

# Glossary

## IT Support

---



### Terms and definitions from Course 5

#### #

**802.1X:** It is the IEEE standard for encapsulating EAP or Extensible Authentication Protocol traffic over the 802 networks

**802.1X with EAP-TLS:** Offers arguably the best security available, assuming proper and secure handling of the PKI aspects of it

#### A

**Access Control Entries:** The individual access permissions per object that make up the ACL

**Access Control List (ACL):** It is a way of defining permissions or authorizations for objects

**Accounting:** Keeping records of what resources and services your users access or what they did when they were using your systems

**Activation threshold:** Triggers a pre-configured action when it is reached and will typically block the identified attack traffic for a specific amount of time

**Advanced Encryption Standard (AES):** The first and only public cipher that's approved for use with top secret information by the United States National Security Agency

**Adware:** Software that displays advertisements and collects data

**Analyzing logs:** The practice of collecting logs from different network and sometimes client devices on your network, then performing an automated analysis on them

**Antivirus software:** It monitors and analyze things like new files being created or being modified on the system in order to watch for any behavior that matches a known malware signature

**Application policies:** Defines boundaries of what applications are permitted or not, but they also help educate folks on how to use software more securely

**Asymmetric encryption:** Systems where different keys are used to encrypt and decrypt

**Attack:** An actual attempt at causing harm to a system

**Attack surface:** It's the sum of all the different attack vectors in a given system

**Attack vector:** Method or mechanism by which an attacker or malware gains access to a network or system

**Auditing:** It involves reviewing records to ensure that nothing is out of the ordinary

**Authentication:** A crucial application for cryptographic hash functions

**Authentication server (AS):** It includes the user ID of the authenticating user

**Authorization:** It pertains to describing what the user account has access to or doesn't have access to

**Availability:** Means that the information we have is readily accessible to those people that should have it

## B

**Backdoor:** A way to get into a system if the other methods to get in a system aren't allowed, it's a secret entryway for attackers

**Baiting:** An attack that happens through actual physical contact, enticing a victim to do something

**Bastion hosts or networks:** A server used to provide access to a private network from an external network

**Binary whitelisting software:** It's a list of known good and trusted software and only things that are on the list are permitted to run

**Biometric authentication:** Authentication that uses Biometric data

**Bind:** It is how clients authenticate to the server

**Botnet:** A collection of one or more Bots

**Bots:** Machines compromised by malware that are utilized to perform tasks centrally controlled by an attacker

**Block ciphers:** The cipher takes data in, places that into a bucket or block of data that's a fixed size, then encodes that entire block as one unit

**Brute force attacks:** A common password attack which consists of just continuously trying different combinations of characters and letters until one gets access

# C

**CA (Certificate authority):** It's the entity that's responsible for storing, issuing, and signing certificates. It's a crucial component of the PKI system

**Caesar cipher:** A substitution alphabet, where you replace characters in the alphabet with others usually by shifting or rotating the alphabet, a set of numbers or characters

**CBC-MAC (Cipher block chaining message authentication codes):** A mechanism for building MACs using block ciphers

**CCMP (counter mode CBC-MAC protocol):** A mode of operation for block ciphers that allows for authenticated encryption

**Central repository:** It is needed to securely store and index keys and a certificate management system of some sort makes managing access to storage certificates and issuance of certificates easier

**Certificate-based authentication:** It is the most secure option, but it requires more support and management overhead since every client must have a certificate

**Certificate fingerprints:** These are just hash digests of the whole certificate, and aren't actually fields in the certificate itself, but are computed by clients when validating or inspecting certificates

**Certificate Revocation List (CRL):** A means to distribute a list of certificates that are no longer valid

**Certificate Signature Algorithm:** This field indicates what public key algorithm is used for the public key and what hashing algorithm is used to sign the certificate

**Certificate Signature Value:** The digital signature data itself

**CIA Triad:** Confidentiality, integrity, and availability. Three key principles of a guiding model for designing information security policies

**Client certificates:** They operate very similarly to server certificates but are presented by clients and allow servers to authenticate and verify clients

