

# Appendix E

## Glossary

### -A-

**Abuse of privilege:** When a user performs an action he or she should not have, according to organizational policy or law.

**Acceptable use:** A policy defining what activities are acceptable to the organization to which the computer or network belongs. Acceptable use policies may define content (such as illegal music downloads) that may not be accessed, activities (such as hacking) that may not be conducted, or bandwidth restrictions (such as no streaming video).

**Access:** The authorization to enter a secured area or a secured system.

**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.

**Access point:** In wireless networks, the connection point between the wireless and wired network. The access point transmits and receives data, and passes it to and from the broader network.

**Adequate security:** Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.

**Adware:** Similar to spyware, adware is installed on users' systems without their knowledge and is used to deliver pop-up advertisements to the user's desktop.

**AES:** Advanced Encryption Standard. An encryption algorithm used to secure material classified as "sensitive" but not "classified" by the federal government, per FIPS 197.

**Antivirus software:** A software package that monitors a computer for virus activity and attempts to remove or isolate infections when they are found.

**Application:** A software organization of related functions, or series of interdependent or closely related programs, that when executed accomplish a specified objective or set of user requirements.

**Application owner:** The individual or group with the responsibility to ensure that the program or programs, which make up the application, accomplish the specified objective or set of user requirements established for that application, including appropriate security safeguards.

**Audit:** An independent evaluation of the controls employed to ensure appropriate protection of an organization's information assets.

**Audit trail:** A set of records that provides documentary evidence of activity. 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.

**Authentication (multifactor):** Any authentication method that requires multiple forms of identity verification. Usually implemented by requiring a combination of something you have (such as a hardware token or a thumbprint) with something you know (such as a password).

**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.

**Authorized person:** A person who has the need-to-know for sensitive information in the performance of official duties and who has been granted authorized access at the required level.

**Awareness:** Activities and materials designed to increase users' or customers' knowledge of security topics, how to keep themselves and their computing assets secure, and how to react in the event of an incident.

## **-B-**

**Back door:** An entry point to a program or a system that is hidden or disguised. Although often created by the software's author for maintenance, if the back door becomes known, unauthorized users (or malicious software) can gain entry and cause damage.

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

**Backup (centralized):** The capability to back up multiple systems in a coordinated way.

**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.

**Botnet:** A group of computers compromised by a hacker, or "botmaster," and used to launch additional attacks, send spam, or pursue other unsavory purposes.

**Breach:** Unauthorized access to a system, network, or data.

**Business continuity:** Plans, processes, and procedures designed to keep critical business operations functioning in the event of a disaster. Business continuity is a broader approach to disaster recovery, which tends to focus on restoring computer systems rather than business capabilities.



**CERT:** The Computer Emergency Response Team that was established at Carnegie Mellon University after the 1988 Internet worm attack. Considered a leading authority on IT security topics.

**Certification:** The comprehensive analysis of the technical and nontechnical features and other safeguards that a computer network must have to meet a set of specified security requirements. Also, a credential issued to security professionals who qualify, indicating their proficiency in the discipline. Common certifications include the CISSP and GIAC.

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

**Chief information officer (CIO):** Generally the most senior executive with responsibility for an organization's information technology functions and capabilities.

**Clear or clearing:** The removal of sensitive data from computer storage and other peripheral devices with storage capacity at the end of a processing period.

**Coded file:** In encryption, a coded file contains unreadable information.

**Compromise:** The disclosure of sensitive information to persons lacking authorized access or not having a need-to-know.

**Computer security:** Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

**Confidentiality:** Protection of information from unauthorized use or disclosure.

**Contingency plan:** The documented organized process for implementing emergency response, backup operations, and postdisaster recovery, maintained for a system as part of its security program, to ensure the availability of critical assets (resources) and facilitate the continuity of operations in an emergency.

