SY0-701

Security + SY0-701

SY0-701 Domains:

- General Security Concepts
- Threats, Vulnerabilities, and Migrations
- Security Architecture
- Security Operations
- Security Program Management and oversight

- **Confidentiality** protects information and systems from unauthorized access. However, can be undermined by disclosure attacks making sensitive information available to individuals without the owner's consent.

- **Integrity**, protects the information from unauthorized modification, can be undermined by alteration attacks which's either seek to alter information or a service disruption affecting the data stored in the system.
- **Availability** ensures that information and systems are available for authorized users when needed. Denial of service attacks seek to undermine availability as they overwhelm a system or cause it to crash.

Authentication, authorization, and accounting (**AAA**)

AAA is part of the Access Control Process, which has 3 steps:

1. **Identification**, the user claims to have an identity, they don't have any proof, the user could be making a false claim. (username)
2. **Authentication**, the user proofs the identity (password)
3. **Authorization**, determines if you are allowed to access the system (permissions)

An additional step is **Accounting**; it allows administrators to track user activity from logs.

TorosTechnology.com

Security Controls

Are procedures and mechanisms that an organization puts in place to manage security risks.

Defense in depth principle**.** Multiple overlapping controls for one objective.

We can group controls by:

Their purpose or type: designed to correct, deter, direct or compensate for security issues.

- Preventive controls: stops a security issue from occurring in the first place (firewall)

- Detective controls: identifies that a potential security issue has taken place (IDS)
- Corrective control: Remediates security issues that have already occurred (Restoring information from back up)
- Deterrent control: prevents an attacker from seeking to violate security policies.
- Directive controls: Inform users what to do to achieve security objectives.
- Compensating controls: fills a known gap in a security environment.

Mechanism of action: technical, operational, managerial and physical controls

- Technical controls: *carried out by technology*, they use technology to achieve security control objectives (firewall, IPS, antivirus)
- Operational controls: *carried out by people*, use human-driven processes to manage technology in a secure manner (User access, log monitoring, security awareness training)
- Managerial controls: they improve the risk management process itself (conducting regular risks & security assessments, change management, project management)
- Physical controls: impact the physical world (fences, perimeters, lightnings)

TorosTechnology.com

Gap analysis

Is a core strategic planning tool, where you bring the below states together to develop a road map for remediation:

Desired state: What controls would you like to have in place to meet security objectives? Internal requirements such as a Policy for having sensitive data encrypted or using MFA to access that data. Regulatory requirements governing your business or practice.

Current state: A security assessment done internally or by an external security consultant.

Zero Trust Network Access (ZTNA) & Secure Access Service Edge (SASE)

Zero trust is the most established, it applies the principle of least privilege to network access, no user or device should be granted access solely based upon on location on the network. ZTNA has 2 planes:

- Control Plane: where network policy decisions are made
- Data plane: where those decisions are enforced, access are granted based on decisions made at the control plane.

ZTNA Capabilities:

Adaptive Identity, it supports all types of users, considering that some users roles might have evolved as the environment changed.

Threat Scope Reduction, supports agility and complexity while keeping the environment as simple as possible.

Physical Access Control

Physical access control creates a security perimeter to prevent and detect intrusions before an intruder gains access to interior secured areas. The purpose of the types of locks below is to restrict access to the user in authorised access list only.

Types:

- Preset locks (traditional physical locks), the lock is preset to open with the correct key, if key is lost or stolen preset lock should be replaced.
- Cypher locks (combination locks), a combination of number/ letters in an electronic keypad to open the lock, used when many people require access.
- Biometrical locks use a physical characteristic of a person to permit access, such as fingerprint, retinal pattern or voice print to unlock the lock.
- Card based locks, required the user to present a card with a magnetic stripe or proximity access card.
- Access control vestibules, they prevent tailgating by allowing one person at the time in a vestibule, suing cameras, sensors to verify only one person is the vestibule.

Toros Technology.com

Facility Monitoring types:

Motion sensors, they detect movement through a room

Noise sensors, they detect unexpected s sounds such as glass breaking

Pressure sensors, detect footsteps in a surface

Microwave sensors, detect the presence of people using microwaves

Ultrasonic sensors, detect presence of people using high frequency sound waves.

Video surveillance act as both deterrent and detective controls, can be cctv (suing coax or power cable) or IP cameras (using network cables).

- Some cameras use motion detectors to detect movement of objects.
- Some cameras use infrared technology to identify the heat
- Video surveillance also provides evidence in security investigations.

Physical barriers:

- Fences, they prevent physical intrusions on foot or by vehicle.
- Cages, may be used to safeguard data center equipment.
- Bollards, block vehicles
- Lighting, increases the likelihood of intruder detection
- Signs, stating that trespassing is prohibited.
- Industrial camouflage, which seeks to hide sensitive facilities in nondescript locations. However, the use of drones and UAVs are a challenge as facilities need to be aware of ground and air as well.

Security guards

Security guards which provide human judgement to grant access to those that are authorized visitors, some facilities use overt uniformed guards to project security and authority, some guards might be guarded

Robot sentries, might replace security patrol.

Two person integrity, two people must enter sensitive areas together.

Two person control, requires two individuals to carry out any action, as an example, 2 keys to launch a nuclear missile.

TorosTechnology.com

Deception technologies

Deception technologies allow analyst to be a step ahead of the attackers. Analysts use a range of tools to detect unauthorized access to systems:

- Darknets: administrators set aside a portion of unused IP addresses (no legitimate systems use those addresses), if a monitor system detects any activity to those addresses is very likely that's attackers are performing network reconnaissance.
- Honeytokens are any type of data that you might falsify and put in an area for an attacker to find, the purpose can give us information of who is attacking the network.
- Honeyfiles, are files that are created to resemble sensitive data; however, they just contain garbage or fake data
- Honeypots, are systems put on a network with the purpose of intentionally attracting attackers, they fool the attackers thinking they have compromised a sensitive system, they send fake telemetry to the attacker and real to the security team.
- Honeynets, are multiple honeypots in the same network.
- DNS Sinkhole, when the client requests the IP address of a FQDN, a response with incorrect or invalid information will be given, it captures traffic to know malicious domains used by attackers.

ToroTechnology.com

Change Management

Change Management it protects organizations from the unforeseen consequences of change; it plans, implements and monitors modifications to systems and processes to minimise risks and maximise benefits, it involves well defined processes:

- Approval process: ensures that changes are carefully evaluated, authorised and documented reducing the risk of unauthorised modifications
- Change ownership: define who is responsible for implementing and overseeing each change.

- Clear ownership: helps to maintain accountability and ensures that changes are managed effectively from start to finish.
- Identifying and engaging stakeholders, it helps to gain valuable insight and perspectives, ensures that changes are truly evaluated before implementation.
- Conducting an impact analysis, assess the potential consequences of a change such as risks, vulnerabilities and conflicts that might arise.
- Testing verifies that the proposed change will work as intended while minimising disruptions or security breaches, enables organizations to make adjustments before moving forward
- Have a back-out plan in the event of issues, minimising the impact of the failed change.
- Deploy changes during planned maintenance windows, minimises disruptions to normal business operations
- Adhering to SOPs, (Standard Operating Procedures), they outline the best practices, guidelines and step to follow to maintain a high level of security and efficiency.

