**A**

**access control**

The mechanism by which subjects are granted or restricted access to objects. It includes hardware, software, and organizational policies or procedures that identify and authenticate subjects, verify authorization to objects, and monitor or record access attempts.

**accountability**

The process of holding someone responsible for something. In this context, it is possible if a subject's identity and actions can be tracked and verified.

**administrative access controls**

The policies and procedures defined by an organization's security policy to implement and enforce overall access control. Examples include hiring practices, background checks, data classification, security training, vacation history reviews, work supervision, personnel controls, and testing.

**admissible evidence**

Evidence that is relevant to determining a fact. The fact that the evidence seeks to determine must be material (in other words, related) to the case. In addition, the evidence must be competent, meaning that it must have been obtained legally. Evidence that results from an illegal search would be inadmissible because it is not competent.

**aggregation**

A number of functions that combine records from one or more tables to produce potentially useful information.

**Agile Software Development**

A set of software development approaches that eschew the rigid models of the past in favor of approaches that place an emphasis on the needs of the customer. Also favors quickly developing new functionality that meets those needs in an iterative fashion.

**AND**

The operation that checks to see whether two values are both true.

**applet**

Code objects sent from a server to a client to perform some action. They are self-contained miniature programs that execute independently of the server that sent them.

**asset valuation**

A dollar value assigned to an asset based on actual cost and nonmonetary expenses. This might include costs to develop, maintain, administer, advertise, support, repair, and replace; as well as other values, such as public confidence, industry support, productivity enhancement, knowledge equity, and ownership benefits.

**asymmetric key**

Public key cryptosystems that use a pair of keys (public and private) for each participant. Messages encrypted with one key from the pair can only be decrypted with the other key from the same pair.

**audit trails**

The records created by recording information about events and occurrences into a database or log file. Some common uses include reconstructing an event, extracting information about an incident, and proving or disproving culpability.

**authentication**

The process of verifying or testing that the identity claimed by a subject is valid.

**authorization**

A process that ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity.

**automatic private IP addressing (APIPA)**

A feature of Windows that assigns an IP address to a system should DHCP address assignment fail. The IP address range used is 169.254.0.0-169.254.255.255.

**availability**

The assurance that authorized subjects are granted timely and uninterrupted access to objects.

**B**

**baseline**

The minimum level of security that every system throughout the organization must meet. It can be more than a security baseline. It can also be a performance baseline (used by behavior-based IDSs) or a configuration baseline (used for configuration management).

**Basic Input/Output System (BIOS)**

The operating system-independent primitive instructions that a computer needs to start up and load the operating system from disk.

**Bell-LaPadula model**

A confidentiality-focused security model based on the state machine model and employing mandatory access controls and the lattice model.

**Biba model**

An integrity-focused security model based on the state machine model and employing mandatory access controls and the lattice model.

**biometrics**

The use of human physiological or behavioral characteristics as authentication factors for logical access and identification for physical access.

**boot sector**

The portion of a storage device used to load the operating system and the types of viruses that attack that process.

**bot**

An intelligent agent that continuously crawls a variety of websites retrieving and processing data on behalf of the user.

**broadcast domain**

A group of networked systems in which all other members receive a broadcast signal when one of the members of the group transmits it.

**brute-force attack**

An attack made against a system to discover the password to a known identity (in other words, username). It uses a systematic trial of all possible character combinations to discover an account's password.

**business continuity planning (BCP)**

The assessment of risks to organizational processes and the creation of policies, plans, and procedures to minimize the impact those risks might have on the organization.

**business impact assessment (BIA)**

An analysis that identifies the resources that are critical to an organization's ongoing viability and the threats posed to those resources. It also assesses the likelihood that each threat will actually occur and the impact those occurrences will have on the business. Also known as business impact analysis (BIA).

**C**

**Caesar cipher**

A simple three-position shifting monoalphabetic substitution cipher employed by Julius Caesar.

**Challenge Handshake Authentication Protocol (CHAP)**

One of the authentication protocols used over PPP links; encrypts usernames and passwords.

**CIA Triad**

The three essential security principles of confidentiality, integrity, and availability.

**cipher**

A system that hides the true meaning of a message. They use a variety of techniques to alter and/or rearrange the characters or words of a message to achieve confidentiality.