**Conventional encryption:** When encryption and decryption are performed using the same key.

**Critical assets:** Those assets that provide direct support to the organization's ability to sustain its mission.

**Critical processing:** Any applications so important to an organization that little or no loss of availability is acceptable.

**Critical infrastructure:** A foundation of services that citizens and businesses rely on for their health and safety. Telecommunications, transportation, energy, and banking services are part of the critical infrastructure, which is often privately owned but which citizens expect the government to protect.

**Cryptography:** A coding method, using an algorithm, in which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format by someone with a secret key) to ensure the secrecy and authenticity of messages.

## -D-

**DNS spoofing:** Assuming the DNS (domain name server—the “yellow pages” of the Internet) name of another system by either corrupting the name service cache of a victim system or compromising a domain name server for a valid domain.

**Data:** A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing.

**Data-driven attack:** A form of attack in which the attack is encoded in innocent-seeming data, which is executed by a user or other software to implement an attack.

**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.

**Data steward:** A designated individual or group charged with controlling the definition and integrity of, and access to, a set of institutional data.

**Deciphering:** The translation of encrypted text or data into original text or data.

**Decode:** The translation of encoded text or data into plaintext through the use of a code.

**Decrypt:** The translation of either encoded or enciphered text into original text or data.

**Defense in-depth:** The security approach whereby each system on the network is secured to the greatest possible degree.

**Denial of service:** 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 (DoS):** An attack in which a server or network 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 a computer system and implemented throughout its life cycle.

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

**Disaster:** An unexpected event or series of events that leads to a disruption of normal business function. Examples of disasters include a natural disaster (such as an earthquake), an isolated event (such as a fire), or a hacking incident that brings down an organization’s network.

**Disaster recovery:** Plans, processes, and procedures for restoring an organization's information technologies following a disaster.

**Discretionary access control (DAC):** A means of restricting access to objects based on the identity of subjects or groups to which they belong or on the possession of an authorization granting access to those objects. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

**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, which are then used to perform the attack.

### -E-

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

**EAP:** Extensible Authentication Protocol. Used for wireless networks, EAP allows multifactor authentication mechanisms to be used when authenticating to a wireless access point.

**Electronic signature:** Generally, using public key encryption, an electronic signature creates a unique identifier that can be attached to a document to prove its sender or signer, as well as the date and time it was signed. It is also sometimes used to verify that a document's contents are unchanged since the time of signature.

**Electronic Signatures Act:** A law 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.

**Emergency response:** Responses to emergencies such as fire, flood, civil commotion, natural disasters, or bomb threats to protect lives, limit property damage, and limit the impact on computer systems.

**Enciphering:** The conversion of plain text or data into unintelligible form by means of a reversible translation that is based on a translation table or algorithm.

**End-to-end encryption:** Encryption at the point of origin in a network, followed by decryption at the destination.

**Encryption:** The conversion of text or data into unintelligible form by means of a reversible translation that is based on a translation table or algorithm. Data can be encrypted in transmission, in storage, or both.

**Enterprise directory:** A database containing information on an organization's users, such as usernames, passwords, and phone numbers, that can be used to provide this information to other systems or individuals.

### -F-

**Fault tolerance:** A design method that ensures continued systems operation in the event of individual failures by providing redundant system elements.

**FERPA:** Family Education Rights and Privacy Act, a piece of federal legislation that restricts access to student records.

**Filtering:** Blocking access to some information passing across a network while allowing other information to pass.

**FIPS:** Federal Information Processing Standard. A set of documents published by the National Institute of Standards and Technology (NIST) that outline the federal government's required or recommended procedures for various IT-related topics.

**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 organization, is allowed to pass through it; (3) the system itself is immune to penetration.

**Firewall (application):** A software-based firewall, also called a host-based firewall, usually residing on a system being utilized for other purposes.

**Firewall (interior):** A firewall installed between segments of a private network, designed to control the flow of traffic between these segments. Interior firewalls are often used to provide additional protection to sensitive areas of the network, such as central data centers.

