cyanide capsule on his person. Instead of committing suicide, when the Soviets shot down his plane, Powers parachuted to earth, and was taken prisoner. Later, after his captors had reaped enormous propaganda benefits from the incident, he was traded for a Soviet spy in a prisoner exchange.

FURTHER READING:

BOOKS:

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

Minnery, John. *CIA Catalog of Clandestine Weapons, Tools, and Gadgets.* Boulder, CO: Paladin Press, 1990.

ELECTRONIC:

Facts About Suicide. Centers for Disease Control. <http://www.bt.cdc.gov/agent/cyanide/index.asp> (March 19, 2003).

International Spy Museum. <http://www.spymuseum.org> (March 19, 2003).

SEE ALSO

Assassination
Assassination Weapons, Mechanical
Biochemical Assassination Weapons
Chemical Warfare
Intelligence Agent
U-2 Incident

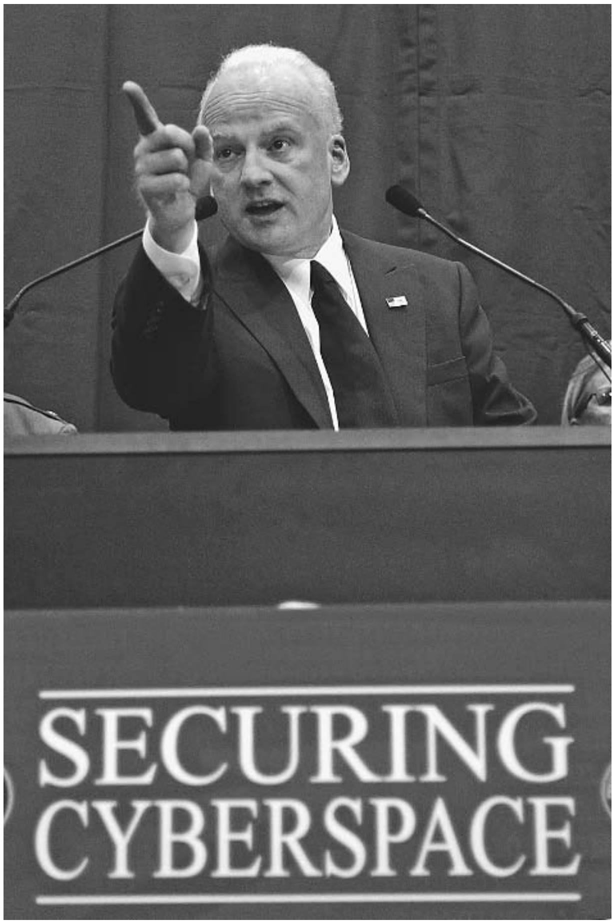
Cyber Security

BRIAN HOYLE

Cyber security—measures taken to protect computers and computer networks from accidental or malicious harm—is an ongoing process. The security of a system is only as strong as its weakest link. When a fault is identified and corrected, the system tends to be stronger. This state is often transient, as other faults are eventually be detected and exploited.

The very nature of the Internet makes cyberspace vulnerable to attack. The vast majority of computers connected to the Internet are IBM compatible, as are the few operating systems that control their function. An attacker who can find a security flaw in even one computer could gain access to many computers that are not protected from intrusion.

An attack can be circuitous, involving many computers. Some computers are used surreptitiously in the attack; thus, the source of an attack becomes difficult to trace, especially if the attack has disguised the source address. While in the past, most breaches of computer security were mischief caused by computer hackers, increasingly, the information contained within computer databanks is probed and in some cases, altered.



Richard Clarke, the White House's senior security advisor, outlines the administration's 2002 cyberspace security recommendations that include educating users and urging market forces, not government mandates, to fix cybersecurity problems. AP/WIDE WORLD PHOTOS.

Such disabling of computer networks can be crippling to business or infrastructure. The 1997 Presidential Commission on Critical Infrastructure concluded that cyber security was as essential to the functioning of the United States as water supplies, and declared cyber security vital to U.S. national interests. In November 2002, the U.S. government passed the Cyber Security Research and Development Act, which dedicates almost one billion dollars to the establishment of cyber security research and training centers.

