Cyber Security

Testimony of Stephen E. Cross
Director, Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Before the
Senate Armed Services Committee
Subcommittee on Emerging Threats and Capabilities

March 1, 2000

Introduction

Mr. Chairman and Members of the SASC Subcommittee on Emerging Threats and Capabilities:

My name is Steve Cross. I am the director of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University. The SEI is the home of the CERT® Coordination Center (CERT/CC). Thank you for the opportunity to testify today. I will give you some background on the CERT/CC, describe the trends we have observed while responding to computer security incidents on the Internet, discuss near-term steps that I believe can be taken to address today's problems, and consider what the future holds.

The CERT/CC was established at the SEI in 1988, after an Internet "worm" stopped 10% of the computers connected to the Internet. This program—the first Internet security incident to make headline news—was the wake-up call for network security. The CERT/CC went into operation in just two weeks with a charter to work with the Internet community to respond to computer security events, raise awareness of computer security issues, and prevent security breaches. The CERT/CC staff is also responsible for the day-to-day operations of FedCIRC, the Federal Computer Incident Response Capability, an organization that provides incident response and other security-related services to Federal civilian agencies. FedCIRC is managed by the General Services Administration.

The CERT/CC is now recognized by both government and industry as a neutral, authoritative source of information assurance information and expertise.

The CERT® Coordination Center (CERT/CC) is part of the SEI Networked Systems Survivability Program. The goals of the program are to 1) establish tools and techniques that enable typical users and administrators to effectively protect systems from damage caused by intruders and 2) establish techniques that help software engineers to model and predict security attributes of systems during development. Areas of work include survivable network management and survivable network technology, along with education and training. The management-oriented effort focuses on publishing best practices for security improvement, developing a self-directed evaluation method for organizations to improve the security of their networked computing systems, and defining an adaptive security improvement process. In the area of technology, the focus is on the technical basis for identifying and preventing security flaws and for preserving essential services if a system is penetrated and compromised. Approaches include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Training courses on security are offered to system administrators, network managers, and computer security incident response teams—both the technical staff and managers.

The Survivable Systems Initiative is also collaborating with other FFRDCs, MITRE, RAND, and Lincoln Laboratory, on a cyber security program. This effort is aimed at establishing a prototype to transition new information assurance technologies to the Department of Defense. Other participants include the Air Force Research Laboratory and Electronic Systems Center.

In the first full year of operation, 1989, the CERT/CC responded to 132 computer security incidents. In 1999, the staff responded to more than 8,000 incidents. In total, the CERT/CC staff

has handled well over 24,000 incidents and analyzed more than 1,500 computer vulnerabilities. This testimony is based on that first-hand experience.

Vulnerability of the Internet

Vulnerabilities associated with the Internet put government, the military, commerce, and individual 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. Because the Internet was not originally designed with security in mind, it is difficult to ensure the integrity, availability, and privacy of information. The Internet was designed to be "open," with distributed control and mutual trust among users. As a result, control is in the hands of users, not in the hands of the provider; and use cannot be administered by a central authority. Furthermore, security issues are not well understood and are rarely given high priority by software developers, vendors, network managers, or consumers.

In addition, because the Internet is digital, not physical, it has no geographic location and no well-defined boundaries. Traditional physical "rules" are difficult or impossible to apply. Instead, new knowledge and a new point of view are required to understand the workings and the vulnerabilities of the Internet.

Another factor is the approach typically taken by the intruder community. There is (loosely) organized development in the intruder community, with only a few months elapsing between "beta" software and active use in attacks. Moreover, intruders take an open-source approach to development. One can draw parallels with open system development: there are many developers and a large, reusable code base.

Intruder tools are becoming increasingly sophisticated and also becoming increasingly user friendly and widely available. For the first time, intruders are developing techniques to harness the power of hundreds of thousands of vulnerable systems on the Internet. Using what are called distributed-system attack tools, intruders can involve a large number of sites simultaneously, focusing all of them to attack one or more victim hosts or networks. The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated intruders can use them.