**Firewall (perimeter):** A firewall installed between a private network and other public networks, such as the Internet. A perimeter firewall controls all traffic between the internal network and other networks.

**FISMA:** The Federal Information Security Management Act, part of the E-Government Act of 2002. It mandates a set of standards, as defined by NIST, to ensure the consistent application of effective security standards and practices by federal agencies and their agents.

**Flooding programs:** A code which, when executed, will bombard the system with requests in an effort to slow or shut down the system.

**Forensics:** Examination of a system to find traces of activity. Usually used during incident response or during criminal investigations.

## -G-

**Global security:** The ability of an access control package to provide protection across a variety of computing environments, providing users with a common security interface.

**Governance:** Formal procedures usually executed by a cross-functional group established to oversee a function or process and make decisions about its activities.

**Gramm-Leach-Bliley Act of 1999:** This act of Congress, mostly focused on the financial services sector, 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.

**-H-**

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

**Hardware token:** An electronic device used for multifactor authentication. This method combines something you have (such as a password generated by the token, or a digital certificate resident on a USB stick) with something you know (such as a unique PIN).

**HIPAA:** Healthcare Insurance Portability and Accountability Act—federal legislation that restricts access to personally identifiable healthcare information.

**Host-based security:** The technique of securing a network through effective management of security vulnerabilities on individual devices connected to the network, with limited or no use of perimeter network defenses.

**HSPD-12:** Homeland Security Presidential Directive 12, which requires the use of uniform standards in issuing government identify credentials.

**-I-**

**Identification:** The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

**Identity management:** The set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities.

**Identity theft:** The use of personal information about someone else to commit a crime, such as credit card fraud.

**Incident response:** A procedure that is used once a security incident has occurred to block the attack, determine what has occurred, communicate to the appropriate constituents, and remediate the issue to prevent it from reoccurring. Many organizations have formal incident response procedures.

**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 the computer system and implemented throughout its life cycle. The chief information security officer, or CISO, is a relatively new position, often reporting to the chief information officer (CIO), responsible for all of an organization's security activities.

**Information systems security:** The protection of information assets from unauthorized access to or modification of information, whether in storage, processing, or transit.

**Insider attack:** An attack originating from inside a protected network. Usually refers to an attack by a trusted member of the community, such as an employee.

**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 represents that in the source documents and has 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:** Detection of break-ins or break-in attempts. KPMG defines network-based intrusion detection as systems that analyze network traffic, 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.

**Intrusion prevention:** Any tool or process used to keep unauthorized users from accessing internal networks and resources. An intrusion prevention system actively monitors the network, looking for patterns indicating malicious activity and taking action, such as blocking all traffic from a suspect port, when an issue is uncovered.

**IP sniffing:** Monitoring traffic over a TCP/IP network, usually to look for unencrypted information of value, such as passwords or confidential data.

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

**-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.

**Key:** A sequence of characters used to encode and decode a file.

**Keylogger:** A device or program that records a user's keystrokes, usually used to steal usernames and passwords.

**-L-**

**Label:** The marking of an item of information that reflects its information security classification.

**Log:** Also called a syslog, a file that tracks activity on a system or device.

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

**Log processing:** How audit logs are processed, searched for key events, or summarized.

**-M-**

**MAC:** Media access control. The MAC address is a unique hardware address associated with any networked device.

**Malicious code:** Software or firmware that is intentionally included in a computer system for an unauthorized purpose. Also referred to as malware.

**Monitoring:** Also called scanning, the activity of proactively examining the network and the devices connected to it for known vulnerabilities, allowing them to be addressed before they can be exploited.

### -N-

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

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

**Network security:** Protection of networks and their services against unauthorized modification, destruction, or disclosure and the provision of assurance that the network performs its critical functions correctly and there are no harmful side effects.

