

Appendix C

Glossary

-A-

Access: The ability to enter a secured area, either physically or virtually.

Access control: A set of procedures and processes performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and limit access to the resources of a system to only authorized persons, programs, processes, or other systems.

AES (advanced encryption standard): A relatively new encryption standard used by the U.S. federal government for unclassified information. It is freely available for worldwide use.

Antivirus: Software used to prevent infection of computers by computer viruses and worms and to remove such infections after they occur.

Audit: An independent review and examination of system records and activities to assess their veracity and completeness.

Audit trail: A set of records that provides documentary evidence of processing. It is often a chronological record of when users log in, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred.

Authenticate/Authentication: A method for confirming a user's identification, often as a prerequisite to allowing access to resources in a system.

Authenticated user: A user who has accessed a computer system with a valid identifier and authentication combination.

Authenticity: The ability of a third party to verify that the content of a message has not been modified in transit.

Authorization: The privileges and permissions granted to an individual by a designated official to access or use a program, process, information, or system.

-B-

Backup: A copy of a program or data file for the purposes of protecting against loss if the original data becomes unavailable.

Biometrics: The identification of a user (and possibly access control) based on a physical, unchangeable characteristic, such as a fingerprint, iris, face, voice, or handwriting.

Breach: A successful attack on an organization's computing resources, resulting in penetration of one or more secured systems or applications. A breach does not necessarily imply that theft or damage has occurred—simply that an attacker was able to access the system.

-C-

CERT: The Computer Emergency Response Team, established at Carnegie Mellon University after the 1988 Internet worm attack.

Challenge/response: A security procedure in which one communicator requests authentication of another communicator, and the latter replies with a pre-established appropriate reply.

CISSP (Certified Information Systems Security Professional): A common security certification developed and maintained by the Information Systems Security Certification Consortium (ISC). Certification requires passing an extensive exam. More information is available at <<https://www.isc2.org/cgi-bin/index.cgi>>.

Compromise: The disclosure of sensitive information to persons not authorized for access or having a "need to know."

Confidentiality: Protection of information from unauthorized use or disclosure.

Content filtering: A system that blocks certain content, such as objectionable Web pages, spam e-mail, or music files, preventing them from being accessed by users.

Cryptography: A coding method, using an algorithm, by which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format) to ensure the secrecy and/or authenticity of data.

-D-

Data integrity: The state that exists when computerized data are the same as those that are in the source documents and have not been exposed to accidental or malicious alterations or destruction.

Denial of service (DoS): The inability of a computer system to perform its designated mission. A denial of service includes the prevention of authorized access to resources or the delaying of time-critical operations.

Denial-of-service attack: An attack in which a mail or Web server is purposely overloaded with fake requests so that it cannot respond properly to valid ones.

Designated security officer: The person responsible for ensuring that security is provided for and implemented throughout the life cycle of the computer system.

DHCP (dynamic host configuration protocol): A common method of assigning IP addresses to network devices without requiring a permanent IP address for each device. Addresses are assigned to a device as it appears on the network and are released and available for reuse when the device is removed.

Digital certificate: The electronic equivalent of an ID card, which works in conjunction with public key encryption to sign digital signatures.

Disaster-recovery plan: A documented, organized process for implementing emergency response, back-up operations, and post-disaster recovery. The plan is maintained to ensure the availability of critical assets (resources) and facilitate the continuity of operations in an emergency.

Distributed denial-of-service attack (DDoS): A denial-of-service attack in which the attackers load their malignant code onto a host of other machines and use them to overload other systems.

DMCA (Digital Millennium Copyright Act): U.S. federal law passed in 1998 that revises U.S. law to address copyright issues associated with digitally formatted intellectual property. A summary of the law is available from the U.S. Copyright Office at <<http://www.loc.gov/copyright/legislation/dmca.pdf>>. EDUCAUSE maintains a Web site that discusses issues facing institutions as a result of the DMCA, located at <<http://www.educause.edu/issues/issue.asp?ISSUE=DMCA>>.

DNS (Domain Name System): A service that translates Internet domain names to IP addresses, allowing users to request a connection to a server with an English, rather than a numeric, identifier.

-E-

EAP (extensible authentication protocol): A standard for wireless security that allows security authentication data to be passed among RADIUS, the wireless access point, and the wireless client.

Electronic signature: A method and tools used to authenticate the identify of the sender of a message, or to ensure the integrity of the content of the message. Electronic signatures use public key encryption techniques to create a verifiable signature for each document signed. Use of electronic signatures was legalized at the federal level by the Electronic Signatures in Global and National Commerce Act of 2000.