The current state of Internet security is the result of many additional factors, such as the ones listed below. A change in any one of these can change the level of Internet security and survivability.

- Because of the dramatically lower cost of communication on the Internet, use of the Internet is replacing other forms of electronic communication. The Internet itself is growing at an amazing rate, as noted in an earlier section.

- The government increasingly relies on commercial off-the-shelf software. As a result, government systems may contain vulnerabilities that put sensitive information and operations at risk.

- There is a continuing movement to distributed, client-server, and heterogeneous configurations. As the technology is being distributed, so is the management of that

technology. 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.

- Internet sites have become so interconnected and intruder tools so effective that the security of any site depends, in part, on the security of all other sites on the Internet.

- 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.

- 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 demand for skilled system administrators far exceeds the supply.

- 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.

- 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. 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.

- 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.

Attack Strategies Illustrating Internet Vulnerabilities

Some attacks are intended to harass a site and deny it the ability to transact business on the Internet. Other attacks enable intruders to gain privileged access to a system so that it effectively belongs to them. With their unauthorized privileges, they can, for example, use the system as a launch platform for attacks on other sites or as one node in an attack using distributed-system intruder tools. Still other attacks are designed to reveal sensitive information, such as passwords or trade secrets. We describe sample attack strategies below. Our descriptions are neither theoretical nor abstract; rather, they present, at a high level, actual attacks reported to the CERT Coordination Center regularly.[1]

Use of Distributed System Intruder Tools

Distributed systems based on the client/server model have become increasingly common. In recent months, there has been an increase in the development and use of distributed network sniffers, scanners, and denial-of-service tools. Attacks using these tools can involve a large number of sites simultaneously and be focused to attack one or more victim hosts or networks.

Damaged systems include those used in the attack as well as the targeted victim. For the victim, the impact can be extensive. For example, in a denial-of-service attack using distributed technology, the attacked system observes simultaneous attacks from all the nodes at once—flooding the network normally used to communicate and trace the attacks and preventing any legitimate traffic from traversing the network.

There are indications that the processes for discovering vulnerable sites, compromising them, installing daemons (programs used in the attack), and concealing the intrusion are largely automated, with each step being performed in "batch" mode against many machines in one "session." Attack daemons have been discovered on a variety of operating systems with varying levels of security and system management.

It is critical to plan and coordinate before an attack to ensure an adequate response when an attack actually happens. Since the attack methodology is complex and there is no single-point solution or "silver bullet," resolution and restoration of systems may be time-consuming. The bottom line is that an organization's systems may be subject at any time to distributed attacks that are extremely difficult to trace or defend against. Only partial solutions are available.

Although an organization may be able to "harden" its own systems to help prevent having its systems used as part of a distributed attack, there is essentially nothing a site can do with currently available technology to prevent becoming a victim of, for example, a coordinated network flood. The impact upon the site and its operations is dictated by the (in)security of other sites and the ability of a remote attacker to implant the tools and, subsequently, to control and direct multiple systems worldwide to launch an attack. The result may be reduced or unavailable network connectivity for extended periods of time, possibly days or even weeks depending upon the number of sites attacking and the number of possible attack networks that could be activated in parallel or sequentially.

Coordinated attacks across national boundaries have occurred. The tools and attacks demonstrate that a network that optimizes its technology for speed and reliability at the expense of security

[1] All the attacks mentioned in this section are described in CERT advisories, published online by the CERT Coordination Center, Pittsburgh, PA, and available from http://www.cert.org/

may experience neither speed nor reliability, as intruders abuse the network or deny its services. The intruder technology is evolving, and future tools may be more difficult to defeat.

Web-Specific Attacks

The CERT/CC has published a number of security alerts about Web-related technology, the most recent of which concerned *cross-site scripting.* In this attack, what users receive from a web site may not be what the operators of that site meant to send. Attackers put malicious code into otherwise legitimate HTML code so that if users click on a specially designed link, they may receive bad data, unwanted pictures, and programs (malicious scripts) to compromise users' data. The attackers can capture passwords and other information the users believe is protected, and they may be able to view protected parts of the users' network, such as an intranet.