**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.

**Notification:** Now required by the laws of at least 22 states, notification is the process of communicating the nature and extent of any security breach that may involve personal data to those individuals whose information may have been compromised.

### -O-

**One-time password:** A password issued only once as a result of a challenge/response authentication process. Used to prevent unauthorized access, as it cannot be reused.

**Overwrite procedure:** A process that removes or destroys data recorded on a computer storage medium by writing patterns of data over, or on top of, the data stored on the medium.

### -P-

**Password:** A protected and private character string assigned to a specific user. Often, knowledge of the password associated with the user ID is considered proof of authorization.

**Password (conventional):** A conventional, or "weak," password does not impose length, character, or other restrictions on users, making them relatively easy to compromise.

**Password (one-time):** A single-use password, often generated by a hardware token, which is entered into a system in response to a challenge at the time of the authentication attempt. This system is more secure than other password methods, since the password can be used only once, making its interception of no value to a hacker.

**Password (strong):** A strong password requires, either through policy, software controls, or both, the use of passwords containing at least a certain number or characters and a combination of letters, numbers, special characters, and so on, that make a password harder to crack.

**Patch:** An interim release of software designed to fix bugs or security vulnerabilities.

**Patch management:** A process for identifying, testing, installing, and monitoring compliance with software patches.

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

**Personal information:** Also called personally identifiable information. Information that can be used to identify or impersonate the individual to which it relates (such as a Social Security number).

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

**Phishing:** A mechanism used by hackers to attempt to trick users into revealing personal information or accessing hostile Web sites. Phishing attacks are often conducted by sending fake e-mails asking users to access a legitimate-appearing Web site, which it in fact is not.

**Physical security:** The application of physical barriers and control procedures (such as locked doors) as preventative measures or safeguards against threats to resources and information.

**Policy:** A formal document describing roles, responsibilities, standards, and enforcement mechanisms with regard to a particular issue.

**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. A commonly used protocol is TCP/IP, the protocol used for communication across the Internet.

**Proxy:** A software agent that acts on behalf of a user.

**Public key:** A two-key system in which the key used to lock data is made public, so everyone can "lock." A second, private key is used to unlock or decrypt.

**Public key cryptography:** 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. Also called PKI.

## **-Q-**

**Quarantine:** Removal of a compromised system from the network. This can be done physically (by removing the wire connecting the system to the network) or logically (by blocking traffic to and from the affected device).

## **-R-**

**RADIUS:** Remote authentication dial-in user service. A security protocol used for authentication and authorization. It stores user profiles on a central server, and remote access servers share these profiles. RADIUS is often used on wireless networks.

**Recovery:** The process of restoring a computer facility and related assets, damaged files, or equipment so as to be useful again after a major emergency that resulted in curtailing of normal operations.

**Remote access:** Gaining access to resources on a private network while not physically (or wirelessly) connected to that network. Access is usually gained across the Internet or via a modem connection.

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

**Risk:** Risk refers to the likelihood that vulnerability will be exploited or that a threat may become harmful.

**Risk assessment:** Process of analyzing threats to and vulnerabilities of a system or organization to determine the risks (potential for losses) and using the analysis as a basis for identifying appropriate and cost-effective defensive measures.

**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 forwards packets to their next destination, en route to their target address. A router also can be used to limit or block the flow of traffic across the network using ACLs, or access control lists.

## -S-

**Safeguards:** The protective measures, countermeasures, specifications, or controls prescribed to meet security requirements for a specific system. Safeguards consist of actions taken to decrease the organization's degree of vulnerability to a given threat probability.

**Scalability:** The ability to expand a computing solution to support large numbers of users without impacting performance.

**Secure disposal:** With regard to physical computer media (such as floppy disks, CDs, and hard disks), a procedure that ensures that data is truly erased or that the media has been destroyed to the point of being unreadable. Secure disposal of nonelectronic records would involve shredding or some other similar procedure.

