Cyber Security as an Emergent Infrastructure

Dorothy E. Denning

When I began studying computer security in late 1972 as a Ph.D. student at Purdue University, the field was in its infancy. There were few academics working in the area, no research conferences or journals devoted to the field, and no professional societies to join. Security papers were presented at conferences and published in journals that covered more established areas of computer science, such as operating systems, or that treated computing and telecommunications broadly. The number of publications and Ph.D. theses relating to computer security was small enough that it was possible to read the entire literature. If there was any security industry at all, I was not aware of it.

The computing environment at Purdue consisted primarily of two mainframes: one used by the faculty and students for academic work, and the other by the administration. Neither was connected to the emerging Internet. The systems were accessed via punched cards and "dumb terminals" (machines with monitors and keyboards but no computing capability or memory). Security consisted mainly of two mechanisms. First, access to the machines was controlled through accounts and passwords. Second, the administrative system was physically separated from and unconnected to the academic system so as to protect the more sensitive data handled by the former. We did not use firewalls, anti-viral tools, vulnerability scanners, or intrusion-detection systems; such tools had not even been invented.

The field has changed dramatically in the 30 years that have passed. Now there is a multi-billion-dollar-a-year security industry offering thousands of products and services

to everyone from large corporate enterprises to home computer users. There are more security conferences than I can keep track of, let alone attend, and enough publications to fill a library. Thirty-six universities have been declared Centers of Academic Excellence in Information Assurance Education, and numerous companies offer training in computer and network security and forensics. There are professional societies devoted to security, and certification programs for security technologies, operating environments, and security professionals. Information security has become a topic of conversation at board meetings and social gatherings. It is a priority in business and government. It has led to new laws and regulations, and to new policies and procedures for handling information. It is on the agenda of Congress, the President, and international bodies.

In recent years, governments have become particularly concerned with protecting critical infrastructures from physical and cyber attacks. In 1996, the Clinton Administration formed the President's Commission on Critical Infrastructure Protection (PCCIP). The PCCIP was tasked to study the critical infrastructures that constitute the life support systems of the nation, determine their vulnerabilities to a wide range of threats, and propose a strategy for protecting them in the future. Eight infrastructures were identified: telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services, and government services. Their recommendations led to several initiatives discussed later in this chapter.

While much of the focus at the national policy level has been on protecting critical infrastructures, cyber security is vital to much more. Information technology is

woven into practically all business processes and control systems. Cyber attacks have real-world consequences that impact the economy and our daily lives.

To address today's threats to information-based systems, security has evolved from the simple access controls of 30 years ago to a complete infrastructure in its own right. This infrastructure serves to protect computers and networks, and the information that is generated, acquired, processed, transmitted, and stored by them. Like many of the systems it protects, the security infrastructure is global and interconnected. It is growing and evolving, and will continue to do so as long as information technology itself evolves.

The objective of this chapter is to explore this emergent infrastructure and the factors that are shaping its development. The focus is on cyber security, which includes computer security and network security, but excludes those aspects of information security that deal with information that is not computerized (e.g., print media).

The factors shaping the development of the security infrastructure are divided into five areas: threats, technology developments, economic factors, psychological factors, and social and political factors. These areas will be discussed after first describing the elements of security infrastructure.

Limitations of space preclude giving more than a broad overview of the topics. Many issues are ignored or brushed over lightly. Further, more attention is paid to developments in the United States than elsewhere. The aim is a conceptual framework for understanding the state of security today rather than complete coverage of all the pieces of the framework.

THE CYBER SECURITY INFRASTRUCTURE

The cyber security infrastructure consists of those elements involved in the protection of networked computers and information from cyber threats. The objective is to deter, prevent, detect, recover from, and respond to threats in cyberspace. The threats take a variety of forms and include unauthorized access to or use of information resources, and computer network attacks that deny, disrupt, degrade, or destroy information and network resources. They include theft of information, computer viruses and worms, defacement of web sites, denial-of-service attacks, computer and network penetrations, and sabotage or fabrication of data. The security infrastructure serves to protect against these threats and ensure the confidentiality, authenticity, integrity, and availability of data.

The security infrastructure includes information technology, procedures and practices, laws and regulations, and people and organizations. These areas are inter-related and impact each other. Developments in technology, for example, can lead to new procedures and practices, new laws or regulations, and the formation of new security companies. Each is discussed briefly below.

INFORMATION TECHNOLOGY

Information technology consists of the hardware and software used to generate, acquire, process, distribute, and store information. Of interest here are technologies that serve to protect cyberspace from attack through prevention, detection, investigation, and recovery. Prevention technologies include authentication systems (e.g., passwords, biometrics, and smart cards), encryption systems (for scrambling data and network communications), access controls, firewalls, vulnerability scanners, and security management systems.

Detection and investigation technologies include auditing and intrusion/misuse detection systems, anti-viral tools, honey pots for trapping and studying intruders, trace back mechanisms for determining the origin of an attack, and computer and network forensic tools for handling and processing evidence. Technologies for recovery include backup systems.

None of the technologies offers a "silver bullet" for security. They all have their limits. Encryption, for example, can protect e-mail from snoops, but not from viruses or spam attacks. Security is possible only through a combination of controls coupled with good management and operating practices, supporting laws, and effective law enforcement – in short, the security infrastructure. Even then, security is never foolproof.

Further, some security technologies are also employed as attack technologies. Password crackers and software tools that scan networks for vulnerabilities are good examples. While system owners use them to find and fix their own problems, their adversaries use them to find security holes, which are then exploited in an attack.

Technology standards play an important role in security. They establish baseline requirements for security and promote interoperability between devices that need to communicate. A good example is the Secure Socket Layer (SSL) protocol. SSL is implemented in web browsers and servers, and used to encrypt confidential data such as credit card numbers that are transmitted between a user's browser and a web site.

Standards have a downside as well. The TCP/IP protocols, which are the foundation of the Internet, facilitate massive attacks against large numbers of computers. That so many of the computers are running the same software (e.g., versions of Microsoft Windows, Linux, and Unix) further aggravates the problems.

PROCEDURES AND PRACTICES

These relate to the management of security and information technology. They include "best practices" for developing, installing, and operating computers and networks so as to minimize security vulnerabilities and risks. Best practices have been developed in areas such as selecting and managing passwords, deploying firewalls, configuring and upgrading systems, and planning for and responding to security incidents.[1]

Good management practices are at least as crucial to security as deploying security technology. Most outsider attacks, perhaps all but one or two percent, exploit known vulnerabilities that could have been avoided by system administrators and users. Humans are often the weak link. They make mistakes, pick weak passwords, and are vulnerable to social engineering (being conned by attackers into providing passwords or access to systems, for example). They develop software with security flaws and open virus-laden e-mail attachments from strangers.