Technical Implications:

- Allow/Deny lists: control access to resources.
- Restricted activities: disabling unnecessary services or restricting privileges
- Downtime: temporary interruptions might be needed, and communication is essential to minimise interruptions
- Service and application restarts: ensure that change take effects and systems continue to function as intended.
- Legacy applications: We need to ensure that modifications don't compromise the functionality of these applications.
- Dependencies on other systems: understanding these dependencies is crucial to avoid disruptions.

Version control: it maintains a record of changes which provides traceability, documenting the purpose, scope and details of every modification.

Updated documentation ensures that all stakeholders have access to accurate documentation

TarosTechnology.com

TorosTechnology.com

Cryptography

Cryptography is the use of mathematic algorithms to transform information into an encrypted form that is not readable by unauthorized individuals, it depends in two basic operations:

- Encryption: Converts information from plaintext to ciphertext
- Decryption: uses an algorithm (mathematical instructions) to transform encrypted information to readable information.

Encryption algorithms operation process:

- Input P: Plaintext message
- Input K: Encryption Key
- Then, performs encryption using the plaintext and the encryption key.
- Output C: Provides an output, the encrypted cyphertext

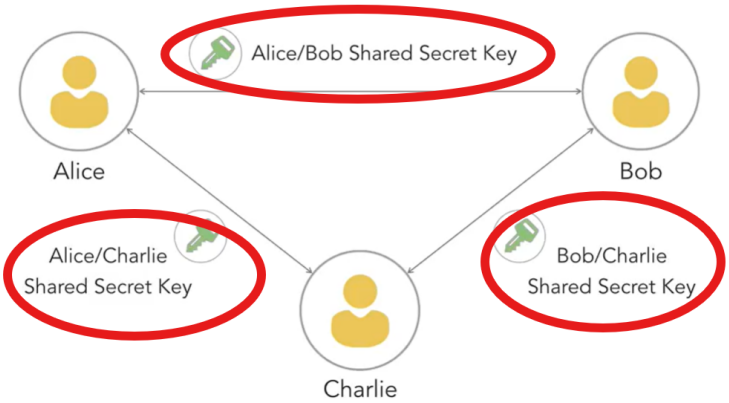
Decryption algorithms operations process:

- Input C: encrypted message / encrypted cyphertext
- Input K: decryption key
- Then, performs decryption using cyphertext and decryption key
- Output P: plaintext message

TorosTechnology.com

Symmetric and Asymmetric cryptography

Symmetric Encryption, also known as shared secret encryption algorithms, the encryption and decryption use the same key



$$\frac{n(n-1)}{2}$$

Keys Required

Group Size	Symmetric Keys
2	1
3	3
10	45
100	4,950
1,000	499,500
10,000	49,995,000

Asymmetric Encryption, use different keys for encryption and decryption, these algorithms are also known as public key cryptography, it's slower than symmetrical but it solves the problem for creating keys for larger organizations, it uses keypairs: (**EXAM TIP:** everything that is encrypted with one key/ public key can be decrypted with the other key from the same pair/private key)

- Public Key, freely distributed to communication partners by users they wish to communicate with, encrypts the message
- Private Key, users kept secret, it decrypts the message by the recipient.

1. Mean time to Failure (MTTF) is the average time a nonrepairable component will last.
2. Mean time between Failures (MTBF) time between failures, on average
3. Mean time to repair (MTTR), average time taking to recover, on average

Keys Required

Group Size	Symmetric Keys	Asymmetric Keys
2	1	4
3	3	6
10	45	20
100	4,950	200
1,000	499,500	2,000
10,000	49,995,000	20,000

Goals of cryptography

1. Confidentiality ensures that unauthorised individuals are not able to gain access to sensitive information, and even if a third party intercepts the communication, they won't be able to read it due its encryption. There are 3 different states of data where encryption is used:
   a. Data at rest, is data store in a storage device (hard drive)
   b. Data in transit, transmitted over a network connection between 2 systems.
   c. Data in use, stored in memory and is actively used by an application

2. Integrity, protects messages from unauthorised modifications.

3. Authentication, proof of identity claims.

4. Obfuscation, hiding sensitive data, as an example replacing the security social number with a unique value.

5. Non-repudiation, the recipient of the message can proof to a third party that the message was sent by the sender, it's only possible with asymmetrical cryptography because the sender had the sole Public Key, digital signatures provide non-repudiation,

TorosTechnology.com

Choosing encryption algorithms

EXAM TIP never use your own encryption algorithm unless you really know what you are doing, encryption requires careful thought, uses sophisticated mathematical algorithms

*If a site claims that they have a secret confidential algorithm better to stay away as it goes again cyber security principle of Security through Obscurity, where no one knows how it works.

You should choose an encryption algorithm that is proven to be secure, they are usually published and open for inspection by the security community.

When you choose you might be able to select the key length, the longer the key the more secure will the information be. However, you give up speed when the key is longer.

Mitigation ends with Stability; how will we implement the algorithm that we've chosen.

Cryptographic lifecycle

The cryptographic lifecycle manages the use of encryption materials over time, as cryptographic algorithms age, they often become insecure.

The NIST (National Institute of Standards and Technologies) offer a 5 stage cryptographic lifecycle:

1. Initiation, the organization realises they need a new cryptographic system, and they start to gather the requirements for that system, ensuring:
   a. Integrity, the correctness of the keys should be preserved and security mechanisms ensured. Authentication, Authorization and Non-repudiation should be supported.
   b. Availability, the security mechanisms should be available at least 95.5% of the time, response to suspected compromise should be minimised
   c. Digital signatures
2. The organization develop and acquires the cryptographic system finding an appropriate combination of software, hardware and algorithms to meet objectives.

ForosTechnology.com

3. Implementation and Assessment the organization configure the system for use and assess if it properly meets their security objectives.
4. Operations and Maintenance, the organization ensures the continued secure operation of the cryptographic system
5. Sunset, when the system is no longer viable the organization phases out the system and destroy/archive keying material

Data de-identification

Deidentification is the process that organizations use to protect themselves again accidental disclosures of personal information by removing all identifying information from datasets (when that information is not necessary to meet business requirements). Information to be removed can be names, social security numbers or any other obvious identifiers.

If we want to completely deidentify we also need to consider the below identifiers that when combined could uniquely identify 87% of the people in the US:

- Zip Codes
- Date of birth
- Gender

Instead of Deidentifation we should be implementing Anonymization, removing the possibility of identification.

The HIPPA (Health Insurance Portability and Accountability Act) De-Identification Standard offers 2 pathways to clear a dataset:

1. Statisticians that analyse your data, includes the possibility of accidental disclosure.
2. Safe Harbour, the removal of 18 identifiers.

TorosTechnology.com

Data obfuscation

Transforms personally identifying information to a form where is no longer possible to tie to an individual person. A few tools that help data obfuscation are:

- Hashing, replaces sensitive fields with hash values (sha-256 or MD5 as an example). However, a breach could occur by using a Rainbow Table attack that compares a hash with precomputed hashes.
- Salting, uses random values to defeat rainbow tables, makes precomputation of hashes impossible.
- Tokenization, replaces sensitive fields with a random and unique identifier using a lookup table (this lookup table should be kept secure)
- Masking, replaces sensitive information from a file with blank values.

