802.1x - An authentication protocol used for network access control. One implementation is the WPA-Enterprise mode on Wi-Fi networks

AAA - Authentication, Authorization, and Accounting. A three-step security framework that comprises verification of a user's identity, specification of the exact resources that user is allowed to access, and tracking that user's actions for later review.

ABAC - Attribute-based access control defines access control policies based on the security attributes of users, resources, and environmental variables.

account expiration - Policies that automatically disable or delete accounts after a set period, either absolute or since the last login.

ACL - Access control list. A list attached to a resource, giving permissions, or rules, about exactly who can access it.

Active Directory - A Microsoft directory service based on LDAP and Kerberos, used by Windows domains.

AES - Advanced Encryption Standard. A strong and widely used encryption standard, supporting 128, 192, and 156-bit key lengths.

AES-CCMP - The strongest available Wi-Fi encryption, supported by WPA2 and most WPA dev ices.

ALE - Annual loss expectancy. In quantitative risk assessment, the cost per year you can expect from a given threat, or the SLE x ARO.

algorithm - A well-defined set of instructions to perform a self-contained task, such as encryption or decryption of data.

allow list - A list of items (e.g., email addresses or domain names) that are granted access to a certain system or protocol. When used, all entities are denied access except those included in the whitelist.

ARO - Annual rate of occurrence. In quantitative risk assessment, the number of times you can expect a given type of loss to occur per year.

ARP - Address Resolution Protocol. Used to identify the physical (MAC) address of a given IP address.

ARP poisoning - A spoofing attack that targets the Layer 2 Address Resolution Protocol.

attack surface - The summary of all points in a host or network that an attacker can target.

attack vector - (Also known as threat vector.) The mechanism of a given threat to an asset. Examples include malware, fraudulent email messages, and password cracking attempts.

auditing - The formal process of reviewing key elements of your network infrastructure. Commonly includes examination of security logs, incident response reports, user/administrator activity logs, user permissions, device configurations, and software installations.

AUP - Acceptable use policy. Specifies how authorized users are allowed to utilize system resources, such as hardware, software, and network services.

authentication - A process that ensures and confirms a user's identity using credentials supplied by the user.

authentication factor - Any element of the authentication process that serves to prove your identity. Common authentication factors include passwords, fingerprints, and smart cards.

authorization - Specifying the exact resources a given authenticated user is allowed to access.

availability - Ensuring that information is always easily accessible to authorized users. This includes preventing data loss and preserving connectivity, performance, and usability.

backdoor - Any hidden way into a system or application that bypasses normal authentication systems.

banner grabbing - Using routine communications with a host to gain information about its running services and open ports.

baseline - A minimum set of defined security standards.

bastion host - A host that's directly exposed to an untrusted network, and hardened against network attacks.

big data - Data sets too large to be handled by traditional data processing applications, but commonly seen in scientific data collection, internet search and tracking data, and business/finance. It requires specialized tools to analyze and secure.

biometrics - Personal physical characteristics, such as fingerprints and retinal patterns, used as inherence elements in the authentication process.

BitLocker - In cryptography, the result of encryption performed on plaintext using an algorithm, called a cipher. Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer.

block list - A permissions list containing only explicit denials.

block cipher - A symmetric cipher that encrypts plaintext in fixed-size blocks, applying the complete key to each block. Blocks are typically 64 or 128 bits, but can use any key size.

botnet - A network of malware-infected computers that can perform attacks or do other tasks as directed by its controller, without the knowledge of the actual system owners.

broadcast address - A MAC or 1Pv4 address that designates a packet that should be read by all listening hosts.

broadcast domain - A network segmentation unit where all nodes can reach each other by broadcast at the data link layer.

buffer overflow - The end result of including too much information in a request sent to an application, thereby overfilling the memory buffer and causing overflow into adjacent memory.

BYOD - Bring your own device. A security policy that allows or even encourages users to employ their own personal devices freely on the network.

