|  |
| --- |
| **SECURITY+ ACRONYMS**  3DES – Triple Digital Encryption Standard |
| AAA – Authentication, Authorization, and Accounting |
| ACL – Access Control List |
| AES - Advanced Encryption Standard |
| AES256 – Advanced Encryption Standards 256bit |
| AH - Authentication Header |
| ALE - Annualized Loss Expectancy |
| AP - Access Point |
| ARO - Annualized Rate of Occurrence |
| ARP - Address Resolution Protocol |
| AUP - Acceptable Use Policy |
| BCP – Business Continuity Planning |
| BIOS – Basic Input / Output System |
| BOTS – Network Robots |
| CA – Certificate Authority |
| CAC - Common Access Card |
| CAN - Controller Area Network |
| CCMP – Counter-Mode/CBC-Mac Protocol |
| CCTV - Closed-circuit television |
| CERT – Computer Emergency Response Team |
| CHAP – Challenge Handshake Authentication Protocol |
| CIRT – Computer Incident Response Team |
| CRC – Cyclical Redundancy Check |
| CRL – Certification Revocation List |
| DAC – Discretionary Access Control |
| DDOS – Distributed Denial of Service |
| DEP – Data Execution Prevention |
| DES – Digital Encryption Standard |
| DHCP – Dynamic Host Configuration Protocol |
| DLL - Dynamic Link Library |
| DLP - Data Loss Prevention |
| DMZ – Demilitarized Zone |
| DNS – Domain Name Service (Server) |
| DOS – Denial of Service |
| DRP – Disaster Recovery Plan |
| DSA – Digital Signature Algorithm |
| EAP - Extensible Authentication Protocol |
| ECC - Elliptic Curve Cryptography |
| EFS – Encrypted File System |
| EMI – Electromagnetic Interference |
| ESP – Encapsulated Security Payload |
| FTP – File Transfer Protocol |
| GPU - Graphic Processing Unit |
| GRE - Generic Routing Encapsulation |
| HDD – Hard Disk Drive |
| HIDS – Host Based Intrusion Detection System |
| HIPS – Host Based Intrusion Prevention System |
| HMAC – Hashed Message Authentication Code |
| HSM – Hardware Security Module |
| HTTP – Hypertext Transfer Protocol |
| HTTPS – Hypertext Transfer Protocol over SSL |
| HVAC – Heating, Ventilation Air Conditioning |
| IaaS - Infrastructure as a Service |
| ICMP - Internet Control Message Protocol |
| ID – Identification |
| IKE – Internet Key Exchange |
| IM - Instant messaging |
| IMAP4 - Internet Message Access Protocol v4 |
| IP - Internet Protocol |
| IPSEC – Internet Protocol Security |
| IRC - Internet Relay Chat |
| ISP – Internet Service Provider |
| IV - Initialization Vector |
| KDC - Key Distribution Center |
| L2TP – Layer 2 Tunneling Protocol |
| LANMAN – Local Area Network Manager |
| LDAP – Lightweight Directory Access Protocol |
| LEAP – Lightweight Extensible Authentication Protocol |
| MAC – Mandatory Access Control / Media Access Control |
| MAC - Message Authentication Code |
| MAN - Metropolitan Area Network |
| MBR – Master Boot Record |
| MD5 – Message Digest 5 |
| MSCHAP – Microsoft Challenge Handshake Authentication Protocol |
| MTU - Maximum Transmission Unit |
| NAC – Network Access Control |
| NAT – Network Address Translation |
| NIDS – Network Based Intrusion Detection System |
| NIPS – Network Based Intrusion Prevention System |
| NIST – National Institute of Standards & Technology |
| NOS – Network Operating System |
| NTFS - New Technology File System |
| NTLM – New Technology LANMAN |
| NTP - Network Time Protocol |
| OS – Operating System |
| OVAL – Open Vulnerability Assessment Language |
| PAP – Password Authentication Protocol |
| PAT - Port Address Translation |
| PBX – Private Branch Exchange |
| PEAP – Protected Extensible Authentication Protocol |
| PED - Personal Electronic Device |
| PGP – Pretty Good Privacy |
| PII – Personally Identifiable Information |
| PKI – Public Key Infrastructure |
| POTS – Plain Old Telephone Service |
| PPP - Point-to-point Protocol |
| PPTP – Point to Point Tunneling Protocol |
| PSK – Pre-Shared Key |
| PTZ – Pan-Tilt-Zoom |
| RA – Recovery Agent |
| RAD - Rapid application development |
| RADIUS – Remote Authentication Dial-in User Server |
| RAID – Redundant Array of Inexpensive Disks |
| RAS – Remote Access Server |
| RBAC – Role Based Access Control |
| RBAC – Rule Based Access Control |
| RSA – Rivest, Shamir, & Adleman |
| RTO – Recovery Time Objective |
| RTP – Real-Time Transport Protocol |
| S/MIME – Secure / Multipurpose internet Mail Extensions |
| SaaS - Software as a Service |
| SCAP - Security Content Automation Protocol |
| SCSI - Small Computer System Interface |
| SDLC - Software Development Life Cycle |
| SDLM - Software Development Life Cycle Methodology |
| SHA – Secure Hashing Algorithm |
| SHTTP – Secure Hypertext Transfer Protocol |
| SIM – Subscriber Identity Module |
| SLA – Service Level Agreement |
| SLE - Single Loss Expectancy |
| SMS - Short Message Service |
| SMTP – Simple Mail Transfer Protocol |
| SNMP - Simple Network Management Protocol |
| SONET – Synchronous Optical Network Technologies |
| SPIM - Spam over Internet Messaging |
| SSH – Secure Shell |
| SSL – Secure Sockets Layer |
| SSO – Single Sign On |
| STP – Shielded Twisted Pair |
| TACACS – Terminal Access Controller Access Control System |
| TCP/IP – Transmission Control Protocol / Internet Protocol |
| TKIP - Temporal Key Integrity Protocol |
| TLS – Transport Layer Security |
| TPM – Trusted Platform Module |
| UAT - User Acceptance Testing |
| UPS - Uninterruptable Power Supply |
| URL - Universal Resource Locator |
| USB – Universal Serial Bus |
| UTP – Unshielded Twisted Pair |
| VLAN – Virtual Local Area Network |
| VoIP - Voice over IP |
| VPN – Virtual Private Network |
| VTC – Video Teleconferencing |
| WAF- Web-Application Firewall |
| WAP – Wireless Access Point |
| WEP – Wired Equivalent Privacy |
| WIDS – Wireless Intrusion Detection System |
| WIPS – Wireless Intrusion Prevention System |
| WPA – Wireless Protected Access |
| XSRF - Cross-Site Request Forgery |
| XSRF- Cross-Site Request Forgery |
| XSS - Cross-Site Scripting |

**3DES** Also known as Triple Digital Encryption Standard (DES). A symmetric block cipher algorithm used for encryption.

**802.1X** The IEEE standard that defines port-based security for wireless network access control. It offers a means of authentication and defines the Extensible Authentication Protocol (EAP) over IEEE 802, and it is often known as EAP over LAN (EAPOL).

**A**

**AAA** Acronym for three key areas of security: Authentication, Authorization, and Accounting.

**acceptable use policy (AUP)** Agreed-upon principles set forth by a company to govern how the employees of that company may use resources such as computers and Internet access.

**access attack** An attack aimed at gaining access to resources.

**access control** The means of giving or restricting user access to network resources. Access control is usually accomplished through the use of an access control list (ACL).

**access control list (ACL)** A table or data file that specifies whether a user or group has access to a specific resource on a PC or NW.

**access point (AP)** The point at which access to a NW is accomplished. This term is often used in relation to a wireless AP (WAP).

**accountability** Being responsible for an item. The administrator is often accountable for the network and the resources on it.

**accounting** The act of keeping track of activity. Most often, this term is used to refer to tracking users’ interactions with network resources via log files that are routinely scanned and checked.

**acknowledgment (ACK)** A message confirming that a data packet was received. Acknowledgment is a TCP function and occurs at the Transport layer of the Open Systems Interconnection (OSI) and TCP/IP models.

**active response** A response generated in real time.

**active sniffing** Involves an attacker gaining access to a host in the NW through a switch and logically disconnecting it from the NW.

**activity** Any action a user undertakes.

**Address Resolution Protocol (ARP)** Protocol used to map known IP addresses to unknown physical addresses.

**AD-IDS** Anomaly-detection intrusion detection system. An AD-IDS works by looking for deviations from a pattern of normal network traffic.

**administrative policies** A set of rules that govern administrative usage of a system.

**administrator** The user who is accountable and responsible for the network.

**Advanced Encryption Standard (AES)** A FIPS publication that specifies a cryptographic algorithm for use by the U.S. government. *See also* Federal Information Processing Standard (FIPS).

**adware** Software that gathers information to pass on to marketers or that intercepts personal data such as credit card numbers and makes them available to third parties.

**AES256** An implementation of Advanced Encryption Standard (AES) that uses 256-bit encryption.

**alert** A notification that an unusual condition exists and should be investigated.

**algorithm** The series of steps/formulas/processes that is followed to arrive at a result.

**analyzer** The component or process that analyzes the data collected by the sensor.

**annualized loss expectancy (ALE)** A calculation that is used to identify risks and calculate the expected loss each year.

**annualized rate of occurrence (ARO)** A calculation of how often a threat will occur. For example, a threat that occurs once every five years has an annualized rate of occurrence of 1/5, or 0.2.