**CMACs (Cipher-based Message Authentication Codes):** The process is similar to HMAC, but instead of using a hashing function to produce a digest, a symmetric cipher with a shared key is used to encrypt the message and the resulting output is used as the MAC

**Code signing certificates:** It is used for signing executable programs and allows users of these signed applications to verify the signatures and ensure that the application was not tampered with

**Confidentiality:** Keeping things hidden

**Correlation analysis:** The process of taking log data from different systems, and matching events across the systems

**Counter-based tokens:** They use a secret seed value along with the secret counter value that's incremented every time a one-time password is generated on the device

**Cross-site scripting (XSS):** A type of injection attack where the attacker can insert malicious code and target the user of the service

**Cryptanalysis:** Looking for hidden messages or trying to decipher coded message

**Cryptographic hashing:** It is distinctly different from encryption because cryptographic hash functions should be one directional

**Cryptography:** The overarching discipline that covers the practice of coding and hiding messages from third parties

**Cryptology:** The study of cryptography

**Cryptosystem:** A collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service

## D

**Data binding and sealing:** It involves using the secret key to derive a unique key that's then used for encryption of data

**Data exfiltration:** The unauthorized transfer of data from a computer. It's also a very important concern when a security incident happens

**Data handling policies:** Should cover the details of how different data is classified

**Data information tree:** A structure where objects will have one parent and can have one or more children that belong to the parent object

**Decryption:** The reverse process from encryption; taking the garbled output and transforming it back into the readable plain text

**Defense in depth:** The concept of having multiple overlapping systems of defense to protect IT systems

**Denial-of-Service (DoS) attack:** An attack that tries to prevent access to a service for legitimate users by overwhelming the network or server

**DES (Data Encryption Standard):** One of the earliest encryption standards

**Deterministic:** It means that the same input value should always return the same hash value

**DH (Diffie-Hellman):** A popular key exchange algorithm, named for its co-inventors

**Dictionary attack:** A type of password attack that tries out words that are commonly used in passwords, like password, monkey, football

**Distinguished name (DN):** A unique identifier for each entry in the directory

**Distributed Denial-of-Service (DDoS) attack:** A DoS attack using multiple systems

**DNS Cache Poisoning Attack:** It works by tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server

**DSA (Digital Signature Algorithm):** It is another example of an asymmetric encryption system, though its used for signing and verifying data

**Dynamic ARP inspection (DAI):** A feature on enterprise switches that prevents certain types of attacks

## E

**EAP-TLS:** One of the more common and secure EAP methods

**ECDH & ECDSA:** Elliptic curve variants of Diffie-Hellman and DSA, respectively

**Elliptic curve cryptography (ECC):** A public key encryption system that uses the algebraic structure of elliptic curves over finite fields to generate secure keys

**Encapsulating security payload:** It's a part of the IPsec suite of protocols, which encapsulates IP packets, providing confidentiality, integrity, and authentication of the packets

**Encryption:** The act of taking a message (plaintext), and applying an operation to it (cipher), so that you receive a garbled, unreadable message as the output (ciphertext)

**Encryption algorithm:** The underlying logic or process that's used to convert the plaintext into ciphertext

**End-entity (leaf certificate):** A certificate that has no authority as a CA

**Entropy pool:** A source of random data to help seed random number generators

**Entry point:** the act to determine the entry point to figure out how the attacker got in, or what vulnerability the malware exploited

**Evil twin:** The premise of an evil twin attack is for you to connect to a network that is identical to yours but that is controlled by an attacker. Once connected to it, they will be able to monitor your traffic

**Exploit:** Software that is used to take advantage of a security bug or vulnerability

**Extensible authentication protocol (EAP over LAN, or EAPOL):** A standard authentication protocol

## F

**Fail to ban:** A common open source flood guard protection tool

**File-based encryption:** Guarantees confidentiality and integrity of files protected by encryption

**FIPS (Federal Information Processing Standard):** The DES that was adopted as a federal standard for encrypting and securing government data

**Flood guards:** Provide protection against DoS or Denial of Service Attacks

**Forward secrecy:** This is a property of a cryptographic system so that even in the event that the private key is compromised, the session keys are still safe