CA - Certificate authority. A third-party entity responsible for assignment, verification, and revocation of digital certificates.

certificate - A special file attesting the identity of the computer or user that presents it. The certificate is cryptographically signed so that other computers can verify its authenticity by one of several possible means

chain of custody - Documentation about the history of a piece of forensic evidence from its discovery, to demonstrate that it was collected legally and was not subsequently altered.

CHAP - Challenge-handshake Authentication Protocol. A PPP protocol that uses a three-way handshake, with security provided by a shared secret that isn't transmitted over the network.

CIA triad - Confidentiality, integrity, and accountability. The three primary goals of all information security.

cipher suite - In SSL/TLS connections, a linked set of cryptographic methods. A suite contains separate algorithms for bulk encryption, key exchange, hashing, and pseudorandom number generation.

ciphertext - In cryptography, data that has been encrypted and is unreadable without the proper key.

client - A piece of computer hardware or software that accesses a service made available by a server.

cloud computing - A service model for network-accessible computing services, which includes on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

confidentiality - Ensuring that information is viewable only by authorized users or systems, and is either inaccessible or unreadable to unauthorized users.

Container (application) - A virtualized software package; unlike a VM it uses the host's kernel.

content filters - Software applications designed to restrict network access to unwanted or objectionable content, as opposed to malware or attacks.

content switch - A higher layer router that balances workload between multiple identical servers, while making them look like a single server to the outside network.

control - Any tool, device, or human activity used to decrease risk or otherwise achieve security goals.

cookies - Small text files stored in a user's browser, containing information relevant to the web sites that user visits.

CRC - Cyclic redundancy check. An error detecting code that can detect accidental alterations of stored or transmitted data, but is not secure against malicious alteration.

cross-site request forgery - (CSRF or XSRF) An attack on a legitimate session between a legitimate web server and another user that exploits the site's trust of the user, forging or altering requests from the client to the server within the context of the session.

cross-site scripting - (XSS) A web application attack where the attacker injects malicious scripts into a web page viewed in the victim's browser. The web page containing the script appears to be from a trusted site so the browser will trust the script as well.

CSR - Certificate signing request. A request sent to a CA containing all identifying information needed to request a new digital certificate.

DAC - Discretionary Access Control. An access control model in which the owner or creator of each controlled object decides who can access it and what permissions they have.

defense in depth - A security strategy that arrays controls in multiple layers so that an attacker who bypasses a single layer will not gain control of the entire system or network.

DHE - Diffie-Hellman Ephemeral. A protocol used to securely exchange temporary (ephemeral) keys used for bulk encryption.

digital certificate - See Certificate. (Or swap, or delete)

DLP - Data loss prevention software is used to prevent users from accidentally or maliciously sharing particular types of data outside your organization.

DMZ - Demilitarized zone, or perimeter network. A network zone that's under the organization's direct control but separate from, and less trusted than, the internal network.

DNS - Domain Name System. A hierarchical directory service that stores assigned domain names and their corresponding IP addresses.

DNS poisoning - An attack that compromises or impersonates domain name servers to redirect or block network requests.

DOM - Document Object Model. The application programming interface used by HTML and XML documents, which defines their structure and the way browsers access and manipulate them, changing objects within the model changes the presentation of the page.

DoS - Denial-of-service. Attacks designed to impair or block legitimate users' ability to use a network resource.

DPI - Deep packet inspection. A firewall feature that can inspect packet contents to enforce rules based on high-level protocols a traditional firewall would not recognize.

DSA - Digital Signature Algorithm. An asymmetric encryption algorithm designed for digital signatures. It has similar uses to RSA, but for some implementation reasons is currently less popular.

dual-homed server - A bastion host with two NICs, configured as a firewall to bridge the inside and outside networks.

EAP - Extensible Authentication Protocol. A PPP extension that can also be used for wireless authentication. Not an authentication method in itself, but rather a message format and set of common functions that can be used to support a wide variety of specific authentication methods.

edge computing - A distributed computing model which performs some level of storage and analysis directly on cloud-enabled devices.

eDiscovery - Electronic discovery. A legal process in which two parties in a court case can obtain digital evidence from each other.

