Glossary

Some terms in this aren't included in the body of *(ISC)²® CISSP® Certified Information Systems Security Professional Official Study Guide, Ninth Edition*. These terms have been included on previous exams and are potentially relevant to the current exam. *See* and *see also* indicate that there is another relevant entry you should read. *Aka* (also known as) indicates other similar terms that are not discussed further.

Numbers and Symbols

*** (star) Integrity Axiom, * Axiom** An axiom of the Biba model that states that a subject at a specific classification level cannot write data to a higher classification level. This is often shortened to "no write up."

*** (star) Security Property, * Property** A property of the Bell–LaPadula model that states that a subject at a specific classification level cannot write data to a lower classification level. This is often shortened to "no write down."

1000BaseT A form of twisted-pair cable that supports 1,000 Mbps or 1 Gbps throughput at 100 meter distances. Often called Gigabit Ethernet.

100BaseTX Another form of twisted-pair cable similar to 100BaseT. 100BaseTX is the most common form of Fast Ethernet.

10Base2 A type of coaxial cable. Often used to connect systems to backbone trunks. 10Base2 has a maximum span of 185 meters with maximum throughput of 10 Mbps. A legacy network connection technology not likely to be found in a modern network. *See also* thinnet.

10Base5 A type of coaxial cable. Often used as a network's backbone. 10Base5 has a maximum span of 500 meters, with maximum throughput of 10 Mbps. A legacy network connection technology not likely to be found in a modern network. *See also* thicknet.

10BaseT A form of twisted-pair cable used for 10 Mbps baseband communications up to 100 meters per segment. *See also* unshielded twisted pair (UTP) or shielded twisted pair (STP) (if shielded).

2.4 GHz One of the radio frequencies used by Wi-Fi.

3DES *See* Triple Data Encryption Standard (3DES).

4G (4th Generation) A mobile service technology that has been in use since the early 2000s which is available for use on mobile phones, tablets, and other equipment.

5G (5th Generation) The latest mobile service technology (as of 2020) that is available for use on mobile phones, tablets, and other equipment.

5 GHz One of the radio frequencies used by Wi-Fi.

802.11 *See* IEEE 802.11.

802.11i (WPA2) An amendment to the 802.11 standard that defines a new authentication and encryption technique that is similar to IPsec. To date, no real-world attack has compromised a properly configured WPA2 wireless network.

802.1q The IEEE standard that defines VLAN tagging. VLAN tagging is used by switches and bridges to manage traffic within and between VLANs. *See also* IEEE 802.1q.

802.1X A form of wireless authentication protection that requires all wireless clients to pass a gauntlet of RADIUS or TACACS services before network access is granted. *See also* IEEE 802.1X.

A

AAA server A server dedicated to performing authentication, authorization, and accounting (auditing) services, typically for remote users. Common examples include Remote Authentication Dial-In User Service (RADIUS), Diameter, Terminal Access Controller Access Control System (TACACS), and TACACS+.

AAA services An acronym that refers to authentication, authorization, and accounting (or sometimes auditing). However, it actually refers to five elements: identification, authentication, authorization, auditing, and accounting.

abnormal activity Any system activity that does not normally occur on your system. Also referred to as suspicious activity.

abstraction The collection of similar elements into groups, classes, or roles for the assignment of security controls, restrictions, or permissions as a collective.

acceptable use policy (AUP) A policy that defines a level of acceptable performance and expectation of behavior and activity for employees. Failure to comply with the policy may result in job action warnings, penalties, or termination. The AUP defines what is and what is not an acceptable activity, practice, or use for company equipment and resources.

acceptance A form of risk management in which you mitigate some of the risk and accept the remainder. Aka accepting risk or tolerating risk. *See also* risk tolerance, assignment, transfer/transference (as related to risk), avoidance, reducing risk, mitigation, rejecting risk, and ignoring risk.

acceptance testing A form of testing that attempts to verify that a system satisfies the stated criteria for functionality and possibly also for security capabilities of a product. It is used to determine whether end users or customers will accept the completed product.

accepting risk The valuation by management of the cost/benefit analysis of possible safeguards and the determination that the cost of the countermeasure greatly outweighs the possible cost of loss because of a risk.

access The transfer of information from an object to a subject.

access aggregation Collecting multiple pieces of nonsensitive information and combining it or aggregating it to learn sensitive information. Reconnaissance attacks often use access aggregation methods.

access control list (ACL) A list of rights that an object (such as a user group) has to resources in the network; a means of restricting access. Uses for access control lists include (but aren't limited to) permitting or denying network traffic through a router or switch; marking a specific type of network traffic as interesting; and allowing or denying read, write, and/or execute permissions to specific files, directories, and even system objects. Also, the column of an access control matrix that specifies what level of access each subject has over an object.

access control matrix A table of subjects and objects that indicates the actions or functions that each subject can perform on each object. Each column of the matrix is an access control list (ACL). Each row of the matrix is a capability list.

access control The means of giving or restricting user access to objects (i.e., resources). This is usually accomplished through the use of an access control list (ACL). *See also* discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC, RoBAC, or role-BAC), attribute-based access control (ABAC), and rule-based access control (RuBAC, Rule-BAC).

access control triplet The three-part relationship of subject/program/object (or subject/transaction/object) used by the Clark–Wilson model of security.

access control types Categories of access controls. Preventive controls attempt to prevent security incidents from occurring, detective controls attempt to discover incidents after they've occurred, and corrective controls attempt to correct any problems caused by detected incidents. Other control types include recovery, deterrent, directive, and compensation access controls. Controls are implemented using administrative, logical/technical, or physical means.

access control vestibule A double set of doors that is often protected by a guard. The purpose is to contain a subject until their identity and authentication are verified. Previously known as a mantrap.

access policies Policies that define what access is to be granted to a subject over an object. Access policies can focus on the object/asset and base granting of use on value, risk, threat, etc. Access policies can focus on a user's job description or role assignment for determining access.

access tracking Auditing, logging, and monitoring the attempted access or activities of a subject. Also referred to as activity tracking.

accessibility The assurance that the widest range of subjects can interact with a resource regardless of their capabilities or limitations, in relation to availability.

account audit, account maintenance The regular or periodic activity of reviewing and assessing the user accounts of an IT environment.

account expiration Automatically disabling a user account or causing the account to expire at a specific time and date.

account lockout A security service that disables a user account after a specified number of failed logon attempts. Account lockout is an effective countermeasure to brute-force and dictionary attacks against a system's logon prompt.

account maintenance The regular or periodic activity of reviewing and assessing the user accounts of an information technology (IT) environment.

account permissions The access activities granted or denied users, often through the use of per-object access control lists (ACLs).

account policy enforcement The collection of password-requirement features in the operating system, often called a password policy.

account revocation The act of deprovisioning an account by deleting it.

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

accounting *See* accountability.

accuracy Being correct and precise in relationship to integrity.

ACID model The letters in ACID represent the four required characteristics of database transactions: atomicity, consistency, isolation, and durability.

acknowledgment (ACK) A message confirming that a data packet was received. This occurs at the Transport layer of the Open Systems Interconnection (OSI) model.

ACL *See* access control list (ACL).

active content Web programs that users download to their own computers for execution rather than consuming server-side resources.

Active Directory The replacement for NT Directory Service (NTDS) that is included with Windows 2000. Because it's an X.500-based directory service, it's similar to Novell's Directory Services (NDS), which is also called eDirectory.

active monitoring Generating traffic on a network or against a system and monitoring the flow or response of the environment. It is using a false load or work to monitor the operations of a target. *See* synthetic monitoring.

active reconnaissance Collecting information about a target through interactive means. By directly interacting with a target, accurate and detailed information can be collected

quickly but at the risk of being identified as an attacker rather than an innocent, benign, random visitor. *See* passive reconnaissance.

active response A response generated in real time.

active sniffing Attacking a switch with media access control (MAC) flooding to force the switch into flooding mode, where it acts like a hub. Active sniffing can also involve sending Address Resolution Protocol (ARP) responses to force traffic toward the sniffer.

active-active, active-active system A form of load balancing that uses all available pathways or systems during normal operations.

active-passive, active-passive system A form of load balancing that keeps some pathways or systems in an unused dormant state during normal operations.

ActiveX A legacy deprecated technology from Microsoft that was based on the Distributed Component Object Model (DCOM) to operate over the web. ActiveX allowed customized controls, icons, and other features to enhance the usability of web-enabled systems. ActiveX was only supported by Microsoft Internet Information Server (IIS) and the Internet Explorer browser.

ad hoc, ad hoc mode A peer-to-peer 802.11 wireless network connection between two (or more) individual systems without the need for a wireless base station. Ad hoc does not support encryption. An updated version is known as Wi-Fi Direct. *See also* peer-to-peer mode and Wi-Fi Direct.

Address Resolution Protocol (ARP) A subprotocol of the TCP/IP protocol suite that operates at the Data Link layer (layer 2). ARP is used to discover the MAC address of a system by polling using its IP address.

Address Space Layout Randomization (ASLR) A malware defensive measure implemented by some OSs when randomizing the memory locations of system components and applications at boot/launch.

addressing The means by which a processor refers to various locations in memory.

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

administrative law Regulations that cover a range of topics, from procedures to be used within a federal agency to immigration policies, that will be used to enforce the laws passed by Congress. Administrative law is published in the Code of Federal Regulations (CFR).

administrative physical security controls Security controls that include facility construction and selection, site management, personnel controls, awareness training, and emergency response and procedures.

admissibility In U.S. courts, for evidence to be considered usable in court (i.e., admissible), it must meet three requirements: relevant, material, and competent. Evidence is relevant if it helps to determine or establish a fact about the case. Evidence is material if the fact determined by the evidence is related to the case. Evidence is competent if it was obtained legally, such as via a search warrant or consent.

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

Advanced Encryption Standard (AES) A widely used symmetric encryption algorithm that uses 128-bit blocks and supports three key sizes: 128, 192, and 256. AES is based on the symmetric Rijndael block cipher.

advanced persistent threat (APT) (1) An organized group of attackers who are highly motivated, skilled, and patient. They are often sponsored by a government, are focused on a specific target, and will continue attacking for a very long time until they achieve their goal. (2) Any form of cyberattack perpetrated by attackers that is able to exploit a target continuously over a considerable period of time. An APT often takes advantage of unknown flaws (that is, not publicly known) and tries to maintain stealth throughout the attack. The name is derived from the concept that the attacks are unique and exploit flaws that are not public knowledge (that is, this state of using an exploit against an unknown flaw is labeled as advanced), that the exploit grants the attackers ongoing remote access to and control over the target (that is, it's persistent), and that the attackers are likely nation-states (that is, it's a threat).

adverse actions The consequences of failing to abide by company policies or actively committing criminal violations within the organization.

advisory policy A policy that discusses behaviors and activities that are acceptable and defines consequences of violations. An advisory policy discusses the senior management's desires for security and compliance within an organization. Most policies are advisory.

adware A variation on the idea of spyware that displays pop-up advertisements to users based on their activities, URLs they have visited, applications they have accessed, and so on. Adware is used to target prospective customers with advertisements.

AES *See* Advanced Encryption Standard (AES).

affinity A configured preference for a client request to be sent to a specific server within the cluster or device cloud managed by the load balancer. *See* persistence (2).

agent A small software application often designed to execute on a client (or other target) and send information back to a server or management system. Multiple types of agents are used in the fields of networking and security. For instance, the Simple Network Management Protocol (SNMP) utilizes an agent for query response. *See also* bot.

agent-based (related to NAC) A typical operation of an agent-based network access control (NAC) system would be to install a NAC monitoring agent on each managed system. The NAC agent retrieves a configuration file on a regular basis, possibly daily or upon network connection, to check the current configuration baseline requirements against the local system. If the system is not compliant, it can be quarantined into a remediation subnet, where it can communicate only with the NAC server. The NAC agent can download and apply updates and configuration files to bring the system into compliance. Once compliance is achieved, the NAC agent returns the system to the normal production network.

agentless (related to NAC) An agentless or network monitoring and assessment NAC solution performs port scans, service queries, and vulnerability scans against networked systems from the NAC server to determine whether devices are authorized and baseline compliant. An agentless system requires an administrator to manually resolve any discovered issues.

aggregate functions SQL functions, such as `COUNT()`, `MIN()`, `MAX()`, `SUM()`, and `AVG()`, that can be run against a database to produce an information set.

aggregation A number of functions that combine records from one or more tables to produce potentially useful, more valuable, or more sensitive information than the original items on their own.

aggregation switch The main or master switch used as the interconnection point for numerous other switches. In the past, this device may have been known as the master distribution frame (MDF), central distribution frame, core distribution frame, or primary distribution frame.

aggregator A type of multiplexor. Numerous inputs are received and directed or transmitted to a single destination. MPLS is an example of an aggregator.

Agile A software development life cycle (SDLC) model based on adaptive development, in which focusing on a working product and fulfilling customer needs is prioritized over rigid adherence to a process, use of specific tools, and detailed documentation.

Agile Manifesto The document that defines 12 principles that underlie the Agile philosophy.

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

AH (Authentication Header) *See* Authentication Header (AH).

AI *See* artificial intelligence (AI).

air gap Another term for physical network segregation.

alarm A mechanism that is separate from a motion detector and triggers a deterrent, triggers a repellent, and/or triggers a notification. Whenever a motion detector registers a significant or meaningful change in the environment, it triggers an alarm. *See* deterrent alarms, repellent alarms, notification alarms, local alarm system, central station system, proprietary system (alarm), and auxiliary alarm system.

alarm triggers Notifications sent to administrators when a specific event occurs.

ALE (annualized loss expectancy) The potential dollar value loss per year per risk. It's calculated by multiplying the single-loss expectancy (SLE) by the annualized rate of occurrence (ARO).

algorithm A formula, process, series of steps, or set of rules or procedures to perform on input data. Commonly related to cryptographic functions that dictate the permutations of encryption and decryption.

allow list A security option that prohibits unauthorized software from being able to execute. In application security, allow listing prevents any software, including malware, from executing unless it's on the preapproved exception list (the allow list). Aka deny by default and application allow listing. *See also* implicit deny.

allowable interruption window (AIW) The maximum amount of time that a critical service can be down or unavailable before it interferes with the achievement of organizational objectives. *See* maximum tolerable downtime (MTD), maximum tolerable outage (MTO).

alternate business practices Any secondary, backup, failback, or fallback plans that can be used in the event that the preferred recovery strategies and planning procedures fail. *See also* backup contingency plan.

always-on VPN A virtual private network (VPN) that attempts to auto-connect to the VPN service every time a network link becomes active.

amplification attack A form of denial-of-service (DoS) attack in which the amount of work or traffic generated by an attacker is multiplied to cause a significant volume of traffic to be delivered to the primary victim.

amplifier *See* repeater.

analog communications A continuous signal that varies in frequency, amplitude, phase, voltage, and so on. The variances in the continuous signal produce a wave shape (as opposed to the square shape of a digital signal). The actual communication occurs by variances in the constant signal.

analytic attack An algebraic manipulation that attempts to reduce the complexity of a cryptographic algorithm. This attack focuses on the logic of the algorithm itself.

AND The operation (represented by the ∧, ., or & symbols) that checks to see whether two values are both true.

Android OS The mobile device operating system based on Linux that was acquired by Google.

announced test A security evaluation where everyone in the organization knows the penetration assessment is taking place and when.

annual cost of the safeguard (ACS) An estimation of the yearly costs for the safeguard to be present in the organization.

annualized loss expectancy (ALE) The possible yearly cost of all instances of a specific realized threat against a specific asset. The ALE is calculated using the formula ALE = single loss expectancy (SLE) * annualized rate of occurrence (ARO).

annualized rate of occurrence (ARO) The expected frequency or statistical probability that a specific threat or risk will occur (in other words, become realized) within a single year. Aka probability determination.

anomaly-based detection, anomaly detection A method of detecting malicious events by looking for abnormal occurrences or violations of specified rules. It's commonly used by intrusion detection systems (IDSs) and/or intrusion prevention systems (IPSs). *See also* behavior-based detection, heuristic-based detection, and signature-based detection.

anonymization A process by which personally identifiable information (PII) is removed from a dataset. Aka deidentification.

anonymous authentication Authentication that doesn't require a user to provide a username, a password, or any other identification before accessing resources. This is considered a poor security practice and is dangerous to security.

anonymous FTP A File Transfer Protocol (FTP) server that accepts unknown visitors. If improperly configured to allow both uploading and downloading, anonymous FTP sites are often compromised or hijacked and used to distribute illegal materials.

ANT A proprietary protocol owned by Garmin that is an open-access multicast sensor network technology. It uses the 2.4 GHz frequency band to support interactions between sensor devices and management devices (such as a smartphone).

antimalware An essential security application and an example of a host-based IDS (HIDS) that focuses on the detection and elimination of malware. It provides both preventive and correction security controls. It monitors the local system for evidence of malware in memory, in active processes, and in storage. Aka antivirus.

antivirus *See* antimalware.

Anything as a service (XaaS) The catchall term to refer to any type of computing service or capability that can be provided to customers through or over a cloud solution/model.

API attacks Malicious usages of software through its API. This includes injection attacks, XSS, CSRF, SSRF, buffer overflows, race conditions, replay attacks, and request forgeries.

API *See* application programming interface (API).

APIPA *See* Automatic Private IP Addressing (APIPA).

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

AppleTalk A suite of protocols developed by Apple for networking of Macintosh systems, originally released in 1984. Support for AppleTalk was removed from the Apple operating system as of the 2009 release of Mac OS X v10.6.

appliance A term used to describe a hardware device designed and deployed for a specific purpose, such as firewalls, routers, switches, wireless access points, and virtual private network (VPN) gateways.

appliance OS A stripped-down or single-purpose operating system (OS) that is typically found on network devices, such as firewalls, routers, switches, wireless access points, and virtual private network (VPN) gateways.

application cells A technology used to virtualize software applications so they can be ported to almost any operating system (OS). Aka application containers.

application firewall A device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a service and all users. It's intended to be an application-specific, server-side firewall to prevent application-specific protocol and payload attacks.

application hardening The task of imposing security on required applications and services. It involves removing what isn't needed and then securing the rest.

Application layer (layer 7 of the OSI) (1) The seventh layer of the OSI model. This layer deals with how applications access the network and describes application functionality, such as file transfers, messaging, and so on. *See also* Open Systems Interconnection (OSI). (2) The alternate name for the fourth layer of the TCP/IP model, which was originally Process.

application management A device management solution that limits which applications can be installed onto a device, force install apps, and enforce configuration settings. Aka application control.

application programming interface (API) An abstract interface to the services and protocols provided by an operating system. APIs allow application developers to bypass traditional web pages and interact directly with the underlying service through function calls. Although offering and using APIs creates tremendous opportunities for service providers, it also poses some security risks. Developers must be aware of these challenges and address them when they create and use APIs.

application-aware device A security device, such as a firewall, intrusion detection system (IDS), intrusion protection system (IPS), or proxy, that operates at a higher layer of the protocol stack to provide focused security filtering and analysis of the content of specific communications.

application-level firewall, application-layer firewall A firewall that operates at OSI layer 7, the Application layer, where it filters traffic for a specific application or service, such as a web proxy. Aka application-level gateway.

arbitrary code execution The ability to run any software on a target system. This ability is usually the focus of hacker exploits and attacks. *See also* remote code execution.

archive bit A file header flag that indicates that a file is either new or changed. The archive bit is a common feature on Windows file systems. Other OSs often use the change timestamp.

Arduino An open source hardware and software organization that creates single-board 8-bit microcontrollers for building digital devices.

Argon2 A key derivation function, sometimes referred to as a key stretching algorithm, that can be used to securely create password hashes.

arithmetic-logical unit (ALU) The "brain" of the CPU that performs the processing calculations.

armored virus Malicious code designed to be difficult to detect and remove.

ARO *See* annualized rate of occurrence (ARO).

arp A command used to display or manipulate the contents of the ARP cache.

ARP cache poisoning, ARP poisoning An attack where an attacker inserts bogus information into the ARP cache (the local memory store of discovered IP to MAC relationships). Aka ARP spoofing.

ARP *See* Address Resolution Protocol (ARP).

ARP table A table used by Address Resolution Protocol (ARP) that contains a list of known Transmission Control Protocol/Internet Protocol (TCP/IP) addresses and their associated media access control (MAC) addresses. The table is cached in memory so that ARP lookups don't have to be performed for frequently accessed TCP/IP and MAC addresses. *See also* media access control (MAC), Transmission Control Protocol/Internet Protocol (TCP/IP).

artifacts Any items of evidence left behind by a suspect when performing a criminal or otherwise violating activity.

artificial intelligence (AI) The science-fiction concept that a machine can think like a human. *See* machine learning.

assembly language A higher-level alternative to machine language code. Assembly languages use mnemonics to represent the basic instruction set of a CPU but still require hardware-specific knowledge.

asset Anything within an environment that should be protected. Any item used in a business task. The loss or disclosure of an asset could result in an overall security compromise, loss of productivity, reduction in profits, additional expenditures, discontinuation of the organization, and numerous intangible consequences.

asset management The process of keeping track of the hardware and software implemented by an organization.

asset owner The person who is responsible for classifying information for placement and protection within the security solution. The asset owner is typically a high-level manager who is ultimately responsible for asset protection. However, the asset owner usually delegates the responsibility of the actual data management tasks to a custodian. Aka system owner.

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

asset value (AV) A dollar value assigned to an asset based on actual cost and nonmonetary expenses.

assigning risk *See* transferring risk.

assignment *See* transfer/transference (as related to risk). *See also* other related terms: acceptance, risk tolerance, transfer/transference (as related to risk), avoidance, reducing risk, mitigation, rejecting risk, and ignoring risk.

assurance The degree of confidence that security needs are satisfied. Assurance must be continually maintained, updated, and reverified.

assurance procedure Formalized processes by which trust is built into the lifecycle of a system.

asymmetric cryptography, asymmetric cryptosystem *See* asymmetric encryption.

asymmetric encryption A form of encryption in which two keys must be used. One key is used to encrypt data, and the other is needed to decrypt the data. This is the opposite of symmetric encryption, in which a single key serves both purposes. *See also* asymmetric cryptography.

asymmetric key A form of cryptography that does not use symmetric keys. It either uses complex formulas to solve problems (such as Diffie–Hellman to generate/exchange symmetric keys) or uses key pair sets to provide digital signatures and digital envelopes. This latter form is aka public key cryptography.

asymmetric key algorithms A form of cryptography that provides key exchange solutions for symmetric cryptography.

asymmetric multiprocessing (AMP) A form of multiprocessing where the processors are often operating independently of each other. Usually each processor has its own OS and/or task instruction set. Under AMP, processors can be configured to execute only specific code or to operate on specific tasks (or vice versa, where specific code or tasks are allowed to run only on specific processors; this might be called affinity in some circumstances).

asynchronous communications A means of data transfer that relies on a stop and start delimiter bit to manage the transmission of data. Because of the use of delimiter bits and the stop and start nature of its transmission, asynchronous communication is best suited for smaller amounts of data. PSTN (public switched telephone network) modems are good examples of asynchronous communication devices.

asynchronous dynamic password token A token device that generates onetime passwords after the user enters a PIN in the token device. The PIN is provided by a server as a challenge, and the user enters the onetime password created by the token as the response.

asynchronous dynamic passwords Passwords generated as needed, often based on a random seed value.

asynchronous transfer mode (ATM) A cell-switching technology rather than a packet-switching technology like Frame Relay. ATM uses virtual circuits much like Frame Relay, but because it uses fixed-size frames or cells, it can guarantee throughput. This makes ATM an excellent WAN technology for voice and videoconferencing.

AT commands The instructions and commands used to control a modem and the resulting dial-up connection. AT is short for attention and is used at the start of every command line or instruction. Modems, fax machines, and MFPs all support AT commands.

atomicity One of the four required characteristics of all database transactions. A database transaction must be an "all-or-nothing" affair. If any part of the transaction fails, the entire transaction must be rolled back as if it never occurred.

attack The attempted exploitation of a vulnerability by a threat agent.

attack framework Collections of information about attacks, exploits, tactics, techniques, and threat agents that can be used as a guide to understand and interpret incidents, evidence, and indicators of compromise (IOCs) experienced by an organization.

attack surface The area that is exposed to untrusted networks or entities and that is vulnerable to attack.

attack vector *See* threat vector.

attacker Any person who attempts to perform a malicious action against a system. Aka adversary, threat agent, or threat actor.

attenuation Loss of signal strength over a distance of a copper cable or wireless transmission, caused by resistance and noise picked up from the environment. Attenuation is what limits the maximum use length of a copper cable and is one factor that limits the distance of wireless transmissions. Fiber-optic connections also experience attenuation in the form of transmission loss (weaker light over greater distance).

attestation The verification and validation of something as true and accurate.

attribute A column within a table of a relational database.

attribute-based access control (ABAC), attribute based access control A mechanism of assigning access and privileges to resources through a scheme of attributes or characteristics. The attributes can be related to the user, the object, the system, the application, the network, the service, time of day, or even other subjective environmental concerns. *See also* discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC, RoBAC, or role-BAC), and rule-based access control (RuBAC, Rule-BAC).

attributes Specific characteristics that are used to differentiate entities from one another as well as identify a specific entity.

audit A methodical examination or review of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or outright crimes.

audit trail The records created by recording information about user and/or system activities, events, and occurrences into a database or log file. Some common uses of audit trails include reconstructing an event, extracting information about an incident, and proving or disproving culpability.

auditing (1) The act of recording event information into an audit log or audit trail to make a historical record of user and system activities. (2) An inspection or evaluation of a process to determine whether an organization is following specific rules or guidelines.

auditor The person or group responsible for testing and verifying that the security policy is properly implemented and the derived security solutions are adequate.

augmented reality (AR) A visual computer overlay that adds information to the view of the real world seen by the observer/user.

authenticated cryptography mode A means to implement symmetric encryption sessions to ensure confidentiality as well as authenticity of the transmitted data. Examples include Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), Hash-based Message Authentication Code (HMAC), Galois/Counter Mode (GCM), Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC) (CCM), Carter–Wegman + Counter (CTR) (CWC), encrypt-then-authenticate-then-translate (EAX), Offset Codebook (OCB), Integrity Aware Parallelizable Mode (IAPM), Integrity Aware Cipher Block Chaining (IACBC), Extended Ciphertext Block Chaining (XCBC). *See* unauthenticated cryptography mode.

authenticated relay, authentication relay An email server that will only accept messages from users after they have successfully authenticated. *See* closed relay and open relay.

authenticated scan A security scanner is granted authenticated read-only access to the servers being scanned (typically via a user account) and can use this access to read configuration information from the target system and use that information when analyzing vulnerability testing results.

authentication The means of verifying that someone is who they say they are. There are various levels (factors) of authentication: single-factor, two-factor, three-factor, and

so on. For instance, under a Public Key Infrastructure (PKI) system, two-factor authentication can be achieved by using both a password and a smartcard containing a digital certificate. Authentication can also be achieved via the authentication mechanisms included in Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+), as well as more specialized protocols such as Kerberos.

authentication applications Software products that assist with logons. These can include credential managers as well as TOTP/HOTP apps.

authentication factor The item(s) presented by a subject to prove or verify their identity, such as passwords, token devices, smartcards, and biometrics.

Authentication Header (AH) One of the subprotocols of Internet Protocol Security (IPsec). AH performs the functions of authentication and link establishment. The Internet Protocol (IP) header protocol field value of AH is 51.

authentication management The oversight and enforcement of strong mechanisms of authentication.

authentication protocols Protocols used to provide the transport mechanism for logon credentials.

Authentication Service (AS) An element of the Kerberos Key Distribution Center (KDC). The AS verifies or rejects the authenticity and timeliness of tickets.

authenticity The security concept that data is authentic or genuine and originates from its alleged source. This is related to integrity, but it's more closely related to verifying that it is from a claimed origin.

authority A social engineering technique based on the concept that most people are likely to respond to authority with obedience.

authorization A process that ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity (in other words, subject). The collection of rights, permissions, and privileges that are assigned to users. It's what users are authorized to do within a secured infrastructure. Commonly represented by access control lists.

authorization to operate (ATO) Often related to government or military agencies or contractors, an ATO is the formal approval to perform business functions once compliance with a contract, standard, framework, or regulation is confirmed. An ATO is often issued for a limited period of time and can be lost or canceled by the approving authority at any time based on any significant change to the environment.

authorized entity A term used to denote the benign nature of the skilled individual. Aka ethical hacker. *See also* ethical hacking.

Authorizing Official (AO) An authorized entity who can evaluate an IT/IS system, its operations, and its risks, and potentially issue an ATO. Aka designated approving authority (DAA), Approving Authority (AA), Security Control Assessor (SCA), and Recommending Official (RA).

Automated Indicator Sharing (AIS) An initiative by the Department of Homeland Security (DHS) to facilitate the open and free exchange of IOCs and other cyberthreat information between the U.S. federal government and the private sector in an automated and timely manner (described as "machine speed").

automatic private IP address (APIPA), Automatic Private IP Addressing The address assigned automatically when DHCP fails to provide a dynamic address, typically found in use on Windows. APIPA assigns an IP address of 169.254.*x*.*y* (where *x* and *y* are selected randomly), uses the subnet mask of 255.255.0.0, but does not assign a default gateway or DNS server.

automatic rollover *See* hot rollover.

Autopsy A free-to-use graphical interface to The Sleuth Kit and other forensic tools. It is widely used by law enforcement, the military, and corporations to determined what happened on a compromised computer. It is designed to be easy to use, as wizards guide the operator through every operation. Autopsy can perform timeline analysis, hash filtering, keyword searches, evaluation of web/internet artifacts, data carving (i.e., damaged file recovery), and multimedia extraction, and it can scan for IOCs.

auxiliary alarm system A function that can be added to either local or centralized alarm systems. The purpose of an auxiliary alarm system is to notify local police or fire services when an alarm is triggered.

availability (1) The security service that provides protection for the use of a resource in a timely and effective manner. It is the assurance that authorized subjects are granted timely and uninterrupted access to objects. (2) The time period during which a resource can be accessed. Many networks limit users' ability to access network resources to working hours as a security precaution.

avalanche effect A feature of cryptographic hashing algorithms that ensures that small changes in the input produce large changes in the output.

avoidance In risk management, the process of selecting alternate options or activities that have less associated risk than the default, common, expedient, or cheap option. *See also* other related terms: acceptance, risk tolerance, assignment, transfer/transference (as related to risk), reducing risk, mitigation, rejecting risk, and ignoring risk.

awareness A prerequisite to actual security training. Its goal is to bring security to the forefront and make it a recognized entity for users. User awareness is considered an integral part of an organization's overall security posture; it may be the primary means of defense against difficult-to-defend-against attacks such as spear phishing.

B

backbone distribution system Provides wired connections between the equipment room and the telecommunications rooms, including cross-floor connections.

backdoor, back door An opening left in a program or software application (usually by the developer) that allows additional access to data. Typically, these are created for debugging purposes and aren't documented. Backdoors may be undocumented command sequences that allow individuals with knowledge of the backdoor to bypass normal access restrictions. Before the product ships, the developer backdoors should be closed and/or removed; when they aren't closed, security loopholes exist. A backdoor can also be a hacker-installed remote-access client. Aka maintenance hooks (when left behind by valid programmers).

background checks An investigative and research technique used to verify that a potential worker is qualified for a position and has no disqualifications.

backout contingency plan The process by which an organization will pull back from preparations, contracts, or agreements.

backup, backing up The process of saving or copying data to a (normally remote) location such as a backup server or external media. Also used to refer to the copy of data on a separate storage device.

backup contingency plan An alternate solution or response to be used if the primary plan fails or isn't as successful as planned.

badge An ID card. Any forms of physical identification and/or of electronic access control devices. *See* PIV.

bag and tag *See* collection of evidence.

baiting When an attacker drops USB sticks, optical discs, or even wallets in a location that a worker is likely to encounter them. The hope is the worker will plug the USB drive or insert the disc into a work computer where the malware will auto-infect the system. The wallet often has a note in it with a URL or IP address along with credentials. The hope is the victim will visit the site from a work computer and be infected by a drive-by-download event or be tricked by a phishing site.

bandwidth monitor A tool used to track the usage level of network connectivity. Such oversight can discover malware communications and track application/protocol/service usage levels, as well as user misuse of company resources.

bandwidth on demand A feature/benefit provided by service providers that allows clients to consume more bandwidth when needed and if the carrier network has the capacity. Such consumption is often charged at a much higher rate.

banner grabbing The process of capturing the initial response or welcome message from a network service. This technique is often used by port scanners and other vulnerability

scanners to identify the variant and version of a service running on a system by opening a connection to the service and reading the details provided on the response banner or welcome screen. Often the banner discloses the application's identity, its version information, and potentially much more.

barricades Physical security mechanisms. K-rails (often seen during road construction), large planters, zigzag queues, bollards, and tire shredders are all examples of barricades.

base antenna The standard straight or pole antenna, which is an omnidirectional antenna that can send and receive signals in all directions perpendicular to the line of the antenna itself. This is the type of antenna found on most base stations and some client devices. *See also* rubber duck antenna.

base+offset addressing An addressing scheme that uses a value stored in one of the CPU's registers as the base location from which to begin counting. The CPU then adds the offset supplied with the instruction to that base address and retrieves the operand from the computed memory location.

baseband, baseband technology A form of communication in which the cable or communication media is able to support only a single transmission at a time.

baseband radio The use of radio waves as a carrier of a single communication.

baseline configuration The initial implementation of a system that implements the standardized minimal level of security.

baseline reporting The act of evaluating the current implemented security when compared with the stated or claimed security baseline.

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

Bash A command-shell and scripting language found on Linux, Unix, macOS, and now even Windows systems. Bash scripts can be used to automate tasks and launch tools, utilities, and programs. Bash supports interactive commands via a shell or terminal window.

basic input/output system (BIOS) The operating system–independent primitive instructions that a computer needs to start up and load the operating system from disk. *See also* Unified Extensible Firmware Interface (UEFI).

basic rate interface (BRI) An ISDN service type that provides two B, or data, channels and one D, or management, channel. Each B channel offers 64 Kbps, and the D channel offers 16 Kbps.

basic service set identifier (BSSID) The name of a wireless network when in ad hoc or peer-to-peer mode (that is, when a base station or wireless access point isn't used).

bastion host, bastion A system specifically designed to withstand attacks. Often a firewall appliance is considered a bastion host.

BCP *See* business continuity planning (BCP).

Bcrypt An example of a key-stretching technology. Based on the Blowfish cipher, Bcrypt uses salting and includes an adaptive function to increase iterations over time. *See* key stretching. Compare with Password-Based Key Derivation Function 2 (PBKDF2).

beacon frame A type of wireless network packet that broadcasts the presence of the wireless network. This management frame contains various information such as the Service Set Identifier (SSID), beacon interval, time stamp, and so on.

BEC *See* business email compromise (BEC).

behavior In the context of object-oriented programming terminology and techniques, the results or output from an object after processing a message using a method.

behavior modification The goal of organizational training and awareness strategies toward improvement in policy compliance and avoiding risky activities.

behavior-based detection, behavioral-based detection An intrusion discovery mechanism used by IDS. Behavior-based detection finds out about the normal activities and events on your system through watching and learning. Once it has accumulated enough data about normal activity, it can detect abnormal and possible malicious activities and events. Aka statistical intrusion detection, anomaly detection, and heuristics-based detection. *See also* anomaly-based detection, heuristic-based detection, and signature-based detection.

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

benchmark A documented list of requirements that is used to determine whether a system, device, or software solution is allowed to operate within a secure management environment. Aka secure configuration guide. *See also* standard and baseline.

benign DoS A denial of service (DoS) that occurs when a service is running on insufficient resources, when there has been an unforeseen popularity or traffic spike, or when something about the supporting system fails, such as drive loss, network link drop, or a corrupted configuration. This type of DoS occurs through no direct or intentional malign action on the part of an adversary. It is due to innocent events, unexpected conditions, or mistakes on the part of the owners/operators.

best evidence rule A rule that states that when a document is used as evidence in a court proceeding, the original document must be introduced. Copies will not be accepted as evidence unless certain exceptions to the rule apply.

beyond a reasonable doubt The standard of evidence in a criminal court case.

BIA *See* business impact analysis (BIA).

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

big data The phrase used to refer to collections of data that have become so large that traditional means of analysis or processing are ineffective, inefficient, and insufficient. Big data involves numerous difficult challenges, including collection, storage, analysis, mining, transfer, distribution, and results presentation.

binary mathematics The rules of computation of bits and bytes used by a computer. Aka Boolean mathematics.

bind variable A placeholder for SQL literal values, such as numbers or character strings.

biometric factors Characteristics of any person that can be used to identify or authenticate the person. Physiological biometric methods include fingerprints, face scans, retina scans, iris scans, palm scans, hand geometry, and voice patterns. Behavioral biometric methods include signature dynamics and keystroke patterns.

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

BIOS (Basic Input/Output System) The basic low-end firmware or software embedded in the hardware's electrically erasable programmable read-only memory (EEPROM). *See also* Unified Extensible Firmware Interface (UEFI).

birthday attack An attack in which the malicious individual seeks to substitute a digitally signed communication with a different message that produces the same message digest, thereby maintaining the validity of the original digital signature. This is based on the statistical anomaly (aka birthday paradox) that in a room containing 23 people, the probability of two or more people having the same birthday is greater than 50 percent. Aka collision attack or reverse hash matching.

bit, bits The individual binary values, 1s and 0s, that are used to communicate information over a network in the Physical layer (layer 1).

bit flipping The activity of changing a bit to its opposite value. A technique commonly used in fuzzing to slightly modify input data. *See* fuzz testing.

bit size The number of binary digits or bits in a value, such as a key, block size, or hash value.

black box (1) This term is deprecated. *See* unknown environment. (2) In relation to phreaking, a device used to manipulate line voltages to steal long-distance services.

black hat This term is deprecated. *See* unauthorized entity.

black-box testing This term is deprecated. *See* unknown environment testing.

blacklist This term is deprecated. *See* blocklist.

blackout A complete loss of power.

blind FTP A configuration of File Transfer Protocol (FTP) in which a folder or the entire site is set so that visitors can upload files but are unable to read or download them. The folder(s) are set to write-only. This prevents an FTP site from being used as a file exchange site by hackers but still allows files to be submitted to the site owner.

blind SQL injection A means to conduct a SQL injection attack even when there is no ability to view the results directly.

block cipher A symmetric encryption algorithm that converts a fixed-length block of plaintext into an equally fixed-length block of encrypted text (ciphertext).

blockchain A collection or ledger of records, transactions, operations, or other events that are verified using hashing, timestamps, and transaction data. Each time a new element is added to the record, the whole ledger is hashed again. *See* public ledger.

blocklist A security stance that allows everything by default and denies by exception. Aka deny list.

Blowfish A type of symmetric encryption in the form of a 64-bit block cipher, created by Bruce Schneier in 1993, that uses variable-length keys ranging from a relatively insecure 32 bits to an extremely strong 448 bits. It's now considered a reasonably secure encryption algorithm. A more recent alternative is the 128-bit Twofish algorithm.

Blue team The group defined as the defenders in a penetration test or security assessment exercise. *See* red team, white team, and purple team.

bluebugging An attack that grants hackers remote control over the hardware and software features and functions of a Bluetooth device. This could include the ability to turn on the microphone to use the phone as an audio bug.

bluejacking The process of sending messages to Bluetooth-capable devices without the permission of the owner/user.

bluesmacking A denial-of-service (DoS) attack against a Bluetooth device.

bluesnarfing An attack that allows hackers to connect with your Bluetooth devices without your knowledge and extract information from them. This form of attack can offer attackers access to your contact lists, your data, and even your conversations.

bluesniffing Eavesdropping or packet-capturing Bluetooth communications.

Bluetooth (IEEE 802.15) A 2.4 GHz wireless protocol used to pair devices together to support communications and control.

Bluetooth Low Energy (Bluetooth LE, BLE), Bluetooth Smart A low-power consumption derivative of standard Bluetooth. BLE was designed for Internet of Things, edge/fog devices, mobile equipment, medical devices, and fitness trackers. It uses less power while maintaining

a similar transmission range to that of standard Bluetooth. Standard Bluetooth and BLE are not compatible, but they can coexist on the same device.

boink A type of denial-of-service attack (DoS). *See also* denial-of-service (DoS) attack.

bollard A physical security mechanism designed to prevent vehicles from driving into buildings or other secured areas. *See* barricades. Aka security bollard.

bonk A type of denial-of-service attack (DoS). *See also* denial-of-service (DoS) attack.

book cipher *See* running key cipher.

Boolean mathematics The rules used for manipulating the bits and bytes that form the nervous system of any computer. Aka binary mathematics.

boot attestation A feature of Unified Extensible Firmware Interface (UEFI) that aims to protect the local operating system by preventing the loading or installing of device drivers or an operating system that is not signed by a preapproved digital certificate. Aka secure boot.

boot sector The first sector of a hard disk, where the program that boots the operating system resides. Microsoft operating systems utilize a proprietary boot manager that resides in the master boot record (MBR); open source operating systems (such as Linux) frequently use the Linux loader (LiLo) or GRUB (GRand Unified Bootloader) boot manager. The boot sector is susceptible to threats such as a boot-sector virus that can load itself into memory prior to operating system (and therefore antivirus) startup. Aka master boot record (MBR).

boot security The protection of essential boot files and settings against corruption by malware. *See* Unified Extensible Firmware Interface (UEFI). *See* measured boot and secure boot.

boot-sector virus A virus that attaches itself to the boot sector of a hard drive and thus is loaded in memory when the drive is activated.

Border Gateway Protocol (BGP) A path vector routing protocol.

bot A malicious remote-control tool deployed on systems to create botnets. Also called a zombie or an agent. These tools can easily and quite effortlessly assimilate a work or personal computer into the botnet and add its resources (processing power, bandwidth, and so on) to the collective, which can be used to perform distributed denial-of-service (DDoS) as well as more sophisticated attacks.

bot herder A nickname for the owner or hacker controlling a botnet. Aka batmaster or handler.

botmaster The hacker who is in control of a botnet. Aka bot herder.

botnet A collection of computers (sometimes thousands or even millions!) across the internet infected by an agent and under the control of an attacker known as the botmaster.

bottom-up approach When the IT staff makes security decisions directly without input from senior management.

bounds The limits to the memory and resources a process can access.

breach The occurrence of a security mechanism being bypassed or thwarted by a threat agent.

Brewer and Nash model A security model designed to permit access controls to change dynamically based on a user's previous activity (making it a kind of state machine model as well). Aka Chinese Wall (deprecated), ethical wall, and cone of silence.

bridge A network device used to connect networks with different speeds, cable types, or topologies that still use the same protocol. A bridge is a layer 2 device.

bridge mode, bridge mode infrastructure A form of wireless access point deployment that is used to link two wired networks together over a wireless bridged connection.

Bridge Protocol Data Unit (BPDU) An STP frame transmitted every 2 seconds between root and bridge switches containing information about port status (i.e., up or down) and identity (i.e., MAC address).

bring your own device (BYOD) A policy allowing employees to connect their personally owned devices to an organization's network. While the devices are the property of their owners, organizational data stored on the devices is still an asset of the organization.

broadband, broadband technology A form of communication in which the cable or communication medium is able to support multiple transmissions at one time.

broadcast A communications transmission to multiple but unidentified recipients.

broadcast address The address that all devices within a given network grouping or container receive data on.

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

broadcast storm A flood of unwanted Ethernet broadcast network traffic.

broadcast technology A communication system based on or dependent on broadcasts rather than unicast signaling.

brouter A network device that first attempts to route and then defaults to bridging if routing fails. A brouter is a legacy networking device that does not seem to have been manufactured since the mid-2000s. You are unlikely to encounter this device in a real-world network, and it is unlikely to be mentioned on the exam.

brownout A period of prolonged low voltage.

browser helper object (BHO) An add-on or plug-in for a web browser used to expand features or add capabilities. Aka add-on, plug-in, and extension.

brute force, brute-force, brute-force attack An attack pattern characterized by a mechanical series of sequential or combinatorial inputs utilized in an automated attempt to identify security properties (usually passwords) in a given system. A type of password guessing/cracking attack that relies purely on trial and error and uses a select character set and an increasing length of password construction.

BSSID (basic service set identifier) *See* basic service set identifier (BSSID).

buffer overflow A vulnerability that can cause a system to crash or allow the user to execute shell commands and gain access to the system.

buffer overflow attack A type of attack that occurs when more data is put into a buffer than it can hold, causing it to overflow. This form of attack is often used to cause software to fail open, permitting the attacker to execute arbitrary code.

bug bounty A payment to programmers, developers, and ethical hackers to discover a flaw in a service, site, product, system, device, etc. and responsibly and privately report it to the vendor. Many organizations now offer a bug bounty program where they are asking for the security community to locate and disclose issues to them in return for payment.

bumping A type of lock picking or lock bypass method that uses a modified key that is tapped into a lock.

bus topology A network structure that connects each system to a trunk or backbone cable. All systems on the bus can transmit data simultaneously, which can result in collisions.

business attack An attack that focuses on illegally obtaining an organization's confidential information. Aka corporate espionage or industrial espionage.

business case A documented argument or stated position in order to define a need to make a decision or take some form of action.

business continuity planning (BCP) A contingency planning process that allows a business to keep running in the event of a disruption to vital resources. The assessment of a variety of risks to organizational processes, the impact those risks might have on the organization if they were to occur, and the development of response scenarios to those concerns.

business email compromise (BEC) A spear phishing attack often focused on convincing members of accounting or financial departments to transfer funds, pay invoices, or purchase products from a message that appears to originate from a boss, manager, or executive. Aka invoice scam, CEO fraud, and CEO spoofing.

business impact analysis (BIA) *See* business impact assessment (BIA).

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

business partners agreement (BPA) A contract between two entities dictating their business relationship. It clearly defines the expectations and obligations of each partner in the endeavor.

BYOD (bring your own device) A policy that allows employees to bring their own personal mobile devices to work and then use those devices to connect to (or through) the company network to business resources and/or the internet.

C

CA *See* certificate authority (CA).

cable lock A combination or key lock that has a tethering cable to secure portable devices to immovable objects.

cable plant management policy The policy governing the collection of interconnected cables and intermediary devices (such as cross-connects, patch panels, and switches) that establish the physical network.

CAC *See* common access card (CAC).

cache (1) The high-speed small-volume memory chips of a CPU, often referenced as level 1 (L1)–L4 cache. (2) The in-memory store of network information, such as the ARP cache and DNS cache. (3) The temporary files of applications, such as document editors and web browsers.

cache RAM A process that takes data from slower devices and temporarily stores it in higher-performance devices when its repeated use is expected.

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

California Consumer Privacy Act (CCPA) California's privacy legislation, modeled after the European Union's GDPR.

callback A feature of dial-up remote access servers that hangs up on a client after initial connection and then calls the client on either a preconfigured number (secure) or a user-defined number (insecure, but reverses toll charges).

Caller ID A feature of phone systems that displays the supposed phone number or identity of the caller. This information is easily spoofed.

campus area network (CAN) A network that spans a college campus, university grounds, or multibuilding office complex or business park.

candidate key A subset of attributes, columns, or fields that can be used to uniquely identify any record in a table. Aka alternate key.

candidate screening Evaluating an applicant for a specific position based on the sensitivity and classification defined by the job description—that is, background checks.

cantenna A type of unidirectional wireless antenna that is constructed from a tube (such as a potato chips can) with one sealed end.

capability list, capabilities list Each row of an access control matrix is a capability list. A capability list is tied to the subject; it lists valid actions that can be taken on each object.

Capability Maturity Model (CMM) A formal software development management concept that describes the process that organizations undertake as they move toward incorporating solid engineering principles into their software development processes. Aka software capability maturity model (SCMM, S-CMM).

capability table A subject-focused table that identifies privileges assigned to subjects. It identifies the actions or functions that each subject can perform on each object.

capacitance motion detector A device which senses changes in the electrical or magnetic field surrounding a monitored object.

CAPTCHA A mechanism to differentiate between humans and software robots, with a backronym of "Completely Automated Public Turing test to tell Computers and Humans Apart."

captive portal An authentication technique that redirects a newly connected wireless web client to a portal access control page. The portal page may require the user to input payment information, provide logon credentials, or input an access code.

capture filter The set of rules to govern which frames are saved into the capture file or buffer and which are discarded by a network sniffer. *See* display filter.

capture the flag A challenge or verification technique often used in penetration testing as a test to see how far into a secured environment can the simulated intruder get before being stopped by the security infrastructure or detected by a user.

card cloning The duplication or skimming of data from a targeted source card, writing it onto a blank new card. Can be used against credit cards, ID cards, and SIMs.

cardinality The number of rows in a relational database.

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

Carrier-Sense Multiple Access (CSMA) A LAN media access technology that does not directly address collisions. If a collision occurs, the communication would not have been successful, and thus an acknowledgment would not be received. This causes the sending system to retransmit the data and perform the CSMA process again.

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) A LAN media access technology that attempts to avoid collisions by granting only a single permission to communicate at any given time. This system requires designation of a primary system, which responds to the requests and grants permission to send data transmissions.

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) A LAN media access technology that responds to collisions by having each member of the collision domain wait for a short but random period of time before starting the process over. Unfortunately, allowing collisions to occur and then responding or reacting to collisions causes delays in transmissions as well as a required repetition of transmissions. This results in about 40 percent loss in potential throughput.

carrier unlocked, carrier unlocking The status of a mobile device that can be used on any compatible telco network rather than being tied to the original network carrier.

cascading A composition theory which states that input for one system comes from the output of another system.

CAST *See* Carlisle Adams and Stafford Tavares (CAST).

cat A command that displays a file to the screen. It can suppress empty/blank lines, number each displayed line, and indicate the end of each line with a $.

CBC (Cipher Block Chaining) *See* Cipher Block Chaining (CBC).

CC *See* Common Criteria (CC).

CCE *See* Common Configuration Enumeration (CCE).

CCMP *See* Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).

cell suppression The act of suppressing (or hiding) individual data items inside a database to prevent aggregation or inference attacks.

cellular, cellular network The primary communications technology that is used by many mobile devices, especially cell phones and smartphones. The network is organized around areas of access called cells, which are centered around a primary transceiver, known as a cell site, cell tower, or base station.

Center for Internet Security (CIS) An organization that provides OS, application, and hardware security configuration guides for a wide range of products. Their mission is to "identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace."

central processing unit (CPU) *See* processor (1).

central station system The alarm is usually silent locally, but off-site monitoring agents are notified so that they can respond to the security breach. Most residential security systems are of this type. Most central station systems are well-known or national security companies, such as Brinks and ADT. *See* proprietary system (alarm).

centralized access control A form of access control in which authorization verification is performed by a single entity within a system. *See* decentralized access control and distributed access control.

centralized alarm system An alarm system that signals a remote or centralized monitoring station when the alarm is triggered.

centralized management Describes a system in which management and administration tasks occur in one or few locations within an environment.

CER (CERtificate) A file extension (`.cer`) that can be used to store a Distinguished Encoding Rules (DER) or Privacy-Enhanced Mail (PEM)–formatted certificate. An alternate form of `.crt`.

certificate A CA-endorsed or -signed copy of a subject's public key that verifies their identity.

certificate A digital entity that establishes who you are (providing nonrepudiation). It contains your name and other identifying data. Aka digital certificate.

certificate authority (CA) An entity that authenticates and distributes digital certificates.

certificate chaining Establishing a chain of trust within a single system or within a private network environment. A common example is the linking of the root certificate authority (CA) to a first level of intermediate CA, and potentially that CA to other intermediate CAs at other levels, then to the bottom-level leaf CA, and finally to the end-user entity.

certificate hold Another term for certificate suspension. *See also* suspension (certificate suspension).

certificate path validation (CPV) Each certificate in a certificate path from the original start or root of trust down to the server or client in question is valid and legitimate.

certificate policies, certificate policy Policies governing the use of certificates. This document sets the rules of use and behavior for customers/end users who are implementing certificates issued by a certificate authority. This policy typically identifies the violations that will result in certificate revocation.

certificate practice statement (CPS) The principles and procedures employed in the issuing and managing of certificates.

certificate revocation list (CRL) The list of certificates that have been revoked by a certificate authority before the lifetimes of the certificates have expired. *See also* Online Certificate Status Protocol (OCSP).

certificate revocation The act of making a certificate invalid. The cancellation of a certificate. Adding the serial number of a certificate to the CRL.

certificate signing request (CSR) The message sent to a certificate authority from a registration authority (RA) on behalf of a user or organization to request and apply for a digital certificate. A CSR often follows the PKCS#10 specification or the Signed Public Key and Challenge (SPKAC) format. It is a formal instruction from an RA to the certificate authority (CA) to actually build, sign, and issue a certificate to the requested subject.

certificate stapling *See* OCSP stapling.

certificate trust list (CTL) *See* trust list.

certificate-based authentication A reliable mechanism for verifying the identity of devices, systems, services, applications, networks, and organizations.

certification The act of passing one or more exams to earn certification credentials (and impressive acronyms to add to your résumé), which verify that you possess certain knowledge, skills, and expertise.

CGI *See* Common Gateway Interface (CGI).

chain of custody A document associated with legal evidence that tracks the people in authoritative control over the evidence between the moment it's discovered and when it's presented in court. Aka chain of evidence.

chain of evidence The process by which an object is uniquely identified in a court of law. Aka chain of custody.

Challenge-Handshake Authentication Protocol (CHAP), Challenge Handshake Authentication Protocol A protocol that challenges a system to verify its identity. CHAP is an improvement over Password Authentication Protocol (PAP), in which one-way hashing is incorporated into a multistep, nonrepeatable challenge-response handshake.

challenge-response A type of authentication in which the server generates and issues a random number challenge to the connecting client. The client uses the challenge number and the hash of the user's password (or other authentication factor) to generate a response.

change approval board (CAB) A group that evaluates proposed changes before approving or denying implementation.

change control *See* change management.

change documentation The process of writing out the details of changes to be made to a system, a computer, software, a network, and so on before they're implemented.

change management A process that helps prevent unintended outages. Before personnel make a configuration change to a system, they submit a change request. Other personnel review the change. If approved, the change is tested, implemented, and documented.

channel overlaps The overlapping of wireless networking channels that causes interference. Wi-Fi band/frequency selection should be based on the purpose or use of the wireless network as well as the level of existing interference.

channel service unit/data service unit (CSU/DSU) A border connection device that converts LAN signals into the format used by the WAN carrier network, and vice versa.

channels Subdivisions of wireless frequencies. Aka wireless channels.

CHAP *See* Challenge-Handshake Authentication Protocol (CHAP).

checklist test A process in which copies of the disaster recovery checklists are distributed to the members of the disaster recovery team for their review.

checksum A type of hash function used to confirm the integrity of network communications. Most protocols include a checksum in their header (although Ethernet stores it in a footer).

chief information officer (CIO) The leadership position that focuses on ensuring information is used effectively to accomplish business objectives.

chief information security officer (CISO) The leader of the InfoSec team who reports directly to senior management. *See also* chief security officer (CSO) and information security officer (ISO).

chief security officer (CSO) This term is sometimes used as an alternative to CISO, but in many organizations the CSO position is a subposition under the CISO and focuses on physical security. *See also* information security officer (ISO) and chief information security officer (CISO).

chief technical officer (CTO) The leadership position that focuses on ensuring that equipment and software work properly to support the business functions.

Children's Online Privacy Protection Act (COPPA) A law in the United States that places specific demands on websites that cater to children or knowingly collect information from children.

`chmod` A command used to manipulate *nix file permission settings. This command can be used to edit or replace file permissions for the owner, group, and/or world. It can use letter syntax or octal syntax.

choose your own device (CYOD) A mobile device management approach that provides users with a list of approved devices from which to select the device to implement. CYOD can be implemented so that employees purchase their own devices from the approved list (a bring your own device [BYOD] variant) or the company can purchase the devices for the employees (a company-owned, personally enabled [COPE] variant).

chosen ciphertext attack An attack in which the attacker has the ability to decrypt chosen portions of the ciphertext message.

chosen plaintext attack An attack in which the attacker has the ability to encrypt plaintext messages of their choosing and then analyze the ciphertext output of the encryption algorithm.

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

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

Cipher Block Chaining (CBC) A symmetric mode of operation that is used to prevent the creation of duplicate ciphertext blocks. This is accomplished by adding an initialization vector (IV) into the operation of encryption. The IV is integrated with the first block using a logical XOR operation. The result is then encrypted using the selected secret key. The ciphertext of the first block is then used as the IV for the second block. This linking or chaining of the blocks for use as an IV ensures that every block results in ciphertext that is unique. *See also* Electronic Code Book (ECB), Counter Mode (CTR), and Galois Counter Mode (GCM).