LAWS AND REGULATIONS

In the United States and elsewhere, it is illegal to access a computer or information stored on a computer or transmitted over a network without authorization and with intent to defraud, trespass, or cause damage to data or systems. It is also illegal to traffic in passwords or similar access codes. Such activity is covered at the federal level by the Computer Fraud and Abuse Act of 1986 and subsequent amendments, and by various other federal and state laws. However, not all countries criminalize these activities, and those that do may not have consistent laws.

A second set of laws and regulations regulate the investigation of cyber attacks

and threats by law enforcement and intelligence officers. These include laws for acquiring data about a subject of investigation from third parties, intercepting a subject's communications, and searching and seizing a subject's computing devices.

A third class of laws and regulations mandate security for certain systems. In the United States, the Office of Management and Budget requires federal agencies to conduct security certifications of systems that process sensitive information or perform critical support systems. Such requirements do not, however, apply to the private sector, which is generally unregulated with respect to security. One exception is the Health Information Portability Accountability Act (HIPAA), which specifies security and privacy requirements for systems that handle patient records. However, many private sector organizations impose internal security policies on their IT operations.

A fourth set of laws and regulations restrict trade in information security technologies. For example, certain encryption technologies are subject to export controls although these controls have been substantially lifted in recent years.

PEOPLE AND ORGANIZATIONS

The security infrastructure includes individuals and organizations with an interest in security. Both formal and informal organizations participate, including government agencies, corporations, educational institutions, professional societies, non-profit organizations, research communities, standards committees, international bodies, and consortia. Some groups come together temporarily for a specific purpose, for example, to participate in a security-related seminar, workshop, or meeting. Groups can operate domestically or internationally, and meet physically, virtually, or both. Many use the

Internet, especially e-mail and the web, to facilitate their activities, collaborate with others, and reach a broader audience.

The people and organizations participating in the security infrastructure perform a variety of different functions. These include education and training, research, publication, product development and marketing, network security administration, security support services, policy and standards making, law enforcement, and research funding.

None of these parties "owns" the security infrastructure. However, individuals and organizations are responsible for the security of their own systems. Governments are not responsible for the security of systems in the private sector, but they can influence the security of those systems through laws and regulations (e.g., HIPAA), public-private partnerships, research programs and grants, and other efforts.

Participants in the security infrastructure constitute a loosely structured network. Organizationally, this network resembles an all-channel or full matrix network[2] where everyone is connected to everyone else through the Internet (and other communications media). There is no central command or headquarters for the network as a whole and decision-making takes place across the network. When a major security incident affecting multiple organizations occurs, as with a major virus outbreak, many participants in the security network respond simultaneously to the attack, issuing alerts, releasing software tools and upgrades, reconfiguring systems, and hunting down the attacker. Even though organizations are responsible only for protecting their own systems, they can draw upon the network for products, services, standards, training, and other types of assistance. We now turn to the factors shaping the security infrastructure.

CYBER THREATS

A major force behind the security infrastructure is the real and perceived threat of cyber attacks. After briefly reviewing the characteristics of the threat, we will summarize some of the incident data showing the prevalence of the threat.

THREAT CHARACTERISTICS

Cyber threats are characterized by an attacker, a target system, a set of actions against the target, and the consequences resulting from the attack, including damages to the target, direct and indirect losses to victims, and impact to third parties. A prolonged denial-of-service attack against an Internet Service Provider (ISP), for example, can result in lost revenue, incident handling costs, and even bankruptcy for the ISP. Customers of the ISP will also suffer; to the extent they depend on the Internet for their business or home activities.

Threats are often classified by the nature and mission of the attacker. There are six major categories: hackers, insiders, corporate spies, criminals, terrorists, and nation states. Although the term “hacker” can denote any computer buff, in the context of cyber threats, it usually means a person who gains access to or breaks into computers and networks in a way that was not intended and is generally not authorized. For example, the objective may be to deface a web site, steal passwords to facilitate further attacks, or launch a computer virus or denial-of-service attack. Not all hacking is illegal, as when users hack their own systems or companies use employees or security consultants to test the security of their systems, so the threat pertains only to those who hack without

authorization. Many hackers are teenagers who pursue hacking more as a game or hobby than an attempt to wreak damage. Nevertheless, their actions do harm their victims.

Insiders consist of employees, former employees, temporaries, contractors, and others with inside access to an organization's information systems. They are behind many of the most serious attacks, including theft of trade secrets, financial fraud, and sabotage of data. Insiders are generally considered to be an organization's biggest threat, accounting for perhaps 80% of all security incidents (not all cyber related) in some firms. However, only 35% of cases involving theft of intellectual property were attributed to insiders, according to a survey conducted by the New York-based security firm Michael G. Kessler & Associates.[3]

Corporate spies include both foreign and domestic companies. They steal trade secrets primarily for competitive advantage. The Kessler study attributed 18% of the thefts to other U.S. companies and another 11% to foreign companies.

The category of criminals generally refers to persons who attack systems for money. They steal credit card numbers, identities, and intellectual property. They siphon money from bank accounts and extort their victims by threatening to expose stolen secrets or cause serious cyber damage. They operate alone, in concert with insiders, and through organized crime rings.

So far, terrorists are using the Internet primarily to support their physical operations rather than to launch cyber attacks. There have been a few incidents of hackers affiliated with or at least sympathetic to terrorist causes engaging in typical hacker-type activity such as web defacements and denial-of-service attacks.[4] For example, after the September 11 attacks, one group of Muslim hackers defaced U.S.

government web sites with messages proclaiming they stood by bin Laden and announcing an "Al-Qaeda Alliance Online."[5]

There is a growing concern that terrorists might launch cyber attacks against critical infrastructures. According to reports, Al Qaeda operatives visited websites that offered software and programming instructions for the digital switches that run power, water, transport, and communications grids. Interrogations of Al Qaeda prisoners revealed general intentions to use those tools. In February 2002, the CIA issued a revised Directorate of Intelligence Memorandum, indicating that Al Qaeda had far more interest in cyber terrorism than previously thought.[6]

Nation states are often considered the most serious threat, if not the most likely. They have the most resources, and may decide to employ cyber weapons to augment or replace physical ones. According to some analysts, as many as 20 countries have cyber-warfare capabilities, including China, Russia, North Korea, and Iraq. China in particular is said to have an aggressive information warfare program, motivated in part by the recognition that it could not defeat the United States with conventional warfare.[7]