Electronic Signatures In Global and National Commerce Act: U.S. Federal law passed in 2000, stating that electronic signatures may be legally binding for contracts and transactions. Electronic signatures may include digital signatures, click-through agreements at Web sites, biometrics, or digitized versions of handwritten signatures. Many states have passed similar laws.

Encryption: The conversion of text or data into unintelligible (coded) form by means of a reversible translation that is based on a translation table or algorithm.

Enterprise directory: A system for centrally organizing information about an organization's users, passwords, and authorizations to access networked resources.

-F-

FERPA (Family Education Rights and Privacy Act): U.S. federal legislation that protects the privacy of students' education records. More information can be found at <<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>>.

Firewall: A system or combination of systems that enforces a boundary between two or more networks. It is a method of guarding a private network by analyzing the data leaving and entering. A firewall generally possesses the following properties: 1) all traffic from inside to outside, and from outside to inside, must pass through it; 2) only authorized traffic, as defined by the firewall's administrator, is allowed to pass through it; 3) the system itself is immune to penetration.

Firewall, interior: Use of firewall technology to create a barrier between a portion of an internal network and the rest of the internal network.

Firewall, perimeter: Use of firewall technology to create a barrier between an organization's enterprise network and outside networks, such as the Internet.

Firewall, personal: A firewall, generally software based, designed to protect one system from attack. A software-based personal firewall is loaded onto the computer it will protect, much as antivirus software is, rather than residing in a separate piece of hardware like larger network firewalls.

-G-

GIAC (Global Information Assurance Certification): A common IT security certification developed and maintained by GIAC, an organization founded by the SANS Institute, a leading resource for IT security professionals. More information can be found at <http://www.giac.org/>.

Gramm-Leach-Bliley Act of 1999: This act of Congress requires higher education to notify people they deal with of their right to keep their financial information confidential and to protect their financial data. Protection involves having a plan or security policy that includes designating an employee to coordinate information security, identify and repair weaknesses in computer systems, continually monitor systems, provide security training for employees, and require service providers to comply with the law through contract language requiring compliance. More information can be found at <http://www.senate.gov/~banking/conf/>.

-H-

Hacker: A name for an unauthorized person who breaks into or attempts to break into a computer system to which he is not entitled entry by circumventing software security safeguards.

Hardware token: A security device carried by a user, required to authenticate to the system. Examples could include a dongle attached to a PC's USB or serial port or a password generator, such as RSA's SecureID product. Such devices are often used in conjunction with a password, resulting in two-factor authentication.

HIPAA (Health Insurance Portability and Accountability Act): A multifaceted U.S. law passed in 1996. In an information security context, the law sets standards for information security and privacy for organizations dealing with patient-identifiable medical data, as well as penalties for noncompliance. More information about HIPAA can be found at <http://www.hipaa.org/>.

Host: Sometimes used as a synonym for "server."

-I-

ICMP (Internet control message protocol): A message control and error-reporting protocol used for communication between servers and Internet gateways. A vulnerability in ICMP results in a type of denial-of-service attack called the "Ping of Death."

Information security: The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information security officer (ISO): The person responsible for ensuring that security is provided for and implemented throughout the life cycle of the computer system.

Insider attack: An attack originating from inside a protected network, generally by an authorized user of that network.

Integrity: Ensures that 1) data is a proper representation of information, 2) data retains its accuracy, 3) data remains in perfect condition, and 4) the computerized data represent those in the source documents and have not been exposed to accidental or malicious alteration or destruction.

Intruder: An individual who gains, or attempts to gain, unauthorized access to a computer system or unauthorized privileges on that system.

Intrusion detection system (IDS): A system used to detect of break-ins or break-in attempts. KPMG defines network-based intrusion detection as systems that analyze network traffic by looking for known patterns of traffic that might indicate an attack. Host-based intrusion detection systems analyze logs produced by operating systems to identify security-related events.

IP (Internet protocol): The most common protocol currently used to send information across data networks. All traffic on the Internet uses this protocol. Using IP, each system on the network is assigned a unique address in the form xxx.xxx.xxx.xxx, which identifies the source and destination of each packet. Standard IP network packets are not encrypted.

IP spoofing: An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.

IRC (Internet relay chat): A system for allowing users to chat across networks, including the Internet.