**cloud computing**

A concept of computing where processing and storage are performed elsewhere over a network connection rather than locally.

**cold sites**

Standby facilities large enough to handle the processing load of an organization and with appropriate electrical and environmental support systems.

**collusion**

An agreement between multiple people to perform an unauthorized or illegal action.

**Computer Fraud and Abuse Act**

A U.S. law written to exclusively cover computer crimes that cross state boundaries to avoid infringing on states' rights.

**Computer Security Act (CSA) of 1987**

A U.S. law that mandates baseline security requirements for all federal agencies.

**confidentiality**

The assurance that information is protected from unauthorized disclosure and the defined level of secrecy is maintained throughout all subject-object interactions.

**conclusive evidence**

Incontrovertible evidence that overrides all other forms of evidence.

**concurrency**

A security mechanism that endeavors to make certain that the information stored in a database is always correct or at least has its integrity and availability protected. It uses a "lock" feature to allow an authorized user to make changes and then "unlocks" data elements only after all changes are complete.

**critical path analysis**

A systematic effort to identify relationships between mission-critical applications, processes, and operations and all of the necessary supporting elements.

**cross-site scripting (XSS)**

A form of web application attack when a site contains some type of reflected input. Often exploited using script injection.

**cryptography**

Algorithms applied to data that are designed to ensure confidentiality, integrity, authentication, and/or nonrepudiation.

**custodian**

A subject that has been assigned or delegated the day-to-day responsibilities of classifying and labeling objects and properly storing and protecting objects. It is typically the IT staff or the system security administrator.

**D**

**deencapsulation**

The process of stripping a layer's header and footer from a PDU as it travels up the OSI model layers.

**denial of service (DoS)**

A type of attack that prevents a system from processing or responding to legitimate traffic or requests for resources and objects.

**Delphi technique**

An anonymous feedback and response process used to arrive at a group consensus.

**dictionary attack**

An attack against a system designed to discover the password to a known identity (in other words, a username). In this attack, a script of common passwords and dictionary words is used to attempt to discover an account's password.

**differential backup**

A type of backup that stores all files that have been modified since the time of the most recent full backup.

**Digital Millennium Copyright Act**

A law that establishes the prohibition of attempts to circumvent copyright protection mechanisms placed on a protected work by the copyright holder. Also limits the liability of Internet service providers when their circuits are used by criminals violating the copyright law.

**direct evidence**

Evidence that proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses.

**documentary evidence**

Any written items brought into court to prove a fact at hand. This type of evidence must also be authenticated.

**E**

**encapsulation**

The process of adding a header and footer to a PDU as it travels down the OSI model layers.

**F**

**fault tolerance**

The ability of a system to suffer a fault but continue to operate. It is achieved by adding redundant components such as additional disks within a redundant array of independent disks (RAID), or additional servers within a failover clustered configuration.

**firewall**

A network device used to filter traffic. It is typically deployed between a private network and a link to the Internet, but it can be deployed between departments within an organization. They filter traffic based on a defined set of rules.

**firmware**

Software that is stored in a ROM chip.

**fraggle**

A form of denial-of-service attack similar to smurf, but it uses UDP packets instead of ICMP.

**full backup**

A complete copy of data contained on the protected device on the backup media. This also refers to the process of making a complete copy of data.

**full-interruption tests**

A disaster recovery test that involves shutting down operations at the primary site and shifting them to the recovery site.

**G**

**Government Information Security Reform Act of 2000**

Act that amends the U.S. Code to implement additional information security policies and procedures.

**Gramm-Leach-Bliley (GLBA) Act**

A law passed in 1999 that eased the strict governmental barriers between financial institutions. Banks, insurance companies, and credit providers were severely limited in the services they could provide and the information they could share with each other. This act somewhat relaxed the regulations concerning the services each organization could provide.

**H**

**hash function**

The process of taking a full message and generating a unique output value derived from the content of the message. This value is commonly referred to as the message digest.

**hearsay evidence**

Evidence consisting of statements made to a witness by someone else outside of court. Computer log files that are not authenticated by a system administrator can also be considered this type evidence.

**hot site**

A configuration in which a backup facility is maintained in constant working order. The site has a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities.

**I**

**identification**

The process by which a subject professes an identity and accountability is initiated. This process can consist of a user providing a username, a logon ID, a PIN, or a smart card or a process providing a process ID number.

