A glossary of security and cyberwarfare terms

It's hard enough for IT leaders to track all the new viruses, worms, and security alerts threatening the enterprise these days, and few have time to keep up on the latest security and cyberterrorism acronyms and terms that describe all the new threats.

TechRepublic wants to keep you in the know by providing this glossary of security and cyberwarfare terms created and continuously updated by United Messaging, a leading enterprise messaging outsourcing provider. United Messaging established this up-to-the-minute lexicon of terms and definitions gleaned from today's security and cyberterrorist subculture. "Potential cyberterrorism is a growing topic of concern for corporate America, and yet it remains very much a mystery to many executives and decision makers," said Ben Trowbridge, CEO of United Messaging.

"It is imperative that we close this education gap, and we believe this glossary is a first step in creating new levels of understanding."

United Messaging, headquartered in West Chester, PA, provides secure enterprise messaging solutions via hosted messaging and professional services, handling over 1,000,000 e-mails each business day. The company serves enterprises with collaborative, business-critical Microsoft Exchange, Lotus Domino, and iPlanet-based messaging applications. United Messaging invites TechRepublic members to visit its Web site (http://www.unitedmessaging.com/) for updates on glossary terms, which the company plans to post on a regular basis.

A

Alderson Loop: A special kind of infinite loop that traps the user by using a false exit condition; i.e., "Click OK" when the "OK" function has been disabled.

AIS (Automated Information System): Any equipment of an interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.

Ankle Biter: A person who aspires to be a hacker/cracker but has very limited knowledge or skills related to AISs. Usually associated with young teens who collect and use simple, malicious programs obtained from the Internet.

Anomaly Detection Model: A model where intrusions are detected by looking for activity that is different from a user's or a system's normal behavior.

ASIM (Automated Security Incident Measurement): Monitors network traffic and collects information on targeted unit networks by detecting unauthorized network activity.

Attacker Traps: Systems used to lure hackers or other information warriors into an attack so that they can be traced.

B

Backdoor (Trapdoor): An intentional breach in the security of a computer system left in place by designers or maintainers. A hidden software or hardware mechanism used to circumvent security controls. A breach created intentionally for the purpose of collecting, altering, or destroying data.

Bastion Host: A system that has been hardened to resist attack at some critical point of entry and that is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls or may be "outside" Web servers or public access systems. Generally, a bastion host is running some form of general-purpose operating system (e.g., LNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system.

BLOB (Binary Large Object): Can be stored in a database but normally not interpretable by a database program. Occasionally used as a mild hacker threat when mailed. Can also be used to hide malicious logic code.

Blue Bomb (a.k.a. Blue Screen of Death or WinNuke): Technique for causing the Windows operating system of someone you're communicating with to crash or suddenly terminate. The blue bomb contains information that the operating system can't process. This condition causes the operating system to "crash" or terminate prematurely. Its name comes from the effect it sometimes causes on the display, as the operating system is terminating a white-on-blue error screen.

Bomb: A generic description for the crashing of software or hardware systems.

Breach: 1) The successful defeat of security that could result in system penetration. 2) Violation of a system's controls that exposes information assets or system components.

"Brute Force" Password Cracker: Guessing the password until you figure it out, whether via manual methods or by using a program that continually guesses passwords. Programs will try passwords like "aa," "ab," "ac," and so on until every legal character combination has been tried.

C

C2 (Command and Control): The arrangement and deployment of personnel, equipment, communications, facilities, and procedures employed in accomplishing a mission.

C2W (Command and Control Warfare): In addition to the traditional physical destruction aspect of war, this includes the integrated use of operations security, military deception, psychological operations, and electronic warfare to degrade or destroy the adversary's command and control capabilities and to protect one's own. It is a subset of information warfare.

C4I: Command, Control, Communications, Computers, and Intelligence.

Carnivore: A controversial FBI system to monitor e-mail and other traffic through Internet service providers.

CERT (Computer Emergency Response Team): The Defense Advanced Research Projects Agency (DARPA) used this term to describe the first computer emergency response team, founded in December 1988 at Carnegie Mellon University's Software Engineering Institute in Pittsburgh. The official term is now CERT/CC, which stands for CERT Coordination Center (http://www.cert.org/).

Chernobyl Packet: An information packet that introduces a broadcast storm and network meltdown.

CIAC (Computer Incident Advisory Capability): Plans for establishing this team were prepared before November 1988. It was founded as a second-incident response team in the spring of 1989. Its constituencies are sites within the DOE.

CIAO (Critical Infrastructure Assurance Office): Created in May 1998 to assist in the coordination of the U.S. Federal Government's initiatives on critical infrastructure protection (http://www.ciao.gov/).

