|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 1** |  | | **accounting** | The ability that provides tracking of events. Pg13 | | **asset** | An item that has value. Pg13 | | **authentication** | The steps that ensure that the individual is who they claim to be. Pg13 | | **authorization** | The act of ensuring that an individual or element is genuine. Pg13 | | **availability** | Security actions that ensure that data is accessible to authorized users. Pg12 | | **California's Database Security Breach Notification Act** | The first state law that covers any state agency, person, or company that does business in California. Pg18 | | **confidentiality Security** | Actions that ensure only authorized parties can view the information. Pg12 | | **cybercrime** | Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information. Pg22 | | **cybercriminals** | A network of attackers, identity thieves, spammers, and financial fraudsters. Pg22 | | **cyberterrorism** | A premeditated, politically motivated attack against information, computer systems, computer programs, and data that results in violence. Pg19 | | **cyberterrorists** | Attackers whose motivation may be defined as ideology, or attacking for the sake of their principles or beliefs. Pg23 | | **exploiting** | The act of taking advantage of a vulnerability. Pg16 | | **Gramm-Leach-Bliley Act (GLBA)** | A law that requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information. Pg18 | | **hacker** | A term used to refer to a person who uses advanced computer skills to attack computers. Pg20 | | **Health Insurance Portability and Accountability Act (HIPAA)** | A law designed to guard protected health information and implement policies and procedures to safeguard it. Pg18 | | **identity theft** | Stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain. Pg17 | | **information security** | The tasks of securing information that is in a digital format. Pg12 | | **integrity Security** | Actions that ensure that the information is correct and no unauthorized person or malicious software has altered the data. Pg12 | | **risk** | The likelihood that a threat agent will exploit the vulnerability. Pg16 | | **Sarbanes-Oxley Act (Sarbox)** | A law designed to fight corporate corruption. Pg18 | | **script kiddies** | Individuals who want to break into computers to create damage, yet lack the advanced knowledge of computers and networks needed to do so. Pg20 | | **spy** | A person who has been hired to break into a computer and steal information. Pg20 | | **threat** | A type of action that has the potential to cause harm. Pg15 | | **threat agent** | A person or element that has the power to carry out a threat. Pg16 | | **vulnerability** | A flaw or weakness that allows a threat agent to bypass security. Pg16 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 2** |  | | **adware** | A software program that delivers advertising content in a manner that is unexpected and unwanted by the user. Pg55 | | **backdoor** | Software code that gives access to a program or a service that circumvents normal security protections. Pg52 | | **botnet** | A logical computer network of zombies under the control of an attacker. Pgs52-54 | | **computer virus (virus)** | A malicious computer code that, like its biological counterpart, reproduces itself on the same computer. Pgs43-47 | | **dumpster diving** | The act of digging through trash receptacles to find information that can be useful in an attack. Pgs64,65 | | **hoax** | A false warning. Pg63 | | **impersonation** | An attack that creates a fictitious character and then plays out the role of that person on a victim. Pgs58-59 | | **keylogger** | Captures and stores each keystroke that a user types on the computer's keyboard. Pg56 | | **logic bomb** | Computer code that lies dormant until it is triggered by a specific logical event. Pgs51-52 | | **malware** | Software that enters a computer system without the user's knowledge or consent and then performs an unwanted-and usually harmful-action. Pgs43-57 | | **pharming** | A phishing attack that automatically redirects the user to a fake site. Pg59 | | **phishing** | Sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information. Pg59-62 | | **rootkit** | A set of software tools used by an attacker to hide the actions or presence of other types of malicious software. Pgs49-51 | | **shoulder surfing** | Watching an authorized user enter a security code on a keypad. Pg66 | | **social engineering** | A means of gathering information for an attack by relying on the weaknesses of individuals.  Pgs57-66 | | **spam** | Unsolicited e-mail. Pgs62-63 | | **spear phishing** | A phishing attack that targets only specific users. Pg59 | | **spim** | A variation of spam, which targets instant messaging users instead of e-mail users. Pg62 | | **spyware** | A general term used to describe software that spies on users by gathering information without consent, thus violating their privacy. Pgs54-55 | | **tailgating** | The act of unauthorized individuals entering a restricted-access building by following an authorized user. Pg64,66 | | **Trojan horse (Trojan)** | An executable program advertised as performing one activity, but actually does something else (or it may perform both the advertised and malicious activities). Pg49 | | **vishing** | A phishing attack that uses a telephone call instead of using e-mail. Pg60 | | **whaling** | A phishing attack that targets only wealthy individuals. Pg59 | | **word splitting** | Horizontally separating words so that they can still be read by the human eye. Pg63 | | **worm** | A malicious program designed to take advantage of a vulnerability in an application or an operating system in order to enter a computer and then self-replicate to other computers. Pg48 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 3** |  | | **add-ons** | Programs that provide additional functionality to Web browsers. Pgs95-96 | | **Address Resolution Protocol (ARP)** | Part of the TCP/IP