**incremental backup**

A backup that stores only those files that have been modified since the time of the most recent full or incremental backup. This is also used to mean the process of creating such a backup.

**integrity**

A state characterized by the assurance that modifications are not made by unauthorized users and authorized users do not make unauthorized modifications.

**intrusion detection system (IDS)**

A product that automates the inspection of audit logs and real-time system events. They are generally used to detect intrusion attempts, but they can also be employed to detect system failures or rate overall performance.

**IP probes**

An attack technique that uses automated tools to ping each address in a range. Systems that respond to the ping request are logged for further analysis. Addresses that do not produce a response are assumed to be unused and are ignored.

**K**

**Kerberos**

A ticket-based authentication mechanism that employs a trusted third party to provide identification and authentication.

**L**

**logging**

The activity of recording information about events or occurrences to a log file or database.

**logic bomb**

Malicious code objects that infect a system and lie dormant until they are triggered by the occurrence of one or more conditions.

**logical access control**

A hardware or software mechanism used to manage access to resources and systems and provide protection for them. They are the same as technical access controls. Examples include encryption, smart cards, passwords, biometrics, constrained interfaces, access control lists, protocols, firewalls, routers, intrusion detection systems, and clipping levels.

**M**

**malicious code**

Code objects that exploit various network, operating system, software, and physical security vulnerabilities to spread malicious payloads to computer systems.

**man-in-the-middle attack**

A type of attack that occurs when malicious users are able to position themselves between the two endpoints of a communication's link. The client and server are unaware that there is a third party intercepting and facilitating their communication session.

**master boot record (MBR)**

The portion of a hard drive or floppy disk that the computer uses to load the operating system during the boot process.

**modulo**

The remainder value left over after a division operation is performed.

**N**

**need-to-know**

The requirement to have access to, knowledge about, or possession of data or a resource in order to perform specific work tasks. A user must have this requirement in order to gain access to data or resources. Even if that user has an equal or greater security classification than the requested information, if they do not have this requirement, they are denied access.

**nondisclosure agreement (NDA)**

A document used to protect the confidential information within an organization from being disclosed by a former employee. When a person signs it, they agree not to disclose any information that is defined as confidential to anyone outside of the organization. Often, violations of this agreement are met with strict penalties.

**nonrepudiation**

A feature of a security control or an application that prevents the sender of a message or the subject of an activity or event from denying that the event occurred.

**NOT**

An operation that reverses the value of an input variable. This function operates on only one variable at a time.

**O**

**object**

A passive entity that provides information or data to subjects. It can be a file, a database, a computer, a program, a process, a file, a printer, a storage media, and so on.

**object-oriented programming (OOP)**

A method of programming that uses encapsulated code sets called objects. It is best suited for eliminating error propagation and mimicking or modeling the real world.

**one-time pad**

An extremely powerful type of substitution cipher that uses a different key for each message. The key length is the same length as the message.

**one-way function**

A mathematical operation that easily produces output values for each possible combination of inputs but makes it impossible to retrieve the input values. Public key cryptosystems are all based on some sort of this operation.

**Open Systems Interconnection (OSI) model**

A standard model developed to establish a common communication structure or standard for all computer systems.

**OR**

An operation that checks to see whether at least one of the input values is true.

**owner**

The person who has final corporate responsibility for the protection and storage of data. They may be liable for negligence if they fail to perform due diligence in establishing and enforcing security policy to protect and sustain sensitive data. They are typically the CEO, president, or department head.

**P**

**packet**

A portion of a message that contains data and the destination address; also called a datagram. Typically located at the Network layer.

**packet sniffing**

The act of capturing packets from the network in hopes of extracting useful information from the packet contents.

**parallel test**

Testing that involves actually relocating personnel to an alternate recovery site and implementing site activation procedures.

**password**

A string of characters entered by a subject as an authentication factor.

**Password Authentication Protocol (PAP)**

A standardized authentication protocol for PPP; transmits usernames and passwords in the clear. It offers no form of encryption; it simply provides a means to transport the logon credentials from the client to the authentication server.

**personally identifiable information (PII)**

Any data item that can be easily and/or obviously traced back to the person of origin or concern.

**phishing**

A form of social engineering that attempts to trick users into giving up sensitive information, opening an attachment, or clicking a link in response to an email. It is sent indiscriminately to a large number of users.