Cipher Feedback (CFB) A mode in which the algorithm is used to encrypt the preceding block of ciphertext. This block is then XORed with the next block of plaintext to produce the next block of ciphertext.

cipher suite A standardized collection of key exchange, digital signature, symmetric encryption, and hashing algorithms used to set or define the parameters for a security network communication. Most often this term is used in relation to Transport Layer Security (TLS) connections.

cipher text, ciphertext Encrypted data. A message that has been encrypted for storage or transmission.

ciphertext-only attack An approach to compromise encryption when the only information you have at your disposal is the encrypted ciphertext message.

circuit-level firewall A firewall that filters traffic around a circuit (i.e., communication session or connection) rather than around only a specific application or protocol. Typically, a circuit-level gateway functions at layer 4 or 5 of the Open Systems Interconnection (OSI) model. Aka circuit-level gateway, circuit-level gateway firewall, and circuit proxies.

circuit switching A dedicated physical pathway is created between the two communicating parties.

CISO *See* chief information security officer (CISO).

civil laws Laws that form the bulk of the body of laws in the United States. They are designed to provide for an orderly society and govern matters that are not crimes but that require an impartial arbiter to settle disputes between individuals and organizations.

Clark–Wilson model A model that employs limited interfaces or programs to control and maintain object integrity. It uses a three-part relationship of subject/program/object (or subject/transaction/object) known as a triple or an access control triplet.

class In the context of object-oriented programming terminology and techniques, a collection of common methods from a set of objects that defines the behavior of those objects.

classification A label that is applied to a resource to indicate its sensitivity or value to an organization and therefore designate the level of security necessary to protect that resource.

classification level Another term for a security label. An assigned importance or value placed on objects and subjects.

classification The process of labeling objects (assets, data, information, and so on) with sensitivity labels, and subjects (users) with clearance labels.

classified A label generally used to refer to any data that is ranked above the sensitive but unclassified level in the government/military classification scheme.

Classless Inter-Domain Routing (CIDR) CIDR provides for a subnet masking notation that uses mask bit counts rather than a full dotted-decimal notation subnet mask. Thus,

instead of 255.255.0.0, a CIDR notation is added to the IP address after a slash, as in 172.16.1.1/16, for example.

clean power Nonfluctuating pure power.

clean-desk policy, clean desk policy A policy used to instruct workers how and why to clean off their desks at the end of each work period. In relation to security, such a policy has a primary goal of reducing disclosure of sensitive information.

cleanup The process of removing any lingering hacking tools, sensors, or devices left behind during the various stages of the penetration test.

clearance level A classification assigned to a subject.

clearing A method of sufficiently deleting media that will be reused in the same secured environment. Clearing involves overwriting data with new data. Aka overwriting.

CLI *See* command-line interface (CLI).

clickjacking A web page–based attack that causes a user's click to link someplace other than the user intended. This is often accomplished by using hidden or invisible layovers, frame sets, or image maps.

Click-through license agreement, click-wrap license agreement A software agreement in which the contract terms are either written on the software box or included in the software documentation. During the installation process, you are required to click a button indicating that you have read the terms of the agreement and agree to abide by them.

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, client/server model 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. *See* distributed architecture.

client-side attack Any attack that is able to compromise a client, as opposed to the more common server-side attack.

clipping level A threshold value used in violation analysis auditing. Crossing the clipping level triggers the recording of relevant event data to an audit log.

closed head system *See* wet pipe system.

closed relay An SMTP server that is locked down so that it only accepts outbound messages from local systems. *See* authenticated relay and open relay.

closed source A solution where the source code and other internal logic is hidden from the public. *See* open source.

closed system A system designed to work well with a narrow range of other systems, generally all from the same manufacturer. The standards for closed systems are often proprietary and not normally disclosed. *See* open system.

closed-circuit television (CCTV) A security camera system that resides inside an organization's facility and is usually connected to monitors for the security guards to view as well as to a recording device. Typically deployed with its own isolated cabling rather than being integrated into the IP network (as is the case with IP, web, or typical security cameras).

cloud access security broker (CASB) A security policy enforcement solution that may be installed on premises or may be cloud based.

cloud computing A concept of computing where processing and storage are performed elsewhere (i.e., remotely) over a network connection rather than locally. Cloud computing can be thought of as internet-based computing.

Cloud Control Matrix (CCM) A cybersecurity framework from the Cloud Security Alliance (CSA) for cloud environments.

cloud models The various forms of cloud services or offerings, often labeled "as a service." *See* security as a service (SECaaS), anything as a service (XaaS), software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

Cloud Security Alliance (CSA) A not-for-profit group that focuses on promoting security best practices in relation to cloud computing.

cloud service provider (CSP) A company that operates a cloud service. *See* crypto service provider (CSP).

cloud services license agreement A click-through license performed through a web browser while activating a cloud service.

cloud shared responsibility model (CSRM) The concept that when an organization uses a cloud solution, there is a division of security and stability responsibility between the provider and the customer.

cloud solution The deployment concept where an organization contracts with a third-party cloud provider.

cloud storage The idea of using storage capacity provided by a cloud vendor as a means to host data files for an organization. Cloud storage can be used as a form of backup or support for online data services.

cloud-based federation A single sign-on solution that uses a third-party service to share federated identities.

clustering A method of balancing loads and providing fault tolerance.

CMOS *See* complementary metal-oxide-semiconductor (CMOS).

coax *See* coaxial cable.

coaxial cable A form of copper cable that is no longer in widespread use for networking because it has been replaced by unshielded twisted pair (UTP), shielded twisted pair (STP), fiber-optic cables, or wireless. Coaxial cable used for networking is known as 10Base2 and 10Base5. A cable with a center core of copper wire surrounded by a layer of insulation and then by a conductive braided shielding and finally encased in an insulation sheath. Coaxial cable is fairly resistant to electromagnetic interference (EMI), has a low cost, and is easy to install.

COBIT *See* Control Objectives for Information and Related Technology (COBIT).

code, codes Cryptographic systems of symbols that represent words or phrases and are sometimes secret, but are not necessarily meant to provide confidentiality. *See also* cipher.

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

code injection A general class of attacks that seek to insert attacker-written code into the legitimate code created by a developer. Any environment that inserts user-supplied input into code written by an application developer may be vulnerable to a code injection attack. *See* injection attack.

code repository, code repositories Software development is a collaborative effort, and large software projects require teams of developers who may simultaneously work on different parts of the code. Code repositories act as a central storage and management point for developers to place their source code.

code reuse The inclusion of preexisting code in a new program.

code review A form of vulnerability assessment where flaws in code or errors in logic are detected by combing through source code.

code signing The activity of crafting a digital signature of a software program to confirm that it was not changed and who it is from.

code signing certificate A type of certificate used to verify the source of source code or compiled code. It is a means for a programmer, developer, or vendor to prove the authenticity and integrity of their software solutions.

cognitive password A variant of the password authentication factor that asks a series of questions about facts or predefined responses that only the subject should know.

cohesive, cohesiveness An object is highly cohesive if it can perform a task with little or no help from other objects. Highly cohesive objects are not as dependent on other objects as objects with lower cohesion. Objects with higher cohesion are often better. Highly cohesive objects perform tasks alone and have low coupling.

cold aisle *See* hot and cold aisles.

cold rollover A fault-tolerance configuration that requires an administrator to perform some change in software or hardware configuration to switch the traffic load over from the down primary to a secondary server. Aka manual rollover.

cold site A physical site (designated as a recovery location) that has few to none of the resources necessary to enable an organization to use it if the main site is inaccessible, destroyed, or otherwise experiencing a disaster.

collection of evidence The procedure of securing evidence by collecting it. Basically, evidence is gathered, placed in a container, and labeled, and then its chain-of-custody document is filled out. Aka bag and tag.

collector, security collector Any system that gathers data into a log or record file. A collector is similar to the functions of auditing, logging, and monitoring. A collector watches for a specific activity, event, or traffic, and then records the information into a record file. *See* sensor.

collision (1) The occurrence when the output of two cryptographic operations produce the same result. Collisions occur in relation to encryption operations as well as hashing operations. (2) When two devices attempt to communicate over the same baseband media.

collision attack *See* birthday attack.

collision domain A group of networked systems that could cause a collision if any two (or more) of the systems in that group transmitted simultaneously. Typically related to the Physical layer (OSI layer 1).

collusion An agreement between individuals to commit fraud, deceit, or otherwise perform an unauthorized or illegal action.

columnar transposition A form of cryptographic transposition based on arranging plaintext in a form that generates columns; then the columns are extracted as the ciphertext.

command and control (C&C) An intermediary serving as the locus of connection between an attacker and bots where commands are distributed and information is exchanged. Aka C2 or herder.

command-line interface (CLI) A computer or device interface that is limited to typed operations and text responses.

commercial business, private-sector classification The security labels commonly employed on secure systems used by corporations. Common corporate or commercial security labels are confidential, proprietary, private, sensitive, and public.

commercial-off-the-shelf (COTS) Software used by organizations that is not developed internally but purchased from third-party vendors.

committed information rate (CIR) A contracted minimum guaranteed bandwidth allocation for a virtual circuit.

common access card (CAC) The smartcard used by the U.S. government and military for authentication purposes. Although the CAC name was assigned by the Department of Defense (DoD), the same technology is widely used in commercial environments. This smartcard is used to host credentials, specifically digital certificates, that can be used to grant access to a facility (i.e., ID badge) or to a computer terminal (i.e., smartcard).

Common Body of Knowledge (CBK) The areas of information prescribed by (ISC)^2 as the source of knowledge for the CISSP exam.

Common Configuration Enumeration (CCE) Security Content Automation Protocol (SCAP) component that provides a naming system for system configuration issues.

Common Criteria (CC) The loosely used phrase for the combination of the Common Criteria for IT Security Evaluation (CC) and the Common Methodology for IT Security Evaluation (CEM). Together these form the Common Criteria Recognition Agreement (CCRA). Simplified, this provides a means via the Common Criteria certification process for independently evaluating products in licensed labs and providing a level of assurance regarding product security. Defined in ISO/IEC 15408.

Common Gateway Interface (CGI) A rule set for hosting applications or scripts via a web server. CGI scripts are often written in the Perl programming language and can offer dynamic content to websites. This is often an attack vector for hackers who look for vulnerabilities in the CGI code.

common mode noise Electromagnetic interference (EMI) noise generated by the difference in power between the hot and ground wires of a power source or operating electrical equipment.

common name (CN) An element of a certificate that can hold only a single name. This can be a name with a wildcard or a non-wildcard name.

Common Object Request Broker Architecture (CORBA) An international standard for distributed computing. CORBA enables code operating on a computer to locate resources located elsewhere on the network.

Common Platform Enumeration (CPE) Security Content Automation Protocol (SCAP) component that provides a naming system for operating systems, applications, and devices.

common router Aka packet-filtering firewall. *See also* packet filtering.

common virus *See* virus.

Common Vulnerabilities and Exposures (CVE) (1) An element of SCAP that assigns standardized identifiers and a naming convention to publicly known system vulnerabilities to be used for cross-link and cross-referencing purposes. (2) A vulnerability database hosted at `cve.mitre.org`, which indexes and serves as a repository of information about threats, exploits, and attacks.

Common Vulnerability Scoring System (CVSS) An open framework for communicating the characteristics and severity of software vulnerabilities. A CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. CVSS is a Security Content Automation Protocol (SCAP) component that provides a standardized scoring system for describing the severity of security vulnerabilities.

communication disconnects Attacks that interrupt or interfere with communication sessions. *See* deauthentication and disassociation.

communications security The access control and protection issues involved in managing and administering remote access connections.

community cloud A cloud environment maintained, used, and paid for by a group of users or organizations for their shared benefit, such as collaboration and data exchange.

companion virus A variation of the file infector virus. A companion virus is a self-contained executable file that escapes detection by using a filename similar to, but slightly different from, a legitimate operating system file. Often, malware that borrows the root filename of a common executable (i.e., EXE) and then gives itself the `.com` extension in an attempt to get itself launched rather than the intended application.

company-owned, personally enabled (COPE) A mobile device management approach in which the organization purchases devices and provides them to employees. Each user is then able to customize the device and use it for both work activities and personal activities.

compartmentalized MAC environment A type of Mandatory Access Control (MAC) environment where there is no relationship between one security domain and another. Each domain represents a separate isolated compartment. To gain access to an object, the subject must have specific clearance for its security domain.

compartmented security mode A security mode in which systems process two or more types of compartmented information. All system users must have an appropriate clearance to access all information processed by the system but do not necessarily need to know all the information in the system.

compensation, compensating A type of access control that is deployed to provide various options to other existing controls to aid in enforcement and support of security policies. A compensation control can be an alternative (such as a hot site), a substitute (such as a failover server), or a resolution/recovery mechanism (such as a backup).

compensation access control A type of access control that provides various options to other existing controls to aid in the enforcement and support of a security policy.

competent A distinction of evidence that means that the evidence must be obtained legally. Evidence that results from an illegal search would be inadmissible because it is not competent.

compiled code Code converted to machine language using a compiler crafting an output executable.

compiled language A computer language that is converted into machine language before distribution or execution.

compiler A software development tool that converts higher-level language code into a machine language executable file designed for use on a specific operating system.

complementary metal-oxide-semiconductor (CMOS) The memory chip on a motherboard that stores the basic input/output system (BIOS) settings.

completeness Having all necessary components or parts in relation to integrity.

compliance The act of conforming to or adhering to rules, policies, regulations, standards, or requirements. Compliance is an important concern in security governance.

compliance testing Verification that a system complies with laws, regulations, baselines, guidelines, standards, best practices, and policies. This is an important part of maintaining security in any environment. Aka compliance checking or compliance checks.

Component Object Model (COM) Microsoft's standard for the use of components within a process or between processes running on the same system.

composition theories Other security models that fall into the information flow category build on the notion of inputs and outputs between multiple systems. They explain how outputs from one system relate to inputs to another system. There are three composition theories: cascading, feedback, and hookup.

comprehensiveness Being complete in scope; the full inclusion of all needed elements, in relation to integrity.

compromise If system security has been broken, the system is considered compromised.

computer architecture An engineering discipline concerned with the construction of computing systems from the logical level.

computer crime Any crime that is perpetrated against or with the use of a computer.

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

computer incident response team (CIRT) Another name for an emergency response team. The group of InfoSec workers who can respond to incidents and system problems.

Computer Security Act (CSA) of 1987 A U.S. law that mandates baseline security requirements for all federal agencies.

computer security incident A violation, or imminent threat of a violation, of a security policy or practice within the organization. Computer security incidents are the result of an attack, malware infection, or inappropriate usage by employees.

computer security incident response teams (CSIRTs) A dedicated team responsible for investigating any computer security incidents that take place. Aka cyber incident response teams (CIRTs) or incident response teams (IRTs).

computer-based training (CBT) Education delivered through a computer screen.

concealment The act of hiding or preventing disclosure.

concentrator *See* repeater.

conclusive evidence Incontrovertible evidence that overrides all other forms of evidence.

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

conditional access The concept of verifying the identity of the device before authenticating a user. A derivative of attribute-based access control, context-aware authentication, and the somewhere-you-are MFA attributes. Conditional access is often used in relation to cloud resources.

confidential A classification label used for data of a confidential nature. The classification label used to indicate the internally valuable and sensitive data of an organization. It may be described as proprietary or trade secret. Unauthorized disclosure of confidential data will have noticeable effects and cause damage to national security (if associated with the government) or significant damage (if associated with a private organization). This classification is used for all data between secret and unclassified classifications.

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

configuration compliance scanner A tool that quickly scans a system to check whether approved updates and patches are installed and whether the system is in compliance with security and general system configuration settings. Aka configuration review.

configuration management (CM) (1) The process of logging, auditing, and monitoring activities related to security controls and security mechanisms over time. This data is then used to identify agents of change, whether objects, subjects, programs, communication pathways, or even the network itself. (2) The administration of setting up and changing configurations, which ensures that systems are deployed in a secure consistent state and that they stay in a secure consistent state throughout their lifetime. (3) Aka software configuration management (SCM). The process used to control the version(s) of software used throughout an organization and formally track and control changes to the software configuration. It has four main components: configuration identification, configuration control, configuration status accounting, and configuration audit.

confinement, confinement property The principle that allows a process to read from and write to certain memory locations and resources only. This is an alternate name for the * (star) Security Property of the Bell–LaPadula model.

confusion A feature or function of a cryptographic algorithm to ensure that details about the key used during the encryption process are not disclosed in the ciphertext.

connection oriented Describes communications between two hosts that have a previous session established for synchronizing sent data. The receiving system acknowledges the data. This method allows for guaranteed delivery of data between systems. Within the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite, TCP is used for connection-oriented communication. A connection-oriented protocol such as TCP provides increased reliability but has more overhead and is therefore slower.

connectionless Describes 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 Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite, User Datagram Protocol (UDP) is used for connectionless communication. The advantage of a connectionless protocol such as UDP is increased speed; however, this comes with less reliability.

consensus A social-engineering technique based on the concept of taking advantage of a person's natural tendency to mimic what others are doing or are perceived as having done in the past. Aka social proof.

consistency One of the four required characteristics of all database transactions (the other three are atomicity, isolation, and durability). All transactions must begin operating in an environment that is consistent with all of the database's rules.

constrained data item (CDI) In relation to the Clark–Wilson model, any data item whose integrity is protected by the security model.

constrained interface An access control used in applications that restrict what users can do or see based on their assigned privileges. Subjects with restricted privileges have limited access. Aka restricted interface.

contactless payment methods A means of financial transaction that does not require direct physical contact between the mobile device and the point-of-sale (PoS) device. Some are based on NFC, others on RFID, some on SMS, and still others on optical camera–based solutions, such as scanning Quick Response (QR) codes. Mobile payments are convenient for the shopper but might not always be a secure mechanism.

container A virtualization tool used to host an application. *See* containerization.

container security The implementation of security measures at the container host as well as within the container itself.

containerization The next step in the evolution of the virtualization trend for both internally hosted systems and cloud providers and services. Containerization is based on the concept of eliminating the duplication of OS elements and removing the hypervisor altogether. Instead, each application is placed into a container that includes only the resources needed to support the enclosed application. There are many different technological solutions that are grouped into the concept of containerization. Some refer to the application instances as containers, zones, cells, virtual private servers, partitions, virtual environments, virtual kernels, or jails. Aka OS virtualization.

containment Often a reactive response to an incident where the offending item is cut off from causing further harm. The prevention of the spread of malicious code or intrusion attacks to other not-yet-affected systems.

contamination The result of mixing of data with a different classification level and/or need-to-know requirement.

content addressable memory (CAM) A table of MAC addresses and ports held in memory by a switch to manage Ethernet frame transmission.

content distribution network (CDN), content delivery network A collection of resource services deployed in numerous data centers across the internet in order to provide low latency, high performance, and high availability of the hosted content. CDNs provide the desired multimedia performance quality demanded by customers through the concept of distributed data hosts. Rather than having media content stored in a single central location to be transmitted to all parts of the internet, the media is distributed to numerous geographically distributed prestaging internet locations that are closer to groups of customers.

content inspection (content filtering) The security filtering function in which the contents of the application protocol payload are inspected.

content management, content management system (CMS) The control over mobile devices and their access to content hosted on company systems as well as controlling access to company data stored on mobile devices. Typically, a mobile content management (MCM) system is used to control company resources and the means by which they are accessed or used on mobile devices.

content-dependent access control A form of access control that restricts access to data based on the contents or payload of an object.

content-distribution networks (CDN), content delivery networks A collection of resource services deployed in numerous data centers across the internet in order to provide low latency, high performance, and high availability of the hosted content. CDNs provide the desired multimedia performance quality demanded by customers through the concept of distributed data hosts.

context analysis, contextual analysis The firewall feature that enables the system to retain knowledge of previous packets in a conversation to detect unwanted or malicious traffic that isn't noticeable or detectable when evaluating only individual packets.

context-aware authentication An authentication system that evaluates the origin and context of a user's attempt to access a system. It can include multiple elements such as the location of the user, time of day, type of connection, and endpoint device. Aka context-based authentication. *See* attribute-based access control (ABAC).

context-dependent access control A form of access control based on the context or surroundings of an object.

continuing education The ongoing training of employees, which should primarily focus on improving efficiency, productivity, and security compliance. However, it can also enable employees to improve their knowledge base and job skills to advance within the organization or leave to pursue other external opportunities.

continuity A goal an organization can accomplish by having plans and procedures to help mitigate the effects a disaster has on its continuing operations and to speed the return to normal operations.

continuity of operations plan (COOP) Actions and preventive measures taken to prevent downtime and maintain the availability of the production environment. Includes the creation of a security policy, BCP, DRP, and many other aspects of preparing for the worst and planning to avoid the consequences of downtime and data loss whenever possible. A COOP can be the combined results of BCP and DRP or a separate plan functioning as a guideline for other specific recovery efforts.

continuous integration/continuous delivery (CI/CD) A DevOps model where code may roll out dozens or even hundreds of times per day. This requires a high degree of automation, including integrating code repositories, the software configuration management process, and the movement of code between development, testing, and production environments.

contractual license agreement A written contract between the software vendor and the customer outlining the responsibilities of each.

control Anything used to implement security. Aka safeguard and security control. *See also* security control, safeguards, and countermeasures.

Control Objectives for Information and Related Technology (COBIT) A security concept infrastructure used to organize the complex security solution of companies. A framework that describes the common requirements that organizations should have in place surrounding their information systems.

control risk The risk that is introduced by the introduction of the countermeasure to an environment.

control The use of access rules or countermeasures to limit a subject's access to an object.

control zone The implementation of either a Faraday cage or noise generation or both to protect a specific area in an environment; the rest of the environment is not affected.

controls gap The amount by which risk is reduced by implementing safeguards. The difference between total risk and residual risk.

converged protocols The merging of specialty or proprietary protocols with standard protocols, such as those from the TCP/IP suite. Some common examples of converged protocols are FCoE, MPLS, iSCSI, and VoIP.

cookie A plaintext file stored on a computer that contains information about a user (and their preferences) for use by a website and/or database server. Although cookies are frequently used for various legitimate purposes, they can also be used by malicious websites to track user activities.

COPE (corporate-owned, personally enabled) *See* corporate-owned, personally enabled (COPE).

Copper Distributed Data Interface (CDDI) Deployment of FDDI using twisted-pair (in other words, copper) wires. This reduces the maximum segment length to 100 meters and is susceptible to interference.

copyright Intellectual property law that guarantees the creators of "original works of authorship" protection against the unauthorized duplication of their work.

corporate-owned A mobile device strategy where the company purchases mobile devices that can support compliance with the security policy. These devices are to be used exclusively for company purposes, and users should not perform any personal tasks on them.

corporate-owned mobile strategy (COMS) The mobile device policy where the company purchases the mobile devices that can support security compliance with the security policy and provides them to employees. Aka corporate-owned, business-only (COBO).

corporate-owned, business-only (COBO) *See* corporate-owned mobile strategy (COMS).

corporate-owned, personally enabled (COPE) A mobile device strategy where the organization purchases devices and provides them to employees. Each user is then able to customize the device and use it for both work activities and personal activities. COPE allows the organization to select exactly which devices are to be allowed on the organizational network—specifically only those devices that can be configured into compliance with the security policy. Aka company-owned, personally enabled.

corrective, corrective controls, corrective access controls A type of access control that modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred.

correlation engine A type of analysis system that reviews the contents of log files or live events. It is programmed to recognize related events, sequential occurrences, and interdependent activity patterns to detect suspicious or violating events.

cost/benefit analysis, cost/benefit calculation An evaluation to determine whether a safeguard actually improves security without costing too much.

counter A common element of many cryptographic modes of operation. A key feature of most counter modes is the ability to enable a standard block cipher to function more like a stream cipher. A great example of this is CCMP, which allows AES to be used as a stream cipher by WPA2.

Counter Mode (CTR) A symmetric mode of operation that is similar to Cipher Block Chaining (CBC) in that an additional value is added or incorporated into each block prior to encryption; the difference is that CTR does not use a random number and does not chain the blocks. Instead, CTR uses an independent counter, which both the sender and receiver have access to; each block uses a counter value as the initialization vector (IV), and then the counter is incremented for the next block. *See also* Electronic Code Book (ECB), Cipher Block Chaining (CBC), and Galois Counter Mode (GCM).

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) The combination of two block cipher modes to enable streaming by a block algorithm. CCMP can be used on many block ciphers. The AES-CCMP implementation was defined as part of WPA2, which replaced WEP and WPA, and is also used in WPA3 as the preferred means of wireless encryption. A wireless security solution used by WPA2 and WPA3 where it implements AES (Advanced Encryption Standard) as a stream cipher. Aka Counter-Mode/CBC-MAC Protocol.

Counter with Cipher Block Chaining Message Authentication Code Mode (CCM) A symmetric cipher mode that combines a confidentiality mode with a data authenticity process.

counterintelligence The actions that might be taken by a perpetrator to minimize relevant evidence or to misdirect an investigation. Aka anti-forensics.

countermeasure A response to a security issue; may be preventive, deterrent, detective, corrective, directive, recovery, or compensating. *See also* control, security control, and safeguards.

country code A two-letter top-level domain (TLD) used to associate a fully qualified domain name (FQDN) with a specific country, sovereign state, or dependent territory.

coupling The level of interaction between objects. Lower coupling means less interaction. Lower coupling delivers better software design because objects are more independent. Lower coupling is easier to troubleshoot and update. Objects with low cohesion require lots of assistance from other objects to perform tasks and have high coupling.

covert channel The means by which data can be communicated outside of normal, expected, or detectable methods. *See* covert storage channel and covert timing channel.

covert storage channel A channel that conveys information by writing data to a common storage area where another process can read it.

covert timing channel A channel that conveys information by altering the performance of a system component or modifying a resource's timing in a predictable manner.

CPE *See* Common Platform Enumeration (CPE).

CPS *See* certificate practice statement (CPS).

CPTED *See* crime prevention through environmental design (CPTED).

cracker A criminal hacker. Malicious entities intent on waging an attack against a person, organization, or system. Crackers may be motivated by greed, power, or recognition. Their actions can result in stolen property (data, ideas, and so on), disabled systems, compromised security, negative public opinion, loss of market share, reduced profitability, and lost productivity. *See also* hacker and unauthorized entity.

CRC *See* cyclic redundancy check (CRC).

credential harvesting The activity of collecting and stealing account credentials.

credential hijacking When an attacker steals and uses a victim's credentials. *See* impersonation and masquerading.

credential management The concept of storing a collection of logon credentials in a central secure location. Aka credential manager, password locker, and password vault.

credential management system A solution that provides a storage space for users to keep their credentials when single sign-on (SSO) isn't available. Users can store credentials for websites and network resources that require a different set of credentials. The management system secures the credentials with encryption to prevent unauthorized access.

credential policies A security policy used to define the requirements of authentication or full AAA for various subjects.

credential stuffing *See* spraying.

credentialed scan A type of security scan in which the logon credentials of a user or administrator are provided to the scanner in order for it to perform its work. A credentialed scan has the ability to provide more accurate information.

creeping privilege(s) The accumulation of user account privileges over time as job roles and assigned tasks change. *See also* privilege creep.

crime prevention through environmental design (CPTED) Guidelines that encourage architects and build-out designers to improve security through building elements. The concept of designing the structure of the physical environment and surroundings to influence individual decisions that potential offenders make before committing any criminal acts. This includes taking advantage of natural surveillance, access control, and territorial reinforcements.

criminal law Body of laws that the police and other law enforcement agencies enforce. Criminal law contains prohibitions against acts such as murder, assault, robbery, arson, theft, and similar offenses.

criminal syndicates Threat actor groups involved in cybercrime activities that may allow criminals to gain access, power, or money. Aka organized crime.

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

critical The classification label that indicates an asset is core and central to the operation of mission-critical business processes.

criticality prioritization The prioritization of mission-critical assets and processes during the creation of BCP/DRP.

criticality The level to which information is mission critical. The higher the level of criticality, the more likely the need to maintain the confidentiality of the information. High levels of criticality are essential to the operation or function of an organization.

CRL *See* certificate revocation list (CRL).

cross-certification A type of trust that occurs when a certificate authority (CA) from one organization elects to trust a CA from another. Aka bridge trust structure.

crossover error rate (CER) The point at which the false acceptance rate (FAR) equals the false rejection rate (FRR) when both are plotted on a graph evaluating errors versus sensitivity. This is the point from which performance is measured in order to compare the capabilities of different biometric devices. Devices with lower CERs are more accurate than devices with higher CERs.

cross-site request forgery (XSRF, CSRF) An attack that is similar in nature to cross-site scripting (XSS). However, with XSRF, the attack is focused on the visiting user's web browser more than the website being visited. The main purpose of XSRF is to trick the user or the user's browser into performing actions they did not intend or would not have authorized against a targeted server, system, or site. Aka client-side request forgery (CSRF).

cross-site scripting (XSS) A form of malicious code-injection attack in which attackers are able to compromise a web server and inject their own malicious code into the content sent to other visitors. A persistent XSS attack plants poisoned material on the website to be served to any future visitors. A reflective XSS attack places the malicious content in the request of the visitor, so the harmful response or result from the website is actually a reflection of the request. Direct object model (DOM)–based XSS attacks take advantage of vulnerabilities in the client-side browser rather than issues on the server side. Variations include reflected/reflective XSS, stored/persistent XSS, and DCOM XSS.

cross-training *See* job rotation.

cryptanalysis The study of methods to defeat codes and ciphers.

crypto malware, cryptomalware, crypto-malware Malware that uses system resources to mine cryptocurrencies. Often confused with ransomware. Aka crypto mining or crypto jacking.

crypto module A hardware or software component that can be used to provide cryptographic services to a device, application, and operation system. A crypto module may provide random number generation, perform hashing, perform encryption and decryption functions, and serve as a secure storage container for encryption keys. *See* HSM.

crypto service provider (CSP) A software library that implements standardized encryption functions, such as the Microsoft CryptoAPI (CAPI). *See* cloud service provider (CSP).

cryptocurrency Digital currency, often created or earned by performing complex mathematical operations or solving cryptographic challenges. Bitcoin is a common example.

cryptographic erasure A security measure where the encryption keys are destroyed in order to prevent data access. This concept does not directly erase or clear the data itself. The hope is that without the encryption key, access to the encrypted data will be impossible.

cryptographic key Cryptographic keys provide the "secret" portion of a cryptographic algorithm used to encrypt and decrypt data. *See* key. Aka cryptovariable.

cryptography Algorithms applied to data that are designed to ensure confidentiality, integrity, authentication, and/or nonrepudiation. The field of mathematics focused on encrypting and decrypting data.

cryptology The combination of cryptography and cryptanalysis.

cryptoshredding *See* cryptographic erasure.

cryptosystem System in which a shared secret key or pairs of public and private keys are used by communicating parties to facilitate secure communication.

cryptovariable Another name for the key used to perform encryption and decryption activities. *See* key. Aka cryptographic key.

CSO *See* chief security officer (CSO).

CSP *See* cloud service provider (CSP) or crypto service provider (CSP).

CSR (certificate signing request) The message sent to a certificate authority from a registration authority (RA), a user, or an organization to request and apply for a digital certificate.

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

CSU/DSU *See* channel service unit/data service unit.

Cuckoo, Cuckoo Sandbox An open source automated malware sandboxing and analysis solution. It can monitor OS API calls, track file manipulation, dump process memory, take screen shots of activities, and collect network traffic.

`curl` A command used to transfer data via URL over a wide range of protocols, such as DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, MQTT, POP3, POP3S, RTMP, RTMPS, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, Telnet, and TFTP.

custodian A person who has been assigned or delegated the day-to-day responsibilities of classifying and labeling objects and properly storing and protecting objects. The custodian is typically the IT staff or the system security administrator.

CVE *See* Common Vulnerabilities and Exposures (CVE).

CVSS *See* Common Vulnerability Scoring System (CVSS).

cyber kill chain The lifecycle of a cyberattack. It is used as a way to dissect or decompose an attack or intrusion to gain a better understanding of the adversary, the means of detecting the vulnerability, the development of the exploit, and the tactics used in performing the attack.

cyberphysical system, cyber-physical system A computer system that can interact with the real world, such as take measurements with a sensor, control lights, open doors, turn on motors, and so forth. *See* Internet of Things (IoT) and industrial control system (ICS).

Cybersecurity Framework (CSF) U.S. government guides for establishing and maintaining security crafted by National Institute of Standards and Technology (NIST), which is designed for critical infrastructure and commercial organizations. Aka NIST Cybersecurity Framework (CSF).

Cyclic redundancy check (CRC) An error-checking method in data communications that runs a formula against data before and after transmission. Similar to a hashing, a mechanism that indicates whether a message has been altered or damaged in transit. 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.

CYOD (choose your own device) *See* choose your own device (CYOD).

D

DAC *See* discretionary access control (DAC).

DAD triad Disclosure, alteration, and destruction make up the DAD Triad. The DAD Triad represents the failures of security protections in the CIA Triad.

daisy chaining The concept of attacking with a series of linked exploits.

dark web The part of the internet that is not accessible by a standard internet connection. Instead, special software is often required, such as TOR (see `torproject.org`), which can be used to redirect a web browser to content hosted on hidden servers.

darknet An unused portion of network space used to monitor for network-based attacks and traffic.

data acquisition The processes and procedures by which data relevant to a criminal action is discovered and collected.

data analytics The science of raw data examination with the focus of extracting useful information out of the bulk information set. The results of data analytics could focus on important outliers or exceptions to normal or standard items, a summary of all data items, or some focused extraction and organization of interesting information.

data at rest, data-at-rest Data stored statically on a storage device. Aka data on storage.

data child A term related to a hierarchical data structure in which the item is downward or further away from the root of the hierarchy compared to a data parent.

data circuit-terminating equipment (DCE) A networking device that performs the actual transmission of data over the Frame Relay as well as establishing and maintaining the virtual circuit for the customer.

data classification Grouping data under labels for the purpose of applying security controls and access restrictions.

data controller In the context of a data processor, as defined by EU data protection laws, the person or entity that controls processing of the data. The entity that makes decisions over the data they have collected and/or are collecting.

data custodian, data steward The subject who is assigned or delegated the task of implementing the prescribed protection defined by the security policy and upper management. The data custodian performs any and all activities necessary to provide adequate protection for data and to fulfill the requirements and responsibilities delegated to them by upper management.

Data Definition Language (DDL) The database programming language that allows for the creation and modification of the database's structure (known as the schema).

data dictionary Central repository of data elements and their relationships. Stores critical information about data usage, relationships, sources, and formats.

data diddling The act of making small changes to data, typically malicious in intent. A type of incremental attack.

data emanation Electrical emanations that occur when data, in the form of electrical signals, travels across a medium such as copper. This presents the threat of a form of electronic eavesdropping; an attacker can utilize sophisticated equipment to monitor these transmissions. Another more prevalent form of data emanation occurs in wireless networks, where the wireless signal is broadcast outside an organization's physical boundaries. One mitigation strategy used to protect against data emanation is called TEMPEST; its mitigations include the use of Faraday cages and jamming devices. *See also* Faraday cage.

Data Encryption Standard (DES) A standard cryptosystem proposed in 1977 for all government communications. DES is a 64-bit block cipher that uses the equivalent of a 56-bit key. DES and 3DES were superseded by Advanced Encryption Standard (AES) in December 2001. DES is an antiquated cipher and should no longer be used.

data execution prevention (DEP) A security feature of many operating systems aimed at blocking a range of memory abuse attacks, including buffer overflows. DEP blocks the execution of code stored in areas of memory designated as data-only areas.

data exfiltration Access by an outsider or unauthorized entity to internal data. This is a data loss or data leakage event.

data exposure The condition of data being potentially harmed, violated, disclosed, exfiltrated, and so on.

data extraction The process of extracting elements of data from a large body of data to construct a meaningful representation or summary of the whole. *See* sampling.

data flow control The movement of data between processes, between devices, across a network, or over communication channels. Management of data flow ensures not only efficient transmission with minimal delays or latency, but also reliable throughput using hashing and confidentiality protection with encryption. Data flow control also ensures that receiving systems are not overloaded with traffic, especially to the point of dropping connections or being subject to a malicious or even self-inflicted denial of service.

data hiding Preventing data from being discovered or accessed by a subject by positioning the data in a logical storage compartment that is not accessible or seen by the subject. This means the subject cannot see or access the data, not just that it is unseen.

data in transit, data-in-transit Data being communicated over a network connection. Aka data in transfer, data being communicated, data in motion, data on the wire, and data being moved.

data in use, data-in-use Data being actively processed by an application. Aka data being processed and data in processing.

data integrity A level of confidence that data won't be altered in transit. This ensures that the data received is exactly the same data that was transmitted.

Data Link layer (layer 2 of the OSI) The second layer of the OSI model. It is the layer where media access control (MAC) addresses reside and frames are transmitted. *See also* Open Systems Interconnection (OSI).

data loss prevention (DLP) Systems specifically implemented to detect and prevent unauthorized access to, use of, or transmission of sensitive information (i.e., exfiltration). Examples include network-based DLP and endpoint-based DLP.

Data Manipulation Language (DML) The database programming language that allows users to interact with the data contained within the schema.

data mart A storage facility used to secure metadata.

data masking The activity of attempting to obfuscate data through manipulation of its characters or content. Data masking attempts to maintain usability of the data while protecting the privacy or sensitivity of the data.

data minimization The reduction of data collected or stored to the minimum necessary to perform essential business tasks.

data mining A technique or tool that allows analysts to comb through data warehouses and look for potential correlated information amid the historical data.

data owner The person who has final corporate responsibility for classifying and labeling objects and protecting and storing data. The owner may be liable for negligence if they fail to perform due diligence in establishing and enforcing security policies to protect and sustain sensitive data.

data packet A unit of data sent over a network. A packet includes a header, addressing information, and the data itself. The packet resides at layer 3 of the Open Systems Interconnection (OSI) model.

data parent A term related to a hierarchical data structure in which the item is upward or closer to the root of the hierarchy than to a data child.

data privacy officer (DPO) A company executive tasked with the responsibilities of crafting the company data privacy policy, implementing that policy, and overseeing its operation and management.

data processor The EU data protection law defines a data processor as "a natural or legal person which processes personal data solely on behalf of the data controller."

data remnants, data remanence Data that remains on media after the data has been supposedly removed. Sanitization methods attempt to ensure that all data is removed from media without any data remnants/remanence remaining.

data sanitization Removing data from a storage device so that it is no longer recoverable.

data sovereignty The concept that once information has been converted into a binary form and stored as digital files it is subject to the laws of the country within which the storage device resides.

data state(s) The possible states of existence of data. *See* data at rest, data in transit, and data in use.

data steward *See* data custodian.

data stream Data from an application sent into a protocol stack. The data stream becomes the initial payload of the top layer protocol.

data terminal equipment (DTE) A networking device that acts like a router or a switch and provides the customer's network access to the Frame Relay network.

data warehouse A large database used to store large amounts of information from a variety of databases for use in specialized analysis techniques.

data wiping The process of removing data from a storage device.

database An electronic filing system for organizing collections of information. Most databases are organized by files, records, and fields.

database contamination What happens when data or records of different values, classifications, security domains, and the like are commingled or mixed together. It can be a form of integrity and confidentiality violation.

database management system (DBMS) An application that enables the storage, modification, and extraction of information from a database.

database partitioning The act of dividing a database into smaller sections or individual databases; often employed to segregate content with varying sensitivity labels.

database vulnerability scanner A tool that allows security professionals to scan both databases and web applications for vulnerabilities that may affect database security.

datacenter, data center *See* server vault.

datagram The combination of Transport layer UDP header and payload.

dd A *nix-based disk duplicator tool. It can be used to copy, move, and restore memory, files, folders, partitions/volumes, or entire drives to any storage location (local or networked). With the right syntax, `dd` can be used to perform data transfer between storage devices or systems, perform in-place file modification (such as resize or truncate), back up and replace the MBR, wipe disks, restore data, benchmark drive performance, generate random data into a file, and convert file contents to uppercase, lowercase, ASCII, or Extended Binary Coded Decimal Interchange Code (EBCDIC).

DDoS attack *See* distributed denial-of-service (DDoS) attack.

dead code Any section of software that is executed but whose output or result is not used by any other process.

deauthentication A wireless networking packet that is normally used immediately after a client initiated WAP authentication but failed to provide proper credentials. However, if sent at any time during a connected session, the client immediately disconnects as if its authentication did fail.

debugging mode A software testing configuration that causes detailed information and errors to be displayed or recorded into a debug log for analysis.

decentralized access control System of access control in which authorization verification is performed by various entities located throughout a system. *See* centralized access control.

decentralized management Describes an organization in which management and administration tasks for a system occur in many locations through an environment, such as on each endpoint device.

decide To choose a response to an unwanted activity.

decision support system (DSS) An application that analyzes business data and presents it so as to make business decisions easy for users. DSS is considered an informational application rather than an operational application. Often a DSS is employed by knowledge workers (such as help desk or customer support) and by sales services (such as phone operators).

declassification The process of assigning an asset a new, lower classification level when necessary as its value depreciates over time. The process of moving a resource into a lower classification level once its value no longer justifies the security protections provided by a higher level of classification. *See* reclassification.

decompiler A specialized programming tool that may be able reverse the compilation process. Decompilers attempt to take binary executables and convert them back into source code form. *See* disassembler.

decomposing *See* reduction analysis.

decrypting The process of reversing a cryptographic algorithm that was used to encrypt a message.

decryption, decrypt The process of converting encrypted data (i.e., ciphertext) back into its original form (i.e., plaintext).

dedicated line A communication link that is continually reserved for use by a specific customer. Aka leased line or point-to-point link.

dedicated mode *See* dedicated security mode.

dedicated security mode The mode in which the system is authorized to process only a specific classification level at a time. All system users must have clearance and a need to know that information.

deencapsulation The process of stripping a layer's header and footer from a protocol data unit (PDU) as it travels up the OSI model layers.

deep packet inspection (DPI) A means to evaluate and filter the payload contents of a communication rather than only on the header values. DPI can also be known as complete packet inspection and information extraction. DPI filtering is able to block domain names, malware, spam, malicious scripts, abusive contents, or other identifiable elements in the payload of a communication. DPI is often integrated with Application-layer firewalls and/or stateful inspection firewalls. Aka payload inspection and content filtering.

deep web A part of the "regular" internet, but it is the content that is not searchable using a standard public search engine. Instead, this is the collection of data, information, and resources that is contained in a walled garden. *See* walled garden.

default configuration Hardware's or software's initial from-the-factory/vendor settings, which are intended for ease of installation and initial configuration to minimize support calls from new customers, rather than for reliable security.

default gateway The Internet Protocol (IP) address of the router interface in a subnet to which all packets are sent when the workstation doesn't know where the destination station is or can't find the destination station on the local subnet. In most network topologies, the default gateway is the router that routes traffic to/toward the internet.

defense in depth The use of multiple types of access controls in literal or theoretical concentric circles or layers. Multiple layers of security are implemented, requiring attackers to circumvent numerous security controls to be successful. Aka layered security and multilayered security. *See* diversity of defense.

degaussing The act of using a magnet or magnetic field to destroy data stored on magnetic media to prevent data leakage attacks or events. For modern large-capacity drives, the strength of the magnetic field needed to sanitize the data may be sufficient to damage the drive itself.

degree The number of columns in a relational database.

delay, delayed To inhibit the quick conclusion of an unwanted activity in order to cause it to take more time.

delegation In the context of object-oriented programming, the forwarding of a request by an object to another object or delegate. An object delegates if it does not have a method to handle the message.

Delphi technique A qualitative risk-assessment process that allows a community to reach an anonymous consensus.

delta rule The feature of neural networks that allows them to learn from experience. Aka the learning rule.

deluge system Another form of dry pipe (fire suppression) system that uses larger pipes and therefore a significantly larger volume of water. Deluge systems are inappropriate for environments that contain electronics and computers.

demarcation point The location where responsibility of wiring changes from the telco to the organization. Often located in the master distribution frame (MDF).

demilitarized zone (DMZ) This term is deprecated. *See* screened subnet.

demonstrative evidence Evidence used to support testimonial evidence. It consists of items that may or may not be admitted into evidence themselves but are used to help a witness explain a concept or clarify an issue.

denial of service (DoS), DoS attack A type of attack that prevents a system from processing or responding to legitimate traffic or requests for resources and objects.

deny, denial To prevent an unwanted activity.

deny risk *See* risk rejection.

deprovisioning (1) Streamlining and fine-tuning resource allocation to existing systems for a more efficient distribution of resources. The release of resources back into a standby, reserve, or availability pool. (2) The release of resources from a server being decommissioned so that those resources return to the availability pool for use by other future servers.

DER (Distinguished Encoding Rules) A certificate file-encoding technique and file extension. DER is a binary formatting rather than ASCII (as is used by Privacy-Enhanced Mail [PEM]). A DER-encoded certificate can be stored in a file with a `.der` or a `.cer` extension.

dereferencing The act of accessing a pointer to read that memory location.

DES *See* Data Encryption Standard (DES).

design flaws Mistakes in the overall concept, theory, implementation, or structure of an application. Design flaws may exist due to misunderstanding the problem that was intended to be solved, misunderstanding the requirements of the solution, violating common or good practice design principles, or failing to account for security measures during initial conception.

detect To discover or track unwanted activity.

detective, detective control, detective access control An access control deployed to discover unwanted or unauthorized activity. Examples of detective access controls include security guards, supervision of users, incident investigations, and intrusion detection systems (IDSs).

deter, deterred To discourage an unwanted activity.

determine To discover the cause or purpose of an unwanted activity.

deterrent, deterrent control, deterrent access control An access control that discourages violations of a security policy.

deterrent alarms Alarms that trigger deterrents may engage additional locks, shut doors, and so on. The goal of such an alarm is to make further intrusion or attack more difficult.

device authentication (1) Authentication on or to a mobile device. (2) When accessing an online website, service, or cloud offering from a mobile device, a form of multifactor authentication (MFA) may be implemented by combining your user credentials with context-aware authentication. Context-aware authentication evaluates the origin and context of a user's attempt to access a system. If the user originates from a known trusted system, such as a system inside the company facility or the same personal mobile device, then a low-risk context is present and a modest level of authentication is mandated for gaining access. If the context and origin of the user is from an unknown device and/or external/unknown location, the context is high risk.

device lockout A lockout mechanism on a mobile device.

DevOps (development and operations) An information technology (IT) movement in which many elements and functions of IT management are being integrated into a single automated solution. This management approach seeks to resolve issues of software development, quality assurance, and technology operations by bringing the three functions

together in a single operational model. Later derivative includes security (i.e., secure DevOps, SecDevOps or DevSecOps).

DevSecOps (development, security, and operations) A derivative of DevOps that integrates development, security, and operations. The DevSecOps approach also supports the concept of software-defined security, where security controls are actively managed by code, allowing them to be directly integrated into the continuous integration/continuous delivery (CI/CD) pipeline.

DH *See* Diffie–Hellman (DH).

DHCP *See* Dynamic Host Configuration Protocol (DHCP).

DHCP snooping A switch feature that monitors for malicious DHCP traffic and rogue DHCP servers.

dialog discipline, dialog control The possible means of data communications over an established link or pathway. Options include simplex, half-duplex, full-duplex. Aka dialogue discipline or dialogue control.

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

differential backup A type of backup that copies only new files or files that have changed since the last full backup onto the backup media. Differential backups differ from incremental backups in that they don't clear the archive bit or change the timestamp on completion.

Diffie–Hellman (DH, D–H) A standard for exchanging keys. This cryptographic algorithm is used primarily to send secret keys across public networks and relies on a discrete logarithm for security. The process isn't used to encrypt or decrypt messages; it's used only for the transmission of keys in a secure manner. *See also* Diffie–Hellman Ephemeral (DHE) and Elliptic Curve Diffie–Hellman Ephemeral (ECDHE).

Diffie–Hellman Ephemeral (DHE), Ephemeral Diffie–Hellman (EDH) A variation of D–H that improves the entropy or randomness of generated and exchanged keys.

Diffie–Hellman group A set of starting parameters that determines the length of the initial prime and integer starting values for DH.

diffusion A feature or function of a cryptographic algorithm to ensure that small changes in input or plaintext would result in distributed or broad changes in output or ciphertext.

`dig` A Linux command used to perform manual DNS queries. Similar to `nslookup`.

digital communications Network transmissions that occur through the use of a discontinuous electrical signal and a state change (i.e., high and low voltages) or on-off pulses.

digital envelope An alternate means of secure key exchange—*see also* Diffie–Hellman (DH or D–H)—that is crafted using a recipient's public key, which can then be opened by the recipient's private key.

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

digital motion detector A device that monitors for significant or meaningful changes in the digital pattern of a monitored area. This is effectively a smart security camera.

digital rights management (DRM) A type of protection software that uses encryption to enforce copyright restrictions on digital media. Over the past decade, publishers attempted to deploy DRM schemes across a variety of media types, including music, movies, and books.

digital signature A method for assuring a recipient that a message truly came from the claimed sender and that the message was not altered while in transit between the sender and recipient. A digital signature is created by encrypting or signing the hash of the message with the private key of the sender.

Digital Signature Standard (DSS), Digital Signature Algorithm (DSA) A method for creating digital signatures that is a Federal Information Processing Standard (FIPS), specifically FIPS 186. Unlike Rivest, Shamir, and Adelman (RSA) encryption, DSA does not use a private key to directly encrypt the hash of the data or message to create signatures. Instead, DSA uses a unique mathematical function that creates a signature consisting of two 160-bit numbers.

direct addressing A process by which the CPU is provided with the actual address of the memory location to be accessed.

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

direct inward system access (DISA) A security tool for private branch exchange (PBX) that adds authentication requirements to all external connections to the PBX.

direct memory access (DMA) A mechanism that allows devices, interfaces, or expansion technologies to exchange data directly with real memory (RAM) without requiring assistance from the CPU, such as FireWire.

direct sequence spread spectrum (DSSS) A wireless or radio wave communication process that employs all the available frequencies simultaneously in parallel.

directed graph A graphic representing the directional transfer of rights in the Take-Grant model.

directional antenna A type of antenna that focuses its sending and receiving capabilities in one primary direction. Some examples of directional antennas are Yagi, cantenna, panel, and parabolic.

directive, directive control, directive access control A type of access control that is deployed to direct, confine, or control the actions of subjects to force or encourage compliance with security policies.

directory A network database that contains a listing of all network resources, such as users, printers, groups, and so on. In the Unix world, a directory is also the name of a type of file that contains other files. Directories are often referred to as folders in the Windows realm.

directory service A centralized database of resources available to the network, much like a telephone directory for network services and assets. Users, clients, and processes consult the directory service to learn where a desired system or resource resides.

directory traversal An attack that enables an attacker to jump out of the web root directory structure and into any other part of the filesystem hosted by the web server's host operating system.

disablement A little-used feature of some operating system user accounts that automatically disables a user account or causes the account to expire at a specific time and on a specific day. *See* account expiration. Often confused with account lockout.

disassembler A specialized programming tool that attempts to convert an executable back into machine-readable assembly language (an intermediate step during the compilation process). *See* decompiler.

disassociation One of the many types of wireless management frames. An attack can send repeated disassociation frames to a client to prevent reassociation, thus causing a denial of service (DoS).

disaster An event that brings great damage, loss, or destruction to a system or environment.

disaster recovery The process of recovering following a disaster that has destroyed the organization's ability to perform mission-critical services.

disaster recovery plan (DRP) The collection of detailed procedures used in the event that business functions are interrupted by a significant damaging event, with the goal of restoring partial or normal operations.

disclosure The occurrence of a violation of confidentiality when resources are made accessible to unauthorized entities.

discretion In regard to confidentiality, an act of decision where an operator can influence or control disclosure to minimize harm or damage.

discretionary access control (DAC) A means of restricting access to objects based on the identity of subjects and/or groups to which they belong that is user-directed or, more specifically, controlled by the owner and creators of the objects (resources) in the environment. DAC access is defined on each object via an ACL.

discretionary security property A property that states that the system uses an access control matrix to enforce discretionary access control.

distributed system A collection of individual systems that work together to support a resource or provide a service. Often a distributed computing environment (DCE) is perceived by users as a single entity rather than numerous individual servers or components. DCEs are designed to support communication and coordination among its members in order to achieve a common function, goal, or operation. Some DCE systems are composed of homogenous members; others are composed of heterogeneous systems. Distributed systems can be implemented to provide resiliency, reliability, performance, and scalability benefits. Most DCEs exhibit numerous duplicate or concurrent components, are asynchronous, and allow for fail-soft or independent failure of components. Aka concurrent computing, parallel computing, distributed computing, and distributed computing environment (DCE).

distributed virtual switches A cloud-based software version of a switch. They help reduce the chance of introducing configuration errors. They are more easily centrally managed and can be managed using an infrastructure as code (IaC) architecture approach.

disk mirroring Technology that keeps identical copies of data on two or more disks to prevent the loss of data if one disk is damaged. Aka RAID 1. A variant is known as duplexing when two different drive controllers are used in addition to two drives. A technology that takes advantage of disk mirroring is a redundant array of independent (or inexpensive) disks (RAID).

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; thus, disk striping by itself doesn't provide fault tolerance. Aka RAID 0.

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. Aka RAID 5.

display filter The set of rules to govern which frames are shown from the packet file or buffer by a network sniffer. *See* capture filter.

distance vector A type of interior routing protocol that only evaluates based on hops (i.e., crossing a router) and prefers routes with fewer hops. *See* Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP).

distance vector routing protocol A routing protocol that maintains a list of destination networks along with metrics of direction and distance as measured in hops (in other words, the number of routers to cross to reach the destination).

distributed access control A form of access control in which authorization verification is performed by various entities located throughout a system. Aka decentralized access control. *See* centralized access control.

distributed architecture A client/server model of networking where clients may be local or connected over WAN links, including virtual private networks (VPNs) and the internet. Aka distributed system.

Distributed Component Object Model (DCOM) An extension of COM to support distributed computing. This is Microsoft's answer to CORBA.

distributed control system (DCS) Industrial control system (ICS) units that are typically found in industrial process plans where the need to gather data and implement control over a large-scale environment from a single location is essential. An important aspect of DCS is that the controlling elements are distributed across the monitored environment, such as a manufacturing floor or a production line, whereas the centralized monitoring location sends commands out of those localized controllers while gathering status and performance data.

distributed data model In a distributed data model, data is stored in more than one database but remains logically connected. The user perceives the database as a single entity, even though it consists of numerous parts interconnected over a network. Each field may have numerous children as well as numerous parents. Thus, the data mapping relationship is many-to-many.

distributed denial-of-service (DDoS), DDoS attack A distributed denial of service occurs when the attacker compromises several systems to be used as launching platforms against one or more victims (i.e., a botnet). The compromised systems used in the attack are often called zombies. A DDoS attack results in the victims being flooded with data from numerous sources. *See also* denial-of-service (DoS) attack, distributed reflective denial of service (DRDoS), and botnet.

distributed reflective denial of service (DRDoS), DRDoS attack DRDoS attacks take advantage of the normal operation mechanisms of key internet services, such as DNS and router update protocols, which are used as an amplification or bounce system. DRDoS attacks function by sending numerous update, session, or control packets to various internet service servers or routers with a spoofed source address of the intended victim. This process causes a "reflection" of the request traffic to potentially be amplified and sent to the spoofed victim's address. A DRDoS attack can result in so much traffic that upstream systems are adversely affected by the sheer volume of data focused on the victim. *See also* denial-of-service (DoS) attack, distributed denial of service (DDoS), and botnet.

distributive allocation, distributed allocation The concept of provisioning resources across multiple servers or services as needed rather than preallocating or concentrating resources based exclusively on physical system location.

diversity of defense Using multiple different technologies, products, and vendors to support cybersecurity resiliency. *See* defense in depth.

DKIM *See* Domain Keys Identified Mail (DKIM).

DLL injection An advanced software exploitation technique that manipulates a process's memory to trick it into loading additional code and thus perform operations the original author did not intend. A dynamic-link library (DLL) is a collection of code that is designed to be loaded and used as needed by a process. Aka DLL hijacking or DLL injection attack.

DLP *See* data loss prevention (DLP).

DMARC *See* Domain Message Authentication Reporting and Conformance (DMARC).

DMZ *See* demilitarized zone (DMZ) and screened subnet.

DNS (Domain Name System) *See* Domain Name System (DNS).

DNS cache poisoning An attack against a caching DNS server where false data is injected. This can potentially occur without notice for a significant period of time.