protocol for determining the MAC address based on the IP address. Pgs100-101 | | **ARP poisoning** | An attack that corrupts the ARP cache. Pgs100-102 | | **attachments** | Files that are coupled to e-mail messages. Pg94 | | **buffer overflow** | An attack that occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer. Pgs96-97 | | **client-side attack** | An attack that targets vulnerabilities in client applications that interact with a compromised server or processes malicious data. Pgs91-97 | | **command injection /directory traversal** | Injecting and executing commands to execute on a server. Pg90 | | **cookie** | A file on a local computer in which a server stores user-specific information. Pgs93-94 | | **cross-site scripting (XSS)** | Application server to direct attacks at clients. Pgs85-87 | | **denial of service (DoS)** | An attack that attempts to prevent a system from performing its normal functions. Pgs97-98 | | **directory traversal /command injection** | An attack that takes advantage of a vulnerability in the Web application program or the Web server software so that a user can move from the root directory to other restricted directories. Pg90 | | **distributed denial of service (DDoS)** | An attack that uses multiple zombie computers (even hundreds or thousands) in a botnet to flood a device with requests. Pg98 | | **DNS poisoning** | An attack that substitutes DNS addresses so that the computer is automatically redirected to another device. Pgs102-104 | | **Domain Name System (DNS)** | A hierarchical name system for matching computer names and numbers. Pgs102-103 | | **first-party cookie** | A cookie that is created from the Web site that currently is being viewed. Pg93 | | **Flash cookie** | A cookie named after the Adobe Flash player. Also known as local shared objects (LSOs). Flash cookies cannot be deleted through the browser's normal configuration settings as regular cookies can. Typically, they are saved in multiple locations on the hard drive and can be take up as much as 100,000 bytes of storage per cookie (about 25 times the size of a normal cookie). Flash cookies can also be used to reinstate regular cookies that a user has deleted or blocked. Pg93 | | **host table** | A list of the mappings of names to computer numbers. Pg102 | | **HTTP header** | Part of HTTP that is composed of fields that contain the different characteristics of the data that is being transmitted. Pgs91-92 | | **HTTP header manipulation** | Modifying HTTP headers to create an attack. Pgs91-92 | | **man-in-the-middle** | An attack that intercepts legitimate communication and forges a fictitious response to the sender. Pgs98-100 | | **persistent cookie (tracking cookie)** | A cookie that is recorded on the hard drive of the computer and does not expire when the browser closes. Pg93 | | **ping** | A utility that sends an ICMP echo request message to a host. Pg97 | | **ping flood** | An attack that uses the Internet Control Message Protocol (ICMP) to flood a victim with packets. Pg97 | | **privilege escalation** | An attack that exploits a vulnerability in software to gain access to resources that the user would normally be restricted from obtaining. Pg104 | | **replay** | An attack that makes a copy of the transmission before sending it to the recipient. Pg100 | | **secure cookie** | A cookie that is only used when a browser is visiting a server using a secure connection. Pg93 | | **session cookie** | A cookie that is stored in Random Access Memory (RAM), instead of on the hard drive, and only lasts for the duration of visiting a Web site. Pg93 | | **session hijacking** | An attack in which an attacker attempts to impersonate the user by using his session token. Pgs94-95 | | **session token** | A form of verification used when accessing a secure Web application. Pg94 | | **smurf attack** | An attack that broadcasts a ping request to all computers on the network yet changes the address from which the request came to that of the target. Pg98 | | **spoofing** | Impersonating another computer or device. Pg98 | | **SQL injection** | An attack that targets SQL servers by injecting commands to be manipulated by the database. Pgs87-89 | | **SYN flood attack** | An attack that takes advantage of the procedures for initiating a TCP session. Pg98 | | **third-party cookies** | A cookie that was created by a third party that is different from the primary Web site. Pg93 | | **transitive access** | An attack involving using a third party to gain access rights. Pg105 | | **XML** | (Extensible Markup Language) A markup language that is designed to carry data instead of indicating how to display it. Pgs89-90 | | **XML injection** | An attack that injects XLM tags and data into a database. Pgs89-90 | | **zero day attacks** | Attacks that exploit previously unknown vulnerabilities, so victims have no time (zero days) to prepare or defend against the attacks. Pg83 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 4** |  | | **Annualized Loss Expectancy (ALE)** | The expected monetary loss that can be expected for an asset due to a risk over a one-year period. Pgs129-130 | | **Annualized Rate of Occurrence (ARO)** | The probability that a risk will occur in a particular year. Pgs129-130 | | **architectural design** | The process of defining a collection of hardware and software components along with their interfaces in order to create the framework for software development. Pg132 | | **attack surface** | The code that can be executed by unauthorized users in a software program. Pg133 | | **baseline reporting** | A comparison of the present state of a system compared to its baseline. Pgs131-132 | | **black box infrastructure** | A test in which the tester has no prior knowledge of the network that is being tested. Pg142 | | **code review** | Presenting the code to multiple reviewers in order to reach agreement about its security. Pg133 | | **design review** | An analysis of the design of a software program by key personnel from different levels of