**anomaly detection** The act of looking for variations from normal operations (anomalies) and reacting to them.

**anonymous authentication** Authentication that doesn’t require a user to provide a username, password, or any other identification before accessing resources.

**antivirus** A category of software that uses various methods to prevent and eliminate viruses in a computer. It typically also protects against future infection. *See also* virus.

**antivirus engine** The core program that runs the virus-scanning process.

**antivirus software** Software that identifies the presence of a virus and is capable of removing or quarantining the virus.

**appliance** A freestanding device that operates in a largely self-contained manner.

**Application layer** The seventh layer of the Open Systems Interconnection (OSI) model. This layer deals with how applications access the network and describes application functionality, such as file transfer, messaging, and so on.

**application programming interface (API)** An abstract interface to the services and protocols provided by an operating system.

**armored virus** A virus that is protected in a way that makes disassembling it difficult. The difficulty makes it “armored” against antivirus programs that have trouble getting to, and understanding, its code.

**ARP table** The table that the Address Resolution Protocol uses. Contains a list of known IP addresses & their associated physical addresses. The table is cached in memory so that ARP lookups don’t have to be performed for frequently accessed addresses

**asset** Any resource of value that you want to secure and protect.

**asymmetric algorithm** An algorithm that utilizes two keys.

**asymmetric encryption** Encryption in which two keys must be used. One key is used to encrypt data, and the other is needed to decrypt the data. Asymmetric encryption is the opposite of symmetric encryption, where a single key serves both purposes.

**attack** Any unauthorized intrusion into the normal operations of a computer or computer network. The attack can be carried out to gain access to the system or any of its resources.

**audit files** Files that hold information about a resource’s access by users.

**auditing** The act of tracking resource usage by users.

**auditors** Individuals involved in auditing log and security files.

**authenticating the evidence** Verifying that the logs and other resources collected are legitimate. This technique can be useful in verifying that an attack has occurred.

**authentication** The means of verifying that someone is who they say they are.

**Authentication Header (AH)** A header used to provide connectionless integrity & data origin authentication for IP datagrams and to provide protection against replays.

**availability** The ability of a resource to be accessed, often expressed as a time period. Many networks limit users’ ability to access network resources to working hours, as a security precaution.

**B**

**back door (backdoor)** An opening left in a program application (usually by the developer) that allows additional access to data. Typically, these are created for debugging purposesand aren’t documented. Before the product ships, the back doors are closed; when they aren’t closed, security loopholes exist.

**backup** A usable copy of data made to media. Ideally, the backup is made to removable media and stored for recovery should anything happen to the original data.

**backup plan** A documented plan governing backup situations.

**backup policy** A written policy detailing the frequency of backups and the location of storage media.

**Bell-LaPadula model** A model designed for the military to address the storage & protection of classified info. This model is specifically designed to prevent unauthorized access to classified info. The model prevents the user from accessing info that has a higher security rating than they are authorized to access. It also prevents information from being written to a lower level of security.

**best practices** A set of rules governing basic operations.

**Biba model** A model similar in concept to the Bell-LaPadula model but more concerned w/info integrity (an area the Bell-LaPadula model doesn’t address). In this model, there is no write up or read down. If you’re assigned access to top-secret info, you can’t read secret info or write to any level higher than the level to which you’re authorized. This model keeps higher-level info pure by preventing less-reliable info from being intermixed with it.

**biometric device** A device that can authenticate an individual based on a physical characteristic.

**biometrics** The science of id’ing a person by using 1 or more of their features. The feature can be a thumbprint, a retinal scan, or any other biological trait.

**BIOS** The basic input/output system for an IBM-based PC. It is the firmware that allows the computer to boot.

**birthday attack** A probability method of finding collision in hash functions.

**Blowfish** A type of symmetric block cipher created by Bruce Schneier.

**boot sector** Also known as the Master Boot Record (MBR). The first sector of the hard disk, where the program that boots the operating system resides. It’s a popular target for viruses.

**Border Gateway Protocol (BGP)** An ISP protocol that allows routers to share information about routes with each other.

**border router** A router used to translate from LAN framing to WAN framing.

**bot** An automated software program (network robot) that collects information on the Web. In the malicious form, a bot is a compromised computer being controlled remotely.

**brute force attack** A type of attack that relies purely on trial and error and tries all possible combinations.

**buffer overflow attack** A type of denial of service (DoS) attack that occurs when more data is put into a buffer than it can hold, thereby overflowing it (as the name implies).

**business continuity planning (BCP)** A contingency plan that allows a business to keep running in the event of a disruption to vital resources.

**business impact analysis (BIA)** A study of the possible impact if a disruption to a business’s vital resources were to occur.

**C**

**Carlisle Adams Stafford Tavares (CAST)** A type of symmetric block cipher defined by RFC 2144.

**central office** The primary office from which most resources extend.

**certificate** A digital entity that establishes who you are and is often used with e-commerce. It contains your name and other identifying data.

**certificate authority (CA)** An issuer of digital certificates (which are then used for digital signatures or key pairs). A certificate authority is occasionally referred to as a certification authority.

**certificate policies** Policies governing the use of certificates.

**Certificate Practice Statement (CPS)** The principles and procedures employed in the issuing and managing of certificates.

**certificate revocation** The act of making a certificate invalid.

**Certificate Revocation List (CRL)** A list of digital certificate revocations that must be regularly downloaded to stay current.

**chain of custody** The log of the history of evidence that has been collected.

**Challenge Handshake Authentication Protocol (CHAP)** A protocol that challenges a system to verify identity. CHAP is an improvement over Password Authentication Protocol (PAP) in which one-way hashing is incorporated into a three-way handshake. RFC 1334 applies to both PAP and CHAP.

**change documentation** Documentation required to make a change in the scope of any particular item. In the realm of project management, a change document is a formal document requiring many signatures before key elements of the project can be modified.

**checkpoint** A certain action or moment in time that is used to perform a check. It allows a restart to begin at the last point the data was saved as opposed to from the beginning.

**checksum** A hexadecimal value computed from transmitted data that is used in error checking routines.

**cipher** *See* cryptographic algorithm.

**circuit switching** A switching method where a dedicated connection between the sender & receiver is maintained thruout the conversation.

**CIRT** *See* Computer Incident Response Team (CIRT).

**Clark-Wilson model** An integrity model for creating a secure architecture.

**clear text** Unencrypted text that can be read with any editor.

**client** The part of a client/server network where the computing is usually done. In a typical setting, a client uses the server for remote storage, backups, or security (such as a firewall).

**client/server network** A server-centric network in which all resources are stored on a file server and processing power is distributed among workstations and the file server.

**closed-circuit television (CCTV)** A surveillance camera used for physical-access monitoring.

**clustering** A method of balancing loads and providing fault tolerance.

**code escrow** The storage and conditions for release of source code provided by a vendor, partner, or other party.

**cold site** A physical site that has all the resources necessary to enable an organization to use it if the main site is inaccessible (destroyed). Commonly, plans call for turning to a cold site within a certain number of hours after the loss of the main site.

**collection of evidence** The means and orderly fashion by which evidence is collected, identified, and marked.

**collusion** An agreement between individuals to commit fraud or deceit.

**Common Access Card (CAC)** A standard ID card used by the DoD & other employers. It is used for authentication as well as an ID.

**Common Criteria (CC)** A document of specifications detailing security evaluation methods for IT products and systems.

**Common Criteria Recognition Agreement (CCRA)** A set of standards, formerly known as the Mutual Recognition Agreement (MRA), that defines Evaluation Assurance Levels (EALs).

**Common Gateway Interface (CGI)** An older form of scripting that was used extensively in early web systems.

**companion virus** A virus that creates a new program that runs in place of an expected program of the same name.

**compartmentalization** Standards that support a nonhierarchical security classification.

**Computer Emergency Response Team (CERT)** A team of experts who respond to computer security incidents.

**Computer Incident Response Team (CIRT)** A team of experts who respond to a security incident. The CIRT acronym is growing in popularity and quickly replacing CERT.

**confidentiality** Assurance that data remains private and no one sees it except for those expected to see it.

**configuration management** The administration of setup and changes to configurations.

**connectionless** Type of communications between two hosts that have no previous session established for synchronizing sent data. The data isn’t acknowledged at the receiving end. This method can allow data loss. Within the TCP/IP suite, the User Datagram Protocol

(UDP) is used for connectionless communication.

**connection-oriented** Type of communications between two hosts that have a previous session established for synchronizing sent data. The receiving PC acknowledges the data. This method allows for guaranteed delivery of data between PCs. Within the TCP/IP suite,

TCP is used for connection-oriented communications.

**cookie** A plain-text file stored on your machine that contains information about you (and your preferences) and is used by a server.

**critical business functions** Functions on which the livelihood of the company depends.

**CRL** *See* Certificate Revocation List (CRL).

**cross-site requires forgery** A form of web-based attack in which unauthorized cmds are sent from a user that a website trusts.

**cryptanalysis** The study and practice of finding weaknesses in ciphers.

**cryptanalyst** A person who does cryptanalysis.

**cryptographer** A person who participates in the study of cryptographic algorithms.

**cryptographic algorithm** A symmetric algorithm, also known as a cipher, used to encrypt and decrypt data.

**cryptography** The field of mathematics focused on encrypting and decrypting data.

**custodian** An individual responsible for maintaining the data, and the integrity of it, within their area.

**cyclic redundancy check (CRC)** An error-checking method in data communications that runs a formula against data before transmission. The sending station then appends the resultant value (called a checksum) to the data and sends it. The receiving station uses the same formula on the data. If the receiving station doesn’t get the same checksum result for the calculation, it considers the transmission invalid, rejects the frame, and asks for retransmission.

