This is the second part of a glossary of basic terms used when discussing computer crime.

* * *

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.

SALAMIS: 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 could be part of an inventory-theft scheme.

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 Dumpster® diving.

SCRIPTS: an inoffensive term for 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, refer to this indiscriminate bulk e-mail as junk e-mail or as UCE (unsolicited commercial e-mail).

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.

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.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.