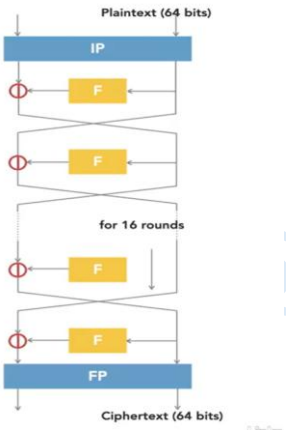
TorosTechnology.com

Symmetric Cryptography

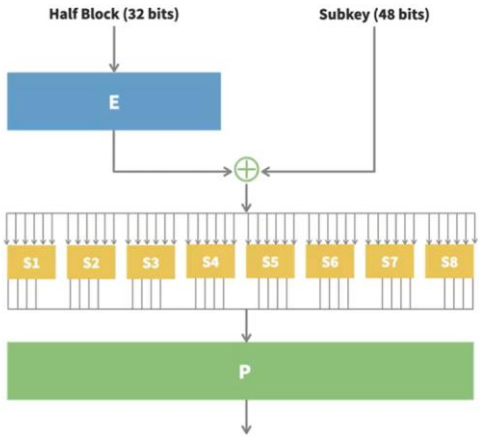
Transforms personally identifying information to a form where is no longer possible to tie to an individual person

Data Encryption Standard (DES)

Nowadays is considered insecure, operates in 64bit blocks using a 56-bit key (2048 bits or higher is considered secure), it was designed by IBM in the 70's to serve as federal encryption standard, DES uses an encryption called the Feistel function for **16 rounds of encryption.**

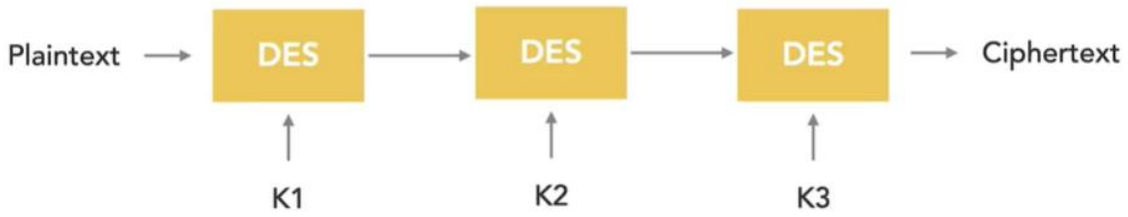


In a single round: Each F box takes half of the 64 bit input (32 bits) and combines with a piece of the encryption key called Subkey (48 bits), the output is then broken up into 8 functions called S (substitution) boxes with a different substitution cipher, the combined 8 substitution boxes form a P (Permutation/ Transposition) box.



Triple DES - 3DES

Considered weak and it's being phased out. Three rounds of DES provide stronger security than DES, it applies DES three times with three keys: K1, K2 & K3. It also operates on 64-bit blocks but provides 112 bits encryption strength if used with 3 different keys.



DES Key options

1. Keying Option 1, is having 3 different keys, this is the strongest option providing an encryption with a strength of 112 bits
2. Keying Option 2, Key 1 and Key 3 are the same, only K2 is different, resulting in an encryption strength of 80 bits.
3. Keying Option 3, All three keys are the same, emulating the standard DES algorithm, is only included for backwards compatibility with DES.

EXAM TIP: Why triple DES, why don't we just use DES twice? The reason why is that we could be victims of meet-in-the-middle-attack

In a meet-in-the-middle attack against DES, an attacker tries to find a pair of keys that produce a specific known plaintext-ciphertext pair. The attacker encrypts the plaintext with all possible keys and stores the results in a table. Then, they decrypt the ciphertext with all possible keys and match the results from both processes to find a pair of keys that yield the desired known plaintext-ciphertext pair. This attack shows that using two separate keys for encrypting and then decrypting a message is not significantly more secure than using a single key, as the attacker can find a pair of keys that achieves the same result as a single key.

AES, Blowfish, and Twofish

Moderns' symmetric algorithms provide strong security

AES (Advanced encryption standard) Like DES, AES uses substitution and transposition to achieve a strong encryption, it uses the same password to encrypt and decrypt the file; block cipher is operating on 128-bit blocks, it allows you to choose key lengths of 128, 192 or 256 bit key

Blowfish is a public domain algorithm, (no longer considered secure) it was designed to replace DES, uses the Feistel network, it combines substitution and

transposition operations, it works on 64bit blocks as a block cipher, you can use any key length between 32 bits and 448 bits

Twofish, (EXAM TIP: considered secure today) works on blocks of 128bits, using key lengths of 128, 192 and 256 bits.

Steganography

Hides data within another file which is invisible in plain sight. It works with text, audio and video.

Asymmetric Cryptography

It gives each user a pair of keys to use for encryption and decryption operations.

RSA (Rivest, Shamir, Adleman)

Is one of the earliest asymmetric cryptographic algorithms (1997) which is still in use today. EXAM TIP: the users create RSA key pairs using two large prime numbers and then RSA uses these numbers to create a public key and a private key. Their key length is between 1024 (not secure as they have been some attacks, safe keys are 2048 or higher) and 4096 bits.

- Sender encrypts the message with the recipient's public key
- Recipient decrypts the message using their own private key

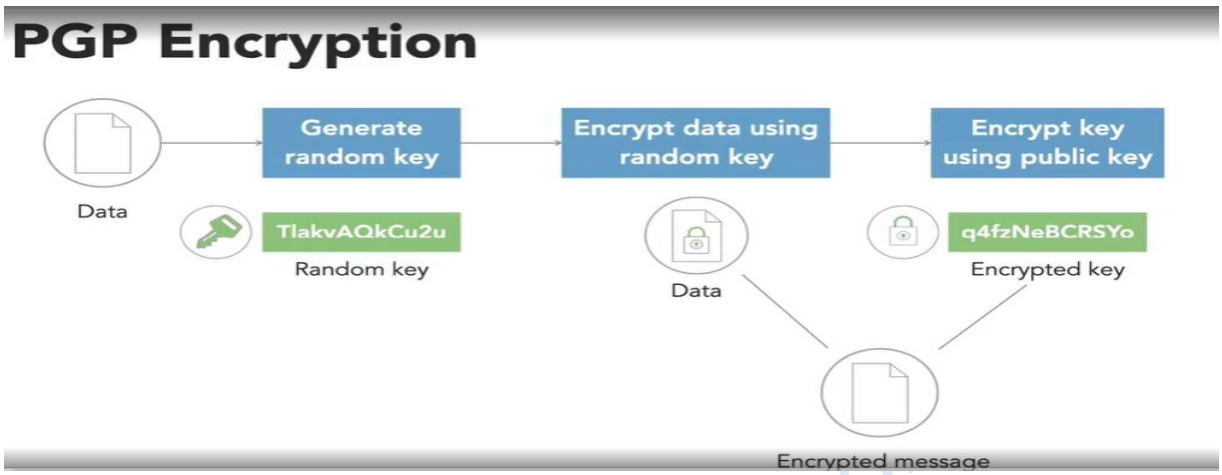
RSA Drawbacks:

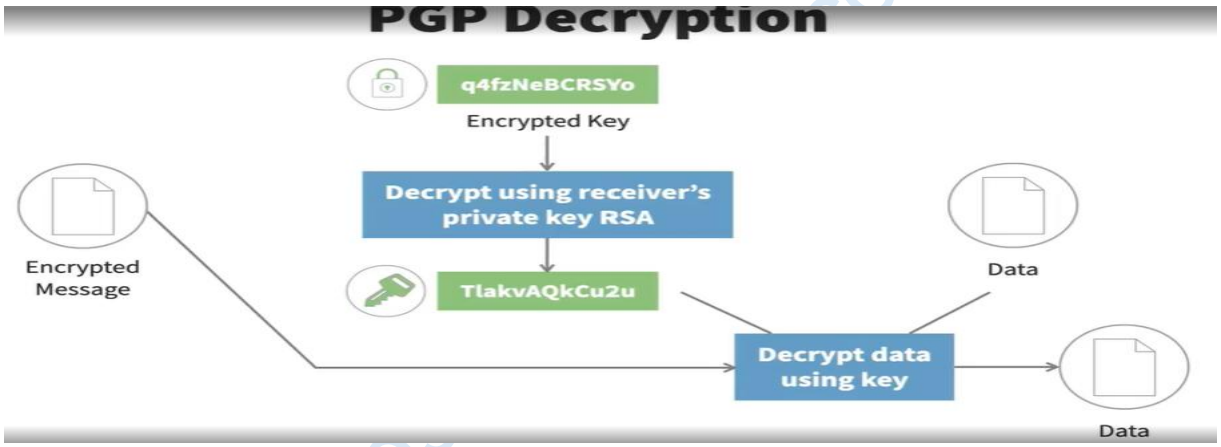
- It's slow
- Its patent has expired.

PGP (Pretty Good Privacy) & GnuPNG

TorosTechnology.com

Is still widely used and is open source, it combines symmetric and asymmetric cryptography, it's not an encryption algorithm itself, it's a framework for using other encryption algorithms, the user of PGP needs to use other symmetric and asymmetric algorithms.





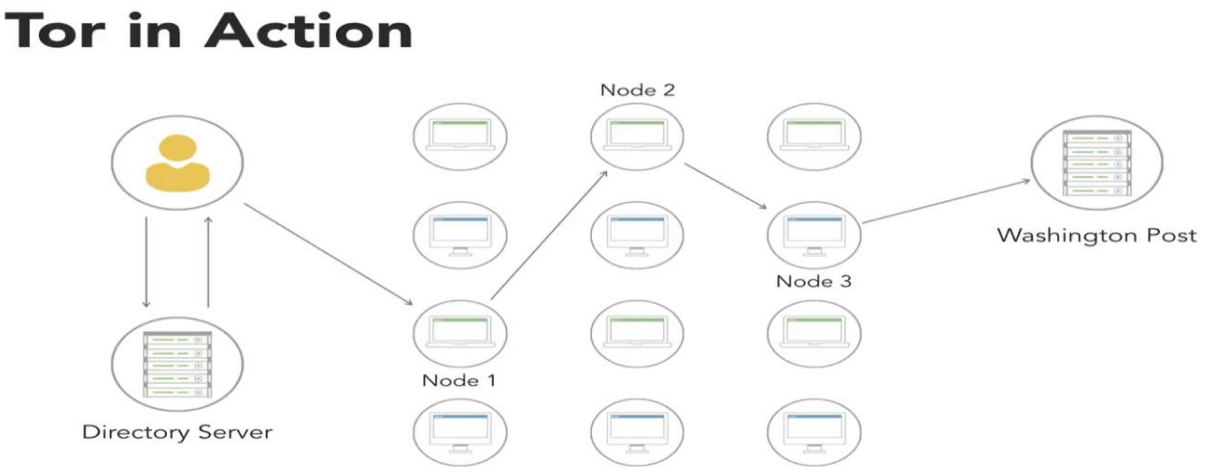
Elliptic Curve and Quantum Cryptography

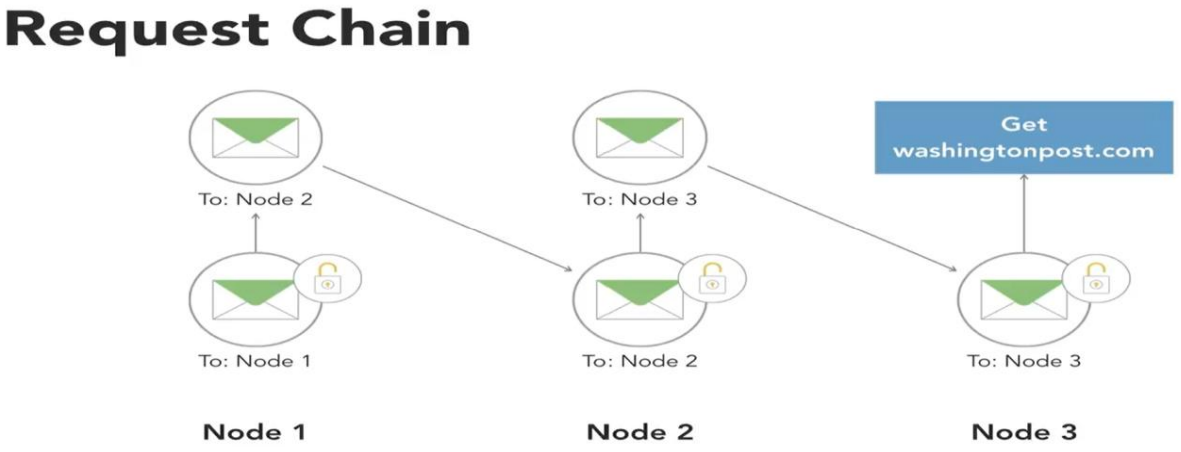
EEL (Elliptic Curve Cryptography) EXAM TIP: does not depend on prime number factorization; it uses the elliptic curve discreet logarithm problem. EEL can't protect against Quantum attacks

Quantum Computing, uses quantum mechanics to perform computing tasks

Tor (The onion router)

Provides anonymous secure way to access the internet, it uses a technology known as Perfect Forward Secrecy, it uses encryption and relay nodes (usually 3) to hide the true source and destination, each of those nodes only knows the identity of the node before and after it.





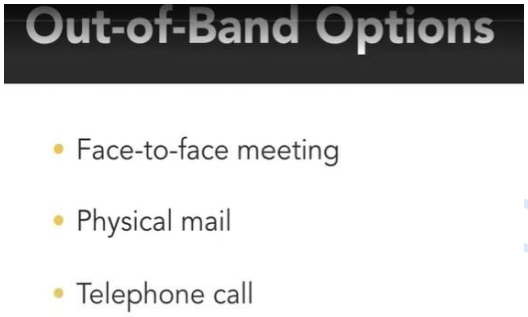
TorosTec

Key Management

It gives each user a pair of keys to use for encryption and decryption operations

Key Exchange

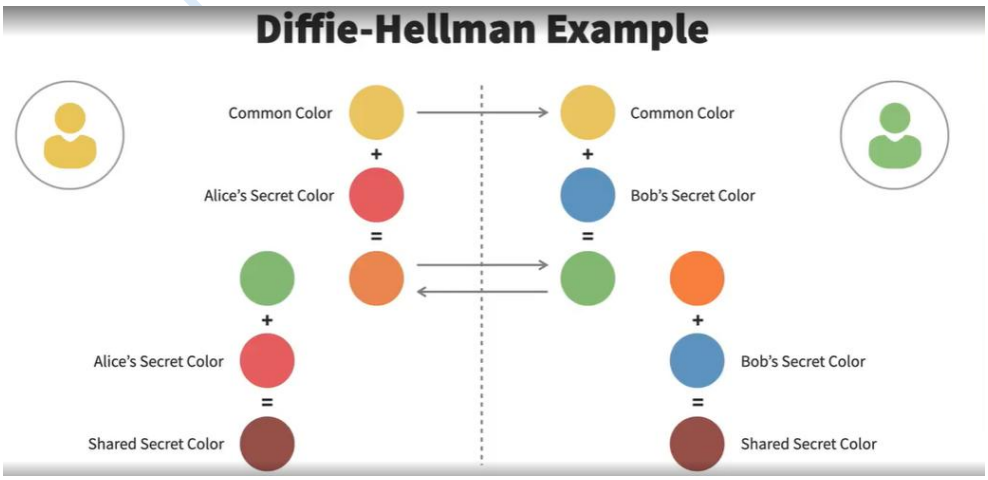
Out-of-band key exchange, the sender and receiver exchange the key in a way both trust and uses a different communications channel. However, this way to exchange the key is difficult and time consuming. Face-to-face can be impossible if there is a great distance between sender and receiver, physical mail might take a few days, and it's very difficult to exchange a key over the phone.

