“True” Computer Crime: Computer as the Target (October 2009)

In the broadest sense, computer crime is a violation of law involving a computer. This broad category of crime is often discussed in terms of two subcategories: “true” computer crime and computer-related crime. “True” computer crime refers to those crimes that target the content of computer operating systems, programs, or networks (hereinafter referred to as “computer systems”) and typically involve one or more of the following:

- Accessing computer systems without permission (unauthorized access)
- Damaging computer systems (sabotage)
- Acquiring information stored on computer systems – without permission (theft of data)
- Acquiring services from computer systems – without permission (theft of services)

How It Happens

Unauthorized Access

Perhaps the most widely discussed form of unauthorized access to computer systems is “hacking,” also known as “cracking.” The original definition of hacking, still used by some, refers to access by computer experts for the purpose of exploring systems, programs, or networks; identifying vulnerabilities; developing ways to correct vulnerabilities; and improving systems, programs, or networks. Hacking, in this sense, is neither malicious nor necessarily unauthorized. It is considered a legitimate practice governed by strict rules of ethical conduct and plays a valuable role in computer technology development. By the mid-1980s, the term “hacking” acquired a second definition. It came to mean unauthorized access with malicious intent – to cause damage, steal property (data or services), or simply leave behind some evidence of a successful break-in. In addition, software programs and websites devoted to sharing hacking information have made it easier for anyone to be a hacker. The term cracking was coined by the hacker community (of the original definition) to distinguish acts of malicious hackers (i.e., “crackers” or “black hats”) from benevolent hackers (i.e., “white hats”). Despite this effort, the term hacking today is usually used to describe a malicious or criminal act.

Other forms of unauthorized access include access to computer systems that exceed authorization. For example, an employee who has been granted limited access to company computer systems, may

- access information to which the employee has not been granted access or
- use, destroy, distribute, or manipulate information in a way that exceeds the employee’s authorization.

Sabotage

Common forms of sabotage include distribution of a “malicious program” (e.g., a virus, worm, logic bomb, or Trojan horse); denial of service; or a combination of these forms. Perhaps the most widely recognized of
these is the virus, which first emerged in the late 1980s. A virus is simply a computer program designed to "infect" a program file or boot sector of a computer. Like a biological virus, a computer virus infects (or copies code to) a "host" and uses the capabilities of its host to replicate. When an infected program is executed, the embedded virus program is also executed, and the instructions in the virus program override the instructions in the infected program. Once executed, a virus can cause damage by erasing or altering data or files, or by simply replicating until no disk space remains. A virus may also produce a message or graphic, with or without causing damage to the infected computer. Typically a virus moves from computer to computer attached to a file – on a disk or in an e-mail, for example.

A worm is a computer program designed to copy itself. Unlike a virus, a worm is self-executing; that is, it does not require a host to replicate. Instead, it exploits weaknesses in a computer operating system, which are largely invisible to the computer user, and replicates through computer networks. A worm, then, is able to enter a computer without any active participation by its user (such as opening an e-mail attachment) and execute without modifying existing files. A worm typically causes damage by slowing Internet traffic; it may also execute mass attacks, such as denial of service (DoS) attacks on specific network addresses.

A logic bomb (also called "slag code") is a program designed to execute (or "explode") under certain conditions specified in the coding, for example, on a certain date, after a lapse of time, or following some response (or lack of response) by the computer user. It is essentially a delayed-action virus or worm. Upon execution, a logic bomb may produce a benign message, delete data, corrupt data, or cause some other undesirable effect.

A Trojan horse is a program that appears to be useful or benign but actually conceals a smaller program that is designed to be damaging, annoying, or "humorous." For example, a Trojan horse may be delivered as an e-mail attachment and described as a computer game. When an unsuspecting user installs the game, programming within the game may contain instructions for deleting data, e-mailing information to the creator of the Trojan horse, or installing a “back door” through which crackers can enter the computer system, access information, or cause damage.

A denial of service (DoS) attack is an explicit effort to prevent legitimate users from accessing computer systems. The most common form of DoS attack is a “buffer overflow attack,” which involves the delivery of traffic to a target network address that is greater in volume than its data buffers are able to handle. Other types of denial of service include a “teardrop attack,” “SYN flood attack,” and “smurf attack.”

In a “teardrop attack,” the attacker exploits the Internet Protocol (IP) requirement for a large packet to be divided into fragments, with the first fragment containing “offset values” that guide the reassembly of packet fragments. By including alternative offset values in later fragments, the attacker attempts to “confuse” the receiving operating system and cause it to crash. In a “SYN flood attack,” the attacker sends multiple session-establishing packets (i.e., requests to a server for connection to that server) and then fails to respond to the server’s reply. While the attacker’s packet remains in the server’s buffer awaiting a reply, legitimate requests are postponed. Although the server eventually drops the attacker’s packet from the buffer, a large number of attacker requests can cause significant delays in servicing legitimate requests. In a “smurf attack,” the attacker sends to a target site an IP ping request (i.e., a request to “echo my message back to me.”) The request includes the target site’s address and the return address, as well as instructions to broadcast the ping request to multiple sites. The intent of the attack is to cause the target site to receive a flood of pings from multiple sites which have received a ping request from the “spoofed” address of the target site, and to diminish the target site’s ability to receive legitimate Internet traffic.

**Theft of Data and Services**

**Theft of data** includes theft of sensitive information, proprietary information, or other intellectual property that is stored on personal, government, or corporate computer systems.
Sensitive information typically targeted in computer crime includes passwords, credit card numbers, account numbers, and social security numbers. This information may be obtained from an individual’s computer or from a computer system of an organization, such as a credit bureau or bank. Other sensitive information includes individual medical records and credit records, military secrets, intelligence information, and other classified information. This type of information is typically obtained from computer systems of government agencies, financial institutions, and other organizations.

"Intellectual property refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. Intellectual property is divided into two categories: Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indications of source; and Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs." 9

Intellectual property theft is executed in a variety of ways, such as

- "softlifting" – "purchasing a single licensed copy of software and loading it onto several computers contrary to the license terms"; 10
- online piracy – uploading or downloading "unauthorized copies of copyrighted software" available to users connected to an online service provider or the Internet; and
- software counterfeiting – "illegally duplicating and selling copyrighted software," often "in a form designed to make it appear legitimate." 11

Theft of services is the use of services with the intent to avoid payment for those services, including use of computer time, data processing, or storage functions provided by online service providers.

Computer Crime Prevention

Computer crime relies significantly on vulnerabilities and opportunities. Although no organization or individual can eliminate vulnerabilities and opportunities, the following precautions can help to reduce the likelihood of victimization:

- Install an anti-virus program, update it regularly, and set it to check all appropriate areas, such as e-mails, Web pages, and disk drives. Anti-virus programs can help protect not only against malicious programs that cause damage but also against programs designed to steal information such as passwords and account numbers.
- Use "strong" passwords that include a combination of numbers and upper- and lower-case alphabetic characters; change passwords frequently; and do not use the same password for multiple applications. Strong passwords can help protect against unauthorized access, including access attempted with programs designed to crack or "sniff" (i.e., detect) passwords.
- Shred any documents that contain personal information, including junk mail, bank statements, and bills. "Dumpster diving" – looking through the trash of individuals and organizations – is used to illegally collect account numbers, social security numbers, passwords, and other personal information.
- Provide personal information over the Internet only through verified and secured Web sites and not in response to unsolicited requests. Spam e-mails that provide links for personal information entry or confirmation under the guise of a legitimate company name are commonly used in illegal attempts to collect social security and account numbers. Once collected, these numbers may be sold online or used as currency to “purchase” software and other digital goods.
Be cautious about providing personal information over the telephone or Internet to unknown individuals. Impersonation of a trusted person, such as a representative of a credit card company or bank, is a common method of obtaining personal information.

**Costs and Statistics**

While there is no exact count on the number of viruses and worms, “more than 100,000 threats exist today.” In June 2005 alone, the anti-virus software company Sophos identified 1,434 new viruses.

Economic loss from sabotage and theft continues to be a significant concern for both private and governmental organizations. Organizations responding to the 2005 CSI/FBI Computer Crime and Security Survey, for instance, reported annual losses (for calendar year 2004) of $42 million from viruses, $32 million from unauthorized access, and $31 million from theft of proprietary information. Respondents to the 2005 E-Crime Watch Survey cited viruses or other malicious code as the most prevalent type of electronic crime or action (eighty-two percent) followed by spyware (sixty-one percent) and phishing (fifty-seven percent). The Anti-Phishing Working Group received 232,779 unique phishing reports from July 2005 to July 2006.

Costs to individuals include losses resulting from identity theft; theft of sensitive information; lost access to personal computers, service providers, and networks; and damage to personal computers, data, and programs. No reliable estimate of the level of these losses is available.

**Examples/Case Studies**

- One of the earliest cases of true computer crime occurred in 1988. Robert Morris Jr., a 23-year-old computer science student wrote a self-replicating, self-propagating program (a worm) that infected an estimated 6,000 computer systems and caused as much as $10 million in losses. Morris was convicted of violating the Computer Fraud and Abuse Act, sentenced to 3 years probation plus community service, and fined $10,000.

- In 1999, David Smith released the “Melissa” virus over the Internet, infecting 1.2 million computers in the U.S. and one-fifth of the country’s largest businesses. Worldwide, the Melissa virus caused an estimated $80 million in damages. Smith was sentenced to 20 months in prison and fined $7,500.

- On July 19, 2001, the “Code Red” worm was detected spreading rapidly over the Internet. Within hours, the worm penetrated several hundred thousand computers and generated 100 copies (or threads) on each affected computer. Millions of Code Red worm threads were programmed to initiate a buffer overflow (or DoS) attack on the White House Web site (IP address: 198.137.240.91). Beginning at 8 PM EST on the 20th of the month and continuing every 4-1/2 hours for seven days, each thread was to simultaneously send 98,304 packets of information to the target address. The attack was avoided when the IP address of the White House homepage was changed before the trigger time. The Code Red worm caused an estimated $2.6 billion in damages, including clean-up costs.

- In January 2004, the “MyDoom” worm became the fastest spreading virus to date. MyDoom is “estimated to have caused $38.5 billion of economic damage worldwide so far in terms of overtime payments, contingency outsourcing, loss of business, bandwidth clogging, productivity erosion, management time reallocation, cost of recovery, and software upgrades.”

- On July 11, 2005, Sven Jaschan, creator of the Sasser worm and Netsky virus, was sentenced by a German court to 21 months probation and 30 hours of community service. Jaschan had admitted to
data manipulation, computer sabotage and interfering with public services.”

“The Sasser internet worm, created by Jaschan, attacked millions of PCs around the world, while versions of his Netsky email virus continue to spread - accounting for over 25% of all virus reports in the first six months of 2005.”

The Response/ Current Efforts

In the past few years, a number of projects have been initiated to facilitate coordination and cooperation among government agencies, corporations, and universities and improve efforts toward reducing computer crime. Among these are the National Software Reference Library (NSRL), the Electronic Crime Partnership Initiative (ECPI), and the CyberScience Laboratory (CSL). In addition, legislation, such as the Piracy Deterrence and Education Act of 2003, has been proposed in Congress to further enhance criminal laws and public education efforts.

Legislation

- Numerous federal and state statutes address computer crime. Some of the more significant legislation includes the following:

  - The **Electronic Communications Privacy Act** of 1986 – In response to concerns about electronic eavesdropping by government, this Act extended to e-mail stored on computer systems protections against unauthorized police interceptions that had previously been applied only to telephone conversations. (18 U.S.C. § 2510-2522, 2701-2711)

  - The **Computer Fraud and Abuse Act** of 1986 – This Act made certain activities designed to access a “federal interest computer” illegal. It has since been amended and broadened to protect essentially any computer with Internet access. (18 U.S.C. § 1030)

  - The **No Electronic Theft (NET) Act** – This Act provided greater copyright protection by amending criminal copyright infringement provisions. It permitted, for example, “federal prosecution of large-scale, willful copyright infringement even where the infringer does not act for a commercial purpose or for private financial gain, thus closing a loophole in criminal enforcement of copyright infringement.” (Pub. L. 105-147)

  - **USA PATRIOT Act** – This Act amended existing laws concerning computer crime and electronic evidence. It also redefined “terrorism” to include crimes such as computer hacking and identified “cyberterrorism” as a crime carrying a penalty of up to 20 years in prison. (Pub. L. 107-56)

“For More Information” Links

- **Symantec Corporation**, producer of Norton anti-virus software – http://www.symantec.com

- **Network Associates**, producer of McAfee anti-virus software – http://www.networkassociates.com

- **Computer Security Institute** – http://www.gocsi.com

Endnotes


For a comprehensive list of computer crime activities (from 1960 to 2003), see *The complete history of hacking*. Available at http://delontin1.wordpress.com/2008/02/27/complete-history-of-hacking/