EMI - Electromagnetic interference. Signal noise from electromagnetic sources that interferes with other equipment, especially data cables or wireless transceivers.

encryption - A security control method that uses mathematical processes to render data unreadable to those without the proper decryption key.

ephemeral key - A cryptographic key that is generated for each execution of a key establishment process.

event - Any meaningful change in a system's state that is both detectable and happened at a specific time.

failover - A method of protecting computer systems in which standby equipment automatically takes over when the main system fails.

false negative - A type of event evaluation in which a problem occurred but the analysis mistook it for benign behavior.

false positive - A type of event evaluation in which the behavior was benign but the analysis mistook it for a problem.

fault tolerance - An availability control system designed to continue functioning even when a hardware or software component fails.

FDE - Full drive encryption. A type of hardware-based encryption that encrypts all data on a drive, rendering it unreadable unless the key is entered during system boot or when it's connected.

federated identity management - Allows authentication systems to be shared across multiple systems or networks that share authentication standards even if they're not directly associated with each other. Members of a federation can share authentication tokens, access shared authentication servers, or otherwise behave as though they're part of a unified security system.

firewall - A computer system or network component that is designed to block unauthorized access while permitting outward communication.

fog computing - A distributed computing model which uses local nodes to perform storage and analysis of data which will be shared with the cloud.

forensics - The science of collecting evidence that's admissible in court. To be admissible, forensic evidence must be relevant to a legal case, sufficient in detail to prove a claim, and have an audit trail proving that it was collected legitimately and hasn't been altered since.

FQDN - Fully qualified domain name. The complete domain name for a specific computer, or host, on the Internet. Consists of two parts: the hostname and the domain name.

frame - A digital data transmission unit in computer networking and telecommunication. A frame typically includes frame synchronization features consisting of a sequence of bits or symbols that indicate to the receiver, the beginning, and end of the payload data within the stream of symbols or bits it receives.

fuzzing - A probe-based attack that inserts random or invalid data into more complex header fields or application data inputs. In extreme cases, fuzzing attacks can crash applications or entire systems, or gain access permissions; more commonly they're a way to learn how a service or application responds to non-standard input, enabling future attacks.

GPG - GNU Privacy Guard. The GNU project's free software implementation of the OpenPGP standard as defined by RFC4880. GPG is specifically a command line tool that enables you to encrypt and sign your data and communication and includes a key management system as well as access modules for all kind of public key directories.

GPO - Group policy object. In Windows 2000, a collection of settings that define what a system will look like and how it will behave for a defined group of users.

guest network - In a WAP system, a separate network access point with its own SS1D and login credentials. Guest clients are on a separate network from internal clients, and can't communicate to them directly. They can only use the WAP for Internet access.

hardening - The process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions. This typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services.

hash table - A database that stores the hashes used to uniquely identify files and other data elements in a storage system. Hash tables are valuable for searching and organizing large amounts of data, for example to recognize duplicate files even if they're stored in different folders or under different names.

hashing - The transformation of a string of

characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value.

HIPAA - Health Insurance Portability and Accountability Act.

HMAC - Hash-based message authentication code.

honeypot - A decoy system designed to be attractive and accessible to attackers. It has no useful resources and is isolated from the rest of the network. A honeypot is monitored to gather information on attackers without actually risking the consequences of an attack on real systems.

host - A computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network.

hosts file - An operating system file, in plain text format, that maps hostnames to IP addresses.

HTTPS - HTTP Secure. A protocol used for secure web pages and sites. It includes encryption services.

hypervisor - A software abstraction layer that runs VMs as applications, effectively an operating system for operating systems. To the VM the hypervisor looks like underlying hardware, but it's actually just allocating host resources and allowing multiple VMs to simultaneously share them.

ICMP - Internet Control Message Protocol. A protocol used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

ICS - Industrial control system. A general teen that encompasses several types of control systems and associated instrumentation used in industrial production technology, including supervisory control and data acquisition systems, distributed control systems, and other smaller control system configurations.

