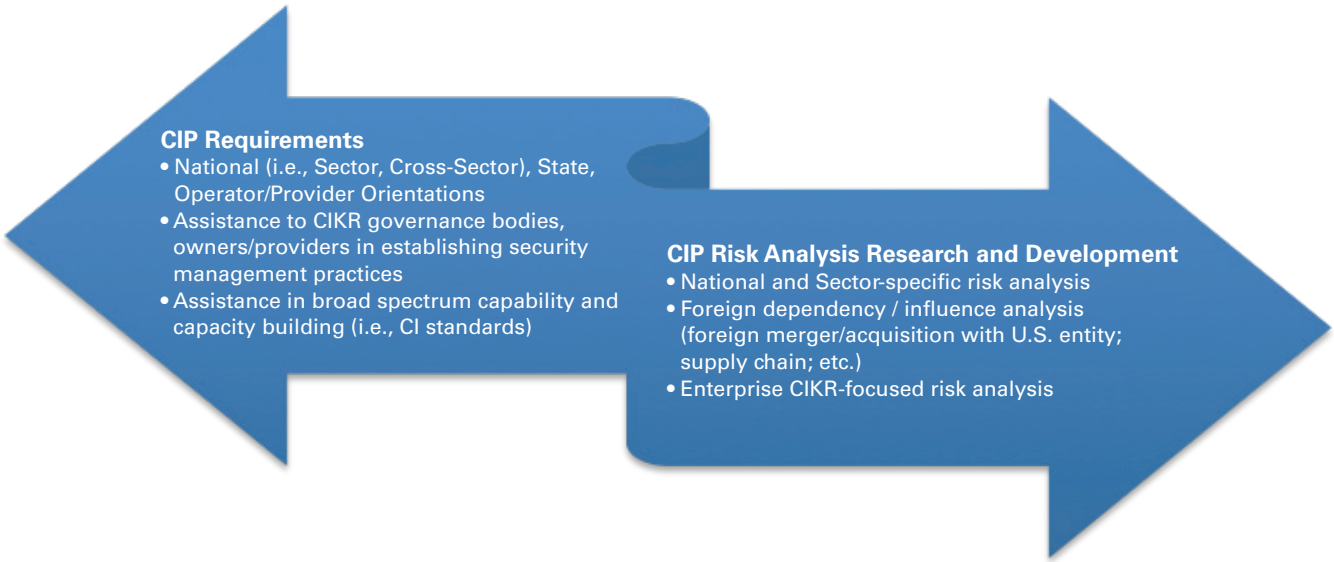
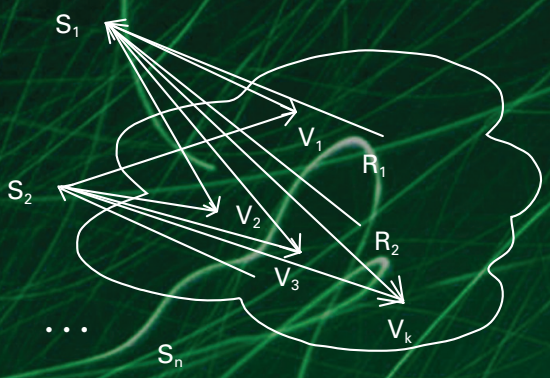


Figure 1: High-Level Considerations for CIP Risk Analysis Research and Development

Direct Response to Spam Email



Timothy Shimeall

Direct Response to Spam Email

Problem Addressed

Spam is a large and growing problem on the Internet. Traffic statistics vary in their estimates, but between 60% and 80% of the email on the Internet appears to be spam email. While many approaches have been identified for detection and reduction of spam, little work has been done on the operationally important issue of detecting individuals who respond to spam from within an organization. This report describes an initial approach to detection of spam responses, specifically emailed responses, with directions for further work.

Research Approach

This research is follow-on work based on the spam-detection research described in the *2007 CERT Research Annual Report* [1]. That effort was a flow-based model for discrimination between spam email and other email. The output of that effort was a list of IP addresses displaying spam-like email behavior during a specified time interval. This research used that list of IP addresses to first identify the hosts receiving spam and secondly identify where the receiving hosts sent non-automatic responses (indicated by time delay) back to the hosts displaying spam-like behavior.

The basic model of spam response is shown in Figure 1. Sources S_1 through S_n are sending spam to potential victims V_1 through V_k, indicated by the lighter arrows. For this model, the presumption is that these sources are able to receive replies. A small minority of the victims will reply via email back to the sources, indicated by the darker arrows. Some of the victims will reply from the initial destination address (V_3 in the diagram), others will reply via servers in their local area (R_1 and R_2 in the diagram).

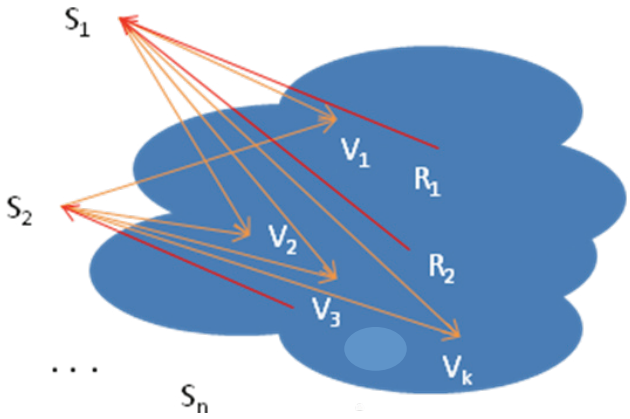


Figure 1: Spam Response Model

One obvious objection to this work is that most spam does not permit an emailed reply (since the return address is forged). However, there are several classes of spam email that desire and support emailed replies: advance-fee frauds, dating frauds, some identity theft schemes, and some online marketing methods. While not the majority of spam, the set is diverse enough to warrant an initial investigation. There have been spam-generating bots, identified on the Internet, that support email reply to compromised hosts.

Benefits

Acting on spam email has been associated with numerous forms of damage, including installation of malware, financial compromise, disclosure of proprietary information, and identity theft. By determining when individuals in the organization are responding to spam email, the exposure to these forms of damage can be assessed. Identification of the individuals involved enables managerial and technical remediation to these forms of damage and improvement to the individuals' behavior.

2008 Accomplishments

In FY2008, this research constructed the spam response detection model and implemented it as an operational tool (a group of scripts) that produces a file of flows that are identified as email responding to spam. This tool was applied to a particular organization, producing the chart shown in Figure 2. This chart shows a portion of the IP address space allocated to the organization, with IP address increasing on the vertical axis. The horizontal axis is hours. Points marked in black are hosts that received email traffic from sources exhibiting spam-like behavior. Points marked in red are hosts that responded to such email sent during or prior to the previous hour. For organizational privacy, the address range has been concealed.

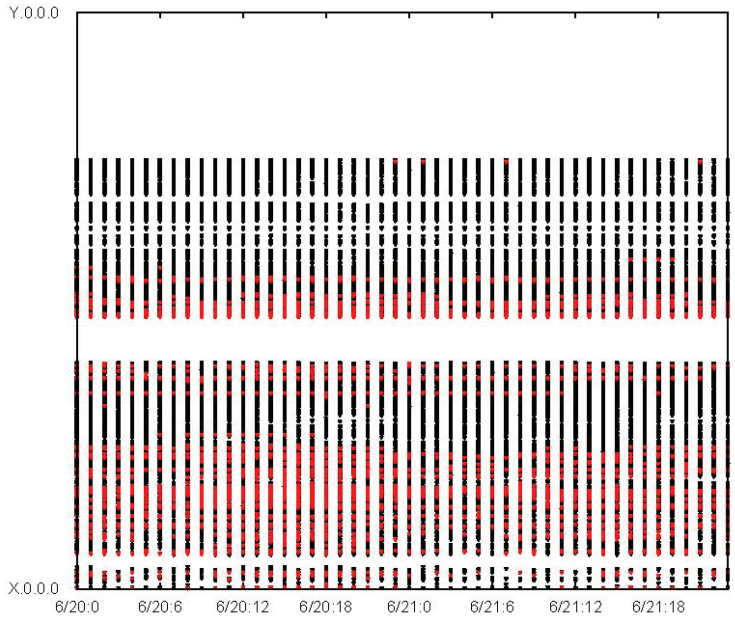


Figure 2: Detected Spam Responses

2009 Plans

During FY2009, the researchers hope to extend the spam response model to non-email responses (in particular, web-based responses or file-download responses). This would facilitate more complete understanding of the threat posed by response to spam email. The researchers also hope to apply the response model to other organizations to facilitate network situational awareness.

References

[1] Shimeall, T., Weaver, R., Janies, J., & Collins, M. "Spam Detection at the ISP Level," *2007 CERT Research Annual Report.*

Bradford Willke

Foreign Cyber Influence Analysis

Foreign Cyber Influence Analysis

Problem Addressed

Nations require an ability to determine the degree to which they depend on and are influenced by foreign partnerships, investments, and operations. Regardless of how much any nation stands in alliance with another, it has social, economic, and security obligations to its citizens to understand negative and inappropriate foreign influence.

One example of an intolerable foreign influence situation, in the United States, happened in 2006. At the center of the case was DP World, a government-owned company in the United Arab Emirates (UAE). The U.S. government (USG) eventually allowed the sale and operation of maritime management for six major U.S. seaports by DP World, but under political pressure DP World divested the port operations back to a U.S. entity, AIG [1].

The port case brought foreign influence and a need for influence analysis of matters of national security to the foreground of politics and national responsibilities. In the 21st century, many more daily but lesser known examples of foreign influence pass with little notice. This is especially true in the arena of cyber security.

Foreign influence in the digital age requires an examination of the information and communications technology produced, managed, operated, and supported by foreign investment and ownership (see Figure 1). As the United States has recently recognized, it also requires the analysis of a host of factors, including national security and cyber security issues, consumer and critical infrastructure (CI) implications, and domestic operations with foreign parent companies to niche and sole-source worldwide operations, such as with specific semiconductors or quality control facilities [2]. Even some of the global supply chain partners for information and communications technologies (ICT), if held to the same standards as the DP World case, would elicit as much of a concerned reaction and political outrage as physical security threats.

Research into foreign influence is not performed to create doomsday "security theater." Rather, its exploration into whether government and industry use appropriate risk management controls is intended to codify analysis requirements and processes and to understand the flux and drift of set points for risk tolerance and appetite. The core goal of such research is to understand foreign influence over technology that might create deliberate pitfalls for consumers, CI owners and operators, and industry.

In CERT research of critical infrastructure protection (CIP) and information assurance, two large areas of foreign influence analysis have emerged: the direct foreign ownership and operation of U.S. critical cyber infrastructure, and foreign ownership of a key ICT, where the latter is used to operate or manage essential functions of U.S. critical infrastructure or U.S. strategic capabilities (in the areas of national security, law enforcement, defense, etc.).

Figure 1: Risk Variables in Foreign Influence Analysis

A number of fundamental questions describe the breadth of research questions related to foreign influence. For example:

- Could product manipulations by foreign partners or owners of a U.S. company introduce deliberate product vulnerabilities or purposefully roll back essential capabilities and functions?
- Where technology comes in the form of service delivery or professional management services, could companies steer U.S. executives or managers to make poor strategic or operational decisions?
- Is the relationship of the parent foreign company to the nation it resides in important? Does the host nation itself matter in the analysis?
- Is the relationship of the foreign company to its own governmental departments important, such as to foreign defense departments and intelligence services?

A core challenge of foreign influence analysis is to filter out the benign and productive business-to-business relationships in a 21st century global economy from those that may harbor geopolitical motivations. At the heart of foreign influence analysis is a decision regarding the viability of the relationship based on actual or perceived risk. Thus, transactions (mergers, acquisitions, joint ventures, etc.) and partnerships should be weighed for acceptable risk. In determining acceptable risk, constraints may have to be considered on foreign influence and direct operations, including

- direct prevention of undue foreign influence
- allowance of the relationship only with enforcement of standards of practice and/or reporting
- allowance with active oversight and/or force divestments
- allowance with severe policy limitations and operating constraints (i.e., "firewall" policies)
- any combination of the above

The challenge of reviewing foreign influence is that each case presents both the complexity of a business transaction and a wide range of potential risk conditions that must be considered. Some situations might present a single dimension, such as issues of business intelligence collection of proprietary information, but many others raise concern over the number and type of sensitive industry and government contracts held in foreign control, especially where U.S. technology is transferred.

Research Approach

In the U.S., the there are a number of analysis techniques for foreign influence that touch on cyber risk. To date, they are disparate, government-led initiatives that cover only a small amount of the space of cyber risk to be managed. The U.S. government role is one of necessity not only in relation to CIP but because the nature of competitive U.S. industry creates the need for a third party to identify and arbitrate national risks.

The formal analysis of foreign company mergers, acquisitions, joint ventures, and direct investment with U.S. companies has been going on for decades. The Committee on Foreign Investment in the United States (CFIUS) was originally established by Executive Order 11858 in 1975 mainly to monitor and evaluate the impact of foreign investment in the United States. In 1988, President Reagan, pursuant to Executive Order 12661, delegated to CFIUS his responsibilities under Section 721. Specifically, E.O. 12661 designated CFIUS to receive notices of foreign acquisitions of U.S. companies, to determine whether a particular acquisition has national security implications sufficient to warrant an investigation, and to undertake an investigation, if necessary, under the Exon-Florio provision. This order also provides for CFIUS to submit a report and recommendation to the President at the conclusion of an investigation.

In February 2003, the Department of Homeland Security was added to CFIUS. This brought the membership of CFIUS to twelve under the chairmanship of the Secretary of the Treasury. The addition of DHS created a formal capability and an opportunity for the U.S. to examine cyber security matters as voluntary notices of foreign investment were reviewed by CFIUS.

CERT currently assists the National Cyber Security Division of DHS to provide input to CFIUS reviews of past and potential acquisitions involving ICT. Under a full spectrum of activities, DHS reviews new and non-notified transactions, drafts national security agreement when mitigations are required, performs compliance visits and monitoring, and reviews cyber incident notification and triage reports.

At present, CERT's involvement in foreign influence analysis and its research approach are evolving. A major objective of our long-term work in this area is to ensure that foreign influence analysis, wherever performed, uses a consistent, *risk-based* process with sufficient flexibility and scalability. At the same time, the decision as to whether analyzed foreign influence situations are risky needs to be connected to past events—linking one decision at one point in time to another. CERT research will concentrate on building a higher order process to ensure national risk tolerance can be calculated and used over time.

The current research approach is constrained to simple data gathering and analysis of foreign influence situations and factors. Initially, the results of analyses performed yielded a simplistic "yes" or "no" answer. However, CERT's research objective is to move this work to a risk-based process that considers a wide range of consequences and potential adverse influences. This portion of foreign influence research will focus on cataloging various implications of technology ownership by a foreign entity, including identifying risk factors for new customers and CI operations as well as potential issues with product integrity and life cycle management.

Reducing information gaps and identifying analysis points are also part of the research approach. Since each situation involves potentially complex estimates of risk, the supporting processes must be flexible and handle missing risk context and factors. Presently information gaps are relegated to being defined by the expert who reviews the circumstances of foreign influence. However, over time, CERT believes requirements will emerge as to which factors the USG and industry view as policy analysis imperatives. Thus, reviewers will have a foundational structure for case analysis when examining CI infrastructure operations versus broad ICT implications. A primary catalyst of analysis is the ease and quality of the public source information. More difficult is the ability to project national risk tolerance, where missing information can have ramifications, undermining the trust of influence analysis.

Finally, our research approach accounts for country-to-company relationships but needs to be extended. In the past, such as the DP World example, the degree of nation-state ownership has had a measurable effect on the degree of scrutiny given a foreign influence situation. Our approach examines the presence of political associations and country ties, which allows the research to account for recognizing the degree of transient risk and unacceptable ICT influences. One area to expand in the presence of nation-state affinity is the degree to which enforceable standards and compliance requirements translate to end-to-end risk mitigation.

Benefits

The benefits of research into foreign influence are self-evident but require complex analysis. In terms of what could be done under national CIP efforts, many foreign influence situations are only examined at the point of supply chain onset or new investment. Performing a one-time analysis ignores the fact that business and industry requirements for ICT and governments' policies towards foreign influence are ever changing. Performing ongoing analysis has the clear benefit of supporting longitudinal trend analysis and accounting for the ebbs and flows of risk sensitivity.

In terms of a benefit that foreign cyber influence analysis brings to global supply chains and multi-national company operations, it appears to confront the downside of a free market economy. For instance, when foreign influence is considered as a factor of product quality and diversity, the market drivers of availability and affordability can be offset by the awareness of national risks. In terms of a risk-and-reward calculation, the benefits are broad and distinct, whether societal, economic, or political.

Another benefit relates to how this analysis brings cyber security back to the forefront as a global concern. Cyber security of a nation's critical infrastructure is under microscopic focus, especially where geopolitical differences and ideologies exist. Outside of the U.S., a number of businesses in many countries have close ties to government. The chance, however small, that technology can be influenced in terms of quality, reliability, functionality, and performance is a significant matter for national security and cyber defense. Weak or untrustworthy technology presents opportunities for nations to infiltrate one another; product vulnerabilities deliberately introduced through foreign manufacturing create the potential for threats to lie dormant.

At present, the number of acquisitions of U.S. assets made by foreign entities is increasing. The clear benefit of CERT research is to bring appropriate, efficient, and judicious evaluation of foreign dependency and influence. We hope that our research incubates a number of other benefits, including the development of

- a streamlined process for foreign influence analysis
- country-to-company profiles for critical infrastructure operations
- sliding severity scales when addressing potential impacts of an acquisition
- proscriptive information gap identification and redress
- boilerplate language to address standards of due care and compliance requirements (when mitigating acceptable foreign relationships)
- formalized criteria to determine the nature and degree of risk to CI sectors, owners, and operators
- risk estimation guidance when decisions for foreign relations are under short suspense, particularly where there are highly complex issues, such as vast corporate structures that need to be examined

2008 Accomplishments

In 2008, CERT assisted the USG in reviewing a number of foreign influence transactions. Researchers reviewed a collection of situations involving dependency and influence, looking for CI sector equity, national and cyber security, and business and consumer implications.

We examined the potentially sensitive nature of the technology transferred. For example, where the foreign influence inferred a net change or transfer of information regarding knowledge of ICT in current CI operations or law enforcement capabilities, we examined the relationship for unacceptable consequences as well as possible mitigations.

In 2008, we paid very close attention to circumstances where a "bad actor" within a foreign operation could compromise a "purchased" ICT, such as software. For example, the insertion of deliberate malicious changes could ultimately inhibit or delay commercial operations, customer support, or even national cyber security operations and capabilities. In addition, if software or systems were modified in a manner that allowed personally identifiable or other sensitive operational security information to be leaked, it could inform unintended audiences as to capabilities of industry competitors, CI owners, and government operations.

Finally, where specific aspects of national security or defense were concerned, we examined properties such as sole-source product developments and service offerings for potential negative impacts.

2009 Plans

In 2009, CERT plans to continue its assistance to the USG in performing foreign influence analysis and by codifying repeatable methods for risk estimation and mitigation.

We fully expect the complexities of foreign cyber influence analysis to increase as the circumstances of CI dependency and influence become more commonly identified. We also realize that while on the surface proposed joint ventures by U.S. and foreign companies may be complex, the substance of ICT use and implications at the root of the transaction may create minimal changes in the national risk position. Thus, the process and research must be pragmatic in evaluating risk and determining impact evaluation criteria. For some, the foreign influence may be as benign as product or service rebranding, such as the case of IBM selling its ThinkPad™ line to Lenovo. If a venture is a fairly straightforward consolidation of the duplicative business lines and technologies of two companies, the market is exhibiting natural interests of consolidation and may not be a condition of unacceptable foreign influence.

Cyber risk analysis within foreign dependency and influence situations is a careful balancing act. Flexibility and extensibility of such risk evaluations is paramount.

References

[1] Associated Press. "DP World Plan to Sell All U.S. Ports Satisfies Lawmakers." *USA Today,* March 2006. http://www.usatoday.com/news/washington/2006-03-15-gop-ports_x.htm

[2] Wyatt, K. "Details Emerge About President's Cyber Plan." *Government Computing News,* Nov. 2008. http://www.gcn.com/online/vol1_no1/47639-1.html

Function Extraction Technology for Software Assurance

Stacy Prowell

Mark Pleszkoch

Luanne Burns

Tim Daly

Richard Linger

Kirk Sayre

AF	auxiliary_carry_flag_add((2*d *EDX*),*EDX*)
CF	(**4294967296** <=((2*d *EDX* +*EDX*))
EAX	(2*d *EDX*)
M	*M*
OF	overflow_flag_add_32((2*d *EDX*),*EDX*)
PF	is_even_parity_lowbyte((3*d *EDX*))
SF	is_neg_signed_32((3*d *EDX*))
ZF	(**0**==(3*d *EDX*))

Function Extraction Technology for Software Assurance

Problem Addressed

CERT recognizes both the importance of software assurance to national defense and economic activity and the difficulty of achieving it. Software assurance depends on knowing and verifying the complete behavior of software. Unfortunately nothing less will do, because behavior that is not known can contain errors, vulnerabilities, and malicious content. Current software engineering lacks practical means for developers to determine the full behavior of software, and no testing effort, no matter how elaborate, can exercise more than a small fraction of possible behavior. Complex software systems are difficult to understand because of their immense numbers of execution paths, any of which can contain errors and security exposures. Faced with innumerable execution possibilities, developers and analysts often achieve no more than a general understanding of system behavior. This technology gap is at the heart of many issues in software and security engineering.

Research Approach

Function-theoretic foundations of software illuminate a challenging but feasible strategy for developing automated tools to calculate the behavior of software with mathematical precision and present it to users in understandable form. CERT is conducting research and development in the emerging technology of function extraction (FX). The objective of FX is to move from an uncertain understanding of program behavior derived in a human time scale of days to a precise understanding automatically computed in a machine time scale of seconds. This technology applies mathematical foundations to automate calculation of the functional behavior of software to the maximum extent possible. These foundations define the transformation of code structures into procedure-free functional form and are the basis for the function extraction process [1,2,3]. While theoretical results impose some constraints on behavior calculation (for example, for certain forms of loops), development of engineering solutions suggests that nearly all software behavior will be amenable to calculation. And any level of behavior calculation can help improve human capabilities for understanding and analysis. Function extraction technology can be applied to any programming language and has potential to impact many aspects of the software engineering life cycle [4].

Expected Benefits

The function extraction system currently under development targets programs written in or compiled into Intel assembly language. The system is expected to help security analysts to determine intruder strategies by providing precise information on the structure and function of malicious code [5]. In terms of broader application, opportunities exist to make progress on the problems of malicious code detection, computational security analysis, correctness verification, legacy system understanding, creation of assured software repositories, anti-tamper and foreign-content analysis, and component composition. Human fallibility may still exist in interpreting the analytical results, but routine availability of calculated behavior can be expected to help reduce errors, vulnerabilities, and malicious code in software and help make software development more manageable and predictable.

2008 Accomplishments

In its current state of development, the FX system demonstrates transformation of spaghetti-logic assembly language programs into understandable structured form, and automated computation of behavior for sequence, branching, and looping structures.

In 2008, development was initiated on a specialized system, FX/IDA, to provide behavior computation capabilities in the IDA Pro disassembler environment often employed by malware analysts. This system is continuing to evolve in response to analyst requirements. FX/IDA is available for use in CERT and can be provided to other organizations engaged in malware analysis. A key feature of the system is use of computed behavior to eliminate no-op code inserted in malware by intruders to confuse analysis and increase demands on scarce human resources. In illustration, Figure 1 shows output from FX/IDA. The window on the left depicts input malware code under analysis. The window in the middle shows only those instructions from the original code that have functional effect, with all no-op code eliminated. Such reductions in the volume of code to be analyzed can help analysts to be more productive. Finally, the window on the lower right defines the computed behavior of the reduced sequence of instructions.

2009 Plans

FX/IDA capabilities will continue to evolve in 2009, with a major focus on transition to malware analysts. Sponsors are welcome to participate in the technology development and transition. CERT is also ready to apply FX to additional languages and phases of the software engineering life cycle.

References

[1] Prowell, S., Trammell, C., Linger, R., & Poore, J. *Cleanroom Software Engineering: Technology and Practice.* Addison Wesley, 1999.

[2] Mills, H. & Linger, R. "Cleanroom Software Engineering." *Encyclopedia of Software Engineering, 2nd ed.* (J. Marciniak, ed.). John Wiley & Sons, 2002.

[3] Collins, R., Walton, G., Hevner, A., & Linger, R. *The CERT Function Extraction Experiment: Quantifying FX Impact on Software Comprehension and Verification* (CMU/SEI-2005-TN-047). Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05tn047.html

[4] Hevner, A., Linger, R., Collins, R., Pleszkoch, M., Prowell, S., & Walton, G. *The Impact of Function Extraction Technology on Next-Generation Software Engineering* (CMU/SEI-2005-TR-015). Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05tr015.html

[5] Pleszkoch, M. & Linger, R. "Improving Network System Security with Function Extraction Technology for Automated Calculation of Program Behavior." *Proceedings of the 37th Hawaii International Conference on System Sciences* (HICSS-37). Waikoloa, HI, Jan. 5–8, 2004. IEEE Computer Society Press, 2004.

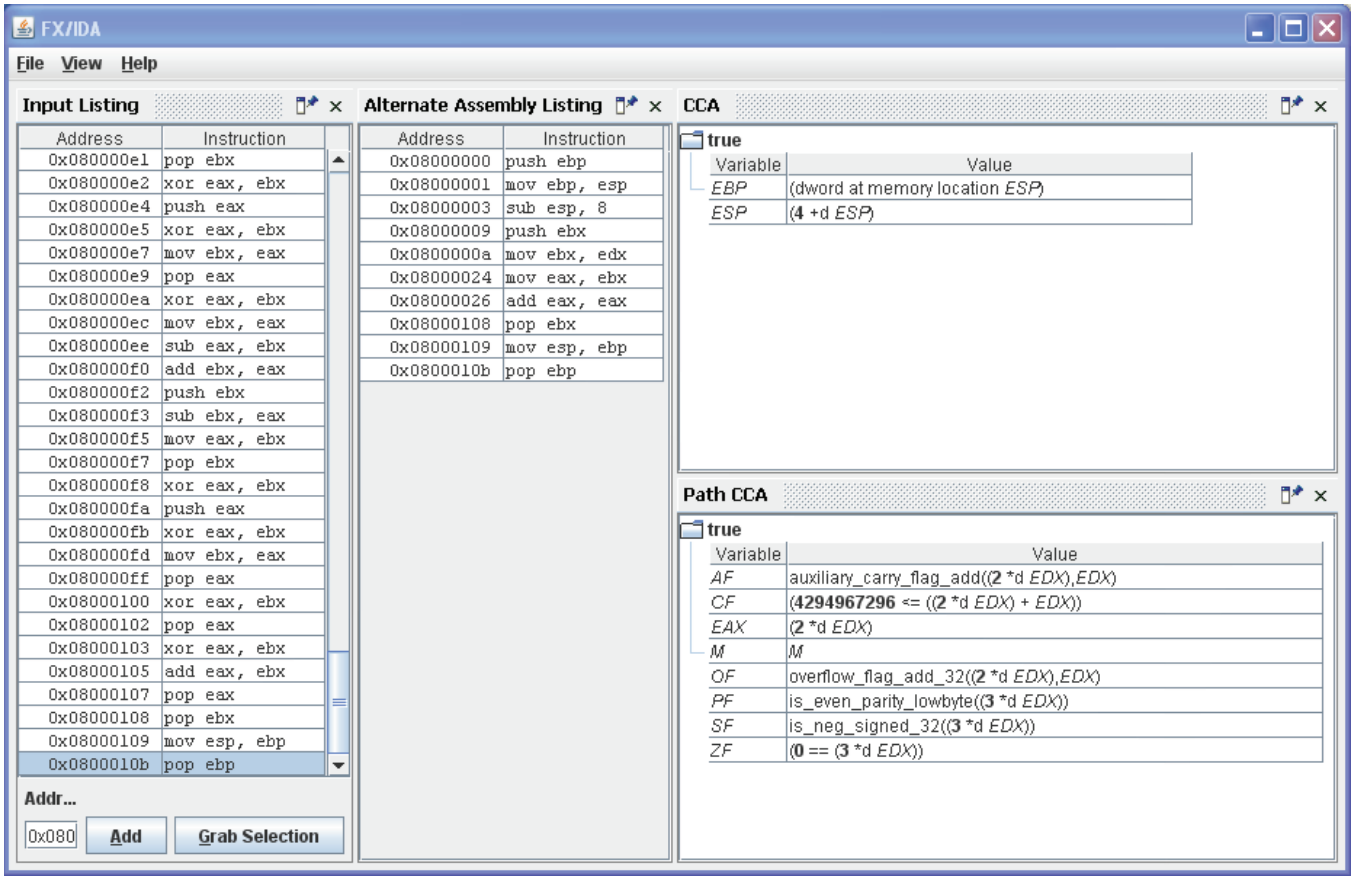
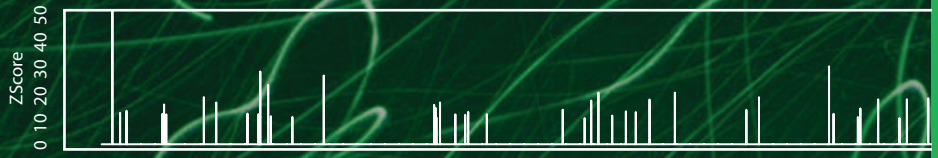


Figure 1: FX/IDA Output Illustrating No-Op Code Elimination

Identifying Port-Specific Network Behavior

Rhiannon Weaver



Identifying Port-Specific Network Behavior

Problem Addressed

A port is an integer value between 0 and 65535 that represents a logical connection place for TCP and UDP communications. Sudden jumps in incoming traffic volume to a single port or slowly increasing trends over time can indicate new or renewed interest in a vulnerability associated with that port [1]. Internet-wide outbreaks of malicious activity associated with newly released exploits can be preceded by port-specific scanning from multiple hosts. Detection of this activity may help forewarn network defenders of an impending attack.

Port-specific network behavior also arises from user activity, such as messaging clients or peer to peer applications, that occurs infrequently or that migrates among unreserved ports (ports that range from 1025 to 65535) in order to evade firewall rules. This activity may represent only a small change in volume relative to daily or weekly trends, but if isolated it can pinpoint internal clients that are bypassing established security policies.