The problem is not with web browsers themselves but with how dynamic web pages are constructed (*dynamic* means they are constructed "on the fly" in response to user input) and how data entering and leaving web sites is validated. "Validate" means ensuring no "unintended" characters are sent back to the client. The attack is possible because web browsers have the capability to interpret scripts embedded in web pages downloaded from a web server. Web browsers are usually installed with the capability turned on by default. The user can unknowingly download the script when visiting a seemingly safe site and completing an interactive form or querying a database; following untrustworthy links in web pages, email, or newsgroups; and viewing dynamically generated web pages. The malicious script then runs on the user's browser. Although attackers have been able to inject malicious code for a long time, the cross-site scripting attack is significant because users can acquire malicious code from legitimate, typically trustworthy sites; avoiding questionable sites is no longer adequate protection.

Most solutions require action from a broad community of web page developers and web site administrators. They must ensure that their web pages are encoded in a way that neutralizes malicious code, apply patches developed by vendors, and filter all data that enters and leaves web servers. In the meantime, users can gain some protection by turning off certain features of their web browsers, limiting the functionality they may be accustomed to having. They cannot fully protect themselves nor easily identify an attack.

The World Wide Web is a young and still immature technology. Until it is "hardened" for safe, effective use, it will continue to be vulnerable to security compromises – and online companies and customers alike will continue to be concerned about the integrity and privacy of information that must be exchanged if they are to do business on the Web.

SYN Attacks: Denial of Service

A *SYN attack* is an attack against a computer that provides service to customers over the Internet. *SYN* refers to the type of message (Synchronize) that is used between computers when a network connection is being made. In this attack, the enemy runs a program from a remote location (anywhere in the world) that jams the service on the victim computer. This is known as a *denial-of-service attack* because the effect of the attack is to prevent the service-providing computer from providing the service. The attack might prevent one site from being able to exchange data with other sites or prevent the site from using the Internet at all. Increasingly, companies are depending on Internet services for day-to-day business, from email to advertising to online product delivery. Some companies' business is entirely dependent on the Internet.

SYN attacks have been used successfully against a wide variety of targets, but they have the greatest impact against Internet service providers, or ISPs, which provide Internet connection services to government, businesses, and individuals. A SYN attack against an ISP usually results in disruption of Internet service to all the service provider's customers.

This type of attack is very difficult to prevent because it exploits a design flaw in the basic technology used for Internet communication today. Experts are currently working on techniques to reduce the problem somewhat, but preventing these attacks from occurring in the future will require a change in the way Internet communications are accomplished by the computers using the Internet. This is likely to take several years.

IP Spoofing: Masquerading

In an attack known as *IP spoofing*, attackers run a software tool that creates Internet messages that appear to come, not from the intruder's actual location, but from a computer trusted by the victim. *IP*, which stands for Internet Protocol, refers to the unique address of a computer. When two computers trust each other, they allow access to sensitive information that is not generally available to other computer systems. The attacker takes advantage of this trust by masquerading as the trusted computer to gain access to sensitive areas or take control of the victim computer by running "privileged" programs. Information that has been compromised through IP spoofing includes credit card information from a major Internet service provider and exploitation scripts that a legitimate user had on hand for a security analysis.

Unfortunately, there are many computer programs and services that rely on other computers to "speak the truth" about their address and have no other mechanism for disallowing access to sensitive information and programs. The CERT Coordination Center has received many reports of attacks in which intruders (even novice intruders) used this technique to gain access to computer systems with the help of publicly available IP spoofing computer programs.

Sniffers: Violating Privacy and Confidentiality

For most users of computer networks, including the Internet, the expectation is that once a message is sent to another computer or address, it will be protected in much the same way letters are protected in the U.S. Postal Service. Unfortunately, this is not the case on the Internet today. The messages are treated more like postcards sent by a very fast, efficient pony express. Information (such as electronic mail, requests for connections to other systems, and other data) is sent from one computer to another in a form easily readable by anyone connected to a part of the network joining the two systems together. For Internet data, these messages are routed through the networks at many locations, any one of which could choose to read and store the data as it goes by. The CERT/CC has handled many incidents in which an intruder ran a program known as a *sniffer* at a junction point of the Internet.