**Four-Way Handshake:** It is designed to allow an AP to confirm that the client has the correct pairwise master key in a WPA-PSK setup without disclosing the PMK

**Frequency analysis:** The practice of studying the frequency with which letters appear in ciphertext

**Full disk encryption (FDE):** It is the practice of encrypting the entire drive in the system

## G

**GTK (Groupwise Transient Key):** A temporal key, which is actually used to encrypt data

## H

**Hacker:** Someone who attempts to break into or exploit a system

**Half-open attacks:** A way to refer to SYN floods

**Hash collisions:** Two different inputs mapping to the same output

**Hashing (Hash function):** A type of function or operation that takes in an arbitrary data input and maps it to an output of a fixed size, called a hash or a digest

**High value data:** usually includes account information, like usernames and passwords. Typically, any kind of user data is considered high value, especially if payment processing is involved

**HMAC (Keyed-Hash Message Authentication Codes):** It uses a cryptographic hash function along with a secret key to generate a MAC

**Host-based firewalls:** Protects individual hosts from being compromised when they're used in untrusted and potentially malicious environments

**HTTPS:** It is the secure version of HTTP, the Hypertext Transfer Protocol

**Hubs:** Devices that serve as a central location through which data travels through; a quick and dirty way of getting packets mirrored to your capture interface

**Identification:** The idea of describing an entity uniquely

**Impact:** The impact of an incident is also an important issue to consider

**Implicit deny:** A network security concept where anything not explicitly permitted or allowed should be denied

**Injection attacks:** A common security exploit that can occur in software development and runs rampant on the web, where an attacker injects malicious code

**Integrity:** Means keeping our data accurate and untampered with

**Intermediary (subordinate) CA:** It means that the entity that this certificate was issued to can now sign other certificates

**Intrusion detection and intrusion protection systems (IDS/IPS):** Operates by monitoring network traffic and analyzing it

**IPsec (Internet Protocol security):** A VPN protocol that was designed in conjunction with IPv6

**IP source guard (IPSG):** It can be enabled on enterprise switches along with DHCP snooping

**Issuer Name:** This field contains information about the authority that signed the certificate

J

K

**Kerberos:** A network authentication protocol that uses tickets to allow entities to prove their identity over potentially insecure channels to provide mutual authentication

**Kerckhoff's principle:** A principle that states that a cryptosystem, or a collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service should remain secure, even if everything about the system is known except for the key

**Key:** A crucial component of a cipher, which introduces something unique into your cipher

**Key escrow:** Allows encryption key to be securely stored for later retrieval by an authorized party

**Key length:** It defines the maximum potential strength of the system

**Key signing parties:** Organized by people who are interested in establishing a web of trust, and participants perform the same verification and signing

**Key size:** It is the total number of bits or data that comprises the encryption key

**Keylogger:** A common type of spyware that's used to record every keystroke you make

## L

**Lightweight Directory Access Protocol (LDAP):** An open industry-standard protocol for accessing and maintaining directory services

**Logic bomb:** A type of Malware that's intentionally installed

**Logs analysis systems:** They are configured using user-defined rules to match interesting or atypical log entries

**L2TP (Layer 2 Tunneling Protocol):** It is typically used to support VPNs

## M

**MACs (Message Authentication Codes):** A bit of information that allows authentication of a received message, ensuring that the message came from the alleged sender and not a third party masquerading as them

**Malware:** A type of malicious software that can be used to obtain your sensitive information or delete or modify files

**MD5:** A popular and widely used hash function designed in the early 1990s as a cryptographic hashing function

**Meddler in the middle (formerly known as Man in the Middle):** An attack that places the attacker in the middle of two hosts that think they're communicating directly with each other

**MIC (Message Integrity Check):** It is essentially a hash digest of the message in question

**Monitor mode:** It allows to scan across channels to see all wireless traffic being sent by APs and clients



**Multifactor authentication (MFA):** A system where users are authenticated by presenting multiple pieces of information or objects

## N

**Network hardening:** Is the process of securing a network by reducing its potential vulnerabilities through configuration changes, and taking specific steps