the project. Pg132 | | **Exposure Factor (EF)** | The proportion of an asset's value that is likely to be destroyed by a particular risk (expressed as a percentage). Pg129 | | **fail-open** | A control that errs on the side of permissiveness in the event of a failure. Pgs143-144 | | **fail-safe (fail-secure)** | A control that errs on the side of security in the event of a failure. Pgs143-144 | | **gray box** | A test where some limited information has been provided to the tester. Pg142 | | **hardening** | The process of eliminating as many security risks as possible and making the system more secure. Pg144 | | **honeynet** | A network set up with intentional vulnerabilities. Pgs139-140 | | **honeypot** | A computer typically located in an area with limited security and loaded with software and data files that appear to be authentic, yet they are actually imitations of real data files, to trick attackers into revealing their attack techniques. Pgs139-140 | | **penetration testing** | A test by an outsider to actually exploit any weaknesses in systems that are vulnerable. Pg141 | | **port scanner** | Software to search a system for any port vulnerabilities. Pgs134-135 | | **protocol analyzer (sniffer)** | Hardware or software that captures packets to decode and analyze the contents. Pgs135-137 | | **Single Loss Expectancy (SLE)** | The expected monetary loss every time a risk occurs. Pgs129-130 | | **vulnerability assessment** | A systematic and methodical evaluation of the exposure of assets to attackers, forces of nature, or any other entity that is a potential harm. Pg125, 125-140 | | **vulnerability scan** | An automated software search through a system for any known security weaknesses that then creates a report of those potential exposures. Pg140-141 | | **vulnerability scanner** | Generic term for a range of products that look for vulnerabilities in networks or systems. Pgs137-139 | | **white box** | A test where the tester has an in-depth knowledge of the network and systems being tested, including network diagrams, IP addresses, and even the source code of custom applications. Pg142 | | **Xmas Tree port scan** | Sending a packet with every option set on for whatever protocol is in use to observe how a host responds. Pg136 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 5** |  | | **access list** | A record or list of individuals who have permission to enter a secure area, the time that they entered, and the time they left the area. Pg167 | | **access log** | A log that can provide details regarding requests for specific files on a system. Pg178 | | **anti-spyware** | Software that helps prevent computers from becoming infected by different types of spyware. Pg177 | | **anti-virus (AV)** | Software that can examine a computer for any infections as well as monitor computer activity and scan new documents that might contain a virus. Pg175-178 | | **audit log** | A log that can track user authentication attempts. Pg178 | | **audit records** | Logs that are the second common type of security-related operating system logs. Pg179 | | **Bayesian filtering** | Spam filtering software that analyzes the contents of every word in an email and determines how frequently a word occurs in order to determine if it is spam. Pg176-177 | | **cable lock** | A device that can be inserted into the security slot of a portable device and rotated so that the cable lock is secured to the device to prevent it from being stolen. Pg168-169 | | **closed-circuit television (CCTV)** | Using video cameras to transmit a signal to a specific and limited set of receivers used for surveillance in areas that require security monitoring. Pg167 | | **cross-site request forgery (XSRF)** | An attack that uses the user's Web browser settings to impersonate the user. Pg183 | | **data loss prevention (DLP)** | A system that can identify critical data, monitor how it is being accessed, and protect it from unauthorized users. Pg185-186 | | **deadbolt lock** | A door lock that extends a solid metal bar into the door frame for extra security. Pg163-165 | | **errors (exceptions)** | Faults in a program that occur while the application is running. Pg182-183 | | **event logs** | Logs that can document any unsuccessful events and the most significant successful events. Pg178-179 | | **fencing** | Securing a restricted area by erecting a barrier. Pg168-169 | | **firewall (packet filter)** | Hardware or software that is designed to prevent malicious packets from entering or leaving computers. Pg177-178 | | **fuzz testing (fuzzing)** | A software testing technique that deliberately provides invalid, unexpected, or random data as inputs to a computer program. Pg183 | | **GPS tracking** | Using the Global Positioning System (GPS) to detect the location of a portable device. Pg170 | | **heuristic detection** | Creating a virtualized environment to simulate the central processing unit (CPU) and memory of the computer to check for the presence of a virus. Pg176 | | **host-based software firewall** | A firewall that runs as a program on a local system to protect it against attacks. Pg177-178 | | **hotfix** | Software that addresses a specific customer situation and often may not be distributed outside that customer's organization. Pg173 | | **input validation** | Verifying a user's input to an application. Pg183 | | **locking cabinet** | A secure storage unit that can be used for storing portable devices. Pg170 | | **log** | A record of events that occur. Pg178-181 | | **mantrap** | A device that monitors and controls two interlocking doors to a small room (a vestibule), designed to separate secure and nonsecure areas. Pg167-168 | | **patch** | A general software security update intended to cover vulnerabilities that have been discovered. Pg172-175 | | **pop-up blocker** | Either a program or a feature incorporated within a browser that stops pop-up advertisements from appearing. Pg177 | | **proximity reader** | A device that detects an emitted signal in order to identify