**D**

**data integrity** A quality that provides a level of confidence that data won’t be jeopardized and will be kept secret.

**Data Link layer** The second layer of the Open Systems Interconnection (OSI) model. It describes the physical topology of a network.

**data loss prevention (DLP)** Any systems that ID, monitor, & protect data to prevent it from unauthorized use, modification, or destruction.

**data packet** A unit of data sent over a network. A packet includes a header, addressing information, and the data itself.

**data repository** A centralized storage location for data, such as a database.

**data source** Where data originates.

**datagram** An OSI Layer 3, User Datagram Protocol (UDP) packet descriptor.

**DDoS attack** *See* Distributed Denial of Service (DDoS) attack.

**decryption** The process of converting encrypted data back into its original form.

**default gateway** The router to which all packets are sent when the workstation doesn’t know where the destination station is or when it can’t find the destination station on the local segment.

**demilitarized zone (DMZ)** An area for placing web and other servers outside the firewall, therefore, isolating them from internal network access.

**Denial of Service (DoS) attack** A type of attack that prevents any users—even legitimate ones—from using a system.

**destination port number** A portion of a complete address of a PC to which data is being sent from a sending PC. The port portion allows for the demultiplexing of data to be sent to a specific application.

**detection** The act of noticing an irregularity as it occurs.

**dictionary attack** The act of attempting to crack PWs by testing them against a list of dictionary words. With today’s powerful PCs, an attacker can combine 1 of many available automated PW-cracking utilities w/several large dictionaries or “wordlists” & crack huge #s of passwords in a matter of minutes. Any password based on any dictionary word is vulnerable to such an attack.

**differential backup** A type of backup that includes only new files or files that have changed since the last full backup. Differential backups differ from incremental backups in that they don’t clear the archive bit upon their completion.

**Diffie-Hellman** An asymmetric std for exchanging keys. This cryptographic algorithm is used primarily to send secret keys across public NWs. The process isn’t used to encrypt or decrypt messages; it’s used merely for the transmission of keys in a secure manner.

**digital signature** An asymmetrically encrypted signature whose sole purpose is to authenticate the sender.

**directory** A network database that contains a listing of all network resources, such as users, printers, groups, and so on.

**directory service** A network service that provides access to a central database of information, which contains detailed information about the resources available on a network.

**direct-sequence (DS)** A method of communication between wireless receivers.

**direct-sequence spread spectrum (DSSS)** A communications technology that is used to communicate in the 802.11 standard.

**disaster recovery** The act of recovering data following a disaster that has destroyed it.

**disaster recovery plan (DRP)** A plan outlining the procedure by which data is recovered after a disaster.

**discretionary access control (DAC)** A method of restricting access to objects based on the identity of the subjects or the groups to which they belong.

**disk mirroring** Technology that keeps identical copies of data on two disks to prevent the loss of data if one disk faults.

**disk striping** Technology that enables writing data to multiple disks simultaneously in small portions called stripes. These stripes maximize use by having all the read/write heads working constantly. Different data is stored on each disk and isn’t automatically duplicated (this means disk striping in and of itself doesn’t provide fault tolerance).

**disk striping with parity** A fault-tolerance solution of writing data across a number of disks and recording the parity on another. In the event any one disk fails, the data on it can be re-created by looking at the remaining data and computing parity to figure out the

missing data.

**Distributed Denial of Service (DDoS) attack** A derivative of a DoS attack in which multiple hosts in multiple locations all focus on one target to reduce its availability to the public. *See* Denial of Service (DoS) attack.

**DLP** *See* Data Loss Prevention (DLP).

**DMZ** *See* demilitarized zone (DMZ).

**DNS server** Any server that performs address resolution from a DNS fully qualified domain name (FQDN) to an IP address. *See also* Domain Name Service (DNS), Internet Protocol (IP).

**DNS zone** An area in the DNS hierarchy that is managed as a single unit. *See also* Domain Name Service (DNS).

**DoD Networking Model** A four-layer conceptual model describing how communications should take place between computer systems. The four layers are Process/Application, Host-to-Host, Internet, and Network Access.

**domain** Within the Internet, a group of computers with shared traits and a common IP address set. A domain can also be a group of networked Windows computers that share a single SAM database. *See also* Security Accounts Manager (SAM).

**Domain Name Service (DNS)** The network service used in TCP/IP networks that translates hostnames to IP addresses. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

**DoS attack** *See* Denial of Service (DoS) attack.

**dual-homed host** A host that resides on more than one network and possesses more than one physical network card.

**dumb terminal** A keyboard and monitor that send keystrokes to a central processing computer (typically a mainframe or minicomputer) that returns screen displays to the monitor. The unit has no processing power of its own, hence the moniker “dumb.”

**Dumpster diving** Looking thru trash for clues—often in the form of paper scraps—to find users’ PWs & other pertinent information.

**duplexed hard drives** Two hard drives to which identical information is written simultaneously. A dedicated controller card controls each drive. Used for fault tolerance, and is known as RAID 1.

**duplicate servers** Two servers that are identical, for use in clustering.

**Dynamic Host Configuration Protocol (DHCP)** A protocol used on a TCP/IP NW to send client config data, including IP address, default gateway, SNM, & DNS configuration, to clients. DHCP uses a 4-step process: Discover, Offer, Request, & Acknowledgement. *See also* default gateway, Domain Name Service (DNS), Transmission Control Protocol/Internet Protocol (TCP/IP).

**dynamic packet filtering** A type of firewall used to accept or reject packets based on their contents.

**dynamic routing** The use of route-discovery protocols to talk to other routers and find out what networks they are attached to. Routers that use dynamic routing send out special packets to request updates from the other routers on the network as well as to send their own updates.

**dynamically allocated port** A TCP/IP port that is not constantly used but accessed by an application when needed.

**E**

**eavesdropping** Any type of passive attack that intercepts data in an unauthorized manner— usually in order to find passwords. Cable sniffing, wiretapping, and man-in-the-middle attacks are eavesdropping attacks.

**electromagnetic interference (EMI)** The interference that can occur during transmissions over copper cable because of electromagnetic energy outside the cable. The result is degradation of the signal.

**elliptic curve cryptography (ECC)** A type of public key cryptosystem that requires a shorter key length than many other cryptography systems (including the de facto industry standard, RSA).

**Encapsulating Security Payload (ESP)** A header used to provide a mix of security services in IPv4 and IPv6. ESP can be used alone or in combination with the IP Authentication Header (AH).

**encoding** The process of translating data into signals that can be transmitted on a transmission medium.

**Encrypting File System (EFS)** A feature in NTFS on Windows-based operating systems that allows for filesystem-level encryption to be applied.

**encryption** The process of converting data into a form that makes it less likely to be usable to anyone intercepting it if they can’t decrypt it.

**encryption key** A string of alphanumeric characters used to decrypt encrypted data.

**enticement** The process of luring someone.

**entrapment** The process of encouraging an attacker to perform an act, even if they don’t want to do it.

**enumeration** An attempt to gain information about a network by specifically targeting network resources, users and groups, and applications running on the system.

**escalation** The act of moving something up in priority. Often, when an incident is escalated, it’s brought to the attention of the next-highest supervisor. *See also* privilege escalation.

**Evaluation Assurance Level (EAL)** A level of assurance, expressed as a numeric value, based on standards set by the Common Criteria Recognition Agreement (CCRA).

**event** Any noticeable action or occurrence.

**exposure factor (EF)** A calculation of how much data (or other assets) could be lost from a single occurrence. If all the data on the network could be jeopardized by a single attack, the exposure factor is 100 percent.

**Extensible Authentication Protocol (EAP)** An authentication protocol used in wireless networks and point-to-point connections.

**external threat** A threat that originates from outside the company.

**extranet** Web (or similar) services set up in a private network to be accessed internally and by select external entities, such as vendors and suppliers.

**extrusion** Examining data leaving a network for signs of malicious traffic.

**F**

**fail-over/failover** The process of reconstructing a system or switching over to other systems when a failure is detected.

**fail-over device** A device that comes online when another fails.

**fail-over server** A hot-site backup system in which the fail-over server is connected to the primary server. A heartbeat is sent from the primary server to the backup server. If the heartbeat stops, the fail-over system starts and takes over. Thus, the system doesn’t go down even if the primary server isn’t running.

**false positive** A flagged event that isn’t really an event and has been falsely triggered.

**Faraday cage** An electrically conductive wire mesh or other conductor woven into a “cage” that surrounds a room and prevents electromagnetic signals from entering or leaving the room through the walls.

**fault-resistant network** A network that is up and running at least 99 percent of the time or that is down less than 8 hours a year.

**fault tolerance** The ability to withstand a fault (failure) without losing data.

**fault-tolerant network** A network that can recover from minor errors.

**Federal Information Processing Standard (FIPS)** An agreed-upon standard published under the Information Technology Management Reform Act. The secretary of commerce approves the standards after they’re developed by the National Institute of Standards and Technology (NIST) for federal computer systems.

**File Transfer Protocol (FTP)** TCP/IP & SW that permit transferring files between computer systems & utilize clear-text passwords. Because FTP has been implemented on numerous types of computer systems, files can be transferred between disparate computer systems (for example, a personal computer & a minicomputer). *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

**fire suppression** The act of stopping a fire and preventing it from spreading.

**firewall** A combination of hardware and software that protects a network from attack by hackers who could gain access through public networks, including the Internet.