**Network separation (network segmentation):** A good security principle for an IT support specialists to implement. It permits more flexible management of the network, and provides some security benefits. This is the concept of using VLANs to create virtual networks for different device classes or types

**Network software hardening:** Includes things like firewalls, proxies, and VPNs

**Network time protocol (NTP):** A network protocol used to synchronize the time between the authenticator token and the authentication server

**NIST:** National Institute of Standards and Technology

**Normalization:** It's the process of taking log data in different formats and converting it into a standardized format that's consistent with a defined log structure

## O

**OAuth:** An open standard that allows users to grant third-party websites and applications access to their information without sharing account credentials

**One-time password (OTP):** A short-lived token, typically a number that's entered along with a username and password

**One-time password (OTP) tokens:** Another very common method for handling multifactor

**OpenID:** An open standard that allows participating sites known as Relying Parties to allow authentication of users utilizing a third party authentication service

**Organizational units (OUs):** Folders that let us group related objects into units like people or groups to distinguish between individual user accounts and groups that accounts can belong to

## P

**Packet sniffing (packet capture):** the process of intercepting network packets in their entirety for analysis

**Pairwise Transient Key (PTK):** It is generated using the PMK, AP nonce, Client nonce, AP MAC address, and Client MAC address

**Password attacks:** Utilize software like password crackers that try and guess your password

**Password salt:** Additional randomized data that's added into the hashing function to generate the hash that's unique to the password and salt combination

**PBKDF2 (Password Based Key Derivation Function 2):** Password Based Key Derivation Function 2

**PCI DSS:** Payment Card Industry Data Security Standard

**Penetration testing:** The practice of attempting to break into a system or network to verify the systems in place

**PGP (Pretty Good Privacy) encryption:** An encryption application that allows authentication of data along with privacy from third parties relying upon asymmetric encryption to achieve this

**Phishing attack:** It usually occurs when a malicious email is sent to a victim disguised as something legitimate

**Physical tokens:** They take a few different forms, such as a USB device with a secret token on it, a standalone device which generates a token, or even a simple key used with a traditional lock

**PIN authentication method:** It uses PINs that are eight-digits long, but the last digit is a checksum that's computed from the first seven digits

**Ping flood:** It sends tons of ping packets to a system. If a computer can't keep up with this, then it's prone to being overwhelmed and taken down

**PKI system:** A system that defines the creation, storage and distribution of digital certificates

**Platform key:** It's the public key corresponding to the private key used to sign the boot files

**Port mirroring:** Allows the switch to take all packets from a specified port, port range, or the entire VLAN and mirror the packets to a specified switch port

Post-fail analysis

**Pre-shared key:** It's the Wi-Fi password you share with people when they come over and want to use your wireless network

**Principle of least privilege:** Helps to ensure that sensitive data is only accessed by people who are authorized to access it

**Privacy policies:** Oversees the access and use of sensitive data

**Promiscuous mode:** A type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode

**Proxy:** Can be useful to protect client devices and their traffic. They also provide secure remote access without using a VPN

**Pseudo-random:** Something that isn't truly random

**Public key authentication:** A key pair is generated by the user who wants to authenticate

**Public key signatures:** Digital signature generated by composing the message and combining it with the private key

Q

R

**RA (Registration Authority):** It is responsible for verifying the identities of any entities requesting certificates to be signed and stored with the CA

**Rainbow table attacks:** To trade computational power for disk space by pre-computing the hashes and storing them in a table

**Rainbow tables:** A pre-computed table of all possible password values and their corresponding hashes

**Random numbers:** A very important concept in encryption because it avoids some kind of pattern that an adversary can discover through close observation and analysis of encrypted messages over time

**Ransomware:** A type of attack that holds your data or system hostage until you pay some sort of ransom

**RC4 (Rivest Cipher 4):** Asymmetric stream cipher that gained widespread adoption because of its simplicity and speed

**Recoverability:** How complicated and time-consuming the recovery effort will be

**Remote attestation:** The idea of a system authenticating its software and hardware configuration to a remote system

**Remote Authentication Dial-in User Service (RADIUS):** A protocol that provides AAA services for users on a network

**Reverse proxy:** A service that might appear to be a single server to external clients, but actually represents many servers living behind it

