- 802.1x

A port-based authentication protocol. Wireless can use 802.1x. For example, WPA2 Enterprise mode uses an 802.1x server (implemented as a RADIUS server). Enterprise mode requires an 802.1x server. PEAP and EAP-TTLS require a certificate on the 802.1x server. EAP-TLS also uses TLS, but it requires certificates on both the 802.1x server and each of the clients.

- 3DES

Triple Digital Encryption Standard. A symmetric algorithm used to encrypt data and provide confidentiality. It is a block cipher that encrypts data in 64-bit blocks. It was originally designed as a replacement for DES, and is still used in some applications, such as when hardware doesn't support AES.

- AAA

Authentication, Authorization, and Accounting. AAA protocols are used in remote access systems. For example, TACACS + is an AAA protocol that uses multiple challenges and responses during a session. Authentication verifies a user's identification. Authorization determines if a user should have access. Accounting tracks a user's access with logs.

- ACE

Access Control Entry. Identifies a user or group that is granted permission to a resource. ACEs are contained within a DACL in NTFS.

- ACK

Acknowledge. A packet in a TCP handshake. In a SYN flood attack, attackers send the SYN packet, but don't complete the handshake after receiving the SYN/ ACK packet.

- ACL

Access control list. Routers and packet-filtering firewalls perform basic filtering using an ACL to control traffic based on networks, subnets, IP addresses, ports, and some protocols. In NTFS, a list of ACEs makes up the ACL for a resource.

- AES

Advanced Encryption Standard. A symmetric algorithm used to encrypt data and provide confidentiality. AES is a block cipher and it encrypts data in 128-bit blocks. It is quick, highly secure, and used in a wide assortment of cryptography schemes. It includes key sizes of 128 bits, 192 bits, or 256 bits.

- AES-256

Advanced Encryption Standard 256 bit. AES sometimes includes the number of bits used in the encryption keys and AES-256 uses 256-bit encryption keys. Interestingly, Blowfish is quicker than AES-256.

- AH

Authentication Header. IPsec includes both AH and ESP. AH provides authentication and integrity using HMAC. ESP provides confidentiality, integrity, and authentication using HMAC, and AES or 3DES. AH is identified with protocol ID number 51.

- ALE

Annual (or annualized) loss expectancy. The ALE identifies the expected annual loss and is used to measure risk with ARO and SLE in a quantitative risk assessment. The calculation is SLE × ARO = ALE.

- AP

Access point, short for wireless access point (WAP). APs provide access to a wired network to wireless clients. Many APs support Isolation mode to segment wireless users from other wireless users.

- API

Application Programming Interface. A software module or component that identifies inputs and outputs for an application.

- APT

Advanced persistent threat. A group that has both the capability and intent to launch sophisticated and targeted attacks.

- ARO

Annual (or annualized) rate of occurrence. The ARO identifies how many times a loss is expected to occur in a year and it is used to measure risk with ALE and SLE in a quantitative risk assessment. The calculation is SLE × ARO = ALE.

• ARP

Address Resolution Protocol. Resolves IPv4 addresses to MAC addresses. ARP poisoning attacks can redirect traffic through an attacker's system by sending false MAC address updates. NDP is used with IPv6 instead of ARP.

• ASCII

American Standard Code for Information Interchange. Code used to display characters.

- ASP

Application Service Provider. Provides an application as a service over a network.

- AUP

Acceptable use policy. An AUP defines proper system usage. It will often describe the purpose of computer systems and networks, how users can access them, and the responsibilities of users when accessing the systems.

- BAC

Business Availability Center. An application that shows availability and performance of applications used or provided by a business.

- BCP

Business continuity plan. A plan that helps an organization predict and plan for potential outages of critical services or functions. It includes disaster recovery elements that provide the steps used to return critical functions to operation after an outage. A BIA is a part of a BCP and the BIA drives decisions to create redundancies such as failover clusters or alternate sites.

- BIA

Business impact analysis. The BIA identifies systems and components that are essential to the organization's success. It identifies various scenarios that can impact these systems and components, maximum downtime limits, and potential losses from an incident. The BIA helps identify RTOs and RPOs.

- BIND

Berkeley Internet Name Domain. BIND is DNS software that runs on Linux and Unix servers. Most Internet-based DNS servers use BIND.

- BIOS

Basic Input/ Output System. A computer's firmware used to manipulate different settings such as the date and time, boot drive, and access password. UEFI is the designated replacement for BIOS.

- BPA

Business partners agreement. A written agreement that details the relationship between business partners, including their obligations toward the partnership.

- BYOD

Bring your own device. A policy allowing employees to connect personally owned devices, such as tablets and smartphones, to a company network. Data security is often a concern with BYOD policies and organizations often use VLANs to isolate mobile devices.

- CA

Certificate Authority. An organization that manages, issues, and signs certificates and is part of a PKI. Certificates are an important part of asymmetric encryption. Certificates include public keys along with details on the owner of the certificate and on the CA that issued the certificate. Certificate owners share their public key by sharing a copy of their certificate.

- CAC

Common Access Card. A specialized type of smart card used by the U.S. Department of Defense. It includes photo identification and provides confidentiality, integrity, authentication, and non-repudiation for the users. It is similar to a PIV.

- CAN

Controller Area Network. A standard that allows microcontrollers and devices to communicate with each other without a host computer.

- CAPTCHA

Completely Automated Public Turing Test to Tell Computers and Humans Apart. Technique used to prevent automated tools from interacting with a web site. Users must type in text, often from a slightly distorted image.

- CAR

Corrective Action Report. A report used to document actions taken to correct an event, incident, or outage.

- CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. An encryption protocol based on AES and used with WPA2 for wireless security. It is more secure then TKIP, which was used with the original release of WPA.

- CCTV

Closed-circuit television. This is a detective control that provides video surveillance. Video surveillance provides reliable proof of a person's location and activity. It is also a physical security control and it can increase the safety of an organization's assets.

- CERT

Computer Emergency Response Team. A group of experts who respond to security incidents. Also known as CIRT, SIRT, or IRT.

- CHAP

Challenge Handshake Authentication Protocol. Authentication mechanism where a server challenges a client. More secure than PAP and uses PPP. MS-CHAPv2 is an improvement over CHAP and uses mutual authentication.

- CIA

Confidentiality, integrity, and availability. These three form the security triad. Confidentiality helps prevent the unauthorized disclosure of data. Integrity provides assurances that data has not been modified, tampered with, or corrupted. Availability indicates that data and services are available when needed.