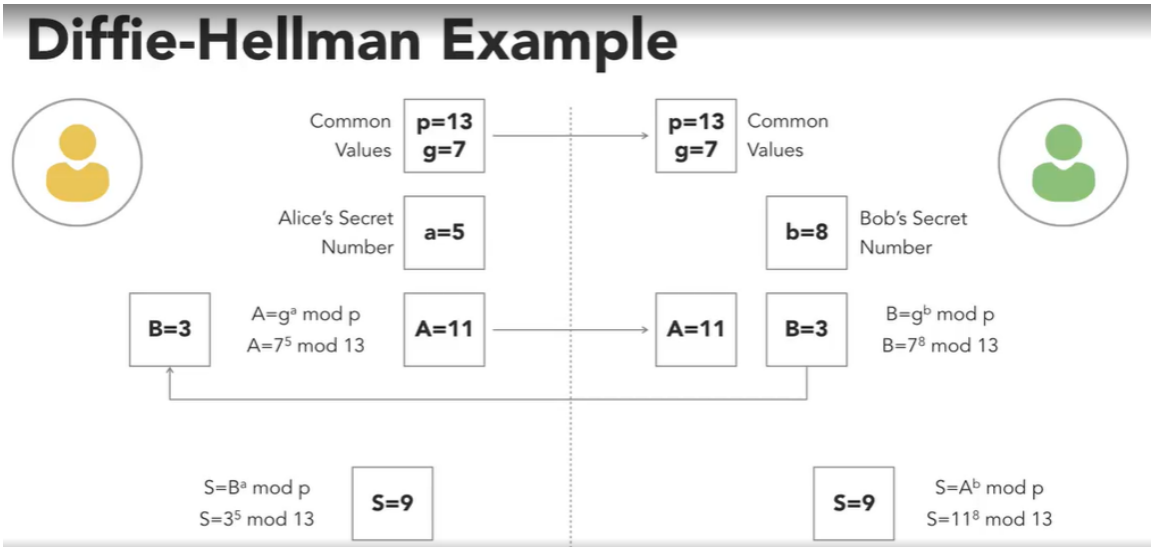


The solution to this is In-band Key Exchange that allows the sender and receiver to exchange the secret key over the network even if there is no secure way to do that.

Diffie-Hellman Algorithm

Invented in 1976, it solves the key exchange for symmetric encryption





There is a variant to the Diffie-Hellman algorithm, called The Elliptic-Curve Diffie-Hellman algorithm ECDH uses a similar approach but relies upon the complexity from the elliptic curve.

Key escrow

Allows governments to access keys through a court order, the clipper chip never was adopted because of opponents and security flaws.

Microsoft Windows Encrypting File System provides the use of a recovery agent (using a master key) in case the user has forgotten the paraphrase

Key stretching

Takes a password and uses mathematical techniques to strengthen it preventing to be cracked. Combines 2 techniques:

- Salting: Adds value to the encryption key.
- Hashing: adds time to the verification process by requiring more math

An algorithm used for key stretching is Password-Based Key Derivation Function v2 (PBKDF2), the salt-hash process should be repeated at least 4000 times.

Bcrypt uses blowfish cipher + salting to stretch the key.

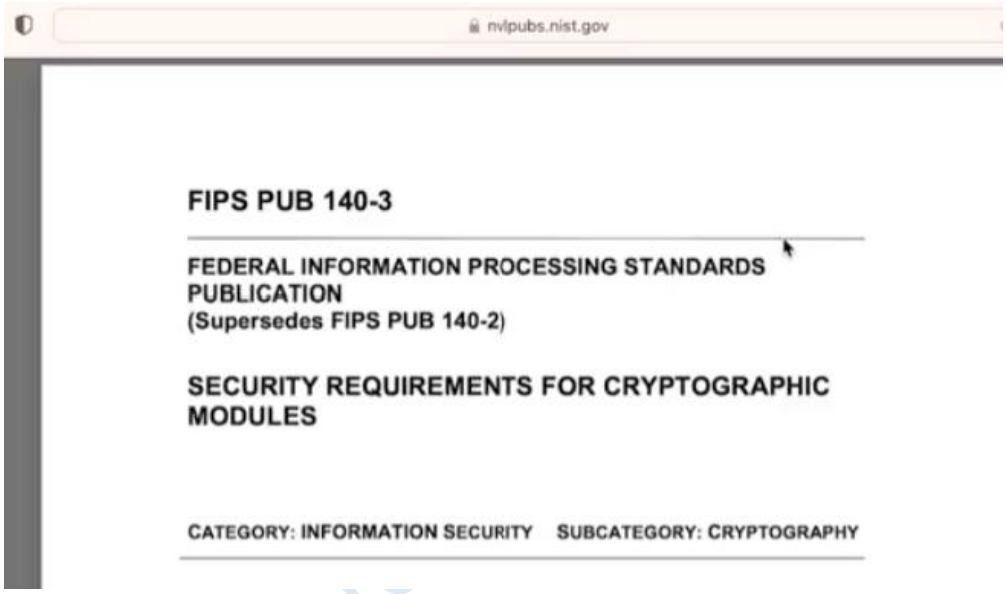
Toros Technology.com

Hardware Security Modules (HSMs)

Are special computer devices (expensive to purchase) that manage encryption keys and perform cryptographic operations.

Cloud Service Providers use HSM for management of their own encryption keys.