Communications Security (COMSEC): Measures taken to deny unauthorized persons information derived from the telecommunications of an entity involved in national or organizational security and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of communications security material and information.

Copernicus: The codename under which the Navy reformulated its command and control structures in the age of Information Warfare. Copernicus enables those in the field to get the information they need to make tactical decisions.

Core Leak: A programming error that causes the program to fail to reclaim discarded memory, leading to eventual collapse due to memory exhaustion. Not as critical a problem as it was before the advent of virtual memory.

Cracker: Like a hacker, a cracker is someone who breaks into secure systems. A cracker's primary aim is to break into secure systems, while hackers want to gain knowledge about computer systems and use this knowledge for pranks or to cause damage. The terms "hack" and "crack" are often used interchangeably.

CSRC (Computer Security Response Center): Another acronym for CERTs.

Cyberwar: Actions taken to achieve information superiority over an adversary—to deny, exploit, corrupt, or destroy an enemy's information while protecting your own. See Information Warfare.

Cyberian Winter: The theoretical aftermath of an all-out cyberwar, characterized by "cold" disabled computer systems and businesses.

D

Daemon: Pronounced "demon" or "damon," daemon is a process that runs in the background and performs a specified operation at predefined times or in response to certain events. Sometimes referred to as *System Agents* and *services*. Typical daemon processes include print spoolers, e-mail handlers, and other programs that perform administrative tasks for the operating system. The term comes from Greek mythology, where daemons were guardian spirits.

Dark-Side Hacker: A malicious hacker.

Data-Driven Attack: An attack form that is encoded in data that appears harmless and is executed by a user or a process, often behind a firewall.

DBA (Dominant battlefield awareness): Applies to own system advantage in terms of sensor, reconnaissance, and intelligence data in a particular "battle space."

DBK (Dominant battlefield knowledge): The ability to recognize and understand what the user sees and to act on it decisively.

Decrypt: To unscramble data that has been encrypted. Decryption is the act of unscrambling data so that it can be understood.

Derf: The act of exploiting a terminal unwittingly left logged on.

Digital Signature: A digital guarantee that a file has not been altered, as if it were carried in an "electronically sealed" envelope. The "signature" is an encrypted digest (one-way hash function) of the text message, executable, or other file.

DOS (Denial of Service) Attack: Action against a host resulting in the target's inability to perform service(s) for other users, particularly over a network.

Dumpster diving: Spying the old-fashioned way: rummaging through garbage or recycling cans for information such as invoices, passwords, and account numbers.

E

Easter Egg: An undocumented function hidden in a program that may or may not be sanctioned by management. Easter Eggs are secret "goodies" found by word-of-mouth or by accident. See also Trapdoor.

ECHELON: A multinational surveillance network centered in Sugar Grove, WV. It has been called the greatest spy network in history. ECHELON intercepts all forms of electronic communications—phone, fax, and e-mail—and automatically searches for predetermined keywords. Member countries are the United States, Britain, Australia, and New Zealand.

E-mail Bombs: Code that when executed sends many messages to the same address(es) for the purpose of using up disk space and/or overloading the e-mail or Web server.

EMP/T Bomb: Electromagnetic pulse transformer, which disables or destroys an electronic network. Similar to a HERF Gun but many times more powerful.

Encryption: Altering data to make it unreadable unless you know how to decrypt it.

Encryption Cracking: Breaking the encryption that is used to protect the contents of e-mail, fax, and voice transmissions, as well as software or other content.

Ethernet Sniffing: Listening with software to the Ethernet interface for packets that interest the user. When the software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like "login" or "password."

F

Firewall: A form of Web security that stands between a private network and the Internet to prevent unwanted traffic from passing either way. Some firewalls have proxy functions built in. Often the distinction between a firewall and a proxy is blurry. True firewalls generally support packet-filtering, proprietary application filtering, and some proxy functions.

Fishbowl: To contain, isolate, and monitor an unauthorized user to gain information about that user.

Flooding programs: Code that when executed will bombard the selected system with requests in an effort to slow down or shut down the system.

Fork Bomb: A disruptive piece of code directed toward a UNIX-based system which replicates, or “forks,” until it eventually “explodes” and devours operating system processes, causing the system to lock up.

H

Hacker: A person who breaks into systems for which he or she has no authorization. Hackers penetrate information systems to browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way.

Hacking Run: An extended hack session that goes beyond normal working times, especially if more than 12 hours long.

HERF (High Energy Radio Frequency) Gun: HERF guns shoot a high-power radio signal at an electronic target and knock it out of commission.