IDS - Intrusion detection systems.

implicit deny - An ACL model in which access is denied unless a rule explicitly allows it.

incident - A warning that there may be a threat to information or computer security. The warning could also be that a threat has already occurred.

information security - The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information.

injection - A class of attacks that rely on injecting data into a web application in order to facilitate the execution or interpretation of malicious data in an unexpected manner. Examples XSS, SQL Injection, Header Injection, Log Injection, and Full Path Disclosure.

integer overflow - Setting an integer variable to a value that exceeds the maximum size set aside to store it, usually through addition or multiplication functions.

integrity - The maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle. Integrity is a critical aspect to the design, implementation, and usage of any system which stores, processes, or retrieves data.

Internet of Things (IoT) - The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Internet Protocol (IPv4 and IPv6) - A set of rules governing the format of data sent over the Internet or other network.

Internet Protocol Security (Ipsec) - A network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session.

Intrusion protection systems (IPS) -Fundamentally passive monitoring systems designed to keep administrators aware of malicious activity: they can record detected intrusions in a database, and send alert notifications, but they rely on humans to actually take action.

IoC - Indicator of Compromise, evidence of adversary activity in a system.

IV - Initialization vector. An arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.

Kerberos - A network authentication protocol that works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

key escrow - An arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys.

Layer 2 Tunneling Protocol (L2TP) - A tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

LDAP - Lightweight Directory Access Protocol. An application protocol used over an IP network to manage and access the distributed directory information service.

LEAP - Lightweight EAP. A Cisco-proprietary version of EAP, the authentication protocol used in wireless networks and point-to-point connections. It is designed to provide more secure authentication for 802.11 WLANs that support 802.1X port access control.

least privilege - A security principle which requires that, in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.

load balancer - A device that acts as a reverse proxy and distributes network or application traffic across a number of servers. Load balancers are used to increase capacity and reliability of applications.

logic bomb - A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files

(such as a salary database trigger), should they ever be terminated from the company.

MAC address - A unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi¬Fi.

MAC filtering - A security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

malware - Software that is intended to damage or disable computers and computer systems.

Mandatory Access Control (MAC) - A type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target.

MD5 - Message Digest 5. A cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. The digest is sometimes also called the "hash" or "fingerprint" of the input.

MDM - Mobile device management. The administrative area dealing with deploying, securing, monitoring, integrating and managing mobile devices, such as smartphones, tablets and laptops, in the workplace.

MTBF - Mean time between failures.

MTBSI - Mean time between service incidents. MTTF - Mean time to failure. MTTR - Mean time to repair.

multifactor authentication - A security framework that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

multihomed firewall - Also known as three-homed firewall. A firewall system connecting the three zones (inside, outside, and DMZ) such that traffic passing between any two zones is protected by the firewall. Thus, not only is the inside protected from both the outside and DMZ, the DMZ is protected from outside.

mutual authentication - A security feature in which a client process must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection.

NAC - Network Access Control. An approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

NAT - Network address translation. A method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

Need to know - A restriction scheme in which, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information unless one has a specific need to know; that is, access to the information must be necessary for one to conduct one's official duties.

network segmentation - The splitting of a computer network into subnetworks, each being a network segment or network layer. This approach allows organizations to enhance security and group applications and like data together for access by a specific group (e.g., finance).

NFC - Near-field communication. A set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1.6 in) of each other.

NGFW - Next-Generation Firewall.

nonce - An arbitrary number used only once in a cryptographic communication.

non-repudiation - A security framework in which authenticity is verified in such a way that even the information's author can't dispute creating it.

oftboarding - The identity and access

management processes surrounding the removal of an identity for an employee who has left the organization. May also be used to describe the

restriction of certain access rights when an employee has changed roles within the organization.

onboarding - The addition of a new employee to an organization's identity and access management system. This term is also used if an employee changes roles within the organization and is granted new or expanded access privileges.

order of volatility - The order in which you should collect forensic security evidence. Highly volatile data is easily lost, such as data in memory when you turn off a computer. Less volatile data, such as printouts, is relatively permanent and the least volatile.