- CIO

Chief Information Officer. A "C" level executive position in some organizations. A CIO focuses on using methods within the organization to answer relevant questions and solve problems.

- CIRT

Computer Incident Response Team. A group of experts who respond to security incidents. Also known as CERT, SIRT, or IRT.

- COOP

Continuity of operations planning. Continuity of operations planning (COOP) sites provide an alternate location for operations after a critical outage. A hot site includes personnel, equipment, software, and communication capabilities of the primary site with all the data up to date. A cold site will have power and connectivity needed for COOP activation, but little else. A warm site is a compromise between a hot site and a cold site. Mobile sites do not have dedicated locations, but can provide temporary support during a disaster.

- CP

Contingency planning. Plans for contingencies in the event of a disaster to keep an organization operational. BCPs include contingency planning.

- CRC

Cyclical Redundancy Check. An error detection code used to detect accidental changes that can affect the integrity of data.

- CRL

Certification revocation list. A list of certificates that a CA has revoked. Certificates are commonly revoked if they are compromised, or issued to an employee who has left the organization. The Certificate Authority (CA) that issued the certificate publishes a CRL, and a CRL is public.

- CSR

Certificate signing request. A method of requesting a certificate from a CA. It starts by creating an RSA-based private/ public key pair and then including the public key in the CSR.

- CSR

Control Status Register. A register in a processor used for temporary storage of data.

- CSU

Channel Service Unit. A line bridging device used with T1 and similar lines. It typically connects with a DSU as a CSU/DSU.

- CTO

Chief Technology Officer. A "C" level executive position in some organizations. CTOs focus on technology and evaluate new technologies.

- CVE

Common Vulnerabilities and Exposures (CVE). A dictionary of publicly known security vulnerabilities and exposures.

- DAC

Discretionary access control. An access control model where all objects have owners and owners can modify permissions for the objects (files and folders). Microsoft NTFS uses the DAC model. Other access control models are MAC and RBAC.

- DACL

Discretionary access control list. List of Access Control Entries (ACEs) in Microsoft NTFS. Each ACE includes a security identifier (SID) and a permission.

- DBA

Database administrator. A DBA administers databases on database servers.

- dBd

Decibels-dipole. Identifies the gain of an antenna compared with a type of dipole antenna. Higher dBd numbers indicate the antenna can transmit and receive over greater distances.

- dBi

Decibels-isotropic. Identifies the gain of an antenna and is commonly used with omnidirectional antennas. It references an isotropic antenna that can theoretically transmit the signal equally in all directions. Higher numbers indicate the antenna can transmit and receive over greater distances.

- dBm

Decibels-milliwatt. Identifies the power level of the WAP and refers to the power ratio in decibels referenced to one milliwatt. Higher numbers indicate the WAP transmits the signal over a greater distance.

- DDoS

Distributed denial-of-service. An attack on a system launched from multiple sources intended to make a computer's resources or services unavailable to users. DDoS attacks typically include sustained, abnormally high network traffic. Compare to DoS.

- DEP

Data Execution Prevention. A security feature in some operating systems. It helps prevent an application or service from executing code from a nonexecutable memory region.

- DES

Digital Encryption Standard. An older symmetric encryption standard used to provide confidentiality. DES is a block cipher and it encrypts data in 64-bit blocks. DES uses 56 bits and is considered cracked. Use AES instead, or 3DES if the hardware doesn't support AES.

- DHCP

Dynamic Host Configuration Protocol. A service used to dynamically assign TCP/ IP configuration information to clients. DHCP is often used to assign IP addresses, subnet masks, default gateways, DNS server addresses, and much more.

- DHE

Data-Handling Electronics. Term used at NASA indicating electronic systems that handle data.

- DHE

Diffie-Hellman Ephemeral. An alternative to traditional Diffie-Hellman. Instead of using static keys that stay the same over a long period, DHE uses ephemeral keys, which change for each new session. Sometimes listed as EDH.

- DLL

Dynamic Link Library. A compiled set of code that can be called from other programs.

- DLP

Data loss prevention. A network-based DLP system can examine and analyze network traffic. It can detect if confidential company data or any PII data is included in email and reduce the risk of internal users emailing sensitive data outside the organization. End-point DLP systems can prevent users from copying or printing sensitive data.

- DMZ

Demilitarized zone. A buffer zone between the Internet and an internal network. It allows access to services while segmenting access to the internal network. Internet clients can access the services hosted on servers in the DMZ, but the DMZ provides a layer of protection for the internal network. DNAT— Dynamic Network Address Translation. A form of NAT that uses multiple public IP addresses. In contrast, PAT uses a single public IP address. It hides addresses on an internal network.

- DNAT

Destination Network Address Translation. A form of NAT that changes the destination IP address for incoming traffic. It is used for port forwarding.

- DNS

Domain Name System. Used to resolve host names to IP addresses. DNS zones include records such as A records for IPv4 addresses and AAAA records for IPv6 addresses. DNS uses UDP port 53 for DNS client queries and TCP port 53 for zone transfers. DNS poisoning attacks attempt to modify or corrupt DNS data. Secure zone transfers help prevent these attacks. A pharming attack is a type of DNS poisoning attack that redirects a web site's traffic to another web site.

- DNSSEC

Domain Name System Security Extensions. A suite of specifications used to protect the integrity of DNS records and prevent DNS poisoning attacks.

- DoS

Denial-of-service. An attack from a single source that attempts to disrupt the services provided by the attacked system. Compare to DDoS.

- DRP

Disaster recovery plan. A document designed to help a company respond to disasters, such as hurricanes, floods, and fires. It includes a hierarchical list of critical systems and often prioritizes services to restore after an outage. Testing validates the plan. The final phase of disaster recovery includes a review to identify any lessons learned and may include an update of the plan.

- DSA

Digital Signature Algorithm. A digital signature is an encrypted hash of a message. The sender's private key encrypts the hash of the message to create the digital signature. The recipient decrypts the hash with the sender's public key, and, if successful, it provides authentication, non-repudiation, and integrity. Authentication identifies the sender. Integrity verifies the message has not been modified. Non-repudiation is used with online transactions and prevents the sender from later denying he sent the email.

- DSL

Digital subscriber line. Improvement over traditional dial-up to access the Internet.

- DSU

Data Service Unit. An interface used to connect equipment to a T1 and similar lines. It typically connects with a CSU as a CSU/ DSU.