**footprinting** The process of systematically identifying the network and its security posture. This is typically a passive process.

**forensics** In terms of security, the act of looking at all the data at your disposal to try to figure out who gained unauthorized access and the extent of that access.

**frequency-hopping spread spectrum (FHSS)** A communications technology used to communicate in the 802.11 standard. FHSS accomplishes communication by hopping the transmission over a range of predefined frequencies.

**FTP proxy** A server that uploads and downloads files from another server on behalf of a workstation.

**full backup** A backup that copies all data to the archive medium.

**full distribution** An information classification stating that the data so classified is available to anyone.

**G**

**Gramm-Leach-Bliley Act** A government act containing rules on privacy of consumer finance information.

**Grandfather, Father, Son** One of the most popular methods of backup tape rotation. Three sets of tapes are rotated in this method. The most recent backup after the full backup is the Son. As newer backups are made, the Son becomes the Father, and the Father, in turn, becomes the Grandfather. At the end of each month, a full backup is performed on all systems. This backup is stored in an off-site facility for a period of one year. Each monthly backup replaces the monthly backup from the previous year. Weekly or daily incremental backups are performed and stored until the next full backup occurs. This full backup is then stored off site, and the weekly or daily backup tapes are reused.

**H**

**hacker** Generally used to refer to someone who gains access to a system, software, or hardware without permission. Also can be called a cracker.

**handshake** The process of agreeing to communicate and share data. TCP uses a three-way handshake to establish connections, and part of this process can be exploited by certain types of attacks.

**hardening** The process of making an entity, usually an OS, more secure by closing known holes & addressing known security issues.

**hash/hashing** The process of transforming characters into other characters that represent (but are not) the originals. Traditionally, the results are smaller and more secure than the original.

**hash value** A single number used to represent an original piece of data.

**Health Insurance Portability and Accountability Act (HIPAA)** An act that addresses security and privacy of health-related data.

**high availability** A clustering solution to provide resource reliability and availability.

**hijacking (TCP/IP hijacking)** *See* man-in-the-middle attack.

**hoax** Typically an email message warning of something that isn’t true, such as the outbreak of a new virus. The hoax can send users into a panic and cause more harm than the virus.

**honeypot (also known as Honey pot)** A bogus system set up to attract and slow down a hacker. A honeypot can also be used to learn of the hacking techniques and methods that hackers employ.

**host** Any network device with a TCP/IP network address.

**host-based IDS (HIDS)** An intrusion detection system that is host based. The alternative is network based.

**host-based IPS (HIPS)** An intrusion prevention system that is host based. To prevent the intrusion, it must first detect it (thus making it a superset of HIDS) and then act accordingly.

**hostile code** Any code that behaves in a way other than in the best interest of the user and the security of data.

**host-to-host** Describes communication that occurs between hosts.

**hot fix/hotfix** Another word for a patch. When Microsoft rolls a bunch of hotfixes together, they become known as a service pack.

**hot site** A location that can provide operations within hours of a failure.

**HVAC** A common acronym for Heating, Ventilation, and Air Conditioning.

**Hypertext Markup Language (HTML)** A set of codes used to format text and graphics that will be displayed in a browser. The codes define how data will be displayed.

**Hypertext Transfer Protocol (HTTP)** The protocol used for communication between a web server and a web browser.

**Hypertext Transfer Protocol over SSL** Also known as HTTPS and HTTP Secure. A combination of HTTP with Secure Sockets Layer (SSL) to make for a secure connection. It uses port 443 by default.

**I**

**ICMP attack** An attack that occurs by triggering a response from the Internet Control Message Protocol (ICMP) when it responds to a seemingly legitimate maintenance request. *See also* Internet Control Message Protocol (ICMP).

**identification and authentication (I&A)** A two-step process of identifying a person (usually when they log on) and authenticating them by challenging their claim to access a resource.

**IEEE** *See* Institute of Electrical and Electronics Engineers, Inc. (IEEE).

**IEEE 802.10 LAN/MAN Security** A series of guidelines dealing with various aspects of network security.

**IEEE 802.11** A family of protocols that provides for wireless communications using radiofrequency transmissions.

**IEEE 802.11 Wireless LAN** Defines the stds for implementing wireless technologies such as infrared and spread-spectrum radio.

**illicit server** An app/program that shouldn’t be there but is operating on the NW, and one that is commonly used to gain unauthorized control by allowing someone to bypass normal authentication. NetBus is one of the best-known examples of an illicit server.

**incident** An attempt to violate a security policy, a successful penetration, a compromise of a system, or unauthorized access to info.

**incident response** How an organization responds to an incident.

**incident response plan (IRP)** A policy that defines how an organization will respond to an incident.

**incident response team (IRT)** Also known as a Computer Security Incident Response Team (CSIRT). The group of individuals responsible for responding when a security breach has occurred.

**incremental backup** A type of backup in which only new files or files that have changed since the last full backup or the last incremental backup are included. Incremental backups clear the archive bit on files upon their completion.

**information classification** The process of determining what information is accessible to what parties and for what purposes.

**information classification policies** Written policies detailing dissemination of information.

**information destruction policies** Policies that define how information is destroyed when it has reached the end of its useful life.

**Information Flow model** A model concerned with all the properties of information flow, not just the direction of the flow.

**information policies** Policies governing the various aspects of info sec. Info policies include access, classifications, marking and storage, and the transmission and destruction of sensitive information. The development of information policies is critical to security.

**information retention** A designation of how long data is retained and any other significant considerations about information.

**information security** Security practices applied to information.

**infrastructure** The hardware and software necessary to run your network.

**infrastructure security** Security on the hardware and software necessary to run your network.

**instant messaging (IM)** Immediate communication that can be sent back and forth between users who are currently logged on. From a security standpoint, there are risks associated with giving out information via IM that can be used in social engineering attacks; in addition, attachments sent can contain viruses.

**Institute of Electrical and Electronics Engineers, Inc. (IEEE)** An international organization that sets standards for various electrical and electronics issues.

**Integrated Services Digital Network (ISDN)** A telecommunications standard that is used to digitally send voice, data, and video signals over the same lines.

**interception** The process of covertly obtaining information not meant for you. Interception can be an active or passive process.

**internal information** Information intended to remain within an organization.

**internal threat** A threat that arises from within an organization.

**International Data Encryption Algorithm (IDEA)** An algorithm that uses a 128-bit key. This product is similar in speed and capability to Digital Encryption Standard (DES), but it’s more secure. IDEA is used in Pretty Good Privacy (PGP).

**International Organization for Standardization (ISO)** The standards organization that developed the Open Systems Interconnection (OSI) model. This model provides a guideline for how communications occur between computers.

**International Telecommunications Union (ITU)** Organization responsible for communications standards, spectrum management, and the development of communications infrastructures in underdeveloped nations.

**Internet** A global network made up of a large number of individual networks that are interconnected and use TCP/IP.

**Internet Architecture Board (IAB)** The committee that oversees management of the Internet. It’s made up of two subcommittees: the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). *See also* Internet Engineering Task Force

(IETF) and Internet Research Task Force (IRTF).

**Internet Assigned Numbers Authority (IANA)** The organization responsible for governing IP addresses. http://www.iana.org.

**Internet Control Message Protocol (ICMP)** A message and management protocol for TCP/IP. The Ping utility uses ICMP. *See also* Ping, Transmission Control Protocol/Internet Protocol (TCP/IP).

**Internet Engineering Task Force (IETF)** An international organization that works under the Internet Architecture Board to establish standards and protocols relating to the Internet. *See also* Internet Architecture Board (IAB).

**Internet Group Management Protocol (IGMP)** A protocol used for multicasting operations across the Internet.

**Internet layer** The network layer responsible for routing, IP addressing, and packaging.

**Internet Message Access Protocol (IMAP)** A protocol with a store-and-forward capability. It can also allow messages to be stored on an email server instead of downloaded to the client.

**Internet Protocol (IP)** The protocol in the TCP/IP suite responsible for network addressing.

**Internet Research Task Force (IRTF)** An international organization that works under the Internet Architecture Board to research new Internet technologies. *See also* Internet Architecture Board (IAB).

**Internet service provider (ISP)** A company that provides direct access to the Internet for home and business computer users.

**Internet Society (ISOC)** A professional membership group composed primarily of Internet experts. It oversees a number of committees and groups, including the Internet Engineering Task Force (IETF).

**intranet** Web (or similar) services set up in a private network to be accessed internally only.

**intrusion** The act of entering a system without authorization to do so.

**intrusion detection system (IDS)** Tools that ID & respond to attacks using defined rules or logic. An IDS can be NW or host based.

**intrusion detector** The item/application performing intrusion detection. *See also* intrusion

detection system (IDS).

**IP proxy** A server that acts as a go-between for clients accessing the Internet. All communications look as if they originated from a proxy server because the IP address of the user making a request is hidden. Also known as Network Address Translation (NAT).

**IP Security (IPSec)** A set of protocols that enable encryption, authentication, and integrity over IP. IPSec is commonly used with virtual private networks (VPNs) and operates at Layer 3.

**IP spoofing** An attack during which a hacker tries to gain access to a network by pretending their interface has the same network address as the internal network.

**J**

**JavaScript** A programming language that allows access to system resources of the system running the script. These scripts can interface with all aspects of an operating system just like programming languages, such as the C language.

