Cyber Attacks

Neil C. Rowe
U.S. Naval Postgraduate School, USA

INTRODUCTION

Information systems (computers and networks) are increasingly the targets of attacks ranging from vandalism to serious crimes (Richardson, 2003). Since government systems are valuable resources for a society, it is important to protect them from such attacks. Unfortunately, however, government systems can be especially vulnerable (Lucasik, Goodman, & Longhurst, 2003). This is in part because government is distributed over many locations, and therefore, it is hard to protect all of its information systems well. Second, many government systems must be accessible to a wide range of people (even if through a government intermediary), unlike the specialized systems used in other settings, and users will include a few fools and criminals. Third, governments often use popular business software, and the more popular that software is, the more attacks are known against it. Finally, there are many people with antipathy or grudges against governments for one reason or another, and they may seek revenge by attacking a government's information system and data. With the global Internet, attackers need not be in the same country as the government they attack.

Therefore, it is important to become familiar with the kinds of possible attackers, attacks, and countermeasures that governments could encounter on their computer systems and computer networks (Boswoth & Kabay, 2002; Schwartau, 2001).

BACKGROUND

Government information systems see several kinds of attackers (The Honeynet Project, 2004):

- Disgruntled citizens who might attack computer systems in revenge. No government can please all of its citizens, and since government procedures can be irritating, there are plenty of motives. However, the disgruntled usually confine themselves to giving false data or to doing simple vandalism such as changing government Web pages.
- Disgruntled government employees and government contractors who may attempt to sabotage or to embarrass government systems. Since they are insiders, they can do considerable damage. Thus, it is important not to give any employee too much power.
- Hackers, or amateur attackers who enjoy breaking into computer systems (Chirillo, 2002). Contrary to media coverage, most do little damage.
- Political opponents who might try to attack computer systems, but this will be rare, since most digital governments should be politically neutral.
- Spies who try to obtain secrets (Shulsky & Schmitt, 2002). All governments have secrets on their computers, and there are many kinds of spies. This involves exploration and may entail setting up electronic backdoors for easier access.
- Criminals who can exploit computer systems, for example, to steal money and services or tools to get them credit card numbers (Boni & Kovacich, 1999; Loader & Thomas, 2000). Computer crime is increasing every year.
- Cyber terrorists, or terrorists who attack information systems (Verton, 2003). There has been little evidence of them so far, but they could create considerable damage with minimal effort.
- Military information-warfare specialists who develop ways to attack the information systems of other countries during war (Denning, 1999). They are well trained, not easily discouraged, and use methods that are difficult to detect. Most computers and networks can be subverted quickly by such determined adversaries.

TYPES OF ATTACKS

The field of information security analyzes attacks on information systems and develops countermeasures (Schneier, 2000; McClure, Scambray, & Kurtz, 2001). Some classic attacks include the following:

- Defacement and modification of Web pages to criticize their owners or to make political points, as by Chinese hackers in 2000 to Japanese government sites to protest a meeting about Japanese actions in 1937.
- Overwhelming a system by sending it too much data or making too many requests. This is called a denial-

of-service (DOS) attack, because it impedes legitimate users who are sharing the same resource. The U.S. White House (president) Web site was attacked this way on May 3, 2001.

- Spam or useless e-mail that wastes mail resources, often combined with phishing, or computerized scams to steal passwords and other private information by fooling a user into volunteering it. These are increasing problems on government computer systems (U.S. Government Accounting Office, 2005).
- Guessing passwords and encryption keys for secrets. This is possible when passwords and keys are short or consist of English words. Then an attacker can impersonate someone on the information system and access his or her files. For example, someone got the password of a U.S. Air Force employee in August 2005 and viewed personnel records of 33,000 people.
- Exploiting flaws in software to circumvent access controls. Unlike most products, software rarely comes with a guarantee that it works correctly. There are plenty of bugs in commercial software (including operating systems), some of which can be exploited by attackers. Many of the dangerous ones involve privilege escalation, or finding loopholes to gain system-administrator privileges. For instance, testers hired by the State of Maryland in the United States in 2003 showed that they could break in to the state's voting machines and modify the votes, even remotely, due to flaws in the software.
- Buffer overflows, the most common type of software flaw, which allow privilege escalation by failing to check for too large of input. While good programmers do not make this error, software (including the Windows operating system) written in the programming languages C and C++ must check this explicitly, and some programmers forget this.
- Inserting Trojan horses, or innocent-looking programs that secretly either damage software or benefit the attacker in some way. To insert them, an attacker can: (a) send them attached to an e-mail message that encourages the reader to run it; (b) encourage a user to download them from a Web site; and (c) induce a user to insert a storage device that contains them into his or her computer. The Taiwan government alleged in 2003 that China was distributing Trojan horses specifically designed to break in to their government systems.
- Computer viruses and worms inserted onto computer systems via Trojan horses or by breaking in. These programs reproduce themselves automatically, wasting resources and causing collateral damage. For instance, some U.S. Customs computer systems were shut down by a virus for five hours on August 18, 2005, creating backups for arriving international flights.
- Spyware is a Trojan horse that tracks what users do on a computer and reports this information surreptitiously to a collection site. Current instances mostly just report what Internet sites a user visits, but spyware could be used for more serious spying, too.
- Directly modifying the operating system of a computer by replacing key parts of it with the attacker's programs (from a rootkit). This gives an attacker complete control over a computer system.
- Eavesdropping on traffic on a computer network. A smart attacker might pick up passwords, keys, and other insufficiently concealed secrets, particularly on local-area networks.
- Eavesdropping on computer systems and networks electronically via inadvertent electromagnetic radiation. Older cell phones are easy targets, and much electronic hardware provides radiation that can be picked up with antennas (Smulders, 1990). The U.S. embassy in Moscow long was a target of Soviet electronic eavesdropping.
- Social engineering (Mitnick, 2002), or manipulation of people to trick them into revealing secrets, passwords, and keys that are necessary to break into computer systems. Some classic methods are (a) calling an employee and claiming an emergency that requires their password and (b) doing favors for an employee and then suggesting reciprocation.
- Physical theft of a computer or its storage media. A stolen computer can give up its secrets rather easily.
- Physical damage to a computer or its storage media as a form of vandalism.

COUNTERMEASURES AGAINST CYBER ATTACKS

Defenders of an information system can use a variety of countermeasures, depending on the kind of attack and their resources.

Education

Employees of an organization must be aware of the kinds of attacks that can occur and what they should do about them. This includes learning proper operating procedures, the key attack targets (like passwords), and the classic attack methods. Some studies have shown education to be more effective than any other countermeasure for protecting information systems, since knowledge of information-systems security is not a requirement for most jobs.