- EAP

Extensible Authentication Protocol. An authentication framework that provides general guidance for authentication methods. Variations include EAP-TLS, EAP-TTLS, LEAP, and PEAP.

- EAP-TLS

Extensible Authentication Protocol-Transport Layer Security. An extension of EAP sometimes used with 802.1x. This is one of the most secure EAP standards and is widely implemented. The primary difference between PEAP and EAP-TLS is that EAP-TLS requires certificates on the 802.1x server and on each of the wireless clients.

- EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security. An extension of EAP sometimes used with 802.1x. It allows systems to use some older authentication methods such as PAP within a TLS tunnel. It requires a certificate on the 802.1x server but not on the clients.

- ECC

Elliptic curve cryptography. An asymmetric encryption algorithm commonly used with smaller wireless devices. It uses smaller key sizes and requires less processing power than many other encryption methods.

- ECDHE

Elliptic Curve Diffie-Hellman Ephemeral. A version of Diffie-Hellman that uses ECC to generate encryption keys. Ephemeral keys are re-created for each session.

- EFS

Encrypting File System. A feature within NTFS on Windows systems that supports encrypting individual files or folders for confidentiality.

- EMI

Electromagnetic interference. Interference caused by motors, power lines, and fluorescent lights. EMI shielding prevents outside interference sources from corrupting data and prevents data from emanating outside the cable.

- ESD

Electrostatic discharge. Release of static electricity. ESD can damage equipment and low humidity causes a higher incidence of electrostatic discharge (ESD). High humidity can cause condensation on the equipment, which causes water damage.

- ESN

Electronic Serial Number. Numbers used to uniquely identify mobile devices.

- ESP

Encapsulating Security Protocol. IPsec includes both AH and ESP. AH provides authentication and integrity using HMAC. ESP provides confidentiality, integrity, and authentication using HMAC and AES or 3DES. ESP is identified with protocol ID number 50.

- FACL

File System Access Control List. An ACL used for file systems. As an example, NTFS uses the DAC model to protect files and folders.

- FCoE

Fibre Channel over Ethernet. A lower-cost alternative to traditional SANs. It supports sending Fibre Channel commands over an IP network.

- FDE

Full Disk Encryption. Method to encrypt an entire disk. TrueCrypt is an example.

- FTP

File Transfer Protocol. Used to upload and download files to an FTP server. FTP uses TCP ports 20 and 21. Secure FTP (SFTP) uses SSH for encryption on TCP port 22. FTP Secure (FTPS) uses SSL or TLS for encryption.

- FTPS

File Transfer Protocol Secure. An extension of FTP that uses SSL to encrypt FTP traffic. Some implementations of FTPS use TCP ports 989 and 990.

- GPG

GNU Privacy Guard (GPG). Free software based on the OpenPGP standard and used to encrypt and decrypt files. It is similar to PGP but avoids any conflict with existing licensing by using open standards.

- GPO

Group Policy Object. Group Policy is used within Microsoft Windows to manage users and computers. It is implemented on a domain controller within a domain. Administrators use it to create password policies, lock down the GUI, configure host-based firewalls, and much more.

- GPS

Global Positioning System. GPS tracking can help locate lost mobile devices. Remote wipe, or remote sanitize, erases all data on lost devices. Full disk encryption protects the data on the device if it is lost.

- GRE

Generic Routing Encapsulation. A tunneling protocol developed by Cisco Systems.

- GUI

Graphical user interface. Users interact with the graphical elements instead of typing in commands from a text interface. Windows is an example of a GUI.

- HDD

Hard disk drive. A disk drive that has one or more platters and a spindle. In contrast, USB flash drives and SSD drives use flash memory.

- HIDS

Host-based intrusion detection system. An IDS used to monitor an individual server or workstation. It protects local resources on the host such as the operating system files, and in some cases, it can detect malicious activity missed by antivirus software.

- HIPS

Host-based intrusion prevention system. An extension of a host-based IDS. Designed to react in real time to catch an attack in action.

- HMAC

Hash-based Message Authentication Code. A hashing algorithm used to verify integrity and authenticity of a message with the use of shared secret. When used with TLS and IPsec, HMAC is combined with MD5 and SHA-1 as HMAC-MD5 and HMAC-SHA1, respectively.

- HOTP

HMAC-based One-Time Password (HOTP). An open standard used for creating one-time passwords, similar to those used in tokens or key fobs. It combines a secret key and an incrementing counter, and then uses HMAC to create a hash of the result. HOTP passwords do not expire until they are used.

- HSM

Hardware security module. A removable or external device that can generate, store, and manage RSA keys used in asymmetric encryption. High-volume e-commerce sites use HSMs to increase the performance of SSL sessions. High-availability clusters needing encryption services can use clustered HSMs.

- HTML

Hypertext Markup Language. Language used to create web pages. HTML documents are displayed by web browsers and delivered over the Internet using HTTP or HTTPS. It uses less-than and greater-than characters (< and >) to create tags. Many sites use input validation to block these tags and prevent cross-site scripting attacks.

- HTTP

Hypertext Transfer Protocol. Used for web traffic on the Internet and in intranets. HTTP uses TCP port 80.

- HTTPS

Hypertext Transfer Protocol Secure. Encrypts HTTP traffic with SSL or TLS using TCP port 443.

- HVAC

Heating, ventilation, and air conditioning. HVAC systems increase availability by regulating airflow within data centers and server rooms. They use hot and cold aisles to regulate the cooling, thermostats to ensure a relatively constant temperature, and humidity controls to reduce the potential for static discharge, and damage from condensation. Higher-tonnage HVAC systems provide more cooling capacity to keep server rooms at operating temperatures, resulting in fewer failures and longer MTBF times. HVAC systems should be integrated with fire alarm systems and either have dampers or the ability to be turned off in the event of a fire.

- IaaS

Infrastructure as a Service. A cloud computing technology that allows an organization to rent access to hardware. It provides customers with access to hardware in a self-managed platform. Customers are responsible for keeping an IaaS system up to date. Compare to PaaS and SaaS.

- ICMP

Internet Control Message Protocol. Used for diagnostics such as ping. Many DoS attacks use ICMP. It is common to block ICMP at firewalls and routers. If ping fails, but other connectivity to a server succeeds, it indicates that ICMP is blocked.

- ID

Identification. For example, a protocol ID identifies a protocol based on a number. AH is identified with protocol ID number 51 and ESP is identified with protocol ID number 50.