SECURITY INCIDENTS

Computer network attacks have been rising steadily, in some cases dramatically, in recent years. Figure 1 shows that the number of incidents reported to the Computer Emergency Response Team Coordination Center (CERT/CC) has more than doubled each year since 1998, reaching 52,658 in 2001.[8] Considering that many, perhaps most, incidents are never reported to CERT/CC or indeed to any third party, the numbers become even more significant. Further, each incident that is reported corresponds to an attack that can

involve thousands of victims. The Code Red worm, which infected about a million servers in July and August, was a single incident. Web defacements have also more than doubled annually in the past few years, according to the London-based firm mi2g, reaching 30,388 in 2001.[9]

The prevalence of computer viruses and worms has been increasing at a similar rate. Message Labs, which scans its clients' e-mail for viruses, reported that 1 in 1,400 messages had a virus in 1999. The infection rate doubled to 1 in 700 in 2000 and then more than doubled to 1 in 300 in 2001. [10] ICSA.net (now TrueSecure) also has reported an increase in infection rate, from about 1% of computers in 1996 to 11% in 2001.[11]

Denial-of-service (DoS) attacks, which until a few years ago were relatively unheard of, are now commonplace. A study conducted at the Cooperative Association for Internet Data Analysis (CAIDA) at the University of San Diego Supercomputer Center observed about 12,000 attacks against 5,000 different targets during a three-week period in February 2001.[12]

Riptech, which offers security management and monitoring services, reported a 28% rise in attack activity in the first 6 months of 2002 as compared with the last 6 months of 2001. On average, their clients each experienced an increase from 25 attacks per week to 32 attacks per week. From this data, they projected an annual growth rate of 64% in attack activity.[13] The majority of attacks came from the United States and its allies. Less than 1% of the attacks came from countries on the U.S. cyber terrorism watch list. There were no attacks from Iraq, Libya, N. Korea, or Syria.

INFORMATION TECHNOLOGY TRENDS

Developments in technology shape the security infrastructure both directly and indirectly. The direct impact comes from technologies that enable new or improved security tools and services. The indirect impact results from technologies that aggravate the threat, thereby leading to actions that enhance security. This section briefly reviews three trend areas: ubiquity, power, and vulnerability.

UBIQUITY

Information technology is becoming increasingly pervasive and connected. It is spreading throughout our offices, homes, automobiles, and elsewhere. It is being integrated into everything from appliances and vehicles to business processes and control systems. It resides in both fixed and mobile devices. Software moves through the networks, carrying computer viruses, worms, Trojan horses, and other forms of malicious code.

This trend toward ubiquitous computing affects information security in two ways. First, there are more targets to attack and more people attacking them. Second, attacks can have real-world consequences. The Code Red worm, for example, led to the delay of 55 Japan Airlines flights after shutting down a computer used for ticketing and check-in.[14] Another incident that took place in early 2000 led to loss of wildlife and environmental damage. In that case, a 49-year-old Brisbane man allegedly penetrated the Maroochy Shire Council's waste management system and used radio transmissions to alter pump station operations. A million litres of raw sewage spilled into public parks

and creeks on Queensland's Sunshine Coast, killing marine life, turning the water black, and creating an unbearable stench. Evidently, the man was angry about being rejected for a council job. He had formerly worked for the company that had installed the system, which gave him inside knowledge and the software needed to conduct the attack. [15]

Approximately 3,000 Supervisory Control and Data Acquisition (SCADA) systems control critical infrastructures such as the power grid, dams, and pipelines.[16] Many of these systems have very poor security. In the past, this did not matter much, because the systems were arcane and isolated. Increasingly, however, they are controlled through networks based on the Internet protocols, potentially making them more open to attack.

The proliferation of mobile computing devices has extended an organization's network security perimeter from the workplace to homes, airports, automobiles, and hotel rooms. Information once confined to office networks can make its way to home PCs, laptop computers, and hand held devices, which may be less protected physically as well as virtually. Each year, tens of thousands of laptops are reported lost or stolen, many with extremely sensitive information, including government classified information.

Organizations are installing wireless networks with little regard for security. Using a technique called "war driving," hackers drive around cities looking for unprotected networks. When one is found, they can access the network to read corporate communications or simply use the network as they would their own. A seven-month audit sponsored by the International Chamber of Commerce found that 92% of the 5,000 wireless networks in London were vulnerable to casual attacks.[17] Network operators had either not turned on the security features or else used them with default settings that were

not secure.

The spread of information technology has also had some positive impact on security, for example, by enabling the development of remote security services. There are now services that check a computer or network for vulnerabilities, scan incoming or outgoing e-mail for viruses, monitor client networks for attacks, provide encryption services, manage public-key certificates, and detect and locate stolen laptops. You can download security products and information from the web, and you can find out about new problems by subscribing to one of several security alert services.

POWER

Information technology is getting smaller, faster, cheaper, and more powerful. Processor speeds are doubling approximately every 18 months according to Moore's law. This yields a factor of 10 improvements every 5 years and a factor of 100 improvements every 10. By some accounts, storage capacity is increasing at a somewhat faster rate, doubling about every 12 months, and network capacity is growing even faster, doubling approximately every 9 months.

Because of these performance trends, spies can steal megabytes of information in just a few seconds, and computer viruses and worms can spread at record-breaking speeds. During the peak of its infection frenzy, the Code Red worm infected more than 2,000 computers per minute.[18] But this was just a prelude of what is coming. At the University of California, Berkeley, a researcher showed how a "Warhol Worm" could infect all vulnerable servers on the Internet in 15 minutes to an hour. Researchers at Silicon Defense took the concept further, showing how a "Flash Worm" could do it in

thirty seconds.[19]

At the same time, high bandwidth data pipes and increased network traffic can make it more difficult to monitor networks for intrusions and other forms of abuse and to intercept particular traffic in support of a criminal investigation or foreign intelligence operation. Higher capacity disks make it more time consuming to scan disks for malicious code and conduct computer forensics examinations.

The relative lag of processor improvements to those of storage and networks could aggravate the challenges, although multiprocessor supercomputers and distributed computing can be used to compensate. A distributed approach is already used by many network-based intrusion detection systems and to break encryption keys in criminal investigations. Breakthrough processor technologies such as quantum and DNA computing might also counter the lag, but these technologies represent long-term solutions and can also benefit the adversary.

Attack tools have become more powerful as developers build on each other's work and program their own knowledge into the tools.[20] The Nimda worm combined features from several previous viruses and worms in order to create a powerful worm that spread by four channels: e-mail, Web downloads, file sharing, and active scanning for and infection of vulnerable Web servers. The advanced distributed denial of service tools have sophisticated command and control capabilities that allow an attacker to direct the actions of potentially thousands of previously compromised "zombie" computers. The zombies carry out the actual attack, using various techniques to thwart tracing.