DNS over HTTPS (DoH) A DNS system that creates an encrypted session with a DNS server using TLS-protected HTTP and then uses that session as a form of virtual private network (VPN) to protect a DNS query and response.

DNS pharming *See* pharming.

DNS poisoning The act of falsifying the Domain Name System (DNS) information used by a client to reach a desired system. Usually employed by planting false information into a zone file, caching DNS system, or a HOSTS file. Often the malicious site looks exactly like the site the user intended to visit and can be difficult to identify.

DNS query spoofing A type of attack that occurs when the hacker is able to eavesdrop on a client's query to a DNS server. The attacker then sends back a reply with false information. In order for this to be successful, the false reply must include the correct query ID (QID) cloned from the query.

DNS sinkhole Systems that provide false responses to DNS queries from malware, such as bots. This technique is effectively DNS spoofing. It can be used for both malicious and benign/investigative/defensive purposes. This is a specific example of a false telemetry system. Aka sinkhole server, internet sinkhole, and blackhole DNS.

DNS spoofing The act of altering or falsifying DNS information using a rogue DNS server to send false DNS replies in order to route or misdirect legitimate traffic.

`dnsenum` A tool used for DNS information harvesting. It can pull data from DNS servers, Google searches, and WHOIS lookups.

DNSSEC (DNS Security) A security improvement to the existing Domain Name System (DNS) infrastructure. The primary function of DNSSEC is to provide reliable authentication between devices during DNS operations. Each DNS server is issued a digital certificate, which is then used to perform mutual certificate authentication.

document store A type of NoSQL database structure that stores information using keys, but the type of information they store is typically more complex than that in a key/value store and is in the form of a document. Common document types used in document stores include Extensible Markup Language (XML) and JavaScript Object Notation (JSON).

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

documentation review The process of reading the exchange materials and verifying them against standards and expectations.

domain (1) A realm of trust or a collection of subjects and objects that share a common security policy. Each domain's access control is maintained independently of other domains' access control. This results in decentralized access control when multiple domains are involved. Aka realm, security domain, or zone. (2) An area of study for the CISSP exam. (3) In a database, the set of allowable values that the attribute can take.

domain hijacking, domain theft The malicious action of changing the registration of a domain name without the authorization of the valid owner. This may be accomplished by stealing the owner's logon credentials; using XSRF, session hijacking, or MitM; or exploiting a flaw in the domain registrar's systems.

Domain Keys Identified Mail (DKIM) A means to assert that valid mail is sent by an organization through verification of domain name identity.

Domain Message Authentication Reporting and Conformance (DMARC) A DNS-based email authentication system. It is intended to protect against Business Email Compromise (BEC), phishing, and other email scams. Email servers can verify if a received message is valid by following the DNS-based instructions; if invalid, the email can be discarded, quarantined, or delivered anyway.

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

Domain Name System Security Extensions (DNSSEC) *See* DNSSEC.

domain reputation A scoring system that can be used to determine whether a site's communications or content are more likely legitimate or more likely malicious or fraudulent.

domain theft *See* domain hijacking.

domain validation (DV) certificate A type of certificate used to validate a domain name rather than a specific device, server, or system hardware.

domain Within the internet, a group of computers with shared traits and a common Internet Protocol (IP) address set. This can also be a group of networked Windows computers that share a single security accounts manager (SAM) database.

DomainKeys Identified Mail (DKIM) A means to assert that valid mail is sent by an organization through verification of domain name identity.

DoS attack *See* denial-of-service (DoS) attack.

downgrade attack An attack that attempts to prevent a client from successfully negotiating robust high-grade encryption with a server. This attack may be performed using a real-time traffic manipulation technique or through a man-in-the-middle attack (a false proxy) to forcibly downgrade the attempted negotiation to a lower-quality level of algorithms and key exchange/generation.

doxing The collection of information about an individual or an organization (which can also include governments and the military) to disclose the collected data publicly for the purpose of changing opinions.

DRDoS *See* distributed reflective denial-of-service (DRDoS) attack.

DREAD A risk rating system designed to provide a flexible rating solution based on asking five main questions of each threat: damage potential, reproducibility, exploitability, affected users, and discoverability.

drive-by download Code downloaded and installed on a user's system without the user's knowledge caused just by visiting a malicious or poisoned website.

driver manipulation A form of software manipulation in which a malicious programmer crafts a system or device driver so that it behaves differently based on certain conditions.

drone *See* uncrewed aerial vehicle (UAV).

dry pipe system A fire suppression system that contains compressed air. Once suppression is triggered, the air escapes, which opens a water valve that in turn causes the pipes to fill and discharge water into the environment.

DSSS *See* direct sequence spread spectrum (DSSS).

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

dual stack Running two protocols on the same system, such as IPv4 and IPv6.

due care Practicing the individual activities that maintain the due diligence effort. Due care is the continued application of this security structure onto the IT infrastructure of an organization. The legal defense against negligence that shows that an organization continued to maintain security after deployment, based on due care. *See* due diligence.

due diligence Establishing a plan, policy, and process to protect the interests of an organization. Due diligence is knowing what should be done and planning for it; due care is doing the right action at the right time. The legal defense against negligence that shows that an organization was aware of its risks and designed protections against loss. *See* due care.

due process The concept that the government must respect all the legal rights of individuals when a person is deprived of their life, liberty, or property due to a court case, legal action, or government/military action.

dumb cards Human-readable-only card IDs that usually have a photo and written information about the authorized bearer. Dumb cards are for use in environments where automated controls are infeasible or unavailable but security guards are practical.

dump file A type of log that is usually a recording of the memory contents of an application or the entire OS. Dump files can be useful in detecting malware, coding errors, memory management violations, and other memory- and process-related issues.

dumpster diving The act of looking through trash for clues—often in the form of paper scraps—to users' passwords and other pertinent information. The act of digging through the refuse, remains, or leftovers from an organization or operation in order to discover or infer information about the organization.

durability One of the four required characteristics of all database transactions (the other three are atomicity, consistency, and isolation). The concept that database transactions must be resilient. Once a transaction is committed to the database, it must be preserved. Databases ensure durability through the use of backup mechanisms, such as transaction logs.

duress system A button or code that sends a distress call. A monitoring entity receives the distress call and responds based on established procedures. Duress systems are useful when personnel are working alone.

dwell time The length of time a key on the keyboard is pressed. This is an element of the keystroke dynamics biometric factor.

dynamic analysis, dynamic code analysis The testing and evaluation of software code while the program is executing. The executing code is then subjected to a range of inputs to evaluate its behavior and responses. *See* static analysis and stress testing.

Dynamic Host Configuration Protocol (DHCP) A protocol used to assign TCP/IP configuration settings to systems upon bootup, including TCP/IP addresses, default gateways, subnet masks, and DNS configurations. DHCP uses UDP port 67 for server point-to-point response and port 68 for client request broadcast. DHCP supports centralized control and management of network addressing.

dynamic NAT The "normal" or standard implementation of network address translation (NAT) that creates temporary session-based outbound IP (and port) mappings when necessary.

dynamic packet-filtering firewalls, dynamic packet firewalls A firewall that enables real-time modification of the filtering rules based on traffic content. *See* Application layer firewall, deep packet inspection, content filtering, and context-based access control.

dynamic passwords Passwords that do not remain static for an extended period of time. Dynamic passwords can change on each use or at a regular interval, such as every 30 days.

dynamic resource allocation *See* elasticity.

dynamic testing Evaluates the security of software in a runtime environment and is often the only option for organizations deploying applications written by someone else. *See* dynamic analysis. Aka dynamic application security testing (DAST).

dynamic-link library (DLL) A collection of code that is designed to be loaded and used as needed by a process. Many DLLs are designed to perform common functions and thus are shared among many applications.

E

EAP *See* Extensible Authentication Protocol (EAP).

EAP-FAST (EAP Flexible Authentication via Secure Tunneling) A Cisco protocol proposed to replace Lightweight Extensible Authentication Protocol (LEAP), which is obsolete thanks to the development of Wi-Fi Protected Access 2 (WPA2).

EAP-MD5 One of the earliest EAP methods. It hashes passwords using MD5. It is now deprecated.

EAP-POTP (EAP Protected One-Time Password) An EAP method that supports the use of OTP tokens (which includes hardware devices and software solutions) in multifactor authentication for use in both one-way and mutual authentication.

EAP-SIM (EAP Subscriber Identity Module) A means of authenticating mobile devices over the Global System for Mobile Communications (GSM) network. Each device/subscriber is issued a subscriber identity module (SIM) card, which is associated with the subscriber's account and service level.

EAP-TLS (EAP Transport Layer Security) An open Internet Engineering Task Force (IETF) standard that is an implementation of the Transport Layer Security (TLS) protocol for use in protecting authentication traffic.

EAP-TTLS (EAP Tunneled Transport Layer Security) An extension of EAP-TLS that creates a virtual private network (VPN)–like tunnel between endpoints prior to authentication.

east-west traffic A term that refers to the traffic flow that occurs within a network, data center, or cloud environment. *See* north-south traffic.

eavesdropping Any type of passive attack that intercepts communications in an unauthorized manner—usually to find passwords. Cable sniffing, wiretapping, and man-in-the-middle (MitM)/on-path attacks are eavesdropping attacks. Aka sniffing. Eavesdropping also includes recording or listening to audio communications, faxes, radio signals, and so on.

ECB (Electronic Code Book) *See* Electronic Code Book (ECB).

ECC *See* elliptic curve cryptosystem (ECC) or elliptic curve cryptography (ECC).

Echo A protocol that has been superseded by ICMP. Echo was used to perform round-trip time tests of network targets.

Economic Espionage Act of 1996 A law that states that anyone found guilty of stealing trade secrets from a U.S. corporation with the intention of benefiting a foreign government or agent may be fined up to $500,000 and imprisoned for up to 15 years and that anyone found guilty of stealing trade secrets under other circumstances may be fined up to $250,000 and imprisoned for up to 10 years.

edge computing A computation architecture that is part of the Industrial Internet of Things (IIoT). In edge computing, the intelligence and processing are contained within each device, which is at or near the edge of the network. *See* fog computing.

education Broad security training, usually focused on teaching users to perform their work tasks securely. This term also describes a more detailed learning endeavor in which students/users learn much more than they actually need to know to perform their work tasks. Education is most often associated with users pursuing certification, seeking job promotion, or career advancement. *See* awareness and training.

EEPROM *See* electrically erasable programmable read-only memory (EEPROM).

EF *See* exposure factor (EF).

efficacy rate The measurement of how well something works or fulfills a security need or requirement.

egress filter A traffic filter on packets leaving a secured area toward the outside (outbound communications).

egress monitoring The process of monitoring outgoing traffic to detect and prevent data exfiltration, which is the unauthorized transfer of data outside the organization.

El Gamal The explanation of how the mathematical principles behind the Diffie–Hellman key exchange algorithm could be extended to support an entire public key cryptosystem used for the encryption and decryption of messages.

elasticity The flexibility of virtualization and cloud solutions to expand or contract based on need and allow the use or consumption of additional available resources.

electrically erasable programmable read-only memory (EEPROM) A version of ROM that can be erased with an electrical signal. EEPROMs can be erased without removal from the computer, giving them much greater flexibility than standard PROM and EPROM chips. Sometimes referred to incorrectly as electronically erasable PROM (EEPROM).

electromagnetic interference (EMI) The interference that can occur during transmissions over copper cable due to electromagnetic energy outside the cable. The result is degradation or loss of the signal. A type of electrical noise that can do more than just cause problems with how equipment functions; it can also interfere with the quality of communications, transmissions, and playback.

electronic access control (EAC) A type of smart lock, door-locking and -access mechanism that uses an electromagnet to keep a door closed, a credential reader to determine authorization, and a door-close spring and sensor to ensure that the door recloses within a reasonable time frame.

Electronic Code Book (ECB), Electronic Codebook The simplest and least secure of the symmetric modes. In this mode, each block of the message is encrypted in a simple and straightforward process using the selected secret key (i.e., it does not incorporate randomness,

nor does it use an IV). *See also* Cipher Block Chaining (CBC), Counter Mode (CTR), and Galois Counter Mode (GCM).

Electronic Communications Privacy Act (ECPA) The law that makes it a crime to invade an individual's electronic privacy. It protects against the monitoring of email and voicemail communications and prevents providers of those services from making unauthorized disclosures of their content.

electronic discovery (e-discovery) In legal proceedings, each side has a duty to preserve evidence related to the case and, through the discovery process, share information with their adversary in the proceedings. This discovery process applies to both paper records and electronic records, and the electronic discovery (or e-discovery) process facilitates the processing of electronic information for disclosure. See Electronic Discovery Reference Model (EDRM).

Electronic Discovery Reference Model (EDRM) A forensic framework that prescribes the primary activities of digital evidence discovery, collection, and processing. See e-discovery.

electronic vaulting A storage scenario in which database backups are transferred to a remote site in a bulk transfer fashion. The remote location may be a dedicated alternative recovery site (such as a hot site) or simply an off-site location managed within the company or by a contractor for the purpose of maintaining backup data.

electro-static discharge (ESD), electrostatic discharge The quick transfer of electrical charge that is accumulated in a human body or physical device when there is low humidity.

elevation of privilege *See* privilege escalation and STRIDE.

ElGamal A public domain extension of Diffie–Hellman that can both provide key exchange and serve as a full public key cryptosystem. However, because it doubles the length of the message encrypted, its use has faded since the patent for Diffie–Hellman expired in 1994.

eliciting information The activity of gathering or collecting information from systems or people. In the context of social engineering, it is used as a research method to craft a more effective pretext.

elliptic curve cryptosystem (ECC), elliptic curve cryptography (ECC) A type of public key cryptosystem that requires a shorter key length than many other cryptosystems (including the de facto industry standards Rivest, Shamir, and Adelman [RSA] and Diffie–Hellman) while maintaining equivalent or superior strength. ECC is based on algebraic elliptical curve theory and offers a bandwidth and computational advantage over these other algorithms. *See* Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman Ephemeral (ECDHE).

Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) An ECC improved version of Diffie–Hellman. Sometimes written as Elliptic Curve Ephemeral Diffie–Hellman (ECEDH).

Elliptic Curve Digital Signature Algorithm (ECDSA) A means to implement perfect forward secrecy through the use of elliptic curve cryptography (ECC). An ECC improved version of DSA. *See* Digital Signature Standard (DSA).

elliptic curve group Each elliptic curve has a corresponding elliptic curve group made up of the points on the elliptic curve along with the point O, located at infinity. Two points within the same elliptic curve group (P and Q) can be added together with an elliptic curve addition algorithm.

email certificate A form of certificate used to verify a specific email address.

emanations Electromagnetic or radio frequency signals that may contain data that can be intercepted through eavesdropping on those signals.

embedded system A computer implemented as part of a larger system. The embedded system is typically designed around a limited set of specific functions in relation to the larger product of which it's a component. It may consist of the same components found in a typical computer system, or it may be a microcontroller (an integrated chip with on-board memory and peripheral ports).

emergency management The plans and practices that help an organization address personnel safety and security after a disaster.

EMI *See* electromagnetic interference (EMI).

employee Often referred to as the user when discussing IT issues. *See also* user.

employee transfer When an employee is moved to a new job position at the same organization, especially when they are shifting between departments, facilities, or geographic locations.

employment agreement A document that outlines an organization's rules and restrictions, security policy, and acceptable use and activities policies; details the job description; outlines violations and consequences; and defines the length of time the position is to be filled by the employee.

Encapsulating Security Payload (ESP) An element of IPsec that provides encryption to protect the confidentiality of transmitted data but can also perform limited authentication. ESP can be used alone or in combination with the IP Authentication Header (AH). ESP performs the primary function of bulk communication encryption. The Internet Protocol (IP) header protocol field value of ESP is 50.

encapsulation The act of enclosing or encasing one item inside another. Commonly used to describe tunneling, in which one protocol is enclosed in another or, in the context of the Open Systems Interconnection (OSI) model, each layer's content is encapsulated as the payload in the next-lower layer and a header is added. The inverse of encapsulation is de-encapsulation.

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

encrypt To convert a message from plaintext into ciphertext.

encrypted virus A virus that uses cryptographic techniques to avoid detection. In their outward appearance, they are quite similar to polymorphic viruses—each infected system has a virus with a different signature. However, they do not generate these modified signatures by changing their code; instead, they alter the way they are stored on the disk.

encryption The process of converting plaintext that is readable by anyone into encrypted or ciphertext. This ciphertext is unreadable to anyone who intercepts it. The general rule is that all encryption can be broken if an attacker has enough time and resources. That said, the idea is to use encryption that is stronger than the data is valuable. See encrypt.

encryption key A string of alphanumeric characters used to encrypt data.

end of life (EOL), end-of-life The point at which a manufacturer no longer produces a product. Service and support may continue for a period of time after EOL, but no new versions will be made available for sale or distribution. *See* end of service (EOS).

end of service (EOS), end of support life (EOSL) Products that are no longer receiving updates and support from the vendor. *See* end of life (EOL). Aka end of support (EOS) or end-of-service.

end user *See* user.

endpoint, endpoint device Any device that can be used by a worker to interact with resources on a company network. This includes desktops, notebooks/laptops, tablets, mobile phones, embedded devices, IoT devices, ICS equipment, and more.

endpoint detection and response (EDR) A security mechanism that is an evolution of traditional antimalware products. EDR seeks to detect, record, evaluate, and respond to suspicious activities and events, which may be caused by problematic software or by valid and invalid users.

endpoint security The concept that each individual device must maintain local security whether or not its network or telecommunications channels provide or offer security. Sometimes this concept is expressed as "The end device is responsible for its own security."

end-to-end encryption An encryption algorithm that protects communications between two parties (in other words, a client and a server) and is performed independently of link encryption. An example of this would be the use of Privacy-Enhanced Mail (PEM) to pass a message between a sender and a receiver. This protects against an intruder who might be monitoring traffic on the secure side of an encrypted link or traffic sent over an unencrypted link.

Enhanced Interior Gateway Routing Protocol (EIGRP) An advanced distance vector routing protocol that replaces IGRP.

enrollment The process of establishing a new user identity or authentication factor on a system. Secure enrollment requires physical proof of a person's identity or authentication factor.

enterprise (ENT) The Wi-Fi authentication option that is Aka IEEE 802.1X/EAP. ENT enables the leveraging of an existing AAA service, such as RADIUS or TACACS+, to be used in authentication.

enterprise extended mode infrastructure An arrangement in which multiple wireless access points (WAPs) are used to support a single wireless network over a larger geographic area than could be supported by a single wireless access point and connect a large physical area to the same wired network.

Enterprise Resource Planning (ERP) A business management software solution that collects, stores, organizes, and evaluates business data. It may be used as a resource in BCP and DRP planning as well as a tool used during recovery.

enterprise risk management (ERM) A formal risk management strategy designed to address the issues of larger organizations.

enticement The process of luring someone to do something.

entity A subject or an object.

entrance facility The entrance point to the building where the cable from the provider connects the internal cable plant. Aka the demarcation point.

entrapment A legal term that describes the process of encouraging a person to perform an illegal act that the individual would not have done without that encouragement.

entropy An assessment of randomness.

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

environmental monitoring The process of measuring and evaluating the quality of the environment within a given structure. This can focus on general or basic concerns, such as temperature, humidity, dust, smoke, and other debris.

ephemeral key A key generated at time of need for use in a short or temporary time frame. An ephemeral key might be used only once or could be used for a communication session before being discarded. Aka ephemeral session key. *See also* session key.

ephemeral ports Ports 49152 to 65535, which are often used randomly and temporarily by clients as a source port. Aka random ports and dynamic ports.

equipment room The main wiring closet for the building, often connected to or adjacent to the entrance facility.

eradication The processes used to remove or eliminate the causes of the incident, such as removing software, deleting malware, changing configurations, firing personnel, disabling compromised accounts, and blocking IP addresses and ports.

erasable PROM (EPROM) A PROM chip that has a small window through which the illumination of a special ultraviolet light causes the contents of the chip to be erased. After this process is complete, the end user can burn new information into the EPROM.

erasing A delete operation against a file, a selection of files, or the entire media. In most cases, the deletion or erasure process removes only the directory or catalog link to the data. The actual data remains on the drive.

error handling *See* exception handling.

escalation, notification escalation A defined order in which various entities or parties are notified based on the type of data involved in a leak and the severity of the consequences of the leak.

escalation of privilege Any attack or exploit that grants the attacker greater privileges, permissions, or access than may have been first achieved by the initial exploitation or that a legitimate user was assigned. *See also* privilege escalation.

escaping (1) The process of marking the metacharacter as merely a normal or common character, such as a letter or number, thus removing its special programmatic powers. This is often done by adding a backslash in front of the character (\&), but there are many ways to escape metacharacters based on the programming language or execution environment. (2) Exploiting a flaw in a VM to access other VMs or the host.

Escrowed Encryption Standard A failed government attempt to create a backdoor to all encryption solutions. The solution employed the Clipper chip, which used the Skipjack algorithm.

ESP *See* Encapsulating Security Payload (ESP).

espionage The malicious act of gathering proprietary, secret, private, sensitive, or confidential information about an organization for the express purpose of disclosing and often selling that data to a competitor or other interested organization (such as a foreign government).

ESSID (extended service set identifier) *See* extended service set identifier (ESSID).

Ethernet A shared-media network architecture. It operates at the Physical and Data Link layers of the Open Systems Interconnection (OSI) model. As the media access method, it uses baseband signaling over either a bus or star topology. The cabling used in Ethernet networks can be coax, twisted pair, or fiber-optic.

Ethernet address *See* MAC address.

ethical disclosure This principle says that security professionals who detect a vulnerability have a responsibility to report that vulnerability to the vendor, providing them with an opportunity to develop a patch or other remediation to protect their customers.

ethical hackers Those trained in responsible network security methodology, with a philosophy toward nondestructive and nonintrusive testing; ethical hackers attack security systems

on behalf of their owners, seeking to identify and document vulnerabilities so that they can be remediated before malicious hackers can exploit them. Ethical hackers use the same methods to test security that unethical ones do, but report what they find rather than seek to turn them to their advantage.

ethical hacking A form of authorized vulnerability scan that is performed by a special team of trained, authorized security specialists rather than by an internal security administrator using an automated tool. *See also* penetration test.

ethics The rules that govern personal conduct. Several organizations have recognized the need for standard ethics rules, or codes, and have devised guidelines for ethical behavior. These rules are not laws but are minimum standards for professional behavior. They should provide you with a basis for sound, professional, ethical judgment.

evaluation assurance levels (EAL) A Common Criteria component used to express the level of reliability testing that a target of evaluation (TOE) was subjected to.

event Any occurrence that takes place during a certain period of time.

evidence In the context of computer crime, any hardware, software, or data that you can use to prove the identity and actions of an attacker in a court of law.

evidence storage A designated system to securely store data items (i.e., evidence) that may be needed for either internal administrative investigations or actual legal investigations.

evil twin An attack in which a hacker operates a false wireless access point (WAP) that will automatically clone, or twin, the identity of another access point based on a client device's automatic request to reconnect to a known wireless network from its connection history. *See* rogue access point.

exception handling The process where a programmer codes in mechanisms to anticipate and defend against errors in order to avoid the termination of execution. Error handling is the inclusion of code that will attempt to handle errors when they arise before they can cause harm or interrupt execution. Aka error handling.

excessive privilege(s) More access, privilege, or permission than a user's assigned work tasks dictate. If a user account is discovered to have excessive privilege, the additional and unnecessary benefits should be immediately curtailed.

exclusive or (XOR) An exclusive disjunction, which means that it produces an output of truth (or 1) whenever the two inputs differ (such as one is a zero [false] and the other is a one [true]). It's referred to in mathematical literature as the XOR function and is commonly represented by the $\oplus$, $\veebar$, or $\not\equiv$ symbol. The XOR function returns a true value when only one of the input values is true. If both values are false or both values are true, the output of the XOR function is false.

executive user Someone in a corporate management position who is granted additional privileges and capabilities beyond those of a typical standard user but likely less than an administrator or privileged user.

exigent circumstances This means that a reasonable person would believe that the evidence would be destroyed if not immediately collected or another emergency exists, such as the risk of physical harm. When officers enter a premises under exigent circumstances, they may conduct a warrantless search.

exit interview A form of debriefing of a released, fired, or exiting employee. An *exit interview* is normally performed by an HR person who specializes in those interviews with the idea of learning from the employee's experience. The purpose of an exit interview is to understand why the employee is leaving, what their perspective is of the organization (its personnel, culture, process, etc.), and what they suggest could be done to improve conditions for current and future employees. Information learned from an exit interview may assist the organization with retaining employees through employment improvements and process/policy changes.

expectation maximization (EM) A data mining technique that develops models of normal user behavior based on a user's affiliation with the organization, the distance between the data center and the user's physical location, the day of the week, the hour of the day, and other attributes.

expert opinion A type of evidence consisting of the opinions and facts offered by an expert. An expert is someone educated in a field and who currently works in that field.

expert system A system that seeks to embody the accumulated knowledge of humankind on a particular subject and apply it in a consistent fashion to future decisions.

expiration The state of an item considered no longer valid or acceptable because it has been static for a specific length of time or beyond a specific point in time. Commonly used in relation to user accounts, certificates, and passwords.

exploitation framework A type of vulnerability analyzer that is able to fully exploit the weaknesses it discovers. It can be an automated or manual exploit assessment tool.

exposure factor (EF) The percentage of asset-value loss that an organization would experience if a specific asset were violated by a realized risk. Aka loss potential.

exposure The condition of being exposed to the potential asset loss because of a threat. Exposure involves being susceptible to the exploitation of a vulnerability by a threat agent or event.

extended service set identifier (ESSID) The name of a wireless network when a wireless base station or wireless access point (WAP) is used (that is, infrastructure mode).

extended validation (EV) certificate A type of certificate issued to a subject when the certificate authority (CA) has expended considerable additional effort to validate and verify the identity of the subject prior to issuing the certificate. Browsers would often display the name of the subject from an EV certificate alongside the locked padlock and before the URL presentation. EV certificates were issued for up to 10 years, but in 2020 that practice was terminated.

Extensible Access Control Markup Language (XACML) A markup language used to define access control policies within an XML format, and it commonly implements role-based access controls. It helps provide assurances to all members in a federation that they are granting the same level of access to different roles.

Extensible Authentication Protocol (EAP) An authentication expansion system in which new or custom mechanisms to perform authentication can be added to existing systems.

Extensible Configuration Checklist Description Format (XCCDF) Security Content Automation Protocol (SCAP) component that provides a language for specifying security checklists.

Extensible Markup Language (XML) A markup language that defines rules and parameters for encoding documents so that the resulting format is both human and computer readable.

exterior routing protocols Routing protocols used on routers external to a private network.

external audit An audit performed by an outside auditing firm. These audits have a high degree of external validity because the auditors performing the assessment theoretically have no conflict of interest with the organization itself. Aka third-party audit.

extranet A privately controlled network segment or subnet that functions as a screened subnet for business-to-business transactions. It allows an organization to offer specialized services to a limited number of specific outsiders but not the entire public, such as business partners, suppliers, distributors, or high-end customers. Often access into an extranet from the internet requires a virtual private network (VPN) connection. Extranets are often used in business-to-business (B2B) applications, between customers and suppliers. *See* screened subnet.

F

face scan An example of a biometric factor, which is a behavioral or physiological characteristic unique to a subject. A face scan is a process by which the shape and feature layout of a person's face is used to establish identity or provide authentication.

facial recognition A biometric technique that analyzes the geometric patterns of faces for detecting authorized individuals. Aka face scans.

Fagan inspections A formal code review process normally used in highly restrictive environments where code flaws may have catastrophic impact.

fail securely A system designed with a specific failure plan, such as fail-soft, fail-safe, fail-secure, fail-open, or fail-closed.

fail-closed *See* fail-secure.

fail-open Describes a system that protects equipment and/or human safety in the event of a system failure. The response of a system to a failure so that it defaults to an "allow" posture.

failover Redirecting workload or traffic to a backup system when the primary system fails. Aka switchover.

failover device A device that comes online or takes over operations when another fails.

failover server A hot (i.e., live, mirrored, and synced) backup system in which a backup or alternative server is connected to the primary server. A heartbeat is sent from the primary server to the backup server. If the heartbeat stops, the failover system starts and takes over. Thus, the system doesn't go down even if the primary server isn't running.

fail-safe The response of a system to a failure so that it defaults to a "deny" posture in a technical or logical arena. In the physical arena, a fail-safe door (or other physical component) will fail to a state to protect the life and safety of people in the event of a system failure or harmful occurrence, often allowing easy and unhindered escape from a building.

fail-secure design A method of programming so that when errors occur, the program should fall back to a secure state.

fail-secure The response of a system to a failure so that it defaults to a "deny" posture in a technical or logical arena. Aka fail-closed. *See* fail-safe.

fail-soft Describes a refinement of the fail-secure capability in which only the portion of a system that encountered or experienced a failure or security breach is disabled or secured, while the rest of the system continues to function normally.

Fair Cryptosystems A failed government attempt to create a backdoor to all encryption solutions. This technology used a segmented key that was divided among several trustees.

fake telemetry Generating false responses that can be used to trick an intruder or malicious code into thinking/perceiving that an attack is occurring against a real target. Fake telemetry can provide simulated responses from other networked equipment, provide falsified DNS results, or be simulated user or production activity on a honeynet/honeypot.

false acceptance rate (FAR) Error that occurs when a biometric device is not sensitive enough and an invalid subject is authenticated. The number of accepted invalid subjects based on device sensitivity. This rate decreases as sensitivity increases. False acceptance is sometimes referred to as a false negative authentication or a Type II error.

false negative (1) A malicious event that occurs without an alarm, detection, or notice. Typically related to an IDS or IPS. (2) Error that occurs when a vulnerability scanner misses a vulnerability and thus fails to alert or inform the administrator to the presence of a dangerous situation. The item is not included on the report produced by the scanner.

false positive The occurrence of an alarm or alert due to a benign activity being initially classified as potentially malicious. The event that might trigger an alarm when a security

scanner may not have enough information to conclusively determine that a vulnerability exists but still reports a vulnerability when there really is no problem. Aka mistaking a benign issue as a malicious event.

false rejection rate (FRR) Error that occurs when a biometric device is too sensitive and a valid subject is not authenticated. The number of failed authentications for valid subjects based on device sensitivity. This rate increases as sensitivity increases. False rejection is sometimes referred to as a false positive authentication or a Type I error.

familiarity A social-engineering technique based on exploiting a person's native trust in that which is familiar. Aka liking.

Family Educational Rights and Privacy Act (FERPA) A specialized privacy bill that affects any educational institution that accepts any form of funding from the federal government (the vast majority of schools). It grants certain privacy rights to students older than the age of 18 and the parents of minor students.

Faraday cage An electrically conductive wire mesh or other conductor woven into a "cage" that surrounds an area and prevents electromagnetic (EM) signals from entering or leaving the contained space. *See also* data emanation.

fat access point A base station that is a fully managed wireless system, which operates as a standalone wireless solution.

fault 1) A momentary loss of power. 2) A failure or problem within a system, device, or process.

fault injection attack An attack where the adversary attempts to compromise the integrity of a cryptographic device by causing some type of external fault.

fault tolerance The ability of a system to suffer a fault but continue to operate and/or without losing data. Fault tolerance is achieved by adding redundant components such as additional disks within a redundant array of independent disks (RAID) or additional servers within a failover clustered configuration.

fault-resistant network A network that can survive faults and failures to prevent or minimize downtime.

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

FCIP (Fibre Channel over IP) An alternate implementation of Fibre Channel signaling that no longer requires any specific network speed and operates over standard Ethernet cables. It is the SAN equivalent of VoIP.

FCoE (Fibre Channel over Ethernet) A means to encapsulate Fibre Channel communications over Ethernet networks. FCoE typically requires 10 Gbps Ethernet to support the Fibre Channel protocol.

Federal Information Processing Standard 140 (FIPS-140) FIPS-140 defines the hardware and software requirements for cryptographic modules that the U.S. federal government uses.

Federal Information Security Management Act (FISMA) A U.S. law passed in 2002 requiring that federal agencies implement an information security program that covers the agency's operations. FISMA also requires that government agencies include the activities of contractors in their security management programs.

Federal Sentencing Guidelines A 1991 law that provides punishment guidelines for breaking federal laws.

federated identity management (FIM) A single sign-on–based identity solution.

federation A means of linking a subject's accounts from several sites, services, or entities in one single account. This is a means of accomplishing single sign-on. Federated solutions often implement trans-site authentication using Security Assertion Markup Language (SAML).

feedback A composition theory stating that one system provides input to another system, which reciprocates by reversing those roles (so that system A first provides input for system B and then system B provides input to system A).

feedback loop characteristic The ability in the modern waterfall model that allows development to return to the previous phase to correct defects discovered during the subsequent phase.

fence, fencing A perimeter-defining device. Fences are used to clearly differentiate between areas that are under a specific level of security protection and those that aren't.

FHSS *See* frequency hopping spread spectrum (FHSS).

Fiber Distributed Data Interface (FDDI) A high-speed token-passing technology that employs two rings with traffic flowing in opposite directions. FDDI is a legacy infrastructure concept that has been mostly replaced by SDH and SONET today.

fiber-optic A cable made of glass or plastic composite, used to transmit computer communications via light instead of electrical signals. This type of cable supports very high rates of throughput over very long distances.

Fibre Channel A form of network data storage solution (storage area network [SAN] or network-attached storage [NAS]) that allows for high-speed file transfers upward of 16 Gbps.

Fibre Channel over Ethernet (FCoE) A converged protocol used to encapsulate Fibre Channel communications over Ethernet networks. It typically requires 10 Gbps Ethernet in order to support the Fibre Channel protocol.

field In a database, a field is a column or attribute of a table.

field-powered proximity device A mechanism that has electronics that activate when the device enters the electromagnetic (EM) field that the reader generates. Such devices actually generate electricity from an EM field to power themselves (such as card readers that require only that the access card be waved within inches of the reader to unlock doors). This is effectively the concept of radio-frequency identification (RFID).

field programmable gate array (FPGA), field-programmable gate array (FPGA) A flexible computing device intended to be programmed by the end user or customer. FPGAs are often used as embedded devices in a wide range of products, including industrial control systems (ICSs).

file inclusion attack A web-focused attack that builds on directory traversal. Instead of simply retrieving a file from the local operating system and displaying it to the attacker, file inclusion attacks actually execute the code contained within a file, allowing the attacker to fool the web server into executing targeted code. Variants include local file inclusion and remote file inclusion.

file infector virus A virus that infects different types of executable files and triggers when the operating system attempts to execute them. For Windows-based systems, these filenames end with `.exe` and `.com`.

file integrity monitor A service/software that compares the current hash of a file to the stored/previous hash of a file. A file integrity checking utility will either display an alert or produce a report of the files that do not pass their hash-based integrity check.

File Transfer Protocol (FTP) A protocol used over TCP/IP that permits the transferring of files between computer systems. Because FTP has been implemented on numerous types of computer systems, files can be transferred between disparate systems (for example, a personal computer and a minicomputer).

File Transfer Protocol Secure (FTPS) A variation of FTP secured by Secure Sockets Layer (SSL, or Transport Layer Security [TLS]).

fileless malware Malware that resides in memory only and does not save itself to the local storage devices.

file system permissions A form of authorization, specifically discretionary access control (DAC). Object access control lists (ACLs) or filesystem access control lists (FACLs) determine which users or groups can access a file and what access they are granted or denied.

filter(s) A set of rules or restrictions commonly found on security devices, such as firewalls and proxies. Aka rules, tuples, and access control lists (ACLs).

financial attack A crime that is carried out to unlawfully obtain money or services.

fingerprint scanner A biometric device that analyzes the visible patterns of skin ridges on the fingers and thumbs of people.

fingerprints The patterns of ridges on the fingers of humans. Often used as a biometric authentication factor.

finite state machine (FSM) An FSM combines an external input with an internal machine state to model all kinds of complex systems, including parsers, decoders, and interpreters. Given an input and a state, an FSM transitions to another state and may create an output.

fire suppression The act of extinguishing (or attempting to extinguish) a fire.

fire triangle A standard fire prevention and resolution training concept. The three corners of the triangle represent fuel, heat, and oxygen. The center of the triangle represents the chemical reaction among these three elements. The purpose of the fire triangle is to illustrate that if you can remove any one of the four items from the fire triangle, the fire can be extinguished.

firewall A network communication product used to filter traffic. A firewall is typically deployed between a private network and a link to the internet, but it can be deployed between departments within an organization as well as on individual systems. Firewalls filter traffic based on a defined set of rules. Software firewalls are installed on the host operating system and defend that system locally from remote threats. Hardware firewalls are often used to defend at the border or perimeter of the network as opposed to locally.

firewall policy A security policy that focuses on the purposes, uses, functions, and security of the firewalls in an organization.

firewire A serial bus interface standard (IEEE 1394) that supports high-speed data transfer via direct memory access (DMA). It was a competing technology to USB.

firmware Software, code, and/or drivers stored on a nonvolatile random-access memory (NVRAM), read-only memory (ROM), electrically erasable programmable read-only memory (EEPROM), or flash memory chip and used to manage or control an expansion device rather than having it rely on an operating system or device driver. Aka microcode.

firmware OTA updates, firmware over-the-air updates Upgrades, patches, and improvements to the existing firmware of a mobile device that are downloaded from the telco or vendor over the air (OTA), such as over the data network or a Wi-Fi network.

fixed-temperature detection A fire detection system that detects a fire and triggers the release of the suppression medium when a specific temperature is reached. This is the most common type of detector and present in most office buildings. The potentially visible sprinkler head serves as both the detection and release mechanism. The trigger is usually a metal or plastic component that is in the sprinkler head and melts at a specific temperature.

flame-actuated detection A fire detection system that detects a fire and triggers the release of the suppression medium based on the detection of the infrared energy of flames. This mechanism is fast and reliable but often fairly expensive. Thus, it is often only used in high-risk environments.

flash memory A concept derived from EEPROM. It is a nonvolatile form of storage media that can be electronically erased and rewritten. The primary difference between EEPROM and flash memory is that EEPROM must be fully erased to be rewritten whereas flash memory can be erased and written in blocks or pages. The most common type of flash memory is NAND flash. It is widely used in memory cards, thumb drives, mobile devices, and SSDs (solid-state drives).

flashcard A form of storage that uses electrically erasable programmable read-only memory (EEPROM) or nonvolatile random access memory (NVRAM) chips in a small form-factor case. Flashcards often use USB connectors or are themselves inserted into devices such as MP3 players and digital cameras.

flashing The process of updating the Unified Extensible Firmware Interface (UEFI), basic input/output system (BIOS), or firmware.

flight time The length of time between key presses. This is an element of the keystroke dynamics form of biometrics.

flip-flop A logical device or component of static RAM that to all intents and purposes is simply an on/off switch that must be moved from one position to another to change a 0 to 1, or vice versa.

flood guard A defense against flooding or massive-traffic denial-of-service (DoS) attacks. The purpose of a flood guard is to detect flooding activity and then automatically begin blocking it.

flooding An attack that involves sending enough traffic to a victim to cause a denial of service (DoS). Also referred to as a stream attack.

FM-200 An EPA-approved gas-based suppression medium to replace Halon.

fog computing A computation architecture that is part of the Industrial Internet of Things (IIoT). Fog computing relies on sensors, IoT devices, or even edge computing devices to collect data and then transfer it back to a central location for processing. The fog computing processing location is positioned in the LAN. *See* edge computing.

footer Information added by a protocol to the end of a payload received from a higher-layer protocol.

footprinting The process of systematically identifying a network and its security posture. *See* reconnaissance.

foreign key A primary key from another table used to cross-link or express relationships between the contents of two tables.

Forensic ToolKit (FTK) Imager The drive cloning utility from the FTK suite of forensic tools. FTK Imager supports most filesystems and drive formats, can clone most storage devices (i.e., HDD, SSD, flash, USB, optical, etc.), supports raw targets on a storage device and target image files, allows for content preview before cloning, can be used for file recovery, supports read-only image mounting, and creates hashes of cloned files.

forensics The collection, protection, and analysis of evidence from a crime to present the facts of the incident in court.

forward proxy A standard or common proxy that acts as an intermediary for queries of external resources. A forward proxy handles queries from internal clients when accessing outside services.

Fourth Amendment An amendment to the U.S. Constitution that prohibits government agents from searching private property without a warrant and probable cause. The courts have expanded their interpretation of the Fourth Amendment to include protections against wiretapping and other invasions of privacy.

fraggle A form of distributed denial-of-service (DDoS) using User Datagram Protocol (UDP) traffic bounced off closed ports to flood a primary victim. It's a variation of the Smurf attack, using UDP packets instead of ICMP.

fragment When a network receives a packet larger than its maximum allowable packet size, it breaks it up into two or more fragments. These fragments are each assigned a size (corresponding to the length of the fragment) and an offset (corresponding to the starting location of the fragment).

fragmentation attack An attack that exploits vulnerabilities in the fragment reassembly functionality of the TCP/IP protocol stack.

frame The combination of Data Link layer header, payload, and footer.

Frame Relay A shared connection medium that uses packet-switching technology to establish virtual circuits for customers.

frequency A measurement of the number of wave oscillations within a specific time identified using the unit Hertz (Hz), or oscillations per second. Radio waves have a frequency between 3 Hz and 300 GHz.

frequency analysis A cryptographic analysis or attack that looks for repetition of letter frequency in an encrypted message and compares that with the statistics of letter usage for a specific written language, such as the frequency of the letters *E*, *T*, *A*, *O*, *N*, *R*, *I*, *S*, and *H* in the English language. This is a common attack against mono-alphabetic substitution ciphers that retain the plaintext language letter use frequency in the resulting substitution ciphertext.

Frequency Hopping Spread Spectrum (FHSS) An early implementation of the spread spectrum concept. This wireless access technology transmits data in a series while constantly changing the frequency in use.

FTP *See* File Transfer Protocol (FTP).

FTPS *See* File Transfer Protocol Secure (FTPS).

full backup A complete copy of data contained on the protected device on the backup media. This process also clears the archive bit or changes the timestamp of files upon completion.

full device encryption (FDE), full-device encryption Storage device encryption on a mobile device. Many mobile devices either are pre-encrypted or can be encrypted by the user/owner. ***See*** full-disk encryption (FDE).

full-duplex Two-way communication, in which data can be sent in both directions simultaneously.

full tunnel A virtual private network (VPN) configuration in which all of the client's traffic is sent to the organizational network over the VPN link, and then any internet-destined traffic is routed out of the organizational network's proxy or firewall interface to the internet. A full tunnel ensures that all traffic is filtered and managed by the organizational network's security infrastructure. *See* split tunnel.

full-disk encryption (FDE) *See* whole-disk encryption (WDE).

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

full-knowledge teams These possess a full body of knowledge of the operation, configuration, and utilization of hardware and software inventory prior to a security assessment or penetration test.

fully qualified domain name (FQDN) The human-friendly name of a system or resource that is associated with an IP address. An FQDN is composed of a hostname or subdomain, a registered domain name, and a top-level domain (TLD) name.

functional recovery plans (FRP) A form of or a subset of BCP and DRP. FRPs focus on restoring the capability to perform a singular or specific business operation or function. It establishes minimal requirements to reenable a process to support a business operation.

fuzz testing A specialized dynamic testing technique that provides many different types of input to software to stress its limits and find previously undetected flaws. Fuzz-testing software supplies invalid input to the software, either randomly generated or specially crafted to trigger known software vulnerabilities. The fuzz tester then monitors the performance of the application, watching for software crashes, buffer overflows, or other undesirable and/or unpredictable outcomes.

fuzzing A dynamic analysis software testing technique that generates inputs for targeted programs. The goal of fuzz testing is to discover input sets that cause errors, failures, and crashes, or to discover other unknown defects in the targeted program. Aka fuzz testing and fuzzer.

fuzzy logic A computational technique designed to more closely approximate human thought patterns than do the rigid mathematics of set theory or algebraic approaches that utilize binary categorizations of data.

G

gait analysis The evaluation of the way someone walks as a form of biometric authentication or identification.

Galbraith's Star Model A business management model that helps businesses organize divisions and departments to achieve business missions and goals and adjust over time for

long-term viability. This model is based around five main areas of business administration that need to be managed, balanced, and harnessed toward the mission and goals of the organization. The five areas of Galbraith's Star Model are Strategy, Structure, Processes, Rewards, and People. This model is not directly related to security.

Galois Counter Mode (GCM) A symmetric mode of operation that is an advancement of Counter Mode (CTR) that adds a hashing function to confirm the integrity of deciphered data. However, though GCM uses hashing to check integrity, it is called an authentication code. *See also* Electronic Codebook (ECB), Cipher Block Chaining (CBC), and Counter Mode (CTR).

gamification A means to encourage compliance and engagement by integrating common elements of game play into other activities. This can include rewarding compliance behaviors and potentially punishing violating behaviors.

Gantt chart A type of bar chart that shows the interrelationships over time between projects and schedules. It provides a graphical illustration of a schedule that helps plan, coordinate, and track specific tasks in a project.

gas discharge system A fire suppression system that releases a gas to extinguish the fire.

gate A controlled exit and entry point in a fence.

gateway A networking device that connects networks that are using different network protocols.

GCM (Galois Counter Mode) *See* Galois Counter Mode (GCM).

GDPR *See* General Data Protection Regulation (GDPR).

general adversarial network (GAN) A machine learning/artificial intelligence (ML/AI) training or programming technique where computational systems are set up to operate in opposition to automate the process of developing system defenses and attacks. Aka adversarial artificial intelligence (AAI) or adversarial machine learning (AML).

General Data Protection Regulation (GDPR) European Union (EU) law that provides a single harmonized law covering data security and privacy. A data protection and privacy law to protect citizens of the EU and the European Economic Area (EEA). It focuses on managing the processing/use and transfer of personally identifiable information (PII) outside of the EU and EEA. Regulation EU 2016/679.

generational fuzzing A form of fuzzing that develops inputs based on models of expected inputs to perform the same task. This is also sometimes called intelligent fuzzing.

generator A device used to generate electricity through the consumption of fuel during a blackout event.

generic account A preset, standard, common, guest, fixed, shared, or anonymous user account.

generic account prohibition The rule that no generic or shared or anonymous accounts should be allowed in private networks or on any system where security is important.

Generic Routing Encapsulation (GRE) A proprietary Cisco tunneling protocol that can be used to establish virtual private networks (VPNs). GRE provides encapsulation but not encryption.

geofencing The designation of a specific geographical area that is then used to implement features on mobile devices. A geofence can be defined by GPS coordinates, wireless indoor positioning systems, or presence or lack of a specific wireless signal.

geographic dispersal A means to increase the benefit and security of redundancy by placing more physical distance between duplicate systems.

geolocation The ability of a mobile device to include details about its location in any media created by the device. Geolocation data is commonly used in navigation tools and by many location-based services, such as offering discounts or coupons to nearby retail stores.

geostationary orbit (GEO) Satellites can be positioned in three primary orbits: low Earth orbit (LEO), 160–2,000 km, medium Earth orbit (MEO), 2,000–35,786 km, and geostationary orbit (GEO), 35,786 km. GEO satellites appear motionless in the sky as they are rotating around the earth at the same angular velocity as the earth rotates. Thus, GEO satellites maintain a fixed position above a terrestrial location. GEO satellites have a larger transmission footprint than MEO satellites but also a higher latency. But GEO satellites do not require that a ground station track the movement of the satellite across the sky as is necessary with LEO and MEO satellites, so GEO ground stations can use fixed antennas. *See* low Earth orbit (LEO) and medium Earth orbit (MEO).

Geotagging, geo-tagging The ability of mobile devices with GPS support to embed geographical location in the form of latitude and longitude as well as date/time information on photos and videos taken with these devices, along with messages posted from the device.

Global Positioning System (GPS) A satellite-based geographical location service supported by most mobile devices.

Global Privacy Standard (GPS) A set of universal and harmonized privacy principles derived from **Privacy by Design** (**PbD**). GPS is to be adopted by countries to use as a guide in developing privacy legislation, used by organizations to integrate privacy protection into their operations, and used by developers to integrate privacy into the products they produce.

GNU Privacy Guard (GnuPG, GPG) A free and open source implementation of the OpenPGP standard. It is a free/open variation of the now-commercial Pretty Good Privacy (PGP) product.

Goguen–Meseguer model An integrity model based on predetermining the set or domain of objects that a subject can access.

golden ticket An attack that obtains the hash of the Kerberos service account, granting the attacker the ability to create tickets at will within Active Directory.

Government Information Security Reform Act of 2000 Act that amends the U.S. Code to implement additional information security policies and procedures.

government classification, military classification The security labels commonly employed on secure systems used by the military. Military security labels range from highest sensitivity to lowest: top secret, secret, confidential, and unclassified (top secret, secret, and confidential are collectively known as classified).

GPS tagging *See* geolocation and geotagging.

Graham–Denning model A security model focused on the secure creation and deletion of both subjects and objects.

Gramm–Leach–Bliley Act (GLBA) A law passed in 1999 that eased the strict governmental barriers between financial institutions. Banks, insurance companies, and credit providers were severely limited in the services they could provide and the information they could share with each other. GLBA somewhat relaxed the regulations concerning the services each organization could provide.

granular object control A very specific and highly detailed level of control over the security settings of an object.

graph database A type of NoSQL database structure that stores data in graph format, using nodes to represent objects and edges to represent relationships. They are useful for representing any type of network, such as social networks, geographic locations, and other datasets that lend themselves to graph representations.

gratuitous ARP A gratuitous Address Resolution Protocol (ARP) broadcast may be sent as an announcement of a node's existence, to update an ARP mapping due to a change in IP address or MAC address, or when redundant devices are in use that share an IP address and may also share the same MAC address (regularly occurring gratuitous ARP announcements help to ensure reliable failover). This occurs when a system announces its MAC-to-IP mapping without being prompted by an ARP query. Aka unsolicited ARP.

gray box This term is deprecated. *See* partially known environment.

gray hat This term is deprecated. *See* semi-authorized entity/hacker.

`grep` A command used to search for a string or a pattern in a file and display the results. This command can search using text strings, regex patterns, or Perl statements.

grid computing A form of parallel distributed processing that loosely groups a significant number of processing nodes toward the completion of a specific processing goal.

ground The wire in an electrical circuit that is grounded (that is, connected with the earth).

group An access control management simplification mechanism similar to a role. Similar users are made members of a group. A group is assigned access to an object. Thus, all members of the group are granted the same access to an object. The use of groups greatly simplifies the administrative overhead of managing user access to objects.

Group Policy Object (GPO) A Windows-specific security configuration control mechanism similar to that of a security template.

group-based privilege The assignment of a privilege or access to a resource to all members of a group as a collective.

grudge attack An attack usually motivated by a feeling of resentment and carried out to damage an organization or a person. The damage could be in the loss of information or harm to the organization or a person's reputation. Often the attacker is a current or former employee or someone who wishes ill will upon an organization.

guard *See* security guard.

guard dog A canine used as a perimeter security control.

guest account (1) A native account on Windows OSs that is disabled by default. (2) A shared account for visitors. (3) A unique account for each guest, with limited privileges.

guest network An area of a private network designated for use by temporary authorized visitors. Aka guest zone.

guest OS An OS operating in a virtual machine.

guideline A document that offers recommendations on how standards and baselines are implemented. Guidelines outline methodologies, include suggested actions, and are not compulsory.

H

hacker Historically, a technology enthusiast who does not have malicious intent. Someone who manipulates computer systems. This can include changing their function or repairing issues. Hackers are ethical if operating with permission and authorization but are often committing crimes when operating without permission or when violating terms of service, terms of agreement, service-level agreements (SLAs), end-user license agreements (EULAs), or laws. *See also* unauthorized entity.

hacktivist Someone who uses their hacking skills for a cause or purpose. A hacktivist commits criminal activities for the furtherance of their cause. Hacktivists attack targets even when they know they will be identified, apprehended, and prosecuted. They do this because they believe their purpose or cause is more important than the consequences to themselves. *See* suicide hacker.

half-duplex Two-way communication, but only one direction can send data at a time.

halon A fire-suppressant material that converts to toxic gases at 900 degrees Fahrenheit and depletes the ozone layer of the atmosphere and is therefore usually replaced by an alternative material.

hand geometry A type of biometric control that recognizes the physical dimensions of a hand. This includes width and length of the palm and fingers. It can be a mechanical or image-edge (in other words, visual silhouette) graphical solution.

handler A nickname for the owner or hacker controlling a botnet. Aka master or bot herder.

handshake The process of agreeing to communicate, establish a session, and share data. Transmission Control Protocol (TCP) uses a three-way handshake to establish connections, and part of this process can be exploited by SYN attacks. TLS uses a multistep process to authenticate endpoints, select a cipher suite, negotiate keys, and establish a secured session between a client and server.

hard drive encryption A security solution to encrypt the contents of a storage device using either a software or hardware mechanism.

hardening, harden The process of reducing vulnerabilities, managing risk, and improving the security provided by a system.

hardware An actual physical device, such as a hard drive, LAN card, printer, router, WAP, and so on.

hardware root of trust The concept that the basis of security or attestation of hardware is founded on a secure supply chain. The security of a system is ultimately dependent on the reliability and security of the components that make up the computer as well as the process it went through to be crafted from original raw materials.

hardware security module (HSM) A cryptoprocessor used to manage/store digital encryption keys, accelerate crypto operations, support faster digital signatures, and improve authentication.

hardware segmentation A technique that implements process isolation at the hardware level by enforcing memory access constraints.

Harrison–Ruzzo–Ullman (HRU) model A security model that focuses on the assignment of object access rights to subjects as well as the resilience of those assigned rights. It is an extension of the Graham–Denning model.

hash, hashing, hash function The process of taking a dataset or message and generating a unique representative output value derived from the content of the message.

hash chain A linked set of passwords and hashes created using a hashing algorithm and a corresponding reduction function (a process that produces a new password from a hash value), which is ultimately used in the password attack known as rainbow tables.

hash, hash value A number known as a message digest generated from a hash function. Aka fingerprint, thumbprint, message digest, and message authenticating code (MAC).

hash total A checksum used to verify the integrity of a transmission. *See also* cyclic redundancy check (CRC).

Hashed Message Authentication Code (HMAC), Hash-based Message Authentication Code An algorithm that implements a partial digital signature—it guarantees the integrity of a message during transmission, but it does not provide for nonrepudiation.

head A Linux/Unix command that displays the first 10 lines of a file. It can also be used to display a customized number of lines or bytes from the beginning of a file.

header Information added by a protocol to the front of a payload received from a higher-layer protocol.

header manipulation A form of attack in which malicious content is submitted to a vulnerable application, typically a web browser or web server, under the guise of a valid HTML/HTTP header value.

Health Information Technology for Economic and Clinical Health Act (HITECH) In 2009, Congress amended HIPAA by passing the Health Information Technology for Economic and Clinical Health (HITECH) Act. This law updated many of HIPAA's privacy and security requirements and was implemented through the HIPAA Omnibus Rule in 2013. One of the changes mandated by the new regulations is a change in the way the law treats business associates (BAs), organizations that handle protected health information (PHI) on behalf of a HIPAA-covered entity. HITECH also introduced new data breach notification requirements.

Health Insurance Portability and Accountability Act (HIPAA) A law passed in 1996 that made numerous changes to the laws governing health insurance and health maintenance organizations (HMOs). Among the provisions of HIPAA are privacy regulations requiring strict security measures for hospitals, physicians, insurance companies, and other organizations that process or store private medical information about individuals.

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

heart pattern, pulse pattern An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The heart/pulse pattern of a person is used to establish identity or provide authentication.

heartbeat sensor A mechanism by which a communication pathway is either constantly or periodically checked with a test signal.

heat map (1) A mapping of wireless signal strength measurements over a building's blueprint. A site survey often produces a heat map. (2) *See* risk matrix.

heating, ventilating, and air conditioning (HVAC) The technology of indoor environmental comfort. Proper HVAC management is essential for security to protect and maintain the operating conditions (such as temperature, humidity, and debris) of servers in a datacenter.

Hertz (Hz) Frequency is a measurement of the number of wave oscillations within a specific time and identified using the unit Hertz (Hz) (i.e., oscillations per second).

heuristic based detection, heuristic detection, heuristic-based detection An intrusion detection method that functions by comparing suspicious or new programs against known examples of malware. *See also* anomaly-based detection, behavior-based detection, and signature-based detection.

