

June 15, 2004

Advanced technology, advanced danger

Standardized technology and increased connectivity jeopardize national cybersecurity

For people who live in developed nations, the 21st century is truly a digital age. Wireless communication and Internet access have become deeply ingrained in daily life, contributing to tremendous productivity gains while creating dangerous vulnerabilities. As quickly as one ingenious individual develops a technological solution to enhance quality of life, another just as rapidly finds a way to exploit the innovation for personal gain.

Government and corporate entities—and many individuals, in fact—cannot afford to lose the competitive advantage made possible by technology, yet they often buy into these solutions without examining, and safeguarding against, the potential vulnerabilities. This dangerous situation is tantamount to electronic Russian roulette, with the stakes ranging from mere annoyance to business interruption and loss of reputation to economic disaster.

Types of threats

As information technology grows in sophistication, so do the criminals who plunder its vulnerabilities. Intruders keep up with the new technology and analyze ways to take advantage of security holes; consequently, they are able to develop new, more complex methods of attack. Even though many of these threats date to the beginning of the Internet age, greater user sophistication makes them more dangerous than ever.

Hackers. While the term “hacker” can refer to any individual especially proficient in programming, it often describes users who use those skills to gain unauthorized entry into computer networks—sometimes for the simple purpose of expanding their computer knowledge, but frequently with malevolent intent.

Malware. Malicious code such as viruses and worms cause huge economic losses each year. The problems created by these programs have become increasingly severe as more computers use the same operating systems with the same vulnerabilities. Compounding the problem is the growing prevalence of cable modems and digital subscriber lines (DSL), which remain connected to the Internet while the computer is on. Once introduced to the Internet, these programs can

wreak global havoc in a matter of hours: the SQL Slammer worm infiltrated networks in Europe, Asia and the Americas in January 2003, shutting down certain ATMs for half a day and forcing one airline to book flights with pen and paper because the worm had disabled its computer systems.

Denial of service. These types of attacks prevent legitimate users from accessing a service, often achieved by overloading or disrupting connections to a network. These assaults can produce significant loss of time and money through business interruption, as well as through loss of customer confidence.

Identity theft. The media have reported numerous accounts of hackers successfully accessing databases that house thousands of credit card and Social Security numbers. The Federal Trade Commission estimates that almost 10 million Americans fell victim to identity thieves last year. The average loss to businesses, including financial institutions, was \$10,200 per identity.

Insiders. In the modern workforce, with employees feeling increasingly disenfranchised, fraud or sabotage by insiders continues to threaten company assets. Workers have the knowledge and the opportunity to exploit system vulnerabilities—sometimes out of desperation, sometimes for retribution.

A small world

Contributing to the tremendous productivity gains of recent years is the increasingly widespread use of standard, off-the-shelf operating systems. This trend enhances connectivity and ensures compatibility, but it also exacerbates the weaknesses created by security flaws in the software.

New vulnerabilities are reported weekly. Upon discovering the hole, the software companies immediately issue a program to repair the problem, known as a “patch.” Users download these fixes free of charge and install them on their systems. Usually, the process takes only a few minutes, but the sheer

(continued on next page)

Advanced technology, advanced danger

Standardized technology and increased connectivity jeopardize national cybersecurity

(continued from preceding page)

volume of security flaws being uncovered—multiplied by the number of computers and users in any given organization—quickly drains a company's resources.

Firms cannot afford to fall behind in patch management, however. Once a hole is publicized, hackers leap to utilize it. "The time it takes from the discovery of a software vulnerability to the use of the first exploitation is diminishing to a matter of days—and in some cases, hours," says Richard A. Clarke, retired Special Adviser to the President for Cyberspace Security and the former Chairman of the President's Critical Infrastructure Protection Board.

In addition, patch installation sometimes creates compatibility problems with other software applications, which require additional time and money to fix.

As a result, there is a growing movement to pressure software developers to improve quality assurance by redesigning their codes to incorporate security into the infrastructure of the product. Last month, the Business Roundtable—an association whose membership includes the CEOs of some of the nation's largest companies—released a statement aimed at advancing cybersecurity policy development, which pointed out that "most of the significant cyber incidents that have harmed American business and consumers over the past several years have had at their root cause defective and readily exploitable software code." Examples include the Blaster worm, which struck more than 1 million computer systems worldwide in August 2003, and the recent Sasser worm.

Potential impact on national security

Besides the debilitating economic tolls of computer crime—a survey of 500 computer security executives released last month reported an estimated \$666 million in losses in 2003—exploita-

tion of information technology could hold dire consequences for homeland security.

For instance, identity theft represents a special threat to national security during this period of rising anti-American sentiment. Terrorist organizations such as al Qaeda could steal the identities of American citizens to facilitate placement of "sleepers"—terrorist agents that embed themselves in communities until called to action. The ease with which computers can be plundered for personal information has helped make identity theft one of the fastest-growing crimes in the United States.

Computer worms and viruses negatively impact productivity by millions of dollars each year, but depending on the specific payload of these malicious codes, they can endanger lives if they propagate as quickly as the Blaster worm, for example. Earlier this year, FBI agents arrested a man for releasing a worm in 2002 to 21 WebTV users that reprogrammed computers to dial 9-1-1 instead of a local Internet access telephone number. As a result of this mischief, police were dispatched to at least 10 homes from California to New York. On a wide scale, timed in concert with a conventional terrorist attack, a similar program could produce devastating consequences for the public health system.