**journaling** The ability of a file system to use a log file of all changes and transactions that have occurred within a set period of time (for example, the last few hours). If a crash occurs, the operating system can look at the log files to see what transactions have been

committed and which ones have not.

**K**

**Kerberos** An authentication scheme that uses tickets (unique keys) embedded within messages. Named after the three-headed guard dog that stood at the gates of Hades in Greek mythology.

**key/certificate life cycle** The time during which the processes of a key or certificate take place.

**key distribution center (KDC)** An organization/facility that generates keys for users.

**key escrow agency** An agency that stores keys for the purpose of law-enforcement access.

**Key Exchange Algorithm (KEA)** A method of offering mutual authentication and establishing data encryption keys.

**key generation** The act of creating keys for use by users.

**key suspension** The temporary deferment of a key for a period of time (such as for a leave of absence).

**Keyed-Hash Message Authentication Code (HMAC)** “A mechanism for message authentication using cryptographic hash functions” per the draft of the Federal Information Processing Standard (FIPS) publication. Addressed in RFC 2104.

**L**

**latency** The wait time between the call for an action or activity and the actual execution of that action.

**lattice** The concept that access differs at different levels. Often used in discussion with the Biba and Bell-LaPadula models as well as with cryptography to differentiate between security levels based on user/group labels.

**Layer 2 Forwarding (L2F)** A tunneling protocol often used with virtual private networks (VPNs). L2F was developed by Cisco.

**Layer 2 Tunneling Protocol (L2TP)** A tunneling protocol that adds functionality to the Point-to-Point Protocol (PPP). This protocol was created by Microsoft and Cisco and is often used with virtual private networks (VPNs).

**Lightweight Directory Access Protocol (LDAP)** A set of protocols that was derived from X.500 and operates at port 389.

**limited distro** Describes info that isn’t intended for release to the public. This category of information isn’t secret, but it’s private.

**Link Control Protocol (LCP)** The protocol used to establish, configure, and test the link between a client and PPP host. *See also* Point-to-Point Protocol (PPP).

**local area network (LAN)** A network that is restricted to a single building, group of buildings, or even a single room. A LAN can have one or more servers.

**local registration authority (LRA)** An authority used to identify or establish the identity of an individual for certificate issuance.

**logic bomb** Any code that is hidden within an application and causes something unexpected to happen based on some criteria being met. For example, a programmer could create a program that always makes sure his name appears on the payroll roster; if it doesn’t, then key files begin to be erased.

**logs and inventories** Tools used to help an organization know what is happening to its systems and assets. System logs tell what is happening with the systems in the network. Inventories refer to both the physical assets and the software assets a company owns.

**M**

**M of N Control method** A rule stating that in order to access the key server if *n* number of administrators have the ability to perform a process, *m* number of those administrators must authenticate for access to occur. M of N Control may involve physical presence.

**MAC address** The address that is either assigned to a network card or burned into the network interface card (NIC). PCs use MAC addresses to keep track of one another and keep each other separate.

**macro virus** A software exploitation virus that works by using the macro feature included in many applications.

**malicious code** Any code that is meant to do harm.

**Mandatory Access Control (MAC)** A security policy wherein labels are used to identify the sensitivity of objects. When a user attempts to access an object, the label is checked to see if access should be allowed (that is, whether the user is operating at the same sensitivity level). This policy is “mandatory,” because labels are automatically applied to all data (and can be changed only by administrative action), as opposed to “discretionary” policies that leave it up to the user to decide whether to apply a label.

**man-in-the-middle attack** An attack that occurs when someone/something that is trusted intercepts packets and retransmits them to another party. Man-in-the-middle attacks have also been called TCP/IP hijacking in the past.

**mantrap** A device, such as a small room, that limits access to one or a few individuals. Mantraps typically use electronic locks and other methods to control access.

**mathematical attack** An attack focused on the encryption algorithm itself, the key mechanism, or any potential area of weakness in the algorithm.

**mean time between failure (MTBF)** The measure of the anticipated incidence of failure of a system or component.

**mean time to repair (MTTR)** The measurement of how long it takes to repair a system or component once a failure occurs.

**Media Access Control (MAC)** A sublayer of the Data Link layer of the Open Systems Interconnection (OSI) model that controls the way multiple devices use the same media channel. It controls which devices can transmit and when they can transmit.

**message authentication code** A common method of verifying integrity. The MAC is derived from the message & a secret key.

**message digest** The signature area within a message.

**Message Digest Algorithm (MDA)** An algorithm that creates a hash value. The hash value is also used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

**Microsoft Challenge Handshake Authentication Protocol (MSCHAP)** An implementation of the Challenge Handshake Authentication Protocol (CHAP) common in Microsoft’s Windows-based operating systems. The latest version, and the only one supported in Windows Vista, is MSCHAPv2.

**misuse-detection IDS (MD-IDS)** A method of evaluating attacks based on attack signatures and audit trails.

**modification attack** An attack that modifies information on your system.

**multicasting** Sending data to more than one address.

**multi-factor** The term employed anytime more than one factor must be considered.

**multipartite virus** A virus that attacks a system in more than one way.

**N**

**NAT** Network Address Translation. *See* IP proxy.

**National Computing Security Center (NCSC)** The agency that developed the Trusted Computer System Evaluation Criteria (TCSEC) and the Trusted Network Interpretation Environmental Guideline (TNIEG).

**National Institute of Standards & Technology (NIST)** An agency (formerly known as the National Bureau of Standards [NBS]) that has been involved in developing & supporting stds for the U.S. gov for over 100 yrs. NIST has become involved in cryptography stds, systems, & tech in a variety of areas. It’s primarily concerned with governmental systems, where it exercises a great deal of influence.

**National Security Agency (NSA)** The U.S. gov agency responsible for protecting U.S. communications & producing foreign intelligence info. It was established by presidential directive in 1952 as a separately organized agency w/in the DoD.

**need-to-know** A method of information dissemination based on passing information only to those who need to know it.

**network** A group of devices connected by some means for the purpose of sharing information or resources.

**Network Access Control (NAC)** The set of standards defined by the network for clients attempting to access it. Usually, NAC requires that clients be virus free and adhere to specified policies before allowing them on the network.

**network attached storage** Storage, such as hard drives, attached to a network for the purpose of storing data for clients on the network. Network attached storage is commonly used for backing up data.

**network-based IPS (N-IPS)** An intrusion prevention system that is network based. To prevent the intrusion, it must first detect it (thus making it a superset of IDS), and then act accordingly.

**Network Control Protocol (NCP)** The protocol Point-to-Point Protocol (PPP) employs for encapsulating network traffic.

**Network File System (NFS)** A protocol that enables users to access files on remote computers as if the files were local.

**network interface card (NIC)** A physical device that connects computers and other network equipment to the transmission medium.

**Network Interface layer** The lowest level of the TCP/IP suite; it is responsible for placing & removing packets on the physical NW.

**Network layer** The third layer of the OSI model, it is responsible for logical addressing and translating logical names into physical addresses. This layer also controls the routing of data from source to destination as well as the building and dismantling of packets.

**Network Operations Center (NOC)** A single, centralized area for network monitoring

and administrative control of systems.

**network operating system (NOS)** The software enabling networking; NOS can be on a LAN or WAN.

**network sniffer** A device that has access to the signaling on the network cable.

**network-based IDS (N-IDS)** An approach to an intrusion detection system (IDS), it attaches the system to a point in the network where it can monitor and report on all network traffic.

**nonessential service** A service that isn’t necessary to keep the server operating at the expected level in its expected role.

**Noninterference model** A model intended to ensure that higher-level security functions don’t interfere with lower-level functions.

**non-repudiation** Verifying (by whatever means) that data was seen by an intended party. It makes sure they received the data and can’t repudiate (dispute) that it arrived.

**notification** The act of being alerted to an event.

**notification policies** A set of rules about what triggers notification.

**O**

**off-site storage** Storing data off the premise, usually in a secure location.

**one-tier model** A model in which the database and applications exist on the same system.

**one-time pad** Words added to values during authentication. The message to be encrypted is added to this random text before hashing.

**on-site storage** Storing backup data at the same site as the servers on which the original data resides.

**Open Shortest Path First (OSPF)** A link-state routing protocol used in IP networks.

**Open Systems Interconnection (OSI) model** A model defined by the ISO to categorize the process of communication between PCs in terms of seven layers. The seven layers are Application, Presentation, Session, Transport, Network, Data Link, and Physical.

**operational security** Security as it relates to how an organization does things (operates).

**operator** The person primarily responsible for the intrusion detection system (IDS).

**OS hardening** The process of applying all security patches and fixes to an operating system to make it as secure as possible.

**out-of-band method** A way to transmit the encryption key by using a method other than the one used to transmit the data. The key value is sent by letter, by courier, or by some other separate means.

**OVAL** An acronym for Open Vulnerability and Assessment Language, it is a community standard for system analysis that focuses on testing, analyzing, and reporting.

**owner** The person responsible for the current existence of a resource.

**P**

**packet filtering** A firewall technology that accepts or rejects packets based on their content.

**packet switching** The process of breaking messages into packets at the sending router for easier transmission over a WAN.

**pad** A number of characters often added to data before an operation such as hashing takes place. Most often unique values, known as one-time pads, are added to make the resulting hash unique.

**partitioning** The process of breaking a network into smaller components that can be individually protected.

**passive detection** A type of intruder detection that logs all network events to a file for an administrator to view later.