HIDS *See* host-based IDS (HIDS)/host-based IPS (HIPS).

hierarchical A form of Mandatory Access Control (MAC) environment. Hierarchical environments relate the various classification labels in an ordered structure from low security to medium security to high security. Each level or classification label in the structure is related. Clearance in a level grants the subject access to objects in that level as well as to all objects in all lower levels but prohibits access to all objects in higher levels. *See also* compartmentalized MAC environment and hybrid MAC environment.

hierarchical data model A form of database that combines records and fields that are related in a logical tree structure. This is done so that each field can have one child or many or no children but each field can have only a single parent. Therefore, the data mapping relationship is one-to-many.

hierarchical data structure A means of data organization in which every data object can have a single data-parent relation and one, many, or no data-child relations.

high availability The use of redundant technology components to allow a system to quickly recover from a failure after experiencing a brief disruption. High availability is often achieved through the use of load balancing and failover servers. High availability is often measured as a percentage of a year when resources are available that is expressed as a number of 9s.

high-performance computing (HPC) systems Computing platforms designed to perform complex calculations or data manipulations at extremely high speeds. Supercomputers and MPP solutions are common examples of HPC systems. HPC systems are used when real-time or near-real-time processing of massive data is necessary for a particular task or application. These applications can include scientific studies, industrial research, medical analysis, societal solutions, and commercial endeavors.

high resiliency system Computing devices that ensure reliable communications and data storage, often requiring more computational capabilities than standard systems and at the expense of higher latency.

High-level Data Link Control (HDLC) A layer 2 protocol used to transmit data over synchronous communication lines. HDLC is an ISO standard based on IBM's SDLC. HDLC supports full-duplex communications, supports both point-to-point and multipoint connections, offers flow control, and includes error detection and correction.

high-level languages Programming languages that are not machine languages or assembly languages. These languages are not hardware dependent and are more understandable by humans. Such languages must be converted to machine language before or during execution.

High-Speed Serial Interface (HSSI) A layer 1 protocol used to connect routers and multiplexers to ATM or Frame Relay connection devices.

hijack attack, hijacking An attack in which a malicious user is positioned between a client and server and then interrupts the session and takes it over. Often, the malicious user impersonates the client so they can extract data from the server. The server is unaware that any change in the communication partner has occurred.

HIPS *See* host-based IDS (HIDS)/host-based IPS (HIPS).

HMAC *See* Hashed Message Authentication Code (HMAC).

HMAC-based one-time password (HOTP) A means by which a device or application generates passwords based on a nonrepeating one-way function, such as a hash or Hash Message Authentication Code (HMAC) operation. An asynchronous dynamic password token uses HOTP.

hoax, virus hoax A form of social engineering attack that uses the specter of malicious code to trick users into damaging their own system. 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 could.

homograph attack A DNS attack that leverages the similarities in character sets to register phony international domain names (IDNs) that to the naked eye appear legitimate.

homomorphic encryption A cryptographic system that enables data to remain in ciphertext form while data manipulation operations are performed against it. This allows for data to retain confidentiality protection while being actively processed (i.e., data in use/data in processing) by a specialized application.

honeyfiles False work files that are used to tempt intruders or problematic insiders.

honeynet Two or more networked honeypots used in tandem to monitor or re-create larger, more diverse network arrangements. *See* honeypot.

honeypot, honeynet A honeypot is an individual computer created to serve as a snare for intruders. An entire network created for this purpose is known as a honeynet. The honeynet/honeypot looks and acts like a legitimate system, but it is 100 percent fake. Honeynets/honeypots tempt intruders with unpatched and unprotected security vulnerabilities as well as hosting attractive, tantalizing, but faux data. Honeynets/honeypots are designed to grab an intruder's attention and direct them into the restricted playground while keeping them away from the legitimate network and confidential resources.

hookup, hook-up A composition theory that states that one system sends input to another system but also sends input to external entities.

hop limit The IPv6 equivalent of the IPv4 TTL. *See* time to live.

horizontal distribution system Provides the connections between the telecommunication room and work areas; often includes cabling, cross-connection blocks, patch panels, and supporting hardware infrastructure (such as cable trays, cable hangers, and conduits).

host Any network device with a Transmission Control Protocol/Internet Protocol (TCP/IP) network address.

host elasticity A feature or function of virtualization in which additional hardware hosts can be booted when needed and then used to distribute the workload of the virtualized services over the newly available capacity.

hostname (1) The local system name. (2) An alternate term for subdomain in a fully qualified domain name (FQDN). *See* subdomain.

host-based firewall A security filtering application that is installed on client systems. Aka personal software firewall, local firewall, OS firewall, and software firewall.

host-based IDS (HIDS) An intrusion detection system (IDS) that is installed on a single computer and can monitor the activities on that computer. A host-based IDS is able to pinpoint the files and processes compromised or employed by a malicious user to perform unauthorized activity. The alternative is a network-based system.

host-based IPS (HIPS) An intrusion prevention system that is host based. The alternative is a network-based system.

Host-to-Host The original name of the third layer of the TCP/IP model, which is sometimes replaced by Transport.

hosted solution A deployment concept in which the organization must license software, which it then operates and maintains. The hosting provider owns, operates, and maintains the hardware that supports the organization's software.

hostile applet Any piece of mobile code that attempts to perform unwanted or malicious activities.

HOSTS file A static local file with DNS entries that are preloaded into a DNS cache when a system boots. HOSTS files predate query-based DNS.

hot aisle *See* hot and cold aisles.

hot and cold aisles, hot aisle cold aisle A means of maintaining optimum operating temperature in large server rooms that creates a type of circulating air pattern intended to optimize the cooling process.

hot rollover A fault-tolerance configuration in which the switch from primary to secondary system is performed automatically as soon as a problem is encountered. Aka automatic rollover.

hot site A configuration in which a backup facility is maintained in constant working order, with a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities. A location that can provide complete operations support within hours of a failure to minimize or eliminate downtime in the event of a disaster affecting a company's primary location.

hotfix A patch that is only modestly tested and usually aimed at a single particular problem.

HOTP *See* HMAC-based one-time password (HOTP).

hotspot A form of tethering where a device's telco data service is shared over Wi-Fi. The mobile device operates as a WAP.

`hping` A network mapper/port scanner and packet generator. It is often used to stress-test firewalls and other network security devices, perform advanced traceroute, perform OS fingerprinting, and more. It is often used as a companion utility to `nmap`.

HSM *See* hardware security module (HSM).

HTML injection A reflected XSS event, but instead of using JavaScript or other code, it plants custom HTML statements. *See* cross-site scripting (XSS) and injection attacks.

HTML *See* Hypertext Markup Language (HTML).

HTTP headers A mechanism of web communication to exchange information between a web client (request headers) and server (response headers). A client's request header will indicate an HTTP method to be used to perform some action. The most common methods are `GET`, `POST`, and `HEAD`, but there are others, such as `PUT`, `TRACE`, `DELETE`, `CONNECT`, `PATCH`, and `OPTIONS`.

HTTP *See* Hypertext Transfer Protocol (HTTP).

HTTP Strict Transport Security (HSTS) Defined in RFC 6797, a server configuration that prohibits access to its contents via plaintext HTTP and mandates that all requests be HTTPS.

HTTPS *See* Hypertext Transfer Protocol Secured (HTTPS).

hub A network device used to connect multiple systems together in a star topology. Hubs repeat inbound traffic over all outbound ports. Hubs are a legacy networking device that you are unlikely to find in standard networks today.

human-made disasters Disasters caused by humans, including explosions, electrical fires, terrorist acts, power outages, utility failures, hardware/software failures, labor difficulties, theft, and vandalism.

HVAC *See* heating, ventilating, and air conditioning (HVAC).

hybrid assessment, hybrid analysis A risk assessment combining quantitative and qualitative analysis into a final assessment of organizational risk.

hybrid attack A form of password attack in which a dictionary attack is first attempted and then a type of brute-force attack is performed. The follow-up brute-force attack is used to add prefix or suffix characters to passwords from the dictionary in order to discover one-upped constructed passwords, two-upped constructed passwords, and so on.

hybrid cloud A cloud model that includes a combination of two or more cloud concepts, such as public, private, and/or community clouds.

hybrid cryptography The approach of combining symmetric and asymmetric cryptography.

hybrid federation An identity management (IdM) or single sign-on solution consisting of elements that are hosted partially on premises and partially in the cloud.

hybrid MAC environment A type of Mandatory Access Control (MAC) environment. A hybrid environment combines the hierarchical and compartmentalized concepts so that each hierarchical level can contain numerous subcompartments that are isolated from the rest of the security domain. A subject must have not only the correct clearance but also the need to know for the specific compartment to have access to the compartmentalized object. Compare with compartmentalized MAC environment and hierarchical MAC environment.

hybrid warfare Combining classical military strategy with modern capabilities, including digital influence campaigns, psychological warfare efforts, political tactics, and cyber warfare capabilities. Aka nonlinear warfare.

hyperlink spoofing An attack used to redirect traffic to a rogue or imposter system or to simply divert traffic away from its intended destination, often through the malicious alteration of the hyperlink URLs in the HTML code of documents sent to clients.

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

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

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) A standard that uses TCP port 443 to negotiate encrypted communications sessions between web servers and browser clients using the now deprecated SSL.

Hypertext Transfer Protocol Secured (HTTPS) The encrypted form of HTTP that currently uses TLS (previously used SSL) and mostly operates over TCP port 443.

Hypertext Transfer Protocol The protocol used to transmit web page elements from a web server to web browsers (over the well-known service TCP/UDP port address 80).

hypervisor The component of virtualization that creates, manages, and operates the virtual machines. The computer running the hypervisor is known as the host and the OSs running within a hypervisor-supported virtual machine are known as guest OSs. Aka virtual machine monitor (VMM) and virtual machine manager (VMM).

I

IaaS *See* infrastructure as a service (IaaS).

iBeacon A location tracking technology developed by Apple based on Bluetooth Low Energy (BLE). iBeacon can be used by a store to track customers while they shop as well as by customers as an indoor positioning system to navigate to an interior location.

ICMP *See* Internet Control Message Protocol (ICMP).

ICMP attack *See* Internet Control Message Protocol (ICMP) attack.

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

identification card A form of physical identification; generally contains a picture of the subject and/or a magnetic strip with additional information about a subject. *See* badge and security ID.

identity and access management (IAM) The combination of authentication and authorization into a single solution.

identity and access provisioning lifecycle The creation, management, and deletion of accounts. Provisioning refers to granting accounts with appropriate privileges when they are created and during the lifetime of the account.

identity as a service, identity and access as a service (IDaaS) A third-party service that provides identity and access management. IDaaS effectively provides SSO for the cloud and is especially useful when internal clients access cloud-based software-as-a-service (SaaS) applications.

identity fraud An attack where someone falsely claims to be someone else through the use of information stolen from the victim. Identity fraud is criminal impersonation or intentional deception for personal or financial gain.

identity management (IdM) The collection of technology, policies, and procedures that ensure that subjects are issued accounts with proper limited access to resources according to their assigned responsibilities. Aka identity and access management (IAM or IdAM).

identity provider (IdP) (1) A system that creates and manages identities and provides identification and authentication services. An IdP is often used within private networks as a centralized system, or it can be a service used to implement federation among distributed systems. (2) A trusted authentication service as related to Security Assertion Markup Language (SAML).

Identity Theft and Assumption Deterrence Act An act that makes identity theft a crime against the person whose identity was stolen and provides severe criminal penalties (up to a 15-year prison term and/or a $250,000 fine) for anyone found guilty of violating it.

identity theft The act of stealing someone's identity.

IDS *See* intrusion detection system (IDS).

IEEE 802.11 A family of protocols that provides for wireless communications using radio frequency transmissions. Wireless networks based on this standard use either 2.4 GHz or 5 GHz frequencies to support communications. The wireless networks made possible by this standard are called Wi-Fi today.

IEEE 802.1q The IEEE standard that defines VLAN tagging. VLAN tagging is used by switches and bridges to manage traffic within and between VLANs.

IEEE 802.1X A port-based authentication mechanism that ensures that clients can't communicate with a resource until proper authentication has taken place. Think of 802.1X as an authentication proxy. This technology enables the leveraging or use of an authentication system elsewhere on the network, rather than requiring on-device/system authentication (which is often limited to static passwords). Aka IEEE 802.1X/EAP. *See* Extensible Authentication Protocol (EAP) and enterprise (ENT).

IETF (Internet Engineering Task Force) *See* Internet Engineering Task Force (IETF).

`ifconfig` A Linux command tool used to manipulate the configuration settings of network interface cards, such as to display the current NIC configuration, enable and disable an interface, set an IP address, and remove an IP address. The `ifconfig` command is slated to be replaced by the newer `ip` command.

IGMP *See* Internet Group Management Protocol (IGMP).

ignoring risk, ignore risk In risk management, denying that a risk exists or hoping that by ignoring a risk it will never be realized. This is not a valid, prudent, due-care response to risk. *See* other related terms: acceptance, risk tolerance, assignment, transfer/transference (as related to risk), avoidance, reducing risk, mitigation, and rejecting risk. Aka risk rejection and reject risk.

IKE *See* Internet Key Exchange (IKE).

IM *See* instant messaging (IM).

IMAP *See* Internet Message Access Protocol (IMAP).

immediate addressing A way of referring to data that is supplied to the CPU as part of an instruction.

immutable system A server or software product that, once configured and deployed, is never altered in place. Instead, when a new version is needed or a change is necessary, a revised version is crafted and the new system is then deployed to replace the old one. Aka immutable architecture.

impact A measurement of the amount of damage or loss that could or would be caused if a potential threat is ever realized.

impersonation The assumption of someone's identity or online account, usually through the mechanisms of spoofing and session replay. An impersonation attack is considered a more active attack than masquerading. This can take place in person, over the phone, or through any other means of communication. Generally considered a form of social engineering.

implementation attack This type of attack exploits weaknesses in the implementation of a cryptography system. It focuses on exploiting the software code, not just errors and flaws but methodology employed to program the encryption system.

implicit deny The default security stance that if a subject isn't specifically/explicitly granted access to or privileges over a resource, then it is denied access by default. *See also* allow list. Aka deny by default.

Implicit SMTPS This is the TLS-encrypted form of SMTP, which assumes the target server supports TLS. If accurate, then an encrypted session is negotiated. If not, then the connection is terminated because plaintext is not accepted. SMTPS communications are initiated against TCP port 465.

inappropriate activities Actions that may take place on a computer or over the IT infrastructure and that may not be actual crimes but are often grounds for internal punishments or termination. Some types of inappropriate activities include viewing inappropriate content, sexual and racial harassment, waste, and abuse.

in-band, in-band key exchange An exchange that takes place within the existing and established communication channel or pathway.

in-band intrusion detection system (IDS) An IDS deployed and configured to monitor and filter both the pre-connect activities and post-connect activities of each session. Pre-connect activities can include authentication as well as verifying compliance with minimal security requirements before a session is allowed to be established. Post-connect activities include traffic monitoring, content filtering, identity-based access controls, and ongoing verification that the connection that was granted is still valid and should be allowed to continue.

incident Any attempt to violate a security policy, a successful penetration, a compromise of a system, or any unauthorized access to information. Any event that has a negative effect on the confidentiality, integrity, or availability of an organization's assets. Aka computer security incident and security incident.

incident response, incident response plan (IRP), incident response procedure (IRP) A planned action to take to handle any violations of security policy. The SOP that defines how to prevent incidents, how to detect incidents, how to respond to incidents, and how to return to normal when the incident is concluded. Aka incident response procedure, incident response process, or incident management.

incremental attack A form of attack that occurs in slow, gradual increments rather than through fast, obvious, or recognizable attempts to compromise system security or integrity. *See* data diddling and salami attack.

incremental backup A type of backup that includes only new files or files that have changed since the last full backup or the last incremental backup. Incremental backups clear the archive bit or change the timestamps of files on completion.

independent service set identifier (ISSID) The SSID used by Wi-Fi Direct and ad hoc mode networks.

indicator An observable along with a hypothesis about a threat. *See* observable.

indicators of compromise (IoCs) Evidence that an intrusion or security breach has taken place. They are the symptoms that security administrators look for to know they need to dig deeper to find more details and attempt to track down the root cause.

indirect addressing The memory address that is supplied to the CPU as part of the instruction and doesn't contain the actual value that the CPU is to use as an operand. Instead, the memory address contains another memory address (perhaps located on a different page). The CPU then retrieves the actual operand from that address.

industrial camouflage The attempt to mask or hide the actual function, purpose, or operations of a facility by providing a façade presenting a believable or convincing alternative.

industrial control system (ICS) A form of computer-management device that controls industrial processes and machines. ICSs are used across a wide range of industries, including manufacturing, fabrication, electricity generation and distribution, water distribution, sewage processing, and oil refining. There are several forms of ICS, including distributed control systems (DCSs), programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA).

industrial espionage The act of someone using illegal means to acquire competitive information.

Industrial Internet of Things (IIoT) A derivative of IoT that focuses more on industrial, engineering, manufacturing, or infrastructure level oversight, automation, management, and sensing. IIoT is an evolution of ICS and DCS that integrates cloud services to perform data collection, analysis, optimization, and automation.

inference An attack that involves using a combination of several pieces of non-sensitive information to gain access to information that should be classified at a higher level.

inference engine The second major component of an expert system that analyzes information in the knowledge base to arrive at the appropriate decision.

influence campaigns Social engineering attacks that attempt to guide, adjust, or change public opinion.

information classification policies Written policies that dictate which classifications or value labels are to be used for particular types of data. Data/information classification defines the importance of data as well as the security mechanisms necessary to provide

sufficient protection for the data based on its value. These policies may also detail the means and methods of information dissemination, such as whether encryption is needed or whether removable media can be used for storage and transfer.

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

information disclosure The revelation or distribution of private, confidential, or controlled information to external or unauthorized entities. *See* STRIDE.

information flow model A model that focuses on the flow of information to ensure that security is maintained and enforced no matter how information flows. Information flow models are based on a state machine model.

information hiding Placing data and a subject at different security domains for the purpose of hiding the data from that subject.

information lifecycle The series of changes of data through its existence. A typical information lifecycle starts at creation or capture and then moves into classification, then secure storage, then protected use, then archiving, then destruction or purging. Aka information life cycle.

information security (InfoSec) officer The role assigned to a trained and experienced network, systems, and security engineer who is responsible for following the directives mandated by senior management. Also serves as the primary lead of the InfoSec team.

information security (InfoSec) team The team or department responsible for security within an organization.

information security officer (ISO) Another potential term for the CISO, but this also can be used as a subposition under the CISO. A leading or managing position on the InfoSec team. *See also* chief security officer (CSO) and chief information security officer (CISO).

information systems (IS) *See* information technology (IT).

information technology (IT) The use of systems, such as computers and networks, for the transfer, storage, and processing of data or information. Aka information systems (IS).

Information Technology Infrastructure Library (ITIL) Initially crafted by the British government, ITIL is a set of recommended best practices for optimization of IT services to support business growth, transformation, and change. ITIL focuses on understanding how IT and security need to be integrated with and aligned to the objectives of an organization. ITIL is often used as a starting point for the crafting of a customized IT security solution within an established infrastructure.

informative policy A policy designed to provide information or knowledge about a specific subject, such as company goals, mission statements, or how the organization interacts with partners and customers. An informative policy is not enforceable.

infrared A line-of-sight–based nonvisible light communications system that can be easily interrupted. Aka PIR (passive infrared).

infrared motion detector A device that monitors for significant or meaningful changes in the heat levels and patterns in a monitored area. Aka heat-based motion detector.

infrastructure as a service (IaaS) A cloud computing concept that can provide not just on-demand operating solutions but complete outsourcing of IT infrastructure.

infrastructure as code (IaC) Infrastructure as code is a change in how hardware management is perceived and handled. Instead of seeing hardware configuration as a manual, direct hands-on, one-on-one administration hassle, it is viewed as just another collection of elements to be managed in the same way that software and code are managed under DevOps.

infrastructure mode A configuration of an 802.11 wireless network in which a wireless access point (WAP) is used to support connections of wireless clients for communication with each other as well as to an attached wired network.

ingress filter A traffic filter on packets coming into a secured area from outside (inbound communications).

inherent risk The level of natural, native, or default risk that exists in an environment, system, or product prior to any risk management efforts being performed. Aka initial risk or starting risk.

inherit, inheritance In object-oriented programming, inheritance refers to a class that has one or more of the same methods from another class. So when a method has one or more of the same methods from another class, it is said to have inherited them.

initial exploitation In a penetration test or a real-world malicious attack, the event that grants the attacker/tester access to the system. It is the first successful breach of the organization's security infrastructure that grants the attacker/tester some level of command control or remote access to the target.

initialization vector (IV) A mathematical and cryptographic term for a random number. Most modern crypto functions use IVs to increase their security by reducing predictability and repeatability through the integration of entropy or randomness. An IV becomes a point of weakness when it's too short, exchanged in plaintext, or selected improperly.

initialization vector (IV) attack An attack that takes advantage of the weakness of IVs to break encryption. Initialization vector is a mathematical and cryptographic term for a random number.

injection attack Any exploitation that allows an attacker to submit code to a target system to modify its operations and/or poison and corrupt its dataset. *See* SQL injection, LDAP injection, DLL injection, HTML injection, and XML injection. Aka injection vulnerabilities.

inline IPS A type of intrusion protection system (IPS) that has two interfaces and requires all traffic to traverse through the IPS. Traffic enters either interface, is evaluated by the IPS analysis engine, and then exits the other interface on its way to the destination.

input blacklisting A means to control user input. With this approach, developers do not try to explicitly describe acceptable input but instead describe potentially malicious input that must be blocked. Aka input block listing.

input sanitization An input filtering concept that checks length, scans for the presence of known malicious content, and escapes metacharacters. Aka input filtering and input checking. *See also* input validation.

input validation An aspect of defensive programming intended to ward off a wide range of input-focused attacks, such as buffer overflows and fuzzing. Checking, scanning, filtering, or sanitizing input received from users (especially over the internet) before processing the received input. *See also* input sanitization.

input whitelisting The most effective form of input validation in which the developer describes the exact type of input that is expected from the user and then verifies that the input matches that specification before passing the input to other processes or servers. Aka input allow listing.

inrush An initial surge of power usually associated with connecting to a power source, whether primary or alternate/secondary.

insecure direct object reference If an application does not perform authorization checks, the user may be permitted to view information that exceeds their authority when directly accessed.

instance awareness An important cloud security feature where a management or security mechanism is able to monitor and differentiate between numerous instances of the same VM, service, app, or resource.

instance In object-oriented programming, an instance can be an object, example, or representation of a class.

instant messaging (IM) Any mechanism that allows for real-time text-based chat between two users located anywhere on the internet. Most IM utilities allow for file transfer, multimedia, voice and videoconferencing, and more. From a security standpoint, risks associated with giving out information via IM can be used in social-engineering attacks; in addition, attachments can contain viruses. The term IM has fallen out of favor in deference to newer terms such as online chat, real-time texting, or just messaging.

intangible assets Intellectual property and other non-physical assets owned by the company.

integer overflow The state that occurs when a mathematical operation attempts to create a numeric value that is too large to be contained or represented by the allocated storage space or memory structure.

Integrated Services Digital Network (ISDN) A digital end-to-end communications mechanism. ISDN was developed by telephone companies to support digital communications over the same equipment and infrastructure that is used to carry voice communications. New installations of ISDN are unlikely since DSL, cable, and wireless-based broadband solutions are faster and less expensive.

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

integrity verification procedure (IVP) In relation to the Clark–Wilson model, a procedure that scans data items and confirms their integrity.

intellectual property (IP) The intangible creation of personal property that is owned and protected by an organization. Examples include confidential data, copyrights, trademarks, patents, and trade secrets.

intelligence fusion The combination of local logs with multiple sources of threat intelligence integrated into a useful analysis or report.

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

interconnection security agreement (ISA) A formal declaration of the security stance, risks, and technical requirements of a link between two organizations' IT infrastructures. The goal of an ISA is to define the expectations and responsibilities of maintaining security over a communications path between two networks.

Interface Definition Language (IDL) A language used to define the interface between client and server processes or objects in a distributed system. IDL enables the creation of interfaces between objects when those objects are in varying locations or are using different programming languages; thus, IDL interfaces are language independent and location independent. There are numerous examples of DCE IDLs or frameworks, such as remote procedure calls (RPCs), the Common Object Request Broker Architecture (CORBA), and the Distributed Component Object Model (DCOM).

interface testing Interface testing assesses the performance of modules against the interface specifications to ensure that they will work together properly when all of the development efforts are complete.

interference *See* electromagnetic interference (EMI) and radio frequency interference (RFI).

Interior Gateway Routing Protocol (IGRP) An example of a distance vector routing protocol.

interior routing protocols A routing protocol used on a router inside a private network.

intermediate CA Any certificate authority (CA) positioned below a root or another CA, but above any leaf CAs. Aka subordinate CA.

intermediate distribution facilities *See* wiring closet.

Intermediate Distribution Frame (IDF) Secondary wiring closets that connect the cabling on other floors to the MDF.

Intermediate System-Intermediate System (IS-IS), Intermediate System to Intermediate System An example of a link state routing protocol.

internal audit An audit performed by an organization's internal audit staff and typically intended for internal audiences.

internal segmentation firewall (ISFW) A firewall deployed between internal network segments or company divisions. Its purpose is to prevent the further spread of malicious code or harmful protocols already within the private network. With an ISFW, network segments can be created without resorting to air gaps, VLANs, or subnet divisions. An ISFW is commonly used in microsegmentation architectures.

International Data Encryption Algorithm (IDEA) A symmetric block cipher that uses a 128-bit key and 64-bit blocks. IDEA is used in Pretty Good Privacy (PGP).

International Organization for Standardization (ISO) An independent oversight organization that defines and maintains computer, networking, and technology standards, along with more than 13,000 other international standards for business, government, and society.

internet (1) A global network made up of a large number of individual networks that are interconnected and use TCP/IP protocols. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP). (2) The alternate name for the second layer of the TCP/IP model, originally Internetworking.

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

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

Internet Engineering Task Force (IETF) An open international community of technical experts that focuses on establishing and maintaining technology standards for the internet, networking, and computing.

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

Internet Group membership Authentication Protocol (IGAP) A multicast protocol that validates members of multicast groups and that often works in concert with Internet Group Management Protocol (IGMP).

Internet Key Exchange (IKE) A component of Internet Protocol Security (IPsec) that manages the cryptography keys needed for secure authentication, hashing, and encryption. The components of IKE are Oakley, Secure Key Exchange Mechanism (SKEME), and Internet Security Association Key Management Protocol (ISAKMP).

Internet layer The Transmission Control Protocol/Internet Protocol (TCP/IP) layer that maps to the Network layer of the Open Systems Interconnection (OSI) model responsible for routing, IP addressing, and packaging.

Internet Message Access Protocol (IMAP) A protocol used to transfer email messages from an email server to an email client. Allows for messages to be saved or archived on the email server rather than the client (as is the limitation with Post Office Protocol [POP]).

Internet of Things (IoT) The collection of devices that can communicate over the internet with each other or with a control console in order to affect and monitor the real world. IoT devices can provide automation, remote control, or AI processing to traditional or new appliances or devices in a home or office setting.

Internet Protocol (IP) The protocol in the TCP/IP suite responsible for network addressing and routing. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

Internet Protocol (IP) schema An organizational plan for the assignment of IP network addresses.

Internet Protocol Security (IPsec) The standard of IP security extensions used as an add-on for IPv4 and integrated into IPv6. IPsec provides encrypted communication tunnels between individual systems or entire networks. *See* Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE), and Internet Security Association and Key Management Protocol (ISAKMP).

internet relay chat (IRC) An early real-time chat service on the internet.

Internet Security Association and Key Management Protocol (ISAKMP) A subcomponent of Internet Key Exchange (IKE) from Internet Protocol Security (IPsec) that manages the per-connection security associations (i.e., encrypt keys associated with a specific virtual private network [VPN] session) or profiles to support multiple simultaneous encrypted links.

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

Internet Small Computer System Interface (iSCSI) A networking storage standard based on IP. This technology can be used to enable location-independent file storage, transmission, and retrieval over LAN, WAN, or public internet connections. iSCSI is often viewed as a low-cost alternative to Fibre Channel.

Internetwork Packet Exchange (IPX) IPX is the Network layer protocol of IPX/SPX. The IPX/SPX protocol suite was commonly used (although not strictly required to be used) on Novell NetWare networks in the 1990s.

Internetworking The original name of the second layer of the TCP/IP model, often replaced by internet.

interoperability agreement A formal contract (or at least a written document) that defines some form of arrangement in which two entities agree to work with each other in some capacity.

interpreted languages Programming languages that are converted to machine language one command at a time at the time of execution.

interrogation Questioning a person suspected of committing a crime. *See also* interview.

interrupt (IRQ) A mechanism used by devices and components in a computer to get the attention of the CPU.

interview Questioning a person to gather information to assist with a criminal investigation. In an interview, the person being questioned is not suspected of committing the crime. *See also* interrogation.

intimidation A social-engineering technique based on the concept that many people will respond or follow when threatened.

intranet A private network or private LAN.

intrusion The condition in which a threat agent has gained access to an organization's infrastructure through the circumvention of security controls and is able to directly imperil assets. Also referred to as penetration, breach, or attack.

intrusion detection A mechanism of detecting violations of security that specifically watches for the occurrences of physical or logical access by unauthorized entities to a secured environment. A specific form of monitoring and analysis of both recorded information and real-time events to detect unwanted system access.

intrusion detection system (IDS) (1) A product that automates the inspection of audit logs and real-time system events. IDSs are generally used to detect intrusion attempts, but they can also be employed to detect system failures or rate overall performance. A security tool that identifies and responds to attacks using defined rules or logic. An IDS can be network-based or host-based. (2) A form of burglar alarm system that detects and responds to physical intrusions of a facility.

intrusion prevention system (IPS) A tool designed to detect attempts to gain unauthorized access and prevent the attempts from becoming successful.

intrusive scan A type of vulnerability scan (aka active evaluation) that attempts to exploit any flaws or vulnerabilities detected.

in-vehicle computing system An embedded computer that is part of a motor vehicle. It includes the components used to monitor engine performance and optimize braking, steering, and suspension, but can also include in-dash elements related to driving, environment controls, and entertainment.

incipient smoke detection A fire detection system that detects a fire and triggers the release of the suppression medium when the sensor is able to detect the chemicals typically associated with the very early stages of combustion before a fire is otherwise detectible via other means. These devices are even more costly than flame-actuated sensors and are also only used in high-risk or critical environments. Aka aspirating sensors.

invoice scams A social-engineering attack that often attempts to steal funds from an organization or individuals through the presentation of a false invoice, often followed by strong inducements to pay. Attackers often try to target members of the financial departments or accounting groups. Some invoice scams are actually spear phishing scams in disguise.

iOS The mobile device operating system from Apple that is available on the iPhone, iPad, iPod, and Apple TV. This term can also refer to the Cisco IOS, which runs on Cisco's networking devices.

IP header protocol field value An element in an IP packet header that identifies the protocol used in the IP packet payload (usually this will be 6 for TCP, 17 for UDP, or 1 for ICMP, or any of a number of other valid routing protocol numbers).

IP Payload Compression (IPComp) protocol A protocol that allows IPsec users to achieve enhanced performance by compression packets prior to the encryption operation.

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

IP scanner Can refer to several tools of similar function, such as Angry IP Scanner and Advanced IP Scanner. These tools perform a network ping sweep and then follow up with various probes and queries to identify MAC address, OS type, and open ports.

IP Security (IPsec) A standards-based mechanism for providing encryption for point-to-point TCP/IP traffic.

IP *See* Internet Protocol (IP).

IP spoofing The process by which a malicious individual reconfigures their system so that it has the IP address of a trusted system and then attempts to gain access to other external resources. Can also be used to claim use of an IP address from a subnet that is not currently in use or assigned to another host.

`ip` The Linux command that is replacing `ifconfig`. This command can perform additional tasks, including adding ARP cache entries, displaying the routing table, and changing the routing table.

`ipconfig` The Windows command-line tool used to display IP configuration and make some modifications to the interface.

IPfix (Internet Protocol Flow Information Export) An IETF protocol used as a standard for exporting IP flow information. IPfix has generally replaced NetFlow for most non-Cisco vendors.

IPS *See* intrusion prevention system (IPS).

IPsec *See* Internet Protocol Security (IPsec).

IPv4 The version of the Internet Protocol that is most widely used around the world as of 2021. IPv4 uses a 32-bit addressing.

IPv6 The version of the Internet Protocol designed to replace IPv4, but it is still in early phases of adoption and deployment worldwide. IPv6 uses 128 bits for addressing. Some of IPv6's new features are scoped addresses, autoconfiguration, and quality of service (QoS) priority values. Scoped addresses give administrators the ability to group and then block or allow access to network services, such as file servers or printing. Autoconfiguration removes the need for both DHCP and network address translation (NAT). QoS priority values allow for traffic management based on prioritized content. Also, IPsec is native to IPv6, but it is an add-on for IPv4.

IRC *See* internet relay chat (IRC).

iris scans, iris scanner An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The colored portion of the eye that surrounds the pupil is used to establish identity or provide authentication.

ISAKMP *See* Internet Security Association and Key Management Protocol (ISAKMP).

iSCSI (Internet Small Computer System Interface) A networking storage standard based on Internet Protocol (IP). This technology can be used to enable location-independent file storage, transmission, and retrieval over local area network (LAN), wide area network (WAN), or public internet connections. iSCSI is often viewed as a low-cost alternative to Fibre Channel.

ISO *See* information security officer (ISO).

ISO *See* International Organization for Standardization (ISO).

ISO 2700 family group The collection of documents that define an international standard, which can be the basis of implementing organizational security and related management practices.

ISO 27001 Establishes the guidelines for implementing an information security management system (ISMS). It is the foundation of numerous other ISO standards, many of which are within the ISO 27000 family group. It prescribes that management perform a systematized evaluation of an organization's assets and threats (i.e., risk assessment), then design and implement a security response strategy to address the identified risks and adopt an ongoing management, oversight, and governance process to maintain and improve the security infrastructure over time.

ISO 27002 Prescribes best practices for the implementation and use of security controls within each of the 14 control groups from ISO 27001. ISO 27002 is effectively an extension of ISO 27001.

ISO 27701 An extension of ISO 27001 that focuses on privacy. It describes how to establish and maintain a privacy information management system (PIMS). It includes guidance on implementing compliance with a range of privacy regulations, including General Data Protection Regulation (GDPR).

ISO 31000 A family of standards and guidelines for implementing a risk management–based security program.

ISO 7816 interface The special contact interface on a smartcard.

isolation The act of keeping something separated from others. Isolation can be used to prevent commingling of information or disclosure of information. A concept that ensures that any behavior will affect only the memory and resources associated with the process. Isolation is often a proactive solution to prevent problems before they occur. *See* quarantine, confinement, and bounds.

ISP *See* internet service provider (ISP).

issue-specific security policy A security policy that focuses on a specific network service, department, function, or other aspect that is distinct from the organization as a whole.

IT as a service (ITaaS) Effectively an XaaS (anything as a service) concept. *See* software-defined data center (SDDC).

IT contingency plan (ITCP) A plan focused on the protection and/or recovery of an IT infrastructure. It's usually part of a business continuity plan (BCP) or a disaster recovery plan (DRP), although separate plans for IT can be crafted.

IT *See* information technology (IT).

IT closet *See* server vault or wiring closet.

IV attack *See* initialization vector (IV) attack.

J

jailbreak, jailbreaking Jailbreaking removes restrictions on Apple iOS devices and permits root-level access to the underlying operating system. It is similar to rooting a device running the Android operating system. *See also* rooting.

jamming The transmission of radio signals to prevent reliable communications by decreasing the effective signal-to-noise ratio.

Java A platform-independent programming language developed by Sun Microsystems. Java is still in use for internal development and business software, but its use on the internet is rare.

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 C. JavaScript is embedded into HTML documents using `<script></script>` enclosure tags.

JavaScript Object Notation (JSON) A common organizational and referencing format used by some NoSQL database options.

jitter Variable latency. *See* latency.

job description A detailed document outlining a specific position needed by an organization. A job description includes information about security classification, work tasks, and so on.

job responsibilities The specific work tasks an employee is required to perform on a regular basis.

job rotation A means by which an organization improves its overall security by rotating employees among numerous job positions. Job rotation serves two functions. First, it provides a type of knowledge redundancy. Second, moving personnel around reduces the risk of fraud, data modification, theft, sabotage, and misuse of information.

`journalctl` A command used to view the contents of logs generated by systemd on *nix systems. The output of this tool is similar to that of syslog in that the output includes date and time of the event, hostname, process name, and then log message.

jump A counterbalance to the application of separation of duties. Aka cross-training or rotation of duties.

jump server, jumpbox A remote access system deployed to make accessing a specific system or network easier or more secure. A jump server is often deployed in extranets, DMZs, or cloud networks where a standard direct link or private channel is not available or is not considered safe.

just-in-time (JIT) provisioning A federated identity solution that automatically creates the relationship between two entities so that new users can access resources. A JIT solution creates the connection without any administrator intervention.

K

KDC *See* key distribution center (KDC).

Keccak algorithm In 2012, the federal government announced the selection of the Keccak algorithm as the SHA-3 standard.

keep it simple A shortened form of the classic statement of "keep it simple, stupid" or "keep it stupid simple." This is sometimes called the KISS principle. In the realm of security, this concept is the encouragement to avoid overcomplicating the environment, organization, or product design. The more complex a system, the more difficult it is to secure.

Kerberos A ticket-based authentication mechanism that employs a trusted third party to provide identification and authentication. Typically used in private LANs as an SSO solution.

Kerckhoffs's assumption, Kerckhoffs's principle The idea that all algorithms should be public but all keys should remain private. Kerckhoffs's assumption or principle is held by a large number of cryptologists, but not all of them.

kernel The part of an operating system that always remains resident in memory (so that it can run on demand at any time).

kernel mode *See* protected mode.

key 1) A secret value used to control the encryption and decryption process. Aka cryptographic key, cryptovariable. 2) A column, attribute, or field of a database.

key clustering A weakness in cryptography where a plaintext message generates identical ciphertext messages using the same algorithm but different keys.

key destruction The removal of the encryption key or certificate from all software and hardware storage devices.

key distribution center (KDC) (1) An organization/facility that generates encryption keys for users. A COMSEC (Communications Security) facility that distributes symmetric crypto keys, especially for government entities. (2) The core element of a Kerberos solution that is composed of an authentication server (AS) and a ticket-granting server (TGS).

key escrow A storage process by which copies of private and/or secret encryption keys are retained by a centralized management system. Aka key escrow database.

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

key escrow system A cryptographic recovery mechanism by which keys are stored in a database and can be recovered only by authorized key escrow agents in the event of key loss or damage.

key exchange The process of transmitting encryption keys between communication partners. *See* Diffie–Hellman and digital envelope.

key length In cryptography, the length of an encryption key as measured in bits.

key management The process of managing encryption keys and/or digital certificates using a defined policy and procedure. Elements often include key creation, key storage, key use limitations, and key destruction. Aka key management practices.

key performance indicators (KPIs) Metrics or measurements of the operation or failure of various aspects of security. The goal of the use of KPIs is to assess the effectiveness of security efforts. Only with such information can management make informed decisions on altering existing security operations in order to achieve a higher level of effective security protection.

key recovery agent *See* recovery agent.

key recovery The process of extracting stored encryption keys from backup or escrow.

key space, keyspace The range of values that are valid for use as cryptographic keys for a specific algorithm.

key strength The relative benefit of a cipher's encryption key based on length and randomness. Generally, the longer the key length in terms of binary digits, the more strength it provides.

key stretching, key-stretching A collection of techniques that can take a weak encryption key or password and stretch it to become potentially more secure, at least against brute-force attacks. *See* Bcrypt and PBKDF2.

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

key/value store A type of NoSQL database structure that stores information in key/value pairs, where the key is essentially an index used to uniquely identify a record, which consists of a data value.

keylogger A potentially unwanted program (PUP) that records keystrokes.

keyspace, key space The range of values that are valid for use as a key for a specific algorithm.

keystroke dynamics A biometric factor that measures how a subject uses a keyboard by analyzing flight time and dwell time.

keystroke monitoring The act of recording the keystrokes a user performs on a physical keyboard. The act of recording can be visual (such as with a video recorder) or logical/technical (such as with a capturing hardware device or a software program).

keystroke patterns An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The pattern and speed of a person typing a passphrase is used to establish identity or provide authentication.

kiosk OS Either a standalone operating system (OS) or a variation of network operating system (NOS). A kiosk OS is designed for end-user use and access. The end user might be an employee of an organization or might be anyone from the general public. A kiosk OS is locked down so that only preauthorized software products and functions are enabled. The goal and purpose of a kiosk OS is to provide a robust information service to a user while preventing accidental or intentional misuse of the system.

knowledge base A component of an expert system, the knowledge base contains the rules known by an expert system and seeks to codify the knowledge of human experts in a series of "if/then" statements.

knowledge-based authentication When the user is asked one or more security questions. The questions may have been preselected (and pre-answered) or pulled from a knowledge base (such as your credit file).

knowledge-based detection An intrusion discovery mechanism used by intrusion detection systems (IDSs) and based on a database of known attack signatures. The primary drawback to a knowledge-based IDS is that it is effective only against known attack methods. Aka signature-based detection or pattern-matching detection.

known ciphertext A cryptographic attack focused on encryption systems that use the same key repeatedly or that select keys in a sequential or otherwise predictable manner. Variations include chosen ciphertext and adaptive chosen ciphertext.

known environment A device whose internal structure or processing is known and understood. This distinction is important in penetration testing, where a known environment testing proceeds and makes use of any knowledge of how an organization is structured, what kinds of hardware and software it uses, or its security policies, processes, and procedures. Aka fully known environment.

known plaintext attack A cryptographic attack focused on encryption systems that use the same key repeatedly or that select keys in a sequential or otherwise predictable manner. The attacker has a copy of the encrypted message along with the plaintext message used to generate the ciphertext (the copy). This greatly assists the attacker in breaking weaker codes. Variations include chosen plaintext and adaptive chosen plaintext.

KryptoKnight A ticket-based authentication mechanism similar to Kerberos but based on peer-to-peer authentication.

L

L2TP *See* Layer 2 Tunneling Protocol (L2TP).

LAN *See* local area network (LAN).

LAN extender A remote access, multilayer switch used to connect distant networks over WAN links. This is a strange beast of a device in that it creates WANs, but marketers of this device steer clear of the term *WAN* and use only the terms *LAN* and *extended LAN*. The idea behind this device was to make the terminology easier to understand and thus make the device easier to sell than a more conventional WAN device grounded in complex concepts and terms.

LAN Manager (LM, LANMAN) A legacy storage mechanism developed by Microsoft to store passwords. LM was replaced by New Technology LAN Manager (NTLM).

land attack A type of denial-of-service (DoS) attack. A land attack occurs when the attacker sends numerous SYN packets to a victim and the SYN packets have been spoofed

to use the same source and destination IP address and port number as the victim. This causes the victim to think it sent a TCP/IP session opening packet to itself, which causes a system failure, usually resulting in a freeze, crash, or reboot.

last known good configuration (LKGC) A collection of settings, services, and device drivers but not likely to include any third-party software elements, such as code present before a patch was applied. A rollback to the LKGC is useful after a setting change that had undesired consequences, but not after installing a new version of a software product (for that, use revert to known state, snapshot, or backup). *See* revert to known state.

latency The delay in a communication. Can be in relation to a one-way transmission or the round-trip time of a response. Often measured in milliseconds. *See* jitter.

lateral movement After an initial successful intrusion and pivoting to a new internal target, the act of gaining remote access control or just remote code execution abilities on another system. *See* pivoting.

lattice Levels, tiers, divisions, or segmentations of an environment typically based around security divisions, such as classifications.

lattice-based access control A variation of nondiscretionary access controls. Lattice-based access controls define upper and lower bounds of access for every relationship between a subject and an object. These boundaries can be arbitrary, but they usually follow the military or corporate security label levels.

layer 1 The Physical layer of the OSI model.

Layer 2 Forwarding (L2F) A protocol developed by Cisco as a mutual authentication tunneling mechanism. L2F does not offer encryption.

layer 2 The Data Link layer of the OSI model.

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). A point-to-point tunneling protocol developed by combining elements from PPTP and L2F. L2TP uses 802.1X for authentication. L2TP lacks a built-in encryption scheme but typically relies on IPsec's ESP as its encryption mechanism.

layer 3 The Network layer of the OSI model.

layer 4 The Transport layer of the OSI model.

layer 5 The Session layer of the OSI model.

layer 6 The Presentation layer of the OSI model.

layer 7 The Application layer of the OSI model.

layered security *See* defense in depth.

layering The use of multiple security controls in series to provide for maximum effectiveness of security deployment.

LDAP injection attack *See* Lightweight Directory Access Protocol (LDAP) injection attack.

LDAP *See* Lightweight Directory Access Protocol (LDAP).

LDAPS The TLS encrypted form of LDAP. *See* Simple Authentication and Security Layer (SASL).

leaf CA A certificate authority (CA) located at the bottom of a trust structure, which interfaces with customers, end users, and devices.

LEAP *See* Lightweight Extensible Authentication Protocol (LEAP).

learning rule *See* delta rule.

least privilege *See* principle of least privilege.

legacy platforms, legacy systems Operating systems, execution environments, or software in general that is no longer maintained or supported by the original vendor. *See* end-of-life (EoL) and end-of-support (EoS).

legal hold An early step in the evidence collection or e-discovery process. It is a legal notice to a data custodian that specific data or information must be preserved and that good faith efforts must be engaged to preserve the indicated evidence.

lessons learned The final step in incident response, which is used to evaluate the response plan and procedures and improve them as necessary. This review can also serve as a means to extract or clarify new information and concepts discovered during an incident response. Aka after-action report (AAR). *See also* postmortem review.

licensing A contract that states how a product is to be used.

lifecycle assurance An assessment of the trust or reliability of a product based on its concepts of design, architecture, creation, testing, and distribution. Ultimately, a judgment as to whether a product was designed with security as a central feature.

lifetime date The specific date when a certificate will expire. Aka expiration date. Sometimes this is stated as "lifetime dates," which includes the date of creation and the date of expiration, which can be labeled as "valid from" and "valid to." *See also* expiration.

LiFi (light fidelity) *See* light fidelity (LiFi).

light fidelity (LiFi) A technology for wireless communications using light. It is used to transmit both data and position information between devices. It uses visible light, infrared, and the ultraviolet light spectrums to support digital transmissions. It has a theoretical transmission rate of 100 Gbps. LiFi has the potential to be used in areas where interference to electromagnetic radiation would be a problem for radio wave–based solutions. Although direct line of sight between devices provides optimum throughput, signals can be transmitted off reflective surfaces in order to maintain at least some level of data transmission.

lighting One of the most commonly used forms of perimeter security control. The primary purpose of lighting is to discourage casual intruders, trespassers, prowlers, and would-be thieves who would rather perform their malicious activities in the dark.

lightweight cryptography The implementation of cryptography for systems and devices with minimal computational and memory resources, such as smartcards, IoT devices, ICS, point-of-sale (POS) systems, fitness trackers, smart watches, medical devices, etc.

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

Lightweight Directory Access Protocol (LDAP) injection attack A variation of a Structured Query Language (SQL) injection (SQLi) attack. However, the focus of the attack is on the back end of an LDAP directory service rather than a database server.

Lightweight Extensible Authentication Protocol (LEAP) A Cisco proprietary alternative to the Temporal Key Integrity Protocol (TKIP) for Wi-Fi Protected Access (WPA). This was developed to address deficiencies in TKIP before the 802.11i/WPA2 system was ratified as a standard. LEAP is now a legacy solution to be avoided.

likelihood The measurement of probability that a threat will become realized within a specific period of time.

liking *See* familiarity.

limit check A type of input validation, where the code checks to ensure that a number falls within an acceptable range.

Line Printer Daemon (LPD) This is a network service that is used to spool print jobs and send print jobs to printers.

Link The original name of the first layer of the TCP/IP model. This is sometimes replaced with network interface or network access.

link encryption An encryption technique that protects entire communications circuits by creating a secure tunnel between two points. This is done by using either a hardware or software solution that encrypts all traffic entering one end of the tunnel and decrypts all traffic exiting the other end of the tunnel.

link state A type of interior routing protocol that takes various characteristics into consideration when making route preference decisions, such as speed, latency, errors, and cost. *See* Open Shortest Path First (OSPF) and Intermediate System – Intermediate System (IS-IS).

link state routing protocol A routing protocol that maintains a topography map of all connected networks and uses this map to determine the shortest path to the destination.

live boot media A portable storage device that can be used to boot a computer. Live boot media contains a read-to-run or portable version of an operating system.

LM, LANMAN *See* LAN Manager (LM, LANMAN).

load balancer, load balancing A system used to spread or distribute network traffic load across several network links or network devices. The purpose of load balancing is to obtain more optimal infrastructure utilization, minimize response time, maximize throughput, reduce overloading, and eliminate bottlenecks.

local alarm systems Alarm systems that broadcast an audible signal that can be easily heard up to 400 feet away. Additionally, local alarm systems must be protected from tampering and disablement, usually by security guards. In order for a local alarm system to be effective, there must be a security team or guards positioned nearby who can respond when the alarm is triggered.

local area network (LAN) A network that is geographically limited, typically is restricted to a single building or even a single room. A LAN can have one or more servers. A network that functions across a group of buildings is known as a campus area network (CAN), across the city (same calling area) is known as a metropolitan area network (MAN), and across a globally connected network is known as a global area network (GAN).

local cache Anything that is temporarily stored on the client for future reuse. There are many local caches on a typical client, including ARP cache, DNS cache, and internet files cache.

local shared objects (LSOs) Small files or datasets that websites may store on a visitor's computer through the Adobe Flash Player. LSOs, aka Flash cookies, are generally used to store user preferences and settings, but they do have some risk. LSOs can be used to track a user's web activities and are not cleared or removed when a browser's HTML cookies are cleared.

location-based policies A means for controlling authorization grant or deny resource access based on where the subject is located, either logically or physically.

location services, location systems Any number of technologies that can provide geographic location data to mobile devices. Options include GPS, IPS/WIPS, cellular/mobile service tower triangulation, Bluetooth location services, and environmental sensors.

lock A security device used to keep a door, gate, or container closed and prevent unauthorized entry or access.

lock picking A means to attempt to bypass a key-based lock.

lockout, account lockout A security service that disables a device after a specified number of failed logon attempts.

log aggregation The collecting of logs pulled from a range of devices throughout the network into a centralized management server.

log analysis The art and science of reviewing audit trails, log files, or other forms of computer-generated records for evidence of policy violations, malicious events, downtimes, bottlenecks, or other issues of concern. The logged information is analyzed in detail to look for trends and patterns as well as abnormal, unauthorized, illegal, and suspicious activities and events.

log collectors Services that record logs, perform aggregation, or implement centralized logging, such as security information and event management (SIEM) and syslog.

log *See* audit trail.

`logger` A command used to add messages into the `/var/log/syslog` file. This command can be used from a command line or within a script. It can be used to inject a string of text, execute a command whose output is inserted into the syslog file, or insert content from a file into the log.

logging The activity of recording information about events or occurrences to a log file or database. *See* auditing.

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

logic bomb Any code hidden within an application or self-contained malicious code that causes something unexpected to happen based on some criteria being met. For example, a programmer could create a program that makes sure their name always appears on the payroll roster; if it doesn't, then key files begin to be erased. Logic bombs can use any number of conditional triggers, such as a countdown, a specific time, a specific date, opening of a certain file, opening an application, visiting a specific URL, or entering a certain keystroke.

logical isolation A form of segmentation that requires the use of classification labels on data and packets, which must be respected and enforced by network management, OSs, and applications.

logical security, logical controls IT security that protects against logical and/or technical attacks implemented by systems through hardware, software, and firmware. *See* technical security, technical controls.

logical topology The logical operation of a network. It defines the arrangement and organization of devices as well as the means used to communicate to and with each other. Aka signal topology.

logon credentials The identity and the authentication factors offered by a subject to establish access.

logon script A script that runs at the moment of user logon. A logon script is often used to map local drive letters to network shares, to launch programs, or to open links to often accessed systems.

loop A transmission pathway that repeats itself.

loop prevention, loop protection Any technique used to prevent or terminate looping. Examples include the Spanning Tree Protocol and the Internet Protocol (IP) header time-to-live (TTL) value.

loopback, loopback address A means to reference the local machine, often used in testing for network faults. Often the IPv4 address of 127.0.0.1 is used, but the entire Class A range of 127 was set aside to be used for this purpose. In IPv6, the loopback address is ::/128. The loopback address is used to create a software interface that connects to itself via TCP/IP. The loopback address is handled by software alone. It permits testing of the TCP/IP protocol stack even if network interfaces or their device drivers are missing or damaged.

loss potential *See* exposure factor (EF).

low Earth orbit (LEO) Satellites can be positioned in three primary orbits: low Earth orbit (LEO), 160–2,000 km, medium Earth orbit (MEO), 2,000–35,786 km, and geostationary orbit (GEO), 35,786 km. LEO satellites often have stronger signals than other orbits, but they do not remain in the same position over the earth, so multiple devices must be used to maintain coverage. Starlink (from SpaceX) is an example of a LEO satellite-based internet service. *See* medium Earth orbit (MEO) and geostationary orbit (GEO).

low latency systems Computing devices that provide real-time or near–real time response and communications for applications and services that demand high performance with low latency.

low-power devices, lower-powered devices Computing systems that may have limited CPU capabilities or memory capacities. These devices require cryptography functions that will not place an undue burden of computation on the device and will minimize latency and delay due to heavy computational loads.

Low Water-Mark Mandatory Access Control (LOMAC) A loadable kernel module for Linux designed to protect the integrity of processes and data. It is an OS security architecture extension or enhancement that provides flexible support for security policies.

M

M of N control A protection measure that requires that a minimum number of agents (*M*) out of the total number of agents (*N*) work together to perform high-security tasks. Typically associated with accessing certificates from an escrow store or keys from a key backup database.

MAC *See* mandatory access control (MAC), media access control (MAC), and message authentication code (MAC).

MAC address The unique media access control address that is assigned to a network interface card (NIC).

MAC filter, MAC filtering A list of authorized wireless client interface media access control (MAC) addresses that is used by a wireless access point (WAP) to block access to all nonauthorized devices. *See* MAC limiting.

MAC flooding A flooding attack used to compromise a switch by overloading its CAM table so that the switch gets stuck into retransmitting all network communications out all of its ports.

MAC limiting A switch feature that restricts the number of MAC addresses that will be accepted into the CAM table from each jack/port.

MAC spoofing A network impersonation attack used to mimic another system, often a valid or authorized network device, to bypass port security or MAC filtering limitations. Aka MAC cloning.

machine language A programming language that can be directly executed by a computer.

machine learning (ML) The real-world concept of programming a computer to solve problems or develop solutions from large and/or complex datasets. Often confused with the science fiction concept of AI.

machine certificate, computer certificate A type of certificate issued to verify the identity of a device rather than a service or a user.

macro virus Malicious code that lives within documents or emails and exploits the scripting capabilities of productivity documents and software.

macros A macro is a program or script written in a language that is embedded into specific files, such as Word documents, Excel spreadsheets, and Adobe PDFs. Macro-based attacks are often successful due to the victim operating old and unpatched versions of software. Many macros focus on Windows targets and thus are programmed in Visual Basic for Applications (VBA).

magnetic stripe card Machine-readable ID cards with a magnetic stripe. Like a credit card, debit card, or ATM card, magnetic stripe cards can retain a small amount of data but are unable to process data like a smartcard. Magnetic stripe cards often function as a type of two-factor control: the card is "something you have" and its PIN is "something you know." However, magnetic stripe cards are easy to copy or duplicate and are insufficient for authentication purposes in a secure environment.

mail-bombing An attack in which sufficient numbers of messages are directed to a single user's inbox or through a specific STMP server to cause a denial of service.

mail storm, email storm When someone responds with a Reply All to a message that has a significant number of other recipients in the To: and CC: lines. As others receive these replies, they in turn Reply All with their comments or demands to be removed from the conversation. This is further exacerbated if recipients have auto-responders set to Reply All for out-of-office notifications or other announcements.

main distribution frame (MDF) *See* wiring closet.

mainframe A high-end computer system used to perform highly complex calculations and provide bulk data processing.

maintenance hook A developer-installed access method that bypasses all security restrictions, often used for debugging or initial setup. Entry point into a system that only the developer of the system knows; aka backdoor.

maintenance The variety of tasks that are necessary to ensure continued operation in the face of changing operational, data processing, storage, and environmental requirements.

malicious code Any code that is meant to do harm. Code objects that include a broad range of programmed computer security threats that exploit various network, operating system, software, and physical security vulnerabilities to spread malicious payloads to computer systems. Aka malware.

malware inspection The use of a malware scanner (aka antivirus scanner or spyware scanner) to detect unwanted software content in network traffic.

malware Malicious software is any script or program that performs an unwanted, unauthorized, or unknown activity on a computer system. Any code that is meant to do harm. Aka malicious code.

managed detection and response (MDR) Many security vendors offer **endpoint detection and response** (EDR) capabilities as a managed service offering where they provide installation, configuration, and monitoring services to reduce the load on customer security teams.

managed power distribution units (PDUs) A means to remotely monitor and control the power consumption of the individual computing systems that are often rack-mounted.

managed service provider (MSP) Third-party (often cloud-based) services that provide remote oversight and management of on-premises IT or cloud IT. Aka managed security service provider (MSSP).

management controls The policies and procedures defined by an organization's security policy to implement and enforce overall access control.

managerial controls Security mechanisms that focus on the management of risk and thus the governance of organizational security.

