International Liability Issues for Software Quality

Nancy R. Mead, PhD
CERT Research Center

July 2003

SPECIAL REPORT
CMU/SEI-2003-SR-001

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

International Liability Issues for Software Quality

CMU/SEI-2003-SR-001

Nancy R. Mead, PhD
CERT Research Center

July 2003

Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

List of Tables

Acknowledgments

I appreciate the technical review and many thoughtful comments by Dr. Howard Lipson. I am also grateful for the excellent editorial assistance from Pamela Curtis.

Abstract

This report focuses on international law related to cybercrime, international information security standards, and software liability issues as they relate to information security for critical infrastructure applications. Each area is explored and implications for U.S. policy and efforts to create cyber security policy worldwide are discussed. Recommendations are made for U.S. government participation and leadership.

This report is one of a series of reports on U.S. policy by the CERT Coordination Center. Prior reports focused on international infrastructure for global security incident response and the technical challenges and global policy issues of tracking and tracing cyber attacks.

1 Introduction

This report is the latest in a series of reports developed by the CERT Coordination Center® on the subject of U.S. policy in cyber security. Prior reports focused on international infrastructure for global security incident response [West-Brown 99] and the technical challenges and global policy issues of tracking and tracing cyber attacks [Lipson 02]. The focus of the current effort is on international standards and liability issues as they relate to information security for critical infrastructure applications.

Information security is a key element in protecting international critical infrastructure that is increasingly dependent on Internet capabilities, such as power, transportation, energy, commerce, and finance. Very few systems exist in total isolation from outside networks, and as such these systems can readily become the object of cyber attacks. In addition to recreational hackers, we now have to be concerned with cyber attacks by hostile nation states and terrorists. This has become all too apparent in the post-9/11 timeframe.

At one time, the networks and application systems that supported critical infrastructure were developed as one-of-a-kind custom systems. The wide availability of commercial products and economies of scale have caused a shift in this development model. These days critical infrastructure systems and networks depend on a variety of commercial off-the-shelf (COTS) products, many of which contain security vulnerabilities that make them attractive targets of cyber attacks. Security standards, such as the Common Criteria and IETF standards [Doraswamy 99], when followed, provide some assurance against cyber attacks. It is also the case that the possibility of being held liable for security flaws is of concern to vendors. Nevertheless, securing COTS products remains a productive area of research [Lipson 01], and virtually no system containing COTS products could be considered completely secure.

Some of the questions that we will explore in this report are: the role of security standards in development of critical infrastructure networks and applications, including COTS products; the expected role of liability issues as related to critical infrastructure; recommended participation by the U.S. in these activities; and their relationship to critical infrastructure risk reduction.

® CERT Coordination Center is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

2 Standardization of International Law

For a number of years, there were no international laws or agreements on cybercrime. This meant that attacks initiated in many countries would go largely unpunished. It was often the case that there were no national laws on cybercrime in those countries, and there was no agreement on jurisdiction. In many cases, perpetrators of cybercrime either went unpunished or received a slap on the wrist. In one well-known case of a student hacker, the student was offered a job by his government on completion of his education!

2.1 International Convention on Cybercrime

A first international convention on cybercrime was developed by an international body and signed in 2001. The press release for the signing ceremony follows [Convention 01]:

> *Budapest, 23.11.2001 - The Convention on Cybercrime was opened for signature today in Budapest. It is the first ever international treaty on criminal offences committed against or with the help of computer networks such as the Internet.*
>
> *Ministers or their representatives from the 26 following Member States signed the treaty:[1] Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, "the Former Yugoslav Republic of Macedonia," Ukraine and the United Kingdom. Canada, Japan, South Africa and the United States, who took part in the drafting, also signed the treaty today. Other non-member States may also be invited by the Committee of Ministers to sign this treaty at a later date.*
>
> *Adopted by the Council of Europe's Committee of Ministers on 8 November last, this binding treaty will come into force as soon as five states, at least three of which must be Council of Europe members, have ratified it.*
>
> *The signing ceremony took place in the Hungarian Parliament in the presence of István Stumpf, Head of the Hungarian Prime Minister's Office, Ibolya David, Minister of Justice of Hungary, Paulius Koverovas, Vice Justice Minister of Lithuania (Chair of the Council of Europe's Committee of Ministers), Lord Rus-*

[1] Thirty countries have signed the treaty. See http://www.cybercrime.gov/intl.html.

sell-Johnston, President of the Parliamentary Assembly, and Hans Christian Krüger, Deputy Secretary General of the Council of Europe.

The Convention deals in particular with offences related to infringements of copyright, computer-related fraud, child pornography, and offences connected with network security. It also covers a series of procedural powers such as searches of and interception of material on computer networks.

Its main aim, as set out in the Preamble, is to pursue "a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation."

A document from the Department of Justice [DOJ 00] indicates the many benefits that would accrue from the Convention:

The Convention breaks new ground by being the first multilateral agreement drafted specifically to address the problems posed by the international nature of computer crime. Although we believe the vast bulk of the obligations and powers contemplated by the draft Convention are already provided for under United States law, the Convention makes progress in this area by (1) requiring signatory countries to establish certain substantive offenses in the area of computer crime, (2) requiring parties to adopt domestic procedural laws to investigate computer crimes, and (3) providing a solid basis for international law enforcement cooperation in combating crime committed through computer systems. If the United States were to become a party to this Convention, it would directly benefit by having better methods of obtaining international assistance from other parties in computer-related crime cases, particularly because the other parties to the Convention would have similar minimum definitions of computer crimes and the domestic procedural tools needed to investigate those crimes.

The United States, in particular the Department of State (DoS), had a significant role in the development of this Convention, as indicated by the following: "The United States, represented by the Department of Justice and the DoS, in close consultation with other U.S. government agencies, has actively participated in the negotiations in both the drafting and plenary sessions, working closely with both CoE and non-CoE Member States. Because the provisions in the draft Convention are generally adopted by consensus both in the drafting and plenary groups, rather than by member state vote, the United States has had a real voice in the drafting process" [DOJ 00].

We can see that there are many countries that have not signed this document, so this is only a partial solution. Even at that, there were many groups who were opposed to U.S. participation in this document.

For example, the UCLA Journal of Law and Technology (JOLT) notes: "Although the changes to U.S. law, required if the Convention were ratified by the Senate, are moderate considering existing legislation, the adoption of these new standards would have far-reaching effects not only on criminal enforcement, but also on the privacy rights enjoyed by U.S. citizens and businesses" [Rosen 02].

Wired News reports: "The Council of Europe's[2] 65KB proposal is designed to aid police in investigations of online miscreants in cases where attacks or intrusions cross national borders. But the details of the Draft Convention on Cybercrime worry U.S. civil libertarians. They warn that the plan would violate longstanding privacy rights and grant the government far too much power" [McCullagh 00]. Further down in the article, we find the following quote: "'I think it's dangerous for the Internet,' says Barry Steinhardt, associate director of the American Civil Liberties Union[3] and a founder of the Global Internet Liberty Campaign.[4] 'I think it will interfere with the ability to speak anonymously. It will interfere with the ability of hackers—using that term in a favorable light—to test their own security and the security of others,' Steinhardt said" [McCullagh 00].

2.2 Convention on Cybercrime Implications for the U.S. Government

The Convention on Cybercrime should provide support to U.S. cyber security policy interests in that it provides some level of international agreement on how to deal with international cybercrime. Of major concern for the U.S. are the implications of cybercrime that occurs across international boundaries and in countries outside the United States. This treaty is therefore an important first step in combating international cybercrime.

Since the U.S. had a significant role in development of the Convention on Cybercrime, it seems natural to recommend that the U.S. continue in such influential roles. Consistent international laws on cybercrime would seem to be in the interest of the United States. This is an area in which the U.S. has appropriately shown leadership, and such leadership should continue.