the owner. Pg166-167 | | **remote wipe/sanitation** | A technology that can remotely erase data from a portable device and reset it to its default factory settings. Pg170 | | **safe** | A ruggedized steel box with a lock. Pg170 | | **security logs** | Logs that are considered the primary source of log data. Pg178 | | **security policy** | A document or series of documents that clearly defines the defense mechanisms an organization will employ to keep information secure. Pg171 & Chapter 14 | | **service pack** | Software that is a cumulative package of all security updates plus additional features. Pg173 | | **signature file** | A sequence of bytes (a string) found in the virus as a virus signature. Pg176 | | **voice encryption** | Using encryption to mask the content of voice communications. Pg171 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 6** |  | | **all-in-one network security appliance** | Network hardware that provides multiple security functions. Pg224 | | **anomaly-based monitoring** | A monitoring technique used by an IDS that creates a baseline of normal activities and compares actions against the baseline. Whenever a significant deviation from this baseline occurs, an alarm is raised. Pg221 | | **behavior-based monitoring** | A monitoring technique used by an IDS that uses the normal processes and actions as the standard and compares actions against it. Pgs221-222 | | **demilitarized zone (DMZ)** | A separate network that rests outside the secure network perimeter; untrusted outside users can access the DMZ but cannot enter the secure network. Pg228 | | **heuristic monitoring** | A monitoring technique used by an IDS that uses an algorithm to determine if a threat exists. Pg222 | | **host intrusion detection system (HIDS)** | A software-based application that runs on a local host computer that can detect an attack as it occurs. Pgs222-223 | | **intrusion detection system (IDS)** | A device designed to be active security; it can detect an attack as it occurs. Pgs220-224 | | **load balancer** | A device that can direct requests to different servers based on a variety of factors, such as the number of server connections, the server's processor utilization, and overall performance of the server. Pg212 | | **network access control (NAC)** | A technique that examines the current state of a system or network device before it is allowed to connect to the network. Pgs226-227 | | **network address translation (NAT)** | A technique that allows private IP addresses to be used on the public Internet. Pgs224-226 | | **network intrusion detection system (NIDS)** | A technology that watches for attacks on the network and reports back to a central device. Pgs223-224 | | **network intrusion prevention system (NIPS)** | A technology that monitors network traffic to immediately react to block a malicious attack. Pg224 | | **proxy server** | A computer or an application program that intercepts a user request from the internal secure network and then processes that request on behalf of the user. Pgs214-216 | | **remote access** | Any combination of hardware and software that enables remote users to access a local internal network. Pgs219, 232 | | **reverse proxy** | A computer or an application program that routes incoming requests to the correct server. Pgs216-217 | | **router** | A device that can forward packets across computer networks. Pg211 | | **signature-based monitoring** | A monitoring technique used by an IDS that examines network traffic to look for well-known patterns and compares the activities against a predefined signature. Pgs221-222 | | **subnetting (subnet addressing)** | A technique that uses IP addresses to divide a network into network, subnet, and host. Pgs228-231 | | **switch** | A device that connects network segments and forwards only frames intended for that specific device or frames sent to all devices. Pgs209-211 | | **virtual LAN (VLAN)** | A technology that allows scattered users to be logically grouped together even though they may be attached to different switches. Pgs231-232 | | **virtual private network (VPN)** | A technology to use an unsecured public network, such as the Internet, like a secure private network. Pg219 | | **VPN concentrator** | A device that aggregates hundreds or thousands of VPN connections. Pg219 | | **Web application firewall** | A special type of firewall that looks more deeply into packets that carry HTTP traffic. Pg214 | | **Web security gateway** | A device that can block malicious content in "real time" as it appears (without first knowing the URL of a dangerous site). Pg220 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 7** |  | | **cloud computing** | A pay-per-use computing model in which customers pay only for the computing resources that they need, and the resources can be easily scaled. Pgs273-275 | | **disabling unused ports** | A security technique to turn off ports on a network device that are not required. Pgs268 | | **File Transfer Protocol (FTP)** | An unsecure TCP/IP protocol that is commonly used for transferring files. Pgs256-258 | | **flood guard** | A feature that controls a device's tolerance for unanswered service requests and helps to prevent a DoS attack. Pgs262-263 | | **FTP using Secure Sockets Layer (FTPS)** | A TCP/IP protocol that uses Secure Sockets Layer/Transport Layer Security (SSL/TLS) to encrypt commands sent over the control port (Port 21) in an FTP session. Pgs258 | | **IEEE 802.1x** | A standard that blocks all traffic on a port-by-port basis until the client is authenticated using credentials stored on an authentication server. Pgs268-269 | | **Internet Control Message Protocol (ICMP)** | A TCP/IP protocol that is used by devices to communicate updates or error information to other devices. Pgs252-254 | | **Internet Protocol version 6 (IPv6)** | The next generation of the IP protocol that addresses weaknesses of IPv4 and provides several significant improvements. Pgs259-260 | | **IP telephony** | Using a data-based IP