Research Approach

Each port in an active network can be characterized by a discrete sequence of measurements over time, called a time series. To identify port-specific behavior, we apply statistical trending and outlier detection to these time series. This method requires eliminating general volume trends and multi-port activity from each series and standardizing the residual activity to reflect its degree of departure from the expected trend. We use correlation-based clustering techniques to eliminate trends due to vertical scans or to gateway server activity that cycles through source ports. We standardize the residual port activity by transforming measurements to a universal scale called a Z-score. The Z-score represents the "oddity" of the port activity as the number of standard deviations an observed value lies away from its expected value. We organize reports based on clusters of ports with similar behavior. We can compare Z-scores across ports based on a common threshold and use statistical diagnostics to check the validity of the results.

An example visualization of three days of activity for a cluster of 70 ports is shown in Figure 1. The Z-scores (top) are calculated based on the number of flow records observed per hour for each port, where a flow record approximates a TCP session or connection request. The 10-hour surge on April 16th corresponds to a scan of port 5110 over several class B networks by multiple external hosts. Although activity post-scan increased on the morning of the 17th, in this instance there was no Internet-wide outbreak. Port 5110 is associated with an older Turkish exploit known as ProRat.[1]

In addition to calculation of Z-scores, we also display diagnostic measures. A histogram and qq-plot of Z-scores (bottom) are used to confirm that healthy Z-scores follow a bell-shaped, Gaussian distribution, with outliers appearing due to surges. We also display a measure of cluster health (middle plot) at any point in time, on a scale from 0 (unhealthy) to 1 (healthy), with a threshold of 0.05 to indicate severe problems.

Cluster health represents the overall odd behavior of all ports in the cluster. A measure called "1-outlier adjusted" cluster health is used to determine the health of all remaining ports in a cluster when the most outlying port is removed. A port-specific surge, such as the one on April 16th, is characterized by low overall cluster health and comparatively high outlier adjusted health. On the other hand, an outbreak of high Z-scores for many ports appears on April 18th at 5 a.m. Any alerts for port-specific activity are suspect, however, due to low cluster health and low outlier-adjusted health at that hour.

Upon further inspection, this outbreak corresponded to a scan of multiple ports. Figure 2 shows a view of activity across all ports from that hour using a "comb plot." This plot selects a threshold value (Z-score > 10 in the example) and creates a bar plot of scores greater than the threshold for all ports in one hour. The unusual activity at 4 a.m. and 5 a.m. appears across a large subset of ports. This unusual activity corresponds to a two-stage scan of many ports across the network.

Benefits

Port clustering provides a way of grouping related ports, displaying information, and classifying events on a cluster-by-cluster basis. This gives analysts a higher level view of the space of 65536 series of individual activity and helps distinguish surges from the normal ebb and flow of network activity. The method of statistical outlier detection produces lower false positive rates than simple thresholding techniques based on heuristics and allows for diagnostics that guide confidence in conclusions.

2008 Accomplishments

In 2008, clustering and standardization were applied to a test set of three weeks of hourly data, using the number of incoming records per hour as the measured value for each time series. Correlation-based clustering was implemented using C libraries. Standardization and event reporting were implemented as a proof of concept using the R statistical programming language. Models were fit using one week of data and tested using the remaining two weeks.

An evaluation was carried out based on expert classification of a sample of 440 events generated by ranking Z-scores with values above 5.0. False positive rates were under 5% in the evaluation. Over 50% of events were traced back to "phantom" peer-to-peer activity, in which an idle internal IP address suddenly starts receiving SYN packets from a number of external addresses known to also be communicating on standard peer-to-peer ports. We suspect this arises from users going offline, while their recently advertised IP addresses persist in external trackers.

1 http://isc.sans.org/port.html?port=5110

2009 Plans

In the coming year, we plan to implement an automatic method for calculating and archiving Z-scores based on two inputs: a preprocessing script that describes how to summarize raw data for input to the algorithm and a model summary file that describes port cluster assignments and modeling parameters. This archive will allow for rapid application of the clustering technique in many different settings. We plan to use this tool to facilitate trending Z-score surges with time and associating features of the scores with events of interest. This application will also aid in choosing useful summarizations to use as inputs for the algorithm—a process in statistical modeling that is called feature selection.

References

[1] McNutt, J. & DeShon, M. "Correlations Between Quiescent Ports in Network Flows." Presented at FloCon 2005, Pittsburgh, Pa. http://www.cert.org/flocon/2005/presentations/McNutt-Correlation-FloCon 2005.pdf

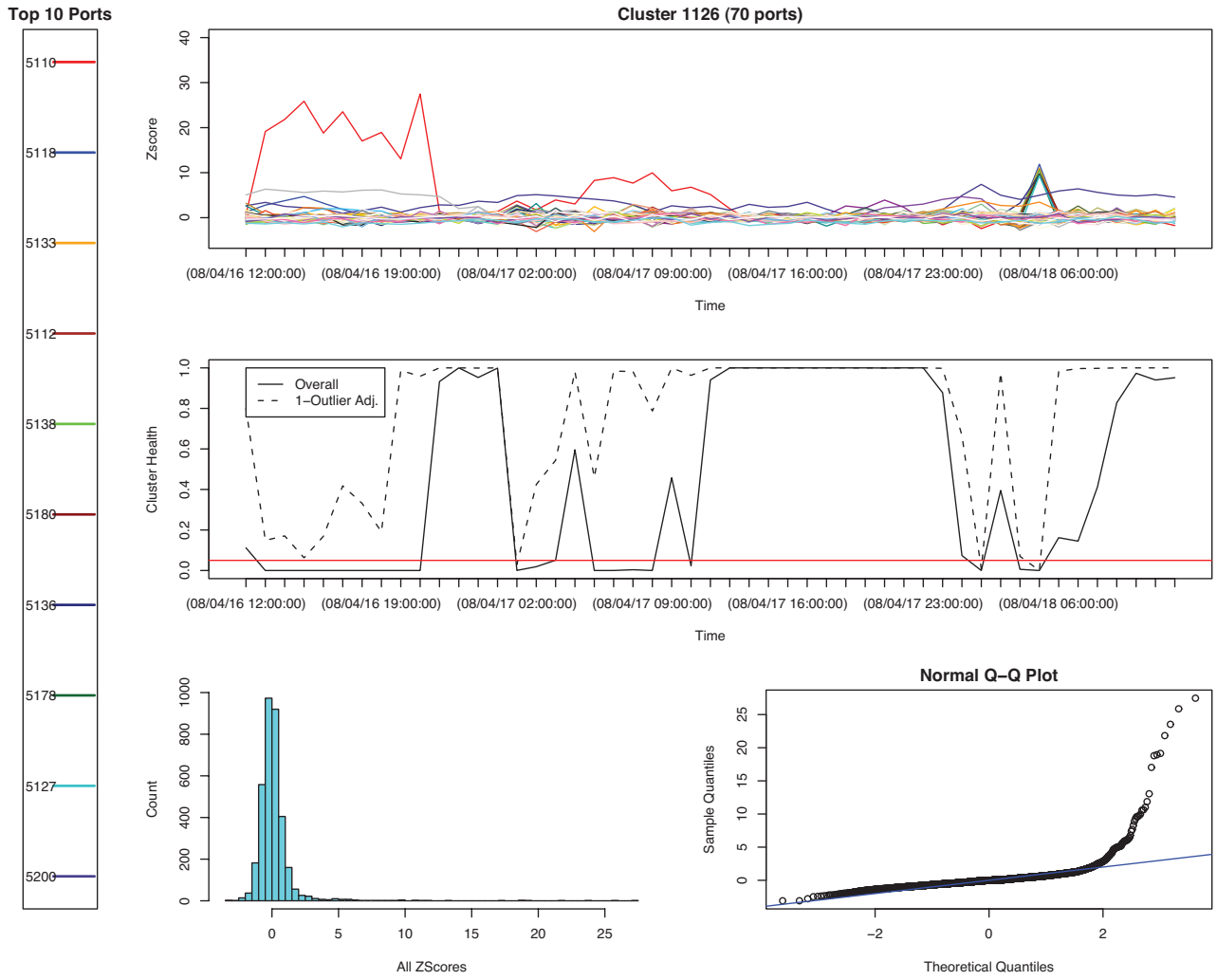


Figure 1: A three-day summary of activity for a port cluster, including time series plots of Z-scores (top) and cluster health (middle), as well as some Z-score diagnostic plots (bottom). The left-hand side lists the top 10 ports with the highest Z-scores in the plotted window. The figure shows a 10-hour surge in port 5110 starting at 12 p.m. on April 16th, corresponding to a port-specific scan by multiple external IP addresses. A spike in several ports appears at 5 a.m. on the 18th. The low cluster health for that hour indicates multi-port activity.

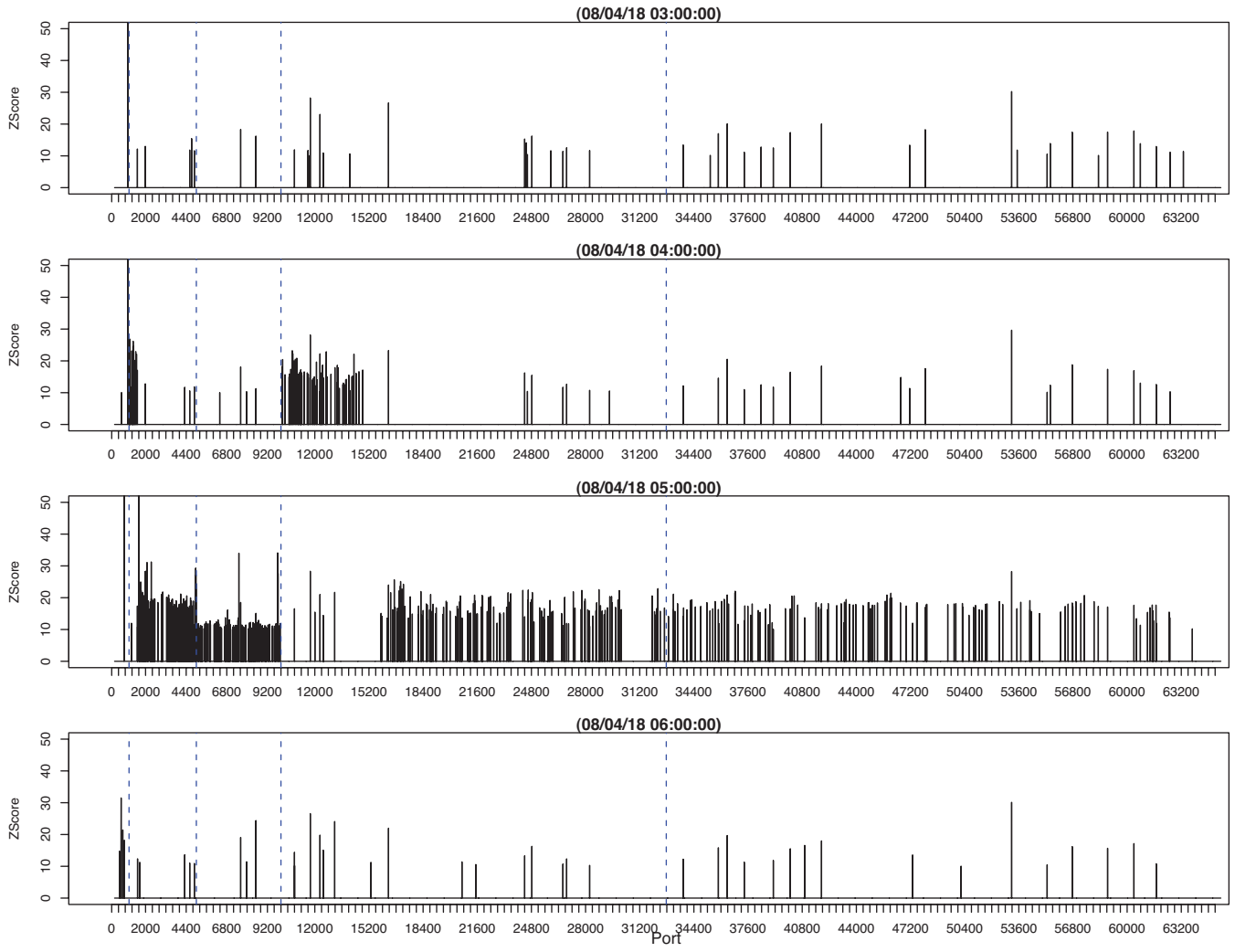


Figure 2: Sequential "comb plots" show the result of a two-stage multi-port scan. For visual reference, blue dashed lines correspond to ports: 1024, 5000, 10000, and 32768. Activity first occurs at 4 a.m. on low-valued Windows server ports (1024 to approx. 1500) and low-valued UNIX ephemeral ports (10000 to approx. 15500). By 5 a.m., the activity migrates across Windows server ports, ephemeral unassigned ports (5000-10000), and a cross-section of the remaining UNIX ephemeral ports. There are indications of reserved port activity (0-1024) for the 6 a.m. hour that may also be associated with the scan.

Making Business-Based Security Investment Decisions – A Dashboard Approach

Julia Allen

Making Business-Based Security Investment Decisions – A Dashboard Approach

Problem Addressed

In today's business climate, we are constantly dealing with the demand to do more with less. The resources required to run the business, let alone to invest in new initiatives, are always at a premium—time, money, staff expertise, information, and facilities, not to mention energy and attention span. All investment decisions are about doing what is best for the organization (and its stakeholders). However, what is best is sometimes hard to define, hard to quantify, and even harder to defend when the demand for investment dollars exceeds the supply.

Business leaders are becoming more aware of the need to invest in information and software assurance—to meet compliance requirements and optimize their total cost of ownership for software-intensive applications and systems. So how do we ensure that security investments are subject to the same decision criteria as other business investments? And by so doing, how are we able to justify investments that increase our confidence in our ability to protect digital information using software that is more able to resist, tolerate, and recover from attack?

One approach may begin to shed some light on this topic. It is based on recent CERT research on how to make well-informed security investment decisions using business-based criteria. Over the past four years, CERT has developed a body of knowledge in enterprise and information security governance, including a detailed framework and implementation guide that describe a robust security governance program.[1] When faced with this framework of tasks, actions, roles and responsibilities, and outcomes, senior leaders say "This is all well and good, but I have many more pressing issues to deal with than security governance. Can you provide me with an aid to select and prioritize these and other security-related actions that I can use as an input to normal planning and capital investment processes?" CERT has responded to this need with the Security Investment Decision Dashboard (SIDD).

Research Approach

SIDD describes seven decision criteria *categories*, each supported by three or more decision *indicators*, totaling 33 in all. A CERT security governance report [1] served as the starting point for selecting business-based criteria that could be used to evaluate candidate investments. In addition, a number of relevant business and security sources [2]-[5] were analyzed for business-based questions and factors that could help inform security investment decisions. The collected set of questions and factors are reflected in the current set of 33 indicators. The seven categories were derived through affinity grouping of the 33 indicators.

Each category is defined in the form of one or two questions to ask. Categories are presented in shaded text in Table 1 and include Cost, Criticality & Risk, Feasibility, Positive Interdependencies, Involvement, Measurability, and Time & Effort Required. The importance of each category is determined by considering the question "What should *any* candidate investment do for the organization and its stakeholders?" or alternatively, "What is the basis or criteria for selecting *any* candidate investment?"

For example, is it most important that an investment (1) be low cost, (2) be critical to meet business objectives or mitigate a high degree of risk, or (3) be feasible in terms of likelihood of success? Priorities or rankings are then assigned to the category based on the importance of the category to the organization's investment selection process. Each category is further elaborated by three or more indicators that are listed following each category in Table 1. This is a "starter set" that can be tailored to reflect a specific organization's decision factors.

A business leader may determine that there are other factors or different factors that they use in their investment decision making processes. The SIDD is designed so that categories and indicators can be changed, added, and deleted, and the dashboard will continue to present meaningful comparisons.

Dashboard results are presented in a comparative bar graph form. Score totals are presented for the 7 categories and the 33 indicators for each investment. An additional result is calculated based on the scores for the 6 indicators ranked highest (1-6). This result has been included to accommodate the situation where a subset of indicators is important for investment selection as a companion to the total scores for all categories and for all indicators.

A more detailed description of SIDD, including sample output, is available on the U.S. Department of Homeland Security Build Security In website.[2]

Expected Benefits

SIDD provides a means for evaluating and comparing several candidate security investments. A foundational principle of the dashboard is that the priorities for candidate investments are driven by the organization's *desired outcome for any given investment*, not just security investments. This ensures that security investments are subject to the same decision criteria as other business investments. They can then be presented, reviewed, analyzed, debated, and compared using the same scales, factors, and investment-selection criteria and processes.

1 http://www.cert.org/governance

2 https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management/985-BSI.html

Dashboard outcomes identify the highest priority (highest scoring) investments based on the category rank, the indicator rank, and the answers to the questions for each investment. Given that the category and indicator ranks are fixed and weighted to normalize the scores, the dashboard results can be meaningfully compared and used to help select which investments to fund, as well as providing a defensible rationale for those that were not selected.

If, based on other factors, these highest scoring investment choices are not justified, this is a valuable opportunity to re-examine the category and indicators rankings and answers to determine if they do indeed reflect how the organization makes investment decisions.

This tool is not intended as a substitute for human judgment. It can be used to make judgments more explicit, to apply a consistent set of decision criteria to all investments which can then be communicated, and to capture trends over time.

2008 Accomplishments

A review process of SIDD was conducted at Carnegie Mellon University and the Software Engineering Institute throughout FY2008. Comments have also been received from ten organizations representing the large commercial, large defense contracting, not-for-profit, U.S. federal government agency, IT consortium, and security consulting/products and services sectors. The current version of the tool executes as a series of Excel spreadsheets.

2009 Plans

Review and improvement of the current version is ongoing. Based on review and pilot feedback, the spreadsheet version of the tool needs to be converted to a standalone and/or web application for ease of introduction, presentation, and use. A number of organizations have expressed interest in conducting in-depth pilot projects using this approach should such a tool be made available. Further development of this application is pending FY2009-FY2010 funding approval.

References

[1] Westby, J. R. & Allen, J. H. *Governing for Enterprise Security (GES) Implementation Guide* (CMU/SEI-2007-TN-020). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 2007. http://www.sei.cmu.edu/publications/documents/07.reports/07tn020.html

[2] Campbell, G. K. "Measures and Metrics in Corporate Security: Communicating Business Value." CSO Executive Council, 2006. https://www.csoexecutivecouncil.com/content/Metrics_Mini_Update_060706.pdf

[3] Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. "Report of the Best Practices and Metrics Teams." Nov. 17, 2004; updated Jan. 10, 2005. http://www.educause.edu/ir/library/pdf/CSD3661.pdf

[4] Drugescu, C. "Maximizing the Return on Investment of Information Security Programs: Program Governance and Metrics." *Information Systems Security Journal,* Taylor & Francis, Dec. 2006.

[5] Kleinfeld, A. "Measuring Security." *Information Systems Security Journal,* Taylor & Francis, Nov. 2006.

Table 1: SIDD Categories and Indicators

Category	Description
Cost	What is the estimated total cost to accomplish this investment, taking into account the potential cost savings and/or risk reduction to the organization?
	Overt cost in dollars at outset to accomplish this investment?
	Estimated life cycle cost in dollars over time to sustain this investment?
	Cost of NOT doing this investment, in terms of potential exposure and residual risk (high = investment is more necessary)?
	Potential cost savings to organization beyond breakeven point, if quantifiable (ROI), over time (high = better)?
Criticality & Risk	What is the degree to which this investment contributes to meeting the organization's business objectives and risk management goals?
	Degree to which this investment is key or mainstream in helping the organization meet its primary objectives and critical success factors?
	Degree of risk (as assessed in terms of likelihood and potential impact—high/medium/low priority) mitigated by this investment?
	Degree to which this investment helps the organization protect stakeholders' (shareholders') interests?
Feasibility	How likely is this investment to succeed?
	Likelihood of success on first try?
	Likelihood of success on subsequent tries (if first try fails)?
	Likelihood that turnover among management and/or board of directors will negate work expended on this investment (low likelihood = better)?
	Likelihood that this investment will need to be rolled back (low = better)?
Positive Interdependencies	(1) To what degree does this investment integrate with or represent reasonable changes to existing organizational processes and practices, rather than requiring new ones? (2) To what degree does this investment pave the way for future investments (compliance, policy, risk management, etc.)?
	Degree to which other investments/tasks are dependent on this one (i.e., degree to which this investment makes it easier to accomplish additional tasks)?
	Degree to which the accomplishment of this investment makes it easier to comply with current laws and regulations?
	Degree to which the accomplishment of this investment makes it easier to comply with potential new laws and regulations in the future?
	Degree to which existing knowledge and/or skills can be used to accomplish this investment, rather than requiring new skills/knowledge?
	Degree to which this investment produces positive side effects (e.g., enhancing brand/reputation, building customer trust, benefiting supply chain partners)?
Involvement	What level of involvement and buy-in are required from various parties for investment success—both within and outside of the organization?
	Level of buy-in required throughout the organization? (Must all employees be on board 100% for this to work? Or only a subset, such as management and certain key employees?)
	To what extent does this investment require the active involvement of many departments across the organization?
	Number of people who need to be actively involved?
	Level of involvement by third parties required (partners, consultants, vendors, etc.)?
	Degree of external, independent assessment/auditing (vs. in-house assessment/auditing) required?
Measurability	How measurable is the outcome of this investment?
	Degree to which this investment can be evaluated using existing approaches and reporting mechanisms?
	What is the measurability of the outcome? Can it be quantified in tangible terms (revenue, market share, stock price, etc.)?
	If the outcome is intangible (e.g., goodwill, increased customer trust, enhanced brand), can the benefits be demonstrated against meaningful business success factors?
Time & Effort Required	(1) What level of staff-hours will be required to accomplish this investment? (2) How long will it take to reach break-even cost for this investment?
	Board of directors time required?
	Senior management time required?
	Cross-organizational team/steering committee time required?
	Middle and lower management time required?
	Other key staff time required?
	Time likely needed to achieve the required level of buy-in?
	Time required to achieve first demonstrated results?
	Time required to achieve full adoption and use of the investment results across all affected business units?
	Time to achieve breakeven, if quantifiable?

Process Improvement in Managing Operational Resiliency Using the CERT Resiliency Engineering Framework


Rich Caralli


David White


Lisa Young

Process Improvement in Managing Operational Resiliency Using the CERT Resiliency Engineering Framework

Problem Addressed

Organizations in every sector—industry, government, and academia—are facing increasingly complex business and operational environments. Technology advances are helping organizations to automate business processes and make them more effective at achieving their mission. But the cost to organizations is that the technology is often more complex, takes specialized support and resources, and creates a rich environment for breeding vulnerabilities and risks. In addition to technology, organizations are also realizing that mission success relies on partnerships—engaging external partners to provide essential skills and functions, with the aim to increase productivity and reduce costs. As a result, the organization must expose itself to new risk environments, often in geographical regions of the world where emerging risks are not readily known. By employing a chain of partners to execute a business process, the organization concedes control and potential reliability of mission assurance in exchange for cost savings. This poses a problem for management in that governance and oversight must cross organizational and geographical lines like never before. And, it must be acknowledged that the emerging worldwide sociopolitical environment is forcing organizations to consider threats and risks that have previously not been on their radar screens. Recent, well-publicized events have changed the view of what is feasible and expanded the range of outcomes that an organization must attempt to prevent and from which they must be prepared to recover. All of these new demands conspire to force organizations to rethink how they perform operational risk management and how they address the resiliency of critical business processes.

Traditional disciplines like security and business continuity must be expanded to provide protection and continuity strategies for critical assets that are commensurate with these new operating complexities. Unfortunately, current business and organizational approaches have not matured sufficiently to position organizations to effectively meet these challenges. For example, funding and staffing models tend to favor separation of security and business continuity activities into organizationally manageable silos, rather than to view security and business continuity as activities that share responsibilities for holistic and convergent management of the entire risk equation—condition + consequence—with shared organizational goals. This path of least resistance often impairs the organization in the long run in making measurable and sustainable improvements in operational resiliency. This also reinforces the perception of senior management that security and business continuity are necessary evils that are funded because of uncertainty and fear or out of a need to comply rather than because they enable the organization to meet strategic objectives.

In addition, organizations lack a reliable means to assess their competency for managing operational resiliency. Typically, competency is measured by the way that an organization has performed during an event, or is described in vague, immeasurable terms. For example, when organizations are asked to describe how well they are managing resiliency they typically revert to characterizing success in terms of events and consequences that they haven't been affected by. In other words, unless they are experiencing tangible pain, they conclude that their strategy must be working.

When organizations attempt to measure their capability for managing operational resiliency, they are prone to using tools and methods that are not purposeful for addressing competency and process maturity. Point-in-time reviews using codes of practice as a benchmark only provide comfort to the organization that they are doing the right things *right now*--they do not address how the organization will perform under times of stress or whether they will be able to sustain and repeat their successes in the long run. Because there will always be new and emerging threats, knowing how well the organization can perform today isn't as important as being able to predict how they will perform in the future when they encounter new events or a risk environment that is previously unknown.

Research Approach

CERT recognizes that organizations face challenges in managing operational resiliency in complex environments. The solution to addressing these challenges must have several dimensions. First and foremost, it must consider that security, business continuity, and IT operations management activities--typical operational risk management activities--are converging towards a continuum of practices that are focused on managing operational resiliency. Second, the solution must address the issues of measurement and metrics, providing a reliable and objective means for assessing competency and providing a basis for improving processes. And finally, the solution must help organizations to improve deficient processes--to close gaps that ultimately translate into weaknesses that diminish operational resiliency and impact the organization's ability to achieve strategic objectives.

Convergence

CERT's early research in this area concentrated on the shifting role of security from a technical specialty to a business and enterprise issue and competency. In this research, the challenges of security are characterized as a business problem that demands the attention of management and as a potential enabler to the organization in meeting its strategic objectives. Relative to this notion, security is described primarily as a risk management activity rather than an IT management activity, having significant enterprise implications. But, traditional security activities were deemed in our work to be too limiting with respect to operational risk management; in other words, the range of the types of operational risk are not expressly addressed by security activities (such as natural disasters) nor are the various components of

operational risk (threat, actor, motive, *and impact*). To do this requires the contribution of other operational risk management activities such as business continuity and IT operations management.

Many organizations are now beginning to realize that security, business continuity, and IT operations management are complimentary and collaborative functions that have the same goal: to improve and sustain operational resiliency. They share this goal because each function is focused on managing operational risk. This convergent view is often substantiated by popular codes of practice in each domain. For example, security practices now explicitly reference and include both business continuity and IT operations management practices as an acknowledgement that security practices alone do not address both the conditions and consequences of risk. In CERT's research, we characterize this convergence of domains and the resulting continuum of practices across these domains as "resiliency engineering."

Figure 1 provides a graphic description of convergence.

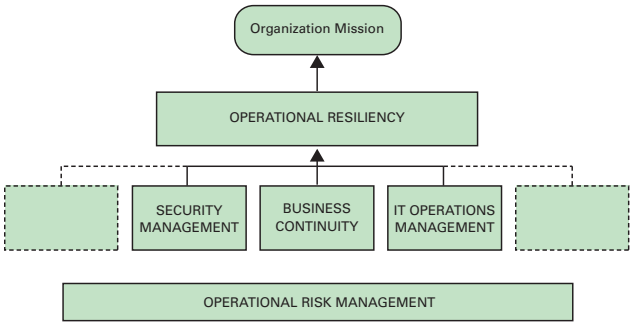


Figure 1: Foundation for Operational Resiliency Management

Resiliency Engineering

Resiliency engineering is defined as the processes and related practices that an organization uses to design, develop, implement, and manage the *protection* and *sustainability* of business-critical services, related business processes, and associated assets such as people, information, technology, and facilities. It collectively addresses the prevention of operational risk (typically through security and IT operations management-related practices) as well as the management of organizational impact if risk is realized—both of which are necessary to manage operational resiliency comprehensively.

To say that something has been "engineered" is to imply that a systematic process of design and construction originating from defined requirements has been undertaken [1]. Requirements are the foundation of all engineering-based processes, and the result of an engineered process is a product or service that substantially meets or exceeds all of the requirements that are established. Requirements also form the basis for managing operational resiliency. The protection and sustainability needs of an organizational service or asset are based on resiliency requirements that reflect how the service and related assets are used to support the organization's strategic objectives. When the organization fails to meet these requirements (either because of poor practices or as a result of disruptive events, threats, and risks), the operational resiliency of the service and assets is diminished, and one or more of the organization's strategic objectives fails to be met. Thus, operational resiliency depends on establishing requirements in order to build resiliency into assets and services and to keep these assets and services productive in the accomplishment of strategic objectives.

Through extensive review of existing codes of practice in the areas of security, business continuity, and IT operations management, as well as from experience with helping organizations to adopt a convergent view, CERT has codified a process definition for resiliency engineering processes in the CERT Resiliency Engineering Framework. The process definition embodies a requirements-driven foundation and describes the range of processes that characterize the organizational capabilities necessary to actively direct, control, and manage operational resiliency.

Providing a Process Improvement View

Defining the concept of resiliency engineering is not sufficient to help an organization transform from a security and business continuity perspective to one that is focused on resiliency and strategic objectives. While it provides a common understanding of the tasks that an organization must perform to manage operational resiliency, a simple definition of the resiliency engineering process will not provide sustainable process management and improvement. This is the domain of a process improvement approach.

As a process improvement model, the CERT Resiliency Engineering Framework seeks to allow organizations to use the process definition as a benchmark for identifying the current level of organizational capability, setting an appropriate and attainable desired target for performance, measuring the gap between current performance and targeted performance, and developing action plans to close the gap. By using the framework process definition as a foundation, the organization can obtain an objective characterization of performance not only against a base set of functional practices but also against practices that indicate successively increasing levels of process maturity. Thus, the organization is able to use the framework to determine its competency with an eye toward predicting its capabilities to perform consistently over time, to repeat its successes, and to perform reliably under times of stress.

More detailed discussion of the topics of convergence, resiliency engineering, and the application of a process improvement approach can be found in the technical notes *Managing for Enterprise Security* [2] and *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* [3] as well as other documents and presentations in the "Security and Resiliency Engineering" section of the CERT "Organizational Security" portal at www.cert.org.