US Federal government agencies using HSMs need to abide by FIPS PUB 140-3



Security Levels for US Federal agencies:

FIPS 140-2 Security Levels

Level	Controls
Security Level 1	Standard operating systems, no physical security
Security Level 2	EAL2 software and firmware, tamper-evident seals
Security Level 3	EAL3 software and firmware, tamper-resistant controls
Security Level 4	EAL4 software and firmware, strict physical security

Public Key Infrastructure

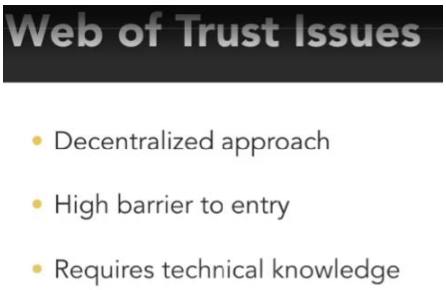
The two parties must be sure:

- they are really communicating with each other and neither is an imposter
- Nobody is eavesdropping the key exchange

Trust Models

Trust Models help us to determine that the parties are who they claim, and neither is an imposter. The models are:

- In person exchange
- Web of Trust (WOT), It relies on indirect relationships (the ones in LinkedIn), participants digitally sign the public keys of people they know personally.
- Public Key Infrastructure (PKI)



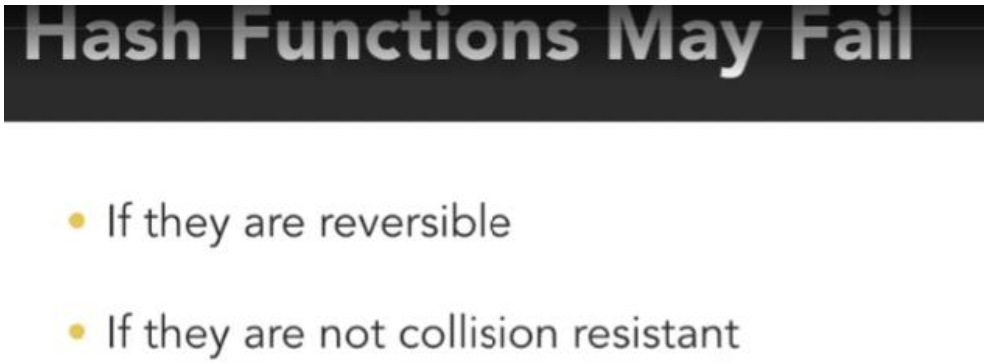
PKI and digital certificates

TutorsTechnology.com

PKI depends on highly trusted certificate authorities (CAs), which are third party organizations that verify the identity of individuals or organizations and then issue digital certificates containing identity information and a copy of the subject public key.

Hash Functions

Hash functions are one-way functions; they can't be reversed; the output will always be the same length regardless of the input size. They are used with asymmetric cryptography for digital signatures and digital certificates.



EXAM TIP: make sure you can identify the common hash functions and its details:

- MD5 (Message Digest 5) No longer secure because is not collision resistant, 1991, created to replace MD4 which was insecure, 128-bit hash
- SHA (Secure Hash Algorithm) for use in federal computer applications. SHA-1 insecure = 160-bit hash value, SHA-2 insecure consists of six hash functions outputting 224,256,384 and 512-bit hashes, SHA-3 2015 it produces a hash of any desired length
- RIPEMD Race Integrity Primitives Evaluation Message Digest, is an alternative to government sponsored hash functions, produces 128 insecure, 160 secure = bitcoin transactions,256,320-bit hashes
- HMAC Hash-based Message Authentication Code, combined symmetric cryptography and hashing, provides authentication and integrity

  Create and verify message authentication code by using a secret key in conjunction with a hash function

Digital Signatures

They provide an electronic counterpart to physical signatures; they use asymmetric cryptography to achieve: integrity authentication and nonrepudiation.

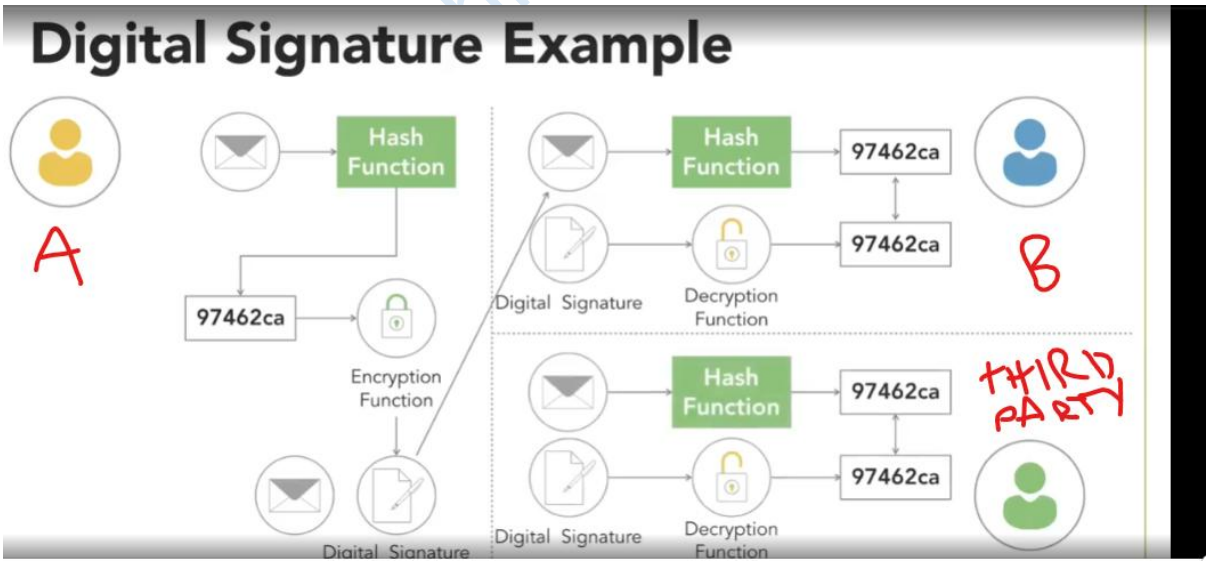
However, does not provide confidentiality, as the sender should be encrypting the message with the recipient's public key.

They are:

- Collision resistant hash function, no 2 inputs produce the same output
- Key pairs = asymmetric cryptography. However, in this case private key is used for encryption and the public key is used to decrypt

The signed message recipients know:

- The owner of the public key is the person who signed the message
- The message was not altered after being signed
- The recipient can prove his identity to a third part



Digital Signatures Standard

Is a US federal standard for appropriate digital signatures algorithms.

FIPS 186-5

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS 186-4)

Digital Signature Standard (DSS)

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

The DDS approves 3 algorithms:

1. RSA (Rivet, Shamir, Aldeman)
2. ECDSA (Elliptic Curve)
3. EdDSA (Edwards Curve)

TorosTechnology.com

How CAs create Digital Certificates

Digital certificates follow the x.509 standard created by ITU.

Certificate Revocation

There are 2 methods to revoke a digital certificate.

- Certificate Revocation List (CRL) it lists the serial number of revoked certificates, anyone accessing a digital certificate should verify the SN in the CRL.
- Online Certificate Status Protocol (OCSP) you check online against the CA to see if the certificate is expired or not.

Certificate Stapling

The main issue with OCSP is that the servers get overloaded with enquires. Certificate Stapling reduces the CA's servers' burden, the stapling has a 24 hour validity, so the web server doesn't need to contact the CA again. Meaning that in one day just a request per certificate is handled.