network to add digital voice clients and new voice applications onto the IP network. Pgs272-273 | | **loop protection** | Preventing broadcast storms by using the IEEE 802.1d standard spanningtree algorithm (STA). Pgs266-267 | | **MAC limiting and filtering** | A security technique to limit the number of media access control (MAC) addresses allowed on a single port. Pgs268 | | **rule-based management** | The process of administration that relies on following procedural and technical rules. Pgs260-261 | | **Secure Copy Protocol (SCP)** | A TCP/IP protocol used mainly on UNIX and Linux devices that securely transports files by encrypting files and commands. Pgs258 | | **Secure FTP (SFTP)** | A secure TCP/IP protocol that is used for transporting files by encrypting and compressing all data and commands. Pgs258 | | **Simple Network Management Protocol (SNMP)** | A TCP/IP protocol that exchanges management information between networked devices. It allows network administrators to remotely monitor, manage, and configure devices on the network. Pgs252-254 | | **Transmission Control Protocol/Internet Protocol (TCP/IP)** | The most common protocol suite used today for local area networks (LANs) and the Internet. Pgs251-252 | | **virtualization** | A means of managing and presenting computer resources by function without regard to their physical layout or location. Pgs269-272 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 8** |  | | **AES-CCMP** | The encryption protocol standard for WPA2. Pg310 | | **bluejacking** | An attack that sends unsolicited messages to Bluetooth-enabled devices. Pg295 | | **bluesnarfing** | An attack that accesses unauthorized information from a wireless device through a Bluetooth connection, often between cell phones and laptop computers. Pg296 | | **Bluetooth** | A wireless technology that uses short-range radio frequency (RF) transmissions and provides for rapid ad hoc device pairings. Pgs293-295 | | **evil twin** | An AP set up by an attacker to mimic an authorized AP and capture transmissions, so a user's device will unknowingly connect to this evil twin instead. Pgs301-302 | | **Extensible Authentication Protocol (EAP)** | A framework for transporting authentication protocols that defines the format of the messages. Pgs311-312 | | **initialization vector (IV)** | A 24-bit value used in WEP that changes each time a packet is encrypted. Pg305 | | **keystream attack (IV attack)** | A method of determining the keystream by analyzing two packets that were created from the same initialization vector (IV). Pgs306-307 | | **Lightweight EAP (LEAP)** | A proprietary EAP method developed by Cisco Systems requiring mutual authentication used for WLAN encryption using Cisco client software. Pgs311-312 | | **Media Access Control (MAC) address filtering** | A method for controlling access to a WLAN based on the device's MAC address. Pgs302-303 | | **preshared key (PSK)** | A key value that must be created and entered into both the access point and all wireless devices ("shared") prior to ("pre") the devices communicating with the AP. Pgs309-312 | | **Protected EAP (PEAP)** | An EAP method designed to simplify the deployment of 802.1x by using Microsoft Windows logins and passwords. Pgs311-312 | | **rogue access point** | An unauthorized AP that allows an attacker to bypass many of the network security configurations and opens the network and its users to attacks. Pgs301, 312-313 | | **Service Set Identifier (SSID)** | The user-supplied network name of a WLAN; it can generally be alphanumeric from 2 to 32 characters. Pgs303-304 | | **SSID broadcast** | The transmission of the SSID from the access point to wireless devices. Pgs303-304 | | **Temporal Key Integrity Protocol (TKIP)** | A WPA encryption technology. Pg308 | | **war chalking** | The process of documenting and then advertising the location of wireless LANs for others to use. Wireless networks were identified by drawing on sidewalks or walls around the area of the network. Pg299 | | **war driving** | Searching for wireless signals from an automobile or on foot using a portable computing device. Pg298-299 | | **Wi-Fi Protected Access (WPA)** | The original set of protections from the Wi-Fi Alliance in 2003 designed to protect both present and future wireless devices. Pgs308-309 | | **Wi-Fi Protected Access 2 (WPA2)** | The second generation of WPA security from the Wi-Fi Alliance in 2004 to address authentication and encryption on WLANs. Pgs310-311 | | **Wired Equivalent Privacy (WEP)** | An IEEE 802.11 security protocol designed to ensure that only authorized parties can view transmitted wireless information. WEP has significant vulnerabilities and is not considered secure. Pgs305-307 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 9** |  | | **access control** | The mechanism used in an information system to allow or restrict access to data or devices. Pgs334-344 | | **access control list (ACL)** | A set of permissions that are attached to an object. Pgs344-345 | | **access control model** | A standard that provides a predefined framework for hardware and software developers who need to implement access control in their devices or applications. Pgs336-341 | | **account expiration** | The process of setting a user's account to expire. Pgs346-348 | | **Discretionary Access Control (DAC)** | The least restrictive access control model in which the owner of the object has total control over it. Pgs338-340 | | **Extended TACACS** | The second version of the Terminal Access Control Access Control System (TACACS) authentication service. Pg351 | | **implicit deny** | Rejecting access unless a condition is explicitly met. Pg343 | | **job rotation** | The act of moving individuals from one job responsibility to another. Pg342 | | **Kerberos** | An authentication system developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of networked users. Pgs350-351 | | **LDAP injection attack** | An attack that constructs LDAP statements based on user input