Mandatory Access Control (MAC) An access control mechanism that uses classification-based security labels to regulate subject access to objects. Implementations include using a hierarchical MAC environment, a compartmentalized MAC environment, and a hybrid MAC environment.

mandatory vacations A security policy that requires all employees to take one to two weeks of vacation annually so their work tasks and privileges can be audited and verified. This often results in easy detection of abuse, fraud, oversight, incompetence, or negligence. A form of user peer auditing.

maneuver To consider the parameters of an attack, exploit, or intrusion and attempt to gain a better understanding by adjusting focus, sensor location, or analysis perspective.

man-in-the-browser (MitB, MiTB, MiB, MIB) This term is deprecated. A form of on-path/MitM attack in which the manipulating malware is operating on the victim's system, where it is able to intercept and manipulate communications immediately after they leave the browser and before they exit the network interface.

man-in-the-middle (MitM) attack This term is deprecated. *See* on-path attack.

mantrap This term is deprecated. *See* access control vestibule. Sometimes man-trap or man trap.

manual code review A form of static code analysis where someone looks over source code searching for flaws, bugs, typos, etc. This can be accomplished in peer review, shoulder review, and supervisory review. *See* static code analysis.

manual rollover *See* cold rollover.

masking The hiding of content when being displayed. The most common type is password masking, where asterisks or dots are displayed instead of the typed password characters. Masking can also be used to obfuscate sensitive data from being displayed by default on a screen or on a printout.

masquerading Using someone else's security ID to gain entry into a facility or system.

massively parallel processing (MPP), massive parallel processing (MPP) Technology used to create systems that house hundreds or even thousands of processors, each of which has its own operating system and memory/bus resources, which are linked together in order to work on a single primary task.

master A nickname for the owner or hacker controlling a botnet. Aka bot herder or handler.

master boot record (MBR) The portion of a hard drive or floppy disk that the computer uses to load the operating system during the boot process. *See* boot sector.

master boot record (MBR) virus A virus that attacks the MBR. When the system reads the infected MBR, the virus instructs it to read and execute the code stored in an alternate location, thereby loading the entire virus into memory and potentially triggering the delivery of the virus's payload.

master distribution frame (MDF) The primary wiring closet where interior cabling is connected to the telco link (i.e., demarcation point).

master image A crafted setup and configuration of a software product or an entire computer system. A master image is created just after the target system has been manually installed, patched, and configured. Aka gold image.

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

maximum tolerable downtime (MTD) The maximum length of time a business function can be inoperable without causing irreparable harm to the business.

maximum tolerable outage (MTO) *See* maximum tolerable downtime (MTD).

MBR (master boot record) *See also* boot sector.

MD2 (Message Digest 2) A hash algorithm developed by Ronald Rivest in 1989 to provide a secure hash function for 8-bit processors.

MD4 An enhanced version of the MD2 algorithm, released in 1990. MD4 pads the message to ensure that the message length is 64 bits smaller than a multiple of 512 bits.

MD5 *See* Message Digest 5 (MD5).

mean time between failures (MTBF) The measure of the anticipated incidence of failure of a system or component. *See also* mean time to failure (MTTF).

mean time to failure (MTTF) The measure of the anticipated initial incidence of failure of a system or component. If this measurement is the same as or similar to mean time between failures (MTBF), then MTBF is often presented/included without the MTTF; thus, the MTBF can represent the time frame to the first failure as well as the interval between subsequent failures. *See also* mean time between failures (MTBF).

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

measured boot A potential feature of Unified Extensible Firmware Interface (UEFI) that takes a hash calculation of every element involved in the booting process. *See* secure boot and boot security.

measurement systems analysis (MSA) A formal and thorough analysis of a measurement process or system.

media access control (MAC) A sublayer of the Data Link layer of the OSI model that controls the way multiple devices use the same media channel. It controls which devices can transmit and when they can transmit.

Media Access Control (MAC) address A 6-byte address written in hexadecimal. The first 3 bytes of the address indicate the vendor or manufacturer of the physical network interface. The last 3 bytes make up a unique number assigned to that interface by the manufacturer. No two devices on the same network can have the same MAC address. Aka hardware address, physical address, Ethernet address, NIC address, and network address.

media analysis A branch of computer forensic analysis involving the identification and extraction of information from storage media.

media gateway Any device or service that converts data from one communication format to another. A media gateway is often located at the intersection of two different types of networks.

media storage facilities A place designed to securely store blank media, reusable media, and installation media. Often a lockable cabinet or a safe.

media, medium Any storage technology, including hard disk drives (HDDs), solid-state drives (SSDs), flash memory, USB storage devices, optical discs (CD-ROM, DVD, Blu-ray), and tapes.

mediated-access model When a process that runs in a higher-numbered ring must ask a handler or a driver in a lower-numbered ring for services they need. Aka system call.

medium Earth orbit (MEO) Satellites can be positioned in three primary orbits: low Earth orbit (LEO), 160–2,000 km, medium Earth orbit (MEO), 2,000–35,786 km, and geostationary orbit (GEO), 35,786 km. MEO satellites are in the sky above a terrestrial location for longer than a LEO satellite. Individual MEO satellites also usually have a larger transmission footprint (area of the earth covered by its transmitter/receiver) than that of LEO satellites. However, due to the higher orbit, there is additional delay and a weaker signal from MEO satellites. *See* low Earth orbit (LEO) and geostationary orbit (GEO).

meet-in-the-middle attack An attack in which the attacker uses a known plaintext message. The plaintext is then encrypted using every possible key (k1), while the equivalent ciphertext is decrypted using all possible keys (k2). Aka meet in the middle attack.

`memdump` A utility that extracts memory/RAM contents into a standard output stream, which can be captured into a file (which can be local or off system, although this may require an additional tool such as `nc` or `openssl`).

memorandum of understanding (MOU) An expression of agreement or aligned intent, will, or purpose between two entities. An MOU isn't typically a legal agreement or commitment, but rather a more formal form of a reciprocal agreement or handshake (neither of which is typically written down). Aka letter of intent, memorandum of agreement (MOA).

memory The main memory resources directly available to a system's CPU. Primary memory normally consists of volatile random access memory (RAM) and is a high-performance storage resource available to a system.

memory addressing The means of referring to various locations in memory. *See* register addressing, immediate addressing, direct addressing, indirect addressing, and base+offset addressing.

memory card (1) A device that can store data but cannot process it; often built around some form of flash memory. (2) A machine-readable ID card with a magnetic stripe. Like a credit card, a debit card, or an ATM card, a memory card can retain a small amount of data but is unable to process data like a smartcard.

memory dump A file that contains the contents of memory. A memory dump may be triggered by a system error or by a forensics tool for investigative purposes.

memory leak What occurs when a program fails to release memory or continues to consume more memory. It's called a leak because the overall computer system ends up with less available free memory when an application is causing a memory leak.

memory-mapped I/O A technique used to manage input/output between system components and the CPU.

memory page A single chunk of memory that can be moved to and from RAM and the paging file on a hard drive as part of a virtual memory system.

memory pointer A commonly used concept in application development. Memory pointers are simply an area of memory that stores an address of another location in memory. *See* pointer.

memory protection A core security component that must be designed and implemented into an operating system that is used to prevent an active process from interacting with an area of memory that was not specifically assigned or allocated to it.

mesh topology A network structure that connects systems to other systems using numerous paths or links. A full-mesh topology connects each system to all other systems on the network. A partial-mesh topology connects many systems to many other systems. Mesh topologies provide redundant connections to systems, allowing multiple segment failures without seriously affecting connectivity.

mesh trust A form of trust requiring that each member trust each other member directly; thus, this technique is difficult to scale, since the trust relationships increase exponentially as the number of trusted elements increases.

message The communications to or input for an object (in the context of object-oriented programming terminology and concepts).

message authentication code (MAC) A common method of verifying integrity. The MAC is derived from the message and a key.

message digest (MD) A summary of a message's content (not unlike a file checksum) produced by a hashing algorithm.

Message Digest 5 (MD5) A hashing algorithm that produces a 128-bit hash. The version of the MD algorithm released in 1991. MD5 processes 512-bit blocks of the message, using four distinct rounds of computation to produce a digest of the same length as the MD2 and MD4 algorithms (128 bits). Generally has been replaced by SHA-1 or other, more modern hashing algorithms.

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.

metacharacters Characters that have been assigned special programmatic meaning. Thus, they have special functions that standard, normal characters do not have. There are many common metacharacters, but typical examples include single and double quotation marks; the open/close square brackets; the backslash; the semicolon; the ampersand; the caret; the dollar sign; the period, or dot; the vertical bar, or pipe symbol; the question mark; the asterisk; the plus sign; open/close curly braces; and open/close parentheses: ' " [] \; & ^ $. | ? * + {} ().

metadata 1) Data about data or information about data. 2) The information about the context surrounding an item of interest, or it can focus on the content of the item. The results of a data mining operation on a data warehouse.

metamodel A model of models. Because the spiral model encapsulates a number of iterations of another model (the waterfall model), it is known as a metamodel.

Metasploit A vulnerability scanning and penetration testing tool used to exploit flaws in applications, computers, and networking systems.

methods The actions or functions performed on input (messages) to produce output (behaviors) by objects in an object-oriented programming environment.

Metropolitan Area Network (MAN) A network within a town or city.

MFA *See* multifactor authentication (MFA).

microcode A term used to describe software that is stored in a ROM chip. Aka firmware.

microcontroller A small computer consisting of a CPU (with one or more cores), memory, various input/output capabilities, RAM, and often nonvolatile storage in the form of flash or ROM/PROM/EEPROM. Examples include Raspberry Pi, Arduino, and a field-programmable gate array (FPGA). A microcontroller is similar to, but less complex than, a system on a chip (SoC). A microcontroller may be a component of an SoC.

microprocessor *See* processor (1).

MicroSD HSM, MicroSD hardware security module A small form-factor hardware encryption and security module that can be added to any mobile device with a MicroSD card slot.

microsegmentation Dividing up an internal network into numerous subzones. Each zone is separated from the others by internal segmentation firewalls (ISFWs), subnets, or VLANs. Zones could be as small as a single device, such as a high-value server or even a client or endpoint device. Any and all communications between zones are filtered, may be required to authenticate, often require session encryption, and may be subjected to allow list and block list control.

micro-services, micro-API, microservices An emerging feature of web-based solutions that derives from service-oriented architecture (SOA). A micro-service is simply one element, feature, capability, business logic, or function of a web application that can be called upon or used by other web applications.

middle management *See* security professional.

military and intelligence attacks Attacks that are launched primarily to obtain secret and restricted information from law enforcement or military and technological research sources.

MIME header *See* Multipurpose Internet Mail Extensions (MIME) header.

MIME Object Security Services (MOSS) An early communications standard that provides authenticity, confidentiality, integrity, and nonrepudiation for email messages. Has been abandoned in favor of other solutions, the most popular of which is PGP.

Mimikatz A hacker tool used to dump passwords, grab hashes, and retrieve Kerberos tickets from Windows system memory. This data grab can then be used to escalate privileges, perform pass-the-hash, and even perform golden ticket attacks against Kerberos.

mission-essential functions, mission-critical functions Any core business tasks that are central to the operation of the organization. These are the functions, processes, or tasks that if stopped, interrupted, or terminated may cause the overall failure of the entire organization.

misuse case testing A process used by software testers to evaluate the vulnerability of their software to known risks. Testers first enumerate the known misuse cases and then attempt to exploit those use cases with manual and/or automated attack techniques. It is testing that attempts to model the activity of an attacker. Aka abuse case testing.

mitigate risk *See* reducing risk.

mitigated The process by which a risk is reduced or removed.

mitigation In risk management, the elimination or reduction of risk. *See* other related terms: acceptance, risk tolerance, assignment, transfer/transference (as related to risk), avoidance, reducing risk, rejecting risk, and ignoring risk.

MitM attack *See* man-in-the-middle (MitM) attack.

MITRE ATT&CK® "A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community." —From `attack.mitre.org`.

mobile application management (MAM) A software product similar to a mobile device management (MDM) product, but it focuses on app management rather than the entire mobile device.

mobile content management (MCM) A content management system for mobile devices. It is used to control company resources and the means by which they are accessed or used on mobile devices. An MCM can take into account a device's capabilities, storage availability, screen size, bandwidth limitations, memory (RAM), and processor capabilities when rendering or sending data to mobile devices.

mobile device Any relatively small, handheld, or portable device with a battery or other form of power supply that does not use a cable and is thus mobile. Aka portable device, mobile device, personal mobile device (PMD), personal electronic device or portable electronic device (PED), and personally owned device (POD).

mobile device deployment policy A security plan for allowing and/or providing mobile devices for employees to use while at work and to perform work tasks when away from the office. *See* bring your own device (BYOD), corporate-owned, personally enabled (COPE), choose your own device (CYOD), and corporate-owned mobile strategy (COMS). Also VDI and VMI solutions could be considered.

mobile device management (MDM) A software solution to the challenging task of managing the myriad mobile devices that employees use to access company resources. The goals of MDM are to improve security, provide monitoring, enable remote management, and support troubleshooting. *See* unified endpoint management (UEM).

mobile OS A mobile operating system (OS) is designed to operate on a portable device. Although a portable device can be defined as any device with a battery, a mobile OS is designed for portable devices for which traditional network operating systems are too large or too resource-demanding.

mobile sites Nonmainstream alternatives to traditional recovery sites that typically consist of self-contained trailers or other easily relocated units.

model verification A part of software development processes that is often used to ensure that the crafted code remains in compliance with a development process, architectural model, or design limitations.

modem (1) A traditional landline modem (modulator-demodulator) is a communications device that covers or modulates between an analog carrier signal and digital information in order to support computer communications of PSTN (public switched telephone network) lines. (2) With the advancement of digital broadband communication technologies, the term *modem* is now often used to refer to the intermediary device between business or personal equipment and the broadband network (typically internet) carrier or service (such as DSL, cable, cellular/wireless/mobile, Wi-Fi, ISDN, etc.), even when modulation and demodulation are not actually taking place.

modes of operation In cryptography, the various methods by which the plaintext blocks are encrypted into ciphertext blocks. There are several modes of operation, including Electronic Code Book (ECB), Cipher Block Chaining (CBC), Counter Mode (CTR), and Galois Counter Mode (GCM).

modification attack An attack in which captured packets are altered and then played against a system. Modified packets are designed to bypass the restrictions of improved authentication mechanisms and session sequencing.

module testing Each independent or self-contained segment of code for which there exists a distinct and separate specification is tested independently of all other modules. Aka component testing, this can be seen as a parent or superclass of unit testing.

modulo The remainder value left over after a division operation is performed. Often written as *mod*. Commonly used as a one-way function in various cryptosystems.

MONDEX A type of electronic payment system and protocol designed to manage cash on smartcards.

monitoring The activity of manually or programmatically reviewing logged information looking for specific information. *See* auditing.

monitoring services Third-party options that will perform auditing and monitoring of on-premises equipment or cloud assets. The monitoring entity may itself be considered security as a service (SECaas) or monitoring as a server (MaaS).

motion detector, motion sensor A physical security device that senses movement or sound in a specific area.

motion sensor *See* motion detector.

MSCHAP (Microsoft CHAP) Microsoft's customized or proprietary version of Challenge-Handshake Authentication Protocol (CHAP). MSCHAPv2 adds data encryption capabilities.

MTBF *See* mean time between failures (MTBF).

MTD *See* maximum tolerable downtime (MTD).

MTTF *See* mean time between failures (MTBF).

MTTR *See* mean time to repair/restore (MTTR).

multicast A communications transmission to multiple identified recipients. Aka multicasting.

multicore A CPU chip containing two, four, eight, dozens, or more independent execution cores that can operate simultaneously and/or independently. There are even some specialty chips with over 10,000 cores.

multifactor authentication (MFA), multi-factor authentication Authentication that uses two or more factors of authentication. Multifactor authentication requires different factors (something you know, something you have, and something you are), not just multiple authentication methods in a single factor such as a password and a PIN, both in the something-you-know factor.

multifunction devices (MFDs) Devices that are combinations of several products into one, such as a combined printer, scanner, and fax machine. Aka all-in-one device. *See* multifunction printers (MFPs).

multifunction printer (MFP) A device that is primarily a printer but that also includes other functions, such as fax, scanning, and copying. *See* multifunction devices (MFDs).

multihomed host, multihomed firewalls A system that has more than one network interface, with each interface on a different subnet or network.

multilayer protocols A protocol suite or collection that operates across multiple layers of the OSI model, typically using encapsulation. A common example is TCP/IP.

multilayer switch A switch that can operate at layers above layer 2. A layer 3 switch that can perform routing for a virtual LAN (VLAN) is an example of a multilayer switch. Aka L3 switch.

multilayered defense *See* defense in depth.

multilayered security *See* defense in depth.

multilevel mode *See* multilevel security mode.

multilevel nesting data structure, cross-referencing data structure A data storage system in which a data object can have multiple data-parent and data-child links and may even have links across multiple levels or among "peer" data items. Aka distributed database model.

multilevel security mode A system that is authorized to process information at more than one level of security even when all system users do not have appropriate clearances or a need to know for all information processed by the system.

multimedia collaboration The use of various multimedia-supporting communication solutions to enhance distance collaboration. Collaboration occurs when people can work on a project together. Often, collaboration allows workers to work simultaneously as well as across different time frames. Collaboration can also be used for tracking changes and including multimedia functions. Collaboration can incorporate email, chat, VoIP, videoconferencing, use of a drawing board, online document editing, real-time file exchange, versioning control, and other tools.

Multimedia Messaging Service (MMS) The telco service supporting texting with media, such as pictures, audio, and video.

multipart virus, multipartite virus Malware that performs multiple tasks and may infect a system in numerous ways.

multipartite virus A virus that uses more than one propagation technique in an attempt to penetrate systems that defend against only one method or the other.

multiparty risk The risk that exists when several entities or organizations are involved in a project.

multipath A disk or storage implementation where multiple pathways are provided between the CPU/RAM and the storage devices.

multiprocessing A technology that makes it possible for a computing system to harness the power of more than one processor to complete the execution of a single application.

multiprogramming The pseudo-simultaneous execution of two tasks on a single processor coordinated by the operating system for the purpose of increasing operational efficiency. Multiprogramming is considered a relatively obsolete technology and is rarely found in use today except in legacy systems.

multiprotocol label switching (MPLS) A high-throughput, high-performance network technology that directs data across a network based on short path labels rather than longer network addresses.

Multipurpose Internet Mail Extensions (MIME) header A header that defines any elements in an email message that are MIME-compliant. MIME is the standard for modern email.

multistate Term used to describe a system that is certified to handle multiple security levels simultaneously by using specialized security mechanisms that are designed to prevent information from crossing between security levels.

multitasking A system handling two or more tasks simultaneously.

multithreading A process that allows multiple users to use the same process without interfering with each other.

mutation fuzzing A form of fuzzing that modifies known inputs to generate synthetic inputs that may trigger unexpected behavior. Aka dumb fuzzing.

mutual assistance agreement (MAA) An agreement in which two organizations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources. Aka reciprocal agreement.

mutual authentication A method of authentication in which each entity proves itself to the other.

N

NAC *See* network access control (NAC).

narrow-band, narrow-band wireless A type of radio wave communication that is widely used by SCADA systems to communicate over a distance or geographic space where cables or traditional wireless are ineffective or inappropriate.

NAT *See* network address translation (NAT).

NAT gateway A network segment edge device, such as a proxy or firewall, that performs network address translation (NAT) operations.

NAT traversal (NAT-T) NAT-T was designed specifically to support IPsec and other tunneling virtual private network (VPN) protocols, such as Layer 2 Tunneling Protocol (L2TP), so that organizations can benefit from both NAT and VPNs across the same border device/interface. Defined in RFC 3947.

natural access control A crime prevention through environmental design (CPTED) concept of the subtle guidance of those entering and leaving a building through placement of entranceways, use of fences and bollards, and placement of lights.

natural disaster A disaster that is not caused by humans, such as earthquakes, mudslides, sinkholes, fires, floods, hurricanes, tornadoes, falling rocks, snow, rainfall, ice, humidity, heat, extreme cold, and so on.

natural surveillance The crime prevention through environmental design (CPTED) concept that involves any means to make criminals feel uneasy through the increase of

opportunities for them to be observed. This can be accomplished by an open and obstacle-free outside area, especially around entrances, with clear lines of sight.

natural territorial reinforcement The crime prevention through environmental design (CPTED) concept where there is an attempt to make the area feel like an inclusive, caring community. The area should be designed so that it looks cared for and respected and that it is actively being defended.

`nbtstat` A tool used to view and purge the NetBIOS over TCP/IP statistics on Windows systems.

near-field communication (NFC) A standard that establishes radio communications between devices in close proximity. It lets you perform a type of automatic synchronization and association between devices by touching them together or bringing them within inches of each other. NFC is a derivative technology from RFID and is itself a form of field-powered or field-triggered device.

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

negligence Failure to exercise the degree of care considered reasonable under the circumstances, resulting in an unintended injury to another party.

Nessus A GUI vulnerability scanner and assessment tool from the company Tenable. It is available as either a free tool or a commercial subscription service.

NetBEUI *See* NetBIOS Extended User Interface (NetBEUI).

NetBIOS Extended User Interface (NetBEUI) A non-routable protocol used to transport Network Basic Input/Output System (NetBIOS) traffic in a local area network (LAN). A Microsoft protocol developed in 1985 to support file and printer sharing. Microsoft has enabled support of NetBEUI on modern networks by devising NBT (NetBIOS over TCP/IP). This in turn supports the Windows sharing protocol of SMB (Server Message Block), which is aka CIFS (Common Internet File System). NetBEUI is no longer supported as a lower-layer protocol; only its SMB and CIFS variants are still in use. Aka NetBIOS Frame (NBF) protocol.

NetBIOS *See* Network Basic Input/Output System (NetBIOS).

`netcat` A flexible network utility used to write to or read from Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) network connections.

NetFlow A traffic monitoring feature on Cisco routers and switches. NetFlow tracks the IP addresses of packets as well as service class (i.e., priority level 0–7), payload protocol, ports, ICMP type and code, miscellaneous protocol header information, and potential causes of network congestion. *See* sFlow.

`netstat` A Windows command that displays information about Transmission Control Protocol (TCP) sessions of a system. The output options include displaying the source and destination IP address and port number of active connections, listing the program associated with a connection, showing traffic bytes, displaying Ethernet statistics, showing the fully qualified domain name (FQDN) for external addresses, and displaying the routing table.

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

network access control (NAC) A concept of controlling access to an environment through strict adherence to and implementation of security policy. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

network address allocation The process of assigning IP addresses to various network segments.

network address translation (NAT) A service that hides the identity of internal clients by translating their source address into a public Internet Protocol (IP) address owned by the NATing device. NAT also allows RFC 1918 private IP addresses to be used in a private network so that an organization isn't required to use a public IP address for every host in that organization, thus conserving IPv4 addresses. Aka Source Network Address Translation (SNAT). *See* port address translation (PAT).

network analysis, network forensic analysis A means of collecting and correlating information from disparate networked sources and producing as comprehensive a picture of network activity as possible.

network appliance A device that has been designed and preconfigured to perform a specific function or operation on a network. Most network appliances offer security features, such as filtering, access control lists (ACLs), IDS, and malware scanning.

network-attached printer A printer directly connected to the network that is also able to operate as its own print server. Commonly a multifunction printer (MFP) or multifunction device (MFD).

network-attached storage (NAS) A network device dedicated as a file server that is used by other systems across the network to store files. A NAS is used as an alternative to local storage.

network-based IDS (NIDS), network-based IPS (NIPS) An intrusion detection system (IDS) or intrusion prevention system (IPS) approach that attaches the system to a point in the network where it can monitor and report on all network traffic.

Network Basic Input/Output System (NetBIOS) The native protocol of Windows PCs. It provides a 15-character naming convention for resources on the network. NetBIOS is a broadcast-oriented network protocol in that all traffic is available to all devices in a

local area network (LAN). The protocol can be transported over IP networks as NetBIOS Extended User Interface (NetBEUI).

network discovery scanning A variety of techniques used to scan a range of IP addresses, searching for systems with open network ports. Network discovery scanners do not actually probe systems for vulnerabilities, but they provide a report showing the systems detected on a network and the list of ports that are exposed through the network and server firewalls that lie on the network path between the scanner and the scanned system.

network-enabled devices Any type of device (whether mobile or stationary) that has native network capabilities. This generally assumes the network in question is a wireless type of network, primarily that provided by a mobile telecommunications company. However, it can also refer to devices that connect to Wi-Fi (especially when they can connect automatically), devices that share data connectivity from a wireless telco service (such as a mobile hot spot), and devices with RJ-45 jacks to receive a standard Ethernet cable for a wired connection.

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

network firewall A hardware security device, typically called an appliance, designed for general network filtering.

Network Functions Virtualization (NFV) The combination of hardware and software networking components into a single integrated entity. Aka virtualized networking. *See* software-defined networking (SDN).

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 Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite, which is responsible for placing and removing packets on the physical network.

Network layer (layer 3 of the OSI) The third layer of the Open Systems Interconnection (OSI) model, which 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. *See also* Open Systems Interconnection (OSI).

network monitoring The act of monitoring traffic patterns to obtain information about a network.

Network News Transfer Protocol (NNTP) An application protocol supporting the posting and retrieval of Usenet news articles.

network operating system (NOS) Any operating system that has native networking capabilities and was designed with networking as a means of communication and data transfer.

network scanner *See* port scanner.

network segmentation A subdivision of a network to control traffic. Transactions can only occur between devices within the same segmented network. Network segmentation can be accomplished using logical or physical means. *See* segmentation.

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

network sniffing *See* sniffing.

network topology The physical layout and organization of computers and networking devices. Aka physical topology.

network vulnerability scanning *See* vulnerability scan.

network zone An area of a network designed for a specific purpose, such as internal use or external use.

neural network A system in which a long chain of computational decisions that feed into each other and eventually add up to produce the desired output is set up. Aka deep learning or cognitive systems.

New Technology LAN Manager (NTLM) A password hash storage system used on Microsoft Windows.

next-generation firewall (NGFW) A unified threat management (UTM) device that is based on a traditional firewall with numerous other integrated network and security services, such as application filtering, deep packet inspection, intrusion prevention, TSL offloading and/or inspection, domain name and website filtering, QoS, bandwidth management, anti-malware, authentication services, and identity management. *See* unified threat management (UTM) and multifunction device (MFD).

next-generation secure web gateway (SWG, NGSWG) A variation of and combination of the ideas of a next-generation firewall and a WAF. An SWG is a cloud-based web gateway solution that is often tied to a subscription service that provides ongoing updates to filters and detection databases.

NFC *See* near-field communication (NFC).

NFS *See* Network File System (NFS).

NIC *See* network interface card (NIC).

NIC teaming The bonding, binding, or grouping of two or more NICs together to act as a single connection to the network. This can be done to increase the usable network capacity or as a form of redundancy.

NIDS *See* network-based IDS (NIDS), network-based IPS (NIPS).

NIPS *See* network-based IDS (NIDS), network-based IPS (NIPS).

nmap A command-line network mapper and port scanner. The nmap tool can be used to perform a wide range of network discovery and enumeration functions, including ping sweeping, port scanning, application identification/banner grabbing, operating system identification, firewall and IDS evasion, and a plethora of script functions to discover details about target applications and OSs. Zenmap is a GUI interface to nmap.

NNTP *See* Network News Transfer Protocol (NNTP).

noise A steady interfering disturbance.

noise detection A security device that is focused on detecting a specific noise, such as the breaking of glass, or of an abnormal noise, such as a door opening at 3 a.m. when no one should be present.

nonce A number used once. Used as a formula reference to a randomization string or function call. A random number generator variable used in cryptography software; creates a new and unique value every time it is used, often based on a timestamped seed value. *See* initialization vector (IV).

noncompete agreement (NCA) A document that attempts to prevent an employee with special knowledge of secrets from one organization from working in a competing organization in order to prevent that second organization from benefiting from the worker's special knowledge of secrets.

noncredentialed scan A type of security scan in which no user accounts are provided to the scanning tool, so only those vulnerabilities that don't require credentials are discovered.

nondedicated line A communications link that requires a connection to be established before data transmission can occur. A nondedicated line can be used to connect with any remote system that uses the same type of nondedicated line.

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

nondiscretionary access control An access control mechanism that regulates subject access to objects by using roles or tasks.

noninterference model A model loosely based on the information flow model. The noninterference model is concerned with the actions of one subject affecting the system state or actions of another subject.

nonintrusive scan A form of vulnerability scan (aka passive evaluation) that only discovers the symptoms of flaws and vulnerabilities and doesn't attempt to exploit them.

non-IP protocols Non-IP protocols are protocols that serve as an alternative to IP at the OSI Network layer (3). In the past, non-IP protocols were widely used. However, with the

dominance and success of TCP/IP, non-IP protocols have become the purview of special-purpose networks. The three most recognized non-IP protocols are IPX, AppleTalk, and NetBEUI. Aka legacy protocols.

nonpersistent system A computer system that does not allow, support, or retain changes. Thus, between uses and/or reboots, the operating environment and installed software are exactly the same. Changes may be blocked or simply discarded after each system use. Changes may be performed by authorized users, administrators, automated processes, or malware. Aka nonpersistence and static system. *See* persistent system.

Nonrepudiation, non-repudiation A feature of a security control or an application that prevents the sender of a message or the subject of an activity or event from denying that the event occurred. A common example is a digital signature.

nontransparent proxy A proxy that manages client traffic because the client is specifically configured to send communications to the proxy.

nonvolatile *See* nonvolatile storage.

nonvolatile storage A storage system that does not depend on the presence of power to maintain its contents, such as magnetic/optical media and nonvolatile RAM (NVRAM).

normal forms Various levels of database organization designed to improve efficiency.

normalization The database process that removes redundant data and ensures that all attributes are dependent on the primary key.

north-south traffic A term that refers to the traffic flow that occurs inbound or outbound between internal systems and external systems. *See* east-west traffic.

NoSQL A database approach that employs nonrelational data structures, such as hierarchies or multilevel nesting/referencing. Some NoSQL database management systems (DBMSs) support SQL expressions.

NOT An operation (represented by the ~, ¬, or ! symbol) that reverses the value of an input variable. This function operates on only one variable at a time.

notification alarms Alarms that trigger notification are often silent from the intruder/attacker perspective but record data about the incident and notify administrators, security guards, and law enforcement. A recording of an incident can take the form of log files and/or security camera recordings. The purpose of a silent alarm is to bring authorized security personnel to the location of the intrusion or attack in hopes of catching the person(s) committing the unwanted or unauthorized acts.

`nslookup` A Windows command used to perform manual DNS queries. Similar to `dig`.

NTLM *See also* New Technology LAN Manager (NTLM).

nuisance alarm rate (NAR) False positives from animals or foliage on Area Perimeter Intrusion Detection Assessment System (PIDAS) fences.

null scan A type of port scan that does not have any Transmission Control Protocol (TCP) header flags enabled.

nxlog A log management tool available on most OSs that can function similarly to syslog but is not limited to syslog file formats. nxlog can handle logs in nearly any format and perform rewrite, correlation, alerting, and pattern matching.

O

OAuth An open standard for authentication and access delegation (federation). OAuth is widely used by websites, web services, and mobile device applications.

obfuscation The practice of crafting code specifically to be difficult to decipher by other programmers. The intentional hiding or masking of a communication or its meaning. Aka camouflage.

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

object identifier (OID) The formal method used to name or reference most object types in an X.509 certificate, such as Distinguished Names and Certificate Practices Statements. The OID is a standardized identifier mechanism defined by the International Telecommunications Union (ITU) and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), which is used to name any object, concept, or thing with an unambiguous persistent name that is unique globally.

object linking and embedding (OLE) A Microsoft technology used to link data objects into or from multiple files or sources on a computer.

object-oriented programming (OOP) A method of programming that uses encapsulated code sets called objects. OOP is best suited for eliminating error propagation and mimicking or modeling the real world.

object-relational database A relational database combined with an object-oriented programming environment.

Oblivious DoH (ODoH) A late 2020 enhancement to DoH that adds a DNS proxy between the client and the DNS resolver so that the identity of the requesting client is isolated from the DNS resolver. Thus, ODoH provides anonymity and privacy to DNS queries.

observable An identified fact of occurrence, such as the presence of a malicious file, usually accompanied by a hash.

occupant emergency plans (OEP) A guide that assists with sustaining personnel safety in the wake of a disaster. The OEP provides guidance on how to minimize threats to life, prevent injury, manage duress, handle travel, provide for safety monitoring, and protect property from damage due to a destructive physical event.

OCSP *See* Online Certificate Status Protocol (OCSP).

OCSP stapling A means for checking the revocation status of X.509 digital certificates. It is a mechanism that enables the presenter of a certificate to append or staple a timestamped OCSP response signed by the issuing certificate authority (CA). Aka stapling, certificate stapling, or previously Transport Layer Security (TLS) Certificate Status Request.

OFDM *See* orthogonal frequency-division multiplexing (OFDM).

offboarding The removal of an employee's identity from the identity and access management (IAM) system once they have left an organization. Can also be used in any context when removing something from being in compliance with a security or configuration policy.

off-by-one problem A potential problem with HMAC-based one-time passwords (HOTPs) that occurs when the non–time-based seed or key synchronization is desynchronized, as the client may be calculating a value that the server has already discarded or has not yet generated. This requires the device to be resynced with the authentication server.

offline attack An attack in which attackers are not working against a live target system but instead are working on their own independent computers.

offline CA A root certificate authority (CA) of a hierarchy that is disconnected from the network and often powered off to be stored in a powered-off state in a physically secure container (such as a vault). The offline CA must be brought back online to re-sign or re-issue certificates to intermediary, subordinate, or even leaf CAs when their respective certificates are about to expire or have expired.

off-premise(s) IT operated by a third party, typically in the cloud. *See* on-premise(s).

off-the-shelf solution A product that already exists that is selected to be deployed by an organization. This is a strategy of security management that is distinct from creating or crafting custom proprietary solutions.

omnidirectional antenna A standard straight or pole antenna, which can send and receive signals in all directions perpendicular to the line of the antenna itself.

onboarding The process of adding new employees to an organization's identity and access management (IAM) system. The onboarding process is also used when the role or position of an employee changes or when they're awarded additional levels of privilege or access. Can also be used in any context when bringing something into compliance with a security or configuration policy.

one-time pad A form of encryption in which the key is a random number that is used only once and then discarded. Each communication partner has a pad or list of the random keys to perform the encryption and/or decryption functions.

one-time password (OTP), onetime password A dynamic password that can be used for only one attempted logon and then becomes invalid. One-time passwords can be implemented via software solutions or hardware tokens.

one-upped constructed password A password with a single-character difference from its present form in a dictionary list.

one-way encryption A mathematical function performed on passwords, messages, cyclic redundancy checks (CRCs), and so on, that creates a cryptographic code that cannot be reversed.

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

online attack An attack in which the attacker is working against a live target system.

online CA A certificate authority (CA) that is kept online and network-connected at all times.

Online Certificate Status Protocol (OCSP) A real-time query-based system for verifying the validity of a digital certificate and confirming that it has not been revoked by the issuing certificate authority.

on-path attack An attack in which the hacker takes a position between a client and a server (or other entities) and then tricks the client into establishing a link with the hacker's computer rather than the intended server. The attacker in turn establishes a link with the server using the client's stolen credentials. Once established, the attacker can view all traffic between client and server as well as change the content. Previously known as man-in-the-middle (MitM).

on-premise(s) The traditional deployment concept in which an organization owns the hardware, licenses the software, and operates and maintains the systems on its own, usually within its own building. *See* off-premise(s).

on-premises federated identity management system A single sign-on solution hosted fully on site.

Opal A SED standard defined by the Trusted Computing Group. Opal is based on the use of 128- or 256-bit AES and pre-decryption authentication.

open relay An SMTP server that is configured to accept email messages from any source and will forward them on to their destination. Open relays are commonly hijacked by spammers and thus are mostly replaced with closed (i.e., internal use only) or authenticated (i.e., authenticate before use) relays. See closed relay and authenticated relay.

Open Shortest Path First (OSPF) An example of a link state routing protocol.

open source intelligence (OSINT) The gathering of information from any publicly available resource. This includes websites, social networks, discussion forums, file services, public databases, and other online sources. It also includes non-internet sources, such as libraries and periodicals.

open source software (OSS) Software that is created and maintained by community-based development projects. These open source projects are freely available for anyone to download and use, either directly or as a component of a larger system. In fact, many commercial off-the-shelf (COTS) software packages incorporate open source code. Most organizations use a combination of commercial and open source depending on business needs and software availability.

open source A solution where the source code, and other internal logic, is exposed to the public. *See* closed source.

open system A system designed using agreed-upon industry standards. Open systems are much easier to integrate with systems from different manufacturers that support the same standards or that use compatible application programming interfaces (APIs). *See* closed system.

open system authentication (OSA) A connection scheme for wireless networks where no real authentication is required; as long as a radio signal can be transmitted between the client and WAP, communications are allowed. An open Wi-Fi network with no authentication and no encryption.

Open Systems Interconnection (OSI) model A standardized reference model defined by ISO to categorize the process of communication between computers in terms of seven layers. The seven layers are Application, Presentation, Session, Transport, Network, Data Link, and Physical. *See also* International Organization for Standardization (ISO) and Presentation layer. Aka OSI Reference Model.

Open Vulnerability and Assessment Language (OVAL) Security Content Automation Protocol (SCAP) component that provides a language for describing security testing procedures.

Open Web Application Security Project (OWASP) A nonprofit security project focusing on improving security for online or web-based applications, mobile device applications, and IoT equipment. OWASP is not just an organization—it is also a large community (`www.owasp.org`) that works together to freely share information, methodology, tools, and techniques related to better coding practices and more secure deployment architectures.

open wireless network A wireless network with no authentication and thus usually no encryption.

OpenID An open SSO standard maintained by the OpenID Foundation that can be used in conjunction with OAuth or on its own. An open source authentication technology developed from OAuth.

OpenID Connect An internet-based single sign-on solution. It operates over the OAuth protocol and can be used in relation to web services as well as smart device apps.

OpenSSL An open source cryptography software library for the implementation of TLS and SSL encrypted connections.

OpenVPN A virtual private network (VPN) solution based on Transport Layer Security (TLS) (formerly Secure Sockets Layer [SSL]) that provides an easy-to-configure but robustly secured VPN option. OpenVPN is an open source implementation that can use either pre-shared secrets (such as passwords) or certificates for authentication.

operational controls The mechanisms and procedures used to ensure or maintain security on a day-to-day basis.

operational plans Short-term and highly detailed plans based on the strategic and tactical plans. Operational plans are valid or useful only for a short time. They must be updated often (such as monthly or quarterly) to retain compliance with tactical plans. Operational plans are detailed plans on how to accomplish the various goals of the organization.

operational technology (OT) The collection of computer systems designed to monitor and manipulate the physical world, such as ICS and SCADA. Aka cyber-physical systems.

operations security triple The relationship between asset, vulnerability, and threat.

operator *See* user.

opportunistic TLS for SMTP This mechanism will attempt to set up an encrypted connection with every other email server in the event that it is supported; otherwise, it will downgrade to plaintext. Using opportunistic TLS for SMTP gateways reduces the opportunities for casual sniffing of email.

Optical Carrier (OC) *See* Synchronous Transport Signals (STS).

OR An operation (represented by the ∨, +, or || symbol) that checks to see whether at least one of the input values is true.

order of restoration The order in which the steps of a recovery effort should proceed.

order of volatility The prioritized order of forensic evidence collection based on the speed or likelihood that digital evidence will be damaged based on time or normal operations of the system.

organizational owner *See* senior management/senior manager.

organizational security policy A security policy that focuses on issues relevant to every aspect of an organization (or the whole of the organization).

organizationally unique identifier (OUI) The first 3 bytes (24 bits) of the MAC address, which denotes the vendor or manufacturer of the physical network interface. OUIs are registered with the Institute of Electrical and Electronics Engineers (IEEE), which controls their issuance.

Orthogonal Frequency-Division Multiplexing (OFDM) A wireless technology that employs a digital multicarrier modulation scheme that allows for a more tightly compacted transmission. It is a variation on frequency multiplexing that employs a digital multicarrier modulation scheme that allows for a more tightly compacted transmission.

OS hardening The process of reducing vulnerabilities, managing risk, and improving the security provided by or for an operating system. Aka system hardening.

OSI, OSI model *See* Open Systems Interconnection (OSI) model.

out-of-band (OOB) management Performing management tasks without using the primary production network. This can be accomplished using a secondary management network, which requires each host to have a second NIC. Other OOB options include using a serial cable connection (such as to the CON [console] port of routers or switches) or direct operation at the local keyboard.

out-of-band IDS An intrusion detection system (IDS) configured to perform pre-connect activity monitoring, but then not be involved with any post-connect activity monitoring.

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

out-of-band pathways An often-overlooked network segmentation concept used to create a separate and distinct network structure for traffic that would otherwise interfere with the production network or that may itself be put at risk if placed on the production network. Secondary (or additional) network paths or segments may be created to support data storage traffic (such as with SANs), VoIP, backup data, patch distribution, and management operations.

output feedback (OFB) An encryption mode in which the algorithm XORs plaintext with a seed value. For the first encrypted block, an initialization vector is used to create the seed value. Future seed values are derived by running the algorithm on the preceding seed value. The major advantage of OFB mode is that transmission errors do not propagate to affect the decryption of future blocks.

OVAL *See* Open Vulnerability and Assessment Language (OVAL).

overt channel An obvious, visible, detectable, known method of communicating that is addressed by a security policy and subsequently controlled by logical or technical access controls.

overwriting *See* clearing.

OWASP *See* Open Web Application Security Project (OWASP).

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

ownership The formal assignment of responsibility (i.e., making someone an owner) to an individual or group.

P

P12 A file format option for PFX-formatted certificates which uses the .p12 file extension. *See also* PKCS#12 (Public Key Cryptography Standards).

P2P *See* peer-to-peer (P2P).

P7B A certificate format that stores certificate data in Base64-encoded ASCII files. P7B-formatted data can be stored in a file with a `.p7b` or `.p7c` extension. P7B certificate files include `-----BEGIN PKCS7-----` and `-----END PKCS7-----` statements. P7B can be used to store only certificates and chain certificates, not private keys. Aka Cryptographic Message Syntax Standard. *See also* PKCS#7 (Public Key Cryptography Standards).

PaaS *See* platform as a service (PaaS).

package In the context of the Common Criteria for information technology security evaluation, a package is a set of security features that can be added to or removed from a target system.

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

packet filtering A firewall technology that accepts or rejects packets based on header contents, such as IP address, port number, or protocol type.

packet sniffing The act of capturing packets from the network in hopes of extracting useful information from the packet header and/or contents.

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

padded cell Similar to a honeypot. When an intruder is detected by an intrusion detection system (IDS), the intruder is transferred to a padded cell. The padded cell has the look and layout of the actual network, but within the padded cell the intruder can neither perform malicious activities nor access any confidential data. A padded cell is a simulated environment that may offer fake data to retain an intruder's interest.

Padding Oracle On Downgraded Legacy Encryption (POODLE) An SSL/TLS downgrade attack that causes the client to fall back to using SSL 3.0, which has less robust encryption cipher suite options than TLS. Aka SSL stripping. *See* downgrade attack.

pairing The connecting or linking of two devices over Bluetooth.

pagefile, page file A specially formatted file that contains data previously stored in real memory but not recently used. Used with virtual memory. Aka swap file or swapfile.

paging When an OS is using virtual memory and needs to access addresses stored in the pagefile, it checks to see whether the page is memory-resident (in which case it can access it immediately) or whether it has been swapped to disk, in which case it reads the data from disk back into real memory.

palm geography An example of a biometric factor, which is a behavioral or physiological characteristic unique to a subject. The shape of a person's hand is used to establish identity or provide authentication.

palm scan An example of a physiological biometric factor, which is unique to a subject. It uses near-infrared light to measure vein patterns in the palm, which are as unique as fingerprints. Some palm scans identify the layout of ridges, creases, and grooves on a person's palm to establish identity or provide authentication. *See* palm topography.

palm topography An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The layout of ridges, creases, and grooves on a person's palm is used to establish identity or provide authentication. This is the same as a palm scan and similar to a fingerprint.

pan, tilt, zoom (PTZ) Common remote control features of security/IP cameras.

panel antenna, flat panel antenna A type of unidirectional wireless antenna that uses a flat transmission surface.

PAP *See* Password Authentication Protocol (PAP).

parabolic antenna A type of unidirectional wireless antenna that uses a parabolic bowl shape to focus signals from very long distances or weak sources.

parallel data systems, parallel computing A computation system designed to perform numerous calculations simultaneously. Parallel data systems often go far beyond basic multiprocessing capabilities. They often include the concept of dividing up a large task into smaller elements and then distributing each subelement to a different processing subsystem for parallel computation. This implementation is based on the idea that some problems can be solved efficiently if they are broken into smaller tasks that can be worked on concurrently. Aka large-scale parallel data systems.

parallel run A type of new system deployment testing in which the new system and the old system are run in parallel. Each major or significant user process is performed on each system simultaneously to ensure that the new system supports all required business functionality that the old system supported or provided.

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

parameter pollution A technique that attackers use to defeat input validation controls. Parameter pollution works by sending a web application more than one value for the same input variable.

parol evidence rule A rule stating that when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements may modify the written agreement.

partial-knowledge teams Teams that possess an incomplete account of organizational assets, including hardware and software inventory, prior to a penetration test. Thus, time must be spent in obtaining additional knowledge about the organization before test attacks can begin.

partially known environment A form of penetration testing that combines the black-box/unknown environment and white-box/known environment techniques and is a popular approach to software validation. Testers approach the software from a user perspective, analyzing inputs and outputs. Previously known as gray box.

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

pass the hash An authentication attack that potentially can be used to gain access as an authorized user without actually knowing or possessing the plaintext of the victim's credentials. This attack is mostly aimed at Windows systems, which maintain a set of cached credentials. Aka the authentication token (the "hash" in the attack name) and pass the key.

passive audio motion detector A device that listens for abnormal sounds in the monitored area.

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

passive IDS, passive IPS A type of intrusion detection system (IDS)/intrusion prevention system (IPS) that uses a promiscuous-mode network interface card (NIC) to eavesdrop on network communication. This type of monitoring allows only for reactive responses to discovered problems, rather than proactive responses.

passive monitoring Website monitoring technique that analyzes actual network traffic sent to a website by capturing it as it travels over the network or reaches the server. *See* real user monitoring (RUM).

passive proximity device A mechanism that has no active electronics; it is just a small magnet with specific properties (like antitheft devices commonly found in or on retail product packaging). A passive device reflects or otherwise alters the electromagnetic (EM) field generated by the reader device. This alteration is detected by the reader device, which triggers the alarm, records a log event, or sends a notification.

passive reconnaissance The activity of gathering information about a target without interacting with the target. Instead, information is collected from sources not owned and controlled by the target (other websites and services) as well as by eavesdropping on communications from the target. *See* active reconnaissance.

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

passphrase A string of characters usually much longer than a password. Once the passphrase is entered, the system converts it into a virtual password for use by the authentication process. Passphrases are often natural-language sentences to allow for simplified memorization.

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

Password Authentication Protocol (PAP) An insecure plaintext password-logon mechanism. A standardized authentication protocol for PPP. PAP transmits usernames and passwords in the clear.

password complexity A security setting that enforces a minimum of three out of four standard character types (uppercase and lowercase letters, numbers, and symbols) to be represented in the password and disallows the username, real name, and email address from appearing in the password.

password cracking The use of methods of reverse-engineering or guessing securely stored passwords. Types include dictionary, brute force, hybrid, and precomputed hash.

password guessing The process of attempting to enter a password by guessing its value.

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

password key A device, often USB but can also be something that connects over Bluetooth like a watch or ring, which can serve as an additional authentication factor just by being present at the time of authentication.

password length An important factor in determining a password's strength. Generally, longer passwords are better.

password management The collection of policies and procedures used to improve and control the use of passwords within an organization. Password management includes complexity requirements, minimum lengths, password age restrictions, history retention, and account lockout.

password policy (1) A set of rules written out as part of the organizational security policy that dictates the requirements of user and device passwords, such as length, complexity, and age; (2) a technical enforcement tool (typically a native part of an operating system) that enforces the password rules.

password recovery The ability to recover and/or reveal a password, which requires that the password storage mechanism be reversible or that passwords be stored in multiple ways. *See also* password replacement.

password replacement A more secure option than password recovery is to require passwords to be changed rather than recovered.

password restrictions The rules that define the minimal requirements of passwords, such as length, character composition, and age.

password reuse When a user attempts to use a password she had used previously on the same system. The management of password history prevents password reuse.

password vault Often software solutions, sometimes hardware based, sometimes local only, sometimes using cloud storage, that are used to generate and store credentials for sites, services, devices, and whatever other secrets you want to keep private. The vault itself is encrypted and must be unlocked to regain access to the stored items. Aka credential manager.

Password-Based Key Derivation Function 2 (PBKDF2) An example of a key stretching technology. PBKDF2 uses a hashing operation, an encryption cipher function, or an HMAC operation (i.e., a symmetric key is used in the hashing process) on the input password, which is combined with a salt. This process is then repeated thousands of times.

PASTA (Process for Attack Simulation and Threat Analysis) A seven-step threat modeling methodology.

PAT *See* port address translation (PAT).

patch management Program that ensures that relevant patches are applied to systems. Ideally, patches are evaluated, tested, and deployed, and systems are audited to verify that the patches are applied and not removed.

patch *See* hotfix, update.

patent A governmental grant that bestows on an invention's creator the sole right to make, use, and sell that invention for a set period of time. Aka utility patent.

`pathping` A CLI on Windows that combines ping and tracert functionality.

path vector, path vector routing protocol An exterior routing protocol which takes the entire pathway into consideration when making a routing decision. *See* Border Gateway Protocol (BGP).

pattern-matching detection *See* knowledge-based detection and signature-based detection.

Payment Card Industry Data Security Standard (PCI DSS) A collection of requirements for improving the security of electronic payment transactions. These standards were defined by the PCI Security Standards Council members, who are primarily credit card banks and financial institutions.

PBKDF2 (Password-Based Key Derivation Function 2) An example of a key-stretching technology. PBKDF2 uses a hashing operation, an encryption cipher function, or a Hashed Message Authentication Code (HMAC) operation (which uses a symmetric key in the hashing process) on the input password, which is combined with a salt. This process is then repeated thousands of times. *See* key stretching.

PBX *See* private branch exchange (PBX).

PDU (protocol data unit) *See* protocol data unit (PDU).

PEAP *See* Protected Extensible Authentication Protocol (PEAP).

peer layer communication Within the OSI model, the information removed by each layer contains instructions, checksums, and so on that can be understood only by the peer layer that originally added or created the information.

peer trust This is similar to mesh trust, but the main difference is that a peer trust does not involve hierarchies or third-party trust structures. Peer trust links are between individual entities without a third party. Aka web of trust.

peer-to-peer (P2P) A form of communication or data-transfer system that makes connections between hosts/peers rather than through a central controlling server or service. Also, a networking and distributed application solution that shares tasks and workloads among peers.

peer-to-peer mode *See* ad hoc mode.

peer-to-peer network A network structure between individual devices without the need or use of a primary controlling entity or device.

PEM (Privacy-enhanced Electronic Mail) A certificate format that uses Base64 (ASCII) to encode the certificate details into a file with a `.pem`, `.crt`, `.cer`, or `.key` extension. PEM certificate files include `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` statements. PEM can be used to store server certificates, intermediate certificates, and private keys.

penetration A breach of an environment's perimeter by an intruder when an attack is successful. Aka owned or pwnd (hacker leet-speak for having taken control of a system through an attack). *See* intrusion.

penetration test, penetration testing A form of customized vulnerability scan that is performed by a special team of trained authorized entity security specialists rather than by an internal security administrator using an automated tool. Penetration tests can take many forms, including hacking in from the outside, simulating a disgruntled employee, social-engineering attacks, physical attacks, and remote connectivity and virtual private network (VPN) attacks. Aka ethical hacking and pentest. Penetration testing should be performed only with the consent and knowledge of the management staff.

pepper A number used to increase the security of passwords that is combined with the password characters just before hashing, similar to the salting process. The salt is stored in the same database as the salted password, but the pepper is stored somewhere else, such as within the application code or as a server configuration value.

perfect forward secrecy A means of ensuring that the compromise of an entity's digital certificates or public/private key pairs doesn't compromise the security of any session keys. Perfect forward secrecy is implemented by using ephemeral keys for each and every session; the keys are generated at the time of need and used only for a specific period of time or volume of data transfer before being discarded and replaced.

perimeter intrusion detection and assessment system (PIDAS) A fence system that has two or three fences used in concert to optimize security. PIDAS fencing is often present around military locations and prisons. Typically, a PIDAS fence has one tall main fence, which may be 8 to 20 feet tall. The main fence may be electrified, may have barbed wire/razor wire elements, and/or can include touch detection technologies. This main fence is then surrounded by an outside fence, which may only be 4 to 6 feet tall. The purpose of this outer fence is to keep animals and casual trespassers from accessing the main fence.

period analysis A second-order form of frequency analysis that is an examination of frequency based on the repeated use of the key or secret that reveals a pattern of encryption. The key length is the period of the repetition. This is often a flaw or vulnerability of polyalphabetic substitution ciphers, which leads to a process of frequency analysis.

permanent virtual circuit (PVC) A predefined virtual circuit that is always available for a Frame Relay customer.

permission An ability or activity that a user account is granted permission to perform. Aka capability. *See also* privilege.

permission auditing A comparative assessment of assigned resource privileges. Aka permission review, privilege review, user access audit, and user right audit.

persistence (1) The characteristic of an attack that maintains remote access to and control over a compromised target. (2) When a session between a client and member of a load-balanced cluster is established, subsequent communications from the same client will be sent to the same server, thus supporting persistence or consistency of communications. Aka affinity.

persistent system A computer system where changes are possible and are saved/retained/committed/made permanent. Thus, changes persist across uses. *See* nonpersistent system.

personal (PER) The Wi-Fi authentication option that uses the concept of a preshared static key or code. Aka PSK (preshared key). *See* preshared key (PSK).

personal identification number (PIN) A number or code assigned to a person to be used as an identification factor. PINs should be kept secret.

personal identification verification (PIV) card Any ID card, such as a badge, an identification card, or a security ID, that is used as a form of physical identification and/or electronic access control device (i.e., a smartcard).

Personal Information Protection and Electronic Documents Act (PIPEDA) A Canadian law that affects the processing of personal information related to Canadian residents by restricting how commercial businesses may collect, use, and disclose personal information.

personal software firewall *See* host-based firewall.

personally identifiable information (PII) Any data item that can be easily and/or obviously traced back to the person of origin or concern.

personnel management An important factor in maintaining operations security. Personnel management is a form of administrative control or administrative management.

PFX (personal information exchange) A certificate format that stores certificate data in binary. PFX files have extensions of `.pfx` or `.p12`. PFX is most commonly used on Windows systems to import and export certificates and private keys. PFX can be used to store server certificates, intermediate certificates, and private keys. *See also* PKCS#12 (Public Key Cryptography Standards).

PGP *See* Pretty Good Privacy (PGP).

phage virus Malware that modifies or infects many aspects of a system so it can regenerate itself from any remaining parts.

pharming, DNS pharming The malicious redirection of a valid website's URL or IP address to a fake website that hosts a false version of the original valid site.