- IDS

Intrusion detection system. A detective control used to detect attacks after they occur. Monitors a network (NIDS) or host (HIDS) for intrusions and provides ongoing protection against various threats. IDSs include sniffing capabilities. Many IDSs use numbering systems to identify vulnerabilities.

- IEEE

Institute of Electrical and Electronics Engineers. IEEE is an international organization with a focus on electrical, electronics, and information technology topics. IEEE standards are well respected and followed by vendors around the world.

- IGMP

Internet Group Management Protocol. Used for multicasting. Computers belonging to a multicasting group have a multicasting IP address in addition to a standard unicast IP address.

- IIS

Internet Information Services. A Microsoft Windows web server. IIS comes free with Microsoft Windows Server products. Linux systems use Apache as a web server.

- IKE

Internet Key Exchange. Used with IPsec to create a secure channel over UDP port 500 in a VPN tunnel.

- IM

Instant messaging. Real-time direct text-based communication between two or more people, often referred to as chat. Spim is a form of spam using IM.

- IMAP4

Internet Message Access Protocol v4. Used to store email on servers and allow clients to manage their email on the server. IMAP4 uses TCP port 143.

- IP

Internet Protocol. Used for addressing. See IPv4 and IPv6.

- IPS

Intrusion prevention system. A preventive control that will stop an attack in progress. It is similar to an active IDS except that it's placed in-line with traffic. An IPS can actively monitor data streams, detect malicious content, and stop attacks in progress. It can be used internally to protect private networks, such as those holding SCADA equipment.

- IPsec

Internet Protocol security. Used to encrypt data in transit and can operate in both Tunnel mode and Transport mode. It uses Tunnel mode for VPN traffic. IPsec is built in to IPv6, but can also work with IPv4. Both versions support AH and ESP. AH provides authentication and integrity using HMAC. ESP provides confidentiality, integrity, and authentication using HMAC and AES or 3DES. IPsec creates secure tunnels for VPNs using UDP port 500 for IKE.

- IPv4

Internet Protocol version 4. Identifies hosts using a 32-bit IP address. IPv4 is expressed in dotted decimal format with decimal numbers separated by dots or periods like this: 192.168.1.1.

- IPv6

Internet Protocol version 6. Identifies hosts using a 128-bit address. IPv6 has a significantly larger address space than IPv4. IPsec is built in to IPv6 and can encrypt any type of IPv6 traffic.

- IR

Incident response. Process of responding to a security incident. Organizations often create an incident response policy that outlines procedures and responsibilities of personnel on incident response teams.

- IRC

Internet Relay Chat. A form of real-time Internet text messaging often used with chat sessions. Some botnets have used IRC channels to control zombie computers through a command-and-control server.

- IRT

Incident Response Team. A group of experts who respond to security incidents. Also known as CERT, CIRT, or SIRT.

- IRP

Incident Response Procedure. Procedures documented in an incident response policy.

- ISA

Interconnection Security Agreement. Specifies technical and security requirements for connections between two or more entities. An ISA includes details on planning, establishing, maintaining, and disconnecting a secure connection between two or more entities.

- iSCSI

Internet Small Computer System Interface. A lower-cost alternative to traditional SANs. It supports sending traditional SCSI commands over an IP network.

- ISP

Internet Service Provider. A company that provides Internet access to customers.

- ISSO

Information Systems Security Officer. A job role within an organization focused on information security.

- IT

Information technology. Computer systems and networks used within organizations.

- ITCP

IT contingency plan. Part of risk management. Plan to ensure that IT resources remain available after a security incident, outage, or disaster.

- IV

Initialization vector. An IV provides randomization of encryption keys to help ensure that keys are not reused. WEP was susceptible to IV attacks because it used relatively small IVs. In an IV attack, the attacker uses packet injection, increasing the number of packets to analyze, and discovers the encryption key.

- JBOD

Just a Bunch of Disks. Disks installed on a computer but not as a RAID.

- KDC

Key Distribution Center. Also known as TGT server. Part of the Kerberos protocol used for network authentication. The KDC issues timestamped tickets that expire.

- L2TP

Layer 2 Tunneling Protocol. Tunneling protocol used with VPNs. L2TP is commonly used with IPsec (L2TP/ IPsec). L2TP uses UDP port 1701. Compare to PPTP, which uses TCP port 1723.

- LAN

Local area network. Group of hosts connected within a network.

- LANMAN

Local area network manager. Older authentication protocol used to provide backward compatibility to Windows 9x clients. LANMAN passwords are easily cracked due to how they are stored.

- LDAP

Lightweight Directory Access Protocol. Language used to communicate with directories such as Microsoft Active Directory. Identifies objects with query strings using codes such as CN = Users and DC = GetCertifiedGetAhead. LDAP uses TCP port 389. Secure LDAP encrypts transmissions with SSL or TLS over TCP port 636. LDAP injection attacks attempt to access or modify data in directory service databases.

- LEAP

Lightweight Extensible Authentication Protocol. A modified version of the Challenge Handshake Authentication Protocol (CHAP) created by Cisco LEAP does not require a digital certificate and Cisco now recommends using stronger protocols such as EAP-TLS.

- LSO

Local shared objects or locally shared objects. A Flash cookie created by Adobe Flash player.

- MaaS

Monitoring as a Service or Management as a Service. Allows an organization to outsource the management and monitoring of IT resources.

• MAC

Mandatory access control. Access control model that uses sensitivity labels assigned to objects (files and folders) and subjects (users). MAC restricts access based on a need-to-know.

• MAC

Media access control. A 48-bit address used to identify network interface cards. It is also called a hardware address or a physical address, and is commonly displayed as six pairs of hexadecimal characters. Port security on a switch or an AP can limit access using MAC filtering.

• MAC

Message authentication code. Method used to provide integrity for messages. A MAC uses a secret key to encrypt the hash. HMAC is a commonly used version.

- Malware

Malicious software. Includes viruses, Trojans, adware, spyware, rootkits, backdoors, logic bombs, and ransomware.

- MAN

Metropolitan area network. A computer network that spans a metropolitan area such as a city or a large campus.

- MBR

Master Boot Record. An area on a hard disk in its first sector. When the BIOS boots a system, it looks at the MBR for instructions and information on how to boot the disk and load the operating system. Some malware tries to hide here.

- MD5

Message Digest 5. A hashing function used to provide integrity. MD5 creates 128-bit hashes, which are also referred to as MD5 checksums. A hash is simply a number created by applying the algorithm to a file or message at different times. Comparing the hashes verifies integrity.