Yet another cybersecurity vulnerability that threatens national security involves computerized control systems, which perform essential functions across many of the country's critical infrastructures. These systems can monitor and control the generation, transmission and distribution of electricity. They can remotely manage the pressure and flow of oil and natural gas pipelines. Control systems are also frighteningly insecure, due to the transition from proprietary software to less expensive, standardized technologies with known vulnerabilities. The General Accounting Office (GAO) published a report last March that focused on the challenges of securing these systems, including limitations of current security technologies, network integration and external connecti-

ty, and the public availability of detailed information about infrastructures and control systems.

In April 2000, Australian police stopped a car and discovered a stolen computer and radio transmitter inside. The driver had used commercially available technology to transform his vehicle into a pirate command center for a sewage treatment plant, systematically leaking hundreds of thousands of gallons of fetid wastewater into rivers and parks over two months. In each of 46 successful intrusions, the man gained complete command over 300 systems controlling sewage and drinking water alike. The case represents the only known instance in which someone deliberately manipulated a digital control system to cause harm: A former employee of the company that provided the utility's remote control equipment, the man was trying to obtain a consulting contract to repair the problems he had caused.

Protecting private systems

Organizations in the private sector can take several actions to help protect their assets against loss and, ultimately, to strengthen the nation's vulnerability to electronic attack. First and foremost, companies need to know who has physical access to their systems by conducting comprehensive background investigations of employees and by requiring the same diligence in selection from external consultants and other vendors. Any changes in service personnel, for instance, must be cleared by management.

Additional steps to strengthen security include the following:

Employ encryption. To safeguard against the interception of sensitive information, companies need to encrypt e-mail communication both within the firm and with external suppliers and business partners. The market offers several good, relatively inexpensive encryption programs, making this security measure highly affordable. In implementing encryption technology, organizations and individuals must remember that encryption simply

shields electronic messages from prying eyes; it neither guarantees the identity of the sender—a process known as authentication—nor does it ensure the safety of the contents.

Use two-factor authentication. Simple password authentication can be easily compromised, primarily because many users follow poor password security: they use easy-to-guess passwords or they write their passwords down and post the reminders at their workstations. As an added security measure, organizations should strengthen their authentication policies through the implementation of tokens, including smart cards that generate dynamic passwords, or even biometrics, to secure especially sensitive information.

Enact strict access management. Network administrators should develop and implement a rigorous access-control policy, granting employees access only to those portions of the network required for their specific jobs. Those computers that store critical information—the loss of which could jeopardize business continuity—should not be connected to an external network or the Internet. This segregation policy is especially important for utilities and other companies that use digital control systems. “Anyone running a digital control system needs to be entirely sure that it's segregated from the Internet,” warns Clarke. Every time his organization has audited a firm that believes these critical systems have no external connections, investigators find that “someone has made a connection—either for billing purposes or something else.”

Conduct automated vulnerability audits. System administrators need to configure the network to automatically perform a vulnerability assessment each night. Such assessments no longer require the expertise of external consultants but can be conducted using widely available software. These automated scans can identify such vulnerabilities as the addition of a machine using outdated antivirus definitions or user tampering.

(continued on next page)

Advanced technology, advanced danger

Standardized technology and increased connectivity jeopardize national cybersecurity

(continued from preceding page)

According to Clarke, these precautions significantly enhance an organization's computer security program. "Increasingly, I think big companies that take cybersecurity seriously are moving to usually three out of those four, if not all four, and they're not that expensive," he said. "You know the old saying: 'Pay me now or pay me later.'"

Strengthening the national cybersecurity initiative, however, requires widespread cooperation within industries and collaboration with federal lawmakers. Since its publication in February 2003, the Bush administration's National Strategy to Secure Cyberspace—a bottom-up initiative created through a series of national town-hall meetings with dozens of professional organizations and trade associations—has not been implemented. Meanwhile, increased interconnectivity and user sophistication have made the nation's computers more vulnerable to attack than ever: Two years ago, it took weeks for computer worms to infect computers around the globe; now, a dangerous worm can spread to hundreds of thousands of machines worldwide within 15 minutes.

By taking the following actions, organizations can help prevent catastrophic exploitation of the nation's electronic vulnerabilities:

Develop industry-wide security initiatives. The banking and finance industry has long focused on hardening its systems against electronic attack, but few other infrastructure sectors have made the same commitment to security. Companies must make a proactive decision to invest in security; failing to do so constitutes a risk that could ultimately jeopardize the viability of the business. To help protect the national infrastructure—as well as shareholder assets—leading firms within each industry need to form a voluntary organization and establish best practices and industry standards for security. Such internal initiatives will prove more effective than external regulations mandated by government officials who do not understand industry needs.

Support cybersecurity legislation. Business leaders need to speak with their government representatives and encourage efforts to legislate the national cybersecurity strategy. No action has been taken to put this important plan into practice. By demonstrating support for this initiative, the private sector can influence policymakers to translate this strategy into stronger security.

In many ways, the realm of cybersecurity remains a wild, untamed frontier. New technologies continue to flood the market, with the majority of these innovations focusing on efficiency and productivity and incorporating security as an afterthought—if at all. Meanwhile, the criminal element takes advantage of these same advancements to further its own goals, often at the expense of others.

The widespread use of standardized software technologies with known vulnerabilities, coupled with increased connectivity, represents a double-edged sword to members of the modern digital society: seamless integration and dangerous exposure. The tremendous expense and subsequent loss of system compatibility required to protect information through development and implementation of proprietary software applications rules out the feasibility of this option as a solution. Consequently, businesses and individuals must make a conscious effort to protect themselves in the current insecure environment.

Computers have become an integral part of daily life, and users have a responsibility to employ technology with a prudent commitment to security. At the very least, a bored hacker or disgruntled employee will take advantage of security laxity and cause an annoying inconvenience. At worst, a terrorist or other criminal will exploit these widespread weaknesses to catastrophic result.



The Lipman Report Editors