statements, allowing the attacker to retrieve information from the LDAP database or modify its content. Pg353 | | **least privilege** | Providing only the minimum amount of privileges necessary to perform a job or function. Pgs342-343 | | **Lightweight Directory Access Protocol (LDAP)** | A protocol for a client application to access an X.500 directory. Pgs352-353 | | **Mandatory Access Control (MAC)** | The most restrictive access control model, typically found in military settings in which security is of supreme importance. Pgs337-338 | | **mandatory vacations** | Requiring that all employees take vacations. Pg344 | | **Remote Authentication Dial In User Service (RADIUS)** | An industry standard authentication service with widespread support across nearly all vendors of networking equipment. Pgs348-350, 352 | | **Role Based Access Control (RBAC)** | A "real-world" access control model in which access is based on a user's job function within the organization. Pgs340-341 | | **Rule Based Access Control (RBAC)** | An access control model that can dynamically assign roles to subjects based on a set of rules defined by a custodian. Pgs340-341 | | **separation of duties** | The practice of requiring that processes should be divided between two or more individuals. Pg341 | | **TACACS+** | The current version of the Terminal Access Control Access Control System (TACACS) authentication service. Pgs351-352 | | **Terminal Access Control Access Control System (TACACS)** | An authentication service commonly used on UNIX devices that communicates by forwarding user authentication information to a centralized server. The current version is TACACS+. Pgs351-352 | | **time of day restrictions** | Limitations imposed as to when a user can log on to a system. Pgs346-347 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 10** |  | | **behavioral biometrics** | Authenticating a user by the normal actions that the user performs. Pgs379-381 | | **brute force attack** | A password attack in which every possible combination of letters, numbers, and characters is used to create encrypted passwords that are matched with those in a stolen password file. Pg370 | | **cognitive biometrics** | Authenticating a user through the perception, thought process, and understanding of the user. Pgs381-382 | | **common access card (CAC)** | A Department of Defense (DoD) smart card used for identification for active-duty and reserve military personnel along with civilian employees and special contractors. Pg378 | | **dictionary attack** | A password attack that creates encrypted versions of common dictionary words and compares them against those in a stolen password file. Pgs370-371 | | **hybrid attack** | A password attack that slightly alters dictionary words by adding numbers to the end of the password, spelling words backward, slightly misspelling words, or including special characters. Pg371 | | **multifactor authentication** | Using more than one type of authentication credential. Pg377 | | **password** | A secret combination of letters, numbers, and/or characters that only the user should know. Pgs368-375 | | **Personal Identity Verification (PIV)** | A government standard for smart cards that covers all government employees. Pg378 | | **rainbow tables** | Large pregenerated data sets of encrypted passwords used in password attacks. Pg371 | | **single sign-on (SSO)** | Using one authentication credential to access multiple accounts or applications. Pgs382-385 | | **single-factor authentication** | Using one type of authentication credentials. Pg377 | | **smart card** | A card that contains an integrated circuit chip that can hold information used as part of the authentication process. Pgs377-378 | | **standard biometrics** | Using fingerprints or other unique physical characteristics of a person's face, hands, or eyes for authentication. Pgs378-379 | | **token** | A small device that can be affixed to a keychain with a window display that shows a code to be used for authentication. Pgs375-377 | | **trusted operating system (trusted OS)** | A hardened operating system that can keep attackers from accessing and controlling critical parts of a computer system. Pgs387-388 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 11** |  | | **Advanced Encryption Standard (AES)** | A symmetric cipher that was approved by the NIST in late 2000 as a replacement for DES. – Pg422 | | **algorithm** | Procedures based on a mathematical formula; used to encrypt data. – Pgs408,411-429 | | **asymmetric cryptographic algorithm** | Encryption that uses two mathematically related keys. – Pgs423-429 | | **block cipher** | A cipher that manipulates an entire block of plaintext at one time. – Pgs420-423 | | **Blowfish** | A block cipher that operates on 64-bit blocks and can have a key length from 32 to 448 bits. – Pg423 | | **ciphertext** | Data that has been encrypted. – Pgs408-409 | | **cleartext** | Unencrypted data. – Pgs408-409 | | **cryptography** | The science of transforming information into a secure form while it is being transmitted or stored so that unauthorized persons cannot access it. – Pgs407-411 | | **Data Encryption Standard (DES)** | A symmetric block cipher that uses a 56-bit key and encrypts data in 64-bit blocks. – Pgs420-422 | | **decryption** | The process of changing ciphertext into plaintext. – Pg408 | | **digital signature** | An electronic verification of the sender. – Pgs424-426 | | **elliptic curve cryptography (ECC)** | An algorithm that uses elliptic curves instead of prime numbers to compute keys. – Pgs427-428 | | **encryption** | The process of changing plaintext into ciphertext. – Pg408 | | **GNU Privacy Guard (GPG)** | Free and open-source software that is commonly used to encrypt and decrypt e-mail messages. – Pg430 | | **Hardware Security Module (HSM)** | A secure cryptographic processor. – Pg433 | | **hash** | The unique digital fingerprint created by a hashing algorithm. – Pgs411-416 | | **Hashed Message** | Authentication Code (HMAC) A variation