-J-

-K-

Kerberos: A secret-key network authentication system used for encryption and authentication. Kerberos was designed to authenticate requests for network resources rather than to authenticate authorship of documents. Kerberos was developed at and continues to be enhanced by MIT. More information can be found at <<http://web.mit.edu/kerberos/>>.

-L-

Logging: The process of storing information about events that occurred on the firewall, network, computer, or application.

-M-

Malicious code: Software that is intentionally included in a computer system for an unauthorized purpose.

-N-

NetBIOS: A networking protocol supported by Microsoft operating systems, used for communication across a local area network.

Network: A communications medium and all components attached to that medium whose responsibility is the transference of information.

Network infrastructure: The links, routers, and switches that allow hosts to communicate with one another.

Nonrepudiation: Method by which the sender is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data. The origin or receipt of a specific message must be verifiable by a third party.

NTP (network time protocol): A protocol used to synchronize systems' clock times across a network.

-O-

-P-

Packet: The unit of data sent across a network during transmission. Files are broken into packets of an efficient size for routing by the sending system and reconstructed at the destination.

Password: A string of characters used to authenticate a user to a system or application.

Password, multilevel: Use of more than one password required to access an information resource. For example, a user may have to log in to the network and then use a different password to access a system on the network. Without both passwords, access cannot be obtained.

Password, multiple use: A password assigned to a user that can be used for an unlimited or specified period of time.

Password, single use: A password that can only be used once. Such passwords are often generated by a hardware token that is synchronized to a server. Single-use passwords remove the danger of a password being compromised during transmission across the network.

Perimeter-based security: The technique of securing a network by controlling access to all entry and exit points of the network.

Personnel security: The procedures established to ensure that all personnel who have access to any sensitive information have all the required authorities or appropriate security authorizations.

Physical security: The application of physical barriers, such as locked doors, and control procedures, such as requiring photo IDs to enter certain areas, as preventative measures or safeguards against threats to resources and information.

Ping: A simple program used on TCP/IP networks to determine if another computer is active on the network. The originating system sends a request, and if active, the pinged computer sends a reply.

Port: A logical connection in TCP/IP networking to connect a client to a service. Port numbers can range from 0 to 65536. Commonly used applications such as HTTP have pre-assigned port numbers (HTTP always uses port 80, for example).

Private key: In encryption, one key (or password) is used to both lock and unlock data.

Privacy: The policies that determine what information is gathered, how it is used, and how customers are informed and involved in this process.

Protocols: Agreed-upon methods of communications used by computers.

Public key encryption (PKI): A coding system in which encryption and decryption are done with public and private keys, allowing users who don't know each other to send secure or verifiable messages.

-Q-**-R-**

RADIUS (remote authentication dial-in user service): A client-server protocol and software that allow remote access servers to communicate with a central server to authenticate users and authorize their access to network resources.

Remote access: The hookup of a remote computing device via communications lines such as ordinary phone lines or wide area networks (WANs) to access network applications and information.

Residual risk: The part of risk remaining after security measures have been implemented.

Risk: The likelihood that a vulnerability will be exploited or that a threat may become harmful.

Risk analysis: The process of identifying an organization's information resources, existing controls, security risks, and vulnerabilities; determining their magnitude; and identifying areas needing safeguards. It establishes a potential level of damage in dollars and/or other assets.

Risk assessment: An estimate of the harm to business likely to result from a security failure and of the likelihood of such a failure occurring, given the threat environment and the measures in place to prevent a failure.

Risk management: The total process of identifying, measuring, controlling, and eliminating or minimizing uncertain events that may affect system resources.

Rogue program: Any program intended to damage programs or data.

Router: A network device that connects multiple networks and forwards network packets to their destinations, based on a series of algorithms. Routers can be configured to allow or block different types of network traffic.

-S-

Scan: Testing of a system to determine whether any known vulnerabilities exist on it.

Security awareness: Activities, materials, and/or training designed to make an organization's user community knowledgeable about potential security threats and how to combat them.

Security incident: Any event and/or condition that has the potential to impact the security of a system and may result from intentional or unintentional actions.

Security policy: The set of laws, rules, and practices that regulate the acceptable use of computer resources and how an organization manages, protects, and distributes controlled information.

SFTP (Secure File Transfer Protocol): An encrypted version of the commonly used FTP file-transfer tool. SFTP functions are often included as part of SSH (secure shell) software.