[2] http://www.coe.int/
[3] http://www.aclu.org/
[4] http://www.gilc.org/

3 Standards for Secure Software

There have been a number of standards efforts that relate to information security. The International Organization for Standardization (ISO) has long provided an excellent umbrella organization for subcommittees (SCs) and working groups (WGs) involved in standards. A good overview article was provided recently by Francois Coallier [Coallier 03]. In 1987 ISO and the International Electromechanical Commission (IEC) joined forces to put a Joint Technical Committee, JTC 1, in place. JTC 1 has responsibility for standardization in the field of information technology [Coallier 03]. There are a number of efforts under ISO JTC 1, Information Technology, SC 27 on IT Security Techniques. Within SC 27 there are three WGs. WG 1 is Requirements, Security Services, and Guidelines; WG 2 is Security Techniques and Mechanisms; and WG 3 is Security Evaluation Criteria. There have been discussions of security for the global information infrastructure within SC 27 [Fumy 98]; however, many of the issues appear to deal with detailed security issues such as cryptography and key management infrastructure. Additional efforts include IP Security Protocol (IPsec), the Common Criteria, a new effort to add safety and security criteria to the CMMI [Ibrahim 02], and a host of earlier standards. In this section we will discuss the IPsec standard, developed by IETF, and the Common Criteria in more detail. There are many older standards, as well as some detailed standards dealing with specific aspects of security. We felt that the IPsec and Common Criteria represented the type of ongoing broad standards activities that could be relevant to U.S. cyber security policy concerns.

ISO, as its name implies, is an international organization that develops a consensus view on international standards. ISO volunteers participate in Technical Committees, which in turn rely on Working Groups, also composed of volunteers. ISO has member countries and a highly defined process for arriving at consensus. IETF, on the other hand, includes an international community of volunteers that work on development of internet standards. IETF standards are publicly developed, but, in contrast to ISO standards, do not represent an official agreement on the part of participating member countries. However, IETF standards are not de facto standards, which are not publicly developed but are widely used.

3.1 The IPsec Security Standard

In this section we turn to the subject of the quality of software components, particularly security software, and standards, such as the Common Criteria and IPsec standards that have been developed to address security software quality.

The IPsec standards have been developed by the Internet Engineering Task Force. "The Internet Engineering Task Force (IETF)[5] is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual" [IETF 03].

"The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists.[6] The IETF holds meetings three times per year. The IETF working groups are grouped into areas, and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG)"[7] [IETF 03].

There is a working group for IPsec. The chairs of the IPsec working group are Barbara Fraser of Cisco Systems and Theodore Ts'o of MIT. There is also a working group on IP Security Policy (IPSP). The chairs of the IPSP working group are Hilarie Orman of MIT and Luis Sanchez of Xapiens Corporation. The security area directors for both groups are Jeffrey Schiller of MIT and Steven Bellovin of AT&T. "Providing architectural oversight is the Internet Architecture Board (IAB).[8] The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC)[9] for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB" [IETF 03].

The charter of the IPsec working group is as follows: "The IP Security Protocol Working Group (IPSEC) will develop mechanisms to protect client protocols of IP. A security protocol in the network layer will be developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality" [IPsec 03].

3.1.1 TCP/IP Protocol and Layers

The TCP/IP protocol architecture includes a protocol stack, an addressing capability, and a routing capability. The protocol stack includes four layers, which we will discuss further. The addressing capability provides for unique identification of a destination. The routing capability provides for efficient determination of the path that a packet must follow to reach its destination [Doraswamy 99].

5 http://www.ietf.org/glossary.html#IETF
6 http://www.ietf.org/maillist.html
7 http://www.ietf.org/glossary.html#IESG
8 http://www.ietf.org/glossary.html#IAB
9 http://www.ietf.org/glossary.html#ISOC

The protocol stack consists of the application layer, the transport layer, the network layer, and the data link layer. This is illustrated in Figure 1. As is often the case in a layered architecture, each layer interacts only with the layers immediately above and below it, using well-defined interfaces.

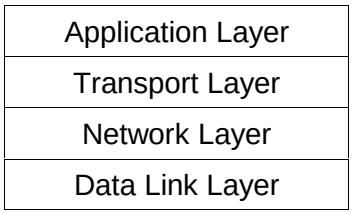

Figure 1: TCP/IP Stack Layering

The application layer provides services that allow an application to send and receive data. These services typically interact with client applications such as email and Web browser applications.

The transport layer in turn provides services to the application layer. These services are as follows: connection-oriented or connectionless transport, reliable or unreliable transport, and security. In connection-oriented transport, once a connection is established, it stays in place until one of the applications gives it up voluntarily. In connectionless transport, a destination must be specified for each packet sent by the application. In reliable transport, if a packet is lost for any reason it is resent automatically by the transport layer. In unreliable transport, the application must decide to resend the packet if it does not reach its destination. Security services associated with the transport layer may include services such as authentication, integrity, and confidentiality. These are relatively new compared to the other transport layer services.

The network layer is responsible for providing connectionless service to the transport layer. It is responsible for routing packets, that is, determining the path that a packet must travel to reach its destination.

The data link layer is responsible for transmitting packets between physical entities. Ethernet is an example of a data link layer, as is token ring.

An example of communication between layers is shown in Figure 2.

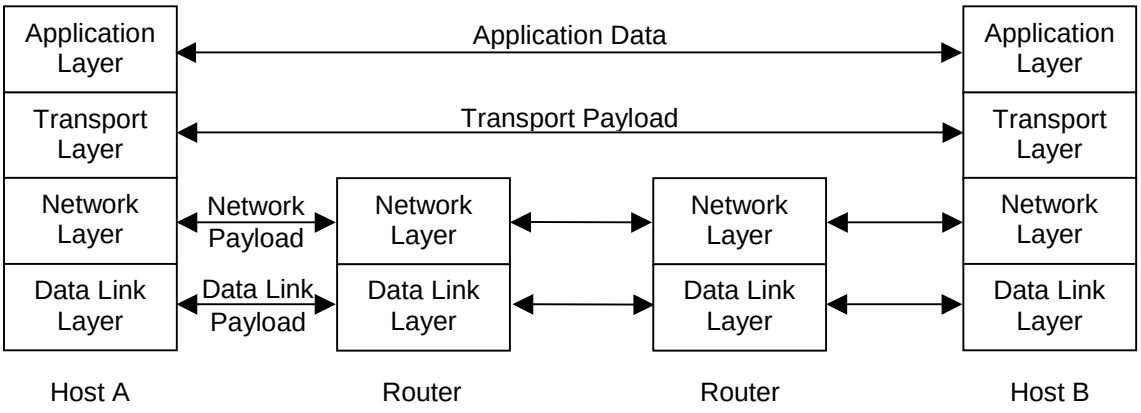

Figure 2: Communication Between Layers

3.1.2 TCP/IP Security

Security services can be implemented at various levels in the stack (TCP/IP layers). Basic security services include key management, confidentiality, nonrepudiation, integrity/ authentication, and authorization. There are advantages and disadvantages of implementing security features at the various layers [Doraswamy 99].

At the application layer, there are several advantages for providing security features. These include the following user facilities: easy access to user credentials, complete access to data the user wants to protect, the ability to extend applications without depending on the operating system to provide these services, and security that is appropriate to the application data. A disadvantage is that security features need to be tailored to each application. Hence, application layer security is attractive when there are very specific security features that need to be implemented for certain applications.

When security is provided at the transport layer, it can be done without having to provide enhancements to each application. However, in order to provide specific user services, the user context becomes more complicated. The underlying model assumes that there is a single user of the system. There are other limitations as well.

When security is implemented at the network layer, the overhead associated with key negotiation decreases. This happens because multiple transport protocols and applications can share the key management infrastructure. When security is implemented at this layer, it is easy to support intranets and virtual private networks (VPNs). A disadvantage of implementing security at this layer is that nonrepudiation is handled more easily at the higher level layers. IP Security is provided at the network layer. We will be discussing this in more detail in the next section.

For dedicated links, security can be implemented at the data link layer using hardware devices. This provides a very high-speed approach, and it works well for dedicated links. However, it does not work well if the devices that need to communicate are not physically connected.

By now you have probably gotten the idea that there is no "ideal" layer for implementation of security features.

3.1.3 IPsec

The IPsec architecture is intended to protect IP packets. It is important to note that there is no security built into IP packets. Therefore, it is relatively easy for a hacker to modify packet contents, forge addresses, inspect the contents of packets, etc. [Doraswamy 99]. There is no way of knowing whether the identity of the sender is correct, whether the content is correct, and whether the content has been intercepted and inspected while it is en route. The purpose of IPsec is to prevent such tampering with IP packets.

IPsec protection includes authentication of header information (including packet origin), connectionless authentication of data integrity, facilities to maintain confidentiality of the data content, protection against replay of previously sent packets, and limited traffic flow confidentiality.

In this report we will discuss in a general way what it is that IPsec does to provide this protection, but not the detailed architectural considerations. Readers who are interested in the technical details of the IPsec architecture are referred to *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks* [Doraswamy 99].