of a hash that encrypts the hash with a shared secret key before transmitting it. – Pg413 | | **hashing** | The process for creating a unique digital fingerprint signature for a set of data. – Pgs411-416 | | **key** | A mathematical value entered into the algorithm to produce ciphertext. – Pg408 | | **Message Digest (MD)** | A common hash algorithm of several different versions. – Pgs414-415 | | **Message Digest 5 (MD5)** | A revision of MD4 that is designed to address its weaknesses. – Pgs414-416 | | **nonrepudiation** | The process of proving that a user performed an action. – Pg410 | | **NTLM (New Technology LAN Manager) hash** | A password hash for Microsoft Windows systems that is no longer recommended for use. – Pg416 | | **NTLMv2 (New Technology LAN Manager Version 2) hash** | An updated version of NTLM that uses HMAC with MD5. – Pg416 | | **one-time pad (OTP)** | Using a unique truly random key to create ciphertext. – Pgs419-420 | | **plaintext** | Data input into an encryption algorithm. – Pgs408-409 | | **Pretty Good Privacy (PGP)** | A commercial product that is commonly used to encrypt e-mail messages. – Pg430 | | **private key** | An asymmetric encryption key that does have to be protected. – Pgs423-426 | | **private key cryptography** | Cryptographic algorithms that use a single key to encrypt and decrypt a message. – Pg415 | | **public key** | An asymmetric encryption key that does not have to be protected. – Pgs423-426 | | **public key cryptography** | Encryption that uses two mathematically related keys. – Pgs423-429 | | **quantum cryptography** | An asymmetric cryptography that attempts to use the unusual and unique behavior of microscopic objects to enable users to securely develop and share keys. – Pgs428-429 | | **RACE Integrity Primitives Evaluation Message Digest (RIPEMD)** | A hash algorithm that uses two different and independent parallel chains of computation and then combines the result at the end of the process. – Pgs415-416 | | **RC4** | An RC stream cipher that will accept keys up to 128 bits in length. – Pg422 | | **Rivest Cipher (RC)** | A family of cipher algorithms designed by Ron Rivest. – Pg422 | | **RSA** | An asymmetric algorithm published in 1977 and patented by MIT in 1983. – Pg427 | | **Secure Hash Algorithm (SHA)** | A secure hash algorithm that creates hash values of longer lengths than Message Digest (MD) algorithms. – Pg415 | | **steganography** | Hiding the existence of data within a text, audio, image, or video file. – Pg407 | | **stream cipher** | An algorithm that takes one character and replaces it with one character. – Pgs417-418 | | **symmetric cryptographic algorithm** | Encryption that uses a single key to encrypt and decrypt a message. – Pgs417-423 | | **Triple Data Encryption Standard (3DES)** | A symmetric cipher that was designed to replace DES. – Pgs421-422 | | **Trusted Platform Module (TPM)** | A chip on the motherboard of the computer that provides cryptographic services. – Pgs432-433 | | **Twofish** | A later derivation of the Blowfish algorithm that is considered to be strong. – Pg423 | | **whole disk encryption** | Cryptography that can be applied to entire disks. – Pg431 | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | | **Glossary** |  | | | | **Chapter 12** |  | | | | **bridge trust model** | A trust model with one CA that acts as a facilitator to interconnect all other CAs. – Pgs465-468 | | | | **Certificate Authority (CA)** | A trusted third-party agency that is responsible for issuing the digital certificates. – Pg454 | | | | **Certificate Repository (CR)** | A publicly accessible centralized directory that contains digital certificates that can be used to view the status of a digital certificate. – Pg456 | | | | **Certificate Revocation List (CRL)** | A repository that lists revoked digital certificates. – Pgs455-456 | | | | **digital certificate** | A technology used to associate a user's identity to a public key, in which the user's public key is "digitally signed" by a trusted third party. – Pg453 | | | | **direct trust** | A type of trust model in which a relationship exists between two individuals because one person knows the other person. – Pg465 | | | | **distributed trust model** | A trust model that has multiple CAs that sign digital certificates. – Pgs465-466 | | | | **hierarchical trust model** | A trust model that has a single hierarchy with one master CA. – Pgs465-466 | | | | **Hypertext Transport Protocol over Secure Sockets Layer (HTTPS)** | | | A secure version of HTTP sent over SSL/TLS. – Pg473 | | **IP security (IPsec)** | A set of protocols developed to support the secure exchange of packets. – Pgs473-475 | | | | **key escrow** | A process in which keys are managed by a third party, such as a trusted CA called the root. – Pg470 | | | | **key recovery agent (KRA)** | A highly trusted person responsible for recovering lost or damaged digital certificates. – Pg470 | | | | **M-of-N control** | A technique to recover a private key by distributing parts to different individuals. – Pgs470-471 | | | | **public key infrastructure (PKI)** | | A framework for all of the entities involved in digital certificates for digital certificate management. – Pgs462-469 | | | **Registration Authority (RA)** | A subordinate entity designed to handle specific CA tasks such as processing certificate requests and authenticating users. – Pgs454-459 | | | | **Secure Shell (SSH)** | A UNIX-based command interface and protocol for securely accessing a remote computer. – Pgs472-473 | | | | **Secure Sockets Layer (SSL)** | A protocol developed by Netscape for securely transmitting documents over the Internet that uses a private key to encrypt data. – Pgs472-473 | | | | **third-party trust** | A trust model in which two individuals trust each other because each individually trusts a third party. – Pg465 | | | | **Transport Layer Security (TLS)** | A protocol that is an extension of SSL and guarantees privacy and data integrity between applications. – Pgs472-473 | | | | **trust model** | The type of trusting relationship that can exist between individuals or entities. – Pgs465-468 | | | | **X.509** | The most widely accepted format for digital certificates as defined by the International Telecommunication Union (ITU). – Pgs461-462 | | | | http://www.cengage.com/images/spacer_tr.gif | |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 13** |  | | **asymmetric server cluster** | A technology in which a standby server exists only to take over for another server in the event of its failure. | | **backout/contingency option** | Rolling back a disaster recovery implementation to the starting point so that a different approach can be taken. | | **business continuity** | The ability of an organization to maintain its operations and services in the face of a disruptive event. | | **business continuity planning and testing** | The process of identifying exposure to threats, creating preventive and recovery procedures, and then testing them to determine if they are sufficient. | | **business impact analysis (BIA)** | An analysis of the most important mission-critical business functions, which identifies and quantifies the impact such a loss of the functions may have on the organization in terms of its operational and financial position. | | **chain of custody** | A process of documentation that shows that the evidence was under strict control at all times and no unauthorized individuals were given the opportunity to corrupt the evidence. | | **cold site** | A remote site that provides office space; the customer must provide and install all the equipment needed to continue operations. | | **computer forensics** | Using technology to search for computer evidence of a crime. | | **data backups** | The process of copying information to a different medium and storing it (preferably at an off-site location) so that it can be used in the event of a disaster. | | **disaster recovery** | The procedures and processes for restoring an organization's IT operations following a disaster. | | **disaster recovery plan (DRP)** | A written document that details the process for restoring IT resources following an event that causes a significant disruption in service. | | **Faraday cage** | A metallic enclosure that prevents the entry or escape of an electromagnetic field. | | **forensics (forensic science)** | The application of science to questions that are of interest to the legal profession. | | **heating, ventilation, and air conditioning (HVAC)** | Systems that provide and regulate heating and cooling. | | **high availability** | A system that can function for an extended period of time with little downtime. | | **hot aisle/cold aisle** | A layout in a data center that can be used to reduce heat by managing the air flow. | | **hot site** | A duplicate of the production site that has all the equipment needed for an organization to continue running, including office space and furniture, telephone jacks, computer equipment, and a live telecommunications link. | | **mean time between failures (MTBF)** | A statistical value that is the average time until a component fails, cannot be repaired, and must be replaced. | | **mean time to restore (MTTR)** | The average time needed to reestablish services to their former state. | | **order of volatility** | The sequence of volatile data that must be preserved in a computer forensic investigation. | | **RAID (Redundant Array of Independent Drives)** | A technology that uses multiple hard disk drives for increased reliability and performance. | | **recovery point objective (RPO)** | The maximum length of time that an organization can tolerate between backups. | | **recovery time objective (RTO)** | The length of time it will take to recover the data that has been backed up. | | **server cluster** | A combination (clustering) of two or more servers that are interconnected to appear as one. | | **single point of failure** | A component or entity in a system which, if it no longer functions, would adversely affect the entire system. | | **succession planning** | Determining in advance who will be authorized to take over in the event of the incapacitation or death of key employees. | | **symmetric server cluster** | A technology in which every server in the cluster performs useful work and if one server fails, the remaining servers continue to perform their normal work as well as that of the failed server. | | **system image** | A snapshot of the current state of the computer that contains all settings and data. | | **warm site** | A remote site that contains computer equipment but does not have active Internet or telecommunication facilities, and does not have backups of data. | | http://www.cengage.com/images/spacer_tr.gif | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Glossary** |  | | **Chapter 14** |  | | **acceptable use policy (AUP)** | A policy that defines the actions users may perform while accessing systems and networking equipment. | | **change management** | A methodology for making modifications to a system and keeping track of those changes. | | **incident management** | The "framework" and functions required to enable incident response and incident handling within an organization. | | **peer-to-peer (P2P) network** | A network that does not have servers, so each device simultaneously functions as both a client and a server to all other devices connected to the network. | | **privacy policy** | A policy that outlines how the organization uses personal information it collects. | | **security policy** | A written document that states how an organization plans to protect the company's information technology assets. | | **social networking** | Grouping individuals and organizations into clusters or groups based on a like affiliation. | | **social networking sites** | Web sites that facilitate linking individuals with common interests like hobbies, religion, politics, or school or work contacts. | | http://www.cengage.com/images/spacer_tr.gif | |