**passive response** A nonactive response, such as logging. Passive response is the most common type of response to many intrusions. In general, passive responses are the easiest to develop and implement.

**Password Authentication Protocol (PAP)** One of the simplest forms of authentication. Authentication is accomplished by sending the username & PW to the server & having them verified. PWs are sent as clear text &, therefore, can be easily seen if intercepted.

**password guessing** Attempting to enter a password by guessing its value.

**password history** A list of passwords that have already been used.

**patch** A fix for a known software problem.

**penetration** The act of gaining access.

**perimeter security** Security set up on the outside of the network or server to protect it.

**personal electronic device (PED)** Any electronic device transported by a user. Examples include smartphones, electronic book readers, and music players.

**personally identifiable information (PII)** Information that can be uniquely used to identify, contact, or locate a single person. Examples include social security number, driver’s license number, fingerprints, and handwriting.

**phage virus** A virus that modifies and alters other programs and databases.

**phishing** A form of social engineering in which you simply ask someone for a piece of information that you are missing by making it look as if it is a legitimate request. Commonly sent via email.

**phreaker** Someone who abuses phone systems, as opposed to data systems.

**physical access control** Control access measures used to restrict physical access to the server(s).

**physical barrier** An object, such as a locked door, used to restrict physical access to network components.

**Physical layer** The first layer of the OSI model; controls the functional interface.

**physical port** On a computer, an interface where you can connect a device.

**physical security** Security that guards the physical aspects of the network.

**Ping** A TCP/IP utility used to test whether another host is reachable. An Internet Control Message Protocol (ICMP) request is sent to the host, which responds with a reply if it’s reachable. The request times out if the host isn’t reachable.

**ping of death** A large ICMP packet sent to overflow the remote host’s buffer. It usually causes the remote host to reboot or hang.

**plain old telephone service (POTS)** Std phone svc, as opposed to other connection technologies like Digital Subscriber Line (DSL).

**point-to-point** Network communication in which two devices have exclusive access to a network medium. For example, a printer connected to only one workstation is using a point-to-point connection.

**Point-to-Point Protocol (PPP)** A full-duplex line protocol that supersedes Serial Line Internet Protocol (SLIP). It’s part of the standard TCP/IP suite and is often used in dial-up connections.

**Point-to-Point Tunneling Protocol (PPTP)** An extension to Point-to-Point Protocol (PPP) that is used in virtual private networks (VPNs). An alternative to PPTP is L2TP. **policies** Rules or standards governing usage. These are typically high level in nature.

**polymorphic** An attribute of some viruses that allows them to mutate and appear differently each time they crop up. The mutations make it harder for virus scanners to detect (and react) to the viruses.

**port** Some kind of opening that allows network data to pass through.

**Port Address Translation (PAT)** A means of translating between ports on a public & private network. Similar to Network Address Translation (NAT), which translates addresses between public and private.

**port scanner** The item (physical or software) that scans a server for open ports that can be taken advantage of. Port scanning is the process of sending messages to ports to see which ones are available and which ones aren’t.

**postmortem** Anything that occurs “after the fact,” such as an audit or review.

**Post Office Protocol (POP)** An email access program that can be used to retrieve email from an email server.

**Post Office Protocol Version 3 (POP3)** The protocol used to download email from an SMTP email server to a network client

**power conditioner** A device that “conditions” the electrical supply to take out spikes and surges.

**power system** A device that provides electrical power.

**Presentation layer** The sixth layer of the OSI model; responsible for formatting data exchange, such as graphic commands, and converting character sets. This layer is also responsible for data compression, data encryption, and data stream redirection.

**preservation of evidence** The process of controlling access to evidence within chain-ofcustody measures, often by placing it in a controlled-access area with a single custodian responsible for all access.

**Pretty Good Privacy (PGP)** An implementation of RSA encryption. *See also* RSA.

**privacy** A state of security in which information isn’t seen by unauthorized parties w/out the express permission of the party involved.

**Private Branch Exchange (PBX)** A system that allows users to connect voice, data, pagers, networks, and almost any other application into a single telecommunications system. A PBX system allows an organization to be its own phone company.

**private information** Information that isn’t for public knowledge.

**private key** An asymmetric encryption technology in which both the sender and the receiver have different keys. A public key is used to encrypt messages and the private key is used to decrypt them. *See also* public key.

**private network** The part of a network that lies behind a firewall and isn’t “seen” on the Internet. *See also* firewall.

**privilege audit** An audit performed to verify that no user is accessing information, or able to access information, beyond the security level at which they should be operating.

**privilege escalation** The result when a user obtains access to a resource they wouldn’t normally be able to access. Privilege escalation can be done inadvertently, by running a program with Set User ID (SUID) or Set Group ID (SGID) permissions or by temporarily

becoming another user (via su or sudo in Unix/Linux or RunAs in Windows). It can also be done purposefully by an attacker seeking full access.

**process list** The list of processes currently running on a system.

**promiscuous mode** A mode wherein a network interface card (NIC) intercepts all traffic crossing the network wire and not just the traffic intended for it.

**protocol analyzer** A software and hardware troubleshooting tool that is used to decode protocol information to try to determine the source of a network problem and to establish baselines.

**protocols** Standards or rules.

**proxy** A type of firewall that prevents direct comm between a client and a host by acting as an intermediary. *See also* firewall.

**proxy cache server** An implementation of a web proxy. The server receives an HTTP request from a web browser and makes the request on behalf of the sending workstation. When the response comes, the proxy cache server caches a copy of the response locally. The next time someone makes a request for the same web page or Internet information, the proxy cache server can fulfill the request out of the cache instead of having to retrieve the resource from the Web.

**proxy firewall** A proxy server that also acts as a firewall, blocking network access from external networks.

**proxy server** A type of server that makes a single Internet connection and services requests on behalf of many users.

**public information** Information that is publicly made available to all.

**public key** A technology that uses 2 keys—a public key and a private key—to facilitate communication. The public key is used to encrypt a message to a receiver. *See also* private key.

**Public Key Cryptography Standards (PKCS)** A set of voluntary standards created by RSA security and industry security leaders.

**Public Key Infrastructure (PKI)** A 2-key encryption sys wherein msgs are encrypted w/a private key & decrypted with a public key.

**Public Key Infrastructure X.509 (PKIX)** The Internet Engineering Task Force (IETF) working group developing standards and models for the Public Key Infrastructure (PKI) environment. The most current version is v3.

**public network** The part of a network outside a firewall that is exposed to the public. *See also* firewall.

**public key system** An encryption system employing a key that is known to users beyond the recipient.

**Q**

**quantum cryptography** Cryptography based on changing the polarity of a photon. Quantum cryptography makes the process of interception difficult because any attempt to intercept the message changes the value of the message.

**R**

**radio frequency (RF)** The part of the radio spectrum that a device uses.

**radio frequency interference (RFI)** The byproduct of electrical processes, similar to electromagnetic interference. The major difference is that RFI is usually projected across a radio spectrum.

**RAID levels** The different types of RAID, such as RAID-0, RAID-1, and so on.

**Redundant Array of Independent (or Inexpensive) Disks (RAID)** A configuration of multiple hard disks used to provide fault tolerance, should a disk fail, or gains in efficiency. Different levels of RAID exist.

**registration authority (RA)** An organization that offloads some of the work from a certificate authority (CA). An RA system operates as a middleman in the process. The RA can distribute keys, accept registrations for the CA, and validate identities. The RA

doesn’t issue certificates; that responsibility remains with the CA.

**relying party** The person receiving a certificate.

**remote access protocol** Any networking protocol that is used to gain access to a network over public communication links.

**remote access server (RAS)** A computer that has one or more modems installed to enable remote connections to the network.

**Remote Authentication Dial-In User Service (RADIUS)** A mechanism that allows authentication of dial-in & other NW connections. RADIUS is commonly used by Internet service providers (ISPs) & in the implementation of virtual private NWs (VPNs).

**replay attack** Any attack where the data is retransmitted repeatedly (often fraudulently or maliciously). In one such possibility, a user can replay a web session and visit sites intended only for the original user.

**replication** The process of copying directory information to other servers to keep them all synchronized.

**repository** A database or database server where the certificates are stored.

**repudiation attack** An attack in which the intruder modifies information in a system.

**Request for Comments (RFC)** A document-creation process & a set of practices that originated in 1969 & is used for proposed changes to Internet standards.

**response** How you react to an event.

**restricted information** Information that isn’t made available to all and to which access is granted based on some criteria.

**retrovirus** A virus that attacks or bypasses the antivirus software installed on a computer.

**reverse DNS** Using an IP address to find a domain name rather than using a domain name to find an IP address (normal DNS). Pointer (PTR) records are used for the reverse lookup, and often reverse DNS is used to authenticate incoming connections.

**reverse engineering** The process of re-creating the functionality of an item by first deciding what the result is and then creating something from scratch that serves the same purpose.

**revocation** The process of canceling credentials that have been lost or stolen (or are no longer valid). With certificates, revocation is accomplished with a Certificate Revocation List (CRL).

**risk analysis** An evaluation of each risk that can be ID’d. Each risk should be outlined, described, and & evaluated on the likelihood of it occurring.

**risk assessment** An evaluation of how much risk you and your organization are willing to take. An assessment must be performed before any other actions—such as how much to spend on security in terms of dollars and manpower—can be decided.

**Rivest Cipher 5 (RC5)** A cipher algorithm created by Ronald Rivest (for RSA) and known for its speed. It works through blocks of variable sizes using three phases: key expansion, encryption, and decryption.