- MITM

Man in the middle. A MITM attack is a form of active interception allowing an attacker to intercept traffic and insert malicious code sent to other clients. Kerberos provides mutual authentication and helps prevent MITM attacks.

- MOU

Memorandum of understanding. Defines responsibilities of each party, but it is not as strict as an SLA or an ISA. If the parties will be handling sensitive data, they should include an ISA to ensure strict guidelines are in place to protect the data while in transit.

- MPLS

Multi-Protocol Layer Switch. A WAN topology provided by some telecommunications companies. Directs data to nodes using labels rather than IP addresses.

• MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. Microsoft implementation of CHAP. MS-CHAPv2 provides mutual authentication.

• MTBF

Mean time between failures. Provides a measure of a system's reliability and is usually represented in hours. The MTBF identifies the average (the arithmetic mean) time between failures. Higher MTBF numbers indicate a higher reliability of a product or system.

• MTTF

Mean time to failure. The length of time you can expect a device to remain in operation before it fails. It is similar to MTBF, but the primary difference is that the MTBF metric indicates you can repair the device after it fails. The MTTF metric indicates that you will not be able to repair a device after it fails.

- MTTR

Mean time to recover. Identifies the average (the arithmetic mean) time it takes to restore a failed system. Organizations that have maintenance contracts often specify the MTTR as a part of the contract.

- MTU

Maximum Transmission Unit. The MTU identifies the size of data that can be transferred.

- NAC

Network access control. Inspects clients for health and can restrict network access to unhealthy clients to a remediation network. Clients run agents and these agents report status to a NAC server. NAC is used for VPN and internal clients. MAC filtering is a form of NAC.

- NAT

Network Address Translation. A service that translates public IP addresses to private IP addresses and private IP addresses to public IP addresses. Compare to PAT and DNAT.

- NDA

Non-disclosure agreement. Ensures that third parties understand their responsibilities. It is commonly embedded as a clause in a contract with the third party. Most NDAs prohibit sharing data unless you are the data owner.

- NDP

Neighbor Discovery Protocol performs several functions on IPv6. For example, it performs functions similar to ARP, which is used on IPv4. It also performs autoconfiguration of device IPv6 addresses and discovers other devices on the network such as the IPv6 address of the default gateway.

- NetBIOS

Network Basic Input/ Output System (NetBIOS) is a name resolution service for NetBIOS names on internal networks. NetBIOS also includes session services for both TCP and UDP communication. NetBIOS uses UDP ports 137 and 138, and TCP port 139. It can use TCP port 137, but rarely does.

- NFC

Near field communication. A group of standards used on mobile devices that allow them to communicate with other nearby mobile devices. Many credit card readers support payments using NFC technologies with a smartphone.

- NIC

Network interface card. Provides connectivity to a network.

- NIDS

Network-based intrusion detection system. A NIDS is installed on network devices, such as routers or firewalls and monitors network traffic. It can detect network-based attacks.

- NIPS

Network-based intrusion prevention system. An IPS that monitors the network. An IPS can actively monitor data streams, detect malicious content, and stop attacks in progress.

- NIST

National Institute of Standards and Technology. NIST is a part of the U.S. Department of Commerce, and it includes an Information Technology Laboratory (ITL). The ITL publishes special publications related to security that are freely available for download at http:// csrc.nist.gov/ publications/ PubsSPs.html.

- NOP

No operation, sometimes listed as NOOP. NOP instructions are often used in a buffer overflow attack. An attacker often writes a large number of NOP instructions as a NOP sled into memory, followed by malicious code. Some processors use hexadecimal code x90 for NOP so a string of x90 characters indicates a potential buffer overflow attack.

- NOS

Network Operating System. Software that runs on a server and enables the server to manage resources on a network.

- NoSQL

Not only Structured Query Language. An alternative to traditional SQL databases. NoSQL databases use unstructured query language queries instead of traditional SQL queries.

- NTFS

NT File System. A file system used in Microsoft operating systems that provides security. NTFS uses the DAC model.

- NTLM

New Technology LANMAN. Authentication protocol intended to improve LANMAN. The LANMAN protocol stores passwords using a hash of the password by first dividing the password into two 7-character blocks, and then converting all lowercase letters to uppercase. This makes LANMAN easy to crack. NTLM stores passwords in LANMAN format for backward compatibility, unless the passwords are greater than 15 characters. NTLMv1 is older and has known vulnerabilities. NTLMv2 is newer and secure.

- NTP

Network Time Protocol. Protocol used to synchronize computer times.

- OCSP

Online Certificate Status Protocol. An alternative to using a CRL. It allows entities to query a CA with the serial number of a certificate. The CA answers with good, revoked, or unknown.

- OLA

Open License Agreement. A volume licensing agreement allowing an organization to install software on multiple systems.

- OS

Operating system. Includes Windows, Linux, and Apple iOS systems. OSs are hardened to make them more secure from their default installation.

- OSI

Open Systems Interconnection. The OSI reference model conceptually divides different networking requirements into seven separate layers.

- OVAL

Open Vulnerability Assessment Language. International standard proposed for vulnerability assessment scanners to follow.

- P2P

Peer-to-peer. P2P applications allow users to share files such as music, video, and data over the Internet. Data leakage occurs when users install P2P software and unintentionally share files. Organizations often block P2P software at the firewall.

- PaaS

Platform as a Service. A cloud computing technology that provides cloud customers with a preconfigured computing platform they can use as needed. PaaS is a fully managed platform, meaning that the vendor keeps the platform up to date with current patches. Compare to IaaS and SaaS.

- PAC

Proxy Auto Configuration. Method used to automatically configure systems to use a proxy server.

- PAM

Pluggable Authentication Modules. A library of APIs used for authentication-related services.

- PAN

Personal area network. A network of devices close to a single person.

- PAP

Password Authentication Protocol. An older authentication protocol where passwords or PINs are sent across the network in cleartext. CHAP is more secure. PAP uses PPP.

- PAT

Port Address Translation. A form of NAT that translates public IP addresses to private IP addresses, and private IP addresses back to public IP addresses. PAT uses a single public IP address. Compare to DNAT.

- PBKDF2

Password-Based Key Derivation Function 2. A key stretching technique that adds additional bits to a password as a salt. This method helps prevent brute force and rainbow table attacks. Bcrypt is a similar key stretching technique.

- PBX

Private Branch Exchange. A telephone switch used with telephone calls.

- PCAP

Packet Capture. A file that contains packets captured from a protocol analyzer or sniffer.

- PDF

Portable Document Format. Type of file for documents. Attackers have embedded malware in PDFs.