**Risk:** The possibility of suffering a loss in the event of an attack on the system

**Risk mitigation:** Understanding the risks your systems face, take measures to reduce those risks, and monitor them

**Rogue Access Point (AP) Attack:** An access point that is installed on the network without the network administrator's knowledge

**Rogue DHCP server attack:** An attacker can hand out DHCP leases with whatever information they want by deploying a rogue DHCP server on your network, setting a gateway address or DNS server, that's actually a machine within their control

**Root certificate authority:** They are self signed because they are the start of the chain of trust, so there's no higher authority that can sign on their behalf

**Rootkit:** A collection of software or tools that an admin would use

**RSA:** One of the first practical asymmetric cryptography systems to be developed, named for the initials of the three co-inventors: Ron Rivest, Adi Shamir and Leonard Adleman

## S

**Screen lock:** A security feature that helps prevent unwanted access by creating an action you have to do to gain entry

**Secure boot protocol:** It uses public key cryptography to secure the encrypted elements of the boot process

**Secure channel:** It is provided by IPsec, which provides confidentiality, integrity, and authentication of data being passed

**Secure element:** It's a tamper resistant chip often embedded in the microprocessor or integrated into the mainboard of a mobile device

**Secure Shell (SSH):** A secure network protocol that uses encryption to allow access to a network service over unsecured networks

**Security:** It's all about determining risks or exposure understanding the likelihood of attacks; and designing defenses around these risks to minimize the impact of an attack

**Security information and event management systems (SIEMS):** Form of centralized logging for security administration purposes

**Security keys:** Small embedded cryptoprocessors, that have secure storage of asymmetric keys and additional slots to run embedded code

**Security through obscurity:** The principle that if no one knows what algorithm is being used or general security practices, then one is safe from attackers

**Seed value:** A secret value that is used to initialize a process that is generated by software using one or more values

**Self-signed certificate:** This certificate has been signed by the same entity that issued the certificate

**Serial number:** A unique identifier for their certificate assigned by the CA which allows the CA to manage and identify individual certificates

**Session hijacking (cookie hijacking):** A common meddler in the middle attack

**Session key:** The shared symmetric encryption key using TLS sessions to encrypt data being sent back and forth

**Severity:** Includes factors like what and how many systems were compromised and how the breach affects business functions

**SHA1:** It is part of the secure hash algorithm suite of functions, designed by the NSA and published in 1995

**Shannon's maxim:** It states that the system should remain secure, even if your adversary knows exactly what kind of encryption systems you're employing, as long as your keys remain secure

**Single Sign-on (SSO):** An authentication concept that allows users to authenticate once to be granted access to a lot of different services and applications

**Social engineering:** An attack method that relies heavily on interactions with humans instead of computers

**Software signing certificate:** Trust mechanism where a software vendor can cryptographically sign binaries they distribute using a private key

**Spear phishing:** Phishing that targets individual or group - the fake emails may contain some personal information like your name, or the names of friends or family

**Spoofing:** When a source is masquerading around as something else

**Spyware:** The type of malware that's meant to spy on you

**SQL Injection Attack:** An attack that targets the entire website if the website is using a SQL database

**SSL 3.0:** The latest revision of SSL that was deprecated in 2015

**SSL/TLS Client Certificate:** Certificates that are bound to clients and are used to authenticate the client to the server, allowing access control to a SSL/TLS service

**SSL/TLS Server Certificate:** A certificate that a web server presents to a client as part of the initial secure setup of an SSL, TLS connection

**StartTLS:** It permits a client to communicate using LDAP v3 over TLS

**Steganography:** The practice of hiding information from observers, but not encoding it

**Stream ciphers:** It takes a stream of input and encrypts the stream one character or one digit at a time, outputting one encrypted character or digit at a time