Certificate Authorities

Self-signed certificates, large organizations set up their own CA, digital certificates are generally used within the organization only

Certificate chaining, organizations that have their own CA trusted by a third party CAs, allowing trust in external users. The internal CA is known as intermediate CA. Google is an example:

Certificate chaining also allows the use of Offline CAs (Intermediate CAs) protect sensitive root keys, are the ones that issue certificate to customers, the root keys are safeguarded and are use only when to certify a new online CA

Certificate subjects

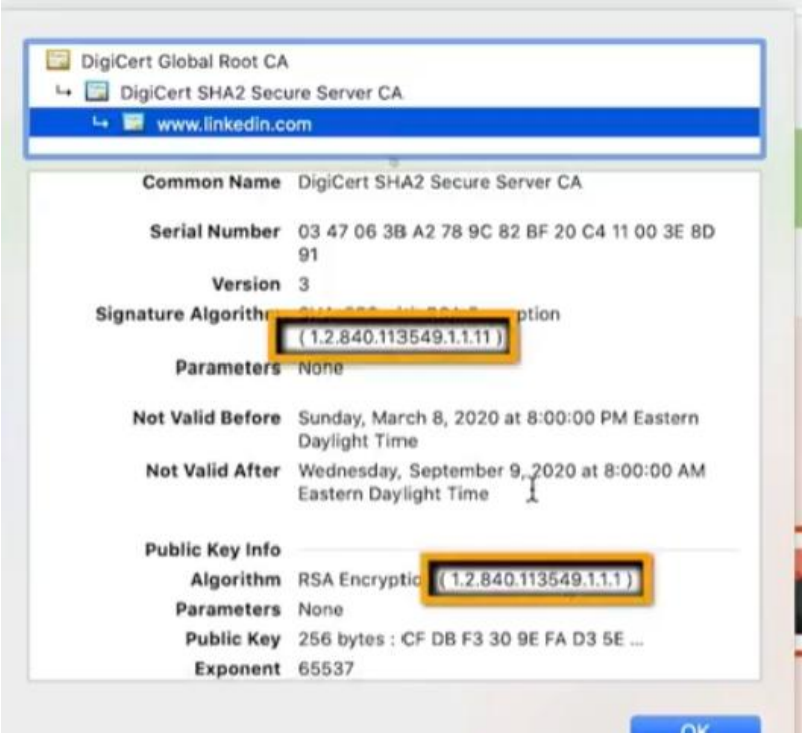
Certificate Subjects

- **Servers** – web, SSH, file, email, etc.
- **Devices** – SANs, routers, switches, VPNs, access points, etc.
- **Individuals** – names, email addresses
- **Developers** – for code signing

The most common use of certificates is to protect web servers, but they also can provide authentication for other web servers, individuals an email address.

The certificate subject is who owns the public key.

EXAM TIP: Object identifiers are used to uniquely identify each element of a digital certificate; they can help you trace back the origin of a digital certificate and its components



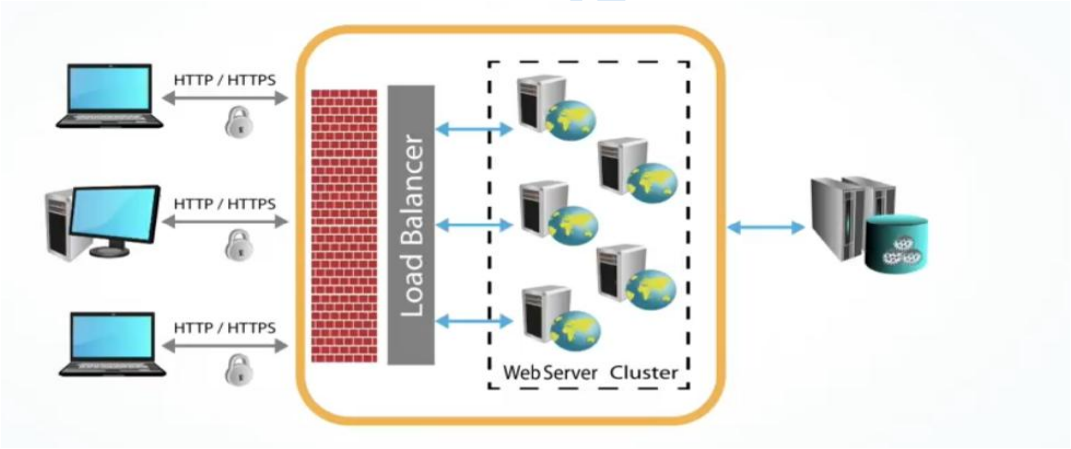
Certificate Pinning is a technology that tells users of certificates that they should not expect a certificate to change

Certificate pinning restricts which certificates are considered valid for a particular website, limiting risk. Instead of allowing any trusted certificate to be used, operators "pin" the certificate authority (CA) issuer(s), public keys or even end-entity certificates of their choice. Clients connecting to that server will treat all other certificates as invalid and refuse to make an HTTPS connection.

Pinning allows websites to control the risk of misissuance, CA compromise, or man-in-the-middle attacks. Pinning takes multiple forms depending on the use case - I can pin my certificate as the only one in my client trust store or write the public key hash into my code so only my key is trusted. When pinning started becoming popular, the hope was that these extra layers of complexity made it harder for bad actors to use certificates in attacks or spoofs.

Certificate Types

- Root certificates, are the core certificates that protect CA private keys
- Wildcard certificates, commonly used as load balancers, cover an entire domain *.linkedin.com and its subject name (subdomains) such as mail.linkedin.com learning.linkedin.com etc



Levels of trust of Digital Certificates:

- Lowest: Domain validation (DV) verifies domain ownership
- Middle: Organizational Validation, + verifies business name (against state business registrations or reputable business databases)
- Highest: Extended Validation: Requires extensive investigation to verify physical existence and legitimacy of the organization.

Certificate Formats

Binary Version	Binary File Extensions	Text Version	Text File Extensions
DER	.der, .crt, .cer	PEM	.pem, .crt
PFX	.pfx, .p12	P7B	.p7b

It comes in various formats; some are binary based some are text based.

- DER (Distinguished Encoding Rules), a binary format, stored with .der *.crt* and .cer extensions. EXAM TIP: *.crt* is used to store both PEM and DER certificate formats
- PEM (Privacy Enhanced Mail), ASCII text versions, stored .pem *.crt*
- PFX (Personal Information Exchange), binary format, used by windows systems, stored with .pfx .p12 extensions,
- P7B format, ASCII text PFX equivalent, .p7b extension

TorosTechnology.com

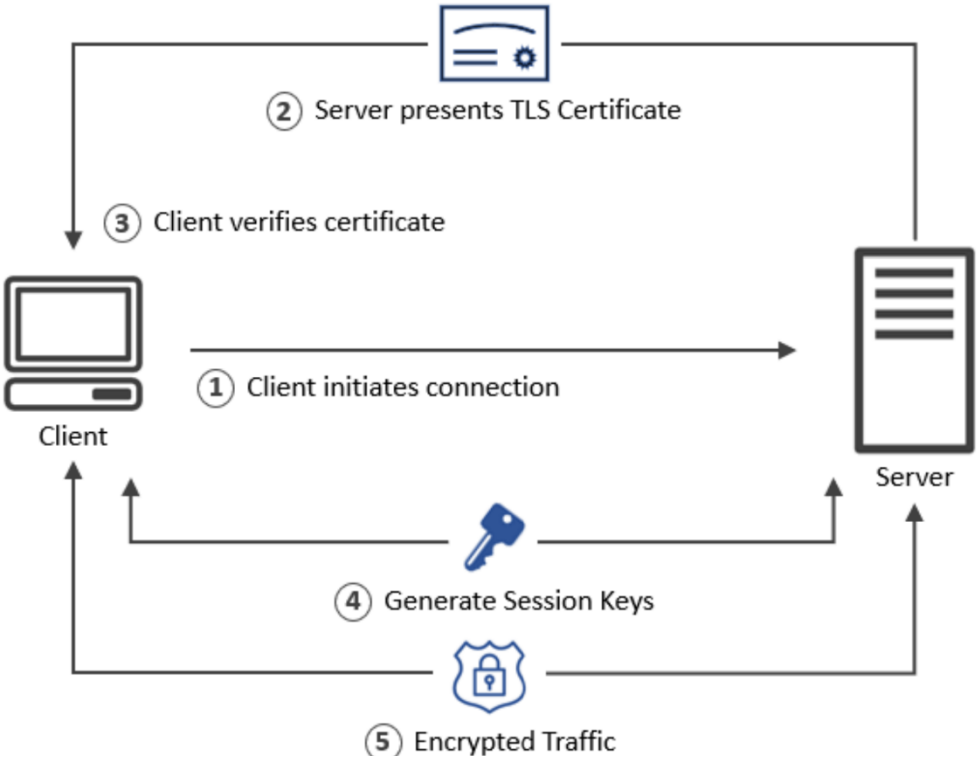
Cryptographic applications

TLS (Transport Layer Security)