- PEAP

Protected Extensible Authentication Protocol. PEAP provides an extra layer of protection for EAP and it is sometimes used with 802.1x. PEAP requires a certificate on the 802.1x server. See also EAP-TTLS and EAP-TLS.

- PED

Personal Electronic Device. Small devices such as cell phones, radios, CD players, DVD players, video cameras, and MP3 players.

- PGP

Pretty Good Privacy. Commonly used to secure email communications between two private individuals but is also used in companies. It provides confidentiality, integrity, authentication, and non-repudiation. It can digitally sign and encrypt email. It uses both asymmetric and symmetric encryption.

- PII

Personally Identifiable Information. Information about individuals that can be used to trace a person's identity, such as a full name, birth date, biometric data, and identifying numbers such as a Social Security number (SSN). Organizations have an obligation to protect PII and often identify procedures for handling and retaining PII in data policies such as encrypting it.

- PIN

Personal identification number. A number known by a user and entered for authentication. PINs are often combined with smart cards to provide dual-factor authentication.

- PIV

Personal Identity Verification card. A specialized type of smart card used by U.S. federal agencies. It includes photo identification and provides confidentiality, integrity, authentication, and non-repudiation for the users. It is similar to a CAC.

- PKI

Public Key Infrastructure. Group of technologies used to request, create, manage, store, distribute, and revoke digital certificates. Certificates include public keys along with details on the owner of the certificate, and on the CA that issued the certificate. Certificate owners share their public key by sharing a copy of their certificate. A PKI requires a trust model between CAs and most trust models are hierarchical and centralized with a central root CA.

- POP3

Post Office Protocol v3. Used to transfer email from mail servers to clients. POP3 uses TCP port 110.

- POTS

Plain old telephone service. Voice-grade telephone service using traditional telephone wires.

- PPP

Point-to-Point Protocol. Used to create remote access connections. Used by PAP and CHAP.

- PPTP

Point-to-Point Tunneling Protocol. Tunneling protocol used with VPNs. PPTP uses TCP port 1723.

- PSK

Preshared key. A secret shared among different systems. Wireless networks support Personal mode, where each device uses the same PSK. In contrast, Enterprise mode uses an 802.1x or RADIUS server for authentication.

- PTZ

Pan tilt zoom. Refers to cameras that can pan (move left and right), tilt (move up and down), and zoom to get a closer or a wider view.

- RA

Recovery agent. A designated individual who can recover or restore cryptographic keys. In the context of a PKI, a recovery agent can recover private keys to access encrypted data, or in some situations, recover the data without recovering the private key. In some cases, recovery agents can recover the private key from a key escrow.

- RADIUS

Remote Authentication Dial-In User Service. Provides central authentication for remote access clients. RADIUS uses symmetric encryption to encrypt the password packets and it uses UDP. In contrast, TACACS + encrypts the entire authentication process and uses TCP. Diameter is an improvement over RADIUS.

- RAID

Redundant array of inexpensive disks. Multiple disks added together to increase performance or provide protection against faults. RAID help prevent disk subsystems from being a single point of failure.

- RAID-0

Disk striping. RAID-0 improves performance, but does not provide fault tolerance.

- RAID-1

Disk mirroring. RAID-1 uses two disks and provides fault tolerance.

- RAID-5

Disk striping with parity. RAID-5 uses three or more disks and provides fault tolerance. It can survive the failure of a single drive.

- RAID-6

Disk striping with parity. RAID-6 uses four or more disks and provides fault tolerance. It can survive the failure of two drives.

- RAM

Random access memory. Volatile memory within a computer that holds active processes, data, and applications. Data in RAM is lost when the computer is turned off. Memory forensics analyzes data in RAM.

- RAS

Remote Access Service. Provides access to an internal network from an outside source location using dial-up or a VPN.

- RAT

Remote access tool. Commonly used by APTs and other attackers. A RAT gives an attacker full control over a user's system from a remote location over the Internet.

- RC

Ron's Code or Rivest's Cipher. Symmetric encryption algorithm that includes versions RC2, RC4, RC5, and RC6. RC4 is a stream cipher, and RC5 and RC6 are block ciphers.

- RC4

Rivest Cipher 4. A popular stream cipher. RC4 was implemented incorrectly in WEP, causing vulnerabilities. A rare spelling for RC4 is RSA Variable Key Size Encryption Algorithm.

- RDP

Remote Desktop Protocol. Used to connect to remote systems. Microsoft uses RDP in different services such as Remote Desktop Services and Remote Assistance. RDP uses either port TCP 3389 or UDP 3389.

- RFI

Radio frequency interference. Interference from RF sources such as AM or FM transmitters. RFI can be filtered to prevent data interference, and cables can be shielded to protect signals from RFI.

- RFID

Radio frequency identification. RFID methods are often used for inventory control.

- RIPEMD

RACE Integrity Primitives Evaluation Message Digest. A hash function used for integrity. It creates fixed-length hashes of 128, 160, 256, or 320 bits.

- ROI

Return of investment or return on investment. A performance measure used to identify when an investment provides a positive benefit to the investor. It is sometimes considered when evaluating the purchase of new security controls.

- Role-BAC

Role-based access control. An access control model that uses roles based on jobs and functions to define access and it is often implemented with groups (providing group-based privileges). Often uses a matrix as a planning document to match roles with the required privileges.

- RPO

Recovery point objective. The recovery point objective (RPO) refers to the amount of data you can afford to lose by identifying a point in time where data loss is acceptable. It is related to RTO and the BIA often includes both RTOs and RPOs.

- RSA

Rivest, Shamir, and Adleman. An asymmetric algorithm used to encrypt data and digitally sign transmissions. It is named after its creators, Rivest, Shamir, and Adleman. RSA uses both a public key and a private key in a matched pair.

- RSTP

Rapid Spanning Tree Protocol. An improvement over STP. STP and RSTP protocols are enabled on most switches and protect against switching loops, such as those caused when two ports of a switch are connected together.

- RTO

Recovery time objective. An RTO identifies the maximum amount of time it should take to restore a system after an outage. It is derived from the maximum allowable outage time identified in the BIA.

- RTP

Real-time Transport Protocol. A standard used for delivering audio and video over an IP network.

- Rule-BAC

Rule-based access control. An access control model that uses rules to define access. Rule-based access control is based on a set of approved instructions, such as an access control list, or rules that trigger in response to an event such as modifying ACLs after detecting an attack.