**physical access control**

A physical barrier deployed to prevent direct contact with systems. Examples include guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, swipe cards, dogs, CCTV, mantraps, and alarms.

**ping-of-death attack**

A type of DoS attack that employs an oversized ping packet. Using special tools, an attacker can send numerous oversized ping packets to a victim. In many cases, when the victimized system attempts to process the packets, an error occurs, causing the system to freeze, crash, or reboot.

**Point-to-Point Protocol (PPP)**

A full-duplex protocol used for the transmission of TCP/IP packets over various non-LAN connections, such as modems, ISDN, VPNs, Frame Relay, and so on. It is widely supported and is the transport protocol of choice for dial-up Internet connections.

**polymorphism**

In OOP terminology, the characteristic of an object to provide different behaviors based on the same message and methods owing to variances in external conditions.

**port scan**

Software used by an intruder to probe all of the active systems on a network and determine what public services are running on each machine.

**Pretty Good Privacy (PGP)**

A public/private key system that uses the IDEA algorithm to encrypt files and email messages. It is not a standard but rather an independently developed product that has wide Internet grassroots support.

**principle of least privilege**

An access control philosophy that states that subjects are granted the minimal access possible for the completion of their work tasks.

**private key**

A secret value that is used to encrypt or decrypt messages and is kept secret and known only to the user; used in conjunction with a public key in asymmetrical cryptography.

**protection rings**

A security design that organizes code and components in an operating system into concentric rings, each having increasing or decreasing levels of capabilities and access. Can also apply to applications, utilities, or other code that runs under the operating system's control.

**proximity reader**

A passive device, field-powered device, or transponder that detects the presence of authorized personnel and grants them physical entry into a facility. The proximity device is worn or held by the authorized bearer. When they pass this device, it is able to determine who the bearer is and whether they have authorized access.

**public key**

A value that is used to encrypt or decrypt messages and is made public to any user and used with a private key in asymmetric cryptography.

**public key infrastructure (PKI)**

A hierarchy of trust relationships that makes it possible to facilitate communication between parties previously unknown to each other.

**R**

**rainbow table**

A database of precomputed hashes for guessed passwords. They are used in password attacks, and they can significantly reduce the time it takes to crack the password.

**Redundant Array of Independent Disks (RAID)**

Storage device technology that uses multiple hard drives in unique combinations to produce a storage solution that provides better throughput and resistance to device failure.

**reference monitor**

A portion of the security kernel that validates user requests against the system's access control mechanisms.

**Remote Authentication Dial-In User Service (RADIUS)**

A service used to centralize the authentication of remote dial-up connections.

**remote mirroring**

Maintaining a live database server at the backup site. It is the most advanced database backup solution.

**risk**

The likelihood that any specific threat will exploit a specific vulnerability to cause harm to an asset. It is an assessment of probability, possibility, or chance. It is calculated as threat \* vulnerability.

**risk management**

A detailed process of identifying factors that could damage or disclose data. Evaluating those factors in light of data value and countermeasure cost, and implementing cost-effective solutions for mitigating or reducing risk.

**running key cipher**

A form of cryptography in which the key is a designation of a changing source, such as the third page of the New York Times.

**S**

**security kernel**

The core set of operating system services that handles all user/application requests for access to system resources.

**security perimeter**

The imaginary boundary that separates the trusted computing base from the rest of the system.

**separation of duties and responsibilities**

A common practice to prevent any single subject from being able to circumvent or disable security mechanisms. By dividing core administration or high-authority responsibilities among several subjects, no one subject has sufficient access to perform significant malicious activities or bypass imposed security controls.

**simulation test**

A test in which disaster recovery team members are presented with a scenario and asked to develop an appropriate response. Some of these response measures are then tested. This may involve the interruption of noncritical business activities and the use of some operational personnel.

**smart card**

Credit-card-sized ID, badge, or security pass that has a magnetic strip, bar code, or integrated circuit chip embedded in it. They can contain information about the authorized bearer that can be used for identification and/or authentication purposes.

**smurf attack**

A type of DoS attack that occurs when an amplifying server or network is used to flood a victim with useless data.

**sniffing**

A form of network traffic monitoring that often involves the capture or duplication of network traffic for examination, re-creation, and extraction.