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

phishing campaigns Planned phishing attacks against a target.

phishing simulation A tool used by penetration testers to evaluate the ability of employees to resist or fall for a phishing campaign.

phlashing A malicious variation of flashing or updating official basic input/output system (BIOS) or firmware that, once installed, introduces remote control or other malicious features into a device.

phone phreaking, phreaking The process of breaking into telephone company computers to place free calls.

photoelectric motion detector A device that senses changes in visible light levels for the monitored area. Photoelectric motion detectors are usually deployed in internal rooms that have no windows and that are kept dark.

phreaker A hacker of telephone systems.

physical access controls Control access measures used to restrict physical access and prevent direct contact with systems or areas in a facility to protect assets and resources. Aka physical controls or physical security.

physical controls for physical security *See* physical access control.

physical isolation A type of segmentation that requires implementing network segmentation or air gaps between networks of different security levels.

Physical layer Layer 1 of the OSI model.

physical topology *See* network topology (aka physical topology).

piggybacking The act of convincing someone to allow an unauthorized entity through a secured gate or doorway without being identified, or authorizing them directly. *See also* tailgating.

PII *See* personally identifiable information (PII).

ping A Transmission Control Protocol/Internet Protocol (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 flood attack An attack that repeatedly sends ping/ICMP requests to a system. It can come from a single system as a DoS attack but is more often launched against a target by multiple systems in a DDoS attack.

ping-of-death attack A type of DoS. A ping-of-death attack employs an oversized ping/ICMP packet. Using special tools and IPv4 fragmentation, an attacker can send numerous oversized ping packets to a victim. In many cases, when the victimized system attempts to process the packets, an error occurs, causing the system to freeze, crash, or reboot.

pinning A deprecated security mechanism that is no longer supported by modern browsers. A security mechanism operating over HTTP that enables an HTTPS (Transport Layer Security [TLS] secured web service) system to prevent impersonation by attackers through the use of fraudulently issued digital certificates. Pinning operates by providing the visitor with an HTTP response header field value, named Public-Key-Pins, which includes the hashes of the certificates used by the server along with a timestamp defining how long to keep these certificates pinned. Aka HTTP Public Key Pinning (HPKP). Aka certificate pinning.

pivoting, pivot In penetration testing (or hacking in general), using the privileges or access gained through an initial intrusion to focus attention on another target that may not have been visible or exploitable initially.

PKCS#12 (Public Key Cryptography Standards) A cryptography file storage and archiving standard that allows for several cryptography objects to be saved in a single file container. Aka Personal Information Exchange Syntax Standard. *See also* P12 and PFX (personal information exchange).

PKCS#7 (Public Key Cryptography Standards) A cryptography file storage and archiving standard created for use with S/MIME, but now implemented in numerous contexts, often related to single sign-on. *See also* P7B.

PKI *See* Public Key Infrastructure (PKI).

plain old telephone service (POTS) Standard telephone service, as opposed to other connection technologies like DSL.

plain view doctrine A law enforcement officer performing a legally permissible duty may seize evidence that is visible to the officer in plain view if the officer has probable cause to believe that the evidence is associated with criminal activity.

plaintext, plain text A message that has not been encrypted. Nonencrypted data.

platform as a service (PaaS) The cloud computing concept of providing a computing platform and software solution stack as a virtual or cloud-based service. Essentially, it is the concept of paying for a service that provides all the aspects of a platform (i.e., operating system and complete solution package). PaaS allows the customer to run their own custom code, services, and applications.

playback attack *See* replay attack.

playbook A checklist of IR steps to be performed by the members of the IRT. A playbook often includes multiple different scenario/situation-specific checklists that can be used based on the specific asset(s) and threat(s) involved in an incident.

plenum The boxes and tubes that distribute conditioned air throughout a building. Plenum spaces are the areas of a building designed to contain the HVAC plenum components. Plenum spaces are typically distinct and separate from human inhabitable spaces within a building. Due to building codes in most countries, anything that is placed into the plenum space must be plenum rated. This is a type of fire rating requiring that those products produce minimal levels of smoke and/or toxic gases, especially if the building has enclosed spaces that could trap gases. Electrical cables and networking cables are common plenum-rated products.

pointer A designated memory location used to store the memory address used in direct, indirect, or base addressing. *See* memory pointer.

pointer dereference The programmatic activity of retrieving the value stored in a memory location by triggering the pulling of the memory based on its address or location as stored in a pointer (a type of variable that holds an address—that is, a memory space location). Aka object dereference.

point-to-multipoint (P2MP, PTMP, PMP) A type of network communication that is a one-to-many link.

point-to-point (P2P, PTP) 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), which was used over various non-LAN connections, such as modem dial-up links.

Point-to-Point Tunneling Protocol (PPTP) An enhancement of PPP that creates encrypted tunnels between communication endpoints (i.e., virtual private networks [VPNs]). PPTP is often replaced by L2TP.

policy *See* security policy.

polling A LAN media access technology that performs communications using a primary-secondary configuration. One system is labeled as the primary system. All other systems are labeled as secondary. The primary system polls or inquires of each secondary system in turn whether they have a need to transmit data. If a secondary system indicates a need, it is granted permission to transmit. Once its transmission is complete, the primary system moves on to poll the next secondary system. Mainframes often supported polling.

polyalphabetic substitution cipher A form of substitution cipher that uses multiple alphabets in the same message to hinder decryption efforts. An example is the Vigenère cipher.

polyinstantiation The event that occurs when two or more rows in the same table appear to have identical primary key elements but contain different data for use at differing classification levels. Polyinstantiation is often used as a defense against some types of inference attacks.

polymorphic An attribute of some malware that allows the malware to mutate and appear differently each time it crops up. It is malware that modifies its own code as it travels from system to system. The mutations make it harder for malware scanners to detect (and react to) the unwanted code, since the signature of the malware is somewhat different each time it infects a new system. Aka polymorphic virus or polymorphic malware.

polymorphism In the context of object-oriented programming terminology and concepts, the characteristic of an object to provide different behaviors based on the same message and methods owing to variances in external conditions.

POP *See* Post Office Protocol (POP).

pop-up blocker A tool used to prevent websites from opening additional web browser windows without your consent.

port A connection address within a protocol.

port address translation (PAT) A means of translating between IP addresses and ports between public and private networks. PAT supports many-to-one mappings of internal to external IP addresses by using ports. Similar to network address translation (NAT), which translates addresses between public and private IP addresses only. However, the term PAT is rarely used; instead, the term NAT is often used to mean PAT. Aka overloaded NAT, network and port address translation (NPAT), and network address and port translation (NAPT).

port An opening that allows network data to pass through.

port blocking A service provided by a software or hardware firewall that blocks or drops packets directed toward disallowed ports.

port disabling, interface disabling A physical option that renders a connection port on a device electrically useless.

port isolation, private ports Private VLANs that are configured to use a dedicated or reserved uplink port. The members of a private VLAN or a port-isolated VLAN can interact only with each other and over the predetermined exit port or uplink port. A common implementation of port isolation occurs in hotels.

port knocking A process used on a security system where all ports appear closed. If the client sends packets to a specific set of ports in a certain order, a bit like a secret knock, then the desired service port opens and allows the client software to connect to the service.

port mirror A common feature found on managed switches that duplicates traffic from one or more other ports out a specific port.

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

port scanner An 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.

port scanning The act of using a port scanner to detect the state of ports on a system (i.e., open, closed, or filtered).

port security (1) The physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized user or devices can attempt to connect into an open port. (2) The management of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports through the use of firewall, intrusion detection system (IDS), and intrusion prevention system (IPS) tools. (3) The need to authenticate to a port before being allowed to communicate through or across the port. This may be implemented on a switch, router, smart patch panel, or even a wireless network. This concept is often referred to as IEEE 802.1X, which is titled Port-Based Network Access Control. (4) Port knocking.

port spanning, port mirroring A common feature found on managed switches; it will duplicate traffic from one or more other ports out a specific port. A switch may have a hardwired Switched Port Analyzer (SPAN) port, which duplicates the traffic for all other ports, or any port can be set as the mirror, audit, IDS, or monitoring port for one or more other ports. Port mirroring or port spanning takes place on the switch itself.

port tap A means to eavesdrop on network communications. Modern inline taps have mostly replaced vampire taps. A port tap may need to be used when port spanning or port mirroring is not supported by a switch. Aka network tap or tap.

positive air pressure The maintaining of a slight overpressure in a datacenter, which reduces the infiltration of dust, debris, microfine particulate matter, and other contaminants (such as cleaning chemicals or vehicle exhaust). Without such efforts, these unwanted particles can build up over time; dust bunnies can attach to surfaces due to static charges or may cause corrosion.

position description *See* job description.

Post Office Protocol (POP) An email access program that can be used to retrieve email from an email server. POP results in archiving messages only on the client; they are fully removed from the server. *See* Internet Message Access Protocol (IMAP).

postmortem review An evaluation of an incident response soon after a resolved incident to ensure that key players in the incident share their knowledge and develop best practices to assist in future incident-response efforts.

post-quantum The study and creation of cryptographic algorithms to defend against quantum supremacy in the area of encryption. Post-quantum encryption is an attempt to create algorithms that are based on hard mathematical problems that even quantum computers cannot solve.

postwhitening A special feature found in the Twofish algorithm which uses a similar operation to prewhitening after the 16th round of encryption. *See* prewhitening.

potentially unwanted programs (PUPs) Any type of questionable software that is not necessarily and obviously malicious code, such as sniffers, password crackers, network mappers, port scanners, and vulnerability scanners. Aka potentially unwanted applications (PUAs) and potentially unwanted software (PUSs).

POTS *See* plain old telephone service (POTS).

power conditioner, power-line conditioner A form of advanced surge protector that is also able to remove or filter line noise.

PowerShell A scripting language as well as a command-line shell for Microsoft Windows. PowerShell is built on top of the .NET Framework and is intended as a tool for administrators to manage not just Windows systems, but Linux and macOS as well. PowerShell scripts use the `.ps1` extension.

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

PPTP *See* Point-to-Point Tunneling Protocol (PPTP).

preaction system A combination dry pipe/wet pipe system. The system exists as a dry pipe until the initial stages of a fire (smoke, heat, and so on) are detected, and then the pipes are filled with water. The water is released only after the sprinkler head activation triggers are melted by sufficient heat. If the fire is quenched before the sprinklers are triggered, the pipes can be manually emptied and reset. This also allows for manual intervention to stop the release of water before sprinkler triggering occurs. Preaction systems are the most appropriate water-based system for environments that include both computers and humans in the same locations.

predictive analysis A threat evaluation technique that aims to employ indicators of compromise (IOCs), observables, and other cyberthreat intelligence to determine when at attack is imminent. The earlier in the cyber kill chain that we can detect an attack, exploit, breach, or intrusion event, the more likely the malicious event will be deflected and stopped.

premises wire distribution room *See* wiring closet.

prepending The adding of a term, expression, or phrase to the beginning or header of a communication. Often prepending is used to further refine or to establish the pretext of a social engineering attack.

preponderance of the evidence The standard of evidence in a civil court case.

Presentation layer (layer 6 of the OSI) The sixth layer of the OSI model, which is 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. *See also* Open Systems Interconnection (OSI).

preservation In relation to forensics, the preventing of any change from occurring as related to collected evidence.

preset lock A common key-based lock found on many facility doors. Aka deadbolt locks and conventional locks.

preshared key (PSK) (1) Cryptographic method in which two separate parties share a key via an out-of-band communication method prior to communication. (2) An encryption key or authentication code that is distributed before clients need it to avoid on-demand key exchange procedures. (3) The authentication method used in WPA and WPA2 where a static password is used. Aka personal (PER).

pretexting A form of social engineering in which the attacker claims to be someone else to convince the victim to give up sensitive or personal information. It is the establishment of a false initial context designed to fool the victim.

Pretty Good Privacy (PGP) An example of a proprietary, open source email security solution that supports digital signatures and message encryption using a proprietary certificate.

preventive, preventative, preventive control, preventive access control Describes a type of access control that is deployed to thwart or stop unwanted or unauthorized activity from occurring.

prewhitening A special feature found in the Twofish algorithm that involves XORing the plaintext with a separate subkey before the first round of encryption. *See* postwhitening.

primary authoritative name server The DNS server that hosts the original zone file for the domain. This is the only DNS server where the zone file can be edited.

primary key A specific key from the set of candidate keys that is used as the main differentiator between records. Every record must have a unique value in its primary key field.

primary memory Storage that normally consists of volatile random access memory (RAM) and is a high-performance storage resource available to a system.

Primary Rate Interface (PRI) An ISDN service type that provides up to 23 B channels and one D channel. Thus, a full PRI ISDN connection offers 1.544 Mbps throughput, the same as a T1 line.

primary storage The RAM that a computer uses to keep necessary information readily available.

principle An authenticated user or subject, often used in relation to Kerberos or Security Assertion Markup Language (SAML) and federation.

principle of least privilege An access control philosophy that states that subjects are granted the minimal access necessary for the completion of their work tasks.

Printer Command Language (PCL) A legacy insecure printer communication and control protocol.

Privacy Act of 1974 A law that mandates that government agencies maintain only records that are necessary to conduct their business and destroy those records when they are no longer needed for a legitimate function of government. It provides a formal procedure for individuals to gain access to records the government maintains about them and to request that incorrect records be amended. The Privacy Act also restricts the way the federal government can deal with private information about individual citizens.

privacy An element of confidentiality aimed at preventing personal or sensitive information about an individual or organization from being disclosed. Also refers to keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace to someone if revealed.

Privacy by Design (PbD) A guideline to integrate privacy protections into products during the early design phase rather than attempting to tack it on at the end of development. It is effectively the same overall concept as "security by design" or "integrated security," where security is to be an element of the design and architecture of a product, starting at initiation and being maintained throughout the software development lifecycle (SDLC).

Privacy Enhanced Mail (PEM) An email encryption mechanism that provides authentication, integrity, confidentiality, and nonrepudiation. PEM is a layer 7 protocol. PEM uses RSA, DES, and X.509.

privacy impact assessment (PIA) A tool used to determine privacy risks, how to mitigate those risks, and whether to notify the affected parties as related to a new or future project or endeavor.

privacy notice Typically an externally facing document informing customers, users, or stakeholders what the organization does with personally identifiable information (PII). Aka a privacy statement.

privacy policy An internally facing document informing employees about what the organization does with the employee's personally identifiable information (PII) and the PII of external entities.

privacy threshold assessment (PTA) A tool used to evaluate the data that an organization has already collected to determine whether such data is PII, business confidential, or nonsensitive data.

private A commercial business/private sector classification used for data of a private or personal nature that is intended for internal use only. A significant negative impact could occur for the company or individuals if private data is disclosed.

private branch exchange (PBX) A computer- or network-controlled telephone system. PBXs are deployed in large organizations; they offer a wide range of telephone services, features, and capabilities, including conference calls, call forwarding, paging, call logging, voicemail, call routing, and remote calling. It is a system that may allow users to connect voice, data, pagers, networks, and almost any other application into a single telecommunications system.

private cloud A cloud service within a corporate network and isolated from the internet. A private cloud is for internal use only; it can be housed within a corporate network and isolated from the internet by a firewall, or it can be hosted by a third party over the internet. A private cloud is deployed as a single tenant configuration. *See* public cloud and hybrid cloud.

private IP addresses, private IPv4 addresses The range of Internet Protocol (IP) addresses from RFC 1918, which are as follows: 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255. These private IP addresses aren't usable (i.e., are not routable) on/over the public internet.

private key The secret key of an asymmetric cryptography solution that must be kept secure. It's one of the keys in the public key/private key pair.

privilege An aspect of authorization, often related to the ability to create, change, or delete objects.

privilege abuse *See also* privilege escalation.

privilege creep The undesired addition of user privileges as a user gains more privileges when changing jobs, but unneeded privileges are not renewed. It violates the principle of user privilege. *See also* creeping privilege(s).

privilege escalation The result when a user obtains access to a resource they wouldn't normally be able to access. This 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). Aka escalation of privilege or elevation of privilege.

privileged access management The control over issuing higher-than-normal user privileges to specific subjects.

privileged account A user account with administrative permissions, privileges, and capabilities.

privileged account management (PAM) Identity and access management (IAM) solutions that restrict access to privileged accounts or that detect when accounts use any elevated privileges. In this context, privileged accounts are administrator accounts or any accounts that have specific elevated privileges.

privileged entity controls *See* privileged operations functions.

privileged mode The mode designed to give the operating system access to the full range of instructions supported by the CPU. Aka kernel mode. *See also* protected mode.

privileged operations functions Activities that require special access or privilege to perform within a secured IT environment. In most cases, these functions are restricted to administrators and system operators.

privileged user Someone granted additional capabilities, permissions, privileges, and user rights above those of a typical standard user.

privileges A combination of rights and permissions. Rights refer to actions a user can perform on a system, such as changing the system time. Permissions refer to the level of access a user is granted to data such as read, write, modify, and delete.

proactive approach, defensive approach A means of threat modeling that takes place during early stages of systems development, specifically during initial design and specifications establishment. This method is based on predicting threats and designing in specific defenses during the coding and crafting process, rather than relying on postdeployment updates and patches.

probability determination *See* annualized rate of occurrence (ARO).

Probability × Damage Potential *See* risk matrix.

problem state The state in which a process is actively executing. *See* running state.

procedure An element of a security policy that prescribes steps to take to perform work tasks and security activities. A detailed step-by-step, how-to document describing the actions necessary to implement a specific security mechanism, control, or solution. *See also* standard operating procedure (SOP).

Process The original name of the fourth layer of the TCP/IP model, which is often replaced by the name Application.

Process for Attack Simulation and Threat Analysis (PASTA) A seven-step threat modeling methodology.

process isolation One of the fundamental security procedures put into place during system design. Basically, using process isolation mechanisms (whether part of the operating system or part of the hardware itself) ensures that each process has its own isolated memory space for storage of data and the actual executing application code itself.

process state The various forms of execution in which a process may run. Aka operating mode. *See* ready state, running state, waiting state, supervisor state, and stopped state.

processor (1) The central processing unit in a PC; it handles all functions on the system. Aka microprocessor. (2) In the context of the General Data Protection Regulation (GDPR), the entity that manipulates data on behalf of a data collector or data holder.

production, production network A network segment where the everyday business tasks and work processes are accomplished. It should only be operating on equipment and systems that have been properly staged and tested.

Program Evaluation Review Technique (PERT) A project-scheduling tool. It is a method used to judge the size of a software product in development and calculate the standard deviation (SD) for risk assessment. PERT relates the estimated lowest possible size, the most likely size, and the highest possible size of each component. PERT is used to direct improvements to project management and software coding in order to produce more efficient software. As the capabilities of programming and management improve, the actual produced size of software should be smaller.

programmable logic controllers (PLC) Industrial control system (ICS) units that are effectively single-purpose or focused-purpose digital computers. They are typically deployed for the management and automation of various industrial electromechanical operations, such as controlling systems on an assembly line or a large-scale digital light display.

programmable read-only memory (PROM) A PROM chip that does not have its contents "burned in" at the factory as is done with standard ROM chips. Instead, special functionality is installed that allows the end user to burn in the contents of the chip.

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

proprietary A form of commercial business/private sector confidential information owned exclusively by the organization. If proprietary data is disclosed, it can have drastic effects on the competitive edge of an organization.

proprietary system (alarm) An alarm system that is similar to a central station system, but the host organization has its own on-site security staff waiting to respond to security breaches. *See* central station system.

protected distribution, protected cable distribution, protective distribution system (PDS) The means by which cables are protected from unauthorized access or harm. Aka protected cabling system. The goals of a PDS are to deter violations, detect access attempts, and otherwise prevent compromise of cables. Elements of PDS implementation can include protective conduits, sealed connections, and regular human inspections.

Protected Extensible Authentication Protocol (PEAP) A protocol tool that encapsulates EAP methods within a Transport Layer Security (TLS) tunnel that provides authentication and potentially encryption.

protected health information (PHI) According to the laws of the United States, PHI is any data that relates to the health status, use of healthcare, payment for healthcare, and other information collected about an individual in relation to their health.

protected mode An alternate name for user mode. The less powerful security domain of the Windows operating environment where user applications reside. User mode is distinct

from kernel mode (aka privileged mode). User mode offers restricted resources, indirect and limited access to hardware, and isolation between processes. *See also* privileged mode.

protection profile (PP) From the Common Criteria for information technology security evaluation, the evaluation element in which a subject states its security needs. PPs specify for a product that is to be evaluated (the target of evaluation [TOE]) the security requirements and protections, which are considered the security desires, or the "I want," from a customer.

protection rings A security design that organizes code and components in an operating system (as well as applications, utilities, or other code that runs under the operating system's control) into concentric rings, each having increasing or decreasing levels of capabilities and access.

protocol A set of rules and restrictions that define how data is transmitted over a network medium (for example, twisted-pair cable, wireless transmission, and so on). Protocols make computer-to-computer communications possible.

protocol analyzer *See also* sniffer.

protocol data unit (PDU) The name of the network container at OSI layers 7, 6, and 5 (Application, Presentation, and Session).

protocol translator A device or software that can translate between protocols. Aka a gateway.

provenance, data provenance, integrity provenance The comparison of the current item (such as a file, application update, firmware version, or configuration setting) to its original status, state, or version. Provenance means place of origin or the earliest known version or history of something.

provisioning When needing to deploy several new instances of a server to increase resource availability, the IT manager must preallocate hardware server resources to the new server instances.

proximity device, proximity card A security device used to manage or control physical access. It can be a passive device, a field-powered device, or a transponder.

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

proxy auto-config (PAC) The settings for a nontransparent proxy. PAC can be implemented with a script or via DHCP.

proxy, proxy server A mechanism that copies packets from one network into another. The copy process also changes the source and destination address to protect the identity of the internal or private network (i.e., NAT/PAT). Proxies may be transparent or nontransparent. Proxies may cache static content to improve network throughput. Aka forward proxy, forwarding proxy, standard proxy, common proxy, or reverse proxy.

proxy falsification Attacks that could modify the local system proxy configuration, the configuration script, or the routing table to redirect communications to a false proxy. This method works only against web communications (or other services or protocols that use a proxy). A rogue proxy server can modify traffic packets to reroute requests to whatever site the hacker wants.

prudent person rule Invoked by the Federal Sentencing Guidelines, the rule that requires senior officials to perform their duties with the care that ordinary, prudent people would exercise under similar circumstances.

pseudo flaws A technique often used on honeypot systems and on critical resources to emulate well-known operating system vulnerabilities.

pseudo-anonymization *See* tokenization.

pseudonymization A technique to mask or obfuscate data using pseudonyms to represent sensitive data. *See* tokenization and anonymization.

pseudo-random number generators A form of random number generation that is based on a predictable entropy source, such as the clocking mechanism of a standard PC.

public cloud A cloud service that is accessible to the general public, typically over an internet connection. Public cloud services often require some form of subscription or pay per use, rather than being offered for free. Generally, public cloud offerings are based on a multitenant configuration. *See* private cloud and hybrid cloud.

public key algorithms The most common example of asymmetric algorithms. In these systems, each user has two keys: a public key, which is shared with all users, and a private key, which is kept secret and known only to the user. But here's a twist: opposite and related keys must be used in tandem to encrypt and decrypt.

public key cryptography, public key cryptosystem *See* asymmetric encryption, asymmetric cryptography.

Public Key Infrastructure (PKI) A framework for deploying asymmetric (or public key) cryptography, along with symmetric cryptography, hashing, and certificates, to obtain a real-world, flexible, and functional secure communications system. PKI isn't a product; rather, it's a blueprint, recipe, or concept for a solution. PKI can provide reliable storage and communication encryption, authentication, digital signatures, digital envelopes, and integrity verification.

public key The shared key of an asymmetric cryptography solution that is freely distributed. It's one of the keys in the public key/private key pair.

public-key cryptosystem, public-key cryptography A subset of asymmetric cryptography based on the use of a key pair set consisting of a public key and a private key. Messages encrypted with one key from the pair can be decrypted only with the other key from the same pair.

public ledger A distributed log of transactions that is hosted by numerous systems across the Internet. This provides for redundancy and further supports the integrity of the blockchain as a whole. Aka distributed ledger.

public, public data The lowest level of commercial business/private sector classification. Used for all data that does not fit in one of the higher classifications. This information is not readily disclosed, but if it is, it should not have a serious negative impact on the organization.

public information sharing centers, private information sharing centers Online locations where information about security compromise events can be posted and access provided to information posted by others. A private information sharing center requires membership. Aka public/private information sharing centers.

public switched telephone network (PSTN) The traditional or legacy landline telephone service. Aka plain old telephone service (POTS).

pulping A paperwork destruction process that involves shredding paper and mixing it with a liquid to create a fibrous mush.

pulverizing A means of device destruction that goes beyond the shredding level to a point where the devices are reduced to a grain or powder.

PUP *See* potentially unwanted programs (PUPs).

purging A data sanitization technique that typically involved multiple overwrites in order to ensure data remnant destruction for the purpose of preventing data recovery.

purple team A single team that performs both the offensive and defensive penetration test or security assessment operations for an organization. *See* red team, blue team, and white team.

push notification services Communication systems that are able to send information to your device rather than having the device (or its apps) pull information from an online resource.

push notifications When a website or online service sends the customer/user a message through an installed mobile app or browser that is then automatically displayed to the user.

Python A programming language used for web server application development, general software development, and automation of system functions. Python is available on most platforms, including many Internet of Things and embedded devices. Python does need an interpreter to execute its scripts; it does not function or operate as a shell.

Q

qualitative decision making A decision-making process that takes nonnumerical factors, such as emotions, investor/customer confidence, workforce stability, and other concerns, into account. This type of data often results in categories of prioritization (such as high, medium, and low).

qualitative risk analysis A risk assessment methodology that assigns subjective and intangible values to the loss of an asset. Scenario-oriented analysis using ranking and grading for exposure ratings and decisions.

quality assurance (QA) An evaluation process employed by many organizations to ensure that newly integrated hardware and software do not reduce performance or efficiency or introduce any unexpected security issues.

quality assurance (QA) check A form of personnel management and project management that oversees the development of a product. QA checks ensure that the product in development is consistent with stated standards, methods of practice, efficiency, and so on.

quality of service (QoS) The oversight and management of the efficiency and performance of network communications. Items to measure include throughput rate, bit rate, packet loss, latency, jitter, transmission delay, and availability.

quantitative decision making The use of numbers and formulas to reach a decision. Options are often expressed in terms of the dollar value to the business.

quantitative risk analysis A risk assessment methodology that assigns real dollar figures to the loss of an asset.

quantum computing An area of advanced theoretical research in computer science and physics. The theory behind it is that we can use principles of quantum mechanics to replace the binary 1 and 0 bits of digital computing with multidimensional quantum bits known as qubits.

quantum cryptography A forward-looking concept that has no publicly known current real-world applications or uses. The idea is to take advantage of the dual nature of light at the quantum level, where it acts both as a wave and as a particle.

quantum key distribution (QKD) An approach to use quantum computing to create a shared secret key between two users, similar to the goal of the Diffie–Hellman algorithm.

quantum supremacy The achievement of creating a quantum computer that can solve a problem that classical computers cannot.

quarantine A type of isolation that prevents an object from interacting with other resources. *See* sandboxing, containerization, and network access control.

query ID (QID) DNS queries are not authenticated, but they do contain a 16-bit value known as the query ID (QID). The DNS response must include the same QID as the query to be accepted.

Quick Response (QR) codes A type of digital bar code that is generally square. Most mobile devices can scan, read, and interpret QR codes natively or with an app. QR codes can be used to encode a wide range of data or information; one common use is to encode a URL.

R

RA *See* registration authority (RA).

race conditions A type of attack or exploit in which the timing of processing is manipulated to cause a negative outcome. *See also* time-of-check-to-time-of-use (TOCTTOU).

RACE Integrity Primitives Evaluation Message Digest *See also* RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest).

radiation monitoring A specific form of sniffing or eavesdropping that involves the detection, capture, and recording of radio frequency signals and other radiated communication methods, including sound and light.

radio frequency identification (RFID) A tracking technology based on the ability to power a radio transmitter using current generated in an antenna when placed in a magnetic field. RFID can be triggered/powered and read from a considerable distance away (often hundreds of meters). Each RFID tag includes a unique identifier so that when a nearby antenna/transceiver activates the tag, it transmits that identifier back to the antenna, where that value is recorded or used to trigger some kind of action. RFID devices may also be used to track individuals (carrying tags), equipment (bearing tags), and so forth, within the premises of an enterprise for security monitoring.

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

RADIUS Federation An option under 802.1X that allows users and their devices to be able to authenticate to other networks in the federated group. This is useful when several companies in the same industry want to grant their workers easy access to internal resources or internet access when traveling or working at an alternate facility.

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

RAID *See* redundant array of independent disks (RAID).

rainbow table A password hash attack based on either precomputed hash databases or hash chains used to quickly reverse-engineer passwords stored in weaker hashing systems, such as LAN Manager.

random access memory (RAM) Readable and writable memory that contains information the computer uses during processing. RAM retains its contents only when power is continuously supplied to it.

random access storage Devices, such as RAM and hard drives, that allow the operating system to request contents from any point within the media.

random number generator A device or system that can produce numbers that cannot be reasonably predicted.

ransomware A form of malware that aims to take over a computer system to block its use while demanding payment. Effectively, it's malware that holds data or an entire computer system hostage in exchange for a ransom payment.

RAS *See* remote access server (RAS).

Raspberry Pi A popular example of a 64-bit microcontroller or a single-board computer.

RAT *See* remote access trojan (RAT).

rate-of-rise detection A fire detection system that detects the fire and triggers the release of the suppression medium when the speed at which the temperature changes reaches a specific level or rate. These are often digital temperature measuring devices, which can be fooled by HVAC heating during winter months and thus are not widely deployed.

RBAC *See* role-based access control (RBAC, RoBAC, or role-BAC). Also an improper acronym for rule-based access control (RuBAC, Rule-BAC).

RC4 *See* Rivest Cipher 4 (RC4).

RC5 *See* Rivest Cipher 5 (RC5).

reactive approach, adversarial approach A means of threat modeling that takes place after a product has been created and deployed. This deployment could be in a test or laboratory environment or to the general marketplace. This technique of threat modeling is the core concept behind ethical hacking, penetration testing, source code review, and fuzz testing.

read-only memory (ROM) Memory that can be read but cannot be written to.

read-through test Copies of disaster recovery plans are distributed to the members of the disaster recovery team for a review performed by reading the plan carefully.

ready state The state in which a process is ready to execute but is waiting for its turn on the CPU.

real evidence Items that can actually be brought into a court of law; aka object evidence.

real memory Typically the largest RAM storage resource available to a computer. It is normally composed of a number of dynamic RAM chips and therefore must be refreshed by the CPU on a periodic basis; aka main memory or primary memory.

real user monitoring (RUM) A variant of passive monitoring where the monitoring tool reassembles the activity of individual users to track their interaction with a website.

realized risk The incident, occurrence, or event when a risk becomes a reality and a breach, attack, penetration, or intrusion has occurred that may or may not result in loss, damage, or disclosure of assets.

realm A collection of users and computers under the same Kerberos authority. Similar to the concept of a domain.

Real-time Transport Protocol (RTP) A common protocol of VoIP that supports the transmission of the data packets of the conversation. *See* Secure Real-time Transport Protocol (SRTP).

real-time operating system (RTOS) An OS designed to process or handle data as it arrives on the system with minimal latency or delay. An RTOS is usually stored on read-only memory (ROM) and is designed to operate in a hard real-time or soft real-time condition.

reasonable expectation of privacy A legal concept used to determine whether a person had a common-sense ability to assume their activities and actions were not being monitored.

reasonableness check The crafting and use of special test suites of data that exercise all paths of the software to the fullest extent possible and comparison of the results to the known correct expected outputs.

recertification (1) Performing a periodic assessment of workers' job responsibilities in relation to their user account's permissions and rights. (2) In relation to formal certification procedures, establishing proof of knowledge and/or skill of a subject; this may relate to the assignment, repeal, or extension of a license or an approval to operate. (3) The act of assessing an organization's compliance with regulations, standards, and their own written security policy. (4) The concept of evaluating the IT infrastructure's mechanisms of account management and privilege assignment to ensure that they continue to provide sufficient authentication and authorization security.

reclassification The process of reevaluating an asset against organizational classification criteria to determine if a new higher or lower classification level should be assigned to the asset due to changes in relative value and importance to the organization over time.

reconnaissance Collecting information about a target, often for the purpose of planning an attack against that target. *See* footprinting, passive reconnaissance, and active reconnaissance.

reconstitution The act of performing a low-level formatting operation on all storage devices on a system, reinstalling the operating system and all applications from trusted original sources, and then restoring files from trusted rootkit-free backups.

record Contents of a table in a relational database.

record retention The organizational policy that defines what information is maintained and for how long. In most cases, the records in question are audit trails of user activity. This may include file and resource access, logon patterns, email, and the use of privileges.

record sequence checking Similar to hash total checking, but instead of verifying content integrity, it involves verifying packet or message sequence integrity.

recovery (1) The process of removing any damaged elements from the environment and replacing or repairing them, as part of an incident response plan (IRP). (2) Bringing business operations and processes back to a working state.

recovery agent A means to retrieve a key from escrow when a user needs to decrypt something. The recovery agent is another user, typically an admin, who has access to an additional key store. Aka key recovery agent.

recovery point objective (RPO) A measurement of how much loss can be accepted by the organization when a disaster occurs.

recovery strategies The practices, policies, and procedures to recover a business that include designating first responders to major incidents, performing critical follow-up tasks, and obtaining insurance to reduce risk of financial loss.

recovery time objective (RTO) The amount of time in which you think you can feasibly recover a function in the event of a disruption. See maximum tolerable downtime (MTD). Aka maximum tolerable outage (MTO).

recovery, recovery control, recovery access control A type of access control that is used to repair or restore resources, functions, and capabilities after a security policy violation. A type of access control that is an extension of corrective controls but has more advanced or complex abilities.

red team The group defined as the attackers in a penetration test or security assessment exercise. *See* blue team, white team, and purple team.

reducing risk The implementation of safeguards and countermeasures to eliminate vulnerabilities or block threats. Aka risk mitigation. *See also* acceptance, risk tolerance, assignment, transfer/transference (as related to risk), avoidance, mitigation, rejecting risk, and ignoring risk.

reduction analysis, decomposing The purpose of this task is to gain a greater understanding of the logic of the product as well as its interactions with external elements. Whether an application, a system, or an entire environment, it needs to be divided into smaller containers or compartments. Those might be subroutines, modules, or objects if focusing on software; computers, operating systems, and protocols if focusing on systems or networks; or departments, tasks, and networks if focusing on an entire business infrastructure. Each identified subelement should be evaluated in order to understand inputs, processing, security, data management, storage, and outputs. This is also sometimes referred to as decomposing the application, system, or environment.

redundancy The implementation of secondary or alternate solutions or means to perform work tasks or accomplish IT functions.

redundant array of independent disks (RAID) A configuration of multiple hard disks used to provide fault tolerance should one or more disks fail. Different levels of RAID exist, depending on the amount and type of fault tolerance provided.

redundant server A mirror or duplicate of a primary server that receives all data changes immediately after they're made on the primary server.

redundant servers A fault-tolerant deployment option that provides for various server recovery or fault tolerance options in the event of a disaster, such as mirroring, electronic vaulting, remote journaling, database shadowing, and clustering.

refactoring A restricting or reorganizing of software code without changing its externally perceived behavior or produced results. Refactoring focuses on improving software's nonfunctional elements, such as quality attributes, nonbehavioral requirements, service requirements, or constraints. Refactoring can improve readability, reduce complexity, ease troubleshooting, and simplify future expansion and extension efforts.

Reference Architecture A result of the Cloud Security Alliance's Trust Cloud Initiative, a set of cloud security tools and an operational methodology to assess the security of a cloud computing environment. Aka CSA Enterprise Architecture (EA).

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

reference profile The digitally stored sample of a biometric factor.

reference template *See* reference profile.

referential integrity Used to enforce relationships between two tables. One table in the relationship contains a foreign key that corresponds to the primary key of the other table in the relationship.

reflected input When a vulnerable website is fed script commands through form fields in such a manner as to trick the site, the input is reflected back to a visitor as if it were original and legitimate content.

register A limited amount of onboard memory in a CPU.

register address, register addressing The address of a register, which is a small memory location directly on the CPU. When the CPU needs information from one of those registers to complete an operation, it can simply use the register address (for example, "register one") to access the information.

registered domain name The name officially registered with a domain registrar off a selected top-level domain (TLD) to establish the base of a fully qualified domain name (FQDN). Example: the term *google* in `www.google.com`.

registered ports, registered software ports Ports 1,024 to 49151, which are registered as being related to one or more networking software products with the International Assigned Numbers Authority (IANA) at `iana.org`.

registration The process of obtaining a certificate.

registration authority (RA) An organization that offloads some of the work from a certificate authority (CA). An RA system operates as a go-between in the process. The RA can distribute cryptography keys, accept registrations for the CA, and validate identities. The RA doesn't issue certificates; that responsibility remains with the CA.

registry, the registry The collection of settings and configurations that control/dictate the operations/functions of the Windows OS and most installed applications.

regression testing A formalized testing process that verifies that the new code performs in the same manner as the old code, other than any changes expected as part of the new release.

regulatory framework A security guidance established by a government regulation or law.

regulatory policy A policy that is required whenever industry or legal standards are applicable to your organization. This policy discusses the regulations that must be followed and outlines the procedures that should be used to elicit compliance.

rejecting risk The act of ignoring risk. To deny that a risk exists or hope that by ignoring a risk it will never be realized. A final but unacceptable possible response to risk. Denying that a risk exists or hoping that it will never be realized isn't a valid, prudent, or due-care response to risk. Aka risk rejection, denying risk, and risk denial. *See other* related terms: acceptance, risk tolerance, assignment, transfer/transference (as related to risk), avoidance, reducing risk, mitigation, and ignoring risk.

relation The table of a relational database.

relational database A database that consists of tables that contain a set of related records.

relationship The association of information in tables of a relational database.

relay agent (1) A service that captures DHCP Discovery requests from clients and forwards them across the network to a DHCP server located in a different subnet. (2) An alternate name for an open SMTP relay. *See* open relay.

relevant Characteristic of evidence that is applicable in determining a fact in a court of law.

remediation The process of dealing with downtime, system compromise, malicious code infection, attack, and so on.

remote access server (RAS) A network server that supports connections from distant users or systems. RAS systems often support modem banks, virtual private network (VPN) links, and even terminal services connections.

remote access trojan (RAT) Malware that grants an attacker some level of remote-control access to a compromised system.

remote access VPN A variant of the site-to-site virtual private network (VPN). The difference is that with a remote access VPN one endpoint is the single entity of a remote user that connects into an organizational network. Aka a host-to-site VPN. *See also* tunnel mode VPN.

remote authentication Any AAA service used to verify the identity of remote users. Examples include Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+), DIAMETER, 802.1X, and Challenge-Handshake Authentication Protocol (CHAP).

Remote Authentication Dial-in User Service (RADIUS) A service used to centralize the authentication of remote access connections. This includes legacy dial-up connections, wireless, and broadband connections via the internet.

remote calling The ability to dial in to a private branch exchange (PBX) system from outside and then access a dial tone to place a call.

remote code execution *See* arbitrary code execution.

remote-control remote access A form of telecommuting that grants a remote user the ability to fully control another system that is physically distant from them. The monitor and keyboard act as if they are directly connected to the remote system.

Remote Desktop Protocol (RDP) A Microsoft protocol that supports remote GUI control over Windows systems. RDP operates over Transmission Control Protocol (TCP) port 3389.

remote journaling Transferring copies of the database transaction logs containing the transactions that occurred since the previous bulk transfer.

remote meeting Technology that enables interaction between remote parties. These technologies and solutions are known by many other terms: digital collaboration, virtual meetings, videoconferencing, software or application collaboration, shared whiteboard services, virtual training solutions, and so on. Any service that enables people to communicate, exchange data, collaborate on materials/data/documents, and otherwise perform work tasks together can be considered a remote meeting technology service.

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

remote node operation A form of telecommuting in which a remote client establishes a direct connection to a local area network (LAN), such as with wireless, virtual private network (VPN), or dial-up connectivity. A remote system connects to a remote access server, which provides the remote client with network services and possible internet access.

Remote Triggered Black Hole (RTBH) An edge filtering concept to discard unwanted traffic based on source or destination address long before it reaches the destination.

remote wipe A security feature that can be used to delete all data and possibly even configuration settings from a device remotely. Typically associated with mobile devices. Aka remote sanitization.

removable media Storage media that is designed to be removed easily and thus is portable between systems.

renewal The process by which a key or certificate is reissued with an extended lifetime date before it expires.

repeater A network device used to amplify signals on network cabling to allow for longer distances between nodes. Aka a concentrator or amplifier.

repellant alarms Alarms that trigger repellants usually sound an audio siren or bell and turn on lights. These kinds of alarms are used to discourage intruders or attackers from continuing their malicious or trespassing activities and force them off the premises.

replay attack Any attack in which data is retransmitted repeatedly (often fraudulently or maliciously). Often replay attacks focus on authentication traffic. For example, an attacker may replay a web session and visit sites intended only for the original user. Aka playback attack.

replication The duplication of data between two locations. Aka cloning and synchronization.

representational state transfer (REST) A common message protocol specification for web services, which at least has a security layer that can be optionally enabled. REST was designed to replace Simple Object Access Protocol (SOAP).

repudiation The ability of a user or attacker to deny having performed an action or activity by maintaining plausible deniability. Repudiation attacks can also result in innocent third parties being blamed for security violations. *See* STRIDE. Aka repudiating or to repudiate.

reputation filtering Several services maintain a grading system of email services in order to determine which are used for standard/normal communications and which are used for spam.

request for comments (RFC) A type of document drafted by the technical community that defines, describes, and prescribes technology specifications. Most RFCs originate from the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), or the Internet Architecture Board (IAB). The RFC concept is an open call for feedback and criticism.

request forgery Attacks that exploit trust relationships and attempt to have users unwittingly execute commands against a remote server. They come in two forms: cross-site request forgery and server-side request forgery.

residual risk The risk that remains after countermeasures are implemented. A concept of residual risk is expressed as follows: total risk + controls gap = residual risk.

resource exhaustion When applications are allowed to operate in an unrestricted and unmonitored manner so that all available system resources are consumed in the attempt to serve the requests of valid users or in response to a denial-of-service (DoS) attack.

resource policies, resource-based policies A means to manage the use of cloud resources, which in turn reduces wasted spending on unnecessary cloud costs. Resource policies can define what resources are provisions, where that takes place, and who is able to trigger and/use those resources. Resource policies provide for granular-level control of cloud resource consumption and can be assigned to services, systems, locations, groups, or individual users.

Resource Record Signatures (RRSIG) A signed resource record in Domain Name System Security Extensions (DNSSEC).

resource records The individual entries in a zone file that define DNS values and relationships, such as an A or Address record that links a fully qualified domain name (FQDN) to an IPv4 address.

response and recovery controls The security mechanisms established by an organization to respond to security incidents. This includes an incident response policy (IRP), business continuity plan (BCP), and disaster recovery plan (DRP).

responsibility Being in charge or having control over something or someone in relation to integrity.

restoration A disaster response strategy that involves bringing a business facility and environment back to a workable state.

restricted interface model A model that uses classification-based restrictions to offer only subject-specific authorized information and functions. One subject at one classification level will see one set of data and have access to one set of functions, whereas another subject at a different classification level will see a different set of data and have access to a different set of functions.

restrictions An alternate name for the rules of rule-based access control. Aka filters.

retention policy A document that defines what data is to be maintained and for what period of time.

retina scan An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The blood vessel pattern at the back of the eyeball is used to establish identity or provide authentication.

retinal scanner A biometric device that analyzes the pattern of blood vessels at the back of the eye.

retrovirus Malware that specifically targets antivirus systems to render them useless.

Reverse Address Resolution Protocol (RARP) A subprotocol of the TCP/IP protocol suite that operates at the Data Link layer (layer 2). RARP is used to discover the IP address of a system by polling using its MAC address.

reverse DNS The process of using an Internet Protocol (IP) address to find a domain name rather than using a domain name to find an IP address (as in the normal Domain Name System [DNS]). Pointer (PTR) records are used for the reverse lookup. Reverse DNS is often used to authenticate incoming connections.

reverse engineering This is considered an unethical form of engineering. Programmers decompile code to understand all the intricate details of its functionality, especially when employed for the purpose of creating a similar, competing, or compatible product.

reverse hash matching An attack used to exploit hashing. The process of discovering the original message that has been hashed by generating potential messages, hashing them, and comparing their hash value to the original. When H(M) = H(M'), then M = M'. *See also* birthday attack.

reverse proxy A proxy system that handles inbound requests from external systems to internally located services. A reverse proxy is similar to the functions of port forwarding and static NAT.

revert to known state A type of backup or recovery process. Many databases support a known state reversion to return to a state of data before edits or changes were implemented. *See* last known good configuration (LKGC).

revocation The process of canceling credentials that have been lost or stolen (or are no longer valid). With certificates, this is accomplished with a certificate revocation list (CRL). Aka to revoke a certificate.

revoke *See* revocation.

RFC *See* request for comments (RFC).

RFC 1918 The public standard that defines the private IP address ranges. *See* private IP addresses.

RFI *See* radio frequency interference (RFI).

RFID *See* radio frequency identification (RFID).

Rich Communication Services (RCS) A communication protocol and service for mobile devices operating over telco services that is intended as a more capable replacement for short message service (SMS) and Multimedia Messaging Service (MMS).

right to audit clause A cloud service provider (CSP) service-level agreement (SLA) statement that gives the customer the ability to investigate performance, compliance, and violation issues in the cloud service.

rights Capabilities assigned to users over objects or the system, such as rebooting, changing system time, or installing updates.

rights management The governance of the permissions and privileges granted to users.

Rijndael block cipher A block cipher that was selected to replace Data Encryption Standard (DES). The Rijndael cipher allows the use of three key strengths: 128 bits, 192 bits, and 256 bits.

ring topology A network structure that connects each system as points on a circle.

RIPEMD-160 (Race Integrity Primitives Evaluation Message Digest) A 160-bit hashing algorithm that is a derivative of RIPEMD, which was itself a variant of MD4. RIPEMD-160 was developed as an alternative to SHA-1, but it has not gained wide popularity and thus isn't widely implemented.

risk The likelihood that any specific threat will exploit a specific vulnerability to cause harm to an asset. Risk is an assessment based on the value of the asset, the amount of potential damage, and the likelihood of the threat occurring. The possibility that something could happen to damage, destroy, or disclose data or other resources.

risk acceptance The result after a cost/benefit analysis shows countermeasure costs would outweigh the possible cost of loss due to a risk. It also means that management has agreed to accept the consequences and the loss if the risk is realized. In most cases, accepting risk requires a clearly written statement that indicates why a safeguard was not implemented, who is responsible for the decision, and who will be responsible for the loss if the risk is realized, usually in the form of a document signed by senior management. Aka accepting risk or acceptance of risk.

risk analysis, risk assessment An element of risk management that includes analyzing an environment for risks, evaluating each risk as to its likelihood of occurring and cost of damage, assessing the cost of various countermeasures for each risk, and creating a cost/benefit report for safeguards to present to upper management. *See also* risk management.

risk appetite The total risk that an organization chooses to or is otherwise able to bear.

risk assessment *See* risk analysis.

risk assignment *See* transferring risk.

risk avoidance The process of selecting alternate options or activities that have less associated risk than the default, common, expedient, or cheap option.

risk awareness The effort to increase the knowledge of risks within an organization.

risk-based access control An access control model attempts to evaluate risk by considering several different elements, such as the environment, the situation, and security policies. Risk-based access control is software code that makes risk- based decisions based on available data. While not recommended, it is sometimes referenced with an acronym of Risk BAC, Risk-BAC or RiskBAC.

risk capacity The level of risk an organization is able to shoulder. An organization's desired risk appetite may be greater than its actual capacity.

risk deterrence The process of implementing deterrents to would-be violators of security and policy.

risk framework A guideline or recipe for how risk is to be assessed, resolved, and monitored. The National Institute of Standards and Technology (NIST) Risk Management Framework is a primary example.

risk limit The maximum level of risk above the risk target that will be tolerated before further risk management actions are taken.

risk management A detailed process of identifying factors that could damage or disclose data, evaluating those factors in light of data value and countermeasure cost, and implementing cost-effective solutions for mitigating or reducing risk. *See also* risk analysis/risk assessment.

Risk Management Framework (RMF) U.S. government guide for establishing and maintaining security crafted by the National Institute of Standards and Technology (NIST) that establishes mandatory requirements for federal agencies. Aka NIST Risk Management Framework (RMF).

risk management strategies Options of risk response or management. Includes acceptance/tolerance, avoidance, assignment/transfer, reduction/mitigation, and rejecting/ignoring.

risk matrix, risk heat map A form of risk assessment that is performed on a basic graph or chart. It is sometimes labeled as a qualitative risk assessment as a 3×3 (or larger) grid comparing probability and damage potential.

Risk Maturity Model (RMM) A risk management tool that assesses the key indicators and activities of a mature, sustainable, and repeatable risk management process. There are several RMM systems, each prescribing various means to achieve greater risk management capability. They generally relate the assessment of risk maturity against a five-level model: ad hoc, preliminary, defined, integrated, and optimized.

risk mitigation *See* reducing risk.

risk register A document that inventories all the identified risks to an organization, system, or within an individual project. Aka risk log.

risk rejection Denying that a risk exists and hoping that it will never be realized are not valid or prudent due care/due diligence responses to risk. Rejecting or ignoring risk may be considered negligence in court. An unacceptable possible response to risk. Aka reject risk, ignoring risk, and ignore risk.

risk reporting The production of a risk report and a presentation of that report to the interested/relevant parties. A key task to perform at the conclusion of a risk analysis.

risk response The process of evaluating countermeasures, safeguards, and security controls using a cost/benefit analysis; adjusting findings based on other conditions, concerns, priorities, and resources; and providing a proposal of response options in a report to senior management. Based on management decisions and guidance, the selected responses can be implemented into the IT infrastructure and integrated into the security policy documentation. *See* risk mitigation, risk assignment, risk deterrence, risk avoidance, risk acceptance, and risk rejection.

risk tolerance The ability of an organization to absorb the losses associated with realized risks. Aka acceptance and tolerating risk.

Rivest Cipher 4 (RC4) A 128-bit stream cipher. RC4 is the foundation of Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) encryption used for wireless networking.

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.

Rivest, Shamir, and Adelman (RSA) (1) One of the providers of cryptography systems to industry and government. RSA stands for the initials of the three founders of RSA Security Inc.: Ron Rivest, Adi Shamir, and Leonard Adleman. RSA has been involved in Public Key Cryptography Standards (PKCS), and it maintains a list of standards for PKCS. Aka RSA Data Security Group. (2) A public key encryption algorithm named after Rivest, Shamir, and Adleman, its inventors. RSA is the most widely used public key cryptography algorithm.

robot network The full term from which the name botnet is derived. *See also* botnet.

robot sentries An automated, often mobile, computer, camera, and sensing system used as an extension of or replacement for security guards.

rogue DNS server A false DNS server that can listen in on network traffic for any DNS query or specific DNS queries related to a target site. Then the rogue DNS server sends a DNS response to the client with false IP information. Once the client receives the response from the rogue DNS server, the client closes the DNS query session, which causes the response from the real DNS server to be dropped and ignored as an out-of-session packet.

rogue access point, rogue wireless access point Any unauthorized access point connected to an open network port or cable that usually isn't configured for security or, if it is, isn't configured properly or isn't in line with the organization's approved access points.

role-based access control (RBAC, RoBAC, Role-BAC) A type of nondiscretionary access control wherein the levels of security closely follow the personnel structure of an organization. RBAC employs job function roles to regulate subject access to objects. The role the person plays in the organization (accountant, salesperson, and so on) corresponds to the level of security access they have to data. *See also* discretionary access control (DAC), mandatory access control (MAC), attribute-based access control (ABAC), and rule-based access control (RuBAC, Rule-BAC).

role-based training A company training program that involves teaching employees to perform their work tasks and to comply with the security policy.

rollback to known configuration A concept similar to that of reverting to a known state, but the difference is that a state retention may address a larger portion of the environment than just configuration. A known configuration is just a collection of settings, not likely to include any software elements, such as code present before a patch was applied.

root, root account The all-powerful user account on Linux and Unix systems.

root CA The certificate authority at the top of a trust structure. It is the first certificate authority (CA) deployed in a trust environment, which must self-sign its own certificates.

root certificate The self-signed certificate issued by a root certificate authority (CA) to itself as the means to establish its trust structure, which other devices can enter into by being issued trusted third-party certificates.

root cause analysis An operational investigation that seeks to identify the reason that an operational issue occurred. The root cause analysis often highlights issues that require remediation to prevent similar incidents in the future.

rooting The action of breaking the digital rights management (DRM) security on the bootloader of a mobile device to be able to operate the device with root or full system privileges. Rooting removes restrictions on Android devices and permits root-level access to the underlying operating system. It is similar to jailbreaking a device running the iOS operating system. *See* jailbreaking.

rootkit A special type of hacker tool that embeds itself deep within an operating system (OS). The rootkit positions itself at the heart of an OS where it can manipulate information seen by the OS and its users.

ROT13 (rotation 13) A substitution cipher based on the 26 letters of the English alphabet (or the basic Latin alphabet). The operation of ROT13 is to shift or substitute each original plaintext letter with the letter located in 13 positions further down the alphabet.

rotation of duties *See* job rotation.

round-robin One of the basic forms of load balancing in which each next request or load is handed to the next server in line.

`route` A command used to view and manipulate the routing table of a system.

route security A protection mechanism where routers are configured to only accept route updates from other authenticated routers.

router A network device used to control traffic flow on networks. A router determines the best path for data packets from source to destination. Routers are often used to connect similar networks together and control traffic flow between them. They can function using statically defined routing tables or employ a dynamic routing system.

Routing Information Protocol (RIP) An example of a distance vector routing protocol.

RPO *See* recovery point objective (RPO).

RSA *See* Rivest, Shamir, and Adelman (RSA).

RSBAC *See* rule set–based access control (RSBAC).

RTO *See* recovery time objective (RTO).

rubber duck antenna *See* base antenna.

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).

rule-based access control (RuBAC, Rule-BAC) A form of access control that is typically used in relation to network devices that filter traffic based on filtering rules. A rule-based system uses a set of rules, restrictions, or filters to determine what can and cannot occur on the system, such as granting subject access, performing an action on an object, or accessing a resource. Firewalls, proxies, and routers are common examples of rule-based access control systems. *See also* discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC, RoBAC, or role-BAC), and attribute-based access control (ABAC).

rule-based management The concept of controlling communication and IT event security through rule- or filter-driven systems.

rules of engagement (RoE) A penetration testing document that defines the means and manner in which the testing is to be performed and conducted. It should include specifics about the scope of the environment to be tested, the types of tests to be performed, and the depth or extent of testing.

runbook An automated series of steps that perform various operations within an incident response event, which could include data enhancement, threat containment, and notification transmission.

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

running state The state in which a process is actively executing. Aka problem state.

runtime code Code that remains in its original human-readable form and is converted into machine language only at the moment of execution. Aka just-in-time (JIT) execution or JIT compilation.

runtime environment A system that allows the portable execution of code across different operating systems. This may include sandboxes, virtual machines, and containerization.

S

S/MIME *See* Secure/Multipurpose Internet Mail Extensions (S/MIME).

SaaS *See* software as a service (SaaS).

sabotage A criminal act committed against an organization by a knowledgeable employee.

safe A movable secured container that is not integrated into a building's construction. *See* vault.

safe harbor A regulatory mechanism that includes a set of Safe Harbor Principles. The seven principles are notice, choice, onward transfer, security, data integrity, access, and enforcement. The goal is to prevent unauthorized disclosure of information, handled by data processors and transmitted between data processors and the data controller. U.S. companies can voluntarily opt into the program if they agree to abide by the seven principles and the requirements outlined in 15 frequently asked questions.

safeguard Anything that removes a vulnerability or protects against one or more specific threats. *See also* control, security control, and countermeasures.

sag Momentary low voltage.

salami attack An attack performed by gathering small amounts of data to construct something of greater value or higher sensitivity. A type of incremental attack.

salt, salting Secret data added to input material prior to the hashing process. Often a value appended to a password before hashing to increase randomness and ensure uniqueness in the resulting stored hash value. This is also known as a cryptographic salt. Bcrypt and Password-Based Key Derivation Function 2 (PBKDF2) are often used to add salts to passwords. Compare with *pepper*.