**SecureID:** A hardware-token-based one-time-password generation product from RSA Security. Its name is synonymous with this type of product, which is actually available from a number of vendors.

**Security plan:** A documented approach that addresses how an organization will implement security measures.

**Security program:** A comprehensive set of plans, policies, procedures, tools, and materials designed to address the threats a specific organization is facing.

**Security incident:** Any event or condition that has the potential to impact the security or accreditation of a management information system (MIS) 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.

**Security requirements:** Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policies.

**Security violation:** An event that may result in disclosure of sensitive information to unauthorized individuals. A security violation may also result in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of any computer system resources.

**Shibboleth:** A cross-organization security platform developed as part of Internet2. Shibboleth is defined as standards-based open source middleware software that provides Web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

**Single sign-on:** A term used to describe any solution that allows users to authenticate once and then passes this authentication on to other systems without requiring other interaction by the user, allowing him or her to log in once and access multiple systems.

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

**Social engineering:** An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by someone telephoning users or operators and pretending to be an authorized user, thereby attempting to gain illicit access to systems.

**Spam:** An unwanted e-mail message, usually pitching a product or service.

**Spoofing:** Changing an e-mail header to make it appear that it came from a different address than it actually did, usually to make it appear that a fake message is legitimate. Often used in conjunction with phishing attacks.

**Spyware:** A software program installed on a system without the owner's permission that sends information back to the installer. Spyware may have a relatively benign purpose, such as tracking a user's Web browsing activity, or it may be a more malicious program, such as a keylogger that attempts to steal usernames and passwords.

**Standard security procedures:** Step-by-step security instructions tailored to users and operators of systems and applications that process sensitive information.

**Stand-alone system:** A single-user computer not connected to any other systems.

**Syslog:** Also called a log, a file that tracks activity on a system or device.

**Syslog (central):** A server that collects syslog data from multiple systems. Often used for intrusion detection and network analysis.

**-T-**

**Threat:** An event, process, activity, or substance perpetuated by one or more threat agents that has an adverse effect on an organization.

**Threat agent:** Any person or thing that acts—or has the power to act—to cause, carry, transmit, or support a threat.

**Time-out:** Ending a user session after a predetermined period of inactivity has passed. This limits the chance that a workstation will be left logged in and unattended.

**Token:** An authentication tool used to send and receive challenges and responses during the user authentication process.

**Trapdoor:** An undisclosed, undocumented entry point into a computer program. A trapdoor is used to gain access without the normal methods of access authentication.

**Trojan horse:** A computer program that disguises itself as a beneficial or entertaining program but that actually contains additional (hidden) functions that damage a computer or install 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.

**Two-factor authentication:** Also called multifactor 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). In order 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 technique that 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.

**-W-**

**WEP:** Wired equivalent privacy. A security protocol used in wireless networks. Early WEP standards used 40-bit encryptions, while later implementations use 128-bit encryption.

**Worm:** A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability, or availability. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.

**-XYZ-**

**Zombie:** A compromised system being controlled as part of a botnet.

**References**

*Glossary of Computer Security Terminology* developed by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and published by NIST as NISTIR 4659. Available from NTIS as PB92-112259.

*Glossary for Computer Security Terms*. National Technical Information Service (NTIS), FIPS PUB 39, Springfield, VA., 02/15/76. Withdrawn 4/93. Replacement is FIPS 11-3.

*Glossary of Security Terms*. Set Solutions Inc. Retrieved September 18, 2006, from <http://www.setsolutions.com/security.htm>

*Introduction to Certification and Accreditation*. (1994, January). National Computer Security Center (NCSC), NCSC-TG-029, Ver. 1, NSA, Ft. Meade, MD: NCSC.

Scalet, S. D. (2002, May). Security Terms Glossary. *CIO Magazine*. Retrieved September 8, 2006, from <http://www.cio.com/security/edit/glossary.html>

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