OTP - One-time password. A single-use PIN or password that is valid for a single session, so can't be stolen and reused. The OTP still has to be known to both the user and the authenticator somehow, so it's a challenge to accurately create one.

PAT - Port address translation. An extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

PBKDF2 - Password-Based Key Derivation Function 2.

PBX - Private branch exchange. A telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines.

PCI DSS - Payment Card Industry Digital Security Standard.

PEAP - Protected EAP. A protocol that secures EAP authentication in a TLS tunnel.

penetration test - An attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and

application flaws, improper configurations or risky end-user behavior.

perfect forward secrecy - A property of secure communication protocols in which compromise of long-term keys does not compromise past session keys.

perimeter network - A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network, such as the Internet. (See also DMZ.)

PGP - Pretty Good Privacy. Data encryption software that uses two digital equivalents of physical keys: a public key used for encrypting data that can be given by its owner to anyone who wants to send a secure transmission; and a private key used for decrypting the data and known only to its owner.

pharming - An application of DNS poisoning in which an attacker redirects traffic for a legitimate website to a malicious imitator. Much like in a phishing attack, victims might be tricked into entering credentials or other sensitive data, or into downloading malware.

phishing - An attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

PTT - Personally identifiable information.

plaintext - Ordinary readable text before being encrypted into ciphertext or after being decrypted.

port forwarding - Routing inbound traffic to local addresses based on the destination port. For example, all traffic addressed to TCP port 80 can be sent to the company web server, while traffic addressed to ports 20-21 is forwarded to the FTP server.

posture assessment - The evaluation of system security based on the applications and settings that a particular system is using. This ensures that the client system meets certain security rules; for example, that it has appropriate anti-virus software installed, and that its operating system and relevant software is updated with the latest security updates.

PPP - Point-to-Point Protocol. A data link (layer 2) protocol used to establish a direct connection between two nodes. It is used on everything from dialup connections to SONET leased lines, and can carry IP, IPX, and other high-level traffic.

PPTP - Point-to-Point Tunneling Protocol. A very basic VPN protocol that encapsulates PPP packets over GRE to provide VPN tunneling features, allowing it to carry any protocol PPP can, including IP, IPX, and NetBEUI.

principal - An entity (user) that can be authenticated by a computer system or network.

private key - A tiny bit of code that is paired with a public key to set off algorithms for text encryption and decryption. It is created as part of public key cryptography during asymmetric-key encryption and used to decrypt and transform a message to a readable format.

private network range - Part of internal LAN configuration, these network addresses aren't routable on the Internet, but are instead commonly used on home or office networks.

privilege escalation - A security attack in which an ordinary user account or application gets administrative rights that enable it do more harm.

Protected distribution system - In US government terminology, a wireline or fiber-optics telecommunication system that includes terminals and adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.



protocol analyzer - Also known as network analyzer or packet analyzer. Captures and analyzes network traffic. Can read packet headers to determine traffic patterns, or view protocol information in depth.

proxy server - An intermediary between a client and a server: instead of the client contacting the server directly, it contacts the proxy server, which in turn contacts the remote server. In return, the remote server communicates with the client through the proxy server.

PSK - Pre-shared key. A shared secret which was previously shared between the two parties using some secure channel before it needs to be used.

public key cryptography - A cryptography method that uses two mathematically-related keys: data encrypted with one key can only be decrypted with the other. Called "public" because one key can be shared with the public without compromising the security of the other.

RADIUS - Remote Authentication Dial-In User Service.

RAID - Redundant array of independent disks.

rainbow table - A precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Commonly used in recovering a plaintext password up to a certain length consisting of a limited set of characters.

RAS - Remote Access Service.

RBAC (Role-based access control) - A method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file.

RBAC (Rule-based access control) - A method of regulating access to computer or network resources that dynamically assigns roles to users based on criteria defined by the custodian or system administrator.