The sniffer program records many kinds of information for later retrieval by the intruder. Of specific interest to most intruders is the user name and password information used in requests to connect to remote computers. With this information, an intruder can attack a computer on the Internet using the name and password of an unsuspecting Internet user. Intruders have captured hundreds of thousands of these user name/password combinations from major companies, governments sites, and universities all over the world.

To prevent attacks of this type, encryption technology must be used for both the access to other computers around the Internet (cryptographic authentication) and the transmission of data across the Internet (data encryption).

Attractiveness of the Internet to Attackers

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.

Internet Attacks Are Easy

Internet users place unwarranted trust in the network. It is common for sites to be unaware of the amount of trust they actually place in the infrastructure of the Internet and its protocols. Unfortunately, the Internet was originally designed for robustness from attacks or events that were external to the Internet infrastructure, that is, physical attacks against the underlying physical wires and computers that make up the system. The Internet was not designed to withstand internal attacks—attacks by people who are part of the network; and now that the Internet has grown to encompass so many sites, millions of users are effectively inside.

The Internet is primarily based on protocols (rules and conventions) for sharing electronically stored information, and a break-in is not physical as it would be in the case of a power plant, for example. It is one thing to be able to break into a power plant, cause some damage, then escape. But if a power plant were like the Internet, intruders would be able to stay inside the plant undetected for weeks. They would come out at night to wander through the plant, dodging a few guards and browsing through offices for sensitive information. They would hitch a ride on the plant's vehicles to gain access to other plants, cloning themselves if they wished to be in both places at once.

Internet attacks are easy in other ways. It is true that some attacks require technical knowledge—the equivalent to that of a college graduate who majored in computer science—but many successful attacks are carried out by technically unsophisticated intruders. As mentioned earlier, technically competent intruders duplicate and share their programs and information at little cost, thus enabling naive "wanna-be" intruders to do the same damage as the experts.

Internet Attacks Are Difficult to Trace

As discussed in the IP spoofing example, 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. Again, a packet can be compared to a postcard—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 US 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 US-based attacks on US sites gain this safety by first breaking into one or more non-US sites before coming back to attack the desired target in the US.

Internet Attacks Are Low Risk

Failed attempts to break into physical infrastructures involve a number of federal offenses; such events have a long history of successful prosecutions. This is not the case for Internet intrusions. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is reduced. In addition, it is not always clear when certain events should be cause for alarm. For example, what appear to be probes and unsuccessful attacks may actually be the legitimate activity of network managers checking the security of their systems. Even in cases where organizations monitor their systems for illegitimate activity, which occurs in only a small minority of Internet-connected sites, real break-ins often go undetected because it is difficult to identify illegitimate activity. In the case of cross-site scripting, web users trigger malicious code without even knowing they have done so, and web sites can unknowingly pass the code along. Finally, because intruders cross multiple geographical and legal domains, an additional cloud is thrown over the legal issues involved in pursuing and prosecuting them.

Impact of Security Breaches

Security breaches can cause a loss of time and resources as personnel investigate the compromise, determine potential damage, and restore the systems. The systems may provide reduced service or be unavailable for a period of time. Sensitive information can be exposed or altered, and public confidence can be lost. After a successful computer system intrusion, it can be very difficult or impossible to determine precisely what subtle damage, if any, was left by the intruder. Loss of confidence can result even if an intruder leaves no damage because the site cannot *prove* none was left. Particularly serious for business are denial-of-service attacks and the exposure of sensitive information. Once an overt denial-of-service attack has been resolved and the service returned, users generally regain trust in the service they receive. But exposure of sensitive information makes an organization highly susceptible to a loss-of-confidence crisis.