Many attack tools are simple to use. "Script kiddies" and others with malicious intent but little skill can download the tools and launch destructive attacks without even

understanding how the tools work. E-mail worms can be constructed with windows-based software such as the VBS Worm Generator. All the attacker needs to do is type in a subject line and message body for the e-mail message carrying the worm and check a few boxes.

Improvements in hardware and software have also benefited security. Advances in artificial intelligence, data mining, and distributed processing have furthered the development of intrusion and misuse detection, for example.

VULNERABILITIES

One might think that over time, security would get better and systems would be less vulnerable to attack. While this is true for some software, overall, the state of security has gotten worse as witnessed by the increases in attacks and also vulnerabilities.

Vulnerabilities arise in two places: first, in the products themselves, and second, in the way they are installed and used. With respect to the first, the number of product vulnerabilities reported to CERT/CC has more than doubled annually in the past few years (see Figure 2). In 1998, CERT/CC received reports of 262 vulnerabilities or less than 1 a day. By 2001, this was up to 2,437 or almost 7 a day. These security holes can be attributed to several factors, including growth in the size and number of software products, inadequate attention to security and reliability during the software development process, and unanticipated side effects and interactions among different products.

With respect to the second source of vulnerabilities, products are frequently installed or used in ways that are not secure. Users pick weak passwords and system administrators fail to install security patches (code fixes) or alter default settings that

leave their systems open to attack. In September 2001, the System Administration, Networking, and Security (SANS) Institute and FBI issued a report identifying the top 20 Internet vulnerabilities.[21] At the top of the list was default installs of operating system and applications. Functions were enabled that were not needed and had security flaws. Second on the list were accounts with no passwords or weak ones.

This trend in vulnerabilities has been shaping the security infrastructure. It has created a market for reports about vulnerabilities and how to correct them. In addition, it is leading software developers to find ways of developing more robust software. In January 2002, for example, Microsoft Chairman Bill Gates sent a memo to all employees saying that security would be a top priority for the company. As part of the new Trustworthy Computing Initiative, Microsoft began training their software developers in security and announced a commitment to ship Windows.NET Server 2003 "secure by default."[22]

Building systems that are immune from any attack is a daunting, indeed impossible, task. Whereas the attacker only needs to find one flaw to launch an attack, the defender must find and fix every single one of them. However, considerable improvement is possible, as many common flaws are avoidable. Researchers have shown that introducing secure software engineering principles into the early stages of software development can yield significant cost savings.[23]

Vulnerability trends are drawing attention to issues of product liability. Software is frequently distributed under shrink wrap and click wrap licenses that absolve vendors of any problems. This practice is being questioned, however, as users become increasingly fed up with faulty software. If vendors are held liable for security flaws, or

at least flaws resulting from sloppy software development practices, this would provide a strong incentive to deliver better products.

The growing vulnerability problem has also stimulated a lively debate over "open source" software, that is, software such as Linux whose source code is open for public scrutiny, vs. closed systems like Windows whose source code is proprietary and kept secret. On the one hand, open systems have the potential of being more secure than closed ones, because it is easier to find and fix flaws when anyone can examine the source code and anyone can post a fix. With closed systems, users are dependent on vendors to fix, if not find, the flaws. On the other hand, hackers also have an advantage when they can get access to source code, and they may decide to exploit the problems they find rather than report them. Moreover, making the code available to public scrutiny does not mean anyone will in fact study it closely. On balance, whether a system is open or closed might not matter much in terms of security.[24] Security might be affected more by the priority and practices of the vendor.

ECONOMIC FACTORS

The economic factors shaping the security infrastructure can be analyzed in terms of three groups of people: buyers, sellers, and donors. Buyers pursue security primarily to avoid economic losses. Sellers, on the other hand, see security as a business opportunity and way of making money. Finally, donors, who are predominantly government agencies, see security as a national issue worthy of funding.

ECONOMIC LOSSES

Organizations invest in security to avoid or at least contain the damages that result from an attack. These damages can include the cost of investigating and responding to an attack (e.g., clearing out viruses and restoring data), lost revenue and employee productivity from system down time, lost business due to lost credibility and customer confidence, and litigation costs. Company stocks can also drop following press reports of certain types of incidents. A study of the economic effect of information security incidents conducted at the University of Maryland found a significant negative stock market reaction to security breaches involving unauthorized access to confidential data. Interestingly, there was no significant market reaction for other types of incidents (e.g., web site defacements and denial-of-service attacks).[25] Finally, some companies have been put out of business by attacks. In February 2002, CloudNine Communications, one of Britain's oldest Internet Service Providers, shut its doors following a distributed denial-of-service attack. They concluded that repairing their network would have required too much downtime to remain in business.[26]

A few studies have attempted to quantify losses on a global or organizational basis. *InformationWeek* and PricewaterhouseCoopers LLP estimated that computer-based attacks took a $1.6 trillion toll on the worldwide economy in the year 2000 based on their global survey. The cost to the United States alone was an estimated $266 billion, or more than 2.5% of the nation's Gross Domestic Product. Computer Economics of Carlsbad, California, estimated that the ILOVEYOU virus and variants, which crippled computers in May 2000, cost $8.5 billion in damage worldwide, vastly exceeding the damages from any previous or subsequent virus.[27] The Computer Security Institute and

FBI reported that their 2002 survey received reports of incidents costing a total of $456 million.[28] These losses represented 223 companies (out of 503 responding to the survey), for an average loss of over $2 million. Whether any of these numbers is accurate or not matters less for security than that they are being used to justify the expenditure of more resources to solve security problems.

Ideally, security would be free, fast, and foolproof. In practice, it is never all three, and companies need to make hard choices about how much to spend and what to spend it on. In determining security expenditures, a reasonable goal is a positive return on investment (ROI): spend X dollars on security and save at least X in losses from attacks. The difficulty, however, is that it can be hard to compute ROI for a given approach. Consequently, security purchases and practices are often based on other factors such as industry best practices, fear of attack, product ratings, salesmanship, advise from consultants, budget restrictions, and so forth.

Quantitative measures, however, have proven effective for evaluating certain security options. Virtual private networks (VPNs) that run over the Internet, for example, have been shown to provide a cheaper means of protecting communications than separate leased lines. And research conducted by @stake Labs has shown that by following certain steps to harden network servers from attack, thruput on their sample networks improved by 1.93% to 3.28% on average.[29] As a third example, RTI International assessed the benefits of role-based access controls (RBAC) relative to alternative access control systems (e.g., lists of specific users authorized to access particular files). From their study, they projected a net present value of RBAC through 2006 of approximately $671 million.[30] The figure takes into account end-user's operational benefits as well as

their implementation costs and research and development costs.