CERT Resiliency Engineering Framework

The CERT Resiliency Engineering Framework is the first step in the development of a process improvement approach to operational resiliency management. It has several key components. The framework is comprised of 21 capability areas that define the major areas of resiliency engineering. A capability area is an area of practice that the organization must master to an appropriate degree to manage operational resiliency. An organization can seek to improve its performance across all capability areas or select one or more areas in which to concentrate benchmarking and improvement efforts.

The architecture of the CERT Resiliency Engineering Framework is arranged in four categories:

- Enterprise Management
- Engineering
- Operations
- Process Management

These categories represent the broad range of activities that are important to managing operational resiliency. However, because resiliency engineering is a process that traverses the organization and is dependent on cooperation and coordination, these categories serve only as a way to group capabilities by their common elements and focus. In reality, there is extensive interaction between capabilities, and thus, the categories provide a foundation from which interaction can be performed.

Enterprise Management

The enterprise is an important concept in the resiliency engineering process. At the enterprise level, the organization establishes and carries out many activities that the resiliency engineering process relies on. In addition, it provides the enterprise focus, oversight, and governance that is required for effective organizational and operational risk management. Typical capabilities in this category include financial resource management, compliance, communications, organizational training and awareness, and risk management.

Engineering

The management of operational resiliency is a requirements-driven engineering function. Thus, the capabilities in the Engineering category represent those that are focused on establishing and implementing resiliency for organizational assets, business processes, and services. These capabilities establish the basic building blocks for resiliency and create the foundation for the protection and sustainability of assets and, by reference, business processes and services. Engineering capabilities include asset definition and management, requirements definition, requirements management, service continuity, and controls management.

Operations

The Operations capabilities represent the core activities for managing the operational resiliency of assets and services. These capabilities are focused on sustaining an adequate level of operational resiliency as prescribed by the organization's strategic drivers, critical success factors, and risk appetite. These capabilities represent core security management, business continuity, and IT operations and service delivery management activities and focus on the resiliency of information, technology, and facilities assets. Operations capability areas include incident management and control, knowledge and information management, environmental control, technology management, vulnerability analysis and resolution, and external dependencies.

Process Management

Process Management capabilities represent those that are focused on measuring, managing, and improving the resiliency engineering process. These capabilities establish the initial extension of process improvement concepts to the resiliency engineering process and, by default, to the disciplines of security and business continuity. Capabilities in this category are intended to catalyze the organization's view of resiliency as a manageable and improvable process over which it has a significant level of control. Capabilities in this area are expected to expand significantly as more process improvement concepts are introduced to the framework, but currently include measurement and analysis and monitoring.

A more detailed description of the CERT Resiliency Engineering Framework that includes a detailed outline of the full framework can be found in the technical report *Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes* [4] and the *CERT Resiliency Engineering Framework Preview version, v0.95R* [6], which are available in the "Security and Resiliency Engineering" section of the CERT "Organizational Security" portal at www.cert.org.

Benefits

A framework-based process improvement approach to resiliency engineering is meant to help an organization be more efficient and effective in managing operational resiliency. Specifically, the CERT Resiliency Engineering Framework aims to

- **Create a common process definition.** A common process definition for resiliency engineering can reduce the ambiguity and vagueness that results from traditionally ill-defined processes like security management. It can also lay the foundation for future improvement because it provides a common understanding that can be discussed, debated, and revised.
- **Create a common language.** A common and sharable process definition brings a common language that can further reduce ambiguity, improve understanding and assimilation, and remove inhibitive barriers to growing a community around resiliency engineering. This is important not only for the organization itself but also in communications with suppliers, vendors, customers, regulators, and any external person or organization that needs to avoid issues that result from miscommunication.

- **Provide a consistent benchmark for measurement.** A common process definition and language are essential for establishing a capability benchmark. A benchmark can be a powerful tool for providing information on current performance, potential gaps, and strengths and weaknesses relative to other organizations. Benchmarking can also strengthen an entire industry by providing a way to communicate with regulators and lawmakers. And, organizations can use the benchmark to assess the capabilities of their vendors, customers, and other stakeholders who can affect their resiliency.
- **Help organizations to eliminate redundancy and cost.** The costs of managing operational resiliency continue to grow as organizations encounter new and increasingly unfamiliar risk environments. This results in mounting pressure to obtain funding (and to find new sources of funding) but also to be more cost effective and responsible in the ways that these funds (and other resources) are used. A process view forces the organization to look at how efficiently the process outcomes are being achieved and provides a foundation upon which the organization can make rational and, in some cases, quantitatively-based decisions regarding the optimal redeployment of resources.
- **Create viable process metrics.** The ability to extract cost from managing operational resiliency and bring value to the organization is dependent upon being able to measure the effectiveness and efficiency of the resiliency engineering process. Organizations have become complacent in accepting the absence of data as a measurement of effectiveness of risk management activities. Therein lies the advantages of a process view—a process that can be defined can also be measured and controlled. Organizations are not left to wonder whether their investment has value or whether the end result of the process is achieved because a process view allows them to objectively measure it.
- **Guide practice selection and implementation.** A process perspective turns the organization's focus to the outcome of the process. Through a process improvement framework, a process view provides a descriptive structure in which the right prescriptive best practices for the organization can be implemented and integrated. With a process view, an organization is less inclined to implement practices without connecting them to processes that can be measured and improved. In addition, because the CERT Resiliency Engineering Framework is industry and domain agnostic, an organization can use any code of practice to achieve process goals. Thus, adoption of the framework does not require an organization to abandon practices that it currently uses and which have been successful.
- **Provide a roadmap for maturing processes.** One of the challenges for security or business continuity is the ability to *sustain* competency and success. The organization's current practices may appear to be effective in managing the protection and sustainability of critical assets and business processes, but the accomplishment may be temporal. As conditions in the operational environment change, the organization may not be able to sustain its capability or repeat its success because it has not established the institutionalizing structures and practices that it needs to adopt mature processes. As a benchmark, the CERT Resiliency Engineering Framework will measure not only how well an organization is performing now (as is typical of existing assessment instruments), but if its performance is sustainable, consistent, and repeatable over time.

2008 Accomplishments

In 2008, significant progress was made on the development and transition of the CERT Resiliency Engineering Framework. The framework was published in April as the *CERT Resiliency Engineering Framework Preview version, v0.95R* for review and comment. The framework expands the key concepts in resiliency engineering to include characterization of capability levels, the organizational effect of capability improvement, and the common goals and practices that represent increasing levels of process maturity in resiliency engineering. The preview version includes 21 of the proposed 24 capability areas that compose version 1.0, which is scheduled for release in early 2009.

A companion document to CERT REF v0.95R, the *CERT Resiliency Engineering Framework: Code of Practice Crosswalk*, was published in June [7]. This document is intended to strengthen understanding of the connection between CERT REF capability areas and commonly used codes of practice that organizations deploy in an operational setting. The Crosswalk helps to achieve a primary goal of CERT REF: to allow security and business continuity practitioners to continue to use their preferred codes of practice at a tactical level while using CERT REF to achieve process improvement and maturity objectives at a process level.

In 2008, framework benchmarking activities were expanded with members of the Financial Services Technology Consortium (FSTC). (Information on the collaboration with FSTC can be found on their website at www.fstc.org.) Using a subset of the framework's capability areas, FSTC member organizations have validated their performance against the model to characterize performance in each capability area, document a repository of evidence that can be used to satisfy internal and external compliance obligations, and begin process improvement efforts in individual organizations. Coincident with this benchmarking activity, CERT has been developing and piloting a framework appraisal methodology that uses core concepts from the SCAMPI method (Standard CMM Appraisal Methodology for Process Improvement) that is used for CMMI appraisals.

As part of CERT's transition plans for CERT REF, a pilot version of the *Introduction to the CERT Resiliency Engineering Framework* course was developed and delivered to various government and industry groups in 2008. This course forms the basis of a larger planned educational effort in 2009, with the aim to provide broad education in resiliency engineering and process improvement.

2009 Plans

In 2009, version 1.0 of the full framework will be released for comment and review. This version of the framework will include updates to existing capability areas, the inclusion of new capability areas, an expansion of maturity practices for each capability area, and extensive examples and elaborations to facilitate adoption. Later in 2009, CERT plans to release additional content in a technical report that will help organizations to develop a process improvement effort and to commence adoption of the framework.

Based on continuing benchmarking activities, CERT plans to complete development on a fully functional REF-focused appraisal methodology, based on the SCAMPI method. A method description document will be released in 2009 and will form the basis for an appraisal program that will take shape late in 2009. The appraisal program will be focused on educating and developing personnel who want to be authorized to perform standard appraisals against the framework and to help organizations improve their management of operational resiliency.

Education is at the core of process improvement. Thus, CERT will begin to offer the *Introduction to the CERT Resiliency Engineering Framework* course beginning in February 2009. This course provides a basic understanding of managing operational resiliency using a process improvement model and provides attendees sufficient knowledge to begin using the concepts in CERT REF in their organizations. Later in 2009, CERT plans to offer additional coursework for instructors and appraisers.

Both the appraisal method and the introductory course will be part of a larger CERT REF licensing program that will be administered by the SEI Partner Network and will be announced in late 2009.

References

[1] MSN Encarta. *engineering.* http://encarta.msn.com /dictionary_/engineering.html (2007).

[2] Caralli, R. A. *Managing for Enterprise Security* (CMU/SEI-2004-TN-046). Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu /publications/documents/04.reports/04tn046.html

[3] Caralli, R. A. *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* (CMU/SEI-2006-TN-009). Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu /publications/documents/06.reports/06tn009.html

[4] Caralli, R. A. *Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes* (CMU/SEI-2007-TR-009). Software Engineering Institute, Carnegie Mellon University, 2007. http://www.sei.cmu.edu /publications/documents/07.reports/07tr009.html

[5] Chrissis, M. B., Konrad, M., & Shrum, S. *CMMI: Guidelines for Process Integration and Product Improvement.* Addison-Wesley, 2003 (ISBN 0-321-15496-7).

[6] Caralli, R. A. *CERT Resiliency Engineering Framework, v0.95R.* http://www.cert.org/resiliency_engineering/framework.html

[7] CERT Resiliency Engineering Framework, *Code of Practice Crosswalk v0.95R.* http://www.cert.org/resiliency_enginering /framework.html

PySiLK – A Language for Scripted Flow Manipulation

```
# This function examines a record at a time tio see if it matches the
# address blocks
def rwfilter(rec):
    global blockdict
    # If the dest has blocks, see if source is in those blocks
    if (rec. dip in blockdict):
        for pattern in blockdict[rec.dip]:
            if rec.sip in pattern:
                return True
    return False
```

Michael Duggan

Timothy Shimeall

PySiLK – A Language for Scripted Flow Manipulation

Problem Addressed

The System for internet-Level Knowledge (SiLK) analysis programs are a very powerful set of tools for the analysis of network flow data. These programs allow a user to do many operations over network flow records, such as filtering, sorting according to arbitrary fields, counting numbers of unique field combinations, and presenting textual representations of flow fields [1]. Many useful analyses can be done by combining these programs in various ways (see Collins and Reither [2] for an example). As flexible as these tools are, however, they are designed to do specific types of analyses. The programmers of these tools cannot predict all possible types of analysis. Consequently, users will always find features that they wish the current tools had implemented and will come up with ideas for completely new tools for new types of analysis. For efficient analytical efforts, the process of adding new features and tools needs to be rapid and iterative. Analysts typically are working under tight time constraints, so extensive development times are precluded. Analysts typically are working with partial knowledge of network behavior, so iterative development is required.

Research Approach

In an effort to solve this problem in a general way, the concept of a SiLK-specific expression language was invented. This domain-specific language, called SiLKScript, is compiled into an efficient byte-code that can be rapidly interpreted by the SiLK packing code. SiLKScript was completed and tested but was never put into production. The language started as a very simple set of expressions that could be evaluated in the context of a single network flow, but it was quickly found that there was much more context necessary for proper packing. Also, it was noted that an expression language would be very useful for doing various types of analysis work outside of the packing domain. As features were added to SiLKScript to make up for its deficiencies, we determined that it was probably not in our best interests to be making a complete, new programming language. This observation led directly to the experiments that led to the creation of PySiLK.

PySiLK [3] is an extension module for the Python programming language. It extends Python to make it easy to work with SiLK flow records. PySiLK does this by wrapping fundamental SiLK data structures within Python classes, allowing the Python scripting language access to the data from these structures.

Expected Benefits

New features and analyses can be written as new programs or modifications of the current programs, but writing or modifying SiLK tools in C or a similar language is a nontrivial task. Nor is a compiled language a very appropriate medium for one-off ideas or rapidly prototyping experiments. By making tool modification easier, PySiLK enables both more efficient customization of analysis and more rapid creation of new analysis methods to meet emerging needs. As both network architectures and security threats develop rapidly, being able to efficiently meet the needs of network defenders is a major benefit of this work. Making PySiLK a set of Python modules allows analysts to use the large body of pre-existing Python modules simply and directly as part of their customizations. Using pre-existing modules acts to reduce programming effort and to increase the quality of the resulting tools.

2008 Accomplishments

The fundamental object implemented was the RWRec, which represents a single SiLK flow record. All of the pieces of data that make up a SiLK flow are exported as attributes, such as source and destination IP address, number of bytes, and TCP flags. These attributes can be accessed and modified from within Python. Objects for IP addresses (IPAddr) and TCP flags (TCPFlags) were also created in order to allow for easy manipulation of these fundamental attribute types.

Also implemented were SilkFile objects, which allow the reading and writing of flow records from and to files, IPWildcard objects, which represent ranges of IP addresses, and IPSet objects, which allow for set operations across IPv4 IP address-space. All objects were written with the goals of exposing as much useful functionality from the SiLK libraries to Python as possible, and doing so in a style that was consistent with normal Python programming.

The PySiLK extension module can be used within a standalone Python program. For example, a program can read a SiLK flow file and examine its data, then arbitrarily modify, write out, or summarize that data in any way that the user implements in Python. However, PySiLK can also be used to create user-defined modifications to the behavior of several fundamental SiLK programs in the form of PySiLK plug-ins.

Several SiLK programs have been written with special consideration for user-extensibility. A plug-in mechanism was created so that users could write their own extensions to these programs. One plug-in called silkpython [4] was written that enables users to use Python to write these extensions.

One program that can be extended is the rwfilter program. The rwfilter program is used to filter out (or in) flows from SiLK files or a SiLK repository based on user-selected criteria. The silkpython plug-in allows a Python program to implement a filter function that takes a single flow as an argument and returns a boolean pass or fail value. Using this plug-in, a user can implement more complicated selection criteria than the base rwfilter program supports and can also maintain state from between flows.

Three other programs—rwcut, rwsort, and rwuniq—do their work based on a set of selected flow fields. These fields are various attributes of a SiLK flow record, such as source or destination IP address, IP protocol number, and TCP flags. The rwcut program outputs human-readable representations of the specified fields, the rwsort program sorts based on the specified fields, and the rwuniq program outputs volume counts for flows based on matches for distinct combinations of the specified fields. The silkpython plug-in allows the user to create new fields with their own distinct text representation, sort order, and binary uniqueness values. The user supplies a name for each new field and functions that will take a SiLK flow and output either a textual representation, binary sorting value, or a binary value for uniqueness binning.

Several useful analyses have now been performed using PySiLK. One is the spam response analysis documented elsewhere in this research report [5]. This analysis plug-in used Python data structures to build a dynamic map and search it for later response traffic. Another analysis used PySiLK to measure the time interval between successive flows (documented in the *SiLK Analysts' Handbook* [1]), which is useful as a precursor to beacon detection. This analysis plug-in uses Python variables to maintain state across flows. PySiLK has also been used to generate visualizations of flow data, implemented as a stand-alone script.

2009 Plans

One of the predecessors of PySiLK was SiLKScript, originally created for the purpose of generalizing SiLK packing. SiLKScript determined how flows were stored in files for archival purposes. SiLK 1.0 did not use a scripting language for this purpose, but instead created a plug-in infrastructure that allows a specific set of packing logic to be selected at runtime. These plug-ins need to be written in a compiled language such as C. One logical future extension is to allow these plug-ins to be written in Python using PySiLK.

Another area of future extension is to implement further flow-specialized data structures using Python's type language. PySiLK currently supports sets, but the SiLK analysis suite also supports bags and prefix maps, which provide volume and type information on addresses. Extensions to the SiLK suite have been implemented on a prototype basis to provide flow graph structures, supporting calculations including spread, extent, and centroid, and flow clusters, facilitating recognition of similarity across groups of flows. Further structures that support inference rules on flow may also be productive extensions to implement in PySiLK.

PySiLK also offers an opportunity for more direct integration of the SiLK suite and other useful analytic and operational environments. Previously, the only integration options were via pipes or files. PySiLK allows for recasting of outputs to better support internal integration, invoking analytic functions from environments such as R [6]. PySiLK is also expected to aid in the interpretation of flow data in the context of other available network data, producing more robust analytical options.

References

[1] Shimeall, T., De Shon, M., Faber, S., & Kompanek, A. *The SiLK Analysts' Handbook.* http://tools.netsa.cert.org/silk/analysis-handbook.pdf (2008).

[2] Collins, M. & Reiter, M. "Hit-List Worm Detection and Bot Identification in Large Networks Using Protocol Graphs." *Proceedings of Recent Advances in Intrusion Detection 2007 10th International Symposium* (RAID 2007).

[3] PySiLK: SiLK in Python. http://tools.netsa.cert.org/silk/pysilk/

[4] silkpython – SiLK Python plug-in. http://tools.netsa.cert.org/silk/silkpython.html

[5] Shimeall, T. "Direct Response to Spam Email," *2008 CERT Research Annual Report.*

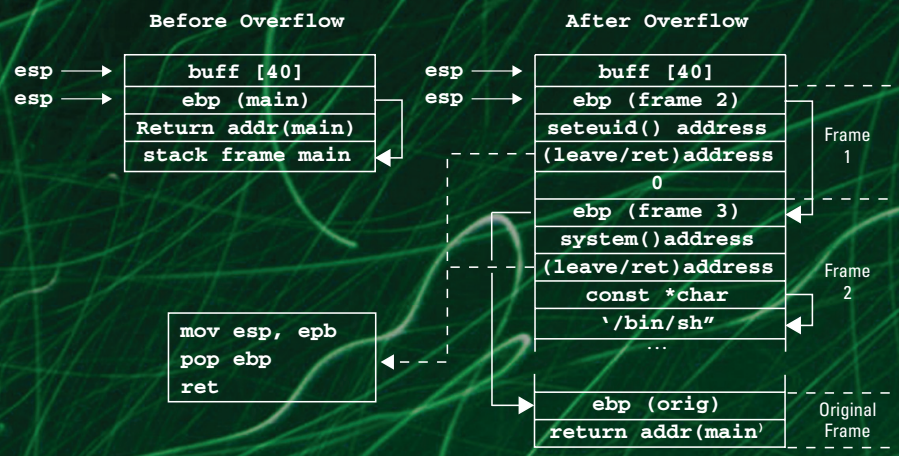
[6] *The R Project for Statistical Computing.* http://www.r-project.org/

Robert Seacord

David Svoboda

Chad Dougherty

Secure Coding Initiative



Secure Coding Initiative

Problem Addressed

Software vulnerability reports continue to grow at an alarming rate, with a significant number of these reports resulting in technical security alerts. To address this growing threat to governments, corporations, educational institutions, and individuals, software must be developed that is free from software vulnerabilities and other software defects.

The Secure Coding Initiative (SCI) was established to work with software developers and software development organizations to eliminate vulnerabilities resulting from coding errors before software is deployed. Additionally, work in the SCI applies to safety-critical applications (those in which it is critical to prevent behavior that might lead to loss of human life, human injury, or damage to human property) and mission-critical applications (those in which it is critical to prevent behavior that might lead to property loss or damage or economic loss or damage).

Research Approach

Secure Coding Standards

The SCI is building a comprehensive approach to secure software development in the C, C++, and Java programming languages.

An essential element of secure software development is a well documented and enforceable coding standard. Coding standards encourage programmers to follow a uniform set of rules and guidelines determined by the requirements of the project and organization, rather than by the programmer's familiarity or preference.

Developers and software designers can apply these coding standards to their code to create secure systems, or they can analyze existing code against these standards. Secure coding standards provide a metric for evaluating and contrasting software security, safety, and reliability, and related properties.

The SCI coordinates development of secure coding standards by security researchers, language experts, and software developers using a wiki-based community process. The *CERT C Secure Coding Standard,* for example, was published in October 2008 as an Addison-Wesley book [1]. Once completed, these standards will be submitted to open standards bodies for consideration and possible publication.

Static Analysis Tools

Secure coding standards alone are inadequate to ensure secure software development because they may not be consistently and correctly applied. To solve this problem, the SCI is developing an application certification process that can be used to verify the conformance of a software product to a secure coding standard. Because this process depends on the application of source code analysis tools, the SCI is working with industry partners such as LDRA and Fortify Software, and with research partners such as JPCERT and Lawrence Livermore National Laboratory, to enhance existing source code analysis tools to verify compliance with CERT guidelines.

Application Certification

The application certification process under development consists of a comprehensive code review that relies heavily on static analysis. Among other tools, the Secure Coding Initiative is using the Compass/ROSE compiler and static analysis suite, which has been extended to check for rules contained within the CERT C Secure Coding Standard.

For each rule and recommendation, the source code is certified as provably nonconforming, deviating, conforming, or provably conforming.

- The code is provably nonconforming if one or more violations of a rule are discovered for which no deviation has been specified.
- Deviating code is code for which the application developer has a documented deviation. This documentation is included with the certification.
- The code is conforming if no violations of a rule could be identified.
- Finally, the code is provably conforming if the code has been verified to adhere to the rule in all possible cases.

Once the process is completed, a report detailing the conformance or nonconformance for each CERT C Secure Coding rule is provided to the customer.

Courses and Education

The SCI has developed a four-day *Secure Coding in C and C++* course that identifies common programming errors in C and C++ and describes how these errors can lead to code that is vulnerable to exploitation. The course concentrates on security issues intrinsic to the C and C++ programming languages and associated libraries and is based on the Addison-Wesley book by the same name [2]. This course is currently being offered by the SEI and by SEI partner organizations.

The SCI is also involved in teaching secure programming to undergraduates in the Computer Science department at Carnegie Mellon and secure software engineering to graduate students in Carnegie Mellon's Information Networking Institute, and is working with other universities to improve their software security courses.

Expected Benefits

The goal of this effort is to reduce the number of vulnerabilities deployed in operational software by preventing their introduction or discovering and eliminating security flaws during implementation and test. Organizations can benefit from this work by

1. participating in the development of CERT Secure Coding Standards and applying these standards in their software development process
2. adopting, extending, and using static analysis tools (some of which are freely available) that have been enhanced to detect violations of CERT Secure Coding guidelines
3. training their software development workforce through secure coding courses developed and offered by the SEI and partner organizations

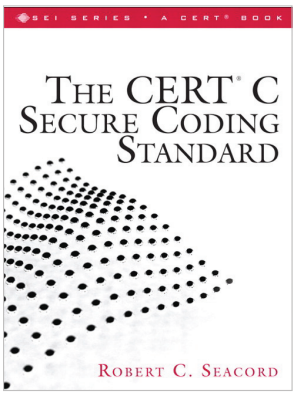
2008 Accomplishments

Industry Study

In 2008, the SCI conducted a joint study with JPCERT, Japan's first computer security incident response team (CSIRT), to evaluate the efficacy of CERT Secure Coding Standards and source code analysis tools in improving the quality and security of commercial software projects [3]. SCI successfully extended two source code analysis tools, Fortify SCA and Lawrence Livermore National Laboratory's Compass/ROSE. The extended versions of these static analysis tools were used by Software Research Associates, Inc. (SRA), a well-established Japanese software development firm, to evaluate a toll collection application written in C++ and a Video Service Communication Protocol written in the C programming language. The study demonstrated that both the CERT Secure Coding Standards and the static analysis tools could be used successfully to improve the quality and security of commercial software applications.

The CERT C Secure Coding Standard

In October 2008, Addison-Wesley published the first official release of *The CERT C Secure Coding Standard.* This standard was developed to provide organizations with the ability to develop code that is robust and more resistant to attack. The standard's guidelines—if applied appropriately—eliminate the critical coding errors that lead to buffer overflows, format string vulnerabilities, and other common software vulnerabilities. Each guideline in the standard provides examples of insecure code and alternative secure code implementations. The standard is currently being used as a basis for the Global Information Assurance Certification (GIAC) Secure Software Programmer-C (GSSP-C) exam and certification.



More than 220 contributors and reviewers participated in the standard's development and review over a period of two and a half years. Additionally, the standard was reviewed by the ISO/IEC WG14 international standardization working group for the programming language C, members of the Association of C and C++ Users (ACCU), and other members of the C language development and software security communities.

International Standards

The CERT Secure Coding Initiative has been sending technical experts to ISO/IEC (the International Organization for Standardization) meetings since 2005.

CERT has worked with the ISO/IEC WG14 standards committee to improve security in the C language and with ISO/IEC WG23 Programming Language Vulnerabilities in the development of TR 24772, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use.*

Software Security Assessments

The SCI conducted software security assessments for the Operationally Responsive Space Satellite Data Model, Areva, and the Office of Navy Intelligence. These assessments included systems developed in C, C++, and Java.

2009 Plans

International Standards Activities

Two major international standards efforts are planned for 2009. The first is to enhance the CERT C Secure Coding Standard and submit it to WG14 and WG23 as the C language Annex to ISO/IEC TR 24772, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use*. The second is to work with the member organizations of WG14 to draft a proposal for an annex to the C1X major revision to the C language standard. This annex will define an informative but optional security profile to be implemented to create safe, secure compilers (as opposed to traditional compilers, which emphasize performance).

Secure Coding Standards

The CERT Secure Coding Initiative will continue to collaborate with Sun Microsystems to develop *The CERT Sun Microsystems Secure Coding Standard for Java*. This standard provides guidance for secure programming in the Java Platform Standard Edition 6 environment. Programmers who adopt the Java standard can avoid vulnerabilities in Java systems. This coding standard affects the wide range of products coded in Java, such as PCs, game players, mobile phones, home appliances, and automotive electronics.

The SCI will also continue to develop a C++ Secure Coding Standard and maintain and enhance the existing C Secure Coding Standard.

Secure Design Patterns

The SCI plans to research and document occurrences of negative and positive secure design patterns. The negative patterns indicate flawed designs that are susceptible to attack. The positive patterns indicate secure design patterns that have been successfully implemented one or more times and have proven effective at preventing or mitigating attacks.

References

[1] Seacord, R. C. *The CERT C Secure Coding Standard.* Addison-Wesley Professional, 2008 (ISBN: 0-321-56321-2).

[2] Seacord, R. C. *Secure Coding in C and C++.* Addison-Wesley Professional, 2005 (ISBN: 0-321-33572-4).

[3] Dewhurst, S., Dougherty, C., Ito, Y., Keaton, D., Saks, D., Seacord, R. C., Svoboda, D., Taschner, C., & Togashi, K. *Evaluation of CERT Secure Coding Rules through Integration with Source Code Analysis Tools* (CMU/SEI-2008-TR-014, ADA482285). Carnegie Mellon University, Software Engineering Institute, 2008. http://www.sei.cmu.edu/pub/documents/08.reports/08tr014.pdf

SQUARE: Requirements Engineering for Improved System Security

Nancy Mead

Justin Zahn

SQUARE: Requirements Engineering for Improved System Security

Problem Addressed

It is well recognized in industry that requirements engineering is critical to the success of any major development project. Several authoritative studies have shown that requirements engineering defects cost 10 to 200 times as much to correct once fielded than if they are detected during requirements development [1,2]. A more recent vendor example indicates that it is 100 times cheaper to fix security flaws at requirements time than after a product has been released [3]. Other studies have shown that reworking requirements, design, and code defects on most software development projects costs 40 to 50 percent of total project effort [4], and the percentage of defects originating during requirements engineering is estimated at more than 50 percent [5]. The total percentage of project budget due to requirements defects is 25 to 40 percent [6].

The National Institute of Standards and Technology (NIST) reports that software faulty in security and reliability costs the economy $59.5 billion annually in breakdowns and repairs [7]. The costs of poor security requirements make apparent that even a small improvement in this area will provide a high value. By the time an application is fielded and in its operational environment, it is very difficult and expensive to significantly improve its security.

Requirements problems are among the top causes of why

- projects are significantly over budget, past schedule, have significantly reduced scope, or are cancelled
- development teams deliver poor-quality applications
- products are not significantly used once delivered

These days we have the further problem that the environment in which we do requirements engineering has changed, resulting in an added element of complexity. Software development occurs in a dynamic environment that changes while projects are still in development, with the result that requirements are in flux from the beginning. This can be due to conflicts between stakeholder groups, rapidly evolving markets, the impact of tradeoff decisions, and so on.

When security requirements are considered at all during the system life cycle, they tend to be general lists of security features such as password protection, firewalls, virus detection tools, and the like. These are, in fact, not security requirements at all but rather implementation mechanisms that are intended to satisfy unstated requirements, such as authenticated access. As a result, security requirements that are specific to the system and that provide for protection of essential services and assets are often neglected. In addition, the attacker perspective is not considered, with the result that security requirements, when they exist, are likely to be incomplete. We believe that a systematic approach to security requirements engineering will help to avoid the problem of generic lists of features and to take into account the attacker perspective.

In reviewing requirements documents, we typically find that security requirements, when they exist, are in a section by themselves and have been copied from a generic set of security requirements. The requirements elicitation and analysis that is needed to get a better set of security requirements seldom takes place.

Much requirements engineering research and practice has addressed the capabilities that the system will provide. So while significant attention is given to the functionality of the system from the user's perspective, little attention is given to what the system should *not* do. In one discussion on requirements prioritization for a specific large system, ease of use was assigned a higher priority than security requirements. Security requirements were in the lower half of the prioritized requirements. This occurred in part because the only security requirements that were considered had to do with access control.

Research Approach

The CERT Program has developed a methodology to help organizations build security into the early stages of the production life cycle. The Security Quality Requirements Engineering (SQUARE) methodology consists of nine steps that generate a final deliverable of categorized and prioritized security requirements. Although SQUARE could likely be generalized to any large-scale design project, it was designed for use with information technology systems.

The SQUARE process involves the interaction of a team of requirements engineers and the stakeholders of an IT project. It begins with the requirements engineering team and project stakeholders agreeing on technical definitions that serve as a baseline for all future communication. Next, assets are identified and business and security goals are outlined. Third, artifacts and documentation are created, which are necessary for a full understanding of the relevant system. A structured risk assessment determines the likelihood and impact of possible threats to the system.