RC4 Rivest Cipher 4.

redundancy - System design in which a component is duplicated so if it fails there will be a backup. (Redundancy has a negative connotation when the duplication is unnecessary or is simply the result of poor planning.)

remote code execution - A security vulnerability that allows an attacker to execute codes from a remote server. The most dangerous result of an application attack, since in conjunction with privilege escalation it can give the attacker full control of the remote computer.

residual risk - The threat that remains after all efforts to identify and eliminate risk have been made.

risk - Any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability.

rogue device - A wireless device that remains connected to a system but does not have permission to access and operate in a network.

role-based training - Training that is customized to the specific role that employee holds in the organization. Training content is tailored to classes of users based on their workplace duties and expected technical expertise.

root certificate - A public key certificate that identifies a root certificate authority (CA). Root certificates are self-signed and form the basis of an X.509-based public key infrastructure (PICT).

rootkit - A set of software tools that enable an unauthorized user to gain control of a computer system without being detected.

routing table - The set of rules and data that the router uses to map its surroundings. On a large network, this could be a lot of information, including planning several hops across multiple routers.

RSA - Rivest, Shamir, & Adleman. A

cryptosystem for public-key encryption, widely used for securing sensitive data, particularly when being sent over an insecure network such as the internet.

S/MIME - Secure/Multipurpose Internet Mail Extensions.

salt - In cryptography, random data that is used as an additional input to a one-way function that "hashes" a password or passphrase. Closely related to the concept of nonce.

SAN - Storage area network. A network that provides access to consolidated, block level data storage. Primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear to the operating system as locally attached devices.

sandbox - A type of software testing environment that enables the isolated execution of software or programs for independent evaluation, monitoring or testing. May be known as a test server, development server, or working directory.

sanitization - Erasing a storage device, such as a computer hard drive, so thoroughly that no residual data can be collected from the device.

SCADA - Supervisory control and data acquisition.

SCSI - Small Computer Systems Interface.

separation of duties (SoD) - An internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate

parts of any task. SoD involves breaking down tasks that might reasonably be completed by a single individual into multiple tasks so that no one person is solely in control.

server - A computer designed to process requests and deliver data to other (client) computers over a local network or the internet. There are a number of categories of servers, including print servers, file servers, network servers and database servers.

session - Refers to a limited time of communication between two systems. Some sessions involve a client and a server, while other sessions involve two personal computers.

session key - A single-use symmetric key used for encrypting all messages in one communication session.

SFTP - SSH File Transfer Protocol. SHA - Secure Hash Algorithm.

SIEM - Security Information and Event Management.

single point of failure - A system component whose failure, by itself, will stop the entire system from working.

SLE - Single loss expectancy. The cost of any single loss.

smart cards - Authentication cards with integrated circuits built in. A smart card's chip holds basic identifying information like a magnetic stripe would; it can also hold digital certificates, store temporary data, or even perform cryptographic processing functions to keep its data secure.

sniffer - A program that monitors and analyzes network traffic, detecting bottlenecks and problems. Also known as protocol analyzer.

SOAP - Simple Object Access Protocol.

SOAR - Security Orchestration, Automation, and Response.

social engineering - The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

spam - Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.

SPI - Stateful packet inspection. A firewal I technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

spoofing - A type of scam where an intruder attempts to gain unauthorized access to a user's system or information by pretending to be the user. The main purpose is to trick the user into releasing sensitive information in order to gain access to one's bank account, computer system or to steal personal information, such as passwords.

SQL - Structured Query Language. SSH - Secure Shell.

SSL - Secure Sockets Layer. The standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

SSO - Single sign-on. Systems that allow one set of user credentials to give access to a large number of services.

steganography - A form of cryptography that hides secret messages in seemingly innocuous information or even out of sight entirely, so that a casual onlooker doesn't even know it's there.

storage segmentation - Separating a particular part of device storage so that it that can be encrypted and controlled separately from the rest.

stream cipher - A symmetric key cipher where plaintext digits are combined with a

pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream.

structured walkthrough - An organized procedure for a group of peers to review and discuss the technical aspects of software development and maintenance deliverables and outputs. Primary objectives are to find errors and to improve the quality of the product.

subnet - An identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN).

switching loop - Formed when multiple paths join any two switches, passing the same frames around and around until they crowd out all other traffic.