Here are just a few examples of security breaches. In addition to examples published in the press, the CERT/CC handles reports of breaches at government sites daily, often working with DoD-CERT to coordinate response to security incidents at DoD sites.

- Attackers apparently working from Russia systematically broke into DoD computers for more than a year and took vast amounts of unclassified but nonetheless sensitive information. Besides penetrating the Pentagon's defenses, the attackers raided unclassified computer networks at Energy Department nuclear weapons and research labs, at the National Aeronautics and Space Administration, and at many university research facilities and defense contractors.

- An intruder installed a packet sniffer at a site in another country in which a conference was being held. As the conference attendees logged into their systems at home from the facilities provided at the conference, the intruder was able to capture authentication information. The attendees included people from US sites. As a consequence, the intruder was able to gain

access to a number of sites in the US, including military, government, and academic institutions.

- An attacker obtained 100,000 credit card numbers from the records of a dozen retailers selling their products through Web sites. He used a packet sniffer to capture the numbers as they traversed the Internet. The credit cards had limits between $2,000 and $25,000, putting the potential cost of theft at $1 billion. This type of intruder activity is one form of "identity theft." The attacker was caught when he tried to sell the card numbers to an apparent organized-crime ring that turned out to be the FBI.

- Hundreds and perhaps thousands of credit card numbers, home addresses, and phone numbers were exposed for months through a security hole on many small Internet auction sites. Records at several sites using older versions of the same auction software were exposed when administrators either did not secure their sites with keys or otherwise failed to use the software properly. The risk varied from site to site, ranging from data immediately accessible with a few mouse clicks to information obtainable through rudimentary hacking. The sites known to have used the software belong to small and medium-sized businesses, in some cases stores trying to capitalize on the e-commerce boom by running their own online auctions. Credit card numbers were not the only information available. One site, for example, also exposed the names, addresses, phone numbers, email, and passwords of more than 100 customers. The same type of information was available—although not as readily—on other sites as well.

- In a case of cyber-extortion, an intruder stole 300,000 credit card numbers from an online music retailer. The intruder, who described himself as a 19-year-old from Russia, sent an email to the New York Times bragging he had accessed the company's financial data through a flaw in its software. The intruder later used the card numbers in an attempt to blackmail the retailer into paying $100,000 in exchange for destroying the sensitive files. When the company refused to comply, the intruder released thousands of the credit card numbers onto the Internet in what turned out to be a public relations disaster for the company. Security experts still do not know how the site was compromised or the full extent of how the break-in affected the site's customers. Credit card companies responded by canceling and replacing the stolen card numbers and notifying affected cardholders by email. E-commerce analysts say many similar attacks go unreported.

- Just last month, in the most serious systematic breach of security ever for British companies, a group of intruders based in the UK broke into the computer systems of at least 12 multinational companies and stolen confidential files. The group issued ransom demands of up to £10 million in exchange for the return of the files. Scotland Yard and the FBI are investigating the break-ins, and are scrutinizing email traffic between England and Scotland. They believe the group is highly professional and may be working for information brokers specializing in corporate espionage.

- A major credit card company confirmed having recently received a sizable ransom demand after intruders stole computer source code and threatened to crash the entire system. The company contacted authorities and began reinforcing its system. It is estimated that if the company's system crashed for just one day, it would cost the company tens of millions of British pounds. Officials are not yet ready to confirm that the attack on the company was the work of the same group responsible for break-ins at other multinational companies in the UK.

- Last spring, service on NATO's home page was erratic for more than a week while attackers in Belgrade tampered with the NATO Web site. At the same time, the NATO email system was saturated by one individual who sent 2,000 emails a day. NATO was also infected by macro viruses sent from Yugoslavia through the email system. A senior NATO diplomat said it was clear how well-organized and prepared Belgrade's offensive was: "It ranges all the way from organized ethnic cleansing to messing up our Web site."

It is obvious from these examples and the ongoing activity of the CERT Coordination Center that there is much work to be done to secure our electronic networks adequately. The next section suggests actions to address the growing security issues relating to networked computers.