**roaming profile** A profile downloaded from a server at each logon. When a user logs out at the end of the session, changes are made and remembered for the next time the user logs on.

**rogue server** An active Dynamic Host Configuration Protocol (DHCP) server that has been added to the network and is now leasing addresses to users instead of them obtaining an address from your server.

**role-based access control (RBAC)** A type of control wherein the levels of security closely follow the structure of an organization. The role the person plays in the org (accountant, salesman, and so on) corresponds to the level of security access they have to data.

**rootkit** Software program that has the ability to obtain root-level access and hide certain things from the operating system.

**route** The path to get to the destination from a source.

**route cost** The number of router hops between the source and the destination in an internetwork.

**router** A device that connects two or more networks and allows packets to be transmitted and received between them. A router determines the best path for data packets from source to destination.

**routing** A function of the Network layer that involves moving data throughout a network. Data passes through several network subnetworks using routers that can select the path the data takes. *See also* router.

**Routing Information Protocol (RIP)** A distance-vector route discovery protocol used by Internetwork Packet Exchange (IPX) & Internet Protocol (IP). IPX uses hops & ticks to determine the cost for a particular route.

**routing table** A table that contains info about the locations of other routers on the network and their distance from the current router.

**RSA** One of the providers of cryptography systems to industry and government. RSA stands for the initials of the three founders of RSA Security Inc.: Rivest, Shamir, and Adleman. RSA maintains a list of standards for Public Key Cryptography Standards (PKCS).

**Rule Set-Based Access Control (RSBAC)** An open-source access control framework for the Linux kernel that uses access control modules to implement Mandatory Access Control (MAC).

**S**

**sandbox** A set of rules used when creating a Java applet that prevents certain functions when the applet is sent as part of a web page.

**scanning** The process that attackers use to gather information about how a network is configured.

**screened host** A router that is in front of a server on the private network. Typically, this server does packet filtering before reaching the firewall/proxy server that services the internal network.

**Secure Electronic Transaction (SET)** A protocol developed by Visa and MasterCard for secure credit card transactions. The protocol is becoming an accepted standard by many companies. SET provides encrypted credit card numbers over the Internet, and it’s most suited to small amounts of data transmission.

**Secure Hash Algorithm (SHA)** A one-way hash algorithm designed to ensure the integrity of a message.

**Secure Hypertext Transfer Protocol (S-HTTP)** A protocol used for secure communications between a web server & a web browser.

**Secure Shell (SSH)** A replacement for rlogin in Unix/Linux that includes security. rlogin allowed one host to establish a connection with another with no real security being employed; SSH replaces it with slogin and digital certificates.

**Secure Sockets Layer (SSL)** A protocol that secures messages by operating between the App layer (HTTP) & the Transport layer.

**Secure WLAN Protocol (SWP)** A method of securing wireless networks that is beginning to gain momentum and acceptance.

**Security Accounts Manager (SAM)** A database within Windows NT–based operating systems that contains information about all users and groups and their associated rights and settings within a domain.

**security audit** An audit of the system (host, network, and so on) for security vulnerabilities and holes.

**security log** A log file used in Windows NT to keep track of security events specified by the domain’s audit policy.

**security policies** Rules set in place by a company to ensure the security of a network. These may include how often a password must be changed or how many characters a password should be.

**security professionals** Individuals who make their living working with computer security.

**security token** A piece of data that contains the rights and access privileges of the token bearer as part of the token.

**security zone** A method of isolating a system from other systems or networks.

**segment** A unit of data transmission found at the Transport layer of the Open Systems Interconnection (OSI) model and used by TCP.

**sensor** A device that collects data from the data source and passes it on to the analyzer.

**separation of duties** A set of policies designed to reduce the risk of fraud and prevent other losses in an organization.

**sequence #** A # used to determine the order in which parts of a pkt are to be reassembled after the packet has been split into sections.

**Serial Line Internet Protocol (SLIP)** An older protocol that was used in early remote access environments. SLIP was originally designed to connect Unix systems together in a dial-up environment, and it supports only serial communications.

**server** A computer that provides resources to the clients on the network.

**server and client configuration** A network in which the resources are located on a server and accessed by clients.

**server authentication** A process that requires the workstation to authenticate against the server.

**service** An item that adds functionality to a network by providing resources or doing tasks for other computers.

**service account** An account created on a server for a user to perform special services, such as a backup operator, an account operator, and a server operator.

**service-level agreement (SLA)** An agreement that specifies performance requirements for a vendor. This agreement may use mean time before failure (MTBF) and mean time to repair (MTTR) as performance measures in the SLA.

**service pack** Operating system updates from Microsoft.

**session key** The agreed-upon (during connection) key used between a client and a server during a session. This key is generated by encrypting the server’s digital ID (after validity has been established). The asymmetric key pair is then used to encrypt and verify the session key that is passed back and forth between client and server during the length of the connection.

**Session layer** The fifth layer of the OSI model. It determines how two computers establish, use, and end a session. Security authentication and network naming functions required for applications occur here. The Session layer establishes, maintains, and breaks dialogs between two stations. *See also* Open Systems Interconnection (OSI) model.

**share-level security** A NW security method that assigns PWs to individual files or other NW resources (such as printers) instead of assigning rights to NW resources to users. The passwords are then given to all users that need access to these resources. All resources are visible from anywhere in the NW, and any user who knows the password for a particular NW resource can make changes to it.

**shoulder surfing** Watching someone when they enter their username/password/sensitive data.

**signal** Transmission from one PC to another. A signal could be a notification to start a session or end a session.

**signal encoding** The process whereby a protocol at the Physical layer receives information from the upper layers and translates all the data into signals that can be transmitted on a transmission medium.

**signaling method** The process of transmitting data across the medium. Two types of signaling are digital and analog.

**signed applet** An applet that doesn’t run in the Java sandbox and has higher system access capabilities. Signed applets aren’t usually downloaded from the Internet but are provided by in-house or custom programming efforts.

**Simple Mail Transfer Protocol (SMTP)** A protocol for sending email between SMTP servers.

**Simple Network Management Protocol (SNMP)** The management protocol created for sending information about the health of the network-to-network management consoles.

**single loss expectancy (SLE)** The cost of a single loss when it occurs. This loss can be a critical failure, or it can be the result of an attack.

**single sign-on (SSO)** A relationship between the client and the network wherein the client is allowed to log on one time, and all resource access is based on that logon (as opposed to needing to log on to each individual server to access the resources there).

**site survey** A generic site survey involves listening in on an existing wireless network using commercially available technologies. A wireless site survey, or wireless survey, is the process of planning and designing a wireless network, in particular an 802.11.

**SMTP relay** A feature designed into many email servers that allows them to forward email to other email servers. While the ability to act as a relay exists to allow networks to grow, the possibility exists for rogue servers to also participate.

**smurf attack** An attack in which large volumes of ICMP echo requests (pings) are broadcast to all other machines on the network and in which the source address of the broadcast system has been spoofed to appear as though it came from the target computer. When all

the machines that received the broadcast respond, they flood the target with more data than it can handle.

**snapshot backup** A method of performing backups that creates a compressed file of a database as it exists at the moment, without taking the users offline. A snapshot backup can take the place of other backups. It’s often run on mirrored servers, but the snapshot captures only the most recent version of files.

**sniffer** A physical device that listens in (sniffs) on network traffic and looks for items it can make sense of. There is a legitimate purpose for these devices: Administrators use them to analyze traffic. However, when they’re used by sources other than the administrator, they become security risks.

**sniffing** Analyzing data to look for passwords and anything else of value. Sniffing is also known as wiretapping, eavesdropping, and a number of other terms (packet sniffing, network sniffing, and so on).

**snooping** Looking through files in hopes of finding something interesting.

**social engineering** An attack that uses others by deceiving them. It does not directly target hardware or software, but instead targets and manipulates people.

**socket** The primary method used to communicate with services and applications such as the Web and Telnet. The socket is a programming construct that enables communication by mapping between ports and addresses.

**software exploitation** An attack launched against applications and higher-level services.

**spam** Unwanted, unsolicited email sent in bulk.

**spike** A momentary or instantaneous increase in power over a power line.

**spoofing attack** An attempt by someone or something to masquerade as someone else.

**spyware** Software programs that work—often actively—on behalf of a third party.

**state table** A firewall security method that monitors the status of all the connections through the firewall.

**stateful packet filtering** Inspections that occur at all levels of the network and provide additional security using a state table that tracks every communications channel.

**static Address Resolution Protocol (ARP) table entry** An entry in the Address Resolution Protocol (ARP) table that a user adds manually when a PC will be accessed often.

**static routing** A method of routing packets where the router’s routing table is updated manually by the network administrator instead of automatically by a route discovery protocol.

**stealth port** A port that is open but might not be obvious (invisible if you don’t know it exists). Trojan horses often exploit them.

**stealth virus** A virus that attempts to avoid detection by masking itself from applications.

**steganography** The science of hiding information within other information, such as a picture.

**strength** The effectiveness of a cryptographic system in preventing unauthorized decryption.

**subscriber** An individual who is attempting to present a certificate proving authenticity.

**surge protector** A device that protects electrical components from momentary or instantaneous increases in a power line.

**switched** A network that has multiple routes to get from a source to a destination. Switching allows for higher speeds.