Economic incentives to invest in security will be influenced by liability and insurance factors. If organizations are held liable for attacks against third party systems that exploit easily avoidable weaknesses in their own, they will be driven to purchase better products and services from vendors and to follow better security practices internally. Similar effects are likely if insurance premiums are tied to the security posture of an organization. Standards and best practices will play an important role in establishing security baselines for negligence and insurance premiums.

BUSINESS OPPORTUNITY

The growing rate of cyber attacks led many entrepreneurs to view the attacks not just as a threat, but also as a business opportunity. In 2000, the worldwide Internet security market reached $5.1 billion in revenue, according to market researcher IDC. This was a 33% increase over 1999. IDC projected that revenues would surpass $14 billion in 2005.[31]

Industry is often accused of hyping the threat or overstating the benefits of their products in order to stimulate demand and increase business. However, the threat is real and serious. Moreover, it is aggravated by hackers, who attack systems and publish vulnerability information and hacking tools, in some cases as a way of getting jobs in the security industry and selling themselves as security consultants.

Until recently, security was not a priority for most organizations. Product selections were based more on factors such as cost, functionality, performance, and ease-of-use than on security. Consequently, vendors could not make a business care for

building secure products in an environment where cost and time-to-market were critical. This is changing, as security has become a higher priority.

The adoption of standards by government and industry groups affects the market by helping some products and vendors, while hurting others. For example, by selecting the Rijndahl encryption algorithm for its Advanced Encryption Standard, the U.S. government pushed the market to favor Rijndahl over certain competing methods. De facto standards also matter, as when the industry began using SSL to encrypt web traffic.

Patents also affect the market. They stimulate innovation by offering inventors a means of protecting their work; this is the usual rationale for patents. They do more than that, however—patents also push companies to invent new technologies so as to avoid paying license fees for products protected by existing patents. In this regard, they stimulate innovation, but at a cost of decreased standardization and interoperability.

Another factor affecting the market is government regulation, including trade restrictions. Until a few years ago, export controls on encryption technologies placed U.S. companies at a disadvantage in international markets and generally held back the spread of encryption. Those controls were substantially liberalized in 1999, however, so this is no longer a significant factor.

Government regulation can take the form of product requirements. In March 2002, Senator Fritz Hollings introduced a bill that would prohibit the sale and distribution of "digital media devices" that did not feature copyright-protection standards to be set by the federal government. The Consumer Broadband and Digital Television Promotion Act received considerable support from Hollywood, which seeks technology to protect their intellectual property from distribution on the Internet in violation of copyrights. The IT

industry, however, generally opposes any government regulation, as it denies them certain business opportunities.

Governments have influenced the security market by issuing criteria for assessing the security offered by a product. The U.S. Department of Defense Trusted Computer System Evaluation Criteria (the "Orange Book") and more recent international Common Criteria, for example, have led to products that meet specified security objective and an industry segment concerned with product evaluations. The cost of building to standards and performing product evaluations, however, has limited the market for evaluated products.

SECURITY FUNDING

Grants issued by the National Science Foundation, Department of Defense, and other public and private sector organizations have encouraged security research and the development of security courses and programs in academia. These efforts have led to innovations in security and to a growing cadre of security specialists.

One grant program specifically aimed at increasing the cyber defense capability of the nation is the Federal Cyber Service Scholarship for Service program. The program offers scholarship and capacity building grants to universities in the area of security. The objective is to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of colleges and universities within the United States to produce professionals in these fields. Students receiving scholarships are required to work for a federal agency for two years as their federal cyber service commitment. The program, which is administered by the National Science

Foundation, ties in with another educational initiative operated by the National Security Agency. Their program promotes higher education in information assurance and security by designating qualified institutions as Centers of Academic Excellence in Information Assurance.[32] Other programs are focused on research and development in security.

Internal funding within government agencies has also significantly impacted the security infrastructure. The National Institute of Standards and Technology (NIST), for example, has contributed numerous standards and guidelines for security, particularly in the area of cryptography, but in other areas as well.[33] The value of NIST to security developments was measured in the RTI study of role-based access control mentioned earlier. RTI found that NIST's contributions accounted for 44% of the benefits of RBAC.[34]

PSYCHOLOGICAL FACTORS

The security infrastructure is driven in part by psychological factors. These are divided into two categories: intellectual and emotional. Both relate to why people get involved in security as attackers, defenders, and participants in policy debates.

INTELLECTUAL FACTORS

I was drawn to security primarily by intellectual interests. I wanted to find ways of making systems secure, not because I had sensitive information that needed to be protected, but because I found the problem to be intellectually challenging. I recognized that security was important for protecting against cyber threats, but I was not out to save the world from hackers and information thieves.

I expect that many people in the field were similarly motivated. I recall in the mid 1990s, during the heat of the debates over cryptography policy, a prominent government official remarked that it was impossible to control cryptography because of its intellectual appeal. He was right, of course.

The intellectual attraction of security comes not only from designing security mechanisms, but also from breaking them or just attempting to break them. This is fortunate, because it is not possible to build secure systems without understanding how they might be attacked. Security is an iterative process between finding and fixing vulnerabilities that can be exploited by an adversary. The downside is that the intellectual appeal of cracking systems also motivates the hackers. A survey of 164 hackers conducted by Nicholas Chantler of Queensland University of Technology in Brisbane, Australia found that the top two reasons for hacking were challenge and knowledge.[35]

EMOTIONAL FACTORS

People pursue security for emotional as well as intellectual reasons. They might enter the field because they see cyber threats as a serious threat to society or are paranoid of being a victim themselves. They might find that working in security gives them a feeling of satisfaction or self-esteem. They might recommend security purchases, funding, or legislation out of fear, uncertainty, or doubt (FUD) over the seriousness of the security threat. FUD is often cited when it appears that it is being used to promote an agenda that does not stand on its own merits.

Hackers also pursue their activities for emotional reasons. Chantler's study found

that the number three reason for hacking was the pursuit of pleasure. After that came an assortment of emotional, social, and financial reasons, including recognition, excitement (of doing something illegal), friendship, self-gratification, addiction, espionage, theft, profit, vengeance, sabotage, and freedom. [36]

If hacking had no intellectual or emotional appeal, it is unlikely we would have the serious problem we have today. Hackers may not be responsible for some of the most serious attacks, but they have contributed substantially to the base of knowledge and tools needed to carry out an attack. Of course, hackers alone cannot be blamed for this, because security professionals also publish information about security vulnerabilities on the grounds that doing so will lead to better security.