IPsec includes a default set of algorithms that are mandatory for any IPsec implementation. These algorithms define interoperability between different implementations, and the set of algorithms can be easily extended while maintaining interoperability. IPsec defines a method for identifying the traffic (packets) to be protected, how it will be protected, and to whom it will be sent. IPsec protects packets between hosts, between gateways, and between hosts and gateways. The protected packet is in effect just another packet. There are two primary protocols for protecting packets. These are known as Encapsulating Security Payload (ESP) and Authentication Header (AH)

3.1.4 Examples of IPsec Usage

One study examines use of IPsec by the Navy in future systems [Chappell 99]. The authors are from the Naval Surface Warfare Center (NSWC) and examine implementation of IPsec in COTS products. Current implementations use physical separation based on classification

level. It is envisioned that in the future data at various classification levels may reside on shared hardware, and security standards such as IPsec are needed to support these environments. The long-term goal is to provide confidentiality and authentication services to applications, so that multilevel security can be implemented without physical separation. In this paper the authors develop a test bed configuration for measuring network performance. They executed three types of tests: one with no IPsec service, one with IPsec confidentiality, and one with IPsec authentication. In their test results, end-to-end throughput was severely impacted by IPsec services. This confirms that IPsec security cannot be accomplished without performance impacts, and that such impacts need to be considered when configuring a system with IPsec security services.

Another study examines Air Traffic Management (ATM) systems, and the expectation for secure communications links in future systems [Patel 01]. It also presumes that COTS products implementing IPsec standards will be used. This paper discusses Public Key Infrastructure (PKI) encryption techniques and how they might be implemented in ATM systems. A PKI laboratory has been established by the FAA for development and validation of PKI certification in FAA systems. Specific cases under consideration are the FAA Ground End system and the Airborne End System or Airborne Router.

3.2 The Common Criteria

The Common Criteria were developed by a combined effort of six countries: the U.S., Canada, France, Germany, the Netherlands, and the U.K. This effort built on earlier standards, including Europe's Information Technology Security Evaluation Criteria (ITSEC), the Trusted Computer System Evaluation Criteria (TCSEC) of the U.S., and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [Caplan 99]. A Common Criteria evaluation allows an objective evaluation to validate that a particular product satisfies a defined set of security requirements.

3.2.1 Common Criteria Overview

The Common Criteria (CC) contain a grouping of 60 security functional requirements in 11 classes [Abrams 00].

A package is an intermediate combination of requirements components that allows expression of a set of functional or assurance requirements that meet a subset of security objectives. A Protection Profile (PP) is an implementation-independent set of security requirements for a class of Targets of Evaluation (TOEs) that meet the specific consumer needs. A TOE is basically an IT product or system, together with its documentation and administration, which is the subject of a CC evaluation. A PP allows security requirements to be expressed using a template in an implementation-independent way, and is thus reusable. A Security Target (ST)

contains a set of security requirements that can be stated explicitly. An ST includes detailed product-specific information. It can be viewed as a refinement of the PP, and forms the agreed-upon basis for evaluation. This hierarchy is shown in Figure 3. Another way of viewing this is to consider the refinement of specifications, as shown in Figure 4, which has a waterfall-like quality.

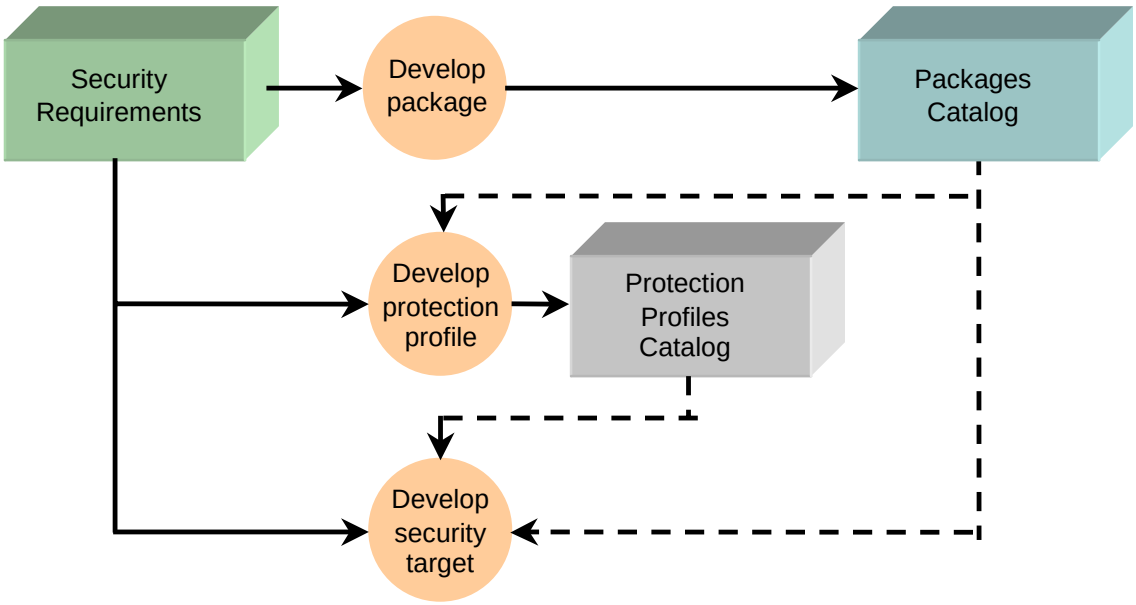

Figure 3: Common Criteria Modular Component Hierarchy

The successful use of the Common Criteria depends on the ability to define the required security capabilities. This should be done in a way that gives consideration to the mission or business, the assets requiring protection, and the purpose of the system under evaluation (the TOE). The focus on mission is very consistent with CERT's focus when considering survivable systems [Ellison 97]. As the Common Criteria have matured, a number of protection profiles have been developed by the National Security Agency (NSA), and then by NSA in conjunction with the National Institute of Standards and Technology (NIST). A working group called the Protection Profile Review Board (PPRB) was formed to review all proposed protection profiles and to work with the authors toward achieving a goal of consistency across PPs. A number of recommendations toward this end have been collected in one document [PP 02].

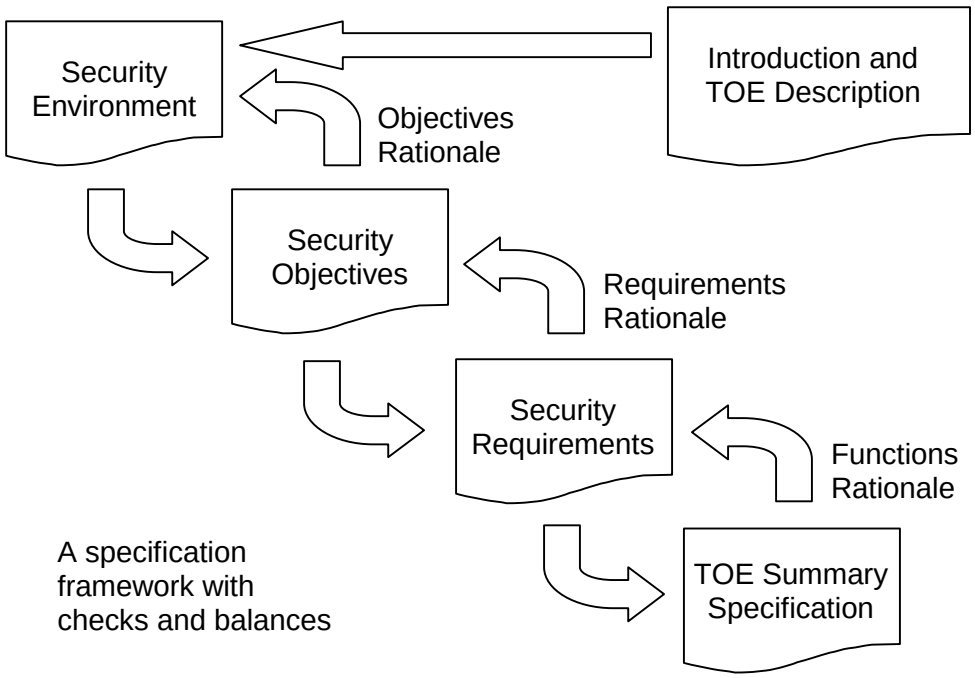

Figure 4: The PP/ST Specification Framework

3.2.2 Common Criteria Evaluation Assurance Levels

Functional and assurance security requirements are the basis for the Common Criteria. There are seven Evaluation Assurance Levels (EALs). The higher the level, the more confidence you can have that the security functional requirements have been met. These levels are:

- **EAL1: Functionally Tested.** Applies when you require confidence in a product's correct operation, but do not view threats to security as serious. An evaluation at this level should provide evidence that the target of evaluation functions in a manner consistent with its documentation and that it provides useful protection against identified threats.
- **EAL2: Structurally Tested.** Applies when developers or users require low to moderate independently assured security, but the complete development record is not readily available. Limited developer access or securing legacy systems may cause this situation.
- **EAL3: Methodically Tested and Checked.** Applies when developers or users require a moderate level of independently assured security, and require a thorough investigation of the target of evaluation and its development, without substantial reengineering.
- **EAL4: Methodically Designed, Tested, and Reviewed.** Applies when developers or users require moderate to high independently assured security in conventional commodity products and are prepared to incur additional security-specific engineering costs.
- **EAL5: Semi-formally Designed and Tested.** Applies when developers or users require high, independently assured security in a planned development and require a rigorous de-

velopment approach that does not incur unreasonable costs from specialist security engineering techniques.