Recommended Solutions

The problem is serious and complex, and a combination of approaches must be used to reduce the risks associated with the ever-increasing dependence on the Internet and the possibility of a sustained attack on it. Effective solutions require multi-disciplinary and cross-domain cooperation that includes information sharing and joint development of comprehensive solutions, as well as support for a long-term research agenda.

Support an established center for collecting, analyzing, and disseminating information assurance information.

The nature of threats to the Internet is changing rapidly and will continue to do so for the foreseeable future. The combination of rapidly changing technology, rapidly expanding use, and the continuously new and often unimagined uses of the Internet creates a volatile situation in which the nature of threats and vulnerabilities is difficult to assess and even more difficult to predict.

To help ensure the survivability of the Internet, and the information infrastructure as a whole, it is essential to continuously monitor and analyze cybersecurity threats and vulnerabilities and identify trends in intrusion activity. The organization doing this should collect, analyze, and report on quantity, trends, and character of cybersecurity incidents. To obtain the required information, the organization must be well trusted throughout the community. Given the universal concerns about privacy and confidentiality and the inherently voluntary nature of reporting, the collection organization should be neither government nor commercial. Nor can it be responsible for public policy, investigation, enforcement, or other activities perceived as conflicting. Organizations that have suffered attacks are often unwilling to discuss their problems for fear of loss of confidence by their customers.

The CERT/CC is establishing an analysis center to expand its work of collecting and analyzing information assurance data. The goals are to identify trends and to develop detection and mitigation strategies that provide high-leverage solutions to information assurance problems, including countermeasures for new vulnerabilities and emerging threats. It takes advantage of the information dissemination channels already in place at the CERT/CC.

The CERT Analysis Center extends current incident response capabilities by developing and transitioning protective measures and mitigation strategies to defend against advanced forms of attack before they are launched. Additionally, it provides the public and private sectors with opportunities for much-needed collaboration and information sharing to improve cyber attack defenses.

The strength of the CERT Analysis Center will come from contributions across the information technology community. SEI affiliate and visiting scientist programs provide an established model to integrate the contribution of diverse participants. These programs bring together members of academic, industry, and government organizations to address problems and meet common needs. The center provides the means for private sector firms to collaborate with technical staff from the CERT Analysis Center on leading-edge information assurance research.

Research includes intruder tool analysis; that is, in-depth analysis of new and emerging cyber-attack methods in order to develop defenses and countermeasures that can be deployed before these new attack methods are widely used. Equally important is in-depth analysis of information technology vulnerabilities and malicious code in order to develop techniques that are effective at eliminating entire classes of vulnerabilities and entire families of malicious code.

Support the growth and use of global detection mechanisms.

Among the ways to gain a global view of threats are to use the experience and expertise of incident response teams to identify new threats and vulnerabilities. The incident response team at the CERT/CC and other response teams have demonstrated their effectiveness at discovering and dealing with vulnerabilities and incidents. Ongoing operation and expansion of open, wide area networks will benefit from stronger response teams and response infrastructures.

Similarly, it is important to encourage Internet service providers to develop security incident response teams and other security improvement services for their customers. Many network service providers are well positioned to offer security services to their clients. These services should include helping clients install and operate secure network connections as well as mechanisms to rapidly disseminate vulnerability information and corrections.

Support education and training to raise the level of security.

As noted earlier, the security of each system on the Internet depends on the security of all other systems on the network. The interconnectedness and interdependency of systems pose a serious threat to commerce.

The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life. As a result, many users of the Internet who have no more understanding of the technology than they do of the engineering behind other infrastructures. Similarly, many system administrators lack adequate knowledge about the network and about security, even while the Internet is becoming increasingly complex and dynamic. 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, both adults and children.** There is a critical need for education and increased awareness of the characteristics, threats, opportunities, and appropriate behavior in cyberspace. This need goes far beyond protecting children from pornography. It relates to how quickly cyberspace will be developed, to how rapidly and effectively cyberspace will be exploited for social and economic benefit, and to what influences will drive the economic, social, and political directions in cyberspace.