Shibboleth: An open-source middleware solution created by Internet2/MACE to allow organizations to exchange information about their users in a secure manner that ensures protection of privacy. The purpose of the exchange is typically to determine if a person using a Web browser has permission to access a target resource based on information such as being a member of an institution or a particular class. More information about Shibboleth can be found at <<http://shibboleth.internet2.edu/>>.

Single sign on: A product or technology that allows users to authenticate once to a central authentication server and be authorized to use multiple applications and network resources without having to log in separately to each one.

Smart card: A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual and/or other information such as digital cash. A smart card holds its own data and applications and does its own processing.

Sniffer: A network device that views all passing packets, allowing the user to see any unencrypted data, including some user name and password traffic.

Social engineering: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by someone pretending to be an authorized user who telephones users or operators in an attempt to gain illicit access to systems.

SSH (secure shell): An application that provides an encrypted connection, both for authentication and data transmission, for remote login to a UNIX system.

SSL (secure sockets layer): A protocol, originally developed by Netscape, that creates a secure connection between a client (typically a Web browser), and a server through the use of either 40-bit or 128-bit public key encryption. Web pages protected with SSL usually use the "https" prefix.

Switch: A networking device that takes input from multiple ports and channels data to the specific output port that will take the data toward its destination.

-T-

TCP/IP: The common networking protocol used for all Internet traffic. Also commonly referred to as IP, or Internet Protocol.

Timeout: A system feature that terminates a user's session after a pre-determined period of inactivity, requiring the user to reauthenticate before being able to access the system again.

Trojan horse: A computer program that disguises itself as a beneficial or entertaining program but actually contains additional (hidden) functions that damage a computer or installs code that can counteract security measures and be detrimental to network security.

Trusted computing system: A computer and operating system that employs secure hardware and software measures to allow its use for processing a range of sensitive information and can be verified to implement a given security policy.

Tunneling router: A system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual de-encapsulation and decryption.

Two-factor authentication: Authentication based on something a user knows, such as a password (factor one), plus something the user has, such as an identification card (factor two). To access a network, the user must have both factors.

-U-

User identification: The process, usually through a unique character string, by which a user identifies himself to the system as a valid user.

-V-

Verification: Comparing two levels of system specifications and ensuring that information has not been changed in transit or in storage, either intentionally or accidentally.

Virus: A self-replicating code segment that causes a copy of itself to be inserted in one or more other programs. The virus usually performs an unwanted function. A program does not need to perform malicious actions to be a virus; it only needs to infect other programs.

VPN (virtual private network): A remote access system that is replacing traditional dial-up modem pools. Allows remote users to connect to an Internet service provider (ISP) or a private IP-based network and establish a secure connection with network servers through an encrypted tunnel.

Vulnerability: An error or a weakness in the design, implementation, or operation of a system.

Vulnerability assessment: A review of a system or systems to identify weaknesses or errors in design, implementation, or operation.

-W-

WAN (wide area network): A network of local area networks (LANs) that provides communication and services over a geographic area larger than that served by a LAN.

WEP (wired equivalent privacy): A protocol used to provide security for wireless LAN connections by encrypting the connection between wireless access points and wireless clients. WEP is part of the IEEE's 802.11b wireless networking standard.

Worm: A computer program that replicates itself and sends copies from computer to computer. Upon arrival, the worm may be activated to replicate and spread again. In addition, the worm usually performs an unwanted function.

-XYZ-

Y2K: An acronym for the Year 2000 Problem that involved three specific issues: two-digit data storage (storing data as 00 instead of 2000), leap-year calculations, and special meanings for dates.

References

National Security Telecommunications and Information Systems Security Committee (NSTISSC), *Glossary of Computer Security Terminology*, published by NIST as NISTIR 4659 and available from National Technical Information Service (NTIS) as PB92-112259.

National Technical Information Service (NTIS), *Glossary for Computer Security Terms*. FIPS PUB 39, Springfield, Va., 15 Feb. 1976. Withdrawn Apr. 1993; replacement is FIPS 11-3.

National Computer Security Center (NCSC), *Introduction to Certification and Accreditation*, NCSC-TG-029, Ver. 1, NSA, Ft. George G. Meade, Md., Jan. 1994.

Treasury Security Manual, TD P 71-10, Appendix B, 1993.

Set Solutions Inc., "Glossary of Security Terms," retrieved 18 Feb. 2003 from <<http://www.setsolutions.com/security.html>>.

S. D. Scalet, "Security Terms Glossary," *CIO Magazine*, May 2002; retrieved 18 Feb. 2003 from <<http://www.cio.com/security/edit/glossary.html>>.