Following this work, the requirements engineering team determines the best method for eliciting initial security requirements from stakeholders. This determination depends on several factors, including the stakeholders involved, the expertise of the requirements engineering team, and the size and complexity of the project. Once a method has been established, the participants rely on artifacts and risk assessment results to elicit an initial set of security requirements. Two subsequent stages are spent categorizing and prioritizing these requirements for management's use in making tradeoff decisions. Finally, an inspection stage is included to ensure the consistency and accuracy of the security requirements that have been generated.

The methodology is most effective and accurate when conducted with a team of requirements engineers with security expertise and the stakeholders of the project. SQUARE's nine discrete steps are outlined in Table 1. Each step identifies the necessary inputs, major participants, suggested techniques, and final output. Generally, the output of each step serves as

the sequential input to the ensuing steps, though some steps may be performed in parallel. For instance, it might be more efficient for the requirements engineering team to perform Step 2 (Identify Assets and Security Goals) and Step 3 (Develop Artifacts) simultaneously, since to some extent they are independent activities. The output of both steps, however, is required for Step 4 (Perform Risk Assessment). In principle, Steps 1-4 are actually activities that precede security requirements engineering but are necessary to ensure that it is successful.

The SQUARE process is described in a technical report [8] and is suitable for incorporation into development practice. SQUARE is described in the Requirements Engineering section of the Build Security In website [9] and in three books [10, 11, 12]. CERT is currently continuing research and application of the process and is working to develop a robust tool to support each stage of the methodology.

Expected Benefits

When SQUARE is applied, the user should expect to have identified, documented, and inspected relevant security requirements for the system or software that is being developed. SQUARE may be more suited to a system under development or one undergoing major modification than one that has already been fielded, although it has been used both ways.

2008 Accomplishments

In conjunction with CyLab, the SQUARE prototype tool, workshop, tutorial, and educational materials were developed and released. A set of invited talks on SQUARE was delivered at the National Institute for Informatics (NII) in Tokyo. The initial version of SQUARE-Lite, a five-step process extracted from SQUARE, was applied in a client organization. We developed an initial privacy requirements engineering capability and integrated it into the SQUARE prototype tool. A technical note on SQUARE [13] discusses ways of integrating SQUARE into standard life-cycle processes. Papers on life-cycle process integration were also presented at conferences [14, 15].

2009 Plans

We are working with a Carnegie Mellon University Master of Software Engineering Studio Team to develop a robust tool to replace the current prototype tool. We plan to integrate privacy considerations more fully with SQUARE and to extend SQUARE for use in acquisition. We will continue to publish and to take advantage of client opportunities to apply SQUARE in the field.

References

[1] Boehm, B. W. & Papaccio, P. N. "Understanding and Controlling Software Costs." *IEEE Transactions on Software Engineering SE-4*, 10 (Oct. 1988): 1462–77.

[2] McConnell, S. "From the Editor - An Ounce of Prevention." *IEEE Software 18*, 3 (May 2001): 5–7.

[3] Meftah, B. "Business Software Assurance: Identifying and Reducing Software Risk in the Enterprise." https://buildsecurityin.us-cert.gov/swa/downloads/Meftah.pdf

[4] Jones, C., ed. *Tutorial: Programming Productivity: Issues for the Eighties, 2nd Ed.* IEEE Computer Society Press, 1986.

[5] Wiegers, K. E. "Inspecting Requirements" (column). *StickyMinds*, July 30, 2001. http://www.stickyminds.com

[6] Leffingwell, D. & Widrig. D. *Managing Software Requirements–A Use Case Approach*, 2nd ed. Addison-Wesley, 2003.

[7] National Institute of Standards and Technology. "Software Errors Cost U.S. Economy $59.5 Billion Annually" (NIST 2002-10). http://www.nist.gov/public_affairs /releases/n02-10.htm (2002).

[8] Mead, N. R., Hough, E., & Stehney, T. *Security Quality Requirements Engineering (SQUARE) Methodology* (CMU/SEI-2005-TR-009). Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu /publications/documents/05.reports/05tr009.html

[9] Software Engineering Institute. Build Security In. https://buildsecurityin.us-cert.gov/ (2008).

[10] Mead, N. R., Davis, N., Dougherty, C., & Mead, R. Ch. 8, "Recommended Practices," 275–308. *Secure Coding in C and C++,* Robert Seacord. Addison Wesley Professional, 2005.

[11] Mead, N. R. Ch. 3, "Identifying Security Requirements Using the SQUARE Method," 44–69. *Integrating Security and Software Engineering: Advances and Future Visions* H. Mouratidis & P. Giorgini. Idea Group, 2006 (ISBN: 1-59904-147-2).

[12] Allen, J., Barnum, S., Ellison, R., McGraw, G., & Mead, N. R. *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley Professional, 2008 (ISBN-13: 978-0-321-50917-8).

[13] Mead, N. R., Viswanathan, V., Padmanabhan, D., & Raveendran, A. *Incorporating Security Quality Requirements Engineering (SQUARE) into Standard Life-Cycle Models* (CMU/SEI-2008-TN-006). Software Engineering Institute, Carnegie Mellon University, 2008. http://www.sei.cmu.edu /publications/documents/08.reports/08tn006.html

[14] Mead, N. R., Viswanathan, V., & Padmanabhan, D. "Incorporating Security Requirements Engineering into the Dynamic Systems Development Method," 949–954. COMPSAC (International Computer Software and Applications Conference) 2008, *IWSSE Workshop (International Workshop on Security and Software Engineering),* July 28, 2008, Turku, Finland. IEEE Computer Society, 2008.

[15] Mead, N. R., Viswanathan, V., & Zhan, J. "Incorporating Security Requirements Engineering into the Rational Unified Process," 537–542. 2008 *International Conference on Information Security and Assurance (ISA)*, Busan, Korea, April 26–28, 2008. IEEE Computer Society, 2008.

Table 1: Security Requirements Elicitation and Analysis Process

	Step	Input	Techniques	Participants	Output
1	Agree on definitions	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Stakeholders, requirements team	Agreed-to definitions
2	Identify assets and security goals	Definitions, candidate goals, business drivers, policies and procedures, examples	Facilitated work session, surveys, interviews	Stakeholders, requirements engineer	Assets and goals
3	Develop artifacts to support security requirements definition	Potential artifacts (e.g., scenarios, misuse cases, templates, forms)	Work session	Requirements engineer	Needed artifacts: scenarios, misuse cases, models, templates, forms
4	Perform risk assessment	Misuse cases, scenarios, security goals	Risk assessment method, analysis of anticipated risk against organizational risk tolerance, including threat analysis	Requirements engineer, risk expert, stakeholders	Risk assessment results
5	Select elicitation techniques	Goals, definitions, candidate techniques, expertise of stakeholders, organizational style, culture, level of security needed, cost benefit analysis, etc.	Work session	Requirements engineer	Selected elicitation techniques
6	Elicit security requirements	Artifacts, risk assessment results, selected techniques	Joint Application Development (JAD), interviews, surveys, model-based analysis, checklists, lists of reusable requirements types, document reviews	Stakeholders facilitated by requirements engineer	Initial cut at security requirements
7	Categorize requirements as to level (system, software, etc.) and whether they are requirements or other kinds of constraints	Initial requirements, architecture	Work session using a standard set of categories	Requirements engineer, other specialists as needed	Categorized requirements
8	Prioritize requirements	Categorized requirements and risk assessment results	Prioritization methods such as Triage, Win-Win	Stakeholders facilitated by requirements engineer	Prioritized requirements
9	Inspect requirements	Prioritized requirements, candidate formal inspection technique	Inspection method such as Fagan, peer reviews	Inspection team	Initial selected requirements, documentation of decision making process and rationale

STAR*Lab: A Software Development Laboratory for Security Technology Automation and Research

Richard Linger

Stacy Prowell

STAR*Lab: A Software Development Laboratory for Security Technology Automation and Research

Developing Engineering Automation for Challenge Problems in System Security

CERT has established a software development capability in response to the growing needs of its customers. The mission of STAR*Lab (Security Technology Automation and Research Laboratory) is development of theory-based prototype automation that provides operational solutions to challenge problems in security engineering and software assurance.

Challenge problems are barriers to progress identified by Department of Defense and other organizations whose solutions can have substantial impact on engineering capabilities. The focus of STAR*Lab is on applying theory to implement practical tools. The purpose of the laboratory is to help its sponsors achieve three objectives:

- **Faster development:** Solutions must replace time- and resource-intensive operations with engineering automation that permits faster system development.
- **Improved quality:** Solutions must augment human processes with foundations-based automation to improve system security and dependability.
- **Fewer resources:** Solutions must increase the span of intellectual control through automation for more effective use of resources in developing systems.

The laboratory operates according to three principles:

- **Foundations-first principle.** Theoretical foundations are necessary to ensure completeness and correctness in automated solutions and confidence in the results they produce. All projects start with sound foundations to avoid ad hoc solutions with limited applicability.
- **Proof-by-automation principle.** Automation is essential to replace resource-intensive human operations with solutions that augment intellectual control. All projects will demonstrate solutions through automated engineering tools.
- **Practical application principle.** Automation must solve challenge problems with practical engineering operations for routine use by practitioners. All projects will scale up engineering solutions for widespread application.

STAR*Lab projects are managed within a gated review structure designed to maintain visibility, reduce risk, and ensure effective use of sponsor resources. Projects must satisfy the requirements of each gate to receive funding to progress to the next gate:

- **Gate 1: Challenge problem definition.** Each project must address a barrier to progress through a project plan that defines team composition, tasks, and schedules.
- **Gate 2: Theoretical feasibility.** Each project must identify theoretical foundations to avoid heuristic or partial approaches of limited value for achieving a comprehensive solution.
- **Gate 3: Proof-of-concept automation.** Each project must develop prototype automation that demonstrates application of the theoretical foundations.
- **Gate 4: Scale-up for application.** Each project must evolve the prototype automation to scale up engineering capabilities for routine application.

STAR*Lab is currently engaged in evolution and transition activities for the Function Extraction (FX) for Software Assurance project, whose objective is computing software behavior. In addition, CERT is ready to capitalize on function extraction technology in three potential FX-based project areas:

- **Computational Security Attribute Analysis**
- **Support for Automated Software Correctness Verification**
- **Support for Component Integration in Network Systems**

These projects are described in other sections of this report.

Support for Automated Software Correctness Verification

Computed Behavior
- condition: ?true
  - Registers
    - EAX := EBX
    - EBX := EAX
    - ESP := (4 +d *ESP*)
  - Flags
    - AF := false
    - CF := false
    - OF := false
    - PF := is_even_parity_lowbyte(*EBX*)
    - SF := is_neg_Signed_32(*EBX*)
    - ZF := (0 == *EBX*)
  - Memory
    - M := update_memory(old_memory=*M*, updates=mem_32((-4 +d *ESP*),*ECX*) $ mem_32((-8 +d *ESP*),*EBX*)
    - label := "exit"
  - External

Mark Pleszkoch

Stacy Prowell

Richard Linger

Support for Automated Software Correctness Verification

Problem Addressed

Software containing errors and vulnerabilities cannot be trustworthy or secure. Yet despite best efforts, software is often developed and delivered with incorrect and even unknown behavior. In the current state of practice, no practical means exists for automation support of large-scale correctness verification of software with respect to intended behavior. As a result, much time and energy is devoted to inspection and testing activities that often provide only limited evidence of correctness.

Research Approach

The objective of this potential project is to develop a prototype function verification system that will help users to check the correctness of programs based on their actual computed behavior. The system will employ the mathematics-based foundations of function extraction to achieve completeness and correctness of results. The system will provide a proof of concept for function verification technology and a foundation for elaboration into industrial-strength verification systems. In addition, the system will provide a standard, machine-processable form for representing intended behavior. Users will be able to code programs to satisfy intended behavior and execute the system to help check correctness.

Function extraction and function verification are closely related. Functional correctness verification requires computing the as-built functional behaviors of program structures, just as in the function extraction process, and then comparing those behaviors to intended behaviors for equivalence or not. The function-theoretic model of software treats programs as rules for mathematical functions or relations—that is, mappings from domains to ranges. While programs can contain an intractable number of execution paths, they are at the same time composed of a finite number of control structures, each of which implements a mathematical function or relation in the transformation of its inputs into outputs.

A theorem defines the mapping of these control structures into procedure-free functional form [1,2]. These mappings are the starting point for the function extraction process and its application to correctness verification.

Figure 1 depicts a miniature illustration of use of computed behavior for correctness verification. The function extraction system has been applied to compute the behavior of the assembly language program on the left. The computed behavior on the right is expressed in terms of a conditional concurrent assignment. The condition is true (the program is a sequence of instructions that always executes), and the concurrent assignments are organized in register, flag, and memory categories. The register assignments indicate that the final value of register EAX is the initial value of register EBX, and the final EBX value is the initial EAX value. That is, the program swaps the values in the two registers and sets the flags and memory as shown. For verification, this behavior can be compared to specifications or simply to intentions to determine whether the program is correctly carrying out intended operations.

Expected Benefits

This project can provide benefits to sponsors who must deal with software failures and vulnerabilities in enterprise operations. It is difficult to achieve trustworthiness and security goals for systems without knowing whether they are correct with respect to intended behavior. Routine availability of functional verification can help reduce errors, vulnerabilities, and malicious code in software. Verification technology can replace much of the labor-intensive and error-prone work of program inspection and testing, with corresponding reductions in resource requirements and improvements in product quality [3].

2008 Accomplishments

The function extraction system currently under development provides a foundation for implementing correctness verification capabilities. Demonstrations of correctness verification have been conducted.

2009 Plans

CERT is ready to extend FX technology for automation of correctness verification for interested sponsors.

References

[1] Prowell, S., Trammell, C., Linger, R., & Poore, J. *Cleanroom Software Engineering: Technology and Practice.* Addison Wesley, 1999.

[2] Mills, H. & Linger, R. "Cleanroom Software Engineering." *Encyclopedia of Software Engineering, 2nd ed.* (J. Marciniak, ed.). John Wiley & Sons, 2002.

[3] Hevner, A., Linger, R., Collins, R., Pleszkoch, M., Prowell, S., & Walton, G. *The Impact of Function Extraction Technology on Next-Generation Software Engineering* (CMU/SEI-2005-TR-015). Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05tr015.html

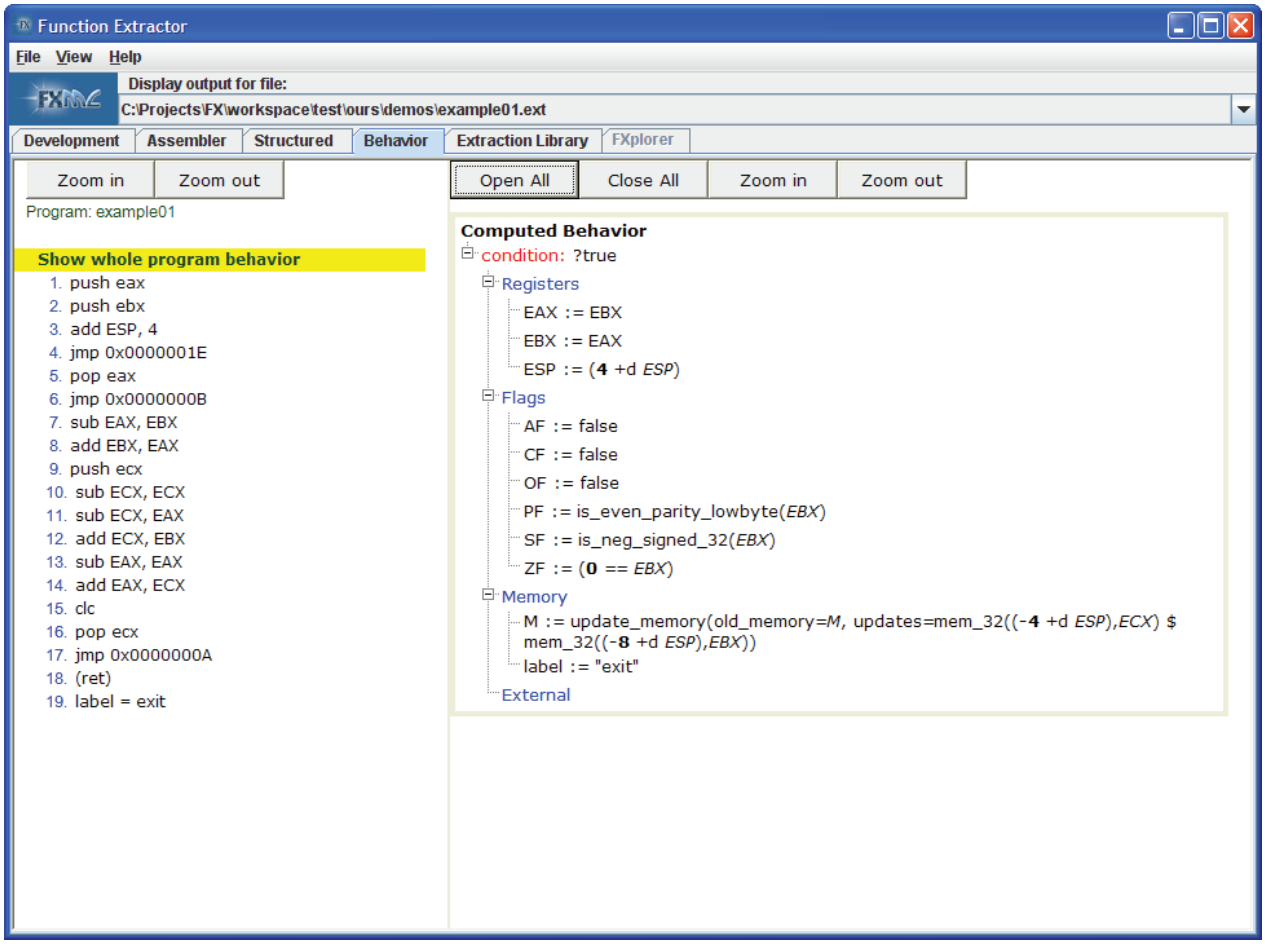


Figure 1: A Miniature Example of Correctness Verification Using Computed Behavior Produced by Function Extraction Technology

Support for Component Integration in Network Systems

Kirk Sayre

Tim Daly

Support for Component Integration in Network Systems

Problem Addressed

Modern systems are characterized by large-scale heterogeneous networks with many components that must be correctly integrated to achieve mission objectives. It is often the case that the components are complex systems in their own right and must be dynamically integrated to provide end-to-end capabilities. System integration today is a complex, labor-intensive process that can require substantial effort for large systems. Automation support for behavior analysis of component compositions could help reduce the time and effort required to achieve operational capabilities [1].

Research Approach

This project will explore the extent to which component compositions can be automatically calculated. The mathematical foundations of Flow Structure technology of Flow-Service-Quality (FSQ) Engineering [2,3,4] form a basis for this effort. Automation support for determining composite behavior of components architected into systems could help enable fast and reliable understanding and development. Composition computation must generate mathematically correct abstractions of behavior at any level and help scale up the reliable unit of construction for systems. Because behavior calculation is essentially a compositional task, function extraction is the key underlying technology for component composition. FX produces behavior databases of individual programs; the databases themselves can be composed to reveal the composite behavior of the programs when combined into systems.

Expected Benefits

Automated derivation of the net effect of program compositions can help reveal combined functionality, illuminate mismatches, facilitate analysis of design alternatives, and support evaluation of commercial off-the-shelf products. This approach can also guide refactoring of components and systems in responding to new system requirements.

2008 Accomplishments

Research and development carried out in the FX project has direct applicability to automated composition of components.

2009 Plans

A key step toward creation of an automated composition capability is extension of FX technology to create a proof-of-concept prototype. Sponsors are welcome to join in this effort.

References

[1] Feiler, P., Goodenough, J., Linger, R., Longstaff, T., Kazman, R., Klein, M., Northrop, L., Wallnau, K., Gabriel, R., Schmidt, D., & Sullivan, Kevin. *Ultra-Large-Scale Systems: The Software Challenge of the Future.* Software Engineering Institute, Carnegie Mellon University, June, 2006. http://www.sei.cmu.edu/uls

[2] Hevner, A., Linger, R., Sobel, A., & Walton, G. "The Flow-Service-Quality Framework: Unified Engineering for Large-Scale, Adaptive Systems." *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS35).* Waikoloa, HI, Jan. 7–10, 2002. IEEE Computer Society Press, 2002.

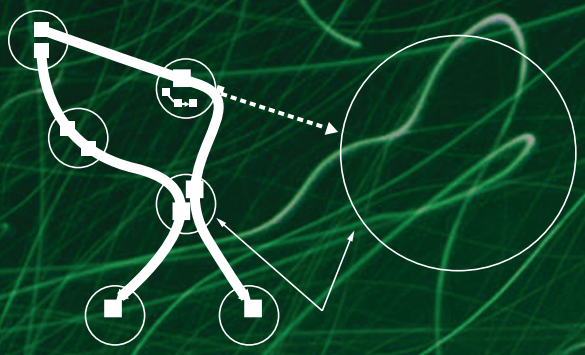
[3] Linger, R., Pleszkoch, M., Walton, G., & Hevner, A. *Flow-Service-Quality (FSQ) Engineering: Foundations for Network System Analysis and Development* (CMU/SEI-2002-TN-019). Software Engineering Institute, Carnegie Mellon University, 2002. http://www.sei.cmu.edu/publications/documents/02.reports/02tn019.html

[4] Hevner, A., Linger, R., Pleszkoch, M., & Walton, G. "Flow-Service-Quality (FSQ) Engineering for the Specification of Complex Systems." *Practical Foundations of Business System Specifications* (H. Kilov & K. Baclawski, eds.). Klewer Academic Publishers, 2003.

System of Systems Assurance Framework

Robert Ellison

Carol Woody



System of Systems Assurance Framework

Problem Addressed

Large systems and particularly systems of systems raise the importance of complexity management. The complexity is an aggregate of technology, scale, scope, operational, and organizational issues. While small system security may have been implemented by a set of point solutions that mitigated specific threats, the mitigation of threats of the magnitude and diversity of those associated with large distributed systems of systems (SoS) requires foundational support.

Separation of concerns is a powerful tactic for managing complexity during design and development. A software architecture may try to maintain separation among security, performance, reliability, and other system quality attributes. However, it is the visibility of these qualities within the operational context as the technology is used to address an organizational need that is of most interest. We frequently have maintained separation among system operations, systems development, and business operations, but that separation was often reflected by the expression "toss it over the wall." This approach worked well as long as all requirements could be effectively established in advance and evaluated prior to implementation. Business integration requirements and the appearance of technologies such as web services to support that integration for distributed systems challenge these traditional separations. Even organizations with well-established processes are finding the complexity overwhelming. A vast range of legacy technology and processes are being hooked together through bridges of software and people without a through consideration of how these connections function under stress and failure. Development is primarily looking at the individual pieces of new functionality, operations is focusing on the infrastructure, and the gray area of business process connectivity is largely ignored, exposing organizations to increased risk of operational failure.

In addition, the requirements that define the levels of consideration for security, performance, reliability, and other qualities are focused on compliance, which is open to broad interpretation by developers, resulting in wide gaps among components that must be constructed to function as a whole. Assurance is needed to have confidence through all stages of the life cycle that the development will lead to the needed operational characteristics and capabilities to establish appropriate operational capability.

This research initially focused on developing assurance analysis methods that are applicable to systems of systems to address the challenge of increased demands for interoperability, integration, and survivability. Having shown the value of the mission focus for analyzing organizational and technology dependencies, this research effort has expanded to address the need for analytical capability of services such as components of a service-oriented architecture (SOA) and the integration of these shared services with organizational mission. In addition, the consideration of quality assurance and exploration of ways in which an integrated view of mission and technology can support the development of a quality assurance case are under development.

There are many existing tools that explore parts and pieces of this problem space. The focus of this research is on building a framework, the System of Systems Assurance Framework (SoSAF), that can connect disparate segments of knowledge into a whole for management to use in decision making. Tradeoff choices must be made among qualities and residual risk needs to be identified to ensure informed management decisions. Much of the information about qualities is buried within design and development decisions and must be assembled for effective management oversight.

Research Approach

Increasingly essential work processes span multiple systems that are geographically distributed and independently managed. The individual systems are useful in their own right addressing a selected subset of organizational needs. The business demands for adaptability and integration result in a mix of systems and work processes that are constantly changing. Development is evolutionary as functions and purposes are added, removed, and modified with experience. We have what Maier characterizes as a system of systems [Maier 98]. Completion of each individual system activity is no longer sufficient to meet organizational needs, and the measures for success must focus on the complete organizational mission, which extends beyond component systems.

Consider Figure 1, where each oval represents a geographically distributed system and the blue and black lines are business processes that use those systems. The right side of the figure expands one of those systems. For a military example, an oval might be a specific Service system, and the work process might be joint activity that requires coordination across the Services. The specific Service system receives both joint and Service-specific requests. A joint Service activity would likely generate a sequence of actions similar to the actions generated for a Service-specific request.

We need to take two perspectives in analyzing that diagram: the end-to-end work process and the individual systems. The is-used-by relationship is critical for the system participants. A work process, especially in an SoS environment, could create usage patterns that were not anticipated in the design of a specific system and hence could adversely affect the operation of that system. An individual system may need to take a defensive posture with respect to external requests to protect local resources. In addition, failure of one piece will have an impact on the organizational mission that cannot be evaluated within the context of the individual component.

The success of the end-to-end work process depends on the successful composition of the individual process steps and acceptable completion of the thread. The key relationship for the work process is depends-on. We would like to assure

the end-to-end behavior of a work process, but the interoperability capabilities and failure conditions for each component could drastically affect an acceptable outcome if that step is critical to mission success and internal quality choices do not match mission quality needs. The work process thread will need to be analyzed end to end and step by step to identify gaps that could indicate insufficient assurance for quality. To do this requires the following detail process thread information: a description of work process success, expected work process quality attributes such as performance and reliability, and scenarios of both expected and unacceptable behavior, which includes the kinds of things that may go wrong and what will happen should they occur. In addition, each work process to be analyzed must be decomposed into required steps with the following types of information about each step: roles in the process, pre-conditions, functions, post-conditions, constraints, and dependencies. Each step may be composed of multiple components (human, software, system, and/or hardware) acting independently or in a coordinated manner. Initial sources for this information are found in use cases for individual components and planned operational procedures, but this content is usually idealized and does not reflect the constraints of the target operational environment. By connecting these data sources and analyzing for potential failure points, gaps and mismatches in expectations can be identified and addressed early in the development life cycle, reducing the risk of operational failure.

Systems and systems of systems can create failure states that are difficult to solve. Historically, system failure analysis has sought to identify a single root cause, but for software-intensive systems that involve human interactions a failure may be the result of multiple software, hardware, or human errors. Each error when considered individually would be perceived as minor. Other failures may arise because of emergent behavior. Each system behaves as specified, but the collective behavior is unacceptable. For example, feedback among systems might generate unexpected resource contention. At this stage, our research considers the stresses that might be induced by a work process thread. Stresses can be induced by unanticipated events, but they are often normal behaviors that can fall outside of an expected range and in such circumstances lead to failure. We initially focus on the interactions among the systems that participate in that thread and the stresses that might be induced by those interactions on the supporting systems. The stress types include

- interaction (data): missing, inconsistent, incorrect, unexpected, incomplete, unintelligible, out of date, duplicate
- resource: insufficient, unavailable, excessive, latency, inappropriate, interrupted
- people: information overload, analysis paralysis, fog of war, distraction (rubbernecking), selective focus (only looking for information for positive reinforcement), diffusion of responsibility, spurious correlations
- flexibility: dynamic changes in mission, dynamic changes in personnel, dynamic changes in configurations

The scenarios of potential quality problems, especially those with anticipated high impact, will be used to identify areas of concern to be highlighted in subsequent reviews of requirements, architecture, development, integration, certification, and accreditation to assemble an understanding of how the components are addressing needed quality and how effectively the components are working together to deliver needed quality.

The analysis framework will be applied at a specific point in time to a selected example mission thread. Since operational missions may change as an understanding of technology capability develops, it is expected that the mission thread example will be reviewed periodically to ensure consistency with operational expectations.

The elements considered by the SoSAF analysis are shown in Figure 2.

Expected Benefits

Expansion of the scope and scale of systems induces new stresses. An objective of the initial phase of this project is to identify indicators of stress that may lead to system failures. Indicators that are appropriate to the early life cycle phases of software development help to change current practice, where software failure analysis typically only concentrates on the errors that are derived from testing.

SoSAF, with its emphasis on business process threads, also enables better traceability between technology risks and business work processes. It can also enable better traceability of design decisions to the requirements of multiple organizational levels.

2008 Accomplishments

We considered integrating into the framework structure techniques already in use that examine quality and risk at various points in the life cycle. An approach to integrate software assurance cases into the framework was conceptualized and documented in a technical report, *Survivability Assurance for System of Systems* [1]. Operational mission threads provide the basis for identifying needed claims, arguments, and evidence to structure an appropriate assurance case.

In addition, an approach for integrating operational mission threads with operational security threat analysis was developed and piloted for the Electronic Systems Center Cryptologic Systems Group Network Services Division to use in evaluating the mission impact of information assurance in proposed mission changes affecting the Airborne Network.

An approach that blends SoSAF with SEI research work underway in mission assurance and interoperable acquisition to provide a multi-view decision making (MVDM) approach was evaluated in a workshop of Army program managers. The approach focuses on three risk areas inherent in the system-of-systems environment. It provides a means for program managers to consider a broad range of risks and potentially improve overall program risk response.