  In particular, 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.[2] 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.

- **Invest in awareness campaigns that stress the need for security training for system administrators, network managers, and chief information officers.** Building, operating, and maintaining secure networks are difficult tasks; and there are few educational and training programs that prepare people to perform them. Training will also enhance the ability of administrators and managers to use available technology for configuration management, network management, auditing, intrusion detection, firewalls, guards, wrappers, and cryptography.

  Furthermore, the increasing need for such roles in organizations of many sizes and descriptions has led to assigning information security responsibilities to inexperienced personnel with little or no training. In the short term, the greatest need is for short "how to" and "what to be aware of" courses. In the long term, there should be undergraduate-level or master's-level specialties in network and information security.

Support research and development in the areas of security and survivability of unbounded systems' architectures with distributed control.

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. 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 these:

- Develop science-based engineering methods for information assurance specification and design through innovative adaptation of existing formal specification theory originally developed for other purposes.

- Develop prototype tools to assess information assurance properties of specifications and designs by adapting core algorithms of existing theory-based analytical tools that were originally developed for other purposes.

- Leverage past investment that has produced an extensive, but little used, body of knowledge in rigorous methods for system analysis and design in general, and for security and survivability in particular. Work needs to be done to extend and unify previous research to deal with new problems of information assurance in a coherent and integrated manner, and to make innovative use of existing research, technology, and tools.

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

Conclusion

The Internet has proven to be an engine that is driving a revolution in the way the US government conducts its business. Because of the tremendous interconnectedness and interdependence among computer systems on the Internet, the security of each system on the Internet depends on the security of all other systems on the network. For the United States to thrive on the Internet, cyber security efforts need to focus on reporting and monitoring threats and vulnerabilities, education and training, and research and development.

Synopsis of Dr. Stephen E. Cross's Testimony

to the Senate Armed Services Committee
Subcommittee on Emerging Threats and Capabilities
March 1, 2000

Steve Cross is the director of the Software Engineering Institute (SEI), a federally funded research and development Center at Carnegie Mellon University in Pittsburgh, Pennsylvania, and the home of the CERT® Coordination Center (CERT/CC).

CERT/CC – trusted, neutral, authoritative source of network security information and expertise

- The CERT/CC was established in 1988, after an Internet "worm" became the first Internet security incident to make headline news, serving as a wake-up call for Internet security. The CERT/CC was operational less than two weeks later.
- Since 1988, the CERT/CC has responded to 24,000 computer security incidents and analyzed 1,500 vulnerabilities. In 1999 alone, it handled 8,000 incidents, a 120% increase from the year before.
- The CERT/CC staff operates FedCIRC, incident response for the Federal civil agencies.
- The CERT/CC coordinated the private-public sector effort to address distributed system intruder tools and cross-site scripting prior to the recent attacks.
- The CERT/CC is part of the SEI Networked Systems Survivability Program, which collaborates with MITRE, RAND, Lincoln Laboratory, and other security experts.

Factors Affecting Security

- The security of each system on the Internet depends on the security of all other systems on the network. The interconnectedness and interdependency of systems pose a serious threat.
- The Internet was not originally designed with security in mind, so it is difficult to ensure the integrity, availability, and privacy of information.
- The Internet was designed to be "open," with distributed control and mutual trust among users – no central authority or control.
- Security issues are not well understood and are rarely given high priority by software developers, vendors, network managers, or consumers.
- The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated intruders can use them.
- Bottom line: Cyber attacks will continue with more frequency and more severity.

Recommended Actions to Address Threats to Network Security

- Cyber security efforts needed for US government and business to operate on the Internet should include increased and sustained resources to
    - support public-private collaborations, such as those by the CERT/CC
    - monitor and report threats and vulnerabilities
    - transfer security knowledge through education and training
    - research solutions to the complex problems of security and survivability
    - provide trusted, immediate, and expert response to security problems

The CERT Coordination Center stands ready to work with Congress, federal agencies and departments, industry, academia, and the world-wide network of other incident response teams to address this serious problem.