SAML *See* Security Assertion Markup Language (SAML).

sampling A form of data reduction that allows an auditor to quickly determine the important issues or events from an audit trail. Aka data extraction.

SAN (subject alternative name) certificate A form of certificate that supports a range of names for a single entity, such as hostname, site name, IP address, and common name. A SAN certificate is used to provide authentication to multiple names, but only those names specifically defined.

sandbox, sandboxing A means of quarantine or isolation. It's implemented to restrict new or otherwise suspicious software from being able to cause harm to production systems. It can be used against applications or entire operating systems. A security technique that provides a security boundary for applications and prevents the application from interacting with other applications. Antimalware applications use sandboxing techniques to test unknown applications. If the application displays suspicious characteristics, the sandboxing technique prevents the application from infecting other applications or the operating system.

sanitization, sanitizing Any number of processes that prepare media for destruction. Sanitization is the process that ensures that data cannot be recovered by any means from destroyed or discarded media. Sanitization can also be the actual means by which media is destroyed. Media can be sanitized by purging or degaussing without physically destroying the media.

SATCOM (satellite communication) *See* satellite communication (SATCOM).

satellite communication (SATCOM) A means of audio and data transmission using satellites orbiting in near-earth orbit.

SCADA (Supervisory Control and Data Acquisition) A type of industrial control system (ICS). An ICS is a form of computer-management device that controls industrial processes and machines.

scalability The ability for a system to handle an ever-increasing level or load of work. It can also be the potential for a system to be expanded to accommodate future growth.

scanless An online public port scan scrapper.

scanning Similar to casing a neighborhood prior to a burglary, it's the process by which a potential intruder looks for possible entryways into a system. Scanning can indicate that illegal activity will follow, so it is a good idea to treat scans as incidents and to collect evidence of scanning activity.

SCAP *See* Security Content Automation Protocol (SCAP).

scarcity A social-engineering technique based on convincing someone that an object has a higher value based on its scarcity.

scavenging A form of dumpster diving performed electronically. Online scavenging searches for useful information in the remnants of data left over after processes or tasks are completed. This could include audit trails, log files, memory dumps, variable settings, port mappings, cached data, and so on.

scenario In relation to risk assessment, it is a written description of a single major threat. The description focuses on how a threat would be instigated and what effects its occurrence could have on the organization, the IT infrastructure, and specific assets.

schema The structure that holds the data that defines or describes a database. The schema is written using a Data Definition Language (DDL).

Scoping Part of the tailoring process and refers to reviewing a list of baseline security controls and selecting only those controls that apply to the IT systems you're trying to protect. *See* tailoring.

SCP *See* secure copy (SCP).

screen filter A display protective device that reduces the range of visibility of a screen down to a maximum of 30 degrees from perpendicular. Aka privacy filter.

screen lock A security-like feature that limits access to a mobile phone or other portable device. Usually it requires a code or a pattern to be entered to unlock the device.

screen scraper, screen scraping 1) Remote control, remote access, or remote desktop–like services. 2) A technology that can allow an automated tool to interact with a human interface in order to parse the results to extract just the relevant information.

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

screened subnet A method of placing web and other servers that serve the general public outside the firewall and, therefore, isolating them from internal network access. These servers should be hardened and trust relationships limited to prevent transitive trust attacks. Placing virtualized servers inside the screened subnet is considered a bad security practice for similar reasons, even though virtualization security has improved significantly in the last few years. Previously known as DMZ. *See* extranet.

script kiddie A threat actor who is less knowledgeable than a professional skilled attacker. A malicious individual who doesn't understand the technology behind security vulnerabilities but downloads ready-to-use software (or scripts) from the internet and uses them to launch attacks against systems. Script kiddies are usually unable to program their own attack tools and may not understand exactly how the attack operates.

scripted access A method to automate the logon process with a script that provides the logon credentials to a system. It is considered a form of single sign-on.

Scrum An agile framework derivative concept that guides the development, delivery, and maintenance of complex products and systems. It is based around teams of 10 or fewer members, which work on goals or tasks that can be completed in two weeks (or no longer than one month), known as sprints, and process tracking occurs via 15-minute daily standing-only meetings (called scrums or daily scrums). Scrums are led by the project's Scrum master, an individual in a project management role who is responsible for helping the team move forward and meet their objectives. *See* sprints. Aka stand-up meeting.

SDH (Synchronous Digital Hierarchy) *See* Synchronous Digital Hierarchy (SDH).

search warrant A document obtained through the judicial system that allows law enforcement personnel to acquire evidence from a location without first alerting the individual believed to have perpetrated a crime.

SECaaS *See* security as a service (SECaaS).

seclusion A means of storing something in an out-of-the-way location. This location can also provide strict access controls and can help enforce confidentiality protections.

secondary authoritative name servers The DNS servers that distribute the load of DNS resolution. This server obtains a read-only copy of the zone file from the primary authoritative name server.

secondary evidence A copy of evidence or an oral description of the contents of best evidence.

secondary memory Magnetic/optical media and other storage devices that contain data not immediately available to the CPU.

secondary storage Data repositories that include magnetic and optical media, such as tapes, disks, hard drives, and CD/DVD storage.

secondary verification mechanism Any means to confirm the detection of the first or primary detection mechanism, usually performed prior to triggering a full response to unwanted activity. This could include a security guard, security camera, or a second detection event.

secondary victim Intermediary systems used in a distributed denial-of-service (DDoS) attack that are innocent but that enable the attacker to generate significant levels of traffic directed toward the primary target and provide anonymity to the attacker.

second-tier attack An assault that relies on information or data gained from eavesdropping or other similar data-gathering techniques. In other words, it is an attack that is launched only after some other attack is completed.

secrecy The act of keeping something a secret or preventing the disclosure of information.

secret A government/military classification, used for data of a secret nature. Unauthorized disclosure of secret data could cause serious damage to national security.

secret key *See* private key.

secrets management The collection of technologies used to manage digital authentication credentials, such as password hashes, session and storage encryption keys, and digital certificates. Secrets management can also oversee API access, application tokens, federation, and identity and access management (IAM).

secure boot A feature of Unified Extensible Firmware Interface (UEFI) that aims to protect the operating environment of the local system by preventing the loading or installing of device drivers or an operating system that is not signed by a preapproved digital certificate. Secure boot thus protects systems against a range of low-level or boot-level malware, such as certain rootkits and backdoors. *See* measured boot and boot attestation.

secure communication protocol A protocol that uses encryption to provide security for the data transmitted by it.

secure copy (SCP) A secure file-transfer facility based on Secure Shell (SSH) and Remote Copy Protocol (RCP).

secure defaults A design philosophy where defaults are selected to be secure rather than prioritizing ease of use and installation.

secure electronic transaction (SET) A security protocol for the transmission of transactions over the internet. SET is based on RSA encryption and DES. SET had the support of major credit card companies, such as Visa and Mastercard. However, it has mostly been abandoned in light of newer and more secure alternatives.

secure facility plan A guide that outlines the security needs of your organization and emphasizes methods or mechanisms to employ to provide security. Such a plan is developed through risk assessment and critical path analysis.

Secure FTP (SFTP) File Transfer Protocol (FTP) based on Secure Shell (SSH) secure connections.

secure hash algorithm (SHA) [SHA-1, SHA-2, SHA-3] A government standard hash function developed by the National Institute of Standards and Technology (NIST) and specified in an official government publication. SHA-1 creates a 160-bit hash value output. Members of the SHA-2 family create a range of hash value outputs: 224, 256, 384, or 512. SHA-3 is a drop-in replacement for SHA-2, which provides the same hash length outputs.

Secure Hypertext Transfer Protocol (S-HTTP) A deprecated protocol used for secure communications between a web server and a web browser. It was encrypted by SSH.

Secure Real-time Transport Protocol (SRTP, Secure RTP) A security improvement over the Real-time Transport Protocol (RTP) that is used in many Voice over IP (VoIP) communications. SRTP aims to minimize the risk of VoIP DoS through robust encryption and reliable authentication.

Secure Remote Procedure Call (S-RPC) An authentication service. S-RPC is a means to prevent unauthorized execution of code on remote systems.

Secure Shell (SSH) An end-to-end encryption technique. This suite of programs provides encrypted alternatives to common internet applications such as FTP, Telnet, and rlogin. There are two versions of SSH. SSH1 supports the DES, 3DES, IDEA, and Blowfish algorithms. SSH2 drops support for DES and IDEA but adds support for several other algorithms.

Secure Sockets Layer (SSL) A legacy protocol that secured application layer protocols by operating at the Transport layer to encrypt TCP payloads. It has been replaced by Transport Layer Security (TLS). *See also* Transport Layer Security (TLS).

secure token A protected, possibly encrypted authentication dataset that proves a particular user or system has been verified through a formal logon procedure. Aka authentication token or token.

Secure/Multipurpose Internet Mail Extensions (S/MIME) An internet standard for encrypting and digitally signing email. S/MIME takes the standard MIME element of email, which enables email to carry attachments and higher-order textual information (fonts, color, size, layout, and so on), and expands this to include message and attachment encryption.

security as a service (SECaaS) A cloud provider concept in which security is provided to an organization through or by an online entity. The purpose of an SECaaS solution is to reduce the cost and overhead of implementing and managing security locally. One example of SECaaS is monitoring as a service (MaaS). *See* managed service provider (MSP) and managed security service provider (MSSP).

Security Assertion Markup Language (SAML) An XML-based open standard convention for communication authentication and authorization details between security domains, systems, services, and devices, often over web protocols. SAML is often used to provide a web-based single sign-on (SSO) solution.

security assessments Comprehensive reviews of the security of a system, application, or other tested environment. During a security assessment, a trained information security professional performs a risk assessment that identifies vulnerabilities in the tested environment that may allow a compromise and makes recommendations for remediation, as needed.

security association (SA) In an IPsec session, the representation of the communication session and the process of recording any configuration and status information about the connection.

security association manager A communication protocol, such as Internet Security Association Key Management Protocol (ISAKMP), that manages the security associations (the agreed-on method of authentication) used by two entities.

security audits Evaluations performed with the purpose of demonstrating the effectiveness of controls to a third party. Security audits use many of the same techniques followed during security assessments but must be performed by independent auditors. The staff members who design, implement, and monitor controls for an organization have an inherent conflict of interest when evaluating the effectiveness of those controls.

security baseline A standardized minimum level of security with which all systems in an organization must comply. This lowest common denominator establishes a firm and reliable security structure on which to build trust and assurance.

security boundary The line of intersection between any two areas, subnets, or environments that have different security requirements or needs.

security camera A device used to record events occurring in the view area of the lens. Typically, a security camera creates a digital record of an event. Security cameras can be used to provide a live feed of an area or just a recording. Aka video surveillance, video monitoring, closed-circuit television (CCTV).

security champions People who take the lead in a project, such as development, leadership, or training, to enable, support, and encourage the adoption of security knowledge and practices through peer leadership, behavior demonstration, and social encouragement. Often a security champion is a member of a group who decides (or is assigned) to take charge of leading the adoption and integration of security concepts into the group's work activities. Security champions are often nonsecurity employees who take up the mantle to encourage others to support and adopt more security practices and behaviors. Security champions are often found in software development, but this concept can be useful in any group of employees in any department.

Security Content Automation Protocol (SCAP) An effort led by the National Institute of Standards and Technology (NIST) in an effort to establish a standardized means to define and communicate security-related event and issue information. SCAP provides a common framework and naming conventions for the discussion of security vulnerabilities and also facilitates the automation of interactions between different security systems.

security control The mechanism used to address security vulnerabilities to reduce or manage risk. *See also* control, safeguards, and countermeasures.

Security Control Assessment (SCA) The formal evaluation of a security infrastructure's individual mechanisms against a baseline or reliability expectation.

security control baselines A mandated set of security controls that provide a starting point for implementing security and ensure a minimum security standard.

security control framework The formal structure of the security solution desired by the organization.

security development lifecycle (SDL) A Microsoft security management process used to consider and implement security at each stage of a product's development. This supports the motto of "Secure by Design, Secure by Default, Secure in Deployment and Communication" (aka SD3+C).

security domain A collection of users and computers under a single authentication, authorization, accounting (AAA) authority, and security policy.

security framework A guide or plan for keeping organizational assets safe. It provides a structure to the implementation of security for both new organizations and those with a long history.

security function The aspect of operating a business that focuses on the task of evaluating and improving security over time. To manage the security function, an organization must implement proper and sufficient security governance.

security governance The collection of practices related to supporting, defining, and directing the security efforts of an organization.

security groups Collections of entities, typically users, but can also be applications and devices, which can be granted or denied access to perform specific tasks or access certain resources or assets.

security guard Personnel who monitor and enforce facility security. Aka guard.

security ID A form of physical identification; generally contains a picture of the subject and/or a magnetic strip with additional information about a subject.

security incident *See* computer security incident.

security information and event management (SIEM) A centralized application to automate the monitoring of network systems across an enterprise network.

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

security label An assigned classification or sensitivity level used in security models to determine the level of security required to protect an object and prevent unauthorized access.

security layers A type of network or environment organization in which devices with different levels of classification or sensitivity are grouped together and isolated from other groups with different security levels.

security management planning The act of thoroughly and systematically designing procedural and policy documentation to reduce risk and then to maintain risk at an acceptable level for a given environment.

security mode The U.S. government has designated four approved security modes for systems that process classified information; *see* dedicated security mode, system-high security mode, compartmented security mode, and multilevel security mode.

security model A way for designers to map abstract statements into a security policy that prescribes the algorithms and data structures necessary to build hardware and software. Thus, a security model gives software designers something against which to measure their design and implementation.

Security Orchestration, Automation, Response (SOAR) A collection of software solutions that can automate the process of collecting and analyzing log and real-time data, evaluate it in light of materials from threat intelligence sources, and then trigger response to low- and mid-level severity issues without the need for human involvement.

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

security policy A document that defines the scope of security needs of an organization, prescribes solutions to manage security issues, and discusses the assets that need protection and the extent to which security solutions should go to provide the necessary protection.

security posture Proper preparation against attacks and other forms of unplanned downtime. The overall security plan and its implementation is a security posture. *See also* security baseline.

security professional Trained and experienced network, systems, and security engineer who is responsible for following the directives mandated by senior management.

security role The part an individual plays in the overall scheme of security implementation and administration within an organization.

security target (ST) The evaluation element from the Common Criteria for information technology security evaluation in which a vendor states the security features of its product. STs specify the claims of security from the vendor that are built into a target of evaluation (TOE). STs are considered the implemented security measures, or the "I will provide," from the vendor.

security template A set of security settings that can be mechanically applied to a computer to establish a specific configuration. Security templates can be used to establish baselines or bring a system into compliance with a security policy. *See* Group Policy Object (GPO).

security tests Security tests verify that a control is functioning properly. These tests include automated scans, tool-assisted penetration tests, and manual attempts to undermine security. Security testing should take place on a regular schedule, with attention paid to each of the key security controls protecting an organization.

security through obscurity The concept of attempting to gain security by hiding or not being noticed among the crowd of other targets. This is effectively security hide-and-seek. It is not considered a valid security approach for any organization.

Security Trust Assurance and Risk (STAR) A Cloud Security Alliance (CSA) program that focuses on improving cloud service provider (CSP) security through auditing, transparency, and integration of standards.

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

Security-Enhanced Android (SEAndroid) A security improvement for Android. SEAndroid is a framework to integrate elements of Security-Enhanced Linux into Android devices.

segment The combination of Transport layer TCP header and payload.

segmentation The act of subdividing a network into numerous smaller units. These smaller units, groupings, segments, or subnetworks (i.e., subnets) can be used to improve various aspects of the network. Segmentation can boost performance, reduce congestion, compartmentalize communication problems (such as broadcast storms), and provide security improvements through traffic isolation. Segments can be created by using switch-based VLANs, routers, or firewalls (as well as combinations of all of these).

self-encrypting drive (SED) A storage device that offers onboard hardware-based encryption services. *See* whole-disk encryption (WDE).

self-signed certificate A certificate signed by the same entity for which it identifies. A root certificate authority (CA) issues its first certificate for itself as a self-signed certificate, and any peer trust members also issue self-signed certificates.

semantic integrity mechanisms A common security feature of a database management system (DBMS). This feature ensures that no structural or semantic rules are violated. It also checks that all stored data types are within valid domain ranges, that only logical values exist, and that any and all uniqueness constraints are met.

semi-authorized entity, semi-authorized hacker A term used to refer to either a reformed criminal or a skilled IT professional operating undercover to perform ethical hacking (aka penetration testing). Previously known as gray hat.

Sender Policy Framework (SPF) An email spam solution that operates by checking that inbound messages originate from a host authorized to send messages by the owners of the SMTP origin domain.

senior management, senior manager A person or group who is ultimately responsible for the security maintained by an organization and who should be most concerned about the protection of its assets. They must sign off on all policy issues, and they will be held liable for the overall success or failure of a security solution. It is the responsibility of senior management to show prudent due care. Also referred to as organizational owner and upper management.

sensitive or sensitive data The classification label used for data that is more important or valuable than public data but is more organizationally related than personnel related. A modest but still negative impact could occur for the company if sensitive data is disclosed. Aka for internal use only (FIUO), for office use only (FOUO), and sensitive information.

Sensitive but Unclassified (SBU) A data classification label used for data that is for internal use or office use only. Often SBU is used to protect information that could violate the privacy rights of individuals.

sensitive compartmented information facility (SCIF) A secure or restricted work area often used by government and military agencies, divisions, and contractors to provide a secure environment for highly sensitive data storage and computation. The purpose of an SCIF is to store, view, and update sensitive compartmented information (SCI), which is a type

of classified information. An SCIF has restricted access to limit entrance to those individuals with a specific business need and authorization to access the data contained within. This is usually determined by the individual's clearance level and SCI approval level. In most cases, an SCIF has restrictions against using or possessing photography, video, or other recording devices while in the secured area. An SCIF can be established in a ground-based facility, an aircraft, or a floating platform. An SCIF can be a permanent installation or a temporary establishment, and it is typically located within a structure, although an entire structure can be implemented as an SCIF.

sensitivity In regard to biometric devices, the level at which the device is configured for scanning. In regard to confidentiality, it refers to the quality of information that could cause harm or damage if disclosed.

sensitivity label The classification placed on an object.

sensor A hardware or software tool used to monitor digital or physical activities or events to record information or at least take notice of an occurrence. A sensor may monitor network activity, heat, humidity, wind movement, doors and windows opening, the movement of data, the types of protocols in use on a network, when a user logs in, any activity against sensitive servers, and much more. A sensor collects information and then transits it back to a central system for storage and analysis. Sensors are common elements of fog computing, ICS, IoT, IDS/IPS, and SIEM/security orchestration, automation, and response (SOAR) solutions. *See* collector.

sentiment analysis The concept of analyzing text information for its content and context to identify and extract subjective information from that written material. This is effectively a programmatic means to analyze human speech and behavior by monitoring and analyzing written communications.

separation of duties (SoD) A set of policies designed to reduce the risk of fraud and prevent other losses in an organization through the application of job responsibility compartmentalization. When it is implemented, organizations have administrators with focused privileges rather than broad systemwide privileges.

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

separation of privilege The principle that builds on the principle of least privilege. It requires the use of granular access permissions—that is, different permissions for each type of privileged operation. This allows designers to assign some processes rights to perform certain supervisory functions without granting them unrestricted access to the system.

Sequenced Packet Exchange (SPX) The Transport layer protocol of the IPX/SPX protocol suite from Novell.

sequential storage Devices that require that you read (or speed past) all of the data physically stored prior to the desired location. A common example of a sequential storage device is a magnetic tape drive.

Serial Line Internet Protocol (SLIP) A legacy 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 only supports serial communications. Was replaced by PPP.

server A computer that provides resources to clients on a network.

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

server cage *See* server vault.

server clustering The grouping of servers into a collective so that they each share the load of offering a service or resource to a network.

server room *See* server vault.

server vault A dedicated room within an office space where mission-critical systems and network devices are stored, operated, and secured. Aka server cage, server room, IT closet, or datacenter/data center.

serverless architecture A cloud computing concept where code is managed by the customer and the platform (i.e., supporting hardware and software) and the server is managed by the CSP. There is always a physical server running the code, but this execution model allows the software designer/architect/programmer/developer to focus on the logic of their code and not have to be concerned about the parameters or limitations of a specific server. Aka function as a service (FaaS).

server-side request forgery (SSRF) A clever exploit where a vulnerable server is coerced into functioning as a proxy.

service account A user account that is used to control the access and capabilities of an application. Aka managed service account.

service bureaus Businesses that lease computer time through contractual agreements and provide all IT needs in the event of some disaster or business interruption that requires a disaster recovery plan or business continuity plan to be enacted. Aka cloud computing service.

service delivery platform (SDP) A collection of components that provide the architecture for service delivery. SDP is often used in relation to telecommunications, but it can be used in many contexts, including VoIP, Internet TV, SaaS, and online gaming. An SDP is similar to a content delivery network (CDN). The goal of an SDP is to provide transparent communication services to other content or service providers. Both SDPs and CDNs can be implemented using microservices.

service delivery objective (SDO) The minimum level of restored services that must be quickly reestablished after a disaster event (i.e., the interruption of a mission-critical service); once the SDO is reached, the disaster is abated and work can focus on returning to normal levels of operation.

Service Organization Controls (SOC) Report A report produced by an auditor that includes the results of security assessments of a cloud provider.

service pack An operating system update from Microsoft.

service provider The resource host, as related to Security Assertion Markup Language (SAML), which allows a subject verified by a trusted and linked identity provider to access its resource.

Service Provisioning Markup Language (SPML) A markup language used with federated identity management systems to exchange user information for federated identity single sign-on purposes. It is derived from the Standard Generalized Markup Language (SGML), the Extensible Markup Language (XML), and the Generalized Markup Language (GML).

Service Set Identifier (SSID) broadcast A wireless network's announcement of its SSID on a regular basis in a special packet known as the beacon frame.

Service Set Identifier (SSID) The name of a wireless network.

service-specific remote access A form of telecommuting that gives users the ability to remotely connect to and manipulate or interact with a single service, such as email.

service ticket (ST) A one-time use derivative of the Kerberos ticket-granting ticket (TGT).

service-level agreement (SLA), service level agreement An agreement that specifies performance requirements for a vendor. A contractual obligation to your clients that requires you to implement sound practices. Also used to ensure acceptable levels of service from suppliers. This agreement may use mean time between failures (MTBF) and mean time to repair (MTTR) as performance measures.

service-oriented architecture (SOA) A means to construct new applications or functions out of existing but separate and distinct software services.

services integration The design and architecture of an IT/IS solution that stiches together elements from on-premises and cloud sources into a seamless productive environment. The goals of services integration is to eliminate data silos (a situation where data is contained in one area and thus inaccessible to other applications or business units), expand access, clarify processing visibility, and improve functional connectivity of on-site and off-site resources. Aka cloud integration, systems integration, and integration platform as a service (iPaas).

SESAME A ticket-based authentication mechanism similar to Kerberos.

session hijacking An attack that occurs when a malicious individual intercepts part of a communication between an authorized user and a resource and then uses a hijacking technique to take over the session and assume the identity of the authorized user. *See* TCP/IP hijacking.

Session Initiation Protocol (SIP) A protocol used as part of VoIP services that enables the establishment of the connection between caller and callee. *See* Real-time Transport Protocol (RTP).

session key The key used between a client and a server during a session, which is agreed on during connection. This key is generated by encrypting the server's digital ID (after validity has been established). The 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. *See also* ephemeral key.

Session layer (layer 5 of the OSI) 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 dialogues between two stations. *See also* Open Systems Interconnection (OSI).

session replay The recording of a subject's visit to a website, interaction with a mobile application, or use of a PC application, which is then played back by an administrator, investigator, or programmer to understand what occurred and why based on the subject's activities.

SET *See* Secure Electronic Transaction (SET).

sFlow An industry-standard packet monitoring service that is similar to Cisco's proprietary NetFlow.

SFTP *See* Secure FTP (SFTP).

SHA *See* Secure Hash Algorithm (SHA).

shadow IT A term used to describe the IT components (physical or virtual) deployed by a department without the knowledge or permission of senior management or the IT group. Aka embedded IT, feral IT, stealth IT, hidden IT, secret IT, and client IT.

shared key authentication (SKA) One of the original authentication options of 802.11 in relation to WEP. A fixed value, similar to a password, is used to authenticate as well as encrypt the session.

shared responsibility The security design principle that indicates that organizations do not operate in isolation. Instead, they are intertwined with the world in numerous ways. It is our task to realize this shared responsibility and take our role in this situation seriously.

Shibboleth An example of an authentication federation and single sign-on solution. Shibboleth is a standards-based open source solution that can be used for website authentication across the internet or within private networks.

shielded twisted-pair (STP) A twisted-pair wire that includes a metal foil shielding wrapper inside the outer sheath to provide additional protection from electromagnetic interference (EMI).

shielding The use of a barrier to absorb or block electromagnetic interference (EMI), radio frequency interference (RFI), or other types of signal or noise.

shimming (1) A means of injecting alternate or compensation code into a system to modify its operations without changing the original or existing code. (2) A form of lock picking.

Shiva Password Authentication Protocol (SPAP) A basic encrypted remote access authentication protocol.

Short Message Service (SMS) The telco service that supports text messaging.

shoulder surfing The act of gathering information from a system by observing the monitor or the use of the keyboard by the operator without proper authorization.

shredding An effective destruction technique for both paperwork and media storage devices; however, different equipment is needed for these two different types of items.

shrink-wrap license agreement A license written on the outside of software packaging. Such licenses get their name because they commonly include a clause stating that you acknowledge agreement to the terms of the contract simply by breaking the shrink-wrap seal on the package.

S-HTTP *See* Secure Hypertext Transfer Protocol (S-HTTP).

side-channel attack A passive, noninvasive attack to observe the operation of a device. Side-channel attacks are used against smartcards. Common side-channel attacks are power monitoring attacks, timing attacks, and fault analysis attacks.

sideloading, sideload The activity of installing an app onto a device by bringing the installer file to the device through some form of file transfer or USB storage method rather than installing from an app store.

Signal Protocol A cryptographic protocol that provides end-to-end encryption for voice communications, videoconferencing, and text message services. The Signal Protocol is nonfederated and is a core element in the messaging app named Signal.

signage Signs that provide directive information, such as declaring areas off-limits to those who are not authorized, indicating that security cameras are in use, and disclosing safety warnings.

signature based detection, signature detection, signature-based detection An intrusion detection system (IDS) method used to compare current traffic or events to a database of signatures, examples, or patterns of known malicious or unwanted activity. *See also* anomaly-based detection, behavior-based detection, and heuristic-based detection.

signature dynamics When used as a biometric, the use of the pattern and speed of a person writing their signature to establish identity or provide authentication.

signed applet An applet or mobile code that has been digitally signed by the owner.

SIM *See* subscriber identity module (SIM). Aka SIM card.

Simple Authentication and Security Layer (SASL) The TLS encrypted authentication option of LDAP/LDAPS.

Simple Certificate Enrollment Protocol (SCEP) A system by which devices can request a certificate automatically using a URL and a preshared secret. Many mobile device management (MDM) solutions use SCEP to issue certificates to enrolled mobile devices.

Simple Integrity Axiom (SI Axiom) An axiom of the Biba model that states that a subject at a specific classification level cannot read data with a lower classification level. This is often shortened to "no read down."

Simple Key Management for IP (SKIP) An encryption tool used to protect sessionless datagram protocols.

Simple Mail Transfer Protocol (SMTP) The primary protocol used to transfer or send email messages from clients to servers and from server to server.

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

Simple Object Access Protocol (SOAP) A common message protocol specification for web services, it is considered insecure since it was designed around plaintext HTTP protocols. SOAP is being replaced by representational state transfer (REST).

Simple Security Property (SS property) A property of the Bell–LaPadula model that states that a subject at a specific classification level cannot read data with a higher classification level. This is often shortened to "no read up."

simplex One-way communication.

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

simulations Re-creations or approximations of real-world events but in a fully controlled environment. Simulations can be performed in secondary facilities, in temporary staged re-creations of production systems, or through virtual reality (VR).

Simultaneous Authentication of Equals (SAE) An authentication option of WPA3 that uses a password, but it no longer encrypts and sends that password across the connection. Instead, SAE performs a zero-knowledge proof process known as Dragonfly Key Exchange, which is itself a derivative of Diffie–Hellman. The process uses a preset password and the MAC addresses of the client and AP to perform authentication and session key exchange.

single loss expectancy (SLE) The cost associated with a single realized risk against a specific asset. The SLE indicates the exact amount of loss an organization would experience if an asset were harmed by a specific threat. SLE = asset value ($) * exposure factor (EF).

single point of failure (SPoF) Any one item, element, or pathway that could cause significant downtime or system failure if broken, offline, or overloaded.

single point of failure Any element of an infrastructure—such as a device, service, protocol, or communication link—that would cause total or significant downtime if compromised, violated, or destroyed, affecting the ability of members of your organization to perform essential work tasks.

single sign-on (SSO) A mechanism that allows subjects to authenticate themselves only once to a system. With SSO, once subjects are authenticated, they can freely roam the network and access resources and services without being rechallenged for authentication.

single state Systems that require the use of policy mechanisms to manage information at different levels. In this type of arrangement, security administrators approve a processor and system to handle only one security level at a time.

single-factor authentication Using only one factor to authenticate. Aka one-factor authentication.

single-loss expectancy (SLE) The potential dollar value loss from a single risk realization incident. It's calculated by multiplying the exposure factor by the asset value.

single-use passwords A variant of dynamic passwords that are changed every time they are used.

site risk assessment, site-specific risk assessment The activity of performing a risk assessment focusing on a specific geographic location or facility.

site survey A formal assessment of wireless signal strength, quality, and interference using an RF signal detector. A site survey is performed by placing a wireless base station in a desired location and then collecting signal measurements from throughout the area. A site survey often produces a heat map.

site-to-site VPN A site-to-site virtual private network (VPN) is a VPN between two organizational networks. *See also* tunnel mode.

skimming The duplication of data from a credit card or other similar type of storage device. Skimming can be accomplished by a small handheld device, by a device planted in a point-of-sale (POS) device (such as an ATM or gas pump), or by a card reader connected to a PC. *See* card cloning.

Skipjack Associated with the Escrowed Encryption Standard, an algorithm that operates on 64-bit blocks of text. It uses an 80-bit key and supports the same four modes of operation supported by DES. Skipjack was proposed but never implemented by the U.S. government. It provides the cryptographic routines supporting the Clipper and Capstone high-speed encryption chips designed for mainstream commercial use.

SLE *See* single-loss expectancy (SLE).

sliding windows The ability of TCP to dynamically alter its transmission window size based on link reliability.

SLIP *See* Serial Line Internet Protocol (SLIP).

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

smart device A range of mobile devices that offer the user a plethora of customization options, typically by installing apps, and may take advantage of on-device or in-the-cloud artificial intelligence (AI) processing. *See* Internet of Things (IoT).

smart meter A remotely accessible utility meter.

smishing A social engineering attack that occurs over or through standard text messaging services or apps.

smoke-actuated detection A fire detection system that detects the fire and triggers the release of the suppression medium when smoke is detected using either photoelectric or radioactive ionization sensors as triggers. Either method monitors for light or radiation obstruction or reduction across an air gap caused by particles in the air. It is intended to be triggered by smoke, but dust and steam can sometimes trigger the alarm.

SMTP relay The email server's normal function of relaying messages using Simple Mail Transfer Protocol (SMTP) to the email server hosting the destination inbox. Open SMTP relays are problematic because they accept and relay any message from any sender, and thus they're popular targets of spammers.

SMTP *See* Simple Mail Transfer Protocol (SMTP).

smurf attack A type of distributed reflective denial of service (DRDoS). A smurf attack occurs when an amplifying server or network is used to flood a victim with useless ICMP reply packets.

`sn1per` A utility that is an automated pentest recon scanner. It is able to perform system discovery, port scanning, and vulnerability scanning against targets. It is available as a free CLI or a professional GUI version.

snapshot A backup of a virtual machine or guest operating system.

sniffer A physical device that listens in on (sniffs) 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. Aka protocol analyzer, network evaluator, network analyzer, traffic monitor, or packet capturing utility.

sniffer attack Any activity that results in a malicious user obtaining information about a network or the traffic over that network. A sniffer is often a packet-capturing program that duplicates the contents of packets traveling over the network medium into a file. Also referred to as a snooping attack.

sniffing The act of examining the contents of network packets (or complete communications) surreptitiously. A form of network traffic monitoring. Sniffing often involves the capture or duplication of network traffic for examination, re-creation, and extraction. Aka wiretapping and sniffing attack. *See also* eavesdropping, packet sniffing, and network sniffing.

sniping Using an automated agent to submit a last-second bid on an online auction.

SNMP *See* Simple Network Management Protocol (SNMP).

SNMPv3 The most current version of SNMP (as of 2020) that allows for encrypted communications between devices and the management console, as well as robust authentication protection customized authentication factors. *See* Simple Network Management Protocol (SNMP).

snooping attack *See* sniffer attack.

snooping The process of looking through files in hopes of finding something interesting.

SOA *See* service-oriented architecture (SOA).

social engineering An attack that abuses people by deceiving them into revealing information, tasking abusive action, or granting unauthorized access.

social media analysis A means to evaluate aspects of the lifestyle and personality of job applicants via online social networks to discard those who don't seem to match the expectations or culture of the organization.

social network An online community where public interaction and discussion take place.

socket The combination of IP address and port used in an active TCP/IP communication session.

SOCKS Short for Socket Secure, as in TCP/IP ports, SOCKS is a common implementation of a circuit-level firewall.

software analysis Conducting forensic reviews of applications or the activity that takes place within a running application.

software as a service (SaaS) A cloud computing concept that provides on-demand online access to specific software applications or suites without the need for local installation.

Software Assurance Maturity Model (SAMM) An open source project maintained by the Open Web Application Security Project (OWASP). It seeks to provide a framework for integrating security activities into the software development and maintenance process as well as offer organizations the ability to assess their maturity.

software configuration management (SCM) *See* configuration management (CM) (3).

software development kits (SDKs) Tools for programmers that provide guidance on software crafting as well as solutions, such as special APIs, subroutines, or stored procedures, which can simplify the creation of software for complex execution environments.

software development life cycle (SDLC) A software development management concept that helps ensure a more reliable and stable product by establishing a standardized process by which new ideas become actual software. *See also* waterfall model, spiral model, and Agile. Aka Software Development Life-cycle Methodology (SDLM).

software escrow agreement (SEA), software escrow arrangement A risk management tool that can protect a company against the failure of a third-party software developer. An SEA can address whether the developer is able to provide adequate support for its products or against the possibility that the developer goes out of business. Under an SEA, the developer provides copies of the source code to an independent third-party organization, i.e., the escrow organization.

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

software IP encryption (swiPe) A layer 3 security protocol for IP. It provides authentication, integrity, and confidentiality using an encapsulation protocol.

software library, Software libraries A collection of reusable code for developers. These libraries perform a variety of functions, ranging from text manipulation to machine learning, and are a common way for developers to improve their efficiency.

software-defined data center (SDDC) The concept of replacing physical IT elements with solutions provided virtually, and often by an external third party, such as a cloud service provider (CSP). SDDC is effectively another XaaS concept, namely IT as a service (ITaaS). It is similar to infrastructure as a service (IaaS), and thus some claim it is nothing more than a marketing or advertising term of misdirection. Aka virtual data center (VDC).

software-defined everything (SDx) The trend of replacing hardware with software using virtualization. SDx includes virtualization, virtualized software, virtual networking, containerization, serverless architecture, infrastructure as code, SDN, VSAN, software-defined storage (SDS), VDI, VMI, SDV, and software-defined data center (SDDC).

software-defined network (SDN), software defined network, software-defined networking, software defined networking A unique approach to network operation, design, and management. The concept is based on the theory that the complexities of a traditional network with on-device configuration (i.e., routers and switches) often force an organization to stick with a single device vendor and limit the flexibility of the network to changing physical and business conditions. SDN aims at separating the infrastructure layer (i.e., hardware and hardware-based settings) from the control layer (i.e., network services of data transmission management). SDN offers a new network design that is directly programmable from a central location, is flexible, is vendor neutral, and is based on open standards. *See* Network Functions Virtualization (NFV). Aka virtualized network, virtual network, and network virtualization.

software-defined security Security controls are actively managed by code, allowing them to be directly integrated into the continuous integration/continuous delivery (CI/CD) pipeline.

software-defined storage (SDS) Another derivative of SDN. SDS is a SDN version of a SAN or NAS. SDS is storage management and provisioning solution that is policy driven and is independent of the actual underlying storage hardware. It is effectively virtual storage.

software-defined visibility (SDV) A framework to automate the processes of network monitoring and response. The goal is to enable the analysis of every packet and make deep intelligence-based decisions on forwarding, dropping, or otherwise responding to threats.

software-defined wide-area networks (SDWAN, SD-WAN) An evolution of SDN that can be used to manage the connectivity and control services between distant data centers, remote locations, and cloud services over WAN links.

someone you know An authentication factor based on a chain of trust, such as being allowed into a building when someone who knows you vouches for you.

something you are An authentication factor based on a physical characteristic, part of your human body.

something you do, something you can do An authentication factor that is a task you complete or a skill or action you can perform, such as a logic puzzle or following a series of steps.

something you exhibit An authentication factor that focuses on some fact that is discoverable about the subject or their connection, such as whether they are local or remote or whether the connection is plaintext or encrypted.

something you have An authentication factor that is a physical object.

something you know An authentication factor based on information memorized.

somewhere you are An authentication factor based on where you are located.

SONET (Synchronous Optical Network) *See* Synchronous Optical Network (SONET).

Source Network Address Translation (SNAT) *See* network address translation (NAT).

spam The term describing unwanted email, newsgroup, or discussion forum messages. Spam can be as innocuous as an advertisement from a well-meaning vendor or as malignant as floods of unrequested messages with viruses or Trojan horses attached.

spamming attacks, spamming Sending significant amounts of spam to a system in order to cause a DoS or general irritation, consume storage space, or consume bandwidth and processing capabilities. Aka mail bombing.

Spanning Tree Protocol (STP) A switch protocol used to eliminate looped switch paths that could result in broadcast storms (loss of network capacity).

SPAP *See* Shiva Password Authentication Protocol (SPAP).

spear phishing A more targeted form of phishing in which the message requesting information appears to originate from a colleague or coworker at a user's company or organization, often someone in a position of authority.

SPF *See* Sender Policy Framework (SPF).

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

spim Spam over instant messaging (IM).

spiral model A software development life cycle (SDLC) model, derived from the waterfall model, which is designed around repeating the earlier phases multiple times, known as iterations, to ensure that each element and aspect of each phase is fulfilled in the final product.

SpIT (Spam over Internet Telephony) *See* vishing.

split DNS, split-DNS Deploying a DNS server for public use and a separate DNS server for internal use. All data in the zone file on the public DNS server is accessible by the public via queries or probing. Aka split-horizon DNS, split-view DNS, and split-brain DNS.

split knowledge A combination of separation of duties and two-man control. The basic idea is that the information or privilege required to perform an operation is divided among multiple users. This ensures that no single person has sufficient privileges to compromise the security of the environment.

split tunnel A virtual private network (VPN) configuration that allows a VPN-connected system to access both the organizational network over the VPN as well as the internet directly at the same time. The split tunnel thus grants a simultaneously open connection to the internet as well as the organizational network. *See* full tunnel.

SPML *See* Service Provisioning Markup Language (SPML).

spoofed email An email message that has a fake or falsified source address. Domain Message Authentication Reporting and Conformance (DMARC) is used to filter spoofed messages.

spoofing An attempt by someone/something to impersonate or masquerade as someone/something else. The act of replacing the valid source and/or destination IP address and node numbers with false ones. Aka spoofing attack.

spraying The attempt to log into a user account through repeated attempts of submitting generated or pulled-from-a-list credentials. Aka password spraying or credential stuffing.

spread spectrum Communication that occurs over multiple frequencies at the same time.

sprints The Scrum methodology organizes work into short sprints of activity. These are well-defined periods of time, typically between 1 and 4 weeks, where the team focuses on achieving short-term objectives that contribute to the broader goals of the project. At the

beginning of each sprint, the team gathers to plan the work that will be conducted during each sprint. At the end of the sprint, the team should have a fully functioning product that could be released, even if it does not yet meet all user requirements. Each subsequent sprint introduces new functionality into the product.

spyware Software that monitors your actions and transmits important details to a remote system that spies on your activity. Sometimes used for malicious and illicit purposes, such as identity theft or account takeover.

SQL injection An attack against vulnerable web applications where a hacker submits SQL database expressions and script code in order to bypass authentication and interact directly with the database management system (DBMS) or underlying operating system.

SQL injection attack (SQLi) *See* Structured Query Language (SQL) injection (SQLi) attack.

sqlmap An open source database vulnerability scanner.

SRTP (Secure Real-time Transport Protocol, Secure RTP) *See* Secure Real-time Transport Protocol (SRTP, Secure RTP)

SSAE *See* Statement on Standards for Attestation Engagements (SSAE).

SSAE SOC reports American Institute of Certified Public Accountants (AICPA) established the auditing standard of Statement on Standards for Attestation Engagements (SSAE). System and Organization Controls (SOC) reports can be of three types: SOC1 focuses on finances, SOC2 focuses on security, and SOC3 is a variant of SOC2 designed for public distribution.

SSH *See* Secure Shell (SSH).

SSID *See* Service Set Identifier (SSID).

SSID broadcast *See* Service Set Identifier (SSID) broadcast.

SSL *See* Secure Sockets Layer (SSL).

SSL/TLS accelerators Devices used to offload the operation of encryption to a dedicated hardware device. Aka Transport Layer Security (TLS) accelerators. Aka SSL/TLS offloader.

SSL/TLS decryptor A dedicated device used to decode secure communications for the purpose of filtering and monitoring. Aka Transport Layer Security (TLS) decryptor and SSL/TLS inspection.

SSO *See* single sign-on (SSO).

staging, staging network A network segment where new equipment or code, whether developed in house or obtained from external vendors, is configured to be in compliance with the company's security policy and configuration baseline.

stakeholder management The attempt to maintain beneficial relationships with those who have the most impact on the operations of an organization.

stakeholders Those who establish, support, and promote an organization as well as those affected by the actions of the organization and the decisions of its leadership.

stand-alone mode, standalone mode A wireless network that uses a wireless access point to connect wireless clients together but does not offer any access to a wired network. Aka stand-alone mode infrastructure.

standard An element of a security policy. Defines the regulatory, legal, contractual, or voluntary security obligations or requirements for the IT infrastructure. *See also* benchmark.

standard naming convention A formal policy that may dictate the parameters of names for systems, shares, user account names, and email addresses.

standard operating procedure (SOP) An organizational policy that provides detailed or granular step-by-step instructions to accomplish a specific task. *See also* procedure.

standards Documents that define compulsory requirements for the homogenous use of hardware, software, technology, and security controls. They provide a course of action by which technology and procedures are uniformly implemented throughout an organization. Standards are tactical documents that define steps or methods to accomplish the goals and overall direction defined by security policies.

Star Integrity Axiom *See* * (star) Integrity Axiom.

star topology A network structure that employs a centralized connection device. This device can be a simple hub or switch. Each system is connected to the central hub by a dedicated segment.

Star Security Property *See* * (star) Security Property.

STARTTLS An SMTP command. Once the initial SMTP connection is made to the email server, the STARTTLS command will be used. If the target system supports TLS, then an encrypted channel will be negotiated. Otherwise, it will remain as plaintext. STARTTLS's secure session will take place on TCP port 587. STARTTLS can also be used with IMAP connections, whereas POP3 connections use the STLS command to perform a similar function.

state A snapshot of a system at a specific instance in time.

state actor An attacker who is operating on behalf of their country's government, military, or other powerful leadership. Typically, a state actor attacks targets in other countries for the benefit of their home country. Generally, state actors are APT groups. Aka nation-state hacker.

state attack Attacks that focus on timing, data flow control, and transition between one system state to another. *See* time of check to time of use (TOCTOU, TOC2TOC, TOCTTOU, TOC/TOU), race conditions, and communication disconnects.

state machine model A system that is designed so that no matter what function is performed, it is always a secure system.

state transition Within the context of the state machine model, a transition occurs when accepting input or producing output. A transition always results in a new state.

stateful Focusing on, paying attention to, or evaluating based on existing local conditions and recent activity and traffic (such as previous packets and established sessions). *See* stateless. Aka context analysis or contextual analysis.

stateful inspection firewall A firewall that evaluates the state or the context of network traffic. By examining source and destination addresses, application usage, source of origin, and relationship between current packets with the previous packets of the same session, stateful inspection firewalls are able to grant a broader range of access for authorized users and activities and actively watch for and block unauthorized users and activities. A type of firewall that is aware that any valid outbound communication (especially related to Transmission Control Protocol [TCP]) will trigger a corresponding response or reply from the external entity. Aka dynamic packet filtering firewall.

stateful NAT The ability or means by which network address translation (NAT) maintains information about the communication sessions between clients and external systems. NAT operates by maintaining a mapping between requests made by internal clients, a client's internal IP address, and the IP address of the internet service contacted.

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.

stateless Filtering actions that consider each packet individually rather than the context of previous packets or established sessions.

stateless firewall A firewall that analyzes packets on an individual basis against the filtering access control lists (ACLs) or rules. The context of the communication (that is, any previous packets) is not used to make an allow or deny decision on the current packet.

Statement on Standards for Attestation Engagements (SSAE) Auditing standard to be used by auditors performing assessments of controls at service organizations. Aka Reporting on Controls. *See* SSAE SOC reports.

static analysis, static code analysis A software evaluation technique that decompiles a program and looks for known malicious subroutines or duplicates of code sections from known malware. Aka static testing. *See* dynamic analysis and manual code review.

static code A value that does not change. It is the same value each time it is used, even when used by multiple subjects. Examples include the combination to a safe, the code for a lock, or the password to a WAP.

static environment A set of conditions, events, and surroundings that don't change. In technology, static environments are applications, operating systems, hardware sets, or networks that are configured for a specific need, capability, or function, and then set to remain unaltered.

static IT environment Any system that is intended to remain unchanged by users and administrators. The goal is to prevent or at least reduce the possibility of a user implementing change that could result in reduced security or functional operation.

static NAT When network address translation (NAT) is configured with a static inbound mapping that allows external entities to initiate sessions with systems behind the NATing device. Aka reserves proxy, port forwarding, and destination network address translation (DNAT).

static OS The concept of a static system/environment or to indicate a slight variation. That variation is that the OS itself is beyond the ability of the user to change but the user can install or use applications. Often, those applications may be limited, restricted, or controlled in order to avoid allowing an application to alter the otherwise static OS.

static packet-filtering firewall A firewall that filters traffic by examining data from a message header. Usually, the rules are concerned with source, destination, and port addresses. Aka screening router.

static password A password that does not change over time or that remains the same for a significant period of time.

static system, static environment A set of conditions, events, and surroundings that don't change. In theory, once understood, a static environment doesn't offer new or surprising elements. A static IT environment is any system that is intended to remain unchanged by users and administrators. The goal is to prevent or at least reduce the possibility of a user implementing change that could result in reduced security or functional operation.

static testing Evaluates the security of software without running it by analyzing either the source code or the compiled application. Aka static application security testing (SAST).

static token A physical means to provide identity, usually not employed as an authentication factor. Examples include a swipe card, a smartcard, a floppy disk, a USB RAM dongle, or even something as simple as a key to operate a physical lock.

station set identifier (SSID) The name of a wireless network that each wireless client must know in order to communicate with the host access point.

statistical attack This type of attack exploits statistical weaknesses in a cryptosystem, such as floating-point errors or an inability to produce random numbers. It attempts to find vulnerabilities in the hardware or operating system hosting the cryptography application.

statistical intrusion detection *See* behavior-based detection.

stealth virus Malicious code that attempts to avoid detection by masking or hiding its activities.

steganography The act of embedding messages or files within another message or file.

stop error The security response of an operating system, such as Windows, when an application performs an illegal operation, such as accessing hardware or modifying/accessing the memory space of another process.

stopped state The state in which a process is finished or must be terminated. At this point, the operating system can recover all memory and other resources allocated to the process and reuse them for other processes as needed.

storage area network (SAN) A secondary network (distinct from the primary communications network) used to consolidate and manage various storage devices.

storage device A memory device designed to hold files, data, and/or information. Aka data storage device. *See* primary storage and secondary storage.

storage policy A document that defines the means, mechanisms, and locations for long-term housing of storage devices.

storage segmentation A device management technique used to artificially compartmentalize various types or values of data on a storage medium. On a mobile device, the device manufacturer and/or the service provider may use storage segmentation to isolate the device's OS and preinstalled apps from user-installed apps and user data. Some mobile device management systems further impose storage segmentation in order to separate company data and apps from user data and apps.

store-and-forward device A networking device that uses a memory buffer to store packets until they can be forwarded on to a slower network segment.

stored procedure A subroutine or software module that can be called on or accessed by applications interacting with a relational database management system (RDBMS).

STP *See* shielded twisted pair (STP), Spanning Tree Protocol (STP).

strategic intelligence gathering, strategic counterintelligence gathering A research technique that consists of the investigative and interviewing skills that some law enforcement officers, military personnel, and deputized civilians in certain cases use to discover information that may be relevant to a criminal activity. Evidence of a crime may not always be obvious and located where expected. It takes the skill, expertise, and experience of a seasoned investigator to approach each investigation with fresh eyes and a flexible methodology. Aka strategic intelligence/counterintelligence gathering.

strategic plan A long-term plan that is fairly stable. It defines the organization's goals, mission, and objectives. A strategic plan is useful for about five years if it is maintained and updated annually. The strategic plan also serves as the planning horizon.

stream attack A type of denial of service (DoS). A stream attack occurs when a large number of packets are sent to numerous ports on the victim system using random source and sequence numbers. The processing performed by the victim system attempting to make sense of the data will result in a DoS. Also referred to as flooding.

stream ciphers Ciphers that operate on each character or bit of a message (or data stream) one character/bit at a time.

streaming audio An audio transmission that is being presented to the end user as it is received based on an ongoing transmission from the provider/server. Streaming media is commonly served over the internet either in real time (i.e., live) or on demand.

streaming video A video transmission that is being presented to the end user as it is received based on an ongoing transmission from the provider/server. Streaming media is commonly served over the internet either in real time (i.e., live) or on demand.

stress testing A variation of dynamic analysis in which a hardware or software product is subjected to various levels of workload to evaluate its ability to operate and function under stress. *See* dynamic code analysis.

STRIDE A Microsoft threat categorization scheme composed of spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

strong authentication Any authentication that uses two or more factors, even if those factors aren't unique. *See* multifactor authentication (MFA).

strong password A password that is resistant to dictionary and brute-force attacks.

Structured Query Language (SQL) injection (SQLi) attack An attack that uses unexpected input to a web application to gain unauthorized access to an underlying database.

Structured Query Language (SQL) The language used to interact with most relational databases.

Structured Threat Information Expression (STIX) An effort to develop a standardized language and repetitional structure for the organization and dissemination of cyber-threat indicators and related information. The STIX framework endeavors to support a broad range of details relating to IoC and specific cyberthreats, while remaining expressive, flexible, automated, and human-readable.

structured walkthrough A procedure in which a group discusses the steps of an emergency response or recovery plan to clarify roles, assess responsibilities, detect deficiencies, address oversights, and conceive of alternative options. *See also* tabletop exercise.

subdomain The portion of a fully qualified domain name (FQDN) to the left of the registered domain name. Example: the *www* in `www.google.com`. Aka hostname.

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

subject alternative name (SAN) An element of a certificate that can hold multiple domain names so that a single certificate can be used to verify multiple domain names, IP addresses, or identities.

subpoena A court order that compels an individual or organization to surrender evidence or to appear in court.

subscriber identity module (SIM) A device used in many mobile phones and other devices to link the device to the account of a customer. Similar to a smartcard.

substitution cipher An encryption algorithm that replaces each character or bit of the plaintext message with a different character. Aka monoalphabetic substitution cipher. *See also* polyalphabetic substitution cipher.

succession planning The process of identifying and preparing specific people, usually existing personnel, who will be called on to replace those in key leadership positions.

suicide hacker A hacker that engages in highly destructive activity with the knowledge that they will most likely be caught. Their motivations may differ, but they feel that they have nothing to lose and do not attempt to hide their activity.

supervised learning A type of machine learning training/programming technique that uses labeled data for training. The analyst creating a machine learning model provides a dataset along with the correct answers and allows the algorithm to develop a model that may then be applied to future cases.

supervisor state, supervisory state The state in which a process is operating in a privileged, all-access mode.

supervisory control and data acquisition (SCADA) An ICS unit that can operate as a standalone device, be networked together with other SCADA systems, or be networked with traditional IT systems. Most SCADA systems are designed with minimal human interfaces. Often, they use mechanical buttons and knobs or simple LCD screen interfaces (similar to what you might have on a business printer or a GPS navigation device). However, networked SCADA devices may have more complex remote-control software interfaces.

supervisory mode Mode in which processes at layer 0 run. Layer 0 is the ring where the operating system itself resides.

supply chain The sequence or preceding processes, operations, and events involved in the development, production, and distribution of a device, product, service, or commodity.

supply chain risk management (SCRM) The means to ensure that all the vendors or links in the supply chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners (although not necessarily to the public).

surge Prolonged high voltage.

surge protector An electrical safety device whose fuse will trip or blow (i.e., burn out) and all power will be cut off in the event of an increase in voltage. Surge protectors should be used only when instant termination of electricity will not cause damage or loss to the equipment.

surveillance system Any device that is intended to monitor and track assets and/or subjects. These can be embedded systems, or they can be dedicated sensors.

suspension, certificate suspension, certificate hold The process of placing a certificate on a temporary hold to use it again in the future before it expires.

Sutherland model An integrity model that focuses on preventing interference in support of integrity.

swap file, pagefile, paging file A special storage file used when virtual memory is enabled to use space on a storage device to expand the addressable memory space of a system.

swIPe *See* software IP encryption (swIPe).

switch A layer 2 network device that tracks the media access control (MAC) addresses of the systems connected on each port. Instead of repeating traffic on every outbound port, a switch repeats only traffic out of the port on which the destination is known to exist. Switches offer greater efficiency for traffic delivery, create separate broadcast and collision domains, and improve the overall throughput of data.

Switched Multimegabit Data Service (SMDS) A connectionless network communication service. SMDS provides bandwidth on demand. SMDS is a preferred connection mechanism for linking remote LANs that communicate infrequently.

switched network A network that has multiple routes to get from a source to a destination, allowing for higher speeds.

Switched Port Analyzer (SPAN) *See* port spanning.

switched virtual circuit (SVC) A virtual circuit that must be rebuilt each time it is used; similar to a dial-up connection.

symmetric cryptography, symmetric cryptosystem A cryptography system that uses a single shared encryption key to encrypt and decrypt data. Aka private key cryptography and secret key cryptography.

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

symmetric multiprocessing (SMP) A type of system in which the processors share not only a common operating system but also a common data bus and memory resources. The collection of processors also works collectively on a single task, code, or project.

SYN flood attack A denial-of-service (DoS) attack in which the hacker sends a barrage of 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.

synchronous communications A means of data transfer that relies on a timing or clocking mechanism based on either an independent clock or a timestamp embedded in the data stream. Synchronous communications are typically able to support very high rates of data transfer.

Synchronous Data Link Control (SDLC) A layer 2 protocol employed by networks with dedicated or leased lines. SDLC was developed by IBM for remote communications with Systems Network Architecture (SNA) systems. SDLC is a bit-oriented synchronous protocol.

Synchronous Digital Hierarchy (SDH) A fiber-optic–based high-speed networking standard defined by the International Telecommunications Union (ITU). Similar to SONET. SDH and SONET are mostly hardware or physical layer standards defining infrastructure and line speed requirements. SDH and SONET use synchronous time-division multiplexing (TDM) to high-speed duplex communications with minimal need for control and management overhead. *See also* Synchronous Optical Network (SONET).

synchronous dynamic password token Token used in a token device that generates passwords at fixed time intervals. Time interval tokens require that the clock of the authentication server and the token device be synchronized. The generated password is entered by the subject along with a PIN, passphrase, or password.

synchronous dynamic passwords Passwords that are time based and synchronized with an authentication server.