Cyber Security Threats

A practice dubbed "dumpster diving" involves routing through the trash to recover paperwork or even used computer components that have been discarded. Even in the computer age, many people print information and then discard it. A diligent search of a person's trash can sometimes obtain a great deal of sensitive information.

Intelligence personnel masquerading as janitors or other staff can gain access to computers in off-hours, and, utilizing deciphered user names and passwords, can delve into databases for information.

Cyber security also focuses on equipment. Computers that are linked via electrical wire (i.e., Ethernet networks) typically have many wall jacks ("network drops"), by which computers are connected to the network. A vacant network drop that has not been disabled can be surreptitiously used to connect with the network. Software is available that enables the connected computer to capture all data that is flowing through the network.

Wireless networks carry other security risks, as a rogue computer does not need to be physically connected to a network drop in order to acquire information. Furthermore, if the signal from a wireless network extends beyond the boundaries of a building, intelligence can be gathered even from someone parked outside.

Usernames and passwords are another vulnerable aspect of a computer network. The tendency of people to trust someone making a request for user information, and to use the same easy-to-decipher identifiers repeatedly can allow an intruder to gain access to a network.

Email is especially prone to breaches in security. The information in most emails, including the username, is in plain text. Applications are available (i.e., MailSnarf) that allow email transiting from sender to receiver to be retrieved and read by a third party. Thus, an attacker can read sensitive information contained in an email and as well, can hijack an email account to send and receive messages. Emails often have documents attached to them. This route is used to deliver malicious codes (i.e., viruses, worms, Trojan Horses) to computers.

Viruses are small programs that become embedded in files. Once a file is infected, the virus can execute its function. Depending on the intent of the virus designer, the result can be merely inconvenient to extremely destructive. Thousands of viruses exist, with new ones appearing daily. Thus, viral cyber security requires constant updating of viral protection software.

Trojan Horses are applications that are disguised as useful programs. Once activated, Trojan Horses permit a remote user to have access to the host computer, via the activated program. This aspect is especially relevant in espionage and the subterfuge can be difficult to detect.

Attackers sometimes utilize authorized network connections, in effect assuming the identity of the authorized user. Another attack strategy is called man-in-the-middle. Here, a third party—the attacker or intelligence-gatherer—impersonates both ends of a connection. The real sender and receiver are unaware that their communications are not proceeding directly to the destination. A third strategy is called the replay attack. In the replay attack, transmissions are intercepted, read, and passed along to the rightful final destination.

Cyber security Measures

The perimeter security model is the most popular type of cyber security model. The defenses are set to prevent intrusion while allowing authorized user activities to proceed unimpeded.

Typical perimeter defenses include firewalls (which filter incoming information according to set criteria for acceptance, such as IP address, domain name, protocol of sender-receiver communication, key words or phrases), intrusion detection systems, and virtual private network servers (where data is encrypted at the sending end and decrypted at the receiving end). When all the components are operating properly, a perimeter defense allows only those authorized activities to proceed from the 'outside' (i.e., the Internet) to the individual computer or computer network. However, improperly configured perimeter devices can create an illusion of security while offering little security at all.

Administrative scrutiny. Data are often backed up onto tapes. Being portable, the tapes are liable to theft. If the tape data are not encrypted, the information can be transferred or copied to another computer.

Another aspect of cyber security is the identification and approval of all hardware. The unapproved installation of a piece of hardware such as a modem or a firewall can compromise an entire network, if the installed item is not properly configured. For example, an improperly configured firewall can allow access to the Internet when only receipt and transmission of email should be permitted. A dedicated systems administrator is the best guarantee of daily scrutiny of a network's performance and vulnerability. A key component of a cyber security plan is the presence of a fallback plan in case of misadventure or deliberate sabotage.

Evaluation of the performance of some security measures is a prudent precaution. This can only be accomplished by triggering the measures by a staged attack. For example, former computer hackers are now employed by companies and government agencies to probe the vulnerabilities of a computer system. This surreptitious testing, even of the security personnel, is known as red-teaming.

Breaching of cyber security. Computer and network security tends to be expensive and can require additional operations on the part of the user. The installation of safeguards does not increase the operational efficiency of a computer system, and can often add more layers to the operation of the computers. Until an attack, the value of the cyber security will be invisible. Thus, users and administrators can resist the implementation of cyber security measures. Without dedicated scrutiny, the cyber security measures that are in place can lapse over time, creating opportunities for breaching of the system.

FURTHER READING:

BOOKS:

Bosworth, Seymour (ed.) and Michel E. Kabay. *Computer Security Handbook.* New York: John Wiley & Sons, 2002.

National Research Council, Computer Science and Telecommunications Board. *Cyber Security Today and Tomorrow: Pay Now or Pay Later.* Washington, DC: The National Academies Press, 2002.

Northcutt, Stephen, Lenny Zeltser, Scott Winters, et al. *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs) Routers, and Intrusion Detection Systems.* Indianapolis: New Riders Publishing, 2002.

ELECTRONIC:

How Stuff Works. "How Firewalls Work." Jeff Tyson. <http://www.howstuffworks.com/firewall.htm> (15 December 2002).

SEE ALSO

Codes and Ciphers
Electromagnetic Pulse
Internet Spider

Cyber Security Warning Network

JOSEPH PATTERSON HYDER

Communication is critical during a time of national crisis. Emergency personnel need the ability to communicate quickly and effective with their colleagues in other parts of the country. In wartime, generals must remain in close contact with commanders and troops in the field. In the computer age, all communications systems—telephones, cellular phones, email, and others–are intertwined. A cyberattack that takes down the Internet by attacking root servers would also have a profound effect on all forms of communications, which rely on switches and routers to relay signals. Therefore, a cyberattack coordinated with other terrorist attacks or occurring during wartime could have catastrophic effects on national security and the economy.

In 2001, the George W. Bush administration and emergency response officials began studying what would have happened if an attack on America's communication infrastructure had coincided with the September 11, 2001 terrorist attacks. The more important question, however, was how to stop such an attack. The result was the Cyber Warning Information Network (CWIN), part of Bush's National Strategy to Secure Cyberspace.

Although the CWIN is not fully operational as of 2003, one proposed function of the CWIN is to prevent cyberattacks. The CWIN will accomplish this by creating several industry specific workgroups, or Information Sharing and Analysis Centers (ISACs). Each ISAC will monitor Internet activity and cyberattacks on Web sites and Internet infrastructure within its sector. The government agencies, companies, and network security firms involved in that ISAC will then communication with each other on cyberattacks and increase security to prevent future attacks. IF action is taken quickly enough, an ISAC will be able to stop the spread of computer viruses before they strike important systems.

The Clinton administration developed the ISAC concept. Currently, ISACs exist for each of the following sectors: information technology, banking and finance, telecommunications, chemical, and energy. The Bush administration worked with government agencies and the private sector to develop ISACs for public transportation infrastructure, water treatment, and agriculture and food.

While the idea of sharing information about particular network security vulnerabilities in order to increase security for all interested parties was considered favorable, many private sector members have been slow to volunteer network and software security problems. The Freedom of Information Act covers the CWIN, so these organizations have shown hesitancy that any information shared with fellow ISAC members might become public. Until these companies receive a privacy guarantee from the government, CWIN will not function as effectively as intended.

The second major function of the CWIN will be to allow each ISAC to operate as an individual network, even if the entire Internet is damaged in a cyberattack. This will allow ISAC members to continue to exchange critical information if all other communications systems are down. The CWIN will accomplish this by establishing an independent IP network for each ISAC.

Critics have found flaws with the CWIN on both conceptual and organizational grounds. Detractors argue that in order for the CWIN to be effective, the private sector and network security professionals will have to play a major role. So far, the government has offered few incentives for the private sector to invest the money and labor necessary to accomplish this objective. The Department of Homeland Security has also concerned some of the private