2006

Cyber-attacks

Rowe, Neil C.

Monterey, California. Naval Postgraduate School

Anttiroiko, A.-V., & Malkia, M. (Eds.), Encylopedia of Digital Government, Hershey, PA, USA: The Idea Group, 2006.
https://hdl.handle.net/10945/36423

Cyber-attacks

Neil C. Rowe
Cebrowski Institute
U.S. Naval Postgraduate School
Monterey; CA 93940 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 it is therefore hard to protect all of its information systems well. Secondly, 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. Thirdly, governments often use popular business software, and the more popular 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 who may seek revenge by attacking its information systems and data. And with the global Internet, attackers need not be in the same country as the government they attack.

It is therefore 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).

This article is to appear in Anttiroiko, A.-V., & Malkia, M. (Eds.), *Encylopedia of Digital Government*, Hershey, PA, USA: The Idea Group, 2006.

BACKGROUND

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

- Disgruntled citizens could attack computer systems in revenge. No government can please all its citizens and government procedures can be irritating, so there are plenty of motives. However, the disgruntled usually confine themselves to giving false data or doing simple vandalism such as changing government Web pages.
- Disgruntled government employees and government contractors can attempt to sabotage or embarrass government systems. Since they are insiders, they can do considerable damage. It is thus important not to give any employee too much power.
- ?Hackers? are amateur attackers who enjoy breaking into computer systems (Chirillo, 2002). Contrary to media coverage, most do little damage.
- Political opponents could try to attack computer systems, but this will be rare since most digital government should be politically neutral.
- Spies try to obtain secrets (Shulsky, 1990). 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 can exploit computer systems to steal money and services, or tools to get them like credit-card numbers (Boni & Kovacich, 1999; Loader & Thomas, 2000). Computer crime is increasing every year.
- Cyber-terrorists are 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 develop ways to attack the information systems of other countries during war (Denning, 1999). They are well trained, not easily discouraged, and use methods difficult to detect. Most computers and networks can be quickly subverted by such determined adversaries.

TYPES OF ATTACKS

The field of information security analyzes attacks on information systems and develops countermeasures (Schneier, 2000; McClure,

Scambray, and Kurtz, 2001). Some classic attacks are:

- Defacement and modification of Web pages to criticize their owners or 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 email 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 English words. Then an attacker can impersonate someone on the information system and access their 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. So 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", finding loopholes to gain system-administrator privileges. For instance, testers hired by the State of Maryland in the United States in 2003 showed 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 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", innocent-looking programs that secretly either damage your software or benefit the attacker in some way. To insert them, an attacker can:
  - Send them attached to an email message encouraging the reader to run it.
  - Encourage a user to download them from a Web site.
  - Induce a user to insert a storage device into their computer that contains them.

  The Taiwan government alleged in 2003 that China was distributing Trojan horses specifically designed to break into 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 own 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 their 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 was long a target of Soviet electronic eavesdropping.
- "Social engineering" (Mitnick, 2002), or manipulation of people to trick them into revealing secrets, passwords, and keys necessary to break into computer systems. Some classic methods are calling an employee and claiming an emergency that requires their password, and 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.

Legal Responses

Laws prohibit all the attacks we have mentioned, but do not do much to prevent them. In the United States, laws prohibit eavesdropping on communications and damage to computers, which covers most of the attacks we have mentioned, and many other countries have similar laws. But most attackers do not worry about getting caught, since it is hard to track them down and laws are hard to apply. Laws can however be effective against repeat offenders within a given legal jurisdiction, like spies selling secrets.

Patches

It is important to fix flaws or bugs in software as soon as they are discovered, since attacks are typically launched within days of the discovery of major flaws. Manufacturers provide "patches", "security updates", or "service packs" to fix flaws, in the form of modified software that you must go to their Web site to download. The Web site www.cert.org, among others, keeps a current listing of known flaws in important commercial software and their patches. Software that has been sold for a significant period of time generally requires fewer future patches because programmers have had more time to find and fix its flaws, so buying just-released software products is not a good idea.

Backups

Since many attacks destroy data or programs, making copies ("backups") of digital information is essential to recovery from attack. Backups need to be done for any critical information, and need to be stored some distance from the systems they track so no common disaster (e.g., fire, flood, and earthquake) affecting both locations is likely. Optical-disk storage is preferable for backups because it cannot be as easily damaged as magnetic media can be. A backup can be an entire duplicate computer system when it is important to maintain continuous operation.

Access Controls

Automated access controls are important for cyberspace (Pfleeger & Pfleeger, 2002). Access controls for computers are generally managed by passwords that must be supplied to log on and use resources. Controls can be set for individuals or for groups of people, and they can apply separately to reading, writing, or execution of resources, or to the ability to extend those privileges to other users. Access controls for networks are enforced by "firewalls", dedicated computers on a local-area network that restrict traffic to and from the network according to simple rules on such features as origin and communications protocol. Unfortunately, access controls are vulnerable to many attacks mentioned above, and will not generally protect against attacks by insiders like staff.

Encryption

Encryption hides data in some form that cannot easily be read; you then supply a character-string "key" to decode it when you need it (Pfleeger & Pfleeger, 2002). Any attempts to modify encrypted data will result in undecipherability, so you can tell if encrypted messages or programs have been modified (or repeated, if a time is included in the message). Strong and virtually unbreakable methods of encryption have been developed recently with "public-key cryptography", and software for it is available for free download from a number of Web sites. Encryption methods can also be used for "authentication" or to provide digital "signatures" on documents to prove who wrote them and when. Encryption has been touted as a solution to many security problems, but is overrated. If an attacker gains system-administrator privileges, they may be able to get keys or disable encryption methods without your knowledge.

Intrusion Detection and Computer Forensics

Logging records the events on a computer system or network. This can generate enormous amounts of data, so "intrusion-detection systems" (IDSs) (Proctor, 2001) can be set up to check and record just the events that might indicate an attack, alerting system administrators when matters become serious. IDSs can be located on individual computers ("host-based") or on networks ("network-based"). They are important defensive tools against a broad range of known attacks including Trojan horses. Most look for

"signatures" or bit patterns of known attacks, but a few look for "anomalies" or statistically suspicious behavior and thus can detect some new kinds of attacks. IDSs are useful but are not perfect since attackers try hard to disguise their attacks. Other signature checking is provided by standalone virus and worm checkers like Norton AntiVirus that examine files on a computer system.

For new or complex attacks, "computer forensics" is needed (Prosise & Mandia, 2001), methods for inspecting computer storage after an attack to determine how the attack was accomplished and what damage it did. Forensics includes a wide variety of techniques, and requires an intelligent investigator to use considerable judgment. Thus it requires time and can only be done after the attacker is gone.

Honeypots

Honeypots and honeynets (networks of honeypots) provide richer log information about cyber-attacks (The Honeynet Project, 2002; Spitzner, 2003). These are systems with no legitimate purpose other than to receive attackers, so everyone using them other than their system administrator is inherently suspicious. Honeypots need not explicitly invite attackers ? once they are on the Internet, attackers can find them with automated tools. However, they can be dangerous if attackers use them as springboards to attack other sites. For this reason, "reverse firewalls" of various kinds must keep the attack from spreading. But an attacker may infer the existence of the honeypot from the restrictions of the reverse firewall, so a honeypot cannot remain effective forever.

Intrusion Prevention Systems

Most of the methods discussed so far just react to attacks. The alternative is an "active network defense", which in its simpler forms is called an ?intrusion-prevention system?. This includes simple things like turning off the Internet connection or logging out a user when they become sufficiently suspicious as judged by an intrusion-detection system. It can also include forms of limiting damage such as denying the user certain resources, downgrading their priority, or delaying them.

Backtracing

Backtracing is a form of active network defense that tries to find where an external attack is coming from so as to stop it more easily. Unfortunately, most Internet protocols do not make it easy to backtrace, since a key idea of the Internet is to make only local decisions about routing of traffic. Backtracing is also virtually impossible with serious attackers, who take care to come in via a long sequence of sites through many countries and jurisdictions; it is hard to get the cooperation of all those jurisdictions, and the attacker will be long gone by the time anyone succeeds in tracing them. One hope for backtracing is when you suspect who is responsible for attacks; then you could get a court order to monitor the machines they use to collect evidence. Another idea is installing modified networking software in Internet routers that would collect details of messages. Assuming this does not violate your privacy laws, such modified software could be mandated for all government computers. But it is easy for attackers to go through at least a few sites outside the government, thereby terminating backtracing there.

Counterattacking

A more irresponsible form of active network defense is trying to counterattack whatever machine is attacking you. This was available in a product from Symbiot Security in 2004, and has undoubtedly been done elsewhere. Again, this won't work against insiders. Since most serious attacks use intermediate machines to attack yours, such a response will often only hurt a site or computer that is an "innocent bystander". Even if it works and you do hurt the attacker, attacks could easily escalate with resultant collateral damage.

Deception

Deliberate deception has also been proposed for active network defense (Rowe & Rothstein, 2004). Systems could lie, cheat, and mislead attackers to prevent them from achieving their goals. Deception is particularly useful for time-critical military-style attacks such as those by cyber-terrorists or information-warfare experts, when just delaying an attack a while could buy time to find a more permanent defense. Deception has been used in honeypots (Cohen, 1999) to keep the attacker interested. Fake files can be put on a honeypot to make it look more like a normal machine, and fake sites can be programmed to respond like real network nodes. Deception is equally useful against insider and outsider attacks.

FUTURE TRENDS

The lack of powerful general countermeasures means that attacks on computer systems and networks will continue to increase in the future. A shift in attackers from amateurs to professionals will continue as basic countermeasures become more effective at deterring amateurs. Among the countermeasures currently available, education, legal responses, backups, access controls, and honeypots will remain important in the future. But patches, encryption, intrusion detection, computer forensics, honeypots, simple active network defense, backtracing, and deception will increase in importance as technical details of their implementation are worked out. Despite their weaknesses, countermeasures do help protect systems since they have raised the necessary level of sophistication required by an attacker to succeed.

CONCLUSION

Attacks on the software and data of computer systems and networks are increasing. Digital government is more vulnerable to these attacks than other information systems because of its accessibility and the number of motivated attackers. While the threats can be exaggerated (Ranum, 2004), it is essential that government systems anticipate threats and plan to respond to them, since relatively modest attacks could bring government to a halt for hours or days. Some of the countermeasures to protect systems involve purchase of software and hardware, some require institution of policies, and some involve new actions to be taken. No single countermeasure will suffice, but a wide range of countermeasures must be employed in a coordinated information-security strategy.

REFERENCES

Boni, W., & Kovacich, G. (1999). *I-way robbery: crime on the Internet.* Boston: Butterworth-Heinemann.

Boswoth, S., & Kabay, M., eds. (2002). *The computer security handbook*. New York: Wiley.

Chirillo, J. (2002). *Hack attacks revealed*. New York: Wiley.

Cohen, F. (1999). Simulating cyber attacks, defenses, and consequences. Retrieved May 6, 2003 from all.net/journal/ntb/simulate/simulate.html.

Denning, D. (1999). *Information warfare and security.* Boston: Addison-Wesley.

The Honeynet Project (2004). *Know your enemy, second edition*. Boston: Addison-Wesley.

Loader, B., & Thomas, D. (2000). *Cybercrime*. London: Routledge.

Lucasik, S., Goodman, S., & Longhurst, D. (2003). *National strategies for protection of critical infrastructures from cyber-attack.* London: Oxford.

McClure, S., Scambray, J., & Kurtz, G. (2001). *Hacking exposed: network security secrets and solutions, third edition*. New York: McGraw-Hill Osborne Media.

Mitnick, K. (2002). *The art of deception*. New York: Cyber Age Books.

Pfleeger, C., & Pfleeger, S. (2002). *Security in computing, third edition.* Upper Saddle River, NJ: Prentice-Hall PTR.

Proctor, P. E. (2001). *Practical intrusion detection handbook*. Upper Saddle River, NJ: Prentice-Hall PTR.

Prosise, C., & Mandia, K. (2001). *Incident response*. New York: McGraw-Hill Osborne Media.

Ranum, M. (2004). *The myth of homeland security.* Indianapolis: Wiley.

Richardson, R. (2003). *2003 CSI/FBI computer crime and security survey.* Retrieved March 10, 2004 from http://www.gocsi.com.

Rowe, N., & Rothstein, H. (2004, July). Two taxonomies of deception for attacks on information systems. *Journal of Information Warfare, 3* (2), 27-39.

Schneier, B. (2000). *Secrets and lies: digital security in a networked world*. New York: Wiley.

Schwartau, W. (2001). *Cybershock*. New York: Thunder's Mouth.

Shulsky, A. N., & Schmitt, G. (2002). *Silent warfare: understanding the world of intelligence, third edition.* Washington, DC: Potomac Books.

Smulders, P. (1990). The threat of information theft by reception of electromagnetic radiation from RS-232 cables. *Computers and Security, 9* (1), 53-58.

Spitzner, L. (2003). *Honeypots: tracking hackers*. Boston: Addison-Wesley.

U.S. Government Accounting Office (2005, May). *Information security: emerging cybersecurity issues threaten federal information systems*. Publication GAO-05-231.

Verton, D. (2003). *Black ice: the invisible threat of cyber-terrorism*. New York: McGraw-Hill Osborne Media.

DEFINITIONS OF TERMS

cyber-terrorism: Terrorism applied to computer systems and networks, typically those relating to critical infrastructure of a country or organization.
cyberwar: Warfare applied to computer systems and networks.
denial of service: An attack on a computer system in which the system is so overwhelmed by useless processing that it cannot adequately serve legitimate users.
encryption: Converting data to a form in which it cannot be read without supplying a "key" or decoding string.
firewall: A computer that protects a local-area computer network by scanning for suspicious data or activity in its incoming or outgoing traffic.
forensics, computer: Methods for analyzing what has happened after your computer has been broken into or attacked.
hacker: An amateur who breaks into computer systems primarily for the fun of it.
honeypot: A computer system designed to encourage attacks to enable study of attack methods.
information security (?infosec?): Methods for protecting computer systems and networks from attack.
information warfare: Attacks on computer systems, networks, and data as a tactic of warfare.
privilege escalation: Surreptitiously obtaining system-administrator privileges on a computer system.
Trojan horse: A computer program hidden within another, designed to change a computer system in some way to benefit an attacker.
social engineering: Systematic manipulation of people for personal gain, a term particularly used for attacks on computer systems through manipulation of their users.
spyware: A Trojan horse that relays information about user activities on a computer.
virus: A Trojan horse that reproduces itself repeatedly on a computer system, damaging the system.
worm: An autonomous program designed to reproduce itself repeatedly on a computer system and thereby waste resources.