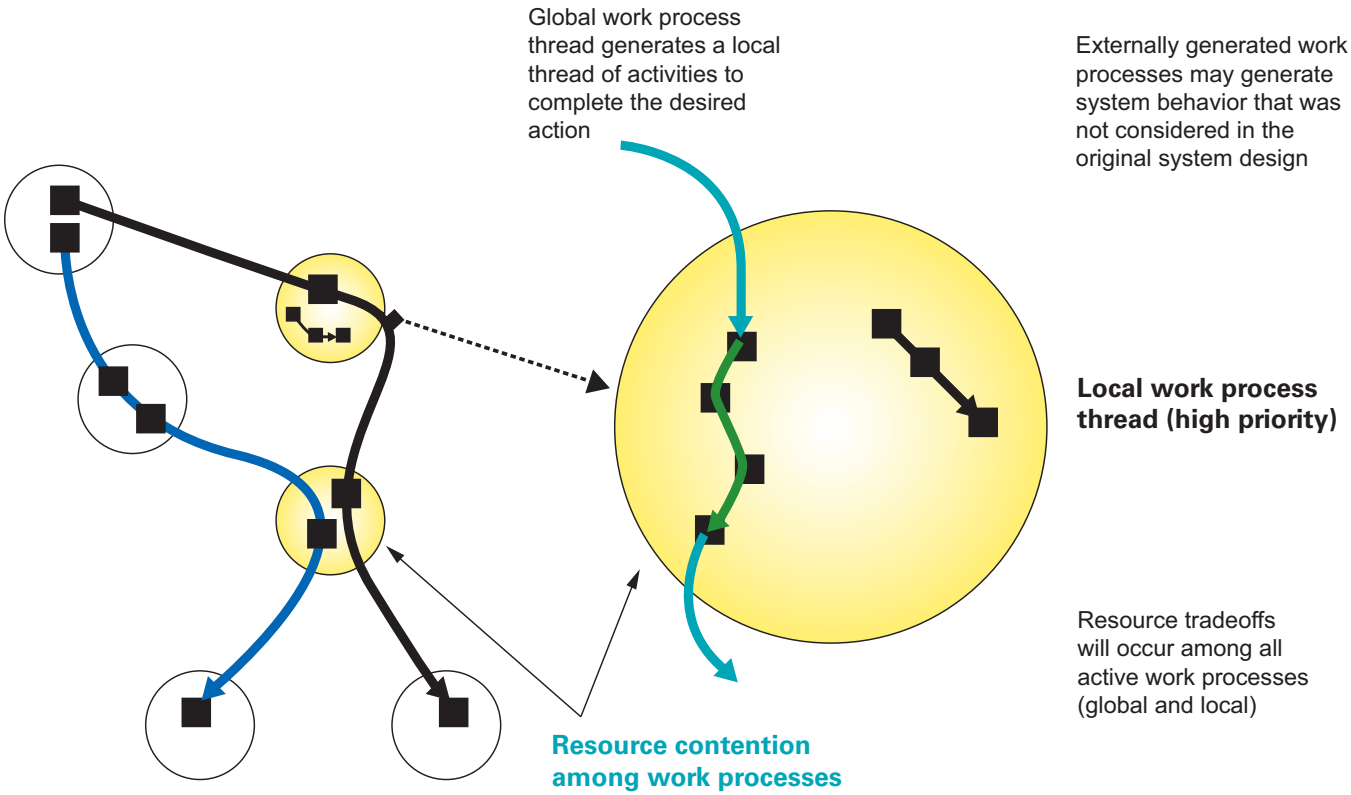


Figure 1: System of Systems Resource Contention

2009 Plans

The objective for further research is to evaluate ways in which the development of SoSAF information can contribute to an understanding of assurance for software, systems, and information and influence tradeoff decisions that impact mission quality early in the design and development processes. Pilot engagements are underway that allow the consideration of organizational and technology options early in the system development life cycle to identify ways to influence the quality tradeoff choices for appropriate consideration of assurance and realistic usage. In addition, pilot work is underway to define ways the mission analysis can be used to guide and evaluate the effectiveness of compliance and certification to meet operational capabilities.

References

Ellison, R. J., Goodenough, J., Weinstock, C., & Woody, C. *Survivability Assurance for System of Systems* (CMU/SEI-2008-TR-008, ADA482312). Carnegie Mellon University, Software Engineering Institute, 2008. http://www.sei.cmu.edu/pub/documents/08.reports/08tr008.pdf

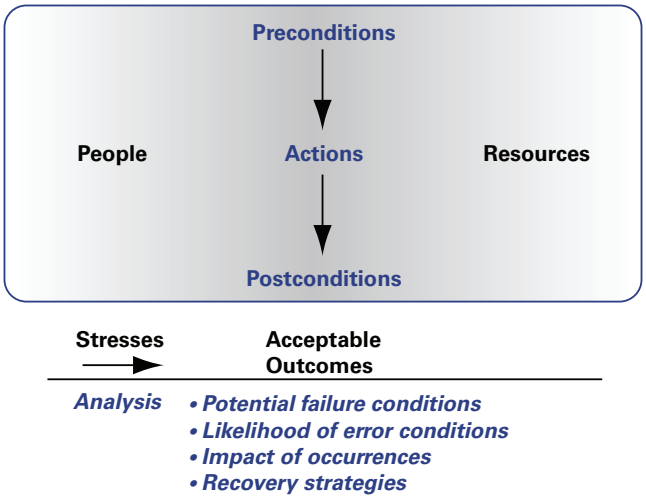


Figure 2: SoSAF Analysis

Evan Wright

Understanding Anycast Routing Behavior

Understanding Anycast Routing Behavior

Problem Addressed

Understanding routing behavior allows insight into tougher technical problems, including identifying performance problems, identifying malicious parties or the heuristics of their attack tools, improving protocols, and predicting the growth and the future of the Internet. Anycast routing has been a recent addition to the Internet to provide load balancing and fault tolerance, but anycast routing also has also impeded the ability to gain global understanding of the routing behavior of packets on the Internet.

Anycast routing is an addressing mechanism and routing technique that intentionally obfuscates global network knowledge by allowing a global destination IP address to represent any number of devices on the Internet. A router sending a packet to an anycasted destination can be expected to route to the closest device that is configured to share that anycast IP. Anycast was initially implemented in IP version 6 (IPv6), but the IP version 4 (IPv4) variant is most prevalent. IPv4 globally scoped anycast implementations include most of the DNS root servers, IPv4 to IPv6 tunnel brokers, and the AS112 initiative.

The AS112 initiative uses the anycast mechanism to allow for distributed servers to collect some of the garbage information (non-localized PTR queries for RFC1918 addresses) contributing to the excessive load on the DNS root servers [1]. This garbage information may be sensitive for certain networks. Furthermore, this information may be routed through suboptimal paths to unknown destinations, due to anycast. There is little information about what parties are receiving this data because these devices advertise themselves via anycast.

The ultimate goal of this research is to provide a way of better understanding the actual devices behind an anycast address. More specifically, this goal includes better understanding the routing behavior from various sources to anycast devices, unicast address identification of anycast devices, and quantitative assessment of the churn of anycasted devices.

Research Approach

To understand the behavior of anycast routing, the first step is to collect data that describes the routing paths from various locations to each anycast server. The type of anycast server implementation mechanism that was assessed is the AS112 servers. AS112 servers share the three IPs of 192.175.48.{1,6,42}. As of April 2008, only 54 AS112 servers are officially registered with as112.net, while active probing is able to identify an additional 8 to 15 servers.

Router-level probing tools, such as traceroute, were used to gather data from two public router sources: looking glass and route servers. Active router probing tools can determine each intermediate hop along the path and enable us to know a priori which destination is actually chosen; passive routing update analysis cannot do either. Each router performs a traceroute, sending out packets and receiving the IP address of each address along the route to the destination represented by an anycast IP address. In many cases, the IP address of the router that we are tracing from is unknown, because we may be interfacing with the router from a tool run elsewhere on the Internet. To find this IP address, the router pings some address that is running a packet sniffer. For each route historical data including the IP addresses, hostnames, and Autonomous System (AS) numbers for each router along the route. Storing the historical data is important for longer term analysis because anycast routing path repeatability is volatile, subject to other routes that it can see and how the source refers those routes.

This data was then used to reconstruct geographical routes that packets take to get to the AS112 servers by using Internet topology maps and public information provided by ISPs and AS112 server operators [2]. The last address in the route is an anycast address and not a unicast address like all others, and thus it does not uniquely identify the last hop.

We were able to identify most IP addresses by correlating data from different sources. First, we determined the AS number of the second to last hop. Then we correlated that AS number with published lists linking that AS number, as a transit AS, to a geographical position and IP address. This method has reasonable accuracy because the space of AS numbers is so much smaller than the number of unique AS112 servers.

In order to consider routing efficiency, we need to geolocate the IP address of each hop along the path from our vantage point to the AS112 node. Topology maps, ASN query services (such as Team Cymru), and hostnames that DNS servers associate with an IP address were used to geolocate an IP address. Routes were categorized as originating outside the U.S. and then coming in, originating inside the U.S. and then leaving, or exhibiting both behaviors, effectively transiting the U.S.

Expected Benefits

One benefit of this work is to identify routing inefficiencies caused by routes being anycasted. For some ISPs, AS112 traffic in Europe travels across the Pacific Ocean into the United States, then on to South America in order to be discarded. This be costly and sends traffic across core network paths unnecessarily. The simple solution is to identify poor routing practices that deploy AS112 servers on each side of such expensive links.

Creating a tool to identify the unicast IP addresses behind an anycast address would provide a new capability for network analysis. This work should serve as progress toward that goal. Such a mechanism would require an input of the anycasted IP address and would output a list of unicast IP address(es) and geolocation information that would allow researchers and operators to gain insight into their networks that was not previously available.

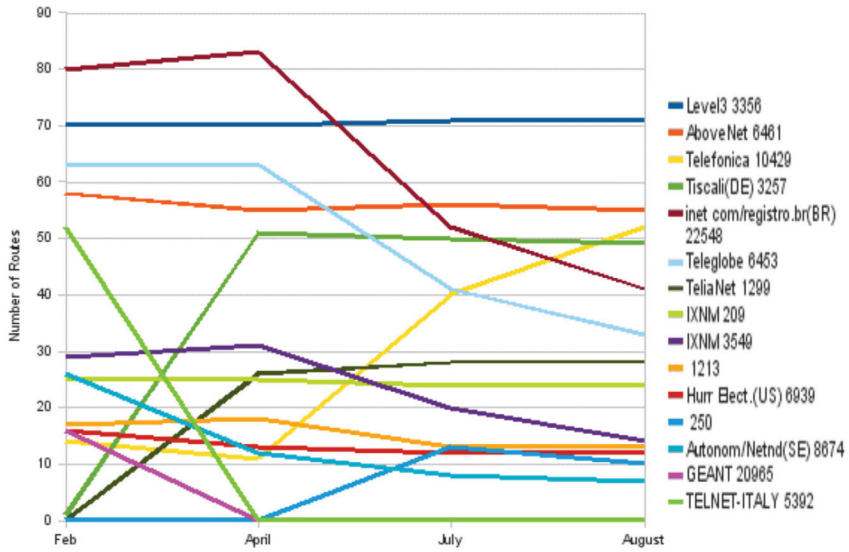


Figure 1: Routes Destined for Each ISP's AS112 Server by AS Number

2008 Accomplishments

All AS112 routing behavior exhibited one of three conditions by ISP, depending on how many AS112 servers were within the ISP's network.

- One AS112 server – All of an ISP's garbage data (and possibly some from other ISPs) went to the same AS112 server.
- Two or more AS112 servers – All the garbage data would stay within the ISP's network and would split (usually on approximate geographic lines) to go to the nearest AS112 server.
- Zero AS112 servers – The data would not only leave the network, but it would often travel great distances, possibly to the other side of the world, to be discarded by the AS112 server.

Approximately 600 different routes to AS112 servers from over 50 different ISPs were followed over the course of six months. Figure 1 shows the volume over time of the largest and most volatile routes going to each of the AS112 destinations. We are able to infer things about traffic shifts of AS112 servers from Figure 1. For example, between February and April, Telnet-Italy lost 52 routes and Tiscali gained exactly that many. Registro.br and Telefonica have complementary relationships; registro.br loses routes, Telefonica seems to gain them. Telefonica is likely the next best route after Registro.br, since both are in geographically close proximity. Also, since the volume shift is so high and complementary, we can infer that registro.br's traffic is shifting to Telefonica.

Eleven different ISPs were found to send traffic exclusively to the United States (with at least 97.3% creditability); five of these are in the United States. Nine ISPs were found to originate in the U.S., and some of their routes were destined outside the U.S. The most prominent was Telefonica, which sent 22 of 106 tested routes to Brazil. Numerous routes transit the U. S. and prefer Ashburn, VA, Miami, FL, New York, NY, and Newark, NJ, as their transit points.

Each month, between 35 and 40 different AS112 servers can be identified [2]; more are known to exist. Of routes studied in April, 36.9% were destined to an AS112 server that was not documented. The most routes went to the AS112 servers in the networks of TATA communications, cgi.br, Abovenet, Global Crossing, and Qwest, respectively. The most new routes that terminated at undocumented AS112 servers were detected in Level3, Telefonica, registro.br, Telianet, GEANT, TELNET-ITALY, and Vollmar, respectively.

2009 Plans

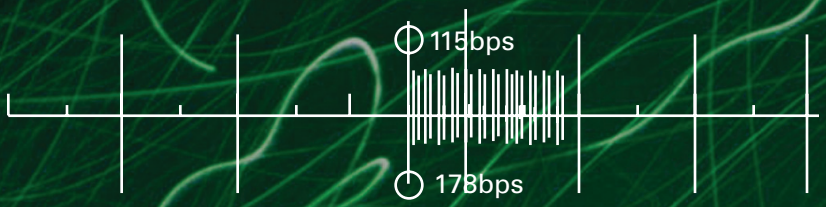
In 2009, we expect to be able to see trends over longer periods of time and to apply this technique to other research. Data from the application of this research is captured monthly so that trends of anycast characteristics can be assessed over time. The existence of the technique and tools for identifying devices behind an anycast IP address can be used toward future anycast address analysis. Specifically, IPv6 tunnels are often anycasted, and this technique allows us to learn about the actual amount and location of any number of devices that may be represented by that anycast IP address.

References

[1] Faber, S. "Leaking Private IP Information: AS112 DNS Traffic Analysis." *2007 CERT Annual Research Report*, pg. 61.

[2] "AS112 Server Operator." AS112 Project, 2008. www.as112.net/node/10

Additional Research



A Comparison of Security Policies and Security Behavior

Timothy Shimeall

In recent years, a number of models of network security behavior, referred to as "Network Reputation," have been developed. These models associate network addresses with questionable activity, such as the propagation of spam and infection with malware. The common presumption is that networks with poor network reputations are not intentionally malicious but are the result of lax security policies or practices. This article describes an initial empirical analysis of this presumption, specifically comparing the state of published security policies with observed network reputation. The benefit from this study is information on how security policies and practices interact, or fail to interact; this information may provide a perspective as to remaining work in the development of information security management.

In FY2008, the analysis began with collection of network behavior data from a large (on the order of a CIDR/8 block) network, evaluating the reputation of networks external to the collection location. From the contacting networks, a group of 300 were randomly selected from three strata: 100 exhibiting good network reputation, 100 exhibiting poor network reputation, and 100 exhibiting neutral network reputation. These networks were then distributed to 12 evaluators, who were instructed to locate and evaluate as many published network security policies associated with these networks as possible. The distribution was done in a double-blind fashion, so that neither the investigators nor the evaluators were aware of the reputation of any of these networks. The distribution was done with a fractional factorial design, so that variation within and between evaluators could be accurately assessed.

The results of the analysis showed no significant relationship between the strength of published network security policies and network reputation. Strong published policies were associated with poor, neutral, and good network reputations about equally often, and similar levels of association were observed for neutral and weak published policies. The variations between evaluators were smaller than the variations within each given level of network reputation.

There are several reasons why this result occurred: first, the published policies were typically user or data-privacy policies, rather than network operations policies. That the presence of a strong external-facing policy does not imply strong network reputation is somewhat surprising. Second, there is a systematic weakness in our understanding of the circumstances of poor network behavior. This invites further investigation of network reputation and the causal factors related to it, since even strong-policy networks may have poor network reputation. Third, commonly applied security policies, even well-written ones, are not effective in managing the operational security risks on computer networks. This invites further investigation into useful policy making for operational security. All of these issues offer investigative directions for FY2009.

Capitalizing on Parallel Forensic Image Acquisition Using the CERT Super-Parallel Investigative Disk Acquisition (SPIDA) System

Kristopher Rush and Cal Waits

Project Description

Capitalizing on our strong relationship with federal law enforcement and security agencies, the CERT Forensics team has worked with these partners to identify gap areas in existing forensic analysis tools and techniques, as well as to identify new challenges arising from emerging technologies. This process is informed by discussion with practitioners, observation of current methodologies and tools, and by our experience in support of operational missions.

As a result of our support of field operations, we have identified a unique problem set for which there currently exists no commercial or government solution. We are currently developing a unique system that enables field personnel to acquire multiple drives in parallel and have all of the digital evidence/data written to a centrally managed collection of storage devices.

The Problem

Under the current serial paradigm, field personnel acquire disk images on a one-to-one basis. For example, a law enforcement agency may send out members of its computer forensics response unit in response to a suspected computer security incident. Once on the scene the forensics unit personnel determine they need to image three 1TB drives, four 500GB drives, and two laptops with 200GB drives. Typically the target drive is imaged to a separate evidence drive. Depending on equipment and training, field personnel maybe able to have two sets of identical equipment operating simultaneously; this doubling of effort yields very little impact because of the serial nature of the current process. A 1TB drive will take approximately 6 to 8 hours to hash, another 6 to 8 hours to image, and yet another 6 to 8 hours to verify the post-image hash with the acquired image. This represents approximately 24 hours to acquire just one image. Even with a doubling of effort there are still five days of imaging. With almost 5.5TB to acquire, the forensics team is in for a long stretch.

The Solution

Our solution is to build a distributed system that enables field personnel to acquire multiple drives simultaneously. This will maximize efficiency and reduce response time. There are three components in our design: the Acquisition Drone, the Storage Drone, and the Central Controller. The ADs are attached to the suspect drive and report to the CC the size and I/O speed of the disk. The SDs are attached to the evidence drives and report similar information to the CC. The key to this system, and the focus of the research, is a smart algorithm used by the Central Controller to balance the bandwidth and disk I/O to achieve the most efficient distribution of data images across the available storage media. This capability will be unique in that it will have a minimal footprint (transferring this algorithm to embedded devices), allowing for easy transportation and field deployment. This new capability will not only reduce the resources necessary to perform an acquisition but more importantly will improve both the efficiency and speed by leveraging parallel processing combined with our developed algorithm.

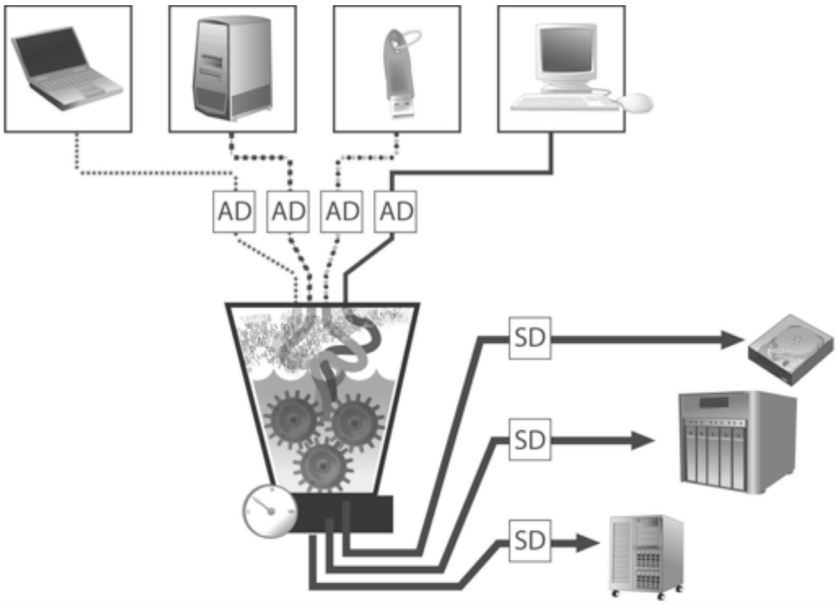


Figure 1: Super-Parallel Investigative Disk Acquisition System

Control System Security and Critical Infrastructure Survivability

Howard Lipson

The complex control systems and devices that automate operation of society's critical infrastructures, including the electric power grid, transportation, oil and natural gas, chemical plants, and manufacturing and industrial processes, are increasingly Internet-connected. Clearly, there are significant economic benefits and efficiency gains for both vendors and utilities for using common Internet-based technologies, built on open Ethernet networking protocols, as the foundation for constructing control system networks and devices. These economic benefits accrue even if such control devices are used solely on private local area networks. Furthermore, these open designs allow for the mass production of commercial off-the shelf (COTS) control system products that can be used throughout and across industry segments. While this high degree of open-standards-based connectivity brings benefits, it is accompanied by growing risks of targeted cyber attacks that could result in economic and societal consequences of substantial proportions. These attacks are literally enabled by common software vulnerabilities and the inherent susceptibility of networked systems to malicious access.

For example, the Internet and its enabling technologies are playing an increasing role in electric power systems, improving the efficiency and sophistication of business and technical operations. However, Internet connectivity also introduces significant new risks to the power grid's automated control systems and hence to the power grid itself. Moreover, the scientific and engineering foundations for secure and survivable system design must be substantially extended to address the scope and complexity of the sophisticated forms of control envisioned for next-generation energy systems. Equally important is the need for technology guidelines to ensure that engineering best practices are consistently employed during system design, development, and evolution.

By undertaking the development, procurement, and deployment of Advanced Metering Infrastructure (AMI) devices and communications networks, the electricity industry is taking the earliest evolutionary steps necessary for realizing the ultimate vision and benefits of smart grid technology. As currently envisioned, smart grid services promise unprecedented levels of automation, situational awareness, and fine-grained control of the generation, transmission, delivery, and use of electric power.

During FY2008, members of the Software Engineering Institute from CERT and the Research, Technology, and System Solutions (RTSS) program contributed expert advice and ongoing support to the Advanced Metering Infrastructure Security (AMI-SEC) Task Force,[1] which is part of the Open Smart Grid (OpenSG) Users Group. The AMI-SEC Task Force "is charged with developing security guidelines, recommendations, and best practices" for end users (i.e., utilities) and vendors of AMI technology. In particular, SEI staff has contributed to the AMI Security Acceleration Project, which also includes collaborators from Idaho National Laboratory, the Electric Power Research Institute, EnerNex, and InGuardians.

In FY2008, CERT presentations on control systems security included "Cyber Security and Survivability of Current and Future Energy Systems: Technical and Policy Challenges" (Fourth Annual Carnegie Mellon Conference on the Electricity Industry[2]) and "Towards a CERT Coordination Center for Control Systems—The Survivability Challenge" (2008 ACS Control Systems Cyber Security Conference[3]). CERT staff participated in a National SCADA Test Bed/ Sandia National Laboratories Workshop on "Cyber Attacks on Control Systems: Evaluating the Real Risk." CERT also participated in the 2008 National Institute of Standards and Technology (NIST) Workshop on Applying NIST Special Publication (SP) 800-53 (an IT cyber security standard) to Industrial Control Systems.[4] A member of CERT took part in a panel on "Responsible Vulnerability Disclosure" at the 2008 Process Control Systems Industry Conference.[5] As has been the case since 2006, CERT has continued to extend its efforts in vulnerability analysis and remediation to include control system networks and devices. A member of CERT also serves as an adjunct research faculty member at the Carnegie Mellon Electricity Industry Center.

CERT plans to continue to expand its operational and research focus on control system security engineering and critical infrastructure survivability in 2009. A primary goal is to use lessons learned from incident and vulnerability analysis to contribute to the creation and enhancement of software engineering methodologies and best practices for secure and survivable control system development, operation, and assurance. Another major objective is to continue to raise vendor and utility awareness of engineering best practices for control system security and survivability, which includes plans for further SEI contributions to the AMI-SEC Task Force in 2009.

1 http://osgug.ucaiug.org/utilisec/amisec/
2 http://www.ece.cmu.edu/~electriconf/2008/presentations1.html
3 http://realtimeacs.com/?page_id=23
4 http://csrc.nist.gov/groups/SMA/fisma/ics/events.html
5 http://www.pcsforum.org/events/2008/

Convergence of Cyber Security and Temporary Events

Samuel A. Merrell

It seems fundamental to set out to protect a mission by first recognizing what objectives must be achieved and then stepwise identifying likely threats and vulnerabilities, articulating risks, and mitigating them. The procedural requirements of such a risk process are well established, codified, tested, and trained. But when it comes to risk management related to temporary events, such as national political conventions, sporting events like the Olympic Games or the Super Bowl, and foreign State visits, there is a consistent lack of methodology to develop and deploy resilient information infrastructures.

Events such as those above have service and information resilience requirements, constraints, and priorities that are different from traditional infrastructure deployments. One such difference is the fact that these events are defined by sensitivity to time, with a set of finite operations established to support a mission that has a fixed beginning, execution, and conclusion. Another difference is related to the ownership of facilities in which these events take place, contrasted with the "owners" of the event, and the rapid deployment, use, and decommissioning of mission essential information systems. A third difference is related to the high visibility of these types of events, and the ability for potential attackers to recognize critical technologies that are in use.

CERT, in partnership with the U.S. Secret Service, created an area of research called the Critical Systems Protection Initiative (CSPI) to more fully describe the problems facing law enforcement and security operations. CSPI provides a process to identify and manage risks to temporary event information infrastructures. The goal of CSPI is to identify practical mitigation strategies that provide risk avoidance and prevention in the context of the smaller window of opportunity for threats to exploit identified vulnerabilities in the temporary event. While CSPI is extensible enough to be applied to other domains (such as CI operations or mission assurance analysis), to date its application has been most frequently used to support law enforcement. This seems valid considering that the focus of CSPI is toward information systems that have a direct impact on the physical security of event attendees, regardless of their role, including delegates, candidates, members of the media, and the general public. For instance, CERT has been developing the CSPI process through its support to such events as the 2004 Olympic Games, the 2005 U.S. Presidential Inauguration, the 2006 Asian Games, and the 2004 and 2008 Democratic and Republican National Conventions.

In 2009, CERT plans to redesign the CSPI methodology. The result will be the engineering of a process to support law-enforcement-designated special events and the maturation of cyber security risk analysis for event success and public safety. We expect to continue the maturation of event-related risk management processes and the development of training and other materials that will enable their transition.

Detecting Network Beacons

Paul Krystosek

Compromised computer systems are often found well after the fact when they exhibit unusual behavior. One significant class of compromised systems is the so-called bot that participates in a botnet, a network of compromised computers used by an attacker to launch attacks. The authors of botnet software have the experience and skill to produce malicious software (malware) that can evade detection by the user of the compromised computer. This research describes exploratory techniques to detect computers exhibiting bot-like behavior through network traffic analysis based on network flow data.

One characteristic of botnets and certain other Internet malware is the stage in their life cycle when they beacon to report their presence or "phone home" to request instructions. This often takes the form of network connections or connection attempts occurring at very regular intervals. Such regular behavior is often first seen in visualizations of network traffic such as Figure 1. An analyst can easily spot such regularity in a visualization. Unfortunately, visual inspection is not practical for high-volume traffic analysis and provides an analyst with little insight into the nature of the traffic.

This project seeks to replace the visual identification of regular traffic patterns with an algorithmic approach. Many legitimate network services operate on regular intervals that look similar to botnet traffic. A significant effort in this project involves identifying legitimate servers and removing their traffic from consideration. The core of the algorithm processes the network flow data to find regular behavior that is within certain parameters such as minimum time between transmissions and minimum number of transmissions. There is additional information that is used to identify beacons as being of particular interest. The instances of regular behavior are then summarized with noteworthy beacons flagged.

On a large network the beacon detector currently reports on hundreds of thousands of potential beacons during a given time period, typically a day. This volume makes further manual analysis impractical. The research challenge is to improve the algorithm's ability to identify compromised computers and reliably rank the activity based on the likelihood that a particular beacon corresponds to a compromised computer.

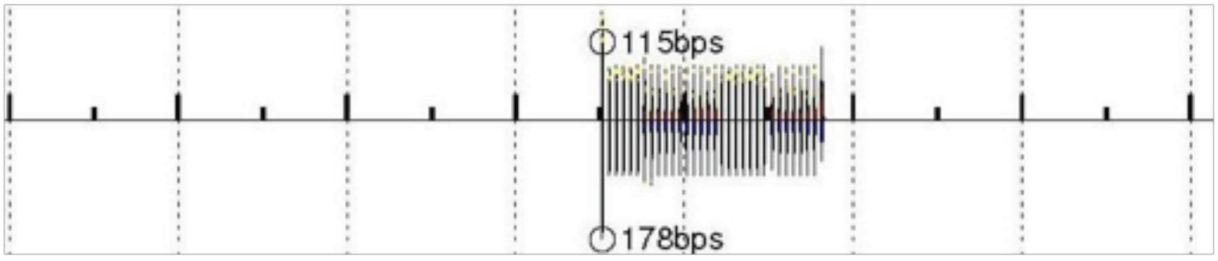


Figure 1: Example Visualization of Regular Network Behavior Likely from a Compromised Computer

Dranzer: Codifying Vulnerability Discovery Processes

William L Fithen, Art Manion, William Dormann, Daniel Plakosh, Sagar Chaki, and Arie Gurfinkel

Over our 20-year history, no concept has been more central to our mission than that of vulnerability. Our organization was born out of a handful of ARPANET vulnerabilities, and we have studied thousands since. We assert that vulnerabilities have a distinct life cycle; they are created, discovered, exploited, hidden, corrected, forgotten, and frequently recreated.

Over the last 20 years, the lion's share of attention—ours and the security industry's in general—has been directed toward correction. Today's well-known patch cycles are primarily a result of that attention. Vendors react to reports of vulnerability by correcting or hiding them (i.e., making them inaccessible) and issuing fixes or patches to their customers to remove them from deployed products. Some years ago, we drew the conclusion that this attention has not resulted in a more secure environment for users of information technology and have been exploring alternative paradigms.

To that end, we, and others, have been directing more attention toward the creation and discovery phases of the vulnerability life cycle. During the process of producing software products, engineers unintentionally create vulnerabilities that are later discovered and reported to be fixed. We hope that by paying greater attention to these phases of the life cycle, we can change the nature of the engineering process to detect and eliminate—and later avoid altogether—vulnerabilities before products ship. We expect to do this by placing knowledge, techniques, and tools in the hands of engineers to help them understand how vulnerabilities are created and discovered, with the goal of learning to avoid them.

The Dranzer project is currently being directed toward some of these goals. Dranzer is a tool used to discover certain classes of vulnerabilities in Microsoft Windows ActiveX controls. ActiveX offered us an opportunity to create a unique vulnerability discovery laboratory because of several key attributes:

1. There are thousands of ActiveX controls readily available on the Internet from a wide range of producers. These made excellent vulnerability discovery test cases.
2. ActiveX controls export self-defining APIs. This permits autonomous exploration of programming interfaces without overwhelming configuration details.
3. ActiveX controls are automatically installable. This permits the dynamic construction of the experimental environment without extensive human supervision.