- **EAL6: Semi-formally Verified Design and Tested.** Applies when developing security targets of evaluation for application in high-risk situations where the value of the protected assets justifies the additional costs.
- **EAL7: Formally Verified Design and Tested.** Applies to the development of security targets of evaluation for application in extremely high-risk situations, as well as when the high values of the assets justifies the higher costs.

3.2.3 Common Criteria Examples

One way in which the Common Criteria can be used is in conjunction with system acquisition [Abrams 00]. A mapping between CC features and system acquisition elements is shown in Table 1. In the first row, the protection profile concept helps to identify, among other things, customer requirements. These can in turn be used in a Request for Proposal (RFP). The fact that there are many protection profile templates in existence is very helpful to this part of the effort. The notion of the security target in the second row gives an indication of how the requirements might be satisfied by specific suppliers. Of course, the TOE is intended to be a specific system or collection of components that can be evaluated. Finally, the evaluated and accepted system should support consistency of the outputs of the previous three rows. From the point of view of a model, this provides a series of representations that can be checked and compared to one another. This is consistent with acquisition activities at the FAA. This sort of example of consistency suggests broad application of the Common Criteria, particularly to critical infrastructure systems.

Table 1: Mapping Between CC Features and System Acquisition Elements

CC Paradigm	System Acquisition Paradigm	Observations Regarding Commonality Among CC & Acquisition Paradigms
Protection Profile (PP)	Request for Proposals	Provides customer desires, needs, and requirements: “What is wanted”
Security Target (ST)	Proposals	Indicates how the above will be satisfied by suppliers: “What will be provided”
Target of Evaluation (TOE)	Delivered System	Is the supplier’s physical manifestation of above
Evaluated System	Accepted System	Shows that the three preceding representations are sufficiently consistent

The FAA’s National Airspace System Infrastructure Management System (NIMS) provided a venue for development of its own PP. Specific requirements were derived from and linked to the CC components. A set of eight example requirements is provided [Abrams 00]. This is followed by a discussion of system integration and acceptance test considerations that result from application of the CC.

The FAA Telecomm services also provided a source for a CC case study [Herrmann 01]. In this study the FAA Telecommunications Infrastructure (FTI) project provides an example of a services contract that is using the CC. FTI provides integrated voice, data, and video telecommunications services in the continental U.S., with connectivity to Hawaii, Alaska, and U.S. territories. FTI requirements are expressed in terms of service classes and service interfaces. In this particular case, the vendor is required to demonstrate EAL3. The authors discuss the meaning of an EAL in the context of a services contract, and also the effort involved in maintaining an EAL during the entire systems lifecycle, after systems development. Both the Common Criteria and process assessments were used to maintain a balanced security assurance program. It was felt that use of the CC was beneficial for this project's acquisition strategy.

In another example the PalME project, an electronic purse application for Palm handhelds, provides a case study for application of the common criteria [Vetterling 02]. It was felt that there was some documentation overhead associated with use of the CC, but nevertheless using the CC for this project was practical.

3.3 Standards Implications for the U.S. Government

The two standards discussed here have rather different implications for the U.S. government. The IPsec protocol is likely to be embedded in a vendor's product or set of products. Either the products incorporate the protocol, or they don't. This suggests that use of the IPsec protocols could be a consideration for the U.S. government in acquisition of COTS software.

The Common Criteria, on the other hand, apply when an entire system is being developed. Although there may be COTS elements, the focus is on security during the entire lifecycle process, from requirements through verification. When critical infrastructure systems involve significant development, or even integration of COTS products, the Common Criteria can be considered to provide additional security assurance.

The Capability Maturity Model Integration provides a mechanism for organizations to measure the maturity of their software engineering processes. Eventually, modifications to Capability Maturity Model® Integration models to take into account safety and security considerations may take place [Ibrahim 02], and these could also be of interest to the U.S. government. It is premature, however, to have a dependency on such changes.

Protection of critical infrastructure suggests the use of standard security protocols, particularly in light of the use of COTS software in many critical infrastructure systems. Systems

® Capability Maturity Model is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

that support the power, financial, and federal infrastructure are good candidates for use of secure COTS software.

The standards described here have a strong U.S. presence. In view of the predominance of U.S. software products, we recommend continued U.S. involvement in these standards activities. For U.S. government and policy interests, either direct involvement or monitoring of standards development is recommended. It would be advisable to look for a good match in areas of direct interest to the U.S. government. Some of the standards activities require a deep technical knowledge of a specific security area (e.g., cryptography). Without that deep technical knowledge, it will be difficult to be an active participant in such a standards effort, so this is a consideration as well.

At an international level, considering the presence of U.S. staff in other countries, and considering the international interdependencies on critical infrastructure, the U.S. should encourage international participation in standards development, and international adoption of COTS products with appropriate security features.

4 Software Manufacturers' Liability

4.1 Liability Overview

The relationship between software and data quality is an important one. Joseph Juran is quoted as saying "Data are of high quality if they are fit for their intended uses by customers in operations, decision making, and planning" [Redman 03]. Recently, we have seen an emphasis on accountability for the quality of data and software. Specifically examining data, we are told:

- "Those who create data models must be held accountable for the quality…of the models."
- "Those who create data values must be held accountable for the accuracy of those values."
- "Those who develop applications must be held accountable for quality dimensions associated with data presentation" [Redman 03].

In a related discussion about corrupted data, it is suggested that the sources of corruption be eliminated, and that resources be applied to the most important data [Pautke 03]. Quoting Redman, "A database is like a lake. To clean up the lake, one must first eliminate the sources of pollution." Of course, corrupted data is only one piece of the puzzle. The suggestion here is that hackers are able to not only disrupt networks, but also applications and data. Indeed, many researchers feel that if applications can be protected, it may not be necessary to defend networks quite so rigorously. The notion of accountability for software and data quality naturally leads to the question of manufacturers' liability for software. Several years ago a study of COTS products used students as attackers, with the following results [Lindqvist 98]:

- Almost all attackers performed successful intrusions.
- Several of the intrusions gave the attacker administrator privileges.
- The Internet provides a vast amount of information on how to successfully attack common systems.
- Many attackers broke into the system by using exploit scripts published on the Internet.

Some companies are demanding liability clauses in contracts with vendors, holding the vendors responsible for any security breach connected to their software [Fisher 02]. Chris Darby, CEO of @Stake, Inc., says "That language is going to become more and more prevalent." Karl Keller, president of IS Power Inc., says, "Contractual liability is a great motiva-

tor. I'm encouraged that liability for vulnerabilities is entering into contracts. Secure programming is a mindset…it will require constant reinforcement….You can be sure that when relatively simple buffer overflows are conquered, fewer but more sophisticated vulnerabilities will be found." Robert Weiler says "Companies are increasingly concerned about the threat of being liable as a result of negligence in security.…To combat the threat of liability, business should adopt and be able to prove compliance to information security standards and best practices" [Weiler 02].

Software liability is a subject of intense discussion. A recent series of articles by two experts in the field indicates just how different individual viewpoints can be. On the one hand it is argued that it is not practical for consumers to create their own security software [Ryan 03]. It is reasonable to assume that manufacturers of such products should ensure the reliability of these products. The notion of fitness for use suggests that such software provides a basis for strict liability. Strict liability has been applied in personal injury cases (when a consumer is physically injured by a defective product), but not so much in property damage cases, and even less in economic damage cases. In these latter cases, the courts often accept contractual disclaimers of liability, such as those found on shrink-wrapped software.