SOCIAL AND POLITICAL FACTORS

The security infrastructure is shaped by social and political factors. This section describes four areas of influence: national security and public safety, privacy, information sharing, and international cooperation.

NATIONAL SECURITY AND PUBLIC SAFETY

Governments are responsible for the national security and public safety of their countries. To address the cyber threats, they have adopted laws that criminalize cyber crimes and regulations mandating security in certain sectors, established organizations and programs that help with cyberspace defense, and allocated money for cyber defense research, education, and other programs.

In the United States, improving the security of critical infrastructures and

cyberspace more generally received greater attention within the Administration and Congress following the formation of the President's Commission on Critical Infrastructure Protection in 1996. Their recommendations led to Presidential Decision Directive (PDD) 63, which created the Critical Infrastructure Assurance Office (CIAO) within the Department of Commerce and the National Infrastructure Protection Center (NIPC), housed at the FBI but with representatives from several agencies. The CIAO was established to coordinate national planning efforts related to critical infrastructure protection.

The NIPC serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. Its focus is as much on prevention as on investigation and response. Towards that end, it issues security assessments, advisories, and alerts, the latter addressing major threats and imminent or in-progress attacks targeting national networks or critical infrastructures. The NIPC also established InfraGard chapters at all 56 FBI field offices. The chapters provide formal and informal channels for the exchange of information about infrastructure threats and vulnerabilities among people in law enforcement and the private sector. As of July 1, 2002, membership had reached 4,609.

PDD 63 also encouraged the private sector to create Information Sharing and Analysis Centers (ISACs) in cooperation with the government. The centers serve as a mechanism for gathering, analyzing, appropriately sanitizing, and disseminating private sector information related to infrastructure vulnerabilities, threats, and incidents. So far, ISACs have been established for numerous sectors, including banking and finance, telecommunications (operated by the National Coordinating Center), electric power

(operated by the North American Electric Reliability Council), oil and gas, and information technology. In addition to the ISACs and InfraGard chapters, numerous other groups facilitate information sharing, including the CERT/CC and other computer emergency response teams, the Partnership for Critical Infrastructure Protection, the High Tech Crime Investigators Association, the United States Secret Service Electronic Crimes Task Forces, the Joint Council on Information Age Crime, and the Center for Internet Security. All of these efforts can help strengthen the cyber defense and crime fighting capabilities of their members.

One of the challenges facing all of these groups is that industry has been reluctant to share information out of concern for its confidentiality. In particular, companies are concerned that sensitive information provided voluntarily might not be adequately protected, or that it could be subject to Freedom of Information Act (FOIA) requests or lawsuits. Industry is also concerned that cooperation with industry partners might violate antitrust laws. Bills have been introduced in the House and Senate to provide limited exemption from FOIA.

On October 16, 2001, President Bush issued an Executive Order on Critical Infrastructure Protection in the Information Age. The order established the President's Critical Infrastructure Protection Board (PCIPB), and charged it to recommend policies and coordinate programs for protecting information systems for critical infrastructures. It assigned several areas of activity to the Board, including outreach to the private sector and to state and local governments; information sharing; incident coordination and response; recruitment, retention, and training of Executive Branch security professionals; research and development; law enforcement coordination with national security

components; international information infrastructure protection; legislation; and coordination with the newly formed Office of Homeland Security.

The Department of Justice has launched several initiatives aimed at strengthening the cyber-crime-fighting capability of the criminal justice community. The Electronic Crimes Partnership Initiative is tackling a broad range of issues, including technology, technical assistance, legal and policy issues, education and training, outreach and awareness, and standards and certification. The partnership includes representatives from law enforcement, industry, and academia.

Within the Department of Defense, the Commander in Chief of Space Command has primary responsibility for computer network operations. Space Command's Joint Task Force Computer Network Operations (JTF-CNO) serves as the operational component for all CNO, which includes both computer network defense and computer network attack. In conjunction with the unified commands, services and DOD agencies, the JTF-CNO coordinates and directs the defense of DOD computer systems and networks.

The events of September 11 and war on terrorism are leading to new initiatives, funding, and legislation aimed at combating all forms of terrorism, including cyber terrorism. These include establishment of a Department of Homeland Defense, which will bring together programs currently housed in other agencies.

PRIVACY

Privacy issues have shaped the security infrastructure in two ways. First, they have led to laws and regulations such as HIPAA that mandate security for the purpose of privacy

protection, and to the development and use of security technologies that protect information and therefore privacy. The popular encryption package Pretty Good Privacy (PGP) was developed primary to protect the private files and e-mail correspondence of citizens from government eavesdroppers and other spies. Its author, Phil Zimmermann, was especially concerned with helping human rights activists in countries with repressive governments. There are numerous other examples of technology that offer encryption and anonymity services to enhance privacy.

Second, privacy issues have led to policies, regulations, and technology that constrain government investigations of cyber crime and cyber terrorism. Although they have provided strong privacy protections, those protections are being challenged by changes in laws and policies aimed at facilitating the fight against terrorism. The U.S. Patriot Act, for example, raised numerous concerns.[37]

In the United Kingdom, the Regulation of Investigatory Powers (RIP) bill has provisions that facilitate government monitoring of Internet traffic and access to encryption keys.[38] Opposition to the bill led one mathematician to develop a new operating system, called M-o-o-t, that would foil government surveillance by storing all data and keys on servers outside the U.K. government's jurisdiction.[39]

INFORMATION SHARING

Information sharing, both publicly and within closed groups, has helped advance the science and practice of security, and increase knowledge and awareness about security. While these effects are all positive, open publication has raised concerns about information getting into the hands of the "bad guys." Today, these concerns generally

involve the publication of information about security vulnerabilities and of software tools that exploit those vulnerabilities. At one time they also included the publication of information relating to particular security technologies, most notably cryptography, but these concerns generally gave way to those recognizing the value of publishing such information so as to promote security.

The open publication of vulnerability information raises two issues: first, how much information should be made public, and second, when should publication take place. At one extreme, under a policy of full and immediate disclosure, all information about vulnerability, including any attack software that can be used to exploit it, is posted following its discovery. The rationale is that it forces vendors to fix problems while also keeping users informed. This is supported by numerous cases in which vendors did not fix problems until the vulnerability information was published.