TLS is a protocol that uses digital certificates to facilitate secure communications over public networks. EXAM TIP: is a protocol that uses other encryption algorithms known as cipher suites. TLS is not a cryptographic algorithm itself.

The list of cipher suites is a long list of encryption algorithms, hash functions and other cryptographic details. Cipher suites are only as strong as the algorithms they include, meaning that they could be weak as well, reason why TLS is considered insecure.

1. Client initiates a connection to a server.
2. Server presents its TLS certificate to the client.
3. Client validates the server by verifying the certificate information.
4. A session key is then generated through information exchange between the two parties.
5. The generated session key is used for encryption of traffic between the two parties.



EXAM TIP: Session Keys are also known as ephemeral keys; sessions keys are symmetric keys that are used for that one communication only

SSL (Secure Sockets Layer)

SSL is the insecure predecessor to TLS

Blockchain

Blockchain is a distributed and immutable and sometimes public ledger, can store records in a way that distribute those records among different systems around the world preventing the records to be destroyed.

Created to support cryptocurrencies such as Bitcoin allowing the tracking of bitcoin transactions without the use of a centralized authority.

Block chain can also be used with Property ownership records, to track materials through the supply chain, vital records such as passports, birth and death certificates.

TorosTechnology.com

DOMAIN 2- Threats, Vulnerabilities and mitigations

Vulnerability types

Vulnerability impact

Vulnerability impacts CIA functions exposing our organizations to the risk of a security breach

Disclosure attacks seek to undermine confidentiality, making sensitive information available to individuals or general public, this data exfiltration (removing sensitive information from an organization control) is also known as data breach.

Alteration attacks seek to undermine Integrity (alter information)

Denial attacks DOS attacks seek to undermine availability (overwhelm a system or crashing it)

Financial risk involves monetary loss to the organization, going from restoring damaged equipment and data, conducting incident response or notifying individuals that their data was stolen

Reputational risk impacts how stakeholders view our organization

Strategic risk is when the organization will be become less efficient in meeting its goals and objectives

Operational risk affects the organization ability to carry out day-to-day activities

Compliance risk involves potential violations of law or regulations.

Supply Chain vulnerabilities

Security issues that might arise in the supply chain can impact organizations

Patch management protect the organisation from vulnerabilities that are discovered every year, organizations should also not use end-of-life software.

TorosTechnology.com

1. **End of sale**
   - The product will no longer be offered for purchase, but the vendor will support existing customers
2. **End of support**
   - The vendor will reduce or eliminate support for existing users of the product
3. **End of life**
   - The vendor will no longer provide any support or updates for the product

Vendors may not disclose the use of embedded systems such as the use of publicity displays with OS that are not supported anymore

Data Storage Providers, these Vendors should always provide you access to your data at some point in the future, a way to mitigate this risk is to keep backups in a secondary environment

Configuration vulnerabilities

A few configurations error could lead to potential risks.

- Not modifying default credentials for networking devices, embedded computers, peripherals such as copiers
- We should follow documented security standards and baselines to install systems in a secure manner
- Cryptographic vulnerabilities such as weak cipher suites or weak cryptographic protocols, poor key management, poor certificate management
- Patch management: OS, apps, firmware
- Account management (least privilege)

Architecture vulnerabilities

Arise when a technical system is improperly designed. A common mistake is to design a system first and then bolt on security after. Another one is that untrained users and weak business processes can be as dangerous as technical flaws.

TorosTechnology.com

Avoid system sprawl when new devices are connected to the network, but old devices are not promptly disconnected

Avoid legacy hardware

Malware

Comparing Viruses, Worms and Trojans

Malware (Malicious software) objects affect computers systems and then perform some type of evil action. Every type of malware has 2 components:

- Propagation mechanism, how the malware spreads from one system to another one
- Payload, the malicious action that the malware performs

Malware types:

Virus (most users misapply the term virus to any type of malware), they spread from system to system based upon some type of user action. The best way to protect against viruses is user education.

Worms, they spread from system to system without user interaction, they exploit system vulnerabilities without the user doing anything. The best way to protect against worms is to keep systems up to date.

Trojan horses, they pretend to be legitimate software that the user might want to download and install, when the user runs the program, it performs as expected but the trojan horse contains a malicious payload that performs unwanted action behind the scenes. The best way to protect against trojan horses is by application control.

TerosTechnology.com

Malware payloads

3 types of malware payload:

- Spyware, gathers information without the user's knowledge or consent, they use techniques such as logging strokes, monitoring web browsers,

searching hard drives and cloud storage, also bloatware is usually slipped to a system by other software installers.

- Ransomware, blocks access to data, it uses cryptography, encrypting files with a secret key and then selling that key for ransom
- Crypto malware, is a malware that takes advantage of the computer capacity of a user's system and uses that capacity to mine cryptocurrencies

Backdoors and logic bombs

Backdoors and logic bombs are not like the malware previously explained where all of them are independent programs written by malware developers. These are pieces of code inserted in other apps with malicious intent.

Backdoor occurs when a programmer provides himself or other access to a system (workaround access) when installed through hardcoded accounts, default passwords or unknown access channels

Logic bombs modify the existing code and when certain conditions (date & time, file contents, API call) are met it executes the payload

TorosTechnology.com

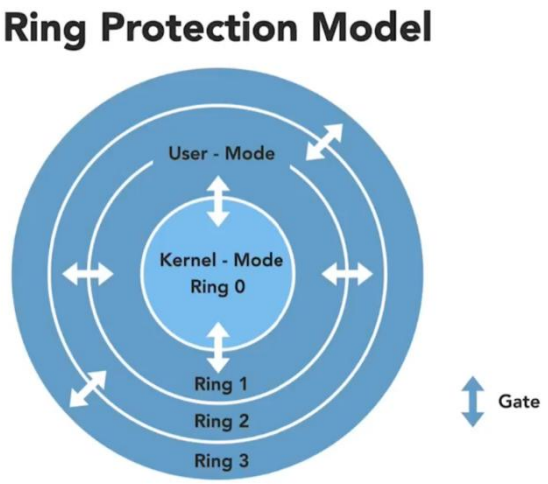
Advanced Malware

Rootkit, escalates user privileges, a hacker gains access to a normal account in the system and the use a rootkit to gain access or escalate to a root account (usually reserved for sys admins) is a superuser account that provides unrestricted access to system resources.

Root kits can run on user mode (easy to write but difficult to detect) or kernel mode (difficult to write but easier to detect)

Rootkit payloads:

