Cyber Security - Growing Risk from Growing Vulnerability

Testimony of Richard D. Pethia

Director, CERT® Centers

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213

Before the

House Select Committee on Homeland Security

Subcommittee on Cybersecurity, Science, and Research and Development

Hearing on

Overview of the Cyber Problem – A Nation Dependent and Dealing with Risk

June 25, 2003

1. Introduction

Mr. Chairman and members of the Subcommittee: My name is Rich Pethia. I am the director of the CERT® Centers, part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. We have 14 years of experience with computer and network security. The CERT Coordination Center (CERT/CC) was established in 1988, after an Internet "worm" became the first Internet security incident to make headline news, acting as a wake-up call for network security. In response, the CERT/CC was established at the SEI. The center was activated in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled well over 200,000 incidents and cataloged more than 8,000 computer vulnerabilities.

Thank you for the opportunity to testify on cyber security problem. Today I will discuss the vulnerability of information technology on the Internet and steps I believe we must take to better protect our critical systems from future attacks.

The current state of Internet security is cause for concern. Vulnerabilities associated with the Internet put users at risk. Security measures that were appropriate for mainframe computers and small, well-defined networks inside an organization are not effective for the Internet, a complex, dynamic world of interconnected networks with no clear boundaries and no central control. Security issues are often not well understood and are rarely given high priority by many software developers, vendors, network managers, or consumers.

Government, commercial, and educational organizations depend on computers to such an extent that day-to-day operations are significantly hindered when the computers are "down." Currently many of the day-to-day operations depend upon connections to the Internet, and new connections are continuously being made to the Internet. Use of the Internet enhances the ability of organizations to conduct their activities in a cost-effective and efficient way. However, along with increased capability and dependence comes increased vulnerability. It is easy to exploit the many security holes in the Internet and in the software commonly used in conjunction with it; and it is easy to disguise or hide the true origin and identity of the people doing the exploiting. Moreover, the Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries.

Computers have become such an integral part of American business and government that computer-related risks cannot be separated from general business, health, and privacy risks. Valuable government and business assets are now at risk over the Internet. For example, customer and personnel information may be exposed to intruders. Financial data, intellectual property, and strategic plans may be at risk. The widespread use of databases leaves the privacy of individuals at risk. Increased use of computers in safety-critical applications, including the storage and processing of medical records data, increases the chance that accidents or attacks on computer systems can cost people their lives.

Techniques that have worked in the past for securing isolated systems are not effective in the world of unbounded networks, mobile computing, distributed applications, and dynamic computing that we live in today. Today there is rapid movement toward increased use of interconnected networks for a broad range of activities, including commerce, education, entertainment, operation of government, and supporting the delivery of health and other human services. Although this trend promises many benefits, it also poses many risks. In short, interconnections are rapidly increasing and opportunities to exploit vulnerabilities in the interconnected systems are increasing as well.

2. Key Factors in the Current State of Internet Security

The current state of Internet security is the result of many factors. A change in any one of these can change the level of Internet security and survivability.

- We are connecting everything with everything else. Because of the dramatically lower cost of communication and ease of connecting to the Internet, use of the Internet is replacing other forms of electronic communication. As critical infrastructure operators strive to improve their efficiency and lower costs, they are connecting formerly isolated systems to the Internet to facilitate remote maintenance functions and improve coordination across distributed systems. Operations of the critical infrastructures are becoming increasingly dependent on the Internet and are vulnerable to Internet based attacks.

- Cyber space and physical space are becoming one. Most threatening of all is the link between cyber space and physical space. Supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have for years been used to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems. Increasingly, these control systems are being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions. These computer-controlled and network-connected systems are potential targets of individuals bent on causing massive disruption and physical damage. This is not just theory; actual attacks have caused major operational problems. Attacks against wastewater treatment systems in Australia, for example, led to the release of hundreds of thousands of gallons of sludge.

- There is a continuing movement to distributed, client-server, and heterogeneous configurations. As the technology is being distributed, the management of the technology is often distributed as well. In these cases, system administration and management often fall upon people who do not have the training, skill, resources, or interest needed to operate their systems securely.

- The Internet is becoming increasingly complex and dynamic, but among those connected to the Internet there is a lack of adequate knowledge about the network and about security. The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, and Web sites result in vulnerabilities that intruders can exploit. Just one naive user with an easy-to-guess password increases an organization's risk.

- There is little evidence of improvement in the security features of most products; developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. The CERT Coordination Center routinely receives reports of new vulnerabilities. In 1995 we received an average of 35 new reports each quarter, 140 for the year. By 2002, the number of annual reports received had skyrocketed to over 4000. We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features. Until their customers demand products that are more secure, the situation is unlikely to change.

- When vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may be too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term—system maintenance is never-ending. Because managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the need for system administrators with strong security skills far exceeds the supply.

- Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.

- As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. Among security-conscious organizations, there is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations that have applied a "silver bullet" are lulled into a false sense of security and become less vigilant, but single solutions applied once are neither foolproof nor adequate. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.

- Compared with other critical infrastructures, the Internet seems to be a virtual breeding ground for attackers. Although some attacks seem playful (for example, students experimenting with the capability of the network) and some are clearly malicious, all have the potential of doing damage. Unfortunately, Internet attacks in general, and denial-of-service attacks in particular, remain easy to accomplish, hard to trace, and a low risk to the attacker. While some attacks require technical knowledge—the equivalent to that of a college graduate who majored in computer science—many other successful attacks are carried out by technically unsophisticated intruders. Technically competent intruders duplicate and share their programs and information at little cost, thus enabling novice intruders to do the same damage as the experts. In addition to being easy and cheap, Internet attacks can be quick. In a matter of seconds, intruders can break into a system; hide evidence of the break-in; install their programs, leaving a "back door" so they can easily return to the now-compromised system; and begin launching attacks at other sites.

- Attackers can lie about their identity and location on the network. Information on the Internet is transmitted in packets, each containing information about the origin and destination. Senders provide their return address, but they can lie about it. Most of the Internet is designed merely to forward packets one step closer to their destination with no attempt to make a record of their source. There is not even a "postmark" to indicate generally where a packet originated. It requires close cooperation among sites and up-to-date equipment to trace malicious packets during an attack. Moreover, the Internet is designed to allow packets to flow easily across geographical, administrative, and political boundaries. Consequently, cooperation in tracing a single attack may involve multiple organizations and jurisdictions, most of which are not directly affected by the attack and may have little incentive to invest time and resources in the effort. This means that it is easy for an adversary to use a foreign site to launch attacks at U.S. systems. The attacker enjoys the added safety of the need for international cooperation in order to trace the attack, compounded by impediments to legal investigations. We have seen U.S.-based attacks on U.S. sites gain this safety by first breaking into one or more non-U.S. sites before coming back to attack the desired target in the U.S.

3. Categories of vulnerabilities

Protecting any complex system (hardware, software, people, and physical plant) and insuring its successful operation in the face of attacks, accidents and failures is a difficult task. Vulnerabilities (weaknesses that can be exploited to compromise the operation of the system) can creep into the system in a variety of areas. Deciding which vulnerabilities really matter and effectively dealing with them, are key steps in an organization's risk management process.

For discussion, it is useful to separate sources of vulnerability into two major categories: weaknesses in the information technology (IT) products as supplied by the vendor(s); and weakness in the ways organizations manage and use the technology.

IT Product Vulnerabilities

As stated above, the number of vulnerabilities in IT products discovered each year is increasing dramatically: from 140 reported to the CERT/CC in 1995 to 4,129 reported in 2002. Each vulnerability represents a weakness in a product that can be exploited in some way to help an attacker achieve the objective of compromising a system.

Some of these vulnerabilities are deep-seated and difficult to correct because they are the result of architecture and design decisions that were made early in the product's development cycle (e.g. operating system architectures that allow the unconstrained execution of application software and thereby allow the easy propagation of viruses). In these cases, the vulnerabilities can only be removed by changing the basic architecture of the product. These types of fundamental changes often have consequences that affect other aspects of the product's operation. In some cases these side effects will cause applications that inter-operate with the product to "break" (i.e. the new version of the product is no longer compatible with earlier versions and users may need to rewrite their applications). These types of vulnerability are typically long-lived and product users must find some other way to protect themselves from attacks that attempt to exploit the vulnerability (e.g. invest in anti-virus software in order to detect and remove viruses before they operate on the vulnerable system).

Other vulnerabilities are easier to correct since they are the result of low-level design decisions or implementation errors (bugs in the programs). It is often that case that these types of vulnerability, once discovered, can quickly be corrected by the vendor and the corrections (oftentimes called "patches") made available to the customers. However, even though the corrections may be available quickly, it is not always the case that they can be deployed quickly. System operators need to insure that the corrections do not have unintended side-effects on their systems and typically test the corrections before deployment. Also, in the case of a widely used product, system operators must often update the software used in thousands of computers to deploy the correction. This in itself is a labor intensive and time consuming task.

In either case, IT product vulnerabilities are often long-lived with many Internet connected systems vulnerable to a particular form of attack many months after vendors produce corrections to the vulnerability that was exploited by the attack.

Weaknesses in Management and Operational Practice

The second major category of vulnerability includes weaknesses in the management and operational practices of system operators. Factors that lead to weaknesses in operational practices include things like:

- Lack of, ambiguous or poorly enforced organizational security policies and regulations; security roles and responsibilities that are not clearly defined or lack of accountability
- Failure to account for security when outsourcing IT services
- Lack of security awareness training for all levels of staff
- Poor account management or password management by all users
- Poor physical security leading to open access to important computers and network devices

- Weak configuration management practices that allow for vulnerable configurations
- Weak authentication practices that allow attackers to masquerade as valid system users
- Lack of vulnerability management practices that require system administrators to quickly correct important vulnerabilities
- Failure to use strong encryption when transmitting sensitive information over the network.
- Lack of monitoring and auditing practices that can detect attacker behavior before damage is done.

Weaknesses in any of these areas open the doors for attackers and give them opportunities to take advantage of the weaknesses to achieve their goals. Managing the risk associated with this category of vulnerability requires that organizations dedicate resources to the risk management task. Operations must be continuously assessed and corrective actions taken when needed.

4. Recommended Actions

Working our way out of the vulnerable position we are in requires a multi-pronged approach that helps us deal with the escalating near-term problem while at the same time building stronger foundations for the future. The work that must be done includes achieving these changes:

- Higher quality information technology products with security mechanisms that are better matched to the knowledge, skills, and abilities of today's system managers, administrators, and users
- Wider adoption of risk analysis and risk management policies and practices that help organizations identify their critical security needs, assess their operations and systems against those needs, and implement security improvements identified through the assessment process
- Expanded research programs that lead to fundamental advances in computer security
- A larger number of technical specialists who have the skills needed to secure large, complex systems
- Increased and ongoing awareness and understanding of cyber-security issues, vulnerabilities, and threats by all stakeholders in cyber space

Higher quality products: In today's Internet environment, a security approach based on "user beware" is unacceptable. The systems are too complex and the attacks happen too fast for this approach to work. Fortunately, good software engineering practices can dramatically improve our ability to withstand attacks. The solutions required are a combination of the following:

- Virus-resistant/virus-proof software – There is nothing intrinsic about digital computers or software that makes them vulnerable to viruses, which propagate

and infect systems because of design choices that have been made by computer and software designers. Designs are susceptible to viruses and their effects when they allow the import of executable code, in one form or another, and allow the unconstrained execution of that code on the machine that received it. Unconstrained execution allows code developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or untrusted sources. Some techniques to do this have been known for decades. Others, such as "sandbox" techniques, are more recent.

- Reducing implementation errors by at least two orders of magnitude – Most vulnerabilities in products come from software implementation errors. They remain in products, waiting to be discovered, and are fixed only after they are found while in use. Worse, the same flaws continue to be introduced in new products. Vendors need to be proactive, and adopt known, effective software engineering practices that dramatically reduce the number of flaws in software products.
- High-security default configurations – With the complexity of today's products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills and training. Small mistakes can leave systems vulnerable and put users at risk. Vendors can help reduce the impact of security problems by shipping products with "out of the box" configurations that have security options turned on rather than require users to turn them on. The users can change these "default" configurations if desired, but they would have the benefit of starting from a secure base.

To encourage product vendors to produce the needed higher quality products, we encourage the government to use its buying power to demand higher quality software. The government should consider upgrading its contracting processes to include "code integrity" clauses, clauses that hold vendors more accountable for defects in released products. Included here as well are upgraded acquisition processes that place more emphasis on the security characteristics of systems being acquired. In addition, to support these new processes, training programs for acquisition professionals should be developed that provide training not only in current government security regulations and policies, but also in the fundamentals of security concepts and architectures. This type of skill building is needed in order to ensure that the government is acquiring systems that meet the spirit, as well as the letter, of the regulations.

Wider adoption of security practices: With our growing dependence on information networks and with the rapid changes in network technology and threats, it is critical that more organizations, large and small, adopt the use of effective information security risk assessments, management policies, and practices. While there is often discussion and debate over which particular body of practices might be in some way "best," it is clear that descriptions of effective practices and policy templates are widely available from both government and private sources such as the National Institute of Standards and Technology, the National Security Agency, and other agencies. What is often missing today is management commitment: senior management's visible endorsement of security

improvement efforts and the provision of the resources needed to implement the required improvements.

Expanded research in information assurance: It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.

Thus, the research agenda should seek new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be the creation of

- A unified and integrated framework for all information assurance analysis and design
- Rigorous methods to assess and manage the risks imposed by threats to information assets
- Quantitative techniques to determine the cost/benefit of risk mitigation strategies
- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures

In this research program, special emphasis should be placed on the overlap between the cyber world and the physical world, and the analysis techniques developed should help policy and decision makers understand the physical impact and disruption of cyber attacks alone or of cyber attacks launched to amplify the impact of concurrent physical attacks.

More technical specialists: Government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction. The current levels of support, however, are far short of what is required to produce the technical specialists we need to secure our systems and networks. These programs should be expanded over the next five years to build the university infrastructure we will need for the long-term development of trained security professionals.

More awareness and training for Internet users: The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life to the Internet. As a result, many Internet users have little understanding of Internet technology or the security practices they should adopt. To encourage “safe computing,” there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace. Because the survivability of systems is dependent on the security of systems at other sites, fixing one’s own systems is not sufficient to ensure those systems will survive attacks. Home users and business users alike need to be

educated on how to operate their computers most securely, and consumers need to be educated on how to select the products they buy. Market pressure, in turn, will encourage vendors to release products that are less vulnerable to compromise.

- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries.[1] Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need be educated as well and should reinforce lessons in security and behavior on computer networks.

5. Conclusion

Interconnections across and among cyber and physical systems are increasing. Our dependence on these interconnected systems is also rapidly increasing, and even short-term disruptions can have major consequences. Cyber attacks are cheap, easy to launch, difficult to trace, and hard to prosecute. Cyber attackers are using the connectivity to exploit widespread vulnerabilities in systems to conduct criminal activities, compromise information, and launch denial-of-service attacks that seriously disrupt legitimate operations.

Reported attacks against Internet systems are almost doubling each year and attack technology will evolve to support attacks that are even more virulent and damaging. Our current solutions are not keeping pace with the increased strength and speed of attacks, and our information infrastructures are at risk. Solutions are not simple, but must be pursued aggressively to allow us to keep our information infrastructures operating at acceptable levels of risk. However, we can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.

[1] National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991, recommendation 3c, p. 37.