TACACS+ - Terminal Access Controller Access Control System.

tailgating - Also known as piggybacking. Getting into a secure area by tagging along right behind someone who has legitimate access, with or without their knowledge.

TCP - Transmission Control Protocol.

thin client - A networked computer with few locally stored programs and a heavy dependence on network resources. It may have very limited resources of its own, perhaps operating without auxiliary drives or even software applications. Typically, a thin client is one of many network computers that share computation needs by using the resources of one server.

threat - Anything that has the potential to cause serious harm to a computer system. It may or may not happen, but has the potential to cause serious damage.

threat hunting - The practice of proactively searching for security threats.

three-way handshake - A three-step method used in a TCP/IP network to create a connection between a local host/client and server. It requires both the client and server to exchange SYN and ACK packets before actual data communication begins.

TKIP - Temporal Key Integrity Protocol. TLS Transport Layer Security.

transitive trust - A two-way relationship automatically created between parent and child domains in a Microsoft Active Directory forest. When a new domain is created, it shares resources with its parent domain by default, enabling an authenticated user to access resources in both the child and parent.

Triple DES (3DES) - A symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

Trojan - A program that appears legitimate but performs some illicit activity when run. May be used to locate password information or make the system more vulnerable to future entry or simply destroy the user's stored software and data.

typo squatting - A form of cybersquatting (and possibly brandjacking) that relies on mistakes such as typos made by internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to any URL, including an alternative website owned by a cybersquatter.

UDP - User Datagram Protocol. UPS - Uninterpretable power supply. URL hijacking - See typo squatting. UTM - Unified threat management.

validation - The process of ensuring that a program operates on clean, correct and useful data. It uses routines that check for correctness, meaningfulness, and security of data that are input to the system.

virtualization - The process of creating a virtual (rather than actual) version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments.

virus - A type of malicious software program that, when executed, replicates itself by modifying other computer programs and inserting its own code.

VLAN - Virtual LAN. Any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

VM - Virtual machine. An operating system (OS) or application environment that is installed on software, which imitates dedicated hardware. The end user has the same experience on a virtual machine as they would have on dedicated hardware.

VoIP - Voice over IP. A category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions of the PSTN.

VPN - Virtual private network. A network that is constructed using public wires (usually the internet) to connect remote users or regional offices to an organization's private, internal network.

vulnerability - Any weakness the asset has against potential threats. Vulnerabilities can be hardware, software, or human/organizational; likewise, they can represent errors or shortcomings in system design, or known tradeoffs for desired features.

WAF - Web application firewall. An application firewall for HTTP applications that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as XSS and SQL injection.

WAP - Wireless access point.

web application - A client-server software application in which the client (or user interface) runs in a web browser. Common web applications include webmail, online retail sales, online auctions, wilds, instant messaging services, and many others.

web of trust - A cryptography framework in which a certificate is signed by one or more third parties to form a decentralized network of trust relationships: if you trust any of the people who have signed the certificate, then you should be able to trust its owner.

WEP - Wired Equivalent Privacy.

work factor - In cryptography, the amount of effort required to break down a cryptosystem.

worm - A type of computer virus that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

WPA - Wi-Fi Protected Access.

WPS - Wi-Fi Protected Setup.

X.509 - In cryptography, a standard that defines the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web.

)(NIL - eXtensible Markup Language. A tagged markup language, designed to be both human- and machine-readable. Related to HTML but more general-

purpose and used for all sorts of documents, databases, and other web application data storage.

zero-day vulnerabilities - Weaknesses that even programmers and security vendors don't know about and haven't countered, and which attackers might learn about first.