Network security and the associated liability issues are also under discussion. A negligence argument can be made in support of liability for insecure networks. This argument would need to show that the insecure party "had a duty to use reasonable care in securing its computer systems, breached that duty by failing to employ adequate security, and was a reasonably recognized cause of actual damages" [Kenneally 02].

Since strict liability cannot be applied in all cases, the courts need to build on other concepts, such as "warranty of fitness, misrepresentation, abnormal danger, negligence, fraud, lack of clarity and unconscionability to find liability for all security product failures" [Ryan 03]. Note that the doctrine of unconscionability has been applied to contracts, and when safety is at issue, disclaimers have been invalidated. This argument suggests that there is at least a class of software products for which liability arguments can be made successfully in the U.S. legal system.

The opposing view suggests that liability is not the appropriate tool for reducing the number and severity of software security holes [Heckman 03]. This argument suggests that software does not have the characteristics of other products (e.g., automobiles, ladders, etc.) that would support legal liability. For one thing, a liability case could be in the courts for years, and software, having a relatively short lifecycle, could become obsolete before the case comes to trial. Thus, even if software liability is confirmed, the outcome could be irrelevant.

Another argument against software liability is that manufacturers cannot predict the purpose for which software will be used or where and how it will be installed. This lack of predictability makes it impossible for manufacturers to warrant software for fitness of use. Many

commercial software products allow users to tailor the products by use of preferences. This is a flexibility that is demanded by users, and yet one which increases the lack of predictability for how a given software product may be used.

The courts have in the past made distinctions between manufacturers' defects and design defects. The notion of software liability typically rests on design defects rather than defects of manufacture. A defect of manufacture for software, for example, could occur if a software CD were improperly produced and the product either could not be installed or was otherwise invalid. Liability actions would seldom take place in such a case, because the standard disclaimers usually provide for replacement or refund of the purchase price.

The final argument that liability is not appropriate for software suggests that many software manufacturers would get out of the business if they were faced with liability suits, leaving few remaining software manufacturers to service a large and burgeoning marketplace.

4.2 UCITA

4.2.1 Overview of UCITA

The Uniform Computer Information Transactions Act (UCITA) was developed over a six-year period by the National Conference of Commissioners on Uniform State Law (NCCUSL). "[NCCUSL] is now in its 112th year. The organization comprises more than 300 lawyers, judges, and law professors, appointed by the states as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, to draft proposals for uniform and model laws on subjects where uniformity is desirable and practicable, and work toward their enactment in legislatures" [NCCUSL 03]. UCITA was developed in a series of more than 20 three-day meetings by the Drafting Committee.[10] Each session was attended by as many as 120 interested observers. The NCCUSL approved UCITA. UCITA is a uniform statute that is intended to codify current law and practice in contracts for computer information. UCITA does not purport to answer every question, but to provide a framework within which courts can analyze questions.

The rationale for development of UCITA is the combination of the growth in the information economy with no corresponding uniform framework for licensing. UCITA sets up a series of default rules that apply in the absence of a specific agreement by the interested parties. UCITA was first adopted in the state of Virginia after a one-year study period by a special legislative committee. Although many amendments were considered, in the end UCITA was adopted with no significant amendment and took effect in the year 2000. It was also enacted in the year 2000 in the state of Maryland.

[10] Dively, M. J. "The Uniform Computer Information Transactions Act." Presentation at the SEI, March, 2003.

UCITA's scope is limited to transactions in computer information. A transaction in computer information is "an agreement or the performance of it to create, modify, transfer, or license computer information or informational rights in computer information." Computer information is defined as information in electronic form, which is obtained from or through the use of a computer, or which is in a form that is capable of being processed by a computer. Under UCITA, contracts are allowed to be made computer to computer or human to computer. Further, it codifies existing case law for shrinkwrap and clickwrap contracts. This is an extremely important point, which we will come back to when we discuss the controversy surrounding UCITA.

Section 105 states that UCITA is preempted by federal law and subject to state consumer protection laws. Contracts under UCITA may not contain terms that violate fundamental public policy. For shrinkwrap contracts, a licensee may not manifest assent to the terms of a license until it has had an opportunity to review the terms. If the license is presented after payment, the license must provide a cost-free right of return for the licensee. For clickwrap contracts, similar rules prevail. The licensee must have the opportunity to review the terms prior to manifesting assent. Pre-transaction disclosure of terms is encouraged in Internet transactions. "You 'manifest assent' if, after having an opportunity to review a record or term, you authenticate the record or term, or intentionally engage in conduct or make statements with reason to know that the other party or its electronic agent may infer from the conduct or statement that you assent to the record or term.…A person has an opportunity to review a record or term only if it is made available in a manner that ought to call it to the attention of a reasonable person and permit review."[11] For the first time, UCITA creates statutory implied warranties in information transactions. The warranties include non-interference and non-infringement, merchantability of the computer program, informational content, fitness for the licensee's purpose, and system integration.

4.2.2 UCITA Controversy

The UCITA framework was perceived as providing protection to vendors from liability. Those involved in development of UCITA, on the other hand, argue that all UCITA does is to transfer existing legal results from one medium to another. Many responsible professional software organizations and engineers feel that UCITA goes too far in protecting vendors from liability. These issues continue to be a subject of considerable discussion.

The viewpoint of the UCITA authors is that consumer advocates sought broad consumer protections within UCITA, rather than leaving it to individual states to develop. Development of consumer protection by individual states is traditional for consumer law. The original UCITA positions on reverse engineering, public comment, and electronic self-help were opposed. The original positions on default rules for number of users and duration of license were sig-

[11] Dively, M. J. "The Uniform Computer Information Transactions Act." Presentation at the SEI, March, 2003.

nificantly opposed. Some professionals are opposed to shrinkwrap contracts on principle. This latter point was not responded to.

In 2001 the American Bar Association (ABA) appointed a special working group to evaluate UCITA. A three-day meeting was held to discuss concerns, and the ABA issued a report suggesting 11 specific changes. Some of the substantive changes made to UCITA as a result include the following [UCITA 02]:

- **Electronic Self-Help Banned**. Vendors (called licensors, mainly) of digital information, including software, may not disable the use of that information by electronic means if there is a breach of an information contract. Vendors have an expedited remedy for a material breach of contract in a court of law.
- **A State's Consumer Protection Law Trumps UCITA.** An information contract is expressly subject to and may not waive any consumer protection provided in state or federal law. Included are laws providing for conspicuous disclosure, unfair or deceptive trade practice laws, and laws relating to electronic signatures and records.
- **Right to Criticize Protected.** Information contract terms that prohibit criticism of an information product are unenforceable. Parties may contract in a manner consistent with other law such as the law of trade secrets.
- **Remedies for Known Material Defect Preserved**. Remedies for a known material defect of a product are expressly made available as fully as for defective goods or services.
- **Reverse Engineering for Interoperability Expressly Authorized**. An information contract may not prohibit reverse engineering that is done for the purpose of making an information product work together with other information products.
- **Special Open-Source Software Provisions.** Open-source software is expressly not covered by the act if only copyright permission is given and is not part of a contract. If there is a contract, there are no implied warranties if there is no commercial gain from the transaction.

NCCUSL also adopted 38 amendments to improve clarity, with no substantive effect. The ABA House of Delegates was to consider approval of UCITA in February of 2003; however, the ABA preferred not to take a position on UCITA when it became clear that a consensus was unlikely to emerge. UCITA is under consideration in additional states. The American Electronics Association (AEA), a high-tech trade association with over 3000 members, has endorsed UCITA. As noted above, software professional organizations and individual professionals continue to express concern.

4.3 The Microsoft Security Push

Microsoft has made a major commitment to security improvements in their software. The now famous Gates memo follows:

From: Bill Gates
Sent: Tuesday, January 15, 2002 2:22 PM
To: Microsoft and Subsidiaries: All FTE
Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing—or able—to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

When we started work on Microsoft .NET more than two years ago, we set a new direction for the company—and articulated a new way to think about our software. Rather than developing standalone applications and Web sites, today we're moving towards smart clients with rich user interfaces interacting with Web services. We're driving the XML Web services standards so that systems from all vendors can share information, while working to make Windows the best client and server for this new era.

There is a lot of excitement about what this architecture makes possible. It allows the dreams about e-business that have been hyped over the last few years to become a reality. It enables people to collaborate in new ways, including how they read, communicate, share annotations, analyze information and meet.