At the other extreme, no information about vulnerability is posted, at least until the vendor has released a patch that fixes the problem; even then, only minimal information is disclosed. The argument in this case is that posting vulnerability information, particularly hacking tools, leads to attacks. Indeed, data reported to CERT/CC showed considerably heightened attack activity following the release of exploit tools associated with certain vulnerabilities.[40] The increased activity lasted many months beyond the release of the patches, as system administrators were slow to install the fixes. Publication of exploit software had a much greater impact than publication of vulnerability information alone, because it enabled script kiddies with little skill to launch attacks.

In between the extremes are policies that favor disclosing information about

vulnerabilities, but generally not the attack tools, and giving vendors a grace period in which to release a patch before publication. The CERT/CC follows a policy giving vendors 45 days to fix their problem.[41] However, many security practitioners favor a shorter grace period. An April 2002 industry survey conducted by the Hurwitz group found that 39% of the more than 300 respondents favored disclosure immediately, with another 28% favoring disclosure within a week. However, only 13% favored posting "proof of concept" exploit software.

Although supporters of full disclosure make their argument on security grounds, they may be motivated as much by self-promotion as a desire to make systems more secure. Being first to publish can increase one's stature in the scientific, security, and hacking communities and lead to new business opportunities.

In general, it is lawful to publish exploit software, even though use of such software to conduct an actual attack is a crime. There are, however, exceptions. The Digital Millennium Copyright Act restricts the production, distribution, and use of software that circumvents copyright protection on the grounds that such software harms copyright owners.

The DMCA and its application has been challenged on First Amendment grounds. In one highly publicized lawsuit, eight movie companies sued *2600 magazine* for posting and linking to the DVD-descrambling program DeCSS.[42] After a federal district court ordered *2600* to remove the software and links from their website, the Electronic Frontier Association asked a federal appeals court to overturn the ruling. The EFF, which represents *2600*, claimed that the ruling was an "unconstitutional constraint on free speech," because it blocked legitimate uses of DeCSS such as for educational purposes.

The court rejected EFF's appeal. However, Professor David Touretzky of Carnegie Mellon University has over two dozen different versions of the DeCSS on his website, including a haiku version and a "dramatic reading" of the code, as well as versions in various programming languages.[43]

INTERNATIONAL COOPERATION

Cyber attacks frequently cross national borders as attackers hack one system after another, using each to launch an attack against the next. Such behavior severely complicates investigations, as it requires cooperation from every country involved. Further, prosecution may not be possible if the attack is not a criminal offense in the perpetrator's own country.

Governments have come together in several forums, including the G8, Council of Europe (CoE), and European Union to address the problems associated with international attacks and facilitate international cooperation. The CoE's effort led to the adoption of Convention on Cyber-Crime in 2001. The Convention aims to harmonize domestic statutes relating to cyber crime and procedures relating to extradition, mutual assistance, and evidence collection and preservation.[44] However, because the signatories to the convention are limited to the Council of Europe members and official observers (the United States, Canada, Japan, and South Africa), a broader-based international treaty is needed to address cyber crime on a global scale. A group at Stanford University proposed an International Convention on Cyber Crime and Terrorism that builds upon the CoE's work[45]

CONCLUSIONS

This chapter has approached the topic of cyber security and critical infrastructure protection from a right angle. Instead of focusing on infrastructure defense, the chapter has viewed cyber security as an infrastructure in its own right, and focused on the factors shaping its development.

This security infrastructure consists of technologies, procedures and practices, laws and regulations, and people and organizations. It is not owned by any party, and is dispersed globally throughout the public and private sector. It is regulated only to the extent that regulations apply to elements of the infrastructure, for example, the adoption of cyber crime laws and the formation of corporations and associations that specialize in security. It is a relatively new infrastructure, tied closely with the emergence of information technology as a fundamental component of business practices, control systems, and other processes.

The factors shaping the infrastructure include threats, technology trends, economic factors, psychological factors, and social and political factors. Examining these factors shows why security is a major problem today. Security threats, amplified by technology trends, have outpaced the economic and social case for developing and operating secure systems. However, that case has been building, stimulating rapid growth of the security infrastructure and lending hope that enough progress can be made to avoid a major catastrophe from a cyber attack against critical infrastructures. Just as the international community responded to the Y2K bug, which also threatened critical infrastructures, it may effectively respond to the security problems that still plague information systems. That security is now a high priority in both the public and private

sector is encouraging.

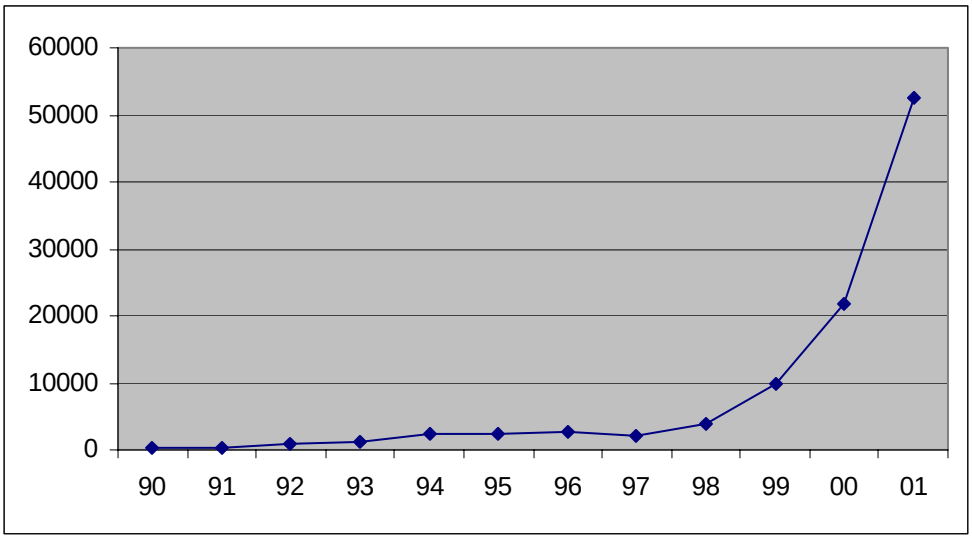

Figure 1. Security Incidents Reported to CERT/CC.