- S/ MIME

Secure/ Multipurpose Internet Mail Extensions. Used to secure email. S/ MIME provides confidentiality, integrity, authentication, and non-repudiation. It can digitally sign and encrypt email, including the encryption of email at rest and in transit. It uses RSA, with public and private keys for encryption and decryption, and depends on a PKI for certificates.

- SaaS

Software as a Service. A cloud computing technology that provides applications over the Internet. Web mail is an example of a cloud-based technology. Compare to IaaS and PaaS.

- SAML

Security Assertions Markup Language. An XML-based standard used to exchange authentication and authorization information between different parties. SAML provides SSO for web-based applications.

- SAN

Storage Area Network. A specialized network of high-speed storage devices.

- SCADA

Supervisory control and data acquisition. Typically industrial control systems within large facilities such as power plants or water treatment facilities. SCADA systems are often contained within isolated networks that do not have access to the Internet, but are still protected with redundant and diverse security controls. SCADA systems can be protected with NIPS systems and VLANs.

- SCAP

Security Content Automation Protocol. A set of security specifications for various applications and operating systems. Compliance tools such as vulnerability scanners use these to check systems for compliance.

- SCEP

Simple Certificate Enrollment Protocol. A method of requesting a certificate from a CA.

- SCP

Secure Copy. Based on SSH, SCP allows users to copy encrypted files over a network. SCP uses TCP port 22.

- SCSI

Small Computer System Interface. Set of standards used to connect peripherals to computers. Commonly used for SCSI hard disks and/ or tape drives.

- SDLC

Software Development Life Cycle. A software development process. Many different models are available.

- SDLM

Software Development Life Cycle Methodology. The practice of using a SDLC when developing applications.

- SEH

Structured Exception Handler. Module within an application that handles errors or exceptions. It prevents applications from crashing or responding to events that can be exploited by attackers.

- SELinux

Security-Enhanced Linux. An operating system platform that prevents malicious or suspicious code from executing on both Linux and Unix systems. It is one of the few operating systems that use the MAC model.

- SFTP

Secure File Transfer Protocol. An extension of Secure Shell (SSH) using SSH to transmit the files in an encrypted format. SFTP transmits data using TCP port 22.

- SHA

Secure Hash Algorithm. A hashing function used to provide integrity. SHA-1 uses 160 bits, and SHA-256 uses 256 bits. As with other hashing algorithms, SHA verifies integrity.

- SHTTP

Secure Hypertext Transfer Protocol. An alternative to HTTPS. Rarely used.

- SID

Security identifier. Unique set of numbers and letters used to identify each user and each group in Microsoft environments.

- SIEM

Security Information and Event Management. A security system that attempts to look at security events throughout the organization.

- SIM

Subscriber Identity Module. A small smart card that contains programming and information for small devices such as cell phones.

- SIRT

Security Incident Response Team. A group of experts who respond to security incidents. Also known as CERT, CIRT, or IRT.

- SLA

Service level agreement. An agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels. Organizations use SLAs when contracting services from service providers such as Internet Service Providers (ISPs).

- SLE

Single loss expectancy. The SLE identifies the amount of each loss and is used to measure risk with ALE and ARO in a quantitative risk assessment. The calculation is SLE × ARO = ALE.

- SMTP

Simple Mail Transfer Protocol. Used to transfer email between clients and servers and between email servers and other email servers. SMTP uses TCP port 25.

- SNMP

Simple Network Management Protocol. Used to manage and monitor network devices such as routers or switches. SNMP agents report information via notifications known as SNMP traps, or SNMP device traps. SNMP uses UDP ports 161 and 162.

• SONET

Synchronous Optical Network Technologies. A multiplexing protocol used to transfer data over fiber-optic cable.

• SPIM

Spam over Internet Messaging. A form of spam using instant messaging that targets instant messaging users.

• SPOF

Single point of failure. An SPOF is any component whose failure results in the failure of an entire system. Elements such as RAID, failover clustering, UPS, and generators remove many single points of failure.

- SQL

Structured Query Language. Used by SQL-based databases, such as Microsoft SQL Server. Web sites integrated with a SQL database are subject to SQL injection attacks. Input validation with forms and stored procedures help prevent SQL injection attacks. Microsoft SQL Server uses TCP port 1433 by default.

- SSD

Solid State Drive. A drive used in place of a traditional hard drive. An SSD has no moving parts, but instead stores the contents as nonvolatile memory. SSDs are much quicker than traditional drives.

- SSH

Secure Shell. SSH encrypts a wide variety of traffic such as SCP, SFTP, Telnet, and TCP Wrappers. SSH uses TCP port 22. SSH is a more secure alternative than Telnet.

- SSID

Service Set Identifier. Identifies the name of a wireless network. Disabling SSID broadcast can hide the network from casual users, but an attacker can easily discover it with a wireless sniffer. It's recommended to change the SSID from the default name.

- SSL

Secure Sockets Layer. Used to encrypt data in transit with the use of certificates. SSL is used with HTTPS to encrypt HTTP traffic and can also encrypt SMTP and LDAP traffic.

- SSO

Single sign-on. Authentication method where users can access multiple resources on a network using a single account. SSO can provide central authentication against a federated database for different operating systems. S

- STP

Secure Socket Tunneling Protocol. A tunneling protocol that encrypts VPN traffic using SSL over TCP port 443.

- STP

Shielded twisted-pair. Cable type used in networks that includes shielding to prevent interference from EMI and RFI. It can also prevent data from emanating outside the cable.

- STP

Spanning Tree Protocol. Protocol enabled on most switches that protects against switching loops. A switching loop can be caused if two ports of a switch are connected together.

- SYN

Synchronize. The first packet in a TCP handshake. In a SYN flood attack, attackers send this packet, but don't complete the handshake after receiving the SYN/ ACK packet. A flood guard is a logical control that protects against SYN flood attacks.

- TACACS +

Terminal Access Controller Access-Control System +. Provides central authentication for remote access clients and used as an alternative to RADIUS. TACACS + uses TCP port 49. It encrypts the entire authentication process, compared with RADIUS, which only encrypts the password. It uses multiple challenges and responses.

• TCO

Total cost of ownership. A factor considered when purchasing new products and services. TCO attempts to identify the cost of a product or service over its lifetime.

• TCP

Transmission Control Protocol. Provides guaranteed delivery of IP traffic using a three-way handshake.

• TCP/ IP

Transmission Control Protocol/ Internet Protocol. Represents the full suite of protocols used on the Internet and most internal networks.