Honeypot: A decoy server set up either inside or outside a firewall to lure and trick an intruder. It is designed to make hackers/crackers think they are on a valid production system. It is used to catch and stop an intruder or detect and track intruder techniques and test system vulnerability.

I

IW (Information Warfare): Actions taken to achieve information superiority over an adversary: to deny, exploit, corrupt, or destroy an enemy’s information while protecting your own. Also known as "third-wave war" or "knowledge war"; see Cyberwar.

INFOSEC: Military abbreviation for Information Security. The protection of classified information that is stored on computers or transmitted by radio, telephone teletype, or any other means.

IP Sniffing: Stealing network addresses by reading the packets. Harmful data is then sent stamped with internal trusted addresses.

IP Spoofing: An attack whereby an active, established session is intercepted and co-opted by the attacker.

K

Key: A symbol or sequence of symbols (or the electrical or mechanical equivalent) applied to text to encrypt or decrypt.

Kluge: A programming trick designed to solve a problem quickly.

Keystroke Monitoring: A device or software that records every key struck by a user and every character of the response that the user gets.

L

Leapfrog Attack: An attack in which the hacker gains access to a site or server from a third-party site. Use of user ID and password information obtained illicitly from one host to compromise another host. The act of telnetting through one or more hosts in order to preclude a trace (a standard cracker procedure).

Letter Bomb: E-mail containing live data intended to perform malicious acts on a machine or terminal.

Logic Bomb: A piece of unauthorized computer code, usually delivered via e-mail. It attacks a system after verifying certain conditions within that system.

M

Mail Bomb: Sent to urge others to send massive amounts of e-mail to a single system with a goal of crashing the recipient's system.

MIPS (Million Instructions Per Second): A measure of computing speed.

Mockingbird: A computer program that mimics the legitimate behavior of a normal system feature but launches into a malicious activity once activated by the user.

N

NIPC (National Infrastructure Protection Center): Established in February 1998, the NIPC is considered the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against critical national infrastructures.

Nano Machines: Tiny robots that attack the hardware of a computer system, as opposed to the software. After being unleashed at a facility, these robots (smaller than insects) can literally crawl through an office until they find a computer, then drop through slots in the computer and shut down the electronic circuits.

Network Worm: A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability, or availability. A network worm may attack from one system to another by establishing a network connection. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.

O

One-Time Password: In network security, a password issued only once as a result of a challenge:response authentication process. Cannot be "stolen" or reused for unauthorized access.

One-Way Hash Function: In cryptography, an algorithm that generates a fixed string of numbers from a text message. The "one-way" means that it is extremely difficult to turn the fixed string back into the text message. One-way hash functions are used for creating digital signatures for message authentication.

OODA (Observation, Orientation, Decision, Action) Loop: Refers to the computerized cycle from data acquisition to information integration through to initiation of a response. Taking out the OODA loop is frequently mentioned as the goal of Information Warfare.

P

Packet Sniffing: A technique in which a software program is planted at remote junctions in a computer network. The program monitors information packets as they are sent through networks and reveals usernames and passwords to the hacker, who is then able to break into the system.

Phreaking: Hacking directed at the telephone system (as opposed to the data communications networks) or hacking with a telephone. Using different "boxes" and "tricks" to manipulate the phone companies and their phones, phreakers can gain many things, two of which are knowledge about telephones and how they work, and free local and long-distance phone calls.

Ping of Death: The Ping of Death is a denial-of-service attack that crashes servers by sending invalid IP ping packets.

Port Scanning: The act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious if someone is looking for a weakened access point.

Prowler: A daemon that is run periodically to seek out and erase core files, truncate admin log files, “nuke” lost-and-found directories, and otherwise clean up the system.

Proxy: Using one computer or device to make requests or “stand in” in place of another. Proxies are often used for Internet security. You can use a proxy to pass data between an internal network and the Internet. The server on the Internet never knows that the request is coming from anywhere but the proxy. Some proxies have caching and site filtering built in.

Q

Quadrant: A short name referring to technology that provides tamper-resistant protection to cryptography equipment.

R

Replicator: Any program, such as a worm, a fork bomb, or virus, that acts to produce copies of itself. It is even claimed by some that UNIX and C are the symbiotic halves of an extremely successful replicator.

RMA (Revolution in Military Affairs): The military’s realization that information and information technologies must be considered as a weapon in plotting any military strategy.

Rainbow Series: A library of technical manuals on evaluating “trusted computer systems” issued by the National Security Agency between 1987 and 1995. So named because each book ‘s cover is a different color.

Retro-virus: A virus that waits until all possible backup media are infected before activating, thereby making it impossible to restore the system to its uninfected state.

Rootkit: A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan horse software.