However, even more important than any of these new capabilities is the fact that it is designed from the ground up to deliver Trustworthy Computing. What I mean by this is that customers will always be able to rely on these systems to be available and to secure their information. Trustworthy Computing is computing that is as available, reliable and secure as electricity, water services and telephony.

Today, in the developed world, we do not worry about electricity and water services being available. With telephony, we rely both on its availability and its security for conducting highly confidential business transactions without worrying that information about who we call or what we say will be compromised. Computing falls well short of this, ranging from the individual user who isn't willing to add a new application because it might destabilize their system, to a corporation that moves slowly to embrace e-business because today's platforms don't make the grade.

The events of last year—from September's terrorist attacks to a number of malicious and highly publicized computer viruses—reminded every one of us how important it is to ensure the integrity and security of our critical infrastructure, whether it's the airlines or computer systems.

Computing is already an important part of many people's lives. Within ten years, it will be an integral and indispensable part of almost everything we do. Microsoft and the computer industry will only succeed in that world if CIOs, consumers and everyone else sees that Microsoft has created a platform for Trustworthy Computing.

Every week there are reports of newly discovered security problems in all kinds of software, from individual applications and services to Windows, Linux, Unix and other platforms. We have done a great job of having teams work around the clock to deliver security fixes for any problems that arise. Our responsiveness has been unmatched—but as an industry leader we can and must do better. Our new design approaches need to dramatically reduce the number of such issues that come up in the software that Microsoft, its partners and its customers create. We need to make it automatic for customers to get the benefits of these fixes. Eventually, our software should be so fundamentally secure that customers never even worry about it.

No Trustworthy Computing platform exists today. It is only in the context of the basic redesign we have done around .NET that we can achieve this. The key design decisions we made around .NET include the advances we need to deliver on this vision. Visual Studio .NET is the first multi-language tool that is optimized for the creation of secure code, so it is a key foundation element.

I've spent the past few months working with Craig Mundie's group and others across the company to define what achieving Trustworthy Computing will entail, and to focus our efforts on building trust into every one of our products and services. Key aspects include:

Availability: Our products should always be available when our customers need them. System outages should become a thing of the past because of a software architecture that supports redundancy and automatic recovery. Self-management should allow for service resumption without user intervention in almost every case.

Security: The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and build into their applications.

Privacy: Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information, including controlling the use of email they send.

Trustworthiness is a much broader concept than security, and winning our customers' trust involves more than just fixing bugs and achieving "five-nines" availability. It's a fundamental challenge that spans the entire computing ecosystem, from individual chips all the way to global Internet services. It's about smart software, services and industry-wide cooperation.

There are many changes Microsoft needs to make as a company to ensure and keep our customers' trust at every level—from the way we develop software, to our support efforts, to our operational and business practices. As software has become ever more complex, interdependent and interconnected, our reputation as a company has in turn become more vulnerable. Flaws in a single Microsoft product, service or policy not only affect the quality of our platform and services overall, but also our customers' view of us as a company.

In recent months, we've stepped up programs and services that help us create better software and increase security for our customers. Last fall, we launched the Strategic Technology Protection Program, making software like IIS and Windows .NET Server secure by default, and educating our customers on how to get—and stay—secure. The error-reporting features built into Office XP and Windows XP are giving us a clear view of how to raise the level of reliability. The Office team is focused on training and processes that will anticipate and prevent security problems. In December, the Visual Studio .NET team conducted a comprehensive review of every aspect of their product for potential security issues. We will be conducting similarly intensive reviews in the Windows division and throughout the company in the coming months.

At the same time, we're in the process of training all our developers in the latest secure coding techniques. We've also published books like "Writing Secure Code," by Michael Howard and David LeBlanc, which gives all developers the tools they need to build secure software from the ground up. In addition, we must have even more highly trained sales, service and support people, along with offerings such as security assessments and broad security solutions. I encourage everyone at Microsoft to look at what we've done so far and think about how they can contribute.

But we need to go much further.

In the past, we've made our software and services more compelling for users by adding new features and functionality, and by making our platform richly extensible. We've done a terrific job at that, but all those great features won't matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve. A good example of this is the changes we made in Outlook to avoid email-borne viruses. If we discover a risk that a feature could compromise someone's privacy, that problem gets solved first. If there is any way we can better protect important data and minimize downtime, we should focus on this. These principles should apply at every stage of the development cycle of every kind of software we create, from operating systems and desktop applications to global Web services.

Going forward, we must develop technologies and policies that help businesses better manage ever larger networks of PCs, servers and other intelligent devices, knowing that their critical business systems are safe from harm. Systems will have to become self-managing and inherently resilient. We need to prepare now for the kind of software that will make this happen, and we must be the kind of company that people can rely on to deliver it.

This priority touches on all the software work we do. By delivering on Trustworthy Computing, customers will get dramatically more value out of our advances than they have in the past. The challenge here is one that Microsoft is uniquely suited to solve.

Bill

This memo resulted in some significant changes within Microsoft, as we see in a retrospective discussion a year later by Michael Howard, a Senior Security Program Manager at Microsoft, and Steve Lipner, Director of Security Assurance at Microsoft [Howard 03]. For one thing, during the months of February and March 2002, all Windows feature development stopped, while the design, code, test plans, and documentation were analyzed by the Microsoft team. For a company that is market-driven to provide more and better features, this is an unusual step, and indicates just how seriously this security initiative was. Training courses were developed and delivered to support the "Windows Security Push." As part of this effort, it was observed that security is not just a "layer" that is added after the fact, but a consideration that pervades all of development. In Howard and Lipner's words, "Secure software means paying attention to detail, understanding threats, building extra defensive layers, reducing attack surface, and using security defaults." A key element of the design process was the construction of threat models. In this regard, there is some parallelism between the Microsoft effort and the guidance of the Common Criteria. The steps in constructing threat models at Microsoft are

1. Decompose the application to determine the system's boundaries or scope.

2. Determine threat targets and categories using components from the decomposition process as threat targets, and determine the threat categories for each target.
3. Identify attack mechanisms using a threat or attack tree approach.
4. Respond to the threats with mitigation techniques appropriate to each threat.

Obviously, this was and continues to be a massive effort for Microsoft. The stated reasons for the "push" are the need for more secure platforms to support future solutions, a prior successful push effort on .NET, and the ability to respond to a new generation of Internet threats. Another stated reason for the push is that customers will perceive improved security in the products. One has to wonder, however, whether a concern about possible future liability is also part of Microsoft's agenda. Regardless of the motives, this effort has great potential benefits for the consumer of commercial software products.

4.4 Liability Implications for the U.S. Government

Critical infrastructure organizations rely on the use of COTS software in their systems. COTS products often appear not just at the lowest operating system level, but often as an intermediate product. At this point, it is not clear how the liability issue will play out in the U.S., let alone internationally. In the U.S., unless some federal laws are enacted, it appears that each state could end up handling liability slightly differently. This brings to mind the differences among states in the aftermath of the Justice Department action against Microsoft with regard to monopolistic practices. One could envision different states having different liability laws and/or different legal results.

We would recommend that U.S. policymakers track liability law and actions, such as adoption of UCITA by individual states, and track similar measures internationally. Lack of uniformity in liability law could make it difficult to create the appropriate consistency in cyber security. In addition, liability law could impact contracts for COTS software worldwide. Since the COTS software market is dominated by the U.S., the U.S. government needs to stay current with what is happening in this area.

5 Critical Infrastructure Risk Reduction

Ultimately, one of the objectives of this report is to recommend steps towards reduction of risk to critical infrastructure. We find, however, that this is not a simple issue. First of all, there is no consensus on the extent of the risks posed by a cyber attack on critical infrastructure. Although it is generally agreed that such attacks are technically feasible, there is no agreement on the likely impact of such an attack. Some feel that such an attack could be crippling. Others feel that it would be more of an annoyance than a threat. There are also distinctions between the threat to military infrastructure versus other infrastructure such as energy, water, and transportation.

5.1 Risks to Military Infrastructure

The military has focused much attention on the cyber threat to military infrastructure. It has employed multi-level security classifications, security measures such as encryption and authentication, emergency preparedness, and response to cyber attacks. However, it is worth noting that the military has much more dependence on commercial infrastructure, such as telephone networks, than was once the case [Buda 01]. There is also a dependence on commercial software and hardware in many military systems. It was once the case that military systems were developed using custom hardware and software. In recent years, however, the military and government in general have decided to use commercial platforms and software in order to contain costs. This does indeed result in cost containment, but can result in greater risks to networks and systems. After all, an attack on a vendor's software can be attempted whether the software resides on a military system or a commercial system. So, we can conclude that all government systems, military or otherwise, have some susceptibility to cyber attacks.