In fact, it's as though ActiveX were specifically designed to support this kind of vulnerability discovery environment. This extraordinary environment has allowed us to experiment with a wide range of techniques aimed at discovering many classes of vulnerabilities. Over time, we have been able to add new techniques that were intuitive, but combinatorially intractable; we continue to focus on these types of techniques today.

We also developed an automated meta-framework that has allowed Dranzer to find some 3,000 defects in 22,000 ActiveX controls without human intervention. This framework supports incremental discovery by recognizing new controls found in the Internet and testing only those—shortening the find, download, and test cycle to the point of being operationally feasible to run every day.

With a much better understanding of vulnerability discovery, we now intend to turn our attention to other technologies, starting with those most similar to ActiveX (remote object invocation). For example, many of the SOA-like protocols incorporate some sort of XML-based remote object invocation mechanism. We believe that many of the techniques we pioneered on ActiveX will work there as well.

Today, several prominent information technology vendors are using our Dranzer tool to help discover vulnerabilities in the ActiveX controls they produce before they ship. We intend to more widely disseminate the Dranzer tool in the information technology producer community and to produce new tools and techniques aimed at technologies other than ActiveX.

Expanding the OCTAVE Method to Perform Continuous Risk Management of Information and Operational Security

Rich Caralli and Lisa Young

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) is a methodology for identifying and evaluating information security risks. It was developed and first released by CERT in 1999 as a means for helping organizations to perform information security risk assessment in the context of operational and strategic drivers that they rely on to meet their missions. The original OCTAVE method was designed for large organizations with significant hierarchies and consisted of a series of workshops conducted and facilitated by interdisciplinary analysis teams drawn from the organizations' business units. Since 1999, additional work has been done to refine and repurpose the OCTAVE method. In September 2003, OCTAVE-S was released as a means to scale the full OCTAVE methodology to smaller settings. OCTAVE-S includes more structured worksheets and guidance than the original OCTAVE method so that users can address a broader range of information security risks with which they may not be familiar. Building on the risk concepts in the OCTAVE and OCTAVE-S methods, the most recent variant is OCTAVE Allegro. The purpose of OCTAVE Allegro is to further improve risk assessment results without the need for extensive risk assessment knowledge. OCTAVE Allegro does this by focusing on how information assets are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result.

All of the current OCTAVE methods share a common limitation: they emphasize risk identification over other aspects of information security risk management such as risk analysis and mitigation. The identification of information security risk is a purposeful activity, but in the end, the analysis of risk in the context of the organization's operational and strategic demands and the proper mitigation of risk (in coordination with the organization's system of internal controls) are what ultimately improve the security of the organization's information infrastructure.

Since the release of the original OCTAVE method, the risk landscape for most organizations has changed dramatically. Foremost, the former focus on information security risk alone has expanded into a need to address *operational* security risks more broadly. Operational security risks encompass the potential threats and vulnerabilities to not only information infrastructures, but also people, broad levels of technology (software, hardware, systems, etc.), and facilities. There are several drivers for this shift, including

- the increasing complexity and convergence of information and technical and physical infrastructures
- a dramatic shift in ownership away from tangible assets to intangible (information-based) assets
- increasing levels of interconnection and interdependencies between organizations in an industry or peer group
- permeable organizational borders (brought about by outsourcing, integrated supply chains, and other external partnerships)
- increasing dependencies on public services (water, gas, power) and public-private partnerships (such as first responders)
- exposure to new and unknown risk environments (as new and innovative business strategies and markets are tapped)

In addition, as capital and human resources for security continue to decrease, organizations must become more efficient at identifying and managing risk so that it does not result in unintended consequences and interruption of mission. As a result, even regularly-scheduled and executed risk assessment activities will not suffice as a means for managing operational security risks. Instead, what is needed is a continuous risk management process that ensures that new risks are continually identified and addressed and that existing risks continue to be monitored and controlled so that they do not pose an ongoing threat to mission assurance.

Indeed, the original OCTAVE method was described as the diagnostic element of a more involved and continuous risk management process that involves planning, implementing, monitoring, and controlling. This larger *plan-do-check-act* cycle is the means by which the organization not only identifies and analyzes operational security risk but actively ensures that this risk (even when considered to be mitigated) poses minimal or manageable ongoing threat to strategic and operational drivers and organizational mission (Figure 1).

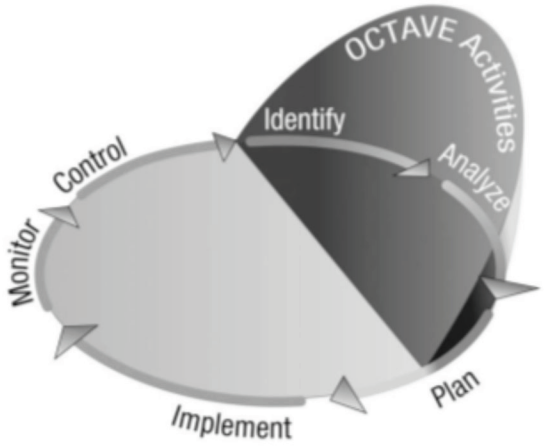


Figure 1: View of OCTAVE in Risk Management Cycle [1]

Because of the significant changes in the organizational risk environment, expansion of the OCTAVE method to address the entire risk management cycle as well as a broad range of operational assets is a necessary next step in providing organizations the tools, techniques, and methods necessary to effectively manage operational risk. Thus, CERT's current security risk management research agenda focuses on these three broad objectives:

- The extension of OCTAVE concepts to the entire operational risk management cycle.
- The definition of a continuous risk management (CRM) framework for operational security.
- The incorporation of additional asset types, such as people and facilities, into the operational risk management cycle.

Extending OCTAVE Concepts

The extension of OCTAVE concepts to the entire risk management cycle involves the development of tools, techniques, methods, and training to address all aspects of operational risk management. This includes

- identification of risk appetite and tolerance in the context of the organization's critical success factors
- development and deployment of organizationally driven risk evaluation criteria and quantitative measurements
- expansion of risk analysis tools and techniques to ensure adequate consideration of risk and consequence
- expansion of risk mitigation activities to include specific focus on the organization's internal control structure and the development of mitigation plans that strengthen and improve this structure

OCTAVE-Based CRM Framework

The development of an OCTAVE-based CRM framework for operational risk management includes the identification and codification of high-maturity practices built around the development and implementation of a *plan-do-check-act* cycle for managing operational security risk. This framework should provide the foundation for the organization's operational risk management activities and provide a roadmap for ongoing management and *improvement* of the operational risk management process.

Expansion of Asset Focus and Application of OCTAVE Method

Operational resiliency in an organization is dependent on many types of organizational assets performing together to achieve a mission. While information and technology assets are important components of operational resiliency, so are people and facilities. The expansion of the OCTAVE method (specifically OCTAVE Allegro) to address the resiliency of people and facilities is a means by which the organization can begin to expand current information security and business continuity activities toward a broader view of mission assurance and operational resiliency management. This expansion also incorporates and highlights physical security issues that are often overlooked in traditional information security risk management. This is especially important as we explore the use and expansion of the OCTAVE method as a primary tool for identifying, analyzing, and mitigating risk in critical infrastructures.

References

[1] Alberts, C. J. & Dorofee, A. J. *OCTAVE Criteria, Version 2.0* (CMU/SEI-2001-TR-016, ADA399229). Software Engineering Institute, Carnegie Mellon University, 2001. http://www.sei.cmu.edu/pub/documents/01.reports/pdf/01tr016.pdf

Malware Clustering Based on Entry Points

Cory F. Cohen and Jeffrey S. Havrilla

Substantial effort is duplicated reanalyzing malicious code that has already been looked at by someone else (or even the same person). One way to leverage existing analysis and reduce duplication of effort is by grouping similar and identical programs into clusters. One approach to reducing this problem uses a custom-built signature database based on program entry points.[1] The primary purpose of this database is to identify the packing technology used by attackers to compress and obfuscate malware. Identifying the packer in an automated way enables large-scale analysis and reduces individual analysis time by a human.

We begin by extracting the first instructions run by a program (those at the program entry point) from a large corpus of malware. These entry points are analyzed to identify patterns and generate signatures used to cluster programs. Using this technique, we're able to automatically generate signatures for many common packers and even some malware families.

Automated generation of signatures greatly reduces the human effort required to cluster similar malware. Unlike manual signature generation, where the quality of the signatures degrades due to constraints on human analytical effort as the size of the corpus grows, automatically generated signatures actually improve. Automatically generating signatures can also detect new packers that have not yet been identified by human analysts, helping to detect emerging threats. In several cases, we generated signatures for packers and malware families not currently detected by antivirus products.

The standardization and transparency of the process yields several benefits. The simplicity and consistency of the methodology allows human analysts to easily verify the correctness of the results, unlike proprietary methods which are often secret and hide the common features of the files matched by the signature. Standardization also allows analysts to gain insights into malware that is not matched by any signature, since the automated process would have found a signature if one existed.

The large-scale automated clustering approach allows us to identify trends in packer development, prioritize our responses, and in turn develop techniques used to combat malicious code circulating on the Internet. We plan to build on this success by applying similar techniques to other code attributes in malware. Clustering based on these attributes may allow us to identify not only the most prevalent packers in a malicious code collection but important clusters of unpacked malware as well.

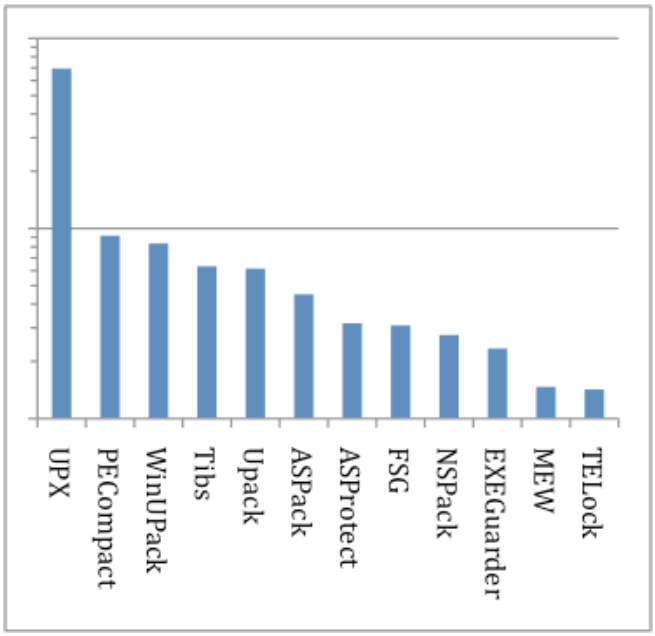


Figure 1: Prevalence of Several Common Packers in the Corpus Based on Entry Point Signatures Using a Logarithmic Scale

1 We named this signature database and the corresponding tool "Pithos."

Malware Detection Through Network Behavior

Sidney Faber

Many innovative approaches have been introduced in the fight against malware. A new and important approach currently under development involves building a better understanding of network behavior generated by malware and using that behavioral model to locate previously undetected malware.

The network traffic of an infected workstation often reveals the common stages of infection exhibited by malware, such as initial infection, communications via a command and control (C2) channel, and a migration between controlling hosts. Each stage often has multiple phases, and each phase presents a unique network behavior. For example, infection through a drive-by download and subsequent downloader installation presents a well-defined sequence of network events. When malware communicates on a C2 channel to an idle controller, the malware often uses very periodic and consistently sized beacons, which can be identified within other routine traffic.

Initial results have shown this method to be very effective at expanding lists of known C2 servers. Infected machines and well-defined network behaviors can be cataloged by watching traffic to known C2 servers. Then, when an infected machine ceases communicating with the known C2 server, a close examination of network traffic often reveals behavior showing that the machine has been migrated to a previously unknown C2 server.

Future plans include formalizing the methods for C2 server expansion to map out malware networks. In addition, behavioral analysis will define more features of network behavior that can be applied to malware artifacts to identify infected machines.

Scan Characterization

John Truelove and Markus De Shon

There are good techniques available for detecting scanning on the Internet [1,2]. Secondary analysis of scanning activity to detect trends in technique and to group scans by their similarities is less developed, or focuses primarily on scans to blackhole networks, though notable exceptions exist [3].

The CERT Network Situational Awareness group has done some initial analysis of a repository of scan data of a large live network. We found that, predictably, scan volumes (number of connection attempts) favor common service ports (HTTP, SSH, web proxy, SMTP). However, when ranking by the unique number of hosts scanning a particular port, certain uncommon port numbers have been very prominent over the last year (1755, 29696, 4663, 13666). Another interesting feature is that while it is common for an attacker to scan a single port (across many hosts), scans of two or three ports are rare. Scanning four or more ports is again common, with a slow decrease thereafter in frequency as the number of scanned ports increases.

Future work will focus on exploring distinguishing features of scans in order to cluster scanners by common characteristics, indicating usage of a common tool or technique. Depending on the rarity of the particular combination of characteristics, such clustering, combined with other information, may assist in attribution of scanning activity.

References

[1] Jung, J., Paxson, V., Berger, H. W., & Balakrishnan, H. "Fast Portscan Detection Using Sequential Hypothesis Testing." *Proceedings of the IEEE Symposium on Security and Privacy*, 2004.

[2] Gates, C., McNutt, J., Kadane, J. & Kellner, M. *Detecting Scans at the ISP Level* (CMU/SEI-2006-TR-005, ADA448156). Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tr005.pdf

[3] Allman, M., Paxson, V., & Terrell, J. "A Brief History of Scanning," 77–82. *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement.* ACM, 2007. DOI= http://doi.acm.org/10.1145/1298306.1298316

Sufficiency of Critical Infrastructure Protection

Samuel A. Merrell, James F. Stevens, and Bradford J. Willke

On January 17, 2008, the Federal Energy Regulatory Commission (FERC) took a number of steps to increase the level of cyber security and reliability of the Bulk Electric System (BES). FERC mandated compliance with the eight Critical Infrastructure Protection (CIP) Reliability Standards developed by the North American Electric Reliability Corporation (NERC) and set a 2010 deadline for auditable compliance. While most agree that these standards are certainly a step in the right direction, others argue the standards do not go far enough in addressing the need for increased security in the BES—even when including the changes mandated by the FERC. The net problem at hand is determining what constitutes sufficiency and, secondarily, what is acceptable as evidence of sufficiency claims.

The answer is neither straightforward nor easily validated without understanding what assurances are needed for BES reliability and what assurances are provided by these standards. One thing is certain, if the practices and processes proscribed are insufficient for ensuring the reliability of the BES, owners and operators will have expended already limited resources for compliance and will have received no reward, such as increased risk tolerance and resiliency.

Many perspectives exist in the promotion and validation of sufficiency claims. BES owners and operators generate and deliver electricity within the confines of unique sets of operating conditions, goals, objectives, levels of capability, and resources. They have operational risks that they must manage in order to meet their organizational missions, and those risks are a factor in the sufficiency of protection as they define it. In addition, regulators, trade associations, consortia, and others who have a significant stake in the resiliency of the BES bring different perspectives to the issue. These stakeholders have set different risk tolerances for information security concerns facing the BES and may have contrasting beliefs as to what constitutes sufficient risk management.

These contrasting perspectives can be seen in the ongoing debate on the sufficiency of the NERC CIP Reliability Standards. Assured reliability requires the CIP Reliability Standards to eliminate this tug-of-war and achieve the needs of operational risk management at a shared, community level *and* at an individual operator level.

The BES subsector is not alone in questioning the sufficiency of security for critical infrastructures. This same problem manifests itself in a number of other critical infrastructure sectors, especially where there is a diverse collection of interconnected stakeholders. In these cases, decisions made by individual organizations can have significant impacts on the resiliency (a measure of security, continuity, and reliability) of the entire sector. Thus, managing the risks to a sector requires a governance and policy structure that is flexible enough to understand the security posture of the individual asset owners and operators without creating an undue burden of effort for compliance.

In 2008, CERT began to explore the use of assurance cases as a tool for communicating governance and policy issues related to the cyber security risk management and the security posture of critical infrastructure owners and operators. An assurance case is a methodological way of demonstrating how arguments and evidence support an articulated claim. Our first dataset for arguments and evidence came from our analysis of sufficiency standards related to the BES.

In 2009, we plan to further explore the use of analytical methods and representations, like assurance cases, to frame critical infrastructure protection requirements and to analyze shared operational risks. At a minimum, CERT plans to leverage the utility of assurance cases for further exploration in the bulk electric sector and other applicable sectors. Some specific objectives include identifying potential design/assurance patterns that can be leveraged across sectors and further examination of regulatory standards.

Toward an Integrated Network Inventory Model

Timothy J. Shimeall

The purpose of the service inventory process is to produce a list of addresses (on a given network) for hosts that provide any of an explicitly identified set of services during a specified time interval. The method behind this is to use a mix of behavioral (flow-based) and administrative (network-service based) information. The result, then, is a confidence-annotated list of addresses for hosts that exhibit behavior associated with any of the desired services during the specified interval and that have administrative information indicative of providing said service. The integrated inventory model supports rapid deployment, rapid extension to the collection of services of interest, and validation of the methods and its results—both from a software engineering sense of validation and a utility sense of validation.

The integrated inventory model assumes that one can describe the network flows that characterize each service of interest either in a port-specific approach (assuming that TCP or UDP ports are accurately associated with the services of interest), or in a port-agnostic approach (assuming that there are characteristic patterns of flows for the services of interest), or both (i.e., to reduce false positives). As the inventory models are employed for a given organization, cumulative results may lead to lists of already-identified servers, further reducing false positive or false negative results from the inventory process.

The resultant process would have several phases. Phase 1 produces a set of flows that meet the criteria associated with each service of interest. Phase 2 retrieves any available administrative information (e.g., DNS query results) that may indicate the service of interest and increases the confidence of any server tentatively identified by Phase 1. Phase 3 compares the volume of flows associated with a service against the total volume of flows involving each server, increasing the confidence of any server that has a large fraction of its flows involving the services of interest. Phase 4 is a service-specific phase in which behavioral models (e.g., client-service, peer-to-peer, and distributed) are applied to determine if the overall patterns of flows match the expectations for the services of interest.

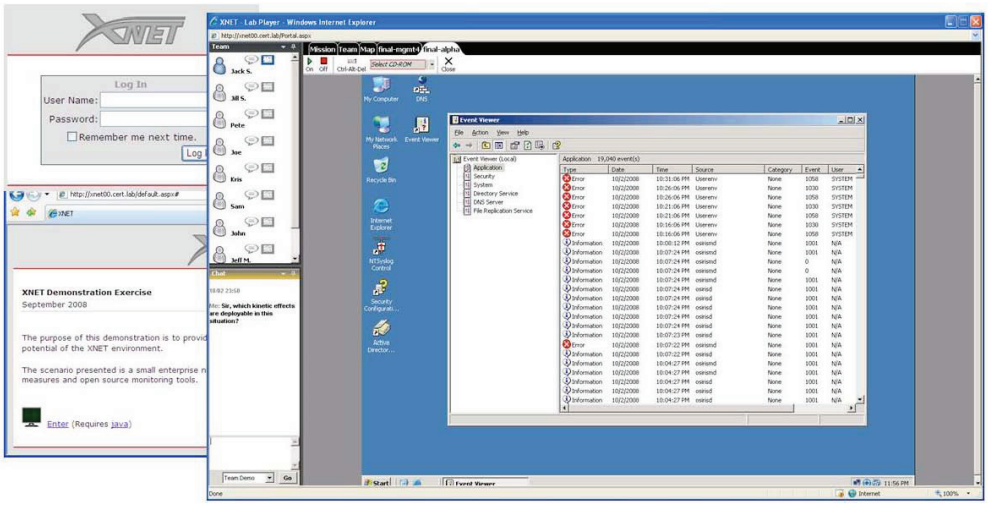
The results of this process allow for efficient identification across a mix of services of interest. This would facilitate both identification of potential unapproved ("rogue") servers and identification of servers that support multiple critical services. The rogue servers can be prioritized for investigation leading either to approval or shut-down. The multi-service servers can be prioritized for defense or for diversification to improve network robustness.

During FY2008, the above integrated model was developed by abstraction from existing inventory models. During FY2009, the researchers plan to implement the integrated model and apply it to several networks. This effort may, in turn, lead to improved defensive modeling for the networks.

Train as You Fight: A Practical Approach for Preparing the Cyber Warrior

Jeffrey Mattson and Chris May

For military units, the best training approaches tend to be realistic exercises specifically designed to hone the skills required for combat operations. "Live-fire" exercises that attempt to replicate real-world cyber attack, defend, and respond missions embody this "train as you fight" goal. Because developing, organizing, and administering these events pose many challenges, exercises are generally relegated to infrequent, large-scale events. This research addresses the current lack of a robust, on-demand, exercise training capability at the small team or unit level. For exercise training and evaluation to be effective, it needs to be realistic, focused on objectives, efficient to administer, and simple to access. CERT's Exercise Network (XNET) is developing in light of these goals.



The impetus for XNET is to free trainers from the resource intensive tasks of building, deploying, and administering the training environment, thereby enabling them to focus on the training objectives. Toward that end, XNET provides an exercise control console that provides simple deployment of network resources for multiple teams. Through this console, trainers select a scenario infrastructure—a logical grouping of virtual machine templates—and applies it to one or more physical hosts running a VMware virtualization product. It leverages the VMware Virtual Infrastructure Management (VIM) web service API to dynamically create, provision, snapshot, and power-on the machines comprising the scenario. The virtual disk images can reside in a common storage location, either a network file system (NFS) share or a virtual machine file system (VMFS) volume. So when trainers deploy the same scenario for multiple teams, like machines all draw from the same base disk and make disk-writes to a local, differential file. Not only does this provide a smaller storage footprint, but it also speeds scenario deployment and allows for efficient alteration and updating of the virtual machines.

Relieved from the administrative burden of instantiating the scenario infrastructure, the trainer can focus on shaping the scenario to cover specific training objectives while monitoring and evaluating exercise participants' actions. Accordingly, the trainer will overlay an exercise timeline with events that will trigger a training or evaluation response, and those events will be executed automatically according to the schedule. To accomplish this, XNET's event engine queries a database of scheduled events, built from a library of event templates, and initiates tasks that are due. It uses the VMware guest tools service to interact with virtual machines and start and stop processes within the specified system.

XNET also provides a simple access strategy for participants, which complements the administrative ease of establishing an exercise. Specifically, in order to bring participants into the same virtual environment regardless of their physical location, XNET merely requires a client web browser that will accept signed applets. After participants authenticate via the browser, XNET returns to them a Remote Desktop Protocol (RDP) Java applet that targets an exercise host. The RDP connection into the XNET environment is a "channel-less" session; only the bitmap screen images are passed out of the exercise environment and rendered by the applet in the browser window. This provides isolation between the participant's local network and the exercise network, preventing any bleed-over of malicious traffic. Furthermore, the RDP session is, by default, wrapped in an SSL tunnel for additional security.

Rather than providing exercise participants with a traditional Windows desktop, users log directly into an XNET portal application. The XNET portal is a terminal services shell application that provides team collaboration, trainer interaction, and scenario infrastructure access. All instances of the portal application are connected by a multicast communications channel, providing a messaging mechanism for teams. Teams communicate as necessary by using a text chat client, a shared marker-board, and a desktop-sharing client. Using these tools, team members interact with each other as if they were in the same physical room. They even have the ability to "look over another teammate's shoulder" by viewing or requesting control of their active system. Additionally, a graphical network diagram provides an intuitive interface for working with computers in the exercise. For example, clicking a computer on this topology map launches a connection to the computer's VMware host, which facilitates the keyboard, mouse, and screen of the console session.

CERT's Workforce Development team is currently engaged in pilot exercises with U.S. Department of Defense organizations. They are exploring several usage models, including hosting a centralized exercise network and distributing an XNET appliance for use at the unit. For more information, email xnet-info@cert.org.

Researcher Activities

List of Selected Publications

Books

Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Mead, N. R. *Software Security Engineering: A Guide for Project Managers.* Addison-Wesley, 2008 (ISBN 978-0-321-50917-8). J. Allen also published four articles in various publications and three podcasts to help promote the book.

Seacord, Robert C. *The CERT C Secure Coding Standard*. Addison-Wesley, 2008.

Book Chapters and Sections

Lipson, H., Goodenough, J., & Weinstock, C. Section 2.4, "How to Assert and Specify Desired Security Properties," 61–70. *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley, 2008.

Mead, N. R. Ch. 2.20, "Identifying Security Requirements Using the Security Quality Requirements Engineering (SQUARE) Method," 943–963. *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications.* Edited by Hamid Nemati. IGI Global, 2007.

Mead, N. R. & Shoemaker, D. Ch. VI, "Novel Methods of Incorporating Security Requirements Engineering into Software Engineering Courses and Curricula," 98–113. *Software Engineering: Effective Teaching and Learning Approaches and Practices.* Edited by Ellis, Demurjian, & Naveda. IGI Global, 2008.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. "The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures," in *Insider Attack and Cyber Security: Beyond the Hacker*. Edited by S. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Sinclair, S. W. Smith, and S. Hershkop. Springer Science + Business Media, LLC, 2008.

Peterson, G. & Lipson, H. Section 6.3.1, "Web Services: Functional Perspective" and Section 6.3.2, "Web Services: Attacker's Perspective," 190–196. *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley, 2008.

Reports

Cappelli, D. M., Moore, A. P., Shimeall, T. J., & Trzeciak, R. F. *Common Sense Guide to Prevention and Detection of Insider Threats: 3rd Edition*. Report of Carnegie Mellon University, CyLab, and the Internet Security Alliance, Sept. 2008 (update of earlier editions).

Caralli, R. *CERT Code of Practices Crosswalk*. Software Engineering Institute, Carnegie Mellon University, Sept. 2008. http://www.cert.org/resiliency_engineering/framework.html

Caralli, R. *CERT Resiliency Engineering Framework*, Preview Version, v0.95R. Software Engineering Institute, Carnegie Mellon University, March 2008. http://www.cert.org/resiliency_engineering/framework.html

Ellison, R. J., Goodenough, J., Weinstock, C., & Woody, C. *Survivability Assurance for System of Systems* (CMU/SEI-2008-TR-008). Software Engineering Institute, Carnegie Mellon University, May 2008.

Gayash, A., Viswanathan, V., & Padmanabhan, D.; Advisor Mead, N. R. *SQUARE-Lite: Case Study on VADSoft Project* (CMU/SEI-2008-SR-017). Software Engineering Institute, Carnegie Mellon University, June 2008.

Mead, N. R., Viswanathan, V., Padmanabhan, D., & Raveendran, A. *Incorporating Security Quality Requirements Engineering (SQUARE) into Standard Life-Cycle Models* (CMU/SEI-2008-TN-006). Software Engineering Institute, Carnegie Mellon University, May 2008.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures* (CMU/SEI-2008-TR-009, ADA482311). Software Engineering Institute, Carnegie Mellon University, 2008. http://www.sei.cmu.edu/pub/documents/08.reports/08tr009.pdf

Papers

Allen, J. H. "Making Business Based Security Investment Decisions – A Dashboard Approach," Department of Homeland Security Build Security In website, September 2008.

Allen, J. H. Guest contributor, "Mastering the Risk/Reward Equation: Optimizing Information Risks while Maximizing Business Innovation Rewards." RSA, August 2008.

Blosser, G. & Zhan, J. "Privacy-Preserving Collaborative E-Voting." Workshop on Social Computing, Taipei, Taiwan, 2008.

Blosser, G. & Zhan, J. "Privacy-Preserving Collaborative Social Networks," 543–548. *Proceedings of the Second International Conference on Information Security and Assurance*, Busan, Korea. IEEE Computer Society, 2008.

Burch, H., Manion, A., & Ito, Y. "Vulnerability Response Decision Assistance," 2008. http://www.cert.org/archive/pdf/VRDA-2008.pdf

Burns, L. & Daly, T. "FXplorer: Exploration of Software Behavior—A New Approach to Understanding and Verification," 1–10. *Proceedings of Hawaii International Conference on System Sciences (HICSS-42)*. IEEE Computer Society Press, 2009.

Collins, M., Shimeall, T. J., Faber, S., Janies, J., Weaver, R., & De Shon, M. "Predicting Future Botnet Addresses with Uncleanliness," 93–104. *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement* (IMC 2007), San Diego, Calif. ACM, 2007.

Gurfinkel, A. & Chaki, S. "Combining Predicate and Numeric Abstraction for Software Model Checking," 127–135. *2008 Formal Methods in Computer Aided Design*, Portland, Ore. IEEE Computer Society, 2008.

Hissam, S. A., Moreno, G. A., Plakosh, D., Savo, I., & Stelmarczyk, M. "Predicting the Behavior of a Highly Configurable Component Based Real-Time System," 57–68. *20th Euromicro Conference on Real-Time Systems (ECRTS '08)*, Prague, 2008.

Hsieh, C., Zhan, J., Zeng, D., & Wang, F. "Preserving Privacy in Joining Recommender Systems," 561–566. *Proceedings of the Second International Conference on Information Security and Assurance*, Busan, Korea. IEEE Computer Society, 2008.

Hsu, C., Zhan, J., Fang, W., & Ma, J. "Towards Improving QoS-Guided Scheduling in Grids." *The 3rd ChinaGrid Annual Conference* (ChinaGrid 2008), Dunhuang, Gansu, China. IEEE Computer Society, 2008.

Klein, M., Moreno, G. A., Parkes, D. C., Plakosh, D., Seuken, S., & Wallnau, K. C. "Handling Interdependent Values in an Auction Mechanism for Bandwidth Allocation in Tactical Data Networks," 73–78. NetEcon '08, Seattle, Wa. http://conferences.sigcomm.org/sigcomm/2008 /workshops/netecon/

Lipson, H. & Van Wyk, K. "Application Firewalls and Proxies—Introduction and Concept of Operations." Department of Homeland Security Build Security In website, Revised Sept. 2008. https://buildsecurityin.us-cert.gov/daisy/bsi /articles/best-practices/assembly/30-BSI.html

Lipson, H. & Weinstock, C. "Evidence of Assurance: Laying the Foundation for a Credible Security Case." Department of Homeland Security Build Security In website, May 2008. https://buildsecurityin.us-cert.gov/daisy/bsi/articles /knowledge/assurance/973-BSI.html

Mead, N. R. "Software Engineering Education: How Far We've Come and How Far We Have To Go," 18–22. *Proceedings, 21st Conference on Software Engineering Education & Training (CSEET'08)*, Charleston, S.C. IEEE Computer Society, 2008.

Mead, N. R., Shoemaker, D., Drommi, A., & Ingalsbe, J. "An Immersion Program to Help Students Understand the Impact of Cross Cultural Differences in Software Engineering Work," 455–459. *32nd Annual IEEE International Computer Software and Applications Conference (COMPSAC 2008)*, Turku, Finland. IEEE Computer Society, 2008.

Mead, N. R., Viswanathan, V., & Padmanabhan, D. "Incorporating Security Requirements Engineering into the Dynamic Systems Development Method," 949–954. *International Workshop on Security and Software Engineering at COMPSAC 2008*, Turku, Finland. IEEE Computer Society, 2008.

Mead, N. R., Viswanathan, V., & Zhan, J. "Incorporating Security Requirements Engineering into the Rational Unified Process," 537–542. *Proceedings of the Second International Conference on Information Security and Assurance (ISA)*, Busan, Korea. IEEE Computer Society, 2008.

Park, H. & Zhan, J. "Privacy-Preserving SQL Queries," 549–554. *Proceedings of the Second International Conference on Information Security and Assurance*, Busan, Korea. IEEE Computer Society, 2008.

Park, H., Lee, D., & Zhan, J. "Attribute-Based Access Control Using Combined Authentication Technologies." *IEEE International Conference on Granular Computing*, Hangzhou, China. IEEE Computer Society, 2008.

Park, H., Zhan, J., & Lee, D. "Privacy-Aware Access Control Through Negotiation in Daily Life Service." Workshop on Social Computing, Taipei, Taiwan, 2008.

Park, H., Zhan, J., Blosser, G., & Lee, D. "Efficient Keyword Index Search over Encrypted Data of Groups," 225–229. *IEEE International Conference on Intelligence and Security Informatics*, Taipei, Taiwan, 2008.

Plakosh, D., Klein, M., & Wallnau, K. C. "Mechanism Design for Sensor Fusion: Tactical Networks as a Foil for Ultra-Large Scale Systems," 53–56. *Proceedings of the 2nd International Workshop on Ultra-Large-Scale Software-Intensive Systems 2008*, Leipzig, Germany. International Conference on Software Engineering archive, 2008.

Prakobphol, K. & Zhan, J. "A Novel Outlier Detection Scheme for Network Intrusion Detection Systems," 555–560 (Best Session Paper). *Proceedings of the Second International Conference on Information Security and Assurance*, Busan, Korea. IEEE Computer Society, 2008.

Shen, C., Zhan, J., Hsu, T., Liau, C., & Wang, D. "Scalar Product-Based Secure Two Party Computation." *IEEE International Conference on Granular Computing*, Hangzhou, China. IEEE Computer Society, 2008.

Shoemaker, D., Drommi, A., Ingalsbe, J., & Mead, N. R. "Integrating Secure Software Assurance Content with SE2004 Recommendations," 59–66. *Proceedings, 21st Conference on Software Engineering Education & Training (CSEET'08)*, Charleston, S.C. IEEE Computer Society, 2008.

Singh, L. & Zhan, J. "Measuring Topological Anonymity in Social Networks." IEEE International Conference on Granular Computing, Silicon Valley, Calif., Nov. 2007.

Walton, G., Longstaff, T., & Linger, R. "Computational Security Attributes." *Proceedings of Hawaii International Conference on System Sciences (HICSS-42)*. IEEE Computer Society Press, 2009.

Wang, I., Shen, C., & Zhan, J. "Towards Empirical Aspect of Secure Scalar Product Protocol," 573–578. *Proceedings of the Second International Conference on Information Security and Assurance*, Bushan, Korea. IEEE Computer Society, 2008.

Wang, J., Zhan, J., & Zhang, J. "Towards Real-time Performance of Data Value Hiding for Frequent Data Updates." *IEEE International Conference on Granular Computing*, Hangzhou, China. IEEE Computer Society, 2008.

Wright, E. "Investigating AS112 Routing and New Server Discovery." *2008 OARC Workshop.* Ottawa, Canada, Sept. 2008. https://www.dns-oarc.net/files/workshop-2008 /wright.pdf

Xu, X. & Zhan, J. "Dynamic Evolution Systems and Applications in Intrusion Detection Systems," 567–572. *Proceedings of the Second International Conference on Information Security and Assurance*, Busan, Korea. IEEE Computer Society, 2008.

Xu, X., Zhan, J., & Zhu, H. "Using Social Networks to Organize Researcher Community." Workshop on Social Computing, Taipei, Taiwan, 2008.

Zhan, J. "The Economics of Privacy: People, Policy and Technology," 579–584. *Proceedings of the Second International Conference on Information Security and Assurance*, Busan, Korea. IEEE Computer Society, 2008.

Zhan, J. & Lin, T. "Granular Computing in Privacy-Preserving Data Mining" (Invited Speech). *IEEE International Conference on Granular Computing*, Hangzhou, China. IEEE Computer Society, 2008.

Zhan, J., Blosser, G., Yang, C., & Singh, L. "Privacy-Preserving Collaborative Social Networks." Pacific Asia Workshop on Intelligence and Security Informatics, Taipei, Taiwan, 2008.

Zhan, J., Cheng, I., Hsieh, C., Hsu, T., Liau, C., & Wang, D. "Towards Efficient Privacy-Preserving Collaborative Recommender Systems." *IEEE International Conference on Granular Computing*, Hangzhou, China. IEEE Computer Society, 2008.

Journal Articles

Caulkins, J., Hough, E. D., Mead, N. R., & Osman, H. "Optimizing Investments in Security Countermeasures: A Practical Tool for Fixed Budgets." *IEEE Security & Privacy 24,* 5 (Sept./Oct. 2007): 24–27.

Chaki, S. & Strichman, O. "Three Optimizations for Assume-Guarantee Reasoning with L*." *Formal Methods in System Design 32*, 3 (2008): 267–284.

Chechik, M. & Gurfinkel, A. "A Framework for Counterexample Generation and Exploration." *International Journal on Software Tools for Technology Transfer 9*, 5–6 (Oct. 2007): 429–445.

Collins, R., Hevner, A., Linger, R., & Walton, G. "The Impacts of Function Extraction Technology on Program Comprehension: A Controlled Experiment." *Journal of Information & Software Technology 50* (2008).

Greitzer, F., Moore, A. P., Cappelli, D. M., Andrews, D., Carroll, L., & Hull, T. "Combating the Insider Cyber Threat." *IEEE Security & Privacy 25*, 1 (Jan./Feb. 2008): 61–64. http://www.cert.org/archive/pdf/combatthreat0408.pdf

Hevner, A., Pleszkoch, M., & Linger, R. "Introducing Function Extraction into Software Testing." *The Data Base for Advances in Information Systems: Special Issue on Software Systems Testing.* ACM SIGMIS, 2008.

Ingalsbe, J. A., Kunimatsu, L., Baeten, T., & Mead, N. R. "Threat Modeling: Diving into the Deep End." *IEEE Software 25*, 1 (Jan./Feb. 2008): 28–34.

Mead, N. R., Shoemaker, D., & Ingalsbe, J. "Integrating Software Assurance Knowledge into Conventional Curricula." *CrossTalk 21*, 1 (Jan. 2008): 16–20.

Mead, N. R., Viswanathan, V., & Zhan, J. (invited paper). "Incorporating Security Requirements Engineering into Standard Lifecycle Processes." *IJSIA 2,* 4 (Oct. 2008): 67–80.

Merrell, S. A. & Stevens, J. F. "Improving the Vulnerability Management Process." *EDPACS 38*, 1 (July 2008): 13–22.

Weaver, R. "Parameters, Predictions, and Evidence in Computational Modeling: A Statistical View Informed by ACT-R." *Cognitive Science 32*, 8 (2008): 1349–1375.

Zhan, J. "Privacy-Preserving Collaborative Data Mining." *IEEE Computational Intelligence Magazine 3*, 2 (May 2008): 31–41.

Talks/Panels/Workshops

Alberts, C., Smith II, J., & Woody, C. "Multi-View Decision Making Workshop" (workshop blending MOSAIC, SoSAF, and Interoperable Acquisition and Programmatics), Army Senior Leadership Program, July 2008.

Allen, J. H. "Build Security In: Software (not Information) Security," ISACA Security Management Conference, Winnipeg, Canada, Nov. 2007.

Allen, J. H. "Characteristics of Effective Security Governance," Fifth Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective, University of Maryland, May 2008.

Allen, J. H. "Characteristics of Effective Security Governance," International Association of Privacy Professionals e-Symposium, June 2008.

Allen, J. H. "Characteristics of Effective Security Governance," Q-CERT Information Security Forum, Feb. 2008.

Allen, J. H. "Governing for Enterprise Security Implementation Guide," ISACA Security Management Conference, Winnipeg, Canada, Nov. 2007.

Allen, J. H. "Making Business-Based Security Investment Decisions – A Dashboard Approach," Making the Business Case for Software Assurance Workshop, Carnegie Mellon University, Sept. 2008.

Allen, J. H. Recorded and published 26 new podcasts as part of CERT's Podcast Series: Security for Business Leaders.

Cappelli, D. M. "CERT Insider Threat Research," Deloitte & Touche, Pittsburgh, Pa., June 2008.

Cappelli, D. M. "CERT Insider Threat Research," Fidelity, July 2008.

Cappelli, D. M. "CERT Insider Threat Research," Idaho National Laboratories, Idaho, Sept. 2008.

Cappelli, D. M. "CERT Insider Threat Research," Infosec Research Council, Washington, D.C., Nov. 2008.

Cappelli, D. M. "CERT Insider Threat Research," NCIX, Washington, D.C., Oct. 2008.

Cappelli, D. M. (Conference Chair). "Risk Mitigation Models: Lessons Learned from Actual Cases of Insider Information Theft," MIS Training Institute Data Leakage Conference, Washington, D.C., June 2008.

Cappelli, D. M. "Improving Situational Awareness and Decision-Making Related to Espionage," Intelligence and National Security Alliance (INSA), State College, Pa., July 2008.

Cappelli, D. M. "Insider Threat and the Software Development Life Cycle," CERT podcast, March 2008. http://www.cert.org/podcast/show/20080304cappelli.html

Cappelli, D. M. "Management, Human Resources, and Information Technology: How to Work Together to Prevent Insider Threats," Financial Sector Information Sharing and Analysis Center (FS ISAC) Annual Meeting, May 2008, St. Petersburg, Florida.

Cappelli, D. M. "Management, Human Resources, and Information Technology: Working Together to Prevent Insider Threats," Information Risks Executive Council, Washington, D.C., Aug. 2008.

Cappelli, D. M. "MERIT Insider Threat Diagnostic," New York Stock Exchange, New York, April 2008.

Cappelli, D. M. "Preventing Insider Threats: Avoiding the Nightmare Scenario of a Good Employee Gone Bad," DHS Security Conference, Washington, D.C., Aug. 2008.

Cappelli, D. M. "Preventing Insider Threats: Avoiding the Nightmare Scenario of a Good Employee Gone Bad," Technologies for Critical Incident Preparedness, Oct. 2008.

Cappelli, D. M. "Preventing Insider Threats: Lessons Learned from Actual Attacks, Amex, Nov. 2008.

Cappelli, D. M. "Preventing Insider Threats: Lessons Learned from Actual Attacks," Chemical Sector IT Conference, Sept. 2008.

Cappelli, D. M. "Preventing Insider Threats: Lessons Learned from Actual Attacks," Gas and Oil Conference, Sept. 2008.

Cappelli, D. M. "Risk Mitigation Models: Lessons Learned from Actual Insider Attacks," UK Workshop on Insider Threat, London, England, Nov. 2008.

Cappelli, D. M. "The MERIT Project: Continuing the Fight Against Insider Threats," 2008 CyLab Partners Conference, Pittsburgh, Pa., Oct. 2008.

Cappelli, D. M. & Moore, A. P. "Risk Mitigation Strategies: Lessons Learned from Actual Attacks," Advanced Metering Infrastructure Security (AMI-SEC), Pittsburgh, Pa., April 2008. http://www.cert.org/archive/pdf/defcappellimoore0804.pdf

Cappelli, D. M. & Moore, A. P. "Risk Mitigation Strategies: Lessons Learned from Actual Attacks," RSA Conference, San Francisco, April 2008. http://www.cert.org/archive /pdf/defcappellimoore0804.pdf

Caralli, R. A. & White, D. W. "Managing and Benchmarking Operational Resiliency," Gartner Business Continuity conference, Chicago, Ill., March 2008.

Caralli, R. A. "The CERT Resiliency Engineering Framework," FFRDC CIO meeting, Pittsburgh, Pa., June 2008.

Caralli, R. A. "The CERT Resiliency Engineering Framework," SEI Webinar Series, Sept. 2008.

Caron, T. "New Methods of Insider Threat Management," CyLab Partners Meeting, Pittsburgh, Pa., Oct. 2008.

Cummings, A. & Moore, A. P. "Insider Threat to National Security: Data Collection and Analysis," Army Senior Leadership Conference, Pittsburgh, Pa., Sept. 2008.

Dunlevy, C. & Merrell, S. A. "Critical Information Infrastructure Protection," GovSec 2008, Washington, D.C., March 2008.

Lipson, H. "Cyber Security and Survivability of Current and Future Energy Systems: Technical and Policy Challenges," Fourth Annual Carnegie Mellon Conference on the Electricity Industry, Carnegie Mellon University, March 2008.

Lipson, H. "Towards a CERT Coordination Center for Control Systems – The Survivability Challenge," 2008 ACS Control Systems Cyber Security Conference, Chicago, Ill., August 2008.

Manion, A. "Managing Security Vulnerabilities Based on What Matters Most," CERT podcast, July 2008. http://www.cert.org/podcast/show/20080722manion.html

Manion, A. Panel discussion on vulnerability disclosure, Process Control Systems Industry Conference, 2008.

Manion, A. "Vulnerability Response Decision Assistance," FIRST-TC and JPCERT/CC infrastructure meetings, 2008.

Mead, N. R. "Computing Education in the Coming Decade," panelist, "The Impact of Software Assurance on Computing Education," COMPSAC Conference, Turku, Finland, July 2008.

Mead, N. R. "Future Challenges of Security Requirements," panelist, Grace Symposium on Security Requirements, National Institute of Informatics (NII), Tokyo, Japan, June 9, 2008.

Mead, N. R. "Identifying Software Security Requirements Early, Not After the Fact," CERT podcast, July 2008. http://www.cert.org/podcast/show/20080708mead.html

Mead, N. R. "Requirements Engineering for Improved System Security," Grace Symposium on Security Requirements, National Institute of Informatics (NII), Tokyo, Japan, June 9, 2008.

Mead, N. R. "SQUARE Tutorial and Demo," Distinguished Lecturer, Nortel, Canada, Nov. 2007.

Merrell, S. A. "Initiating a Security Metrics Program: Key Points to Consider," CERT podcast, March 2008. http://www.cert.org/podcast/show/20080318merrell.html

Merrell, S. A. "Risk Assessment," Pennsylvania Association of Community Bankers 2008 Technology Conference, Camp Hill, Pa., Nov. 2008.

Moore, A. P. "Protecting the Flanks from All Sides: The Insider Threat," Financial Services Technology Consortium, Santa Rosa, Calif., June 2008.

Moore, A. P. "What Organizations Need to Know about Insider Threat," TechTarget Conference – Information Security Decisions, Chicago, Ill., Nov. 2008.

Moore, A. P. & Cappelli, D. M. "Focusing on Transition: An Update on CyLab's MERIT* Insider Threat Research," ARO Sponsor Review, Pittsburgh, Pa., Oct. 2008.

Seacord, R. C. "Developing Secure Code," 2008 Census Bureau Software Process Improvement Conference, Sept. 11, 2008.

Seacord, R. C. "Producing Secure Programs in C and C++," NASA IS&T Colloquium, April 30, 2008.

Seacord, R. C. "Secure Coding," Software Assurance Working Group Meeting, Dec. 2, 2008.

Seacord, R. C. "Secure Coding in C and C++: Strings" and "Secure Coding in C and C++: Integers," 2008 Software Development Best Practices, Oct. 28, 2008.

Shimeall, T. "Anonymizing Network Flow Information," FloCon 2008, Savannah, Ga., Jan. 2008.

Trzeciak, R. F. "Insider Information Theft – How to Identify It," Charlotte Federal Conference on Emerging Cyber Threats to Financial Institutions and their Customers, Charlotte, N.C., Oct. 2008.

Trzeciak, R. F. "Insider Theft of Confidential or Sensitive Information: Trends and Patterns in Almost 90 Actual Cases," International Information Integrity Institute (I4), Austin, Texas, Feb. 2008.

Trzeciak, R. F. "Insider Threat: Illicit Cyber Activity in the Banking and Finance Sector," FinSec2008 Conference, New York, N.Y., Dec. 2008.

Trzeciak, R. F. "Insider Threat Workshop: Management, Human Resources, and Information Technology: Working Together to Prevent or Detect Insider Threats," CIO Institute, Arlington, Va., Nov. 2008.

Trzeciak, R. F. (Keynote Speaker). "Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks," Government Information Management Information Science (GMIS) International Conference, Atlantic City, N.J., June 2008.

Trzeciak, R. F. "Preventing Insider Threats: Lessons Learned from Actual Attacks," Hancock County Bank, Hancock County, Pa., Sept. 2008.

Trzeciak, R. F. "Risk Mitigation Strategies: Lessons Learned from Actual Attacks," RSA Japan Conference, Tokyo, Japan, April 2008. http://www.cert.org/archive/pdf/defcappellimoore0804.pdf

Trzeciak, R. F. "Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks," Fidelity Investments Information Security Board, Boston, April 2008.

Trzeciak, R. F. "You Can't Stop It if You Don't Know What to Look For: Understanding Insider Threats," BAI Combating Payments Fraud Conference, Washington, D.C., Oct. 2008.

Waits, C. "Computer Forensics for Business Leaders: Building Robust Policies and Processes," CERT podcast, Oct. 2007. http://www.cert.org/podcast/show/20071030waits.html

White, D. W. "CERT® Resiliency Engineering Framework—Improving Operational Resiliency," Association of Continuity Planners, NYC Chapter Meeting, New York, N.Y., Feb. 2008.

White, D. W. "Managing Operational Resiliency," FST Summit conference, New York, N.Y., June 2008.

White, D. W. "Software Acquisition," Defense Acquisition University, Ft. Belvoir, Va., Aug. 2008.

White, D. W. "Software Acquisition," Defense Acquisition University, Ft. Belvoir, Va., Dec. 2008.

White, D. W. "The CERT® Resiliency Engineering Framework—Achieving and Sustaining Operational Resiliency," Securities Industry and Financial Markets Association Business Continuity Planning conference, New York, N.Y., Oct. 2008.

White, D. W. "The CERT® Resiliency Engineering Framework—A Maturity Model for Enterprise Security and Business Continuity," Wachovia, May 2008.

White, D. W. "The CERT® Resiliency Engineering Framework—A Process Improvement Approach for Enterprise Security and Business Continuity," Citigroup, New York, N.Y., 2008.

White, D. W. "The CERT® Resiliency Engineering Framework—A Process Improvement Approach for Enterprise Security and Business Continuity," public tutorial hosted by the SEI, Arlington, Va., March 2008.

White, D. W. "The CERT® Resiliency Engineering Framework—A Process Improvement Approach for Enterprise Security and Business Continuity," SEPG Europe conference, Munich, Germany, June 2008.

White, D. W. & Caralli, R. A. "The CERT® Resiliency Engineering Framework," Environmental Protection Agency, May 2008.

White, D. W. & Wallen, C. "A Roadmap for Managing Operational Resiliency," public tutorial hosted by JPMorgan Chase, New York, N.Y., March 2008.

White, D. W. & Young, L. R. "FSTC-CERT Resiliency Workshop," two-day private workshop, SEI, Pittsburgh, Pa., Oct. 2008.

White, D. W. & Young, L. R. "The CERT® Resiliency Engineering Framework—A Process Improvement Approach for Enterprise Security and Business Continuity," SEPG North America conference, Tampa, Fla., March 2008.

Willke, B. "CSIRT Contributions to National Efforts in Critical Information Infrastructure Protection," Computer Security Incident Response Team (CSIRT) Workshop hosted by Organization for American States and the Implementation Agency for Crime and Security, Trinidad and Tobago, Dec. 2008.

Willke, B. "CSIRT Contribution to National Response: An Architecture Approach with U.S. Examples," CERTs in Europe Workshop, European Network and Information Security Agency, Athens, Greece, May 2008.

Willke, B. "Developing a Multinational Capability & Contributing to National Cyber Incident Response," Computer Security Incident Response Team (CSIRT) Workshop hosted by Organization for American States and the Implementation Agency for Crime and Security, Trinidad and Tobago, Dec. 2008.

Willke, B. "Government-Industry Collaboration," International Telecommunications Union Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection, Doha, Qatar, Feb. 2008.

Willke, B. "Managing Risk to Critical Infrastructures at the National Level," CERT podcast, Aug. 2008. http://www.cert.org/podcast/show/20080805willke.html

Woody, C. Information Assurance Focus Session, 76th MORS Symposium, New London, Conn., June 2008.

Woody, C. "Framework Linking Technology Risk to Mission Success," System and Software Technical Conference (SSTC) 2008, Las Vegas, N.M., May 2008.

Woody, C. Analyzing the Impact of Emerging Societies on National Security workshop, Military Operations Research Society (MORS), Chicago, Ill., April 2008.

Woody, C. "Megasystem Survivability Analysis Framework," Computer Security Institute (CSI) 2007, Crystal City, Va., Nov. 2007.

Wright, E. "Is Your Wireless Network Safe from Hackers?" Television interview, May 2, 2007, 11 p.m., WTAE Channel 4 Action News, Pittsburgh.

Young, L. R. "Enterprise Resiliency: Building Competencies to Adapt to Dynamic Risk Environments," ISACA EuroCACS conference, Stockholm, Sweden, March 2008.

Young, L. R. "Focus on Operational Resiliency: A Process Improvement Approach to Security Management," ISACA EuroCACS conference, Stockholm, Sweden, March 2008.

Young, L. R. "Managing Operational Resiliency—A Process of Convergence and Continuous Improvement," DHS Software Assurance conference, Vienna, Va., May 2008.

Young, L. R. "Security Risk Assessment Using OCTAVE® Allegro," CERT podcast, Sept. 2008. http://www.cert.org/podcast/show/20080916young.html

Young, L. R. "The CERT® Resiliency Engineering Framework—A Benchmarking Case Study," FSTC Annual Meeting, Sonoma, Calif., June 2008.

Young, L. R. "The CERT® Resiliency Engineering Framework: A Process Improvement Approach for Enterprise Security & Business Continuity," SEPG NA, Tampa, Fla., March 2008.

Zahn, J. (Invited) "Combining Predicate and Numeric Abstraction for Software Model Checking," Microsoft Research, Redmond, Wash., Nov. 20, 2008.

Zahn, J. (Invited) "Machine Learning & Privacy Protection," Keynote Speech, iCAST, Taiwan, Jan. 8, 2008.

Zahn, J. (Invited) "National Privacy Challenges," ChengKong University, Jan. 10, 2008.

Zahn, J. (Invited) "Privacy Enhancing System," Korea University, April 28, 2008.

Zahn, J. (TWISC Invited) "Privacy in Digital Age," Guest Lectures in Taiwan Information Security Center, July 21–25, 2008.

Zahn, J. (Invited) "Privacy-Preserving Data Mining Systems," Yunnan University of Finance and Economics, June 30, 2008.

Zahn, J. (Invited) "The Fundamental Problems in Privacy Research," IEEE International Conference on Granular Computing, 2008.

Technical Leadership

Julia H. Allen

CERT representative to the EDUCAUSE Security Task Force Risk Management Working Group

Program committee member, Information Security, Compliance, and Risk Management Institute, Sept. 2008

Program committee member, Making the Business Case for Software Assurance Workshop, Sept. 2008

Sagar Chaki

Program committee member, 15th International Conference on Logic for Programming, Artificial Intelligence and Reasoning, Nov. 2008

Markus De Shon

Program committee chair, FloCon 2009

Arie Gurfinkel

Program committee member, 19th International Conference on Concurrency Theory, Aug. 2008

Program committee member, 18th Annual Conference on Computer Science and Software Engineering, Oct. 2008

Reviewer for 20th International Conference on Computer Aided Verification, July 2008

Howard Lipson

Invited presentation, "Towards a CERT Coordination Center for Control Systems –The Survivability Challenge," 2008 ACS Control Systems Cyber Security Conference, Chicago, Ill., Aug. 2008

Member, Advisory Board for Duquesne University's Graduate Program in Computational Mathematics, 1999–present (chair 2002–2004)

Member (founding), Carnegie Mellon Electricity Industry Center

Program co-chair, Third ACM Workshop on Digital Identity Management, ACM CCS, Nov. 2007

Program committee member, Fourth ACM Workshop on Digital Identity Management, ACM Conference on Computer and Communications Security, Oct. 2008

Reviewer, *Computers & Security Journal*

Reviewer, *Journal of Service Science and Management*

Scientific advisor, Ambient Intelligence Laboratory, Carnegie Mellon University

Served in an advisory role to the Advanced Metering Infrastructure Security Task Force, part of the Open Smart Grid Users Group

Session chair, "Usability and Authentication," Third ACM Workshop on Digital Identity Management, ACM CCS, Nov. 2007

Art Manion

Member of INCITS CS1, which is the U.S. Technical Advisory Group for ISO/IEC JTC 1/SC 27 and all SC 27 Working Groups

Nancy R. Mead

IEEE Conference on Software Engineering Education & Training (CSEET 2008), Charleston, S.C., April 2008, Nancy Mead track; establishment of Nancy Mead Award for Excellence in Software Engineering Education

Editorial board member, *Requirements Engineering Journal*

Education Track co-chair and program committee member, International Computer Software and Applications Conference, July 28-Aug. 1, 2008

Keynote speaker, "Software Engineering Education: How Far We've Come and How Far We Have to Go," CSEET 2008, April 2008

Local arrangements chair, CSEET 2008, April 2008

Program committee member, International Workshop on Security and Software Engineering, July 2008

Track co-chair, Special Session on Engineering Security Requirements and Privacy Informatics, Information Security & Assurance Conference, April 2008

Workshop program chair, Making the Business Case for Software Assurance Workshop, Sept. 2008

Robert C. Seacord

Represents Carnegie Mellon at PL22.11 (ANSI "C")

Technical expert for the JTC1/SC22/WG14 international standardization working group for the C programming language

Timothy J. Shimeall

Program committee member, FIRST Workshop on Network Data Anonymization

General chair, FloCon 2008, Jan. 2008

Randall F. Trzeciak

Keynote speaker, "Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks," Government Information Management Information Science International Conference, Atlantic City, N.J., June 2008

David White

Keynote speaker, "Managing Operational Resiliency—A Process of Convergence and Continuous Improvement," Ontario Public Service Security Forum and Workshops, Toronto, Ontario, April 2008

Carol Woody

Workshop program committee, Sixth International Workshop on Requirements for High Assurance Systems, Delhi, India, Oct. 2007

Security track chairperson, SEPG 2008, Tampa, Fla., March 2008

Program committee, Quality-of-Service Concerns in Service Oriented Architectures Workshop, International Conference on Service Oriented Computing, Sydney, Dec. 2008

Justin Zahn

Advisory board member, International Conference on Information Security and Assurance, April 2008

Advisory/editorial board member, *Journal of Security Engineering*, Oct. 2006–present

Associate editor, *International Journal of Information Systems in the Service Sector*, July 2007–present

Board member, *Journal of Information, Information Technology, and Organization*, May 2005–present

Board member, *International Journal of Doctoral Studies*, Aug. 2005–July 2008

Chair, Graduates of Last Decade, IEEE Computational Intelligence Society (CIS), 2007, 2008

Chair, Security and Information Technical Committee Task Force, IEEE CIS, June 2007–present

Editor, *International Journal of Medical Informatics*, Jan. 2008–present

Editor board member, *Asian Journal of Information Technology*, June 2007–present

Editor board member, *International Business Management*, June 2007–present

Editor board member, *International Journal of Information Systems in the Service Sector*, July 2007–present

Editor board member, *International Journal of Mobile Communication*, June 2007–present

Editor board member, *International Journal of Soft Computing*, June 2007–present

Editor board member, *Journal of Engineering and Applied Sciences*, June 2007–present

Editor board member, *Journal of Modern Mathematics and Statistics*, June 2007–present

Editor board member, *Research Journal of Applied Sciences*, June 2007–present

Editorial board member, *International Journal of Informatics Society*, Aug. 2008–present

Editorial board member, *International Journal of Network Security*, Aug. 2004–present

Editor-in-chief, *International Journal of Modern Mathematics and Statistics*, Jan. 2008–present

Program co-chair, International Conference on Information Security and Assurance, April 2008

Program committee member, 2008 IEEE International Conference on Granular Computing, Aug. 2008

Program committee member, 2008 Workshop on Collaborative Distributed Knowledge Discovery, May 2008

Program committee member, ICMLC, July 2008

Program committee member, International Conference on Data Mining, July 2008

Program committee member, Seventh Wuhan International Conference on E-business, May 2008

Biographies

Julia H. Allen
Julia H. Allen is a Senior Researcher at CERT. Allen is engaged in developing and transitioning executive outreach programs in enterprise security and governance and conducting research in software security and assurance.

Prior to this technical assignment, Allen served as Acting Director of the SEI for six months and Deputy Director/Chief Operating Officer for three years. Before joining the SEI, she was a vice president in embedded systems software development for Science Applications International Corporation and managed large software development programs for TRW (now Northrop Grumman).

In addition to her work in security governance, Ms. Allen is the author of *The CERT Guide to System and Network Security Practices* and the CERT Podcast Series: Security for Business Leaders. She is a co-author of *Software Security Engineering: A Guide for Project Managers*. Her degrees include a BS in Computer Science (University of Michigan), an MS in Electrical Engineering (University of Southern California), and an Executive Business Certificate (University of California – Los Angeles).

Luanne Burns
Dr. Luanne Burns is a Senior Member of the Technical Staff at the SEI and is currently serving as a member of the FX/MC (Function Extraction for Malicious Code) team. Dr. Burns is an expert on human-computer interaction. Her work on the function extraction project for computing software behavior has focused on design and development of the user interface and the system repository for storing behavior databases. She also produced a video on FX technology concepts to better communicate the concepts to non-specialists.