**social engineering**

Skill by which an unauthorized person gains the trust of someone inside your organization and encourages them to make a change to the IT system in order to grant them access.

**split knowledge**

The specific application of the ideas of separation of duties and two-man control into a single solution. The basic idea is that the information or privilege required to perform an operation is divided among multiple users. This ensures that no single person has sufficient privileges to compromise the security of the environment.

**spoofing**

The act of replacing the valid source and/or destination IP address and node numbers with false ones.

**spread spectrum**

A means or method of communication that occurs over multiple frequencies at the same time.

**structured walkthrough**

A type of disaster recovery test, in which members of the disaster recovery team gather in a large conference room and role-play a disaster scenario. Often referred to as a "table-top  
Exercise."

**subject**

An active entity that seeks information about or data from passive objects through the exercise of access. It can be a user, a program, a process, a file, a computer, a database, and so on.

**symmetric key**

An algorithm that relies on a "shared secret" encryption key that is distributed to all members who participate in communications. This key is used by all parties to both encrypt and decrypt messages.

**SYN flood attack**

A type of DoS attack, waged by not sending the final ACK packet, which breaks the standard three-way handshake used by TCP/IP to initiate communication sessions.

**T**

**teardrop attack**

A type of DoS attack that occurs when an attacker exploits a bug in operating systems. The bug exists in the routines used to reassemble fragmented packets. An attacker sends numerous specially formatted fragmented packets to the victim, which causes the system to freeze or crash.

**Terminal Access Controller Access Control System (TACACS)**

An alternative to RADIUS. It integrates the authentication and authorization processes.

**testimonial evidence**

Evidence that consists of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition.

**threat modeling**

The process of identifying, understanding, and categorizing potential threats. It attempts to identify a potential list of threats to valuable assets, along with an analysis of the threat.

**token device**

A password-generating device that subjects must carry with them. They are a form of a "something you have" (Type 2) authentication factor.

**Trojan horse**

A malicious code object that appears to be a benevolent program. The code may appear to be something such as a game or simple utility that performs the "cover" functions as advertised but also carries an unknown payload, such as a virus.

**trusted computing base (TCB)**

The combination of hardware, software, and controls that form a trusted base that enforces your security policy.

**trusted path**

Secure channel used by the TCB to communicate with the rest of the system.

**tunneling**

A network communications process that protects the contents of protocol packets by encapsulating them in packets of another protocol.

**Type 1 authentication factor**

Something you know, such as a password, personal identification number (PIN), combination lock, passphrase, mother's maiden name, or favorite color.

**Type 2 authentication factor**

Something you have, such as a smart card, ATM card, token device, or memory card.

**Type 3 authentication factor**

Something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, or hand geometry.

**U**

**user**

Any person who has access to the secured system. This person's access is tied to their work tasks and is limited so they have only enough access to perform the tasks necessary for their job position (in other words, principle of least privilege). Also referred to as an end user and employee.

**V**

**virtual private network (VPN)**

A network connection established between two systems over an existing private or public network. It provides confidentiality and integrity for network traffic through the use of encryption.

**virus**

The oldest form of malicious code objects that plague cyberspace. Once they are in a system, they attach themselves to legitimate operating system and user files and applications and normally perform some sort of undesirable action, ranging from the somewhat innocuous display of an annoying message on the screen to the more malicious destruction of the entire local filesystem.

**vulnerability analysis**

A process used to identify vulnerabilities, or weaknesses. It can include both technical means, such as vulnerability scans, and nontechnical means, such as an evaluation or inspection of existing data on threats and vulnerabilities.

**vulnerability scan**

A test performed on a system to find weaknesses in the security infrastructure.

**W**

**worm**

A form of malicious code that is self-replicating but is not designed to impose direct harm on host systems. Its primary purpose is to replicate itself to other systems and gather information. They are usually very prolific and often cause a denial of service because of their consumption of system resources and network bandwidth in their attempt to self-replicate.

**X**

**XOR**

A function that returns a true value when only one of the input values is true. If both values are false or both values are true, the output of the function is false.

**Z**

**zero day exploit**

An attack on a system that exploits vulnerabilities that are unknown to others. Typically, it indicates a vulnerability known to one or more attackers isn't known to the vendor. In some cases the vendor may know about the vulnerability but hasn't written or released a patch for the vulnerability yet.