Although the risks to military systems may be low, if the risks are realized then the consequences are high. Therefore, although not the primary focus of this report, vigilance is needed to safeguard military systems, and the commercial systems on which they depend. It is important for military organizations to quantify their dependence on commercial systems and infrastructure and to protect against problems, no matter how unlikely they may be.

5.2 Risks to Critical Infrastructure

We have seen the full range of views on how vulnerable critical infrastructure may be to cyber attack. Such infrastructure includes power, water, and transportation. We have seen many warnings about cyber threats to critical infrastructure. However, in recent years, the terrorist threats have tended to be physical. We have seen many articles about presumed terrorists making inquiries about crop-dusting, and acting in a suspicious manner in the vicinity of reservoirs. We have also seen physical attacks on transportation, ranging from the 9/11 attacks to train derailments. However, we have seen little in the way of cyber attacks by terrorists [Lewis 02]. Moreover, given the diversity of systems that support critical infrastructure, some researchers feel that cyber attacks would be little more than annoyance. In their view, it's possible that power could be lost to some part of the United States for a few hours, but this is hardly a disaster. They believe that it's likely that a cyber attack, if one occurred, would be used to bolster a physical attack, but probably to little effect. Furthermore, these researchers feel there is no evidence that such sophisticated scenarios are under development either by terrorists or hostile nation states.

A strongly opposing view can be seen in a recent PBS documentary focused on the work of Richard Clarke. In this documentary, it was indicated that it would be possible for a cyber attack to cause power outages of up to six months. Researchers find continuing evidence of attempts to gather information about critical infrastructure networks, possibly in preparation for future attacks. This view holds that isolation and diversity are in fact decreasing. As an example, many critical infrastructure systems depend on supervisory control and data acquisition (SCADA) components.

On the other hand, insiders frequently report single points of failure in critical infrastructure systems. An attack on one of those points could have serious consequences. Moreover, the argument that such an attack has not occurred does not mean that such an attack cannot or will not occur. After all, prior to 9/11, one could argue that such a massive attack could not occur. Nevertheless, it did. So what we must do is to develop worst-case scenarios and guard against them. This needs to be done not just in the United States, but in other countries as well. We have an enormous dependence on international resources, such as foreign oil, food, international stock markets, stability of international monetary systems, etc.

It has been argued that during 9/11 there were critical infrastructure failures [Krings 03]. For example, local communications were overwhelmed. Organizations with distributed physical space and distributed communications facilities recovered more quickly than those with centralized facilities in the World Trade Center. More recently, we have seen attacks on infrastructure with unanticipated consequences. The "Slammer" worm resulted in outages of hundreds of ATM machines and critical infrastructure elements such as some 911 emergency response systems [Cybenko 03].

We believe that critical infrastructure risk reduction is an essential area of research and worthy of executive management attention. New modeling techniques are needed to support study of critical infrastructure failures [Krings 03].

5.3 Implications for the U.S. Government

The U.S. government and its policy makers should be concerned with risk of critical infrastructure failure or compromise. It is particularly important since much of the critical infrastructure crosses national boundaries. We recommend that the U.S. government be proactive in activities to identify and mitigate such risk. This could include standards development, studies of specific classes of systems (e.g., aviation) and associated risk reduction, and treaties to support critical infrastructure protection. The United States should undertake such activities both unilaterally and in concert with other nations.

6 Conclusions

In this report we have discussed various information security topics as they relate to the U.S. government and its policy makers. These areas include standardization of international law, standards for secure software, software manufacturers' liability, and critical infrastructure risk reduction.

The U.S. government has participated in many of these areas, and in some cases has taken on a leadership role. Note that all of these areas represent work in progress. There are no "final" conclusions for any of the areas. Each has involvement of international boards or other interested parties, and each is undergoing active scrutiny and modification.

The U.S. government has a vested interest in all of these areas; however, its resources are limited. It is therefore appropriate for the U.S. government to carefully weigh its level of involvement. For the very detailed standards, such as IETF standards for secure software, it is probably best for the U.S. government to keep abreast of the effort and track it, but not necessarily take on a leadership role. For other areas, such as standardization of international law, it is more appropriate for the U.S. government to take a leadership role. It is likely that the area of software liability will evolve in U.S. and international court settings. It is appropriate for the U.S. government to track this area, but not necessarily to take a leadership role or try to influence outcomes. Critical infrastructure risk reduction is extremely important for the U.S. government, given the international implications, and it would be worthwhile for the U.S. government to have a leadership role in this area. A multi-lateral capability to collect data on software and system failures and to share information about attacks would be very useful.

Critical infrastructure risk reduction remains one of the more controversial areas, and the area where much remains to be done. If only one action could be taken, we recommend that the U.S. government dedicate some resource to this area, attempting to quantify and mitigate the risk, particularly as it relates to energy, water, transportation, and other critical infrastructure elements.

This report represents a snapshot as of a specific point in time. The field is not static, and these recommendations should be revisited and updated periodically. As information security threats continue to evolve, our responses must also evolve.

References

URLs are valid as of the publication date of this document.

[Abrams 00] Abrams, M. D. & Brusil, P. J. "Application of the Common Criteria to a System: A Real-World Example." *Computer Security Journal 16*, 2 (Spring 2000): 11-21.

[Bergeron 99] Bergeron, J.; Debbabi, M.; Erhioui, M. M.; & Ktari, B. "Static Analysis of Binary Code to Isolate Malicious Behaviors," 184-189. *Proceedings of IEEE 8th International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'99).* Los Alamitos, CA: IEEE Computer Society, 1999.

[Buda 01] Buda, G.; Choi, D.; Graveman, R.; & Kubic, C. "Security Standards for the Global Information Grid," 617-621, Vol.1. *Proceedings of MILCOM 2001—Communications for Network-Centric Operations: Creating the Information Force*. Vienna, VA, Oct. 28-31, 2001. Piscataway, NJ: IEEE Computer Society, 2001.

[Caplan 99] Caplan, K. & Sanders, J. L. "Building an International Security Standard." *IEEE IT Professional 1*, 2 (March/April 1999): 29-34.

[Chappell 99] Chappell, B. L.; Marlow, D. T.; Irey, P. M., IV; & O'Donoghue, K. "An Approach for Measuring IP Security Performance in a Distributed Environment," 389-394. *Parallel and Distributed Processing: Proceedings of the 11th IPPS/SPDP Workshops Held in Conjunction with the 13th International Parallel Processing Symposium and the 10th Symposium on Parallel and Distributed Processing*. San Juan, Puerto Rico, April 12-16, 1999. Berlin, Germany: Springer-Verlag, 1999 (ISBN 3-540-65831-9).

[Coallier 03] Coallier, F. "International Standardization in Software and Systems Engineering." *CrossTalk 16*, 2 (February 2003): 18-22. <http://www.stsc.hill.af.mil/crosstalk/2003/02/coallier.html>.

[Convention 01] "30 states sign the Convention on Cybercrime at the opening ceremony." <http://press.coe.int/cp/2001/875a(2001).htm> (November 23, 2001).

[Cybenko 03] Cybenko, G. "Sapphire/Slammer Redux." From the Editor, *IEEE Security & Privacy 1*, 2 (March/April 2003): 6.

[Dean 02] Dean, J. C. & Li, Li. "Issues in Developing Security Wrapper Technology for COTS Software Products," 76-85. *COTS-Based Software Systems: Proceedings of ICCBSS 2002.* Orlando, FL, Feb. 4-6, 2002 (LNCS 2255). Berlin, Germany: Springer-Verlag, 2002.

[DOJ 00] U.S. Department of Justice. "Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime (Draft 24REV2)." <http://www.usdoj.gov/criminal/cybercrime /COEFAQs.htm> (December 1, 2000).

[Doraswamy 99] Doraswamy, N. & Harkins, D. *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Upper Saddle River, NJ: Prentice Hall PTR, 1999.

[Ellison 97] Ellison, Robert; Fisher, David; Linger, Richard; Lipson, Howard; Longstaff, Thomas; & Mead, Nancy. *Survivable Network Systems: An Emerging Discipline* (CMU/SEI-97-TR-013, ADA341963). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997 < http://www.sei.cmu.edu/publications /documents/97.reports/97tr013/97tr013abstract.html >.

[Fisher 02] Fisher, D. "Contracts Getting Tough on Security." *eWeek*, April 15, 2002 <http://www.eweek.com/article2/0,3959,9921,00.asp>.