Dr. Burns received her MS in Computer Science and her PhD in Cognitive Science from Columbia University. Dr. Burns was a Research Staff Member at IBM's Thomas J. Watson Research Center for 18 years. The focus of her work has been on user interface design and implementation in the database, education, and internet domains. She participated in research efforts at IBM that eventually became commercial products, including Visualizer Ultimedia Query, Websphere Web Analyzer Viewer, the IBM SchoolVista Assessment Suite, and a web application for reporting Olympic scores. Dr. Burns has worked extensively in website design, programming, Flash development, database design, e-commerce, and graphics, and teaches courses in programming, logic, and web development.

Dawn Cappelli
Dawn Cappelli is Technical Manager of the Threat and Incident Management Team at CERT. Her team's mission is to assist organizations in improving their security posture and incident response capability by researching technical threat areas; developing information security assessment methods and techniques; and providing information, solutions, and training for preventing, detecting, and responding to illicit activity. Team members are domain experts in insider threat and incident response. Team capabilities include threat analysis and modeling, development of security metrics and assessment methodologies, and creation and delivery of training and workshops.

Dawn has 28 years experience in software engineering, including programming, technical project management, information security, and research. She regularly presents at national and international conferences, and is adjunct professor in Carnegie Mellon's Heinz School of Public Policy and Management. Before joining Carnegie Mellon in 1988, she worked for Westinghouse as a software engineer developing nuclear power systems.

Richard Caralli
Richard Caralli is the Technical Manager for the Resiliency Engineering and Management team at CERT. His work includes the exploration and development of process oriented approaches to security management. In other work at the SEI, Caralli has been active in developing and delivering information security risk assessment, analysis, and management technologies for customers in the government and private sector.

Rich has over 25 years experience in information technology (particularly systems analysis and information systems audit and security) in Fortune 1000 companies covering banking and finance, steel production, light manufacturing, and energy industries. He holds a BS degree in Accounting from St. Vincent College and an MBA with a concentration in Information Technology from the John F. Donahue Graduate School of Business at Duquesne University. He has been on the adjunct faculty at Community College of Allegheny County and is a frequent lecturer in Carnegie Mellon's Heinz School of Public Policy and Management and the CIO Institute's Executive Education programs.

Sagar Chaki
Sagar Chaki is a Senior Member of the Technical Staff at the SEI. He received a B. Tech in Computer Science & Engineering from the Indian Institute of Technology, Kharagpur, in 1999 and a PhD in Computer Science from Carnegie Mellon University in 2005. He works mainly on automating formal techniques for software analysis, but is generally interested in rigorous and automated approaches for improving software quality. He has developed several automated software verification tools, including two model checkers for C programs, MAGIC and Copper. He has co-authored over 29 peer reviewed publications. More details about Sagar and his current work can be found at http://www.sei.cmu.edu/staff/chaki.

Cory F. Cohen
Cory F. Cohen is a Senior Member of the Technical Staff at CERT, guiding the research and development work of the Malicious Code Analysis team. During his 12 years at CERT, he has worked as a security incident handler, a vulnerability analyst, and a malicious code analyst. His recent work has focused on large-scale automated analysis of malicious code samples collected by CERT.

Prior to joining CERT, Cohen worked for the University of Louisville as HP/UX System Administrator in the engineering school, where he managed the primary computing cluster. He also worked for the university as an IDMS/R database administrator maintaining production payroll and student record systems. Cohen holds a BS in Information Science and Data Processing from the University of Louisville.

Timothy Daly
Timothy Daly is a Senior Member of the Technical Staff at the SEI and is currently serving as a member of the team developing Function Extraction (FX) technology for computing software behavior. Prior to this, he served as a research scientist at the Center for Algorithms and Interactive Scientific Software at City College in New York, where he was the lead developer on Axiom (a General Purpose Computer Algebra System) and Magnus (an Infinite Group Theory system). Formerly he was employed at IBM Research in Yorktown, New York, where he participated in projects on rewritable paper, natural language understanding, expert systems, knowledge representation, computer algebra, and industrial robotics. He holds one patent in the area of robotics. He helped develop four commercial programming languages. He has published a tutorial book on Axiom and is the lead developer on that open source project. He has taught at City College of New York, Vassar College, and William Patterson College. He holds a master's degree in Computer Science from Fairleigh Dickinson University and a BS in Mathematics from Montclair State University.

Markus De Shon
Markus De Shon is a Senior Member of the Technical Staff at CERT. As the analysis team lead for the Network Situational Awareness team, Markus guides the research activities of the network security analysts and provides support to analysis operations for government agency customers.

Prior to joining the SEI, Markus was Chief Scientist at SecureWorks, Inc. His work included designing intrusion prevention (IPS) technologies, IPS signature development based upon vulnerabilities and reverse engineering of malicious code, analysis of network activity, and acting as the final incident handling escalation point for an IPS service to nearly 1,000 small to medium-sized businesses.

De Shon holds a PhD in Nuclear Physics and an MS in Health Physics from the Georgia Institute of Technology.

Will Dormann
Will Dormann has been a software vulnerability analyst with the CERT Coordination Center (CERT/CC) for over four years. His focus area includes web browser technologies and ActiveX in particular. Will has discovered thousands of vulnerabilities, most of which by using the CERT Dranzer tool.

Chad Dougherty
Chad Dougherty is an internet security analyst on the CERT Coordination Center (CERT/CC) Vulnerability Analysis team. Dougherty analyzes information about security vulnerabilities in networked computer systems and communicates this information to others, such as affected vendors, security researchers, and the public.

Prior to joining the SEI, Dougherty worked as a systems and network administrator at the University of Pittsburgh Medical Center and at Lycos.

Michael Duggan
Michael Duggan is a software developer for CERT's Network Situational Awareness team. He has been a staff member of CERT since 2003. He has primarily worked on network flow collection and analysis infrastructure.

Prior to joining the SEI, Duggan was a programmer and designer for the Language Technologies Institute at Carnegie Mellon University. Duggan has a BS in Electrical and Computer Engineering from Carnegie Mellon.

Robert J. Ellison
As a member of the CERT Survivable Systems Engineering group, Robert J. Ellison has served in a number of technical and management roles. He was a project leader for the evaluation of software engineering development environments and associated software development tools. He was also a member of the Carnegie Mellon University team that wrote the proposal for the SEI; he joined the new FFRDC in 1985 as a founding member.

Before coming to Carnegie Mellon, Ellison taught mathematics at Brown University, Williams College, and Hamilton College. At Hamilton, he directed the creation of the Computer Science curriculum. Ellison belongs to the Association for Computing Machinery (ACM) and the IEEE Computer Society.

Ellison regularly participates in the evaluation of software architectures and contributes from the perspective of security and reliability measures. His research draws on that experience to integrate security issues into the overall architecture design process.

Sidney Faber
As a member of the CERT network analysis team, Sid supports customers by providing detailed reports of current and historical network activities. Much of his time is spent studying normal network usage and malicious traffic and routing patterns of very large networks, and in understanding large-scale DNS trends.

Prior to joining the SEI, Sid worked as a security architect with Federated Investors, one of the largest investment managers in the United States. His experience includes over 10 years in software application development and evaluation, and 5 years in the U.S. Navy Nuclear Power program. Sid holds GIAC certifications for Intrusion Detection (GCIA), Windows Security Administrator (GCWN), and Forensics Analyst (GCFA).

Bill Fithen
William L. Fithen is a Senior Member of the Technical Staff at the CERT Coordination Center. His current responsibilities include research into security and survivability of current information technologies and methods and techniques to improve security and survivability of future information technologies. Fithen holds a BS in Physics and an MS in Computer Science from Louisiana Tech University in Ruston, La.

Arie Gurfinkel
Arie Gurfinkel received a PhD, an MSc, and a BSc in Computer Science from the Computer Science Department of University of Toronto in 2007, 2003, and 2000, respectively. He is currently a Member of the Technical Staff at the SEI. His research interests lie in the intersection of formal methods and software engineering, with an emphasis on automated techniques for program verification. He was a lead developer for a number of automated verification tools, including a multi-valued model-checker, XChek, and a software model-checker, Yasm. He has more than 28 publications in peer reviewed journals and conferences.

Jeffrey Havrilla
Jeffrey Havrilla is a Senior Member of the Technical Staff at CERT. His 10 years with CERT have been spent solving challenges in software security engineering. His current area of work is reverse engineering malicious code and analyzing software artifacts associated with computer security attacks. While Technical Leader of the CERT Vulnerability Analysis team, he focused on improving engineering practices and tools designed to prevent and detect vulnerabilities in software systems before being deployed.

Prior to working at the SEI, Havrilla worked at the University of Pittsburgh Medical Center and University of Pittsburgh School of Medicine as a database and network administrator and research systems programmer. Havrilla received a BS in Information Sciences and an MS in Telecommunications from the University of Pittsburgh. He is a member of the Institute of Electrical and Electronics Engineers, IEEE Computer Society, and Internet Society.

Paul Krystosek
Paul Krystosek joined the CERT Network Situational Awareness group in April 2008. In his role as an analyst he supports customers in their analysis efforts and produces prototype analysis systems.

Prior to joining the SEI, Krystosek worked at Lawrence Livermore National Laboratory as a member of CIAC, the Department of Energy computer security team. He also worked at Argonne National Laboratory in various capacities, taught computer science at North Central College and Bradley University, and worked at Fermi National Accelerator Laboratory. He holds a BA from Albion College, an MS in Computer Science from Bradley University, and a PhD in Computer Science from Illinois Institute of Technology.

Richard Linger
Richard Linger is Manager of the CERT Survivable Systems Engineering group. He has extensive experience in function-theoretic foundations for software engineering. Linger directs research and development for the function extraction project for software behavior computation and the Flow-Service-Quality (FSQ) engineering project for network-centric system development. He serves as a member of the faculty at Carnegie Mellon's H. John Heinz III School of Public Policy and Management. At IBM, Linger partnered with Dr. Harlan Mills, IBM Fellow, to create Cleanroom Software Engineering technology for development of ultra-reliable software systems, including box-structure specification, function-theoretic design and correctness verification, and statistical usage-based testing for certification of software fitness for use.

He has extensive experience in project management; system specification, architecture, design, verification, and certification; software re-engineering and reverse engineering; and technology transfer and education. He has published three software engineering textbooks, 12 book chapters, and over 60 papers and journal articles. He is a member of the AIAA and ACM, and a Senior Member of the IEEE.

Howard F. Lipson
Howard F. Lipson is a Senior Member of the Technical Staff in the CERT Program at the SEI. Lipson has been a computer security researcher at CERT for more than 16 years. He is also an adjunct professor in Carnegie Mellon University's Department of Engineering and Public Policy and an adjunct research faculty member at the Carnegie Mellon Electricity Industry Center. He has played a major role in developing the foundational concepts and methodologies necessary to extend security research into the new realm of survivability, and was a chair of three IEEE Information Survivability Workshops. His research interests include the analysis and design of survivable systems and architectures, software assurance, and critical infrastructure protection.

Prior to joining Carnegie Mellon, Lipson was a systems design consultant, helping to manage the complexity and improve the usability of leading-edge software systems. Earlier, he was a computer scientist at AT&T Bell Labs. Lipson holds a PhD in Computer Science from Columbia University.

Art Manion
Art Manion leads the Vulnerability Analysis Team at the CERT Coordination Center. Manion supervises technical analysis and research to make improvements in vulnerability coordination and mitigation. He also researches new ways to manage and make decisions about vulnerabilities and ways to improve software quality and security. In his previous position, Manion analyzed vulnerabilities and wrote Advisories, Alerts, and Vulnerability Notes for CERT and US-CERT.

Before joining CERT, Manion was the Director of Network Infrastructure at Juniata College. He holds a BS in Quantitative Business Analysis from the Pennsylvania State University.

Jeff Mattson
After earning a BS in Computer Science from the United States Military Academy at West Point, New York, Jeff served as a U.S. Army Infantry Officer in the United States and Europe. He then re-engaged the IT industry as a software developer. As a Microsoft Certified Solution Developer (MCSD), his responsibilities grew into a nexus of client programs, server applications, and network administration, which drew him into the field of Information Security. He received an MS in Information Security Policy and Management from Carnegie Mellon University in 2006. He currently develops and enhances cyber security training for CERT's Workforce Development team.

Chris May
Chris is Technical Manager for CERT's Workforce Development program. He is heavily involved in projects with the Department of Homeland Security and the Department of Defense. Prior to joining the SEI, he served eight years in the U.S. Air Force as a communications/computer systems officer. He served in various IT positions in Korea, Japan, and throughout Europe and the United States. May's last Air Force assignment was Chief of the Network Control Center at the United States Air Force Academy in Colorado Springs, Colorado. He led over 90 technicians, supporting 9,000 users, in the daily operations and maintenance of the third largest network in the U.S. Air Force. May received his bachelor's in Education from Indiana University of Pennsylvania in Indiana, Pennsylvania, and a master's in Computer Resources Management from Webster University in St. Louis, Missouri. He is a Certified Information Systems Security Professional (CISSP), a Microsoft Certified Trainer (MCT) and a Microsoft Certified Systems Engineer (MCSE). May is also a Cisco Certified Network Associate (CCNA) and a distinguished graduate of the U.S. Air Force Basic/Advanced Communications Officer Training School in Biloxi, Mississippi.

Nancy R. Mead
Nancy R. Mead is a Senior Member of the Technical Staff in the CERT Survivable Systems Engineering group. Mead is also a faculty member in the Master of Software Engineering and Master of Information Systems Management programs at Carnegie Mellon University. She is currently involved in the study of secure systems engineering and the development of professional infrastructure for software engineers.

Prior to joining the SEI, Mead was a senior technical staff member at IBM Federal Systems, where she developed and managed large real-time systems. She also worked in IBM's software engineering technology area and managed IBM Federal Systems' software engineering education department. She has developed and taught numerous courses on software engineering topics.

Mead has more than 100 publications and invited presentations, and has a biographical citation in Who's Who in America. She is a Fellow of IEEE and the IEEE Computer Society and a member of the ACM. Mead received her PhD in Mathematics from the Polytechnic Institute of New York, and a BA and an MS in Mathematics from New York University.

Samuel A. Merrell
Sam Merrell is a Member of the Technical Staff on the Resilient Enterprise Management Team at CERT. Merrell works with organizations to improve their information security risk management capabilities. This work includes Critical Infrastructure Protection projects within the Department of Homeland Security and analysis of federal (DoD and civilian agency) information security programs, including Federal Information Security Management Act (FISMA) compliance efforts. Recent projects include assisting in the development of the CERT Resilient Enterprise Framework and evaluating Service Oriented Architecture initiatives within the U.S. military.

Prior to joining the SEI, Merrell spent seven years as the Information Technology Manager for a Pittsburgh-area community bank. Before that, he was an information technology consultant, primarily supporting the IBM AS/400. Merrell holds an undergraduate degree from the University of Pittsburgh, the Certified Information Systems Security Professional (CISSP) certification, and a number of SANS certificates, and is currently working towards a master's degree in Information Security at Carnegie Mellon University.

Andrew P. Moore
Andrew Moore is a Senior Member of the Technical Staff at CERT. Moore explores ways to improve the security, survivability, and resiliency of enterprise systems through insider threat and defense modeling, incident processing and analysis, and architecture engineering and analysis. Before joining the SEI in 2000, he worked for the Naval Research Laboratory investigating high assurance system development methods for the Navy. He has over 20 years experience developing and applying mission-critical system analysis methods and tools. Moore received a BA in Mathematics from the College of Wooster and an MA in Computer Science from Duke University.

Moore has served on numerous computer assurance and security conference program committees and working groups. He has published a book chapter and a wide variety of technical journal and conference papers. His research interests include computer and network attack modeling and analysis, IT management control analysis, survivable systems engineering, formal assurance techniques, and security risk analysis.

Richard Pethia
Richard Pethia is the Director of the CERT Program. The program conducts research and development activities to produce technology and systems management practices that help organizations recognize, resist, and recover from attacks on networked systems. The program's CERT Coordination Center (CERT/CC) has formed a partnership with the Department of Homeland Security to provide a national cyber security system, US-CERT. In 2003, Pethia was awarded the position of SEI Fellow for his vision and leadership in establishing the CERT/CC, for his development of the research and development program, and for his ongoing work and leadership in the areas of information assurance and computer and network security. Pethia is also a co-director of Carnegie Mellon University's CyLab. CyLab is a public/private partnership to develop new technologies for measurable, available, secure, trustworthy, and sustainable computing and communications systems. This university-wide, multidisciplinary initiative involves more than 200 faculty, students, and staff at Carnegie Mellon.

Daniel Plakosh
Daniel Plakosh is a Senior Member of the Technical Staff at the SEI. Prior to joining the SEI, Plakosh was the lead software engineer for the Systems Engineering Department at the Naval Surface Warfare Center. Plakosh has over 20 years of software development experience in defense, research, and industry. Plakosh's expertise includes real-time distributed systems, network communications and protocols, systems engineering, real-time graphics, and OS internals. Mr. Plakosh is currently a researcher in the Research Technology and System Solutions (RTSS) program at the SEI.

Mark Pleszkoch
Mark Pleszkoch is a Senior Member of the Technical Staff at CERT. He is an expert in function-theoretic mathematical foundations of software, and focuses on automation of formal methods. As a member of the function extraction research and development team, he is responsible for creating theoretical foundations and engineering automation for FX systems.

Prior to joining CERT, Pleszkoch worked at IBM for 21 years in various capacities. As a member of IBM's Cleanroom Software Technology Center, he provided education and consultation to clients in software process, software engineering technologies, and software testing. He was the principal architect of the IBM Cleanroom Certification Assistant tool set for statistical testing automation.

Pleszkoch received his PhD in Computer Science from the University of Maryland and an MA and a BA in Mathematics from the University of Virginia. He is a member of the IEEE and the Association for Symbolic Logic.

Stacy Prowell
Stacy Prowell is a Senior Member of the Technical Staff at CERT, and chief scientist of STAR*Lab. He is an expert in the function-theoretic foundations of software, and is currently conducting research and development for function extraction technology. Prowell has managed both commercial and academic software development projects and consulted on design, development, and testing of applications ranging from consumer electronics to medical scanners, from small embedded real-time systems to very large distributed applications.

Prior to joining the SEI in 2005, Prowell was a research professor at the University of Tennessee. To support wider adoption of rigorous methods in industry, he started the Experimentation, Simulation, and Prototyping (ESP) project at the University of Tennessee, which develops software libraries and tools to support application of model-based testing and sequence-based specification. Software developed by this program is in use by over 30 organizations.

Prior to working at the university, he served as a consultant in the software industry. His research interests include rigorous software specification methods, automated statistical testing, and function-theoretic analysis of program behavior. Prowell holds a PhD in Computer Science from the University of Tennessee and is a member of the ACM, IEEE, and Sigma Xi.

Kristopher Rush
Kristopher Rush is a Member of the Technical Staff on the CERT Forensics Team. His work with CERT includes both operational and educational initiatives in the fields of computer forensics, network attack and defense, penetration testing, and vulnerability assessment.

Prior to joining the SEI, Kristopher worked with the U. S. Department of State as a member of the Antiterrorism Assistance Program. During this time he developed and taught courses relating to terrorism and cyber crime to foreign military and police.

Rush received a BA in Cultural Anthropology from the University of Florida and an MS in Information Security Policy and Management from the H. John Heinz III School of Public Policy and Management, Carnegie Mellon University. Kristopher is a GIAC Certified Forensic Analyst (GCFA) and a Certified Expert Penetration Tester (CEPT). He is the co-author of several SEI publications, including the First Responders Guide to Computer Forensics: Advanced (CMU/SEI-2005-HB-003) and Defense-in-Depth: Foundations for Secure and Resilient Enterprises (CMU/SEI-2006-HB-003).

Kirk Sayre
Kirk Sayre is an expert in the function-theoretic mathematical foundations that are the basis for function extraction technology. He is currently working on development of the core rewriting engine for the FX system, as well as on formal testing for the system. In addition, Sayre is involved in research involving the application of programming patterns to the development of secure software.

Prior to joining CERT, Sayre was a research professor at the University of Tennessee, where he developed an automated testing framework for the certification of generic scientific computing libraries. In his position at UT, Sayre also developed a CASE tool to support the editing and creation of rigorous sequence-based software specifications. This tool is currently being used on software projects at Oak Ridge National Laboratory and Bosch. Sayre has developed software in many different areas, including educational web applications, automated testing tools, CASE tools, medical devices, and weapons systems.

Robert Seacord
Robert C. Seacord leads the Secure Coding Initiative at CERT. Robert is an adjunct professor in the Carnegie Mellon University School of Computer Science and in the Information Networking Institute, and is part-time faculty at the University of Pittsburgh. An eclectic technologist, Robert is author of four books and more than 40 papers on software security, component-based software engineering, web-based system design, legacy-system modernization, component repositories and search engines, and user interface design and development. Robert started programming professionally for IBM in 1982, working in communications and operating system software, processor development, and software engineering. Robert also has worked at the X Consortium, where he developed and maintained code for the Common Desktop Environment and the X Window System.

Timothy J. Shimeall
Dr. Timothy Shimeall is a Senior Member of the Technical Staff with the CERT Network Situational Awareness Group, where he is responsible for overseeing and participating in the development of analysis methods in the area of network systems security and survivability. This work includes development of methods to identify trends in security incidents and in the development of software used by computer and network intruders. Of particular interest are incidents affecting defended systems and malicious software that are effective despite common defenses.

Tim served as general chair for FloCon 2006 and 2008, a conference dedicated to security analysis using network flow, with approximately 80 participants drawn from more than 12 countries. Tim has more than 30 refereed publications and has supervised the work of more than 40 MS and PhD students.

Matthew Sisk
Matthew Sisk is a Member of the Technical Staff in the Network Situational Awareness (NetSA) group at CERT. Sisk is involved in research and development in support of prototyping and implementing production-level analytical processes.

Sisk spent years working for a variety of groups within Royal Dutch Shell. Starting as a UNIX system administrator, Sisk progressed through more senior roles such as data security analyst and network application/infrastructure developer. The lure of lucrative contracting, the changing organizational environment, as well as an opportunity to travel the globe for over a year led Sisk to join Bluware, Inc.'s roster of consultants. During Sisk's tenure with Bluware, he continued to pursue network security development roles for Shell and a wide variety of clients, including Network Security Solutions and ERCOT (The Electric Reliability Council of Texas). The opportunity to expand his experience and knowledge in a research based environment led Sisk to join CERT in July of 2007.

Sisk holds a BE in Electrical Engineering and Computer Science from Vanderbilt University. He is active in a number of projects in the open source community.

James Stevens
James F. Stevens is a member of the Resiliency Engineering and Management team and a Senior Member of the Technical Staff at CERT. Stevens performs information and infrastructure resiliency research and develops methods, tools, and techniques for resilient enterprise management. This work includes designing and delivering various information security risk assessment, analysis, and management technologies for customers in the government and the private sector. Stevens has been working in information security for over 15 years and holds a BS degree in Electrical Engineering from the University of Notre Dame and an MBA from Carnegie Mellon University's Tepper School of Business. Stevens holds the CISSP certification as well.

David Svoboda
David Svoboda is a Software Security Engineer at CERT. David has been the primary developer on a diverse set of software development projects at Carnegie Mellon since 1991, ranging from hierarchical chip modeling and social organization simulation to automated machine translation (AMT). His KANTOO AMT software, developed in 1996, is still (as of 2008) in production use at Caterpillar. David is also actively involved in several ISO standards groups: the JTC1/SC22/WG14 group for the C programming language and the JTC1/SC22/WG21 group for C++.

Randall F. Trzeciak
Randy Trzeciak is currently a Senior Member of the Technical Staff at CERT. He is a member of a team focusing on insider threat research, including insider threat studies being conducted with the U.S. Secret Service National Threat Assessment Center, the U.S. Department of Defense Personnel Security Research Center, and Carnegie Mellon's CyLab. Trzeciak also is an adjunct professor at Carnegie Mellon's H. John Heinz III School of Public Policy and Management. Prior to his current role at CERT, Trzeciak managed the Management Information Systems team in the Information Technology Department at the SEI.

Prior to working at the SEI, Trzeciak was a software engineer at the Carnegie Mellon Research Institute. Previously he was a lead developer and database administrator at Computing Services at Carnegie Mellon. Prior to his career at Carnegie Mellon, Trzeciak worked for Software Technology, Inc. in Alexandria, Virginia. He holds an MS in Management from the University of Maryland and a BS in Management Information Systems and a BA in Business Administration from Geneva College.

Cal Waits
As a member of the Forensic team in CERT's Practices, Development, and Training group, Cal Waits develops digital forensic training material for law enforcement and intelligence agencies. Cal's research also focuses on emerging trends in the forensic field and tool development.

Before joining the SEI, Mr. Waits worked for the National Security Agency. He holds an MS degree in Information Security from Carnegie Mellon University.

Gwendolyn H. Walton
Gwendolyn H. Walton is a Visiting Scientist with the Survivable Systems Engineering group, where she is currently involved in research on theoretical foundations for computation and automated analysis of software security attributes and function extraction for malicious code.

Prior to joining the SEI, Walton held faculty positions at Florida Southern College and the University of Central Florida. She published over 30 journal and conference papers and directed the research of 2 PhD students, 15 MS students, and 4 undergraduate students. Previously Walton served as President of Software Engineering Technology Inc.; Assistant Vice President, Division Manager, Project Manager, and Senior Systems Analyst for Science Applications International Corporation; Senior Data Systems Programmer for Lockheed Missiles and Space Company; and Research Associate for Oak Ridge National Laboratory.

Walton received her PhD in Computer Science, MS in Mathematics, and BS in Mathematics Education from the University of Tennessee. She is a senior member of IEEE and the IEEE Computer Society, a senior member of the Society of Women Engineers, and a member of the ACM.

Rhiannon Weaver
Rhiannon Weaver is a Member of the Technical Staff in the Network Situational Awareness Group. She holds a BS in Mathematics and a BS in Computer Science from Penn State University, and an MS in Statistics from Carnegie Mellon University, where she is also pursuing her PhD in statistics.

Weaver provides support for advanced modeling techniques for network anomaly detection and large-scale trending of Internet-wide phenomena. Her research interests include time series analysis of network data, data collection and inference in hierarchical and Bayesian models, and addressing the challenges of evaluating and applying advanced modeling and data mining techniques in operational environments.

David W. White
David White is a Senior Member of the Technical Staff at CERT. White is responsible for developing and implementing strategies that lead to the widespread dissemination and use of methods, techniques, and tools that help organizations manage information security risks. He is also a member of the development team for the CERT Resiliency Engineering Framework, a process improvement framework that provides guidelines for managing security and business continuity from an enterprise risk management perspective.

White has a bachelor's degree in Civil Engineering and Public Policy from Carnegie Mellon University and a master's degree in Civil Engineering with a specialization in robotics from Carnegie Mellon University. He is currently based in New York City.

Bradford J. Willke
Bradford Willke is a member of the Resiliency Engineering and Management team and a Senior Member of the Technical Staff at CERT. Willke leads Information and Infrastructure Resiliency research and development and supports national cyber security programs. Willke leads projects to develop process improvements for national and international infrastructure protection communities.

Before joining the SEI, Willke was a technical intern with Southern Illinois University at Carbondale. He managed computing resources for the 90th Security Police Squadron, Francis E. Warren Air Force Base. Willke served in the United States Air Force as a law enforcement specialist and computer security officer from 1993 to 1997.

Willke received a professional certificate in Information Protection and Security from the University of New Haven, a BS in Information Systems Technologies from Southern Illinois University at Carbondale, and an AAS from the Community College of the Air Force. He is also a Certified Information System Security Professional.

Carol Woody
Carol Woody is a Senior Member of the Technical Staff at CERT. She is leading a team of researchers in projects that are focused on ways to address software design and development that improve the security of the implemented results.

Before coming to the SEI, Woody consulted for New York City as a strategic planner for the Administration of Children's Services. She also managed the user testing for a timekeeping application purchased by NYC to handle 160,000 employees in over 100 agencies.

Woody has a biographical citation in Who's Who in American Women and Who's Who in Finance and Industry. She is a member of Upsilon Phi Epsilon, the international honor society for computing and information disciplines, IEEE, the ACM, and PMI. Woody holds a BS in Mathematics from The College of William and Mary, an MBA with distinction from Wake Forest University, and a PhD in Information Systems from NOVA Southeastern University.

Evan Wright
Evan is an analyst for the Network Situational Awareness Team (NetSA) Team. Evan's research interests include next-generation technologies, network design, routing protocols, and design of network attack tools.

Prior to joining the SEI, Wright completed graduate school at Carnegie Mellon, where he obtained his MS in Information Security and Technology Management from the School of Engineering. He also holds a BS in Technology Systems from East Carolina University. Wright worked as Network Administrator at ABC Phones in North Carolina and as a consultant for various other companies. Evan holds the Cisco Certified Networking Professional certificate and four other IT certifications.

Lisa Young
Lisa Young is a Senior Member of the Technical Staff at CERT, where she serves as a contributing developer of the Resiliency Engineering Framework (REF) and the Appraisal Team lead. She holds the designation of Certified Information Systems Auditor (CISA) and Certified Information Systems Security Professional (CISSP) and is experienced in IT governance, audit, security, and risk management. Lisa teaches the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) risk-based assessment methodology at the SEI.

Justin Zhan
Dr. Justin Zhan is a faculty member at Carnegie Mellon University and a research director of the privacy, security, and decision informatics lab at Carnegie Mellon CyLab Japan. His research interests include the privacy and security aspects of data mining, privacy and security issues in social networks, privacy-preserving scientific computing, privacy-preserving electronic business, artificial intelligence applied in the information security domain, data mining approaches for privacy management, and security technologies associated with compliance and security intelligence. He has served as an editor/advisory/editorial board member for many international journals and a committee chair/member for over 80 international conferences. He has published over one hundred articles in various peer reviewed journals and conferences.

Software Engineering Institute
Carnegie Mellon

The 2008 CERT Research Annual Report was produced by SEI Communications.

Executive Editor
Richard Linger

Editor-in-Chief
Pamela Curtis

Design
Robert Fantazier

Production
David Gregg
Melissa Neely

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Fax: 412-268-5758
www.cert.org

Software Engineering Institute
Carnegie Mellon