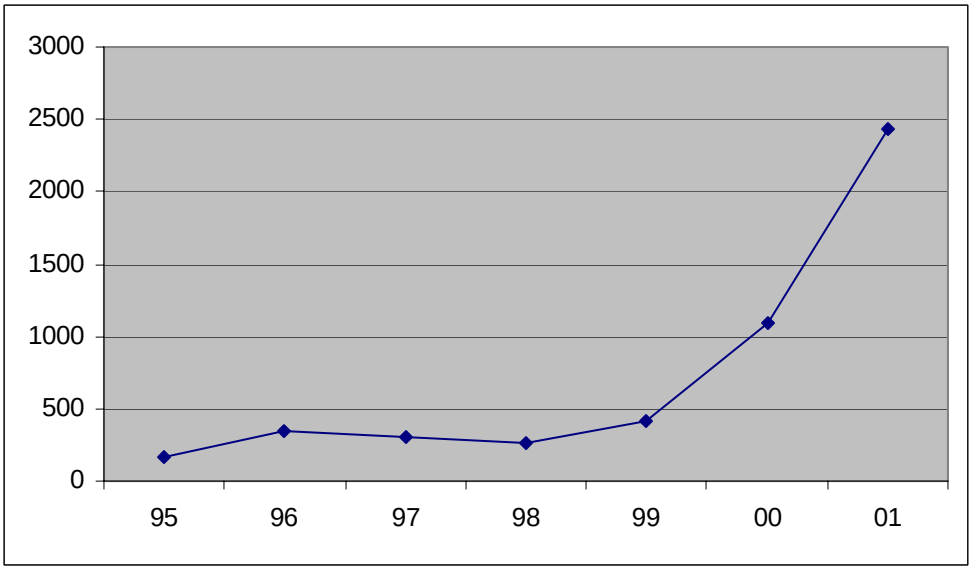

Figure 2. Vulnerabilities Reported to CERT/CC.

[1] The NIST web site has information about best security practices for federal agencies http://csrc.nist.gov/fasp/

[2] For a discussion of networks in the context of conflict and net wars, see John Arquilla and David Ronfeldt (eds.), *Networks and Netwars*, in RAND (2001).

[3] David Noack, "Employees, Not Hackers, Greatest Computer Threat," in *APBNewscenter* (January 4, 2000).

[4] Dorothy E. Denning, "Is Cyber Terror Next?" The Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm

[5] Ibid.

[6] Barton Gellman, "U.S. Fears Al Qaeda Cyber Attacks," in *Washington Post* (June 26, 2002).

[7] Tim McDonald, "CIA to Congress: We're Vulnerable to Cyber-Warfare," in *NewsFactor Network* (June 22, 2001).

[8] For the latest figures, see http://www.cert.org.

[9] mi2g press release, London (January 8, 2002).

[10] http://www.messagelabs.com/

[11] http://www.truesecure.com/

[12] David Moore, Geoffrey M. Voelker, and Stefan Savage, "Inferring Internet Denial-of-Service Activity," Proc. USENIX Security Symposium (August 2001).

[13] Riptech Internet Security Threat Report (January 2002). www.riptech.com.

[14] "Attack on Japan Airline affected 15,000 passengers," in *Security News Portal* (August 11, 2001).

[15] "Sewage Hacker Jailed," in *Herald Sun* (October 31, 2001).

[16] Robert Vamosi, "Cyberterrorists Don't Care About Your PC," in *ZDNet Reviews* (July 10, 2002).

[17] "Wireless London is Wide Open," in *BBC News* (March 26, 2002).

[18] David Moore, "The Spread of the Code-Red Worm (CRv2)," Cooperative Association for Internet Data Analysis (July 2001), www.caida.org.

[19] Stuart Staniford, Gary Grim, Roelof Jonkman, "Flash Worms: Thirty Seconds to Infect the Internet," Silicon Defense (August 16, 2001).

[20] For a description of advanced hacking tools and how to counteract them, see Edward Skoudis, "Faster, Stealthier … More Dangerous," in *Information Security* (July 2002), pp. 40-49.

[21] http://66.129.1.101/top20.htm

[22] Elinor Mills Abreu, "Gates Says Microsoft Security Push Cost $100 Million," in *Reuters* (July 18, 2002).

[23] Kevin Soo Hoo, Andrew W. Sudbury, and Andrew R. Jaquith, "Tangible ROI Through Secure Software Engineering, *SBQ*, 1:2 (Fourth Quarter, 2001), pp. 8-10.

[24] Ross Anderson, "Security in Open versus Closed Systems – the Dance of Boltzmann, Coase, and Moore," (2002).

[25] Lawrence A. Gordon, Martin P. Loeb, Lei Zhou, and Katherine Campbell, "Information Security Breaches: The Economic Effect on Corporations," The University of Maryland, School of Business, May 2002.

[26] "How CloudNine Wound Up in Hell," in *Reuters* (February 1, 2002).

[27] The Computer Economics Security Review 2002 (April 2002); http://www.computereconomics.com/article.cfm?id=356.

[28] "CSI/FBI 2002 Computer Crime and Security Survey," *Computer Security Journal*, XVIII:2 (Spring 2002), pp. 7-30. For a summary, see www.gocsi.com/press/20020407.html.

[29] @Stake Labs, "Defined Security Creates Efficiencies," *SBQ*, 1:2 (Fourth Quarter, 2001), pp. 10-13.

[30] The Economic Impacts of Role-Based Access Control, prepared by RTI International for NIST, March 2002; http://www.nist.gov/director/prog-ofc/report02-1.pdf.

[31] Robert Lemos, "Networking Report: No Slump for Security Biz," *ZDNET News*, (August 22, 2001).

[32] http://www.nsa.gov/isso/programs/coeiae/index.htm

[33] See http://csrc.nist.gov/fasp/ for information about NIST's security projects.

[34] The Economic Impacts of Role-Based Access Control, prepared by RTI International for NIST, March 2002; http://www.nist.gov/director/prog-ofc/report02-1.pdf.

[35] Nicolas Chantler, *Profile of a Computer Hacker* (Seminole, FL: Inter.Pact Press, May 1997).

[36] Nicolas Chantler, *Profile of a Computer Hacker*.

[37] See the Center for Democracy and Technology website: http://www.cdt.org/security/010911response.shtml.

[38] See, for example, http://www.fipr.org/rip/

[39] Will Knight, "Anti-Snooping Operating System Close to Launch," *NewScientist,* (May 28, 2002).

[40] William A. Arbaugh, William L. Fithen, and John McHugh, "Windows of Vulnerability: A Case Study Analysis," in *IEEE Computer*, 33:12 (December 2000), pp. 52-59.

[41] http://www.kb.cert.org/vuls/html/disclosure.

[42] Declan McCullagh, "DeCSS Allies Ganging Up," in *Wired News* (January 26, 2001).

[43] http://www.cs.cmu.edu/~dst/DeCSS/Gallery/index.html

[44] http://conventions.coe.int

[45] Abraham D. Sofaer and Seymour E. Goodman, A Proposal for an International Convention on Cyber Crime and Terrorism, Center for International Security and Cooperation, Stanford University (August 2000).