[Fumy 98] Fumy, W. & Haas, I. "Security Techniques for the Global Information Infrastructure," 3141 -3146, Vol. 6. *Proceedings of Global Telecommunications Conference, 1998: The Bridge to Global Integration*. IEEE. Piscataway, NJ: IEEE Computer Society, 1998.

[Germanow 02] Germanow, A.; Wysopal, C.; Geer, D.; & Darby, C. "The Injustice of Insecure Software." <http://www.atstake.com/research /reports/index.html> (February 2002).

[Heckman 03] Heckman, C. “Two Views on Security Software Liability: Using the Right Legal Tools.” On the Horizon, *IEEE Security & Privacy 1*, 1 (2003): 70-72.

[Herrmann 01] Herrmann, D. & Keith, S. “Application of Common Criteria to Telecomm Services: A Case Study.” *Computer Security Journal XVII*, 2 (Spring 2001): 21-28.

[Hollingworth 00] Hollingworth, D. & Redmond, T. “Enhancing Operating System Resistance to Information Warfare,” 1037-1041, Vol. 2. *Proceedings of MILCOM 2000—21st Century Military Communications: Architectures and Technologies for Information Superiority*. IEEE 2000. Piscataway, NJ: IEEE Computer Society, 2000.

[Howard 03] Howard, M. & Lipner, S. “Inside the Windows Security Push.” *IEEE Security & Privacy 1*, 1 (2003): 57-61.

[Ibrahim 02] Ibrahim, R.; Jarzombek, J.; & Ashford, M. “Integrity Assurance: Extending the CMMI & iCMM for Safety and Security.” <http://www.dtic.mil/ndia/2002cmmi/ibrahim3a2.pdf> (2002).

[IETF 03] The Internet Engineering Task Force. <http://www.ietf.org>.

[IPsec 03] IP Security Protocol (ipsec) Charter. <http://www.ietf.org/html.charters/ipsec-charter.html>.

[Jaquith 02] Jaquith, A., “The Security of Applications: Not All Are Created Equal.” <http://www.atstake.com/research/reports/index.html> (February 2002).

[Kenneally 02] Kenneally, E. “Who’s Liable for Insecure Networks?” *IEEE Computer 25*, 6 (June 2002): 93-94.

[Krings 03] Krings, A. & Oman, P. “A Simple GSPN for Modeling Common Mode Failures in Critical Infrastructures.” *Proceedings of the 36th Hawaii International Conference on System Sciences*. Hawaii, Jan. 6-9, 2003. Piscataway, NJ: IEEE Computer Society, 2003.

[Lewis 02] Lewis, J. A. “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.” Center for Strategic & International Studies. <http://www.csis.org/tech/0211_lewis.pdf> (December 2002).

[Lindqvist 98] Lindqvist, U. & Jonsson, E. “A Map of Security Risks Associated with Using COTS.” *IEEE Computer 31,* 6 (June 1998): 60-66.

[Lipson 01] Lipson, H.F., Mead, N.R., & Moore, A.P., *Can We Ever Build Survivable Systems from COTS Components?* (CMU/SEI-2001-TN-030, ADA399238). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2002. <http://www.sei.cmu.edu /publications/documents/01.reports/01tn030.html>.

[Lipson 02] Lipson, H. F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (CMU/SEI-2002-SR-009, ADA408853). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2002. <http://www.sei.cmu.edu /publications/documents/02.reports/02sr009.html>.

[McCullagh 00] McCullagh, D. “Cybercrime Solution Has Bugs.” *Wired News*, May 3, 2000. <http://www.wired.com/news/politics/0,1283,36047,00.html>.

[Mead 01] Mead, N. R.; Lipson, H. F.; & Sledge, C.A. “Toward Survivable COTS-Based Systems.” *Cutter IT Journal 14*, 2 (February 2001): 4-11.

[NCCUSL 03] Uniform Law Commissioners—The National Conference of Commissioners on Uniform State Laws. <http://www.nccusl.org/>.

[O’Guin 99] O’Guin, S.; Williams, C. K.; & Selimis, N. “Application of Virtual Private Networking Technology to Standard-Based Management Protocols Across Heterogeneous Firewall-Protected Networks,” 1251-1255. *Proceedings of MILCOM 1999—IEEE Military Communications Conference*. Atlantic City, NJ, Nov. 1-3, 1999. Piscataway, NJ: IEEE Computer Society, 1999.

[Patel 01] Patel, V. & McParland, T. “Public Key Infrastructure for Air Traffic Management Systems,” 7.A.5-1-7.A.5-7. *20th Digital Avionics Systems Conference Proceedings.* Daytona Beach, FL, Oct. 14-18, 2001. Piscataway, NJ: IEEE Computer Society, 2001.

[Pautke 03] Pautke, R. W. “To Clean or Not to Clean, That Is the Question.” *Cutter IT Journal 16,* 1 (January 2003): 11-12.

[Payne 01] Payne, C. N., Jr. & Smith, R.E. “The Releasable Data Products Framework,” 203-213. *Proceedings of DISCEX-II: 2nd DARPA Information Survivability Conference and Exposition*. Anaheim, CA, June 12-14, 2001. Los Alamitos, CA: IEEE Computer Society, 2001.

[Payton 02] Payton, J.; Jonsdottir, G.; Flagg, D.; & Gamble, R. “Merging Integration Solutions for Architecture and Security Mismatch,” 199-208. *Proceedings of ICCBSS 2002.* Orlando, FL, Feb. 4-6, 2002 (LNCS 2255). Berlin, Germany: Springer-Verlag, 2002.

[PP 02] Protection Profile (PP) Consistency Guidance for Basic Robustness, Release 1.1, September 2002. <http://www.iatf.net/protection_profiles /file_serve.cfm?chapter=guidance.pdf>.

[Redman 03] Redman, T. C. “Opening Statement.” *Cutter IT Journal 16*, 1 (January 2003): 2-5.

[Rosen 02] Rosen, M. “The US-EU Convention on Cybercrime.” *UCLA Journal of Law and Technology Notes 19*. <http://www.lawtechjournal.com/notes/2002 /19_020819_rosen.php>.

[Roy 00] Roy, A. “Security Strategy for US Air Force to Use Commercial Data Link,” 7E4/1-8. *19th Digital Avionics Systems Conference Proceedings.* Philadelphia, PA, Oct. 7-13, 2000. Piscataway, NJ: IEEE Computer Society, 2000.

[Ryan 03] Ryan, D. J. “Two Views on Security Software Liability: Let the Legal System Decide.” *IEEE Security & Privacy 1*, 1 (2003): 70-72.

[UCITA 02] The National Conference of Commissioners on Uniform State Laws. UCITA 2002 Revisions Memorandum and Chart: August 23, 2002. <http://www.nccusl.org/nccusl/ucita/UCITA_082602_MEMO_and_CHART.pdf>.

[Vetterling 02] Vetterling, M.; Wimmel, G.; & Wisspeintner, A. "Secure Systems Development Based on the Common Criteria: The PalME Project," 129-138. *Proceedings of SIGSOFT 2002/FSE-10*. Nov. 18-22, 2002, Charleston, SC. New York, NY: Association for Computing Machinery, 2002.

[Weiler 02] Weiler, R. "Decision Support: You Can't Outsource Liability for Security." *InformationWeek*, August 26, 2002. <http://www.informationweek.com/story/IWK20020822S0003>.

[West-Brown 99] West-Brown, M. & Kossakowski, K-P. "International Infrastructure for Global Security Incident Response." CERT Coordination Center, Carnegie Mellon University, June 4, 1999. <http://www.cert.org/inter_infra/inter_infra.pdf>.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	June 2003	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
International Liability Issues for Software Quality	F19628-00-C-0003

6. AUTHOR(S)

Nancy R. Mead, PhD

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2003-SR-001

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report focuses on international law related to cybercrime, international information security standards, and software liability issues as they relate to information security for critical infrastructure applications. Each area is explored and implications for U.S. policy and efforts to create cyber security policy worldwide are discussed. Recommendations are made for U.S. government participation and leadership.

This report is one of a series of reports on U.S. policy by the CERT Coordination Center. Prior reports focused on international infrastructure for global security incident response and the technical challenges and global policy issues of tracking and tracing cyber attacks.

14. SUBJECT TERMS	15. NUMBER OF PAGES
international law, cybercrime, international information security standards, software liability, information security, critical infrastructure applications, software quality	54

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL