Glossary of Computer Crime Terms

By M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA
CTO, School of Graduate Studies
Norwich University, Northfield, VT 05663-1035 USA

Revised April 2008

In coming weeks, we'll be looking at the history and current status of different kinds of computer crime techniques. The following glossary will be useful for you as you expand your knowledge of this field. In addition, you have received the *Computer Desktop Encyclopedia* CD-ROM which has recently been updated with hundreds of security terms.

- **Back door***:* secret (undocumented), hard-coded access codes or procedures for accessing information. Some back doors exist in commercially-provided software packages; e.g., consistent (canonical) passwords for third-party software accounts. Alternatively, back doors can be inserted into an existing program or system to provide unauthorized access later. A program with an undocumented access method is an example of a Trojan Horse.

- ***Bot****:* for “robot” – a program used for a specific function such as keeping a port open or launching a flood of packets in a distributed denial-of-service attack.

- ***Botnet****:* a set of bots installed (usually surreptitiously) on a number of victimized computers (zombies or slaves) to launch distributed denial-of-service attacks or to send spam.

- ***Cracking****:* malicious or criminal hacking. Unauthorized penetration of computer systems and networks, abuse of privilege, unauthorized use of services.

- ***Data diddling****:* modifying data for fun and profit; e.g., modifying grades, changing credit ratings, altering security clearance information, fixing salaries, or circumventing book-keeping and audit regulations.

- ***Data leakage****:* uncontrolled, unauthorized transmission of classified information from a data centre or computer system to the outside. Such leakage can be accomplished by physical removal of data storage devices (diskettes, tapes, listings, printouts and photographs of screen copies or handwritten notes) or by more subtle means such as data hiding (steganography) or even plain old human memory.

- ***Denial-of-service (DoS) attack****:* overwhelming or saturating resources on a target system to cause a reduction of availability to legitimate users. On the Internet, usually involves spoofing packets or e-mail headers.

- ***Distributed DoS (DDoS) attack****:* Internet-mediated attack accomplished by enlisting the services of many compromised systems to launch a denial of service (DoS).

- ***DNS cache poisoning****:* modifying data in a Domain Name System (DNS) server so that calls to particular Websites or even entire domains are misdirected for fraudulent purposes.

- ***Easter egg:*** undocumented, unauthorized program functions in a production program; a kind of Trojan Horse.

- ***Exploit****:* a method for exploiting a vulnerability to take control of a system or otherwise compromise it. Exploits are sometimes automated in scripts.

- ***Hacking****:* for many years, a noble endeavor involving intense study, dedicated analysis and hands-on learning about any technical field, including computing. Unfortunately, despite the best efforts of computer hobbyists worldwide, since the early 1980s, thanks largely to the ignorance of undereducated journalists, the term has become almost synonymous with cracking. Some die-hards continue the battle by referring to “criminal hacking” but it’s probably too late to reverse the shift in meaning.

- ***Hacktivism (sometimes spelled hactivism):*** politically- or ideologically-motivated vandalism. Defacing a Web site for no particular reason is vandalism; the same defacement to post political propaganda or to cause harm to an ideological opponent is hacktivism.

- ***Identity theft****:* creating a false identity using someone else’s identifying information (e.g., name, Social Security Number, birthday) to create new credit cards or establish loans which then go into default and affect the original victim’s credit record.

- ***Impersonation****:* pretending to be authorized to enter a secure location. Examples include swaggering into a site equipped with what look like tool kits of the manufacturer of computer equipment, or pretending to be a janitor. Impersonation is a key element of social engineering.

- ***Latency****:* the period during which a time bomb, logic bomb, virus or worm refrains from overt activity or damage (delivery of the payload). Long latency coupled with vigorous reproduction can result in severe consequences for infected or otherwise compromised systems.

- ***Logic bomb****:* A program in which damage (the payload) is delivered when a particular logical condition occurs; e.g., not having the author's name in the payroll file. Logic bombs are a kind of Trojan Horse; time bombs are a type of logic bomb. Most viruses are logic bombs.

- ***Mail-bombing****:* sending large numbers of unwanted e-mail messages to a single recipient or to a group of such recipients. To be distinguished from spamming. Mail-bombing is a form of denial of service.

- ***Malware****:* malicious software, including Trojan Horses, viruses, worms, logic bombs, exploits and time bombs.

- ***Master program****:* in distributed denial-of-service (DDoS) attacks, a program that communicates with implanted zombie or slave programs on compromised systems. The master program usually transmits encrypted instructions to zombies with details of which targeted system to swamp with junk transmissions at exactly what time.

- ***Payload****:* the unauthorized activities of malicious software.

- ***Penetration****:* unauthorized access to restricted systems or resources.

- ***Piggybacking****:* entering secure premises by following an authorized person through the security grid; also unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification).

- ***Pharming****:* misdirecting traffic from one Website to a Website controlled by a criminal hacker by altering the domain name system (e.g., by DNS cache poisoning) or by altering configuration files on a victim's computer.

- ***Phishing****:* using a forged or spoofed e-mail or Web site that imitates or duplicates an official communication or page to trick victims into revealing logon or other confidential information that can be used for penetration, financial fraud or identity theft.

- ***Root kit:*** a script or set of scripts for gaining unauthorized *root* privileges (or equivalent supervisory powers) on a compromised system. Much used by *script kiddies.*

- ***Sabotage****:* the word comes from the French for wooden shoe (*sabot*). Such footwear made a handy weapon for throwing into the gears of new mechanical systems that were causing unemployment during the industrial revolution of the 18th and 19th centuries. The term now means any deliberate damage to operations or equipment.

- ***Salami theft****:* technique of accumulating round-off errors or other small quantities in calculations and saving them up for later withdrawal; usually applied to money, although it can be part of an inventory-theft scheme (for example).

- ***Scavenging****:* using discarded listings, tapes, or other information storage media to determine useful information such as access codes, passwords, or sensitive data. Finding a listing for the source code for a new version of a popular proprietary program could be highly profitable for a computer crook. Also known as D*umpster® diving.*

- ***Scripts****:* any simple program, especially using a *scripting* or *macro* language; in computer crime work, however, scripts usually refer to automated systems for executing *exploits*.

- ***Simulation****:* using computers to simulate a complex system in order to defraud it; e.g., inventing transactions to produce a pre-arranged bottom line in a financial report.

- ***Spamming****:* a popular name for e-mail sent to many unwilling recipients in order to sell products or services (or sometimes to cheat naïve customers). Those wishing to avoid offending the innocent Hormel Corporation, owners of the Spam® trademark, may refer to this indiscriminate bulk e-mail as junk e-mail or as UCE (unsolicited commercial e-mail).

- ***Spim***: spam over instant messenger

- ***Spit***: spam over internet telephony

- ***Spoofing****:* using incorrect identification; usually applied to electronic misrepresentation such as putting the wrong originating address on a TCP/IP packet. Much used in denial-of-service (DoS) and distributed DoS (DDoS) attacks.

- ***Superzapping****:* using powerful utility software (originally the superzap utility on IBM mainframes) to access secure information while bypassing normal controls. Debug programs, and disk editors are examples of tools used for superzapping.

- ***Time bomb****:* program or batch file waits for a specific time before causing damage. Often used by disgruntled and dishonest employees who find out they're to be fired or by dishonest consultants who put unauthorized time-outs into their programs without notifying their clients. Logic bombs and time bombs are Trojan Horse programs; time bombs are a type of logic bomb.

- ***Trojan horse****:* innocent-looking program that has undocumented and nefarious functions. So called by reference to Odysseus' wooden horse filled with soldiers that helped to capture Troy. Trojan Horse programs can, for example, alter data in a particular way, record passwords for later inspection, send confidential information to unauthorized destinations or open *back doors* into compromised systems.

- ***Vandalism****:* obvious, unauthorized, malicious modification or destruction of data such as information on Web sites.

- ***Virus****:* Viruses infect executable code such as programs (e.g., .EXE and .COM files under DOS), boot sectors on disks and macro programs. The viral code reproduces with the *host* code is loaded into memory. So called by analogy with biological viruses, which subvert the functions of normal cells. Viruses are similar to worms but reside inside programs at all times. A virus can transform an ordinary program into an unintended Trojan horse.

- ***Vulnerability***: a weakness or flaw permitting an attack on a computer system or network.

- ***Wiretapping****:* eavesdropping on data or voice transmissions by attaching unauthorized equipment or software to the communications medium (in the case of wires, coaxial metal cables and optical cables) or by intercepting and interpreting broadcast data (in the case of wireless phones, cellular phones, and wireless networks).

- ***Worm****:* program which spreads through a computer system or network by replicating (like a virus) but without integrating itself into other executable code.

- ***Zombie****:* a program inserted into a vulnerable system to await further instructions; usually part of a distributed denial-of-service (DDoS) attack.

Online Glossaries

- Committee on National Security Systems (CNSS) publication number 4009, the "National Information Assurance (IA) Glossary", revised June 2006 < http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf >

- Internet Request for Comments 2828 (RFC2828) *Internet Security Glossary* by R. Shirey was last updated in May 2000 and provides definitions and commentary on 284 important terms and acronyms in our field. The entire document is available at < http://www.faqs.org/rfcs/rfc2828.html > and also has a search facility that covers more than 3100 RFCs.

- The downloadable "Draft Comprehensive Information Assurance Dictionary" < http://www.niatec.org/niatecglossary.htm > was compiled by Dr Corey Schou, Dr James Frost and their colleagues Nathan Wingert, Jason Larsen, Herbert Lafond and Edward Munson from the National Information Assurance Training and Education Center at Idaho State University < http://security.isu.edu/ >. This massive work in progress has reached 417 pages in length and is still open to comments and suggestions from readers. This is a resource that everyone can use, especially with the helpful bookmarks that allow immediate access to specific terms. The 3.9 MB PDF file may be downloaded from < http://security.isu.edu/pdf/NIATECV30d.pdf > and can then be referred to quickly from your own hard disk as long as you have Acrobat or the free Acrobat Reader.