**symmetrical keys** The keys used when the same key encrypts and decrypts data.

**SYN flood** A Denial of Service attack in which the hacker sends a barrage of spoofed SYN packets. The receiving station tries to respond to each SYN request for a connection, thereby tying up all the resources. All incoming connections are rejected until all current connections can be established.

**system architecture** Documents that provide you with the blueprint of your organization’s software and hardware infrastructure.

**T**

**tap** A type of connection that directly attaches to a cable.

**TCP ACK attack** An attack that begins as a normal TCP connection and whose purpose is to deny service. It’s also known as a TCP SYN flood.

**TCP sequence attack** An attack wherein the attacker intercepts and then responds with a sequence number similar to the one used in the original session. The attack can either disrupt a session or hijack a valid session.

**TCP wrapper** A low-level logging package designed for Unix systems.

**TCP/IP** *See* Transmission Control Protocol/Internet Protocol (TCP/IP).

**TCP/IP hijacking** An attack in which the attacker commandeers a TCP session from a legitimate user after the legitimate user has achieved authentication, thereby removing the need for the attacker to authenticate himself.

**teardrop attack** A DoS attack that uses large packets and odd offset values to confuse the receiver and help facilitate a crash.

**Telnet** A protocol that functions at the Application layer of the OSI model, providing terminal emulation capabilities

**Temporal Key Interchange/Integrity Protocol (TKIP)** A wrapper that works with wireless encryption to strengthen WEP implementations. It was designed to provide more secure encryption than the notoriously weak Wired Equivalent Privacy (WEP).

**Terminal Access Controller Access-Control System (TACACS)** An authentication system that allows credentials to be accepted from multiple methods, including Kerberos. The TACACS client/server process occurs in the same manner as the Remote Authentication Dial-In User Service (RADIUS) process.

**terminal emulator** A program that enables a PC to act as a terminal for a mainframe or a Unix system.

**termination policy** A clear process of informing affected departments of a voluntary or involuntary termination.

**test account** An administrator-created account for confirming the basic functionality of a newly installed application, for example. The test account has equal rights to accounts that will use the new functionality. It’s important to use test accounts instead of administrator accounts to test new functionality. If an administrator account is used, problems related to user rights might not manifest themselves because administrator accounts typically have full rights to all network resources.

**thin client** Systems that don’t provide any disk storage or removable media on their workstations.

**third party** A party responsible for providing assurance to the relying party that a subscriber is genuine.

**threat** Any perceivable risk.

**three-tier model** A system that effectively isolates the end user from the database by introducing a middle-tier server.

**time to live (TTL)** A field in an IP packet that indicates how many routers the packet can cross & how long it takes before it’s discarded. TTL is also used in Address Resolution Protocol (ARP) tables to indicate how long an entry should remain in the table.

**token** A piece of data holding information about the user. This information can contain group IDs, user IDs, privilege level, and so on.

**Tracert** The command-line utility that shows the user every router interface a packet passes through on its way to a destination.

**trailer** A section of a data packet that contains error-checking information.

**transceiver** A device that allows the network interface card (NIC) to connect to the network.

**transmission** Sending packets from the PC to the server. The trans can occur over a NW cable, wireless connection, or other medium.

**Transmission Control Protocol (TCP)** The protocol found at the Host-to-Host layer of the Department of Defense (DoD) model. This protocol breaks data packets into segments, numbers them, and sends them in order. The receiving computer reassembles the data so that the information is readable for the user. In the process, the sender and the receiver confirm that all data has been received; if not, it’s resent. TCP is a connection-oriented protocol. *See also* connection-oriented.

**Transmission Control Protocol/Internet Protocol (TCP/IP)** The protocol suite developed by the Department of Defense (DoD) in conjunction with the Internet. It was designed as an internetworking protocol suite that could route information around network failures. Today it’s the de facto standard for communications on the Internet.

**transmission media** Physical cables and/or wireless technology across which computers are able to communicate.

**Transport layer** The fourth layer of the OSI model. It’s responsible for checking that the data packet created in the Session layer was received. If necessary, it also changes the length of messages for transport up or down the remaining layers.

**Transport Layer Security (TLS)** A protocol whose purpose is to verify that secure communications between a server and a client remain secure. Defined in RFC 2246.

**Triple-DES (3DES)** A symmetric block cipher algorithm used for encryption.

**Trivial File Transfer Protocol (TFTP)** A UDP-based protocol similar to FTP that doesn’t provide the security or error-checking features of FTP. *See also* File Transfer Protocol (FTP).

**Trojan horse** Any application that masquerades as one thing in order to get past scrutiny and then does something malicious. One of the major differences between Trojan horses and viruses is that Trojan horses tend not to replicate themselves.

**Trust List** A list of objects signed by a trusted entity. Also known as a Certificate Trust List (CTL).

**Trusted Platform Module (TPM)** A method of utilizing encryption and storing the passwords on a chip. The hardware holding the chip is then needed to unencrypt the data and make it readable.

**tunneling** The act of sending data across a public network by encapsulating it into other packets.

**two-factor authentication** Using two access methods as a part of the authentication process.

**2-tier model** A model in which the client PC runs an app that communicates with a database that is running on a different server.

**U**

**Uniform Resource Locator (URL)** A way of identifying a document on the Internet. It consists of the protocol used to access the document and the domain name or IP address of the host that holds the document; for example, http://www.sybex.com.

**uninterruptible power supply (UPS)** A device that can provide short-term power, usually by using batteries.

**uptime** The amount of time a particular computer or network component has been functional.

**usage policies** Defined policies governing computer usage.

**user** The person who is using a computer or network or a resource.

**User Datagram Protocol (UDP)** The protocol at the Host-to-Host layer of the TCP/IP Department of Defense (DoD) model, which corresponds to the Transport layer of the OSI model. Packets are divided into datagrams, given numbers, sent, and put back together at

the receiving end. UDP is a connectionless protocol. *See also* connectionless, Open Systems Interconnection (OSI) model.

**user-level security** A type of NW sec in which user accts can read, write, change, & take ownership of files. Rights are assigned to user accounts, and each user knows only their own username and password—which makes this the preferred method for securing files.

**user management policies** Defined policies that detail user management.

**V**

**virtual LAN (VLAN)** Local area network (LAN) that allows users on different switch ports to participate in their own network separate from, but still connected to, the other stations on the same or a connected switch.

**virtual link** A link created by using a switch to limit network traffic.

**virtual private network (VPN)** Uses the public Internet as a backbone for a private interconnection (network) between locations.

**virus** A program intended to damage a computer system. Sophisticated viruses are encrypted and hide in a computer, and might not appear until the user performs a certain action or until a certain date. *See also* antivirus.

**volume** The loudness of a sound, or the portion of a hard disk that functions as if it were a separate hard disk.

**W**

**war driving** Driving around with a laptop looking for open wireless access points with which to communicate.

**warm site** A site that provides some capabilities in the event of a disaster. The organization that wants to use a warm site will need to install, configure, and reestablish operations on systems that might already exist in the warm site.

**weak key** A cipher hole that can be exploited.

**weak key attack** An attack that looks for cipher holes.

**web proxy** A type of proxy that is used to act on behalf of a web client or web server.

**web server** A server that holds and delivers web pages and other web content using HTTP.

**wide area network (WAN)** A network that crosses local, regional, and/or international boundaries.

**Wi-Fi protected access (WPA)** Security protocol developed by the Wi-Fi Alliance to protect wireless networks and surpass what WEP offered. There are two versions, WPA and WPA2, with the latter being the full implementation of the security features.

**Windows socket** A Microsoft API used to interact with TCP/IP.

**Wired Equivalent Privacy (WEP)** A security protocol for 802.11b (wireless) networks that attempts to establish the same security for them as would be present in a wired network.

**wireless access point** A wireless bridge used in a multipoint radio frequency (RF) network.

**wireless bridge** A bridge that performs all the functions of a regular bridge but uses RF instead of cables to transmit signals.

**Wireless Fidelity (Wi-Fi)** A wireless network operating in the 2.4 Ghz or 5 Ghz range.

**wireless local area network (WLAN)** A LAN that employs wireless access points (WAPs) and clients using the 802.11 standards.

**wireless portal** The primary method of connecting a wireless device to a network.

**wireless technologies** Technologies employing wireless communications.

**Wireless Transport Layer Security (WTLS)** The security layer of the Wireless Applications Protocol (WAP). WTLS provides authentication, encryption, and data integrity for wireless devices.

**work factor** An estimate of the amount of time and effort that would be needed to break a system.

**workgroup** A specific group of users or network devices, organized by job function or proximity to shared resources.

**working copy** The copy of the data currently in use on a network.

**workstation** A PC that isn’t a server but is on a NW. Generally, a workstation is used to do work, whereas a server is used to store data or perform a network function.

**World Wide Web Consortium (W3C)** An association concerned with interoperability, growth, and standardization of the World Wide Web (WWW). This group is the primary sponsor of XML and other web-enabled technologies.

**worm** A program similar to a virus. Worms, however, propagate themselves over a network. *See also* virus.

**WPA** *See* Wi-FI protected access (WPA).

**X**

**X.500** The International Telecommunications Union (ITU) standard for directory services in the late 1980s. The standard was the basis for later models of directory structure, such as Lightweight Directory Access Protocol (LDAP).

**XSRF** *See* cross-site request forgery (XSRF).

**Z**

**zombie** Any system taking directions from a master control computer. Zombies are often utilized in distributed denial of service (DDoS) and botnet attacks.

**zone** An area in a building where access is individually monitored and controlled.