S

Samurai: A hacker who hires out for legal cracking jobs like snooping for factions in corporate political fights or doing work for lawyers pursuing privacy rights and First Amendment cases, and hacking for other parties with legitimate reasons to need an electronic locksmith.

Script Kiddie: A low-level amateurish hacker. They are generally regarded as mischief makers as opposed to real threats.

Secure Sockets Layer (SSL): A protocol from Netscape that allows for "secure" passage of data. It uses public key encryption, including digital certificates and digital signatures, to pass data between a browser and a server. It is an open standard and is supported by Netscape's Navigator and Microsoft's Internet Explorer.

Self-Garbling Viruses: Viruses that attempt to hide from virus scanning programs by keeping most of their code garbled in some way. They change the garbling each time they spread. When such a virus runs, a small header degarbles the body of the virus and then branches to it.

SET (Secure Electronic Transaction): A new standard that enables secure credit card transactions on the Internet. The SET standard has been endorsed by virtually all the major players in the electronic-commerce arena.

Smurf: A type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A Smurf attacker sends PING requests to an Internet broadcast address.

Sneaker: A person hired to break into a system to test its security.

Sniffer: A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere, making them a favorite weapon of hackers.

Solar Sunrise: A 1998 series of attacks that targeted Defense Department network domain name servers to exploit the vulnerability in the Solaris Operating System computers that operated there. The attacks were thought to be a reconnaissance for a widespread attack on the entire Pentagon information infrastructure.

Spoofing: 1) Faking the sending address of a transmission to make it look like it is coming from a trusted host or address in order to gain illegal entry into a secure system. 2) A generic label for activities in which trusted relationships or protocols are exploited. Impersonating, masquerading, and mimicking are forms of spoofing.

Stateful Inspection: Also referred to as dynamic packet filtering. It’s a firewall architecture that works at the network layer. Stateful inspection checks both the header information and contents of the packet. As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested.

Stealth Viruses: Viruses that attempt to hide from detection programs by masking their presence in boot records or files. When such viruses are run, they install a resident extension. This resident extension intercepts various disk accesses, determines if its own code is part of the disk access, and removes the code before giving the data to the calling program. The result is that the virus can be in several places on the disk. Normal reads of the disk will not reveal it.

T

Tempest U.S.: Government code word for a program launched in the 1950s to reduce the chances of electromagnetic radiation "leakage" from devices used to process, transmit, or store sensitive information. It was believed that such leakage could pose a security threat.

Tentacle: An artificial identity created in cyberspace for malicious and deceptive purposes. The implication is that a single person may have multiple tentacles.

Tiger team: A team of sneakers whose purpose is to penetrate and test security measures.

Trapdoor: A secret way of gaining access to a program or online service. See also Easter Egg, Backdoor, and One-way Hash Function.

Trojan Horse: A program containing additional, hidden code that causes it to launch unauthorized functions, including possible data destruction.

Troll: Deliberately posting provocative online messages with the intent of distracting others into response, usually designed to make them look foolish.

Turn Commands: Commands inserted to forward mail to another address for interception.

U

User Identification: User identification is the process by which a user identifies himself to the system as a valid user. (As opposed to authentication, which is the process of establishing that the user is indeed that user and has a right to use the system.)

V

van Eck monitoring: Monitoring the activity of a computer or other electronic equipment by detecting low levels of electromagnetic emissions from the device. Named for Dr. Wim van Eck.

Venona Project: A secret cryptology project launched at the height of World War II (February 1943) by the forerunner to the National Security Agency. It was designed to examine and possibly exploit encrypted Soviet diplomatic communications and is considered a tremendous success.

Virus: A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

Vulnerability: This term refers to any weakness in any system (either hardware or software) that allows intruders to gain unauthorized access or deny service.

W

Web Bug: A graphic on a Web page or in an e-mail message that monitors who is reading the Web page or e-mail message. Web bugs are often invisible because they are typically only 1x1 pixel in size. They are represented as HTML IMG tags. They are invisible in order to hide the fact that the monitoring is taking place.

Worm: An independent program that reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs.

WinNuke: Technique for causing the Windows operating system of someone you are communicating with to crash or suddenly terminate. See also Blue Bomb.

XYZ

Zombie: A computer that has been implanted with a daemon that puts it under the control of a malicious hacker or organization without the knowledge of the computer owner. Zombies are used by malicious hackers to launch DOS attacks. The hacker sends commands to the zombie through an open port. On command, the zombie computer sends an enormous amount of packets of useless information to a targeted Web site in order to clog the site's routers and keep legitimate users from gaining access to the site. The traffic sent to the Web site is confusing, and therefore, the computer receiving the data spends time and resources trying to understand the influx of data that has been transmitted by the zombies.