**Subject:** This field contains identifying information about the entity the certificate was issued to

**Subject Public Key Info:** These two subfields define the algorithm of the public key along with the public key itself

**Substitution cipher:** An encryption mechanism that replaces parts of your plaintext with ciphertext

**Symmetric key algorithm:** Encryption algorithms that use the same key to encrypt and decrypt messages

**SYN flood:** The server is bombarded with SYN packets

## T

**TACACS+:** It is a device access AAA system that manages who has access to your network devices and what they do on them

**Tailgating:** Gaining access into a restricted area or building by following a real employee in

**Tcpdump:** It's a super popular, lightweight command-line based utility that you can use to capture and analyze packets

**Threat:** The possibility of danger that could exploit a vulnerability

**Threats & password policies:** Protects Data & IP, Data Protection, Infrastructure Defense, Identity Management, and users

**Ticket granting service (TGS):** It decrypts the Ticket Granting Ticket using the Ticket Granting Service secret key, which provides the Ticket Granting Service with the client Ticket Granting Service session key

**Time-based token (TOTP):** A One-Time-Password that's rotated periodically

**TKIP (Temporal Key Integrity Protocol):** To address the shortcomings of WEP security

**TLS 1.2:** The current recommended revision of SSL

**TLS 1.2 with AES GCM:** A specific mode of operation for the AES block cipher that essentially turns it into a stream cipher

**TLS Handshake:** A mechanism to initially establish a channel for an application to communicate with a service

**TPM (Trusted Platform Module):** This is a hardware device that's typically integrated into the hardware of a computer, that's a dedicated crypto processor

**Transport mode:** One of the two modes of operations supported by IPsec. When used, only the payload of the IP packet is encrypted, leaving the IP headers untouched

**Trojan:** malware that disguises itself as one thing but does something else

**Trusted execution environment (TEE):** It provides a full-blown isolated execution environment that runs alongside the main OS

**Tunnel:** It is provided by L2TP, which permits the passing of unmodified packets from one network to another

**Tunnel mode:** One of the two modes of operations supported by IPsec. When used, the entire IP packet, header, payload, and all, is encrypted and encapsulated inside a new IP packet with new headers

## U

**Unbind:** It closes the connection to the LDAP server

**Username and password authentication:** Can be used in conjunction with certificate authentication, providing additional layers of security

**U2F (Universal 2nd Factor):** It's a standard developed jointly by Google, Yubico and NXP Semiconductors that incorporates a challenge-response mechanism, along with public key cryptography to implement a more secure and more convenient second-factor authentication solution

## V

**Validity:** This field contains two subfields, Not Before and Not After, which define the dates when the certificate is valid for

**Vendor risk review:** Questionnaire that covers different aspects of their security policies procedures and defenses

**Version:** What version of the X.509 standard certificate adheres to

**Viruses:** The best known type of malware

**VPN (Virtual Private Network):** A secure method of connecting a device to a private network over the internet

**VPNs:** Commonly used to provide secure remote access, and link two networks securely

**Vulnerability:** A flaw in the system that could be exploited to compromise the system

**Vulnerability scanner:** Detect lots of things, ranging from misconfigured services that represent potential risks, to detecting the presence of back doors and systems

## W

**Web of trust:** It is where individuals instead of certificate authorities sign other individuals' public keys

**WEP (Wired Equivalent Privacy):** First security protocol introduced for Wi-Fi networks

**Wireshark:** It's another packet capture and analysis tool that you can use, but it's way more powerful when it comes to application and packet analysis, compared to tcpdump

**Worms:** They are similar to viruses except that instead of having to attach themselves onto something to spread, worms can live on their own and spread through channels like the network

**WPA (Wi-fi protected access):** Designed as a short-term replacement that would be compatible with older WEP-enabled hardware with a simple firmware update

**WPA2 Enterprise:** It's an 802.1x authentication to Wi-Fi networks

**WPS (Wifi Protected Setup):** It's a convenience feature designed to make it easier for clients to join a WPA-PSK protected network

## X

**X.509 standard:** It is what defines the format of digital certificates, as well as a certificate revocation list or CRL

**XTACACS:** It stands for Extended TACACS, which was a Cisco proprietary extension on top of TACACS

## Y



# Z

**0-Day Vulnerability (Zero Day):** A vulnerability that is not known to the software developer or vendor, but is known to an attacker