- TFTP

Trivial File Transfer Protocol. Used to transfer small amounts of data with UDP port 69. In contrast, FTP is used to transfer larger files using TCP ports 20 and 21.

- TGT

Ticket Granting Ticket. Used with Kerberos. A KDC (or TGT server) issues timestamped tickets that expire after a certain time period.

- TKIP

Temporal Key Integrity Protocol. Wireless security protocol introduced to address the problems with WEP. TKIP was used with WPA but has been deprecated. WPA2 with CCMP is recommended instead.

- TLS

Transport Layer Security. Used to encrypt data in transit. TLS is the replacement for SSL and like SSL, it uses certificates issued by CAs. PEAP-TLS uses TLS to encrypt the authentication process and PEAP-TLS requires a CA to issue certificates.

- TOTP

Time-based One-Time Password. Similar to HOTP, but it uses a timestamp instead of a counter. One-time passwords created with TOTP expire after 30 seconds.

- TPM

Trusted Platform Module. A hardware chip on the motherboard included on many newer laptops. A TPM includes a unique RSA asymmetric key, and when first used, creates a storage root key. TPMs generate and store other keys used for encryption, decryption, and authentication. TPM provides full disk encryption.

- TSIG

Transaction Signature. A method of securely providing updates to DNS with the use of authentication.

- UAT

User Acceptance Testing. One of the last phases of testing an application before its release.

- UDP

User Datagram Protocol. Used instead of TCP when guaranteed delivery of each packet is not necessary. UDP uses a best-effort delivery mechanism.

- UEFI

Unified Extensible Firmware Interface. A method used to boot some systems and intended to replace Basic Input/ Output System (BIOS) firmware.

- UPS

Uninterruptible power supply. A battery backup system that provides fault tolerance for power and can protect against power fluctuations. A UPS provides short-term power giving the system enough time to shut down smoothly, or to transfer to generator power. Generators provide long-term power in extended outages.

- URI

Uniform Resource Identifier. Used to identify the name of a resource and always includes the protocol such as http:// GetCertifiedGetAhead.com.

• URL

Uniform Resource Locator. A type of URI. Address used to access web resources, such as http:// GetCertifiedGetAhead.com. Pop-up blockers can include URLs of sites where pop-ups are allowed.

• USB

Universal Serial Bus. A serial connection used to connect peripherals such as printers, flash drives, and external hard disk drives. Data on USB drives can be protected against loss of confidentiality with encryption. Attackers have spread malware through Trojans.

• UTM

Unified threat management. A security appliance that combined multiple security controls into a single solution. UTM appliances can inspect data streams for malicious content and often include URL filtering, malware inspection, and content inspection components.

- UTP

Unshielded twisted-pair. Cable type used in networks that do not have any concerns over EMI, RFI, or cross talk. If these are a concern, STP is used.

- VDI

Virtualization Desktop Infrastructure. Virtualization software designed to reproduce a desktop operating system as a virtual machine on a remote server.

- VLAN

Virtual local area network. A VLAN separates or segments traffic. A VLAN can logically group several different computers together, or logically separate computers, without regard to their physical location. It is possible to create multiple VLANs with a single switch. You can also create VLANs with virtual switches.

- VM

Virtual machine. A virtual system hosted on a physical system. A physical server can host multiple VMs as servers. Virtualization helps reduce the amount of physical equipment required, reducing overall physical security requirements such as HVAC and power.

- VoIP

Voice over IP. A group of technologies used to transmit voice over IP networks. Vishing is a form of phishing that sometimes uses VoIP.

- VPN

Virtual private network. Provides access to a private network over a public network such as the Internet. VPN concentrators provide VPN access to large groups of users.

- VSAN

Virtual Storage Area Network. A lower-cost alternative to traditional SANs.

- VTC

Video teleconferencing. A group of interactive telecommunication technologies that allow people in two or more locations to interact with two-way video and audio transmissions.

- WAF

Web application firewall. A firewall specifically designed to protect a web application, such as a web server. A WAF inspects the contents of traffic to a web server, can detect malicious content such as code used in a cross-scripting attack, and block it.

- WAP

Wireless access point, sometimes called an access point (AP). Provides wireless clients connectivity to a wired network. Most WAPs use an omnidirectional antenna. You can connect two WLANs together using high-gain directional Yagi antennas. Increasing the power level of a WAP increases the wireless coverage of the WAP. Decreasing the power levels decreases the coverage.

- WEP

Wired Equivalent Privacy. Original wireless security protocol. Had significant security flaws and was replaced with WPA, and ultimately WPA2. WEP used RC4 incorrectly making it susceptible to IV attacks, especially when the attacker used packet injection techniques.

- WIDS

Wireless intrusion detection system. An IDS used for wireless networks.

- WIPS

Wireless intrusion prevention system. An IPS used for wireless networks.

- WLAN

Wireless local area network. Network connected wirelessly.

- WPA

Wi-Fi Protected Access. Replaced WEP as a wireless security protocol without replacing hardware. Originally used TKIP with RC4 and later implementations support AES. Superseded by WPA2. In WPA cracking attacks, attackers capture the four-way authentication handshake and then use a brute force attack to discover the passphrase.

- WPA2

Wi-Fi Protected Access II. Security protocol used to protect wireless transmissions. It supports CCMP for encryption, which is based on AES and is stronger than TKIP, which was originally released with WPA. It uses an 802.1x server for authentication in WPA2 Enterprise mode and a preshared key for WPA2 Personal mode, also called WPA2-PSK.

- WPS

Wi-Fi Protected Setup. Allowed users to easily configure a wireless network, often by using only a PIN. WPS brute force attacks can discover the PIN.

- WTLS

Wireless Transport Layer Security. Used to encrypt traffic for smaller wireless devices.

- XML

Extensible Markup Language. Used by many databases for inputting or exporting data. XML uses formatting rules to describe the data.

- XSRF

Cross-site request forgery. Attackers use XSRF attacks to trick users into performing actions on web sites, such as making purchases, without their knowledge. In some cases, it allows an attacker to steal cookies and harvest passwords.

- XSS

Cross-site scripting. Attackers use XSS to capture user information such as cookies. Input validation techniques on the server-side help prevent XSS attacks by blocking HTML and JavaScript tags. Many sites prevent the use of < and > characters to block cross-site scripting.

- XTACACS

Extended Terminal Access Controller Access-Control System. An improvement over TACACS developed by Cisco Systems and proprietary to Cisco systems. TACACS + is used more commonly.