Synchronous Optical Network (SONET) A fiber-optic–based high-speed networking standard defined by the American National Standards Institute (ANSI). Similar to Synchronous Digital Hierarchy (SDH). SONET and SDH are mostly hardware or physical layer standards defining infrastructure and line speed requirements. SDH and SONET use synchronous time-division multiplexing (TDM) to high-speed duplex communications with minimal need for control and management overhead.

Synchronous Transport Modules (STM) The communications method used by SDH.

Synchronous Transport Signal (STS) The communications method used by SONET. Aka Optical Carrier (OC).

synthetic monitoring Website monitoring technique that performs artificial transactions against a website to assess performance. *See* active monitoring.

synthetic transactions Scripted transactions with known expected results. The testers run the synthetic transactions against the tested code and then compare the output of the transactions to the expected state. Any deviations between the actual and expected results represent possible flaws in the code and must be further investigated.

syslog (System Logging Protocol) A standardized mechanism to transit logs and event messages to a centralized specific retention server. Aka rsyslog, syslog-ng.

system administrator The individual tasked with the responsibilities of implementing the security and functionality policies and requirements as established by the organization and the system owner.

system call A process by which an object in a less-trusted protection ring requests access to resources or functionality by objects in more trusted protection rings.

system compromise A situation in which the security of a system has been breached. Aka a security breach, security compromise, intrusion, or violation.

system high mode *See* system-high security mode.

system on a chip (SoC) An integrated circuit (IC) or chip that has all of the elements of a computer integrated into a single chip. This often includes the main central processing unit (CPU), memory, a graphics processing unit (GPU), Wi-Fi, wired networking, peripheral interfaces (such as Universal Serial Bus [USB]), and power management.

system owner The entity responsible for setting the requirements for a system. The system owner may be the organization as a whole or an individual network/IT manager.

system resilience The ability of a system to maintain an acceptable level of service during an adverse event. It relies on fault-tolerant components and also effective intrusion detection and intrusion prevention systems.

system scanning The act of using a vulnerability scanner to review and examine the security and configuration state of a system.

system security policy A how-to manual used to inform and guide the design, development, implementation, testing, and maintenance of a particular system. Thus, this kind of security policy tightly targets a single implementation effort.

system sprawl The situation in which numerous underutilized servers are operating in an organization's server room. These servers are taking up space, consuming electricity, and placing demands on other resources, but not in a ratio to their provided workload or productivity that would justify their presence. Aka server sprawl.

system testing Early development process testing performed by the programmers/developers to seek any obvious errors.

system-high security mode Mode in which systems are authorized to process only information that all system users are cleared to read and have a valid need to know. Systems running in this mode are not trusted to maintain separation between security levels, and all information processed by these systems must be handled as if it were classified at the same level as the most highly classified information processed by the system.

system-specific security policy A security policy that focuses on individual systems or types of systems and prescribes approved hardware and software, outlines methods for locking down a system, and even mandates firewall or other specific security controls.

T

table The main building block of a relational database; Aka a relation.

tabletop exercise, table-top exercise A discussion meeting focused on a potential emergency event, usually performed verbally or with minimal visual aids (such as blueprints, charts, or board game miniatures representing resources). It's a means to walk through and evaluate an emergency plan in a stress-free environment.

TACACS+ *See* Terminal Access Controller Access Control System Plus (TACACS+).

tactical plan A midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan. A tactical plan is typically useful for about a year. It often prescribes and schedules the tasks necessary to accomplish organizational goals.

tactics, techniques, and procedures (TTPs) The collection of information about the means, motivations, and opportunities related to advanced persistent threats (APTs). The goal of collecting TTP information is to gain a fuller understanding of who the group is, what their purposes and intentions are, and their reconnaissance and attack techniques.

`tail` A Linux/Unix command that displays the last 10 lines of a file. It can also be used to display a custom number of lines or bytes from the end of a file.

tailgating A means by which an unauthorized person gains access or entry to a secured environment using the credentials of an authorized person who is unaware that the tailgater is present. *See also* piggybacking.

tailoring Modifying the list of security controls within a baseline to align with the organization's mission.

Take-Grant model A model that employs a directed graph to dictate how rights can be passed from one subject to another or from a subject to an object. Simply put, a subject with the grant right can grant another subject or another object any other right they possess. Likewise, a subject with the take right can take a right from another subject.

tampering Any action resulting in unauthorized changes or manipulation of data, whether in transit or in storage. *See* STRIDE.

tangible asset Physical assets owned by the company.

tap A means to eavesdrop on network communications.

task-based An access control methodology in which access is granted based on work tasks or operations.

TCP *See* Transmission Control Protocol (TCP).

TCP sequence attack *See* Transmission Control Protocol (TCP) sequence attack.

TCP wrapper An application that can serve as a basic firewall by restricting access based on user IDs or system IDs.

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

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

TCP/IP model A protocol model based directly on the TCP/IP protocol stack that consists of four layers. The four layers of the TCP/IP model are Application (also known as Process), Transport (also known as Host-to-Host), Internet (sometimes Internetworking), and Link (although Network Interface and sometimes Network Access are used). Aka DARPA model or the DOD model.

`tcpdump` A raw packet-capturing CLI utility found on Linux. It can be used to capture packets into a capture file. It supports command-line capture filters to collect specific packets.

`tcprelay` A suite of packet manipulation utilities used to edit and transmit previously captured network traffic. It was designed originally to stress-test IDSs, but it can be used to send traffic to any target.

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

technical access control, technical control The hardware or software mechanisms used to manage access to resources and systems and provide protection for those resources and systems. Examples of logical or technical access controls include encryption, smartcards, passwords, biometrics, constrained interfaces, access control lists, protocols, firewalls, routers, IDEs, and clipping levels. The same as logical access control or logical control.

technical physical security controls Security controls that use technology to implement some form of physical security, including intrusion detection systems, alarms, CCTV, monitoring, HVAC, power supplies, and fire detection and suppression.

technical security, technical controls *See* logical security, logical controls.

technology convergence The tendency for various technologies, solutions, utilities, and systems to evolve and merge over time. Often this results in multiple systems performing similar or redundant tasks or one system taking over the features and abilities of another. Though in some instances this can result in improved efficiency and cost savings, it can also represent a single point of failure and become a more valuable target for malicious hackers and intruders.

telecommunications room Serves the connection needs of a floor or a section of a large building by providing space for networking equipment and cabling systems. It also serves as the interconnection point between the backbone distribution system and the horizontal distribution system. This is also known as the wiring closet.

telecommuting, telecommute Performing work at a remote location (i.e., other than the primary office), such as one's home or while traveling, often connecting into the primary office network over a VPN.

telephony The collection of methods by which telephone services are provided to an organization, or the mechanisms by which an organization uses telephone services for either voice and/or data communications. Traditionally, telephony included plain old telephone service (POTS) or public switched telephone network (PSTN) services combined with modems. However, this has expanded to include private branch exchange (PBX), Voice over IP (VoIP), and virtual private networks (VPNs).

Telnet A protocol that functions at the Application layer of the OSI model, providing terminal-emulation capabilities. Telnet has been deprecated in favor of Secure Shell (SSH).

TEMPEST The study and control of electronic signals produced by various types of electronic hardware, such as computers, televisions, phones, and so on. Its primary goal is to prevent EM and RF radiation from leaving a strictly defined area so as to eliminate the possibility of external radiation monitoring, eavesdropping, and signal sniffing.

template A preestablished starting point. A template can be crafted for a plethora of concerns in an environment, including a security policy, a procedure, a contract, a submission form, a system image, a software configuration, and a firewall rule set.

Temporal Key Integrity Protocol (TKIP) A security solution designed as the replacement for Wired Equivalent Privacy (WEP) without requiring replacement of legacy wireless hardware. TKIP was implemented in 802.11 wireless networking under the name Wi-Fi Protected Access (WPA). TKIP and WPA were officially replaced by WPA2 in 2004.

temporary internet files The temporary storage of files downloaded from internet sites that are being held by the client's utility (typically a browser) for current and possibly future use. Mostly this cache contains website content, but other internet services can use a file cache as well. Aka internet files cache.

Terminal Access Controller Access Control System Plus (TACACS+) A Cisco proprietary authentication system that allows credentials to be accepted from multiple methods, including Kerberos. The TACACS+ client/server process is similar to that of Remote Authentication Dial-In User Service (RADIUS). There are three versions of TACACS: the original TACACS, XTACACS (extended TACACS), and TACACS+. TACACS integrates the authentication and authorization processes. XTACACS keeps the authentication, authorization, and accounting processes separate. TACACS+ improves XTACACS by adding two-factor authentication. TACACS+ is the most commonly used of the three.

terrorist attacks Attacks that differ from military and intelligence attacks in that the purpose is to disrupt normal life, whereas a military or intelligence attack is designed to extract secret information.

test coverage analysis A test evaluation technique that estimates the degree of testing conducted against new software.

test data method A form of program testing that examines the extent of the system testing to locate untested program logic.

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

tethering The activity of sharing the cellular network data connection of a mobile device with other devices. The sharing of data connection can take place over Wi-Fi, Bluetooth, or USB cable.

TFTP *See* Trivial File Transfer Protocol (TFTP).

The Diamond Model of Intrusion Analysis A tool designed to assist incident analysts in characterizing threats, track attack evolution, differentiate variations, and determine countermeasures. The Diamond Model focuses on the characteristics of and relationships between four elements: the adversary, capabilities, infrastructure, and victims.

`theHarvester` A tool used for OSINT gathering. It automatically interacts with dozens of online datasets, search engines, and information services to produce a dossier on the specified target.

thicknet *See* 10Base5.

thin access point A WAP that is little more than a wireless transmitter/receiver, which must be managed from a separate external centralized management console called a wireless controller.

thin client A term used to describe a workstation that has little or no local processing or storage capacity. A thin client is used to remotely access and control a mainframe, virtual machine, or virtual desktop infrastructure (VDI).

thinnet *See* 10Base2.

third-party app store Sources of apps that are something other than the official app store for a particular device or product line.

third-party audit An audit conducted by, or on behalf of, another organization, such as a regulatory authority.

third-party connectivity Very few organizations operate exclusively using internal resources; most organizations interact with outside third-party providers. Most of these external entities do not need to interact directly with an organization's IT/IS. However, for those few that do, it is important to consider the risks and ramifications.

third-party governance The system of oversight that may be mandated by law, regulation, industry standards, or licensing requirements.

threat A potential harmful occurrence that may cause an undesirable or unwanted outcome for an organization or a specific asset.

threat actor, threat agent The person or entity responsible for causing or controlling any security violating incidents experienced by an organization or individual.

threat events Accidental exploitations of vulnerabilities.

threat feed Sources of information about attacks and exploits.

threat hunting The activity of security professionals to seek out and identify new threats. A threat hunt is a proactive search through IoCs, log files, or other observables to locate malware or intruders lurking on a system.

threat intelligence The collection of information about threat actors and the threats they represent. The goal of threat intelligence is to learn enough about potential harms that defenses can be implemented to mitigate those harms.

threat map A real-time map of cyberattacks that are taking place. Aka cyber threat maps, cyberattack maps, and DoS maps.

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

threat probability, threat likelihood A calculation of the potential for a threat to cause damage to an asset.

threat vector The path or means by which an attacker can gain access to a target to cause harm. Aka attack vector.

three-way handshake, TCP three-way handshake The three-packet process used by TCP to establish a connection between a client and a server.

thrill attack An attack launched by crackers/hackers with few true skills. The main motivation behind thrill attacks is the "high" of getting into a system.

throughput rate (1) The rate at which a biometric device can scan and authenticate subjects. A rate of about six seconds or faster is required for general acceptance of a specific biometric control. (2) The speed at which bits are transmitted over a network medium.

ticket An electronic authentication factor used by the Kerberos authentication system.

ticket-granting service (TGS) An element of the Kerberos authentication system. The TGS manages the assignment and expiration of tickets. Tickets are used by subjects to gain access to objects.

ticket-granting ticket (TGT) The primary authentication token used by Kerberos that is a hashed form of the subject's password with the addition of a timestamp that indicates a valid lifetime.

time of check (TOC) The time at which a subject checks on the status of an object.

time of check to time of use (TOCTOU, TOC2TOC, TOCTTOU, TOC/TOU) A timing vulnerability that occurs when a program checks access permissions too far in advance of a resource request. A type of exploitation in which attackers abuse the predictability and precision of task execution to cause a loophole in security filtering or authentication. *See also* race conditions.

time of use (TOU) The time at which the decision is made by a subject to access an object.

time offset The difference in time between a system's clock and a known time standard or between two different system clocks. Time offset is relevant when synchronizing log files.

time slice A single chunk or division of processing time.

time to live (TTL), time-to-live A field in an Internet Protocol (IPv4) packet that indicates how many routers the packet can cross (hops it can make) 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. *See* hop limit.

time-based one-time password (TOTP) Devices or applications that generate passwords at fixed time intervals, such as every 60 seconds. These one-time passwords are based on the timestamp, a key associated with the user, and the TOTP algorithm. A synchronous dynamic password token uses TOTP.

timeliness Being prompt, on time, within a reasonable time frame, or providing low-latency response, in relation to availability.

time-of-day restrictions Limitations on what time of day, and often what day of the week, a specific user account can log on to the network or a specific system can be accessed by users.

TKIP *See* Temporal Key Integrity Protocol (TKIP).

TLS *See* Transport Layer Security (TLS).

token A software or hardware element used to verify the identity of an entity or define the authorization for that entity.

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

token passing A LAN media access technology that performs communications using a digital token. Possession of the token allows a host to transmit data. Once its transmission is complete, it releases the token to the next system. Token passing was used by ring topology–based networks.

token ring A token-passing LAN technology.

tokenization A technique to mask or obfuscate data using tokens (i.e., unique identifying symbols/characters) to represent sensitive data. *See* pseudonymization and anonymization.

tolerance, risk tolerance *See also* risk tolerance and acceptance. *See* other related terms: acceptance, assignment, transfer, transference (as related to risk), avoidance, reducing risk, mitigation, rejecting risk, and ignoring risk.

top secret The highest level of government/military classification. Unauthorized disclosure of top-secret data will cause exceptionally grave damage to national security.

top-down approach Upper, or senior, management is responsible for initiating and defining policies for the organization.

top-level domain (TLD) The far-right portion of a FQDN. Examples include `.com`, `.org`, and `.net`.

topology The physical layout of network devices and connective cabling. The common network topologies are ring, bus, star, and mesh.

total risk The amount of risk an organization would face if no safeguards were implemented. A formula for total risk is threats * vulnerabilities * asset value = total risk.

TOTP *See* time-based one-time password (TOTP).

TPM *See* Trusted Platform Module (TPM).

`traceroute` A TCP/IP command-line utility on Mac, Linux, and Unix operating systems that shows the user every router interface a TCP/IP packet passes through on its way to a destination. On Mac, Linux, and Unix operating systems, the command is `traceroute`; on Windows operating systems, the command is `tracert`. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

`tracert` A truncated form of the `traceroute` command, used due to the Microsoft 8.3 filename convention. *See also* `traceroute`.

trade secret Intellectual property that is absolutely critical to a business and would cause significant damage if it were disclosed to competitors and/or the public.

trademark A registered word, slogan, or logo used to identify a company and its products or services.

traffic analysis A form of monitoring in which the flow of packets rather than the actual content of packets is examined. Also referred to as trend analysis.

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

training The task of teaching employees to perform their work tasks and to comply with the security policy. All new employees require some level of training so they will be able to properly comply with all standards, guidelines, and procedures mandated by the security policy.

transborder data flow The movement of data across country boundaries and/or between countries. Many countries implement laws and restrictions in regard to the movement of data across these boundaries.

transfer, transference (as related to risk) A form of risk management in which the risk is transferred or assigned to another entity through outsourcing or obtaining insurance. *See* other related terms: acceptance, risk tolerance, assignment, avoidance, reducing risk, mitigation, rejecting risk, and ignoring risk.

transferring risk The placement of the responsibility of loss due to a risk onto another entity or organization. Purchasing cybersecurity or traditional insurance and outsourcing are common forms of assigning or transferring risk. Aka assignment of risk, assigning risk, risk assignment, and transference of risk.

transformation procedures (TPs) In relation to the Clark–Wilson model, the only procedures that are allowed to modify a CDI. The limited access to constrained data items (CDIs) through TPs forms the backbone of the Clark–Wilson integrity model.

transient noise A short duration of line noise disturbance.

transit gateway A technology that establishes a simple and seamless integration of virtual private clouds (VPCs) and local systems through a central hub or cloud router.

transitive access A potential backdoor or way to work around traditional means of access control.

transitive trust, transitive authentication A security concern when a security blockade can be bypassed using a third party. The concept that if A trusts B and B trusts C, then A inherits trust of C through the transitive property, which works like it would in a mathematical equation: if A = B, and B = C, then A = C. Transitive trust is a serious security concern because it may enable bypassing of restrictions or limitations between A and C, especially if A and C both support interaction with B.

Transmission Control Protocol (TCP) A connection-oriented protocol located at layer 4 of the OSI model. This protocol breaks data packets into segments, numbers them, and sends them in random order. The receiving computer reassembles the data so that the information is readable by the user. In the process, the sender and the receiver confirm that all data has been received; if not, it's sent again.

Transmission Control Protocol (TCP) sequence attack An attack in which the attacker intercepts session communication packets 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.

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 Control Protocol/Internet Protocol (TCP/IP) hijacking An attack in which the attacker gains access to a host in the network and logically disconnects it from the network. The attacker then inserts another machine with the same IP address onto the network.

transmission error correction A capability built into connection- or session-oriented protocols and services. If it is determined that a message, in whole or in part, was corrupted, altered, or lost, a request can be made for the source to resend all or part of the message.

transmission logging A form of auditing focused on communications. Transmission logging records the details about source, destination, timestamps, identification codes, transmission status, number of packets, size of message, and so on.

transmission media The type of connectivity media employed in a network to support communications; it is important to the network's design, layout, and capabilities.

transmission window The number of packets transmitted before an acknowledge packet is sent.

transparency The characteristic of a service, security control, or access mechanism that ensures that it is unseen by users. Transparency is often a desirable feature for security controls. The more transparent a security mechanism is, the less likely a user will be able to circumvent it or even be aware that it exists.

transparent proxy A proxy that handles client traffic because routers direct the communications to the proxy without the client being configured to use the proxy specifically.

transponder proximity device A mechanism that is self-powered and transmits a signal received by the reader. This can occur consistently or only at the press of a button (like a garage door opener or car alarm key fob). Such devices may have batteries or capacitors, or may even be solar powered.

transport encryption A means to ensure the security of information while it's being transmitted between two endpoints.

Transport layer (layer 4 of the OSI) (1) The fourth layer of the OSI model. It's responsible for checking that data packets created in the Session layer are received error-free. If necessary, it also changes the length of messages for transport up or down the remaining layers. *See also* Open Systems Interconnection (OSI). (2) The alternate name for the third layer of the TCP/IP model, which was originally Host-to-Host.

Transport Layer Security (TLS) Based on SSL technology, TLS incorporated many security enhancements and was eventually adopted as a replacement for SSL in most applications. Early versions of TLS supported downgrading communications to SSL v3.0 when both parties did not support TLS. However, in 2011, TLS v1.2 dropped this backward compatibility. TLS uses TCP port 443.

transport mode One of two virtual private network (VPN) modes. Transport mode only encrypts the payload, leaving the header in plaintext. Aka end-to-end encryption tunnel, end-to-end encrypted VPN, and host-to-host VPN. *See also* tunnel mode.

transposition cipher Cipher that uses an encryption algorithm to rearrange the letters of a plaintext message to form the ciphertext message.

trap door Undocumented command sequence that allows software developers to bypass normal access restrictions.

trap message The SNMP communication from a monitored system back to the management console when an event or threshold violation occurs.

traverse mode noise Electromagnetic interference (EMI) noise generated by the difference in power between the hot and neutral wires of a power source or operating electrical equipment.

trend analysis *See* traffic analysis.

trend Changes that are recognized over time because each individual occurrence of a change is small or deemed inconsequential. Trends are discovered through historical analyses and long-term event and log tracking.

Trike A threat modeling methodology that focuses on a risk-based approach instead of depending on the aggregated threat model used in STRIDE and DREAD.

Triple Data Encryption Standard (3DES, Triple DES) A deprecated block cipher algorithm used for encryption.

Trivial File Transfer Protocol (TFTP) A protocol similar to FTP that doesn't provide the security or error-checking features of FTP. This is a network application that supports an exchange of files that does not require authentication. Used to host network device configuration files and can support multicasting. TFTP should not be used since it operates in cleartext. *See* File Transfer Protocol (FTP).

Trojan (previously Trojan horse) Any application that masquerades as something benign to get past scrutiny and then does something malicious. A malicious code object that appears to be a benevolent program, such as a game or simple utility that performs the "cover" functions as advertised but also carries an unknown payload, such as a virus. One of the major differences between Trojans and viruses is that Trojans tend not to replicate themselves.

true negative Benign events that should not/do not trigger an alarm/alert.

true positive Malicious events that trigger an alarm/alert.

trust (1) A security bridge established to share resources from one domain to another. A trust is established between two domains to allow users from one domain to access resources in another. Trusts can be one-way only, or they can be two-way. (2) A social-engineering technique based on an attacker working to develop a relationship with a victim.

trust but verify A more traditional security approach of trusting subjects and devices within the company's security perimeter (i.e., internal entities) automatically (as opposed to zero trust). This type of security approach leaves an organization vulnerable to insider attacks and grants intruders the ability to easily perform lateral movement among internal systems.

trust list A list of objects that have been signed by a trusted entity. Aka certificate trust list (CTL).

trust model A defined linking or pathway of trust. Examples include bridge, mesh, peer-to-peer, cross-bridge, cross-link, hierarchical, and one-way.

Trusted Automated Exchange of Intelligence Information (TAXII) A standardized set of communication services, protocols, and message exchanges to support the effective communication and exchange of cyber threat indicators. TAXII helps organizations exchange STIX information related to IoCs.

trusted computing base (TCB) The combination of hardware, software, and controls that forms a trusted base that enforces your security policy.

trusted operating system (OS) (1) An access control feature that requires a specific OS to be present to gain access to a resource. (2) Any OS that has security features in compliance with government and/or military security standards that enable the enforcement of multilevel security policies (that is, enforcing mandatory access control using classification labels on subjects and objects).

trusted path Secure channel used by the trusted computing base (TCB) to communicate with the rest of the system.

Trusted Platform Module (TPM) A specification for a cryptoprocessor as well as the chip in a mainboard supporting this function. A TPM chip is used to store and process cryptographic keys for the purposes of a hardware-supported/implemented hard drive encryption system.

trusted recovery process On a secured system, a process that ensures the system always returns to a secure state after an error, failure, or reboot.

trusted shell An execution environment that allows a subject to perform command-line operations without risk to the trusted computing base (TCB) or the subject. A trusted shell prevents the subject from being able to break out of isolation to affect the TCB and in turn prevents other processes from breaking into the shell to affect the subject.

trusted system A secured computer system.

trusted third party A separate entity trusted or relied on by first and second parties/entities. This theory states that if user A (a first party) trusts user C (the third party) and user B (a second party) trusts user C (the third party), then user A can trust B, and vice versa. With certificates, the trusted third party is a certificate authority (CA).

truthfulness Being a true reflection of reality in relation to integrity.

`try...catch` statement A programming or coding functionality that allows developers to explicitly specify how errors should be handled. In this approach, the developer writes code that may cause an error and includes it in a `try` clause. When the code executes, if it does cause an error, the `catch` clause specifies how the application should handle that error situation.

TTL *See* time to live (TTL).

tunnel A communication pathway across an intermediary (often untrusted) network crafted by a virtual private network (VPN) protocol.

tunnel mode One of two virtual private network (VPN) modes. Tunnel mode encrypts the original header and payload and then adds a link or tunnel header to guide the message to the other end of the tunnel. Aka link encryption VPN and link encrypted VPN. *See also* transport mode and remote access VPN.

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

tunneling protocols Virtual private network (VPN) protocols, but with an emphasis on the tunneling or encapsulation aspect of the technology.

tuple (1) A record or row in a database. (2) A collection of related data items.

turnstile A form of gate that prevents more than one person at a time from gaining entry and often restricts movement in one direction.

twisted pair cable, twisted-pair cabling A form of cable commonly used in network applications. It's named after its twisting of pairs of conductors within the cable itself. Standard networking cable has eight wires or four pairs. *See also* unshielded twisted pair (UTP) or shielded twisted pair (STP) (if shielded). *See* 10BaseT.

two-factor authentication (TFA) A process that uses two factors as a part of authentication. *See* multifactor authentication (MFA).

Twofish A block cipher algorithm developed by Bruce Schneier (also the creator of Blowfish). It operates on 128-bit blocks of data and is capable of using cryptographic keys up to 256 bits in length.

Type 1 authentication factor Something you know, such as a password, personal identification number (PIN), combination lock, passphrase, mother's maiden name, or favorite color.

Type 1 error, type I error *See* false rejection rate (FRR).

type 1 hypervisor A native or bare-metal hypervisor. In this configuration, there is no host operating system (OS); instead, the hypervisor installs directly onto the hardware where the host OS would normally reside.

Type 2 authentication factor Something you have, such as a smartcard, ATM card, token device, or memory card.

Type 2 error, Type II error *See* false acceptance rate (FAR).

type 2 hypervisor A hosted hypervisor. In this configuration, a standard regular operating system (OS) is present on the hardware, and then the hypervisor is installed as another software application.

Type 3 authentication factor Something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, or hand geometry.

Type I hypervisor A native or bare-metal hypervisor. In this configuration, there is no host OS; instead, the hypervisor installs directly onto the hardware where the host OS would normally reside.

Type II hypervisor A hosted hypervisor. In this configuration, a standard regular OS is present on the hardware, and then the hypervisor is installed as another software application.

typosquatting, typo squatting A practice employed to capture traffic when a user mistypes the domain name or Internet Protocol (IP) address of an intended resource. A squatter predicts URL typos and then registers those domain names to direct traffic to their own site. This can be done for competition or for malicious intent. Aka URL hijacking.

U

UDP *See* User Datagram Protocol (UDP).

UEFI *See* Unified Extensible Firmware Interface (UEFI).

UltraViolet EPROMs (UVEPROMs) A type of EPROM that can be erased using an ultraviolet light.

unannounced test A security evaluation in which only senior management is aware of the penetration test taking place.

unauthenticated cryptography mode A means to implement symmetric encryption sessions to ensure confidentiality but not authenticity of the transmitted data. Examples include cipher feedback (CFB) and output feedback (OFB). Some even earlier modes did not include integrity either, such as Electronic Code Book (ECB) and cipher block chaining (CBC). *See* authenticated cryptography mode.

unauthenticated scan A form of vulnerability scan that tests the target systems without having passwords or other special information that would grant the scanner special privileges. This allows the scan to run from the perspective of an attacker but also limits the ability of the scanner to fully evaluate possible vulnerabilities.

unauthorized entity A name to describe a criminal hacker. *See also* hacker, cracker, or phreaker.

unclassified The lowest level of government/military classification. Used for data that is neither sensitive nor classified. Disclosure of unclassified data does not compromise confidentiality, and it doesn't cause any noticeable damage.

unconstrained data item (UDI) In relation to the Clark–Wilson model, any data item that is not controlled by the security model. Any data that is to be input and hasn't been validated, or any output, would be considered an unconstrained data item.

uncrewed aerial vehicle (UAV) An automated or remote-controlled flying device that can be used to perform reconnaissance to both gather visual information and pick up radio wave signals. Aka drone.

underflow This error happens when the write buffer of the drive empties during the writing process, which causes an error on the media, rendering it useless.

unicast A communications transmission to a single identified recipient.

unified endpoint management (UEM) A type of software tool that provides a single management platform to control mobile, PC, IoT, wearables, ICS, and other devices. It replaces mobile device management (MDM) and enterprise mobility management (EMM) products.

Unified Extensible Firmware Interface (UEFI) A replacement or improvement to the basic input/output system (BIOS) that provides support for all of the same functions as BIOS with many improvements, such as support for larger hard drives (especially for booting), faster boot times, enhanced security features, and even the ability to use a mouse when making system changes (BIOS was limited to keyboard control only). *See* measured boot.

Unified Threat Management (UTM) An all-in-one security appliance designed to operate inline between an internet connection and a network. Its goal is to detect and filter all manner of malicious, wasteful, or otherwise unwanted traffic. UTMs are implemented to perform firewall, intrusion detection system (IDS), intrusion protection system (IPS), and network address translation (NAT) functions, and to provide denial-of-service (DoS) protection, spam filtering, virus scanning, privacy protection, web filtering, spyware blocking, and activity tracking. *See* next-generation firewall (NGFW).

Uniform Computer Information Transactions Act (UCITA) A federal law designed for adoption by each of the 50 states to provide a common framework for the conduct of computer-related business transactions.

uniform resource locator (URL) A means of identifying a document on the internet. It consists of the protocol used to access the document and the domain name or Internet Protocol (IP) address of the host that holds the document; for example, `http://www.sybex.com`.

uninterruptible power supply (UPS) A type of self-charging battery that can be used to supply consistent clean power to sensitive equipment. A UPS functions by taking power in from the wall outlet, storing it in a battery, pulling power out of the battery, and then feeding that power to whatever devices are connected to it. By directing current through its battery, it is able to maintain a consistent clean power supply. Two main types are double conversion UPS and line-interactive UPS.

unit testing A method of testing software. Each unit of code is tested independently to discover any errors or omissions and to ensure that it functions properly. Unit testing should be performed by the development staff.

Universal Serial Bus (USB) A standard for connecting peripheral devices and primary computers over a wired link. There are a range of specifications and adapter/connection variations.

unknown environment A device of unknown composition whose internal circuits, makeup, and processing functions are unknown but whose outputs in response to various kinds of inputs can be observed and analyzed. Unknown environment penetration testing proceeds without using any knowledge of how an organization is structured, what kinds of hardware and software it uses, or its security policies, processes, and procedures.

unknown environment testing A form of program testing that examines the input and output of a program without focusing on its internal logical structures.

unshielded twisted-pair (UTP) A twisted-pair wire that does not include additional electromagnetic interference (EMI) protection. Most twisted-pair wiring is UTP.

unsupervised learning A type of machine learning training/programming technique that uses unlabeled data for training. The dataset provided to the algorithm does not contain the "correct" answers; instead, the algorithm is asked to develop a model independently.

upper management *See* senior management/senior manager.

urgency A social-engineering technique based on the concept that the need to act quickly increases as scarcity indicates a greater risk of missing out.

URL *See* uniform resource locator (URL).

URL filtering The process of filtering network traffic based on all or part of the URL used to request access to a resource. A form of content filtering. Aka web filtering.

URL hijacking (1) *See* typosquatting. (2) The practice of displaying a link or advertisement that looks like that of a well-known product, service, or site, but when clicked redirects the user to an alternate location, service, or product. This may be accomplished by posting sites and pages and exploiting search engine optimization (SEO), or through the use of adware that replaces legitimate ads and links with those leading to alternate or malicious locations.

URL redirection A means to make a web page available through multiple URL addresses or domain names. Aka URL forwarding.

USA Patriot Act of 2001 An act implemented after the September 11, 2001, terrorist attacks. It greatly broadened the powers of law enforcement organizations and intelligence agencies across a number of areas, including the monitoring of electronic communications.

usability The state of being easy to use or learn or being able to be understood and controlled by a subject, in relation to availability.

USB data blocker An adapter that blocks the data channels of a USB device from connecting with a PC.

USB encryption The encryption of a Universal Serial Bus (USB) storage device, either a USB thumbdrive or a USB-attached hard drive or solid-state drive (SSD).

USB On-the-Go (OTG) A specification that allows mobile devices with a Universal Serial Bus (USB) port to act as a host and use other standard peripheral USB equipment, such as storage devices, mice, keyboards, and digital cameras.

use case testing, use cases A form of software testing where the developer checks how the product handles normal and valid input data with an aim at mirroring normal activity.

USENET A worldwide-distributed messaging and discussion platform supported by Network News Transfer Protocol (NNTP), which preceded the web.

user acceptance testing (UAT) A form of dynamic analysis that evaluates whether a typical end user will be able to work with the new software with minimal issues.

user account The most common type of account in a typical network, since everyone is assigned a user account if they have computer and network privileges. A user account is limited because this type of account is to be used for regular, normal daily operation tasks. Aka standard account, limited account, regular account, or even a normal account.

user and entity behavior analysis (UEBA), user and entity behavior analytics The *E* in UEBA extends the UBA concept to include entity activities that take place but that are not necessarily directly linked or tied to a user's specific actions, but that can still correlate to a vulnerability, reconnaissance, intrusion, breach, or exploit occurrence. Information collected from UBA/UEBA monitoring can be used to improve personnel security policies, procedures, training, and related security oversight programs.

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

user awareness The process of training all employees in regard to standard, common, and foundational security topics.

user behavior analytics (UBA) The concept of analyzing the behavior of users, subjects, visitors, customers, and so forth for some specific goal or purpose. *See* user and entity behavior analysis (UEBA). Aka user behavior analysis (UBA).

user certificate A type of certificate that is used to verify a specific individual.

User Datagram Protocol (UDP) A connectionless protocol located at layer 4 of the OSI model.

user mode The basic mode used by the CPU when executing user applications.

user-assigned privileges Those permissions that are granted or denied on a specific individual user basis.

username The most common form of identification. It's any name used by a subject to be recognized as a valid user of a system.

UTP *See* unshielded twisted pair (UTP).

V

validity Being factually or logically sound in relation to integrity.

Van Eck phreaking Eavesdropping, intercepting, or listening in on the electromagnetic emanations that electronic devices produce.

Van Eck radiation The electromagnetic emanations that electronic devices produce.

variable length subnet masking (VLSM) A flexible system of grouping and subdividing IPv4 subnets. *See* Classless Inter-Domain Routing (CIDR).

VAST (Visual, Agile, and Simple Threat) A threat modeling concept based on Agile project management and programming principles.

vault A permanent safe or strongroom that is integrated into a building's construction. *See* safe.

vein recognition A biometric that measures the unique vein pattern through the use of near-infrared light to "see" through the skin. Aka vascular biometrics.

vendor management system (VMS) A software solution that assists with the management and procurement of staffing services, hardware, software, and other needed products and services. A VMS can offer ordering convenience, order distribution, order training, consolidated billing, and more.

VENONA One of the major intelligence successes of the United States resulted when cryptanalysts broke a top-secret Soviet cryptosystem, i.e., VENONA, that relied on the use of onetime pads.

Vernam cipher A device that implements a 26-character modulo 26 substitution cipher. It functions as a onetime pad.

version control The management of the progress of changes in software code, which often allows for rollback of code to earlier versions when required.

video monitoring The process of using video cameras to record events. Aka video surveillance.

view A client interface used to interact with a database. The view limits what clients can see and what functions they can perform.

Vigenère cipher A polyalphabetic substitution cipher.

violation analysis A form of auditing that uses clipping levels.

virtual application A software product deployed in such a way that it is fooled into believing it is interacting with a full host OS. A virtual (or virtualized) application has been packaged or encapsulated so that it can execute but operate without full access to the host OS or platform. Aka guest application and virtual software.

virtual circuit A logical pathway or circuit created over a packet-switched network between two specific endpoints. Aka a communication path. *See* permanent virtual circuit (PVC) and switched virtual circuits (SVC).

virtual desktop (1) A remote access tool that grants the user access to a distant computer system by allowing remote viewing and control of the distant desktop's display, keyboard, mouse, and so on. (2) An extension of the virtual application concept encapsulating multiple applications and some form of "desktop" or shell for portability or cross-OS operation. This technology offers some of the features/benefits/applications of one platform to users of another without the need for using multiple computers, dual-booting, or virtualizing an entire OS platform. (3) An extended or expanded desktop larger than the display being used allows the user to employ multiple application layouts, switching between them using keystrokes or mouse movements.

virtual desktop infrastructure (VDI) A means to reduce the security risk and performance requirements of end devices by hosting virtual machines on central servers that are remotely accessed by users. A VDI provides users with a desktop hosted on a server. Users can typically access the desktop from any device including desktop computers and mobile devices. Virtual desktops can be persistent (meaning that they retain changes made by the user) or nonpersistent (meaning that the desktop reverts to its original state after the user logs off). It is sometimes called a virtual desktop environment (VDE).

Virtual Extensible LAN (VXLAN) An encapsulation protocol that enables VLANs to be stretched across subnets and geographic distances. VLANs are typically restricted to layer 2 network areas and are not able to include members from other networks that are accessible only through a router portal. Additionally, VXLAN allows for up to 16 million virtual networks to be created, whereas traditional VLANs are limited to only 4,096. VXLAN can be used as a means to implement microsegmentation without limiting segments to local entities only. VXLAN is defined in RFC 7348.

virtual firewall A firewall created for use in a virtualized or hypervisor environment or the cloud. A virtual firewall is a software re-creation of an appliance firewall or a standard host-based firewall installed into a guest OS in a VM.

virtual IP, virtual IP address A mechanism used by load balancers to present a single IP to users/visitors, but the IP address is not actually assigned to a specific system. Instead, as communications are received at the IP address, they are distributed in a load-balancing schedule to the actual systems operating on some other set of IP addresses.

virtual LAN (VLAN), virtual local area network A logical network segmentation implemented on switches and bridges to manage traffic. Multiple VLANs can be hosted on the same switch but are isolated as if they are separate physical networks. Only through a routing function, often provided by a multilayer switch, can cross-VLAN communications occur.

virtual machine (VM) A software simulation of a computer within which a process executes. Each virtual machine has its own memory address space, and communication between virtual machines is securely controlled.

virtual memory A special type of secondary memory that is managed by the operating system in such a manner that it appears to be real memory.

virtual mobile infrastructure (VMI) A virtualization system for mobile devices where the operating system of a mobile device is virtualized on a central server. Similar to VDI.

virtual network segmentation Customized segmentation mechanisms used in relation to virtual machines to make guest OSs members of the same network division as that of the host, or guest OSs can be placed into alternate network divisions. A virtual machine can be made a member of a different network segment from that of the host or placed into a network that only exists virtually and does not relate to the physical network media. *See* software-defined network (SDN).

virtual private cloud (VPC) A feature of some cloud service providers (CSPs) where customers can initiate or provision an isolated section of their cloud resources and then create/control the virtual network related to the isolated resource set.

virtual private cloud (VPC) endpoint A VM, VDI, or VMI instance that serves as a virtual endpoint for accessing cloud assets and services.

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

virtual reality (VR) A computer simulation that fully encloses the viewer in an artificial environment that can be similar to or completely different from reality.

virtual SAN A virtual storage area network (SAN) or a software-defined shared storage system is a virtual re-creation of a SAN on top of a virtualized network or a software-defined network (SDN).

virtual tape libraries (VTL) A backup technology that supports the use of disks by using software to make disk storage appear as tapes to backup software.

virtualization A technology used to host one or more operating systems within the memory of a single host computer. This mechanism allows practically any operating system to operate on any hardware. Aka virtualization technology.

virus A program intended to damage a computer system. Often, sophisticated viruses are encrypted; they hide in a computer and may not appear until the user performs a certain action or until a certain date. Once they are in a system, they attach themselves to legitimate operating system and user files and applications and normally perform some sort of undesirable action, ranging from the somewhat innocuous display of an annoying message on the screen to the more malicious destruction of the entire local filesystem.

virus decryption routine In an encrypted virus, a short segment of code that contains the cryptographic information necessary to load and decrypt the main virus code stored elsewhere on the disk.

virus hoax *See* hoax.

vishing A form of phishing that uses Voice over IP (VoIP) to trick users. It will often spoof the caller's actual phone number by fooling the caller ID system.

visitor logs A manual or automated list of nonemployee entries or access to a facility or location.

Visual Basic for Applications (VBA) Microsoft's Visual Basic for Applications 7 programming language is integrated into Microsoft Office applications, such as Word, Excel, and PowerPoint. It is casually referred to as Visual Basic. It is the primary language that Office macros are written in.

VLAN (virtual local area network) *See* virtual LAN (VLAN).

VLAN hopping The ability to make network traffic jump between VLANs through an abuse of IEEE 802.1Q VLAN tagging known as double encapsulation.

VLAN management The use of VLANs to control traffic for security or performance reasons. VLANs can be used to isolate traffic between network segments. This can be accomplished by not defining a route between different VLANs or by specifying a deny filter between certain VLANs (or certain members of a VLAN).

VM escaping When software within a guest operating system (OS) is able to breach the isolation protection provided by the hypervisor to violate the container of other guest OSs or to infiltrate a host OS.

VM sprawl An organization's deployment of numerous virtual machines without an overarching IT management or security plan in place.

Voice over IP (VoIP) A network service that provides voice communication services by transporting the voice traffic as network packets over an IP network.

voice pattern An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The speech, tone, modulation, and pitch patterns of a person's voice are used to establish identity or provide authentication.

voice recognition A biometric device that analyzes the characteristics of a person's speaking voice. Aka voiceprint or voice pattern.

VoIP *See* Voice over IP (VoIP).

volatile *See* volatile storage.

volatile storage A storage medium, such as RAM, that loses its contents when power is removed from the resource.

voluntary surrender, voluntarily surrender The act of willingly handing over evidence.

VPN *See* virtual private network (VPN).

VPN concentrator A dedicated hardware device designed to support a large number of simultaneous virtual private network (VPN) connections, often hundreds to thousands. Aka VPN server, a VPN gateway, a VPN firewall, a VPN remote access server (RAS), a VPN device, a VPN proxy, or a VPN appliance.

vulnerability A weakness in an environment or an object that may be the target of an attack by a hacker or cause an accident. It can be due to the existence of a flaw, loophole, oversight, error, limitation, frailty, or susceptibility in the IT infrastructure or any other aspect of an organization. It can also be the result of the absence of a safeguard or countermeasure or a weakness in a protection measure.

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

vulnerability databases Indexes and repositories of information about threats, exploits, and attacks. The two dominant examples are the Common Vulnerabilities and Exposures (CVE) hosted at `cve.mitre.org` and the National Vulnerability Database (NVD) hosted at `nvd.nist.gov`. Aka vulnerability feeds and threat feeds.

vulnerability management A program used to detect weaknesses within an organization. Vulnerability scans and vulnerability assessments are two common elements of a vulnerability management program. Vulnerability scans are technical scans performed regularly, and vulnerability assessments are normally combined with a risk assessment.

vulnerability scan, vulnerability scanner, vulnerability scanning A test performed on a system to find known holes, weaknesses, or vulnerabilities in the security infrastructure. Vulnerability scans automatically probe systems, applications, and networks looking for weaknesses that may be exploited by an attacker. The scanning tools used in these tests provide quick point-and-click tests that perform otherwise tedious tasks without requiring manual intervention.

W

wait state, waiting state The state in which a process is ready to execute but is waiting for an operation such as keyboard input, printing, or file writing to complete.

walkthrough, walk-through, walk through An exercise that focuses on helping each computer incident response team (CIRT) member learn and understand their individual responsibilities.

walled garden A separate network from that of the internet itself. Many walled gardens grant easy access to their content, but you have to access it through their own portal.

WAN *See* wide area network (WAN).

WAP *See* wireless access point (WAP).

war chalking A type of geek graffiti that some wireless hackers used during the early years of wireless (1997–2002). It's a way to physically mark an area with information about the presence of a wireless network.

war dialing The act of using a modem to dial all the PSTN (public switched telephone network) numbers in an area code or a prefix to find other modems that answer the incoming call.

war driving The act of searching for wireless networks using any of a variety of wireless-detection tools, from handheld scanners to notebook computers. Originally named after the method of driving around office buildings looking for open access points.

war flying War flying is the use of remote control airplanes, helicopters, rockets, drones, or uncrewed aerial vehicles (UAVs) for the purposes of detecting radio waves.

warm site A middle ground between hot sites and cold sites for disaster recovery specialists. A warm site always contains the equipment and data circuits necessary to rapidly establish operations but does not typically contain copies of the client's data.

warning banners Messages used to inform would-be intruders or attempted security policy violators that their intended activities are restricted and that any further activities will be audited and monitored. A warning banner is basically an electronic equivalent of a no-trespassing sign.

waterfall model A software development life cycle (SDLC) model that consists of seven stages, or steps: 1) system requirements, 2) software requirements, 3) preliminary design, 4) detailed design, 5) code and debug, 6) testing, and 7) operations and maintenance.

watering hole attack A form of targeted attack against a region, a group, or an organization. The attack is performed by focusing on a common resource, site, or location that one or more members of the target frequent.

watermarking The process of digital watermarking hides information within a file that is known only to the file's creator. If someone later creates an unauthorized copy of the content, the watermark can be used to detect the copy and (if uniquely watermarked files are provided to each original recipient) trace the offending copy back to the source.

weak key attack An attack that looks for cipher holes.

wearables An offshoot of smart devices and Internet of Things (IoT) devices that are specifically designed to be worn by an individual. Aka wearable technology.

web application firewall (WAF) An appliance, server add-on, virtual service, or system filter that defines a strict set of communication rules for a website. It's intended to prevent web application attacks and exploitation. A WAF is an example of an application-level firewall.

wave pattern motion detector A device that transmits a consistent low ultrasonic or high microwave frequency signal into a monitored area and monitors for significant or meaningful changes or disturbances in the reflected pattern.

web bot Agents that continuously crawl a variety of websites retrieving and processing data on behalf of the user.

web security gateway (WSG) A web content filter (often URL- and content keyword–based) that also supports malware scanning. In most cases, a web security gateway is implemented by an organization to provide better policy enforcement over employee web activity. *See* web application firewall (WAF).

web server A server that holds and delivers web pages and other web content using HTTP and/or HTTPS. *See also* Hypertext Transfer Protocol (HTTP).

web shell An attack that allows the attacker to execute commands on the server and view the results in the browser. A web shell may be injected code or may be accessing the native command prompt or shell mechanism of the target OS. This approach provides the attacker with access to the server over commonly used HTTP and HTTPS ports, making their traffic less vulnerable to detection by security tools.

web vulnerability scanning *See* vulnerability scan.

webcasting A form of media distribution occurring over the internet (in contrast to more traditional means such as over-the-air or cable TV broadcasts and radio stations). Can also include and is related to videocasting, audiocasting, podcasting, netcasting, internet television, and IP TV.

well-known ports The first 1,024 ports of TCP and UDP. They are usually assigned to commonly used services and applications. Aka service ports.

WEP *See* Wired Equivalent Privacy (WEP).

wet pipe system A fire suppression system that is always full of water. Water discharges immediately when triggered by a fire or smoke. Aka a closed head system.

whaling A form of phishing that targets specific individuals (by title, by industry, from media coverage, and so forth) and sends messages tailored to the needs and interests of those individuals.

white box (1) This term is deprecated. *See* known environment. (2) Device used to control and manipulate the PSTN phone system. A white box is a dual-tone multifrequency (DTMF) generator (that is, a keypad).

white hat This term is deprecated. *See* authorized entity.

white noise The activity of broadcasting false traffic at all times to mask and hide the presence of real emanations.

white team The group defined as the referees in a penetration test or security assessment exercise. They establish the rules of engagement (RoE), other guidelines, and boundaries of the security evaluation. They oversee the event and ensure that both sides of the simulated conflict/breach/intrusion are operating by the rules. *See* red team, blue team, and purple team.

whitelist This term has been deprecated. *See* allow list.

whole-disk encryption (WDE) A storage security mechanism that encrypts all of the data on a storage device with a single master symmetric encryption key. Aka full-disk encryption (FDE).

wide area network (WAN) A network or a network of LANs that is geographically diverse. Often dedicated leased lines are used to establish connections between distant components. A network that crosses local, regional, and/or international boundaries.

Wi-Fi analyzer A network sniffer that is designed to interpret the radio signals of wireless networks in addition to evaluating the contents of headers and payloads of frames, packets, etc.

Wi-Fi Direct The name for the wireless topology of ad hoc or peer-to-peer connections. It is a means for wireless devices to connect directly to each other without the need for an intermediary mbase station.

Wi-Fi Protected Access (WPA) An early alternative to WEP was Wi-Fi Protected Access (WPA), which was based on a secret passphrase and employed the LEAP and TKIP cryptosystems. WPA uses the RC4 algorithm and employs the Temporal Key Integrity Protocol (TKIP) or the Cisco alternative Lightweight Extensible Authentication Protocol (LEAP). However, it is no longer secure enough to use. It is attackable through passphrase guessing and encryption key compromise/discovery. WPA can be deployed using authentication in personal mode with a preshared key authentication or in enterprise mode using 802.1X to use existing network authentication.

Wi-Fi Protected Access 2 (WPA2) A revision of WPA that upgraded the encryption to an Advanced Encryption Standard (AES) variant known as Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). WPA2 supports two authentication options: preshared key (PSK) or personal (PER) and IEEE 802.1X or enterprise (ENT). Aka IEEE 802.11i.

Wi-Fi Protected Access 3 (WPA3) The replacement or upgrade of wireless authentication and encryption of WPA2. WPA3-ENT uses 192-bit AES CCMP encryption. WPA3-PER replaces the preshared key authentication with Simultaneous Authentication of Equals (SAE). WPA3 also implements IEEE 802.11w-2009 management frame protection so that a majority of network management operations have confidentiality, integrity, authentication of source, and replay protection.

Wi-Fi Protected Setup (WPS) A wireless technology intended to simplify the effort involved in adding new clients to a secured wireless network. It operates by autoconnecting the first new wireless client to seek the network once WPS is triggered. WPS can be initiated by a button on the WAP or a code or PIN that can be sent to the base station remotely. This can allow for a brute-force guessing attack to discover the WPS code in less than six hours.

wildcard certificate A form of certificate that provides validation for all subdomains under a registered domain. *See* common name (CN).

WiMax (802.16) A wireless standard that defines citywide wireless access technologies. This standard has yet to be widely deployed.

window of vulnerability The necessary delay between the discovery of a new type of malicious code and the issuance of patches and antivirus updates.

WinHex A GUI Windows utility that can edit hex information located anywhere (i.e., in-a-file, not-in-a-file, orphaned data, bad sector data, slack space, unpartitioned space, etc.) on a storage device. This tool can be useful in inspecting unknown file types, recovering data from corrupted files, extracting evidence from damaged files, and repairing drive management elements (such as the MBR or directory table).

wiping The act of removing data from a storage device. Often the intention is to prevent data remnants from being recovered and thus leading to data leakage.

Wired Equivalent Privacy (WEP) A security protocol for wireless networks defined by the IEEE 802.11 that uses the RC4 algorithm. WEP was cracked almost as soon as it was released. Today, it's possible to crack WEP in less than a minute, thus rendering it worthless.

wired extension mode A wireless network configuration where the wireless access point acts as a connection point to link the wireless clients to the wired network. Aka wired extension mode infrastructure.

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

wireless cell An area within a physical environment where a wireless device can connect to a wireless access point (WAP).

wireless channels *See* channels.

wireless controller A separate external centralized management console used to control thin access points.

wireless local area network (WLAN) A local area network (LAN) that employs wireless access points (WAPs) and clients using any of various 802.11 standards, including 802.11b, 802.11a, and 802.11g.

wireless networking (802.11) A form of networking that uses radio waves as the connection medium following the 802.11 standard. Often called Wi-Fi.

wireless positioning system (WiPS), Wi-Fi positioning system (WFPS) A location service based on the geographic location of WAPs. Aka indoor wireless positioning system (IWPS).

wireless scanner A device used to detect the presence of a wireless network. Any active wireless network that is not enclosed in a Faraday cage can be detected, since the base station will be transmitting radio waves, even those with SSID broadcast disabled.

Wireless Transport Layer Security (WTLS) The security layer of the Wireless Applications Protocol (WAP) used by early smartphones to support internet connectivity over limited bandwidth and device capabilities. But WAP and WTLS were no longer necessary as mobile devices supported true protocol stacks just like PCs.

wireless wide area network (WWAN) A wide area network (WAN) based on wireless technologies.

Wireshark A free-to-use GUI protocol analyzer/sniffer. It is available for Windows, macOS, Linux, and Unix. It can be used to capture packets on any available interface. It has robust capture and display filter expression capabilities, it can preserve captures into a file, it can import captures from other tools, and it can follow TCP sessions.

wiring closet The room where the networking cables for a whole building or just a floor are connected to other essential equipment, such as patch panels, switches, routers, LAN extenders, backbone channels, and so on. More technical names include premises wire distribution room, main distribution frame (MDF), intermediate distribution frame (IDF), telecommunications room, and intermediate distribution facilities.

witness Someone who experienced an event or incident through one or more of their five senses. A witness can provide information about what occurred, where the occurrence took place, and the chronological order of related events.

WLAN *See* wireless local area network (WLAN).

work function, work factor A way of measuring the strength of a cryptography system by measuring the effort in terms of cost and/or time. Usually, the time and effort required to perform a complete brute-force attack against an encryption system is what the work function rating represents. The security and protection offered by a cryptosystem is directly proportional to the value of the work function/factor.

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

workstation A computer that isn't a server but that is on a network. Generally, a workstation is used to do work, whereas a server is used to store data or perform a network function. Aka client, terminal, end-user computer, or endpoint device.

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

WPA *See* Wi-Fi Protected Access (WPA).

WPA2 *See* Wi-Fi Protected Access 2 (WPA2).

WPA3 *See* Wi-Fi Protected Access 3 (WPA3).

wrapper Something used to enclose or contain something else. Wrappers are well known in the security community in relation to Trojan horse malware. A wrapper of this sort is used to combine a benign host with a malicious payload. Wrappers are also used as encapsulation solutions. Some static environments may be configured to reject updates, changes, or software installations unless they're introduced through a controlled channel or wrapper.

write blocker Hardware adapters that physically sever the portion of the cable used to connect the storage device that would write data to the device, reducing the likelihood of accidental tampering with the device. A software write blocker is a common feature of most data duplication products, but it is not as reliable as a hardware write blocker.

WTLS *See* Wireless Transport Layer Security (WTLS).

WWAN *See* wireless wide area network (WWAN).

X

X Window A GUI API for command-line operating systems.

X.25 An older WAN protocol that uses carrier switching to provide end-to-end connections over a shared network medium.

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

X.509 V3 The official certificate standard used by most public and private certificate authorities (CAs).

XCCDF *See* Extensible Configuration Checklist Description Format (XCCDF).

Xmas attack, Xmas scan A form of port scanning that can be performed by a wide number of common port scanners, including Nmap, Xprobe, and hping. The Xmas scan sends a Transmission Control Protocol (TCP) packet to a target port with the URG, PSH, and FIN flags all turned on. This creates a flag byte in the TCP header of 00101001, which is claimed to represent alternating lights flashing on a Christmas tree.

XML injection A variant of SQL injection, in which the back-end target is an XML application. Aka XML injection attack.

XML *See* Extensible Markup Language (XML).

XOR (exclusive OR) A Boolean function that returns a true value when only one of the input values is true. If both values are false or both values are true, the output of the XOR function is false.

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

XSS *See* cross-site scripting (XSS).

Y

yagi antenna A type of unidirectional wireless antenna. It is similar in structure to a traditional roof TV antenna; it's crafted from a straight bar with cross-sections to catch specific radio frequencies in the direction of the main bar.

Z

Zephyr analysis chart An analysis and evaluation chart that presents the relative strengths and weaknesses of various characteristics of biometric factor options.

zero trust The security concept that nothing should be trusted automatically or by default. Instead, the stance should be deny by default, grant by explicit exception.

zero-day attack *See* zero-day exploit.

zero-day exploit A newly discovered attack that was previously unknown or undisclosed to the world in general. Also implies that a direct or specific defense to the attack does not yet exist (i.e., a patch from a vendor); thus, most systems with the targeted vulnerable asset are at risk.

zeroize, zeroization A hard drive sanitation technique that writes a binary zero to every bit position on the storage device.

zero-knowledge proof A concept of communication whereby a specific type of information is exchanged but no real data is exchanged. Good examples of this idea are digital signatures and digital certificates.

zero-knowledge teams These possess only primary information about an organization during a security assessment or penetration test.

Zigbee An IoT equipment communication's concept that is based on Bluetooth. Zigbee has low power consumption, has a low throughput rate, and requires close proximity of devices.

zombie A system compromised by a botnet agent that is mindlessly performing actions under the remote control of a remote attacker. *See* bot.

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

zone file In the Domain Name System (DNS), the collection of resource records or details about the specific domain.

zone transfer A DNS communication between DNS servers that transfers all or part of a domain's zone file that typically occurs over TCP and is initiated on port 53.

zzuf A software testing tool that automates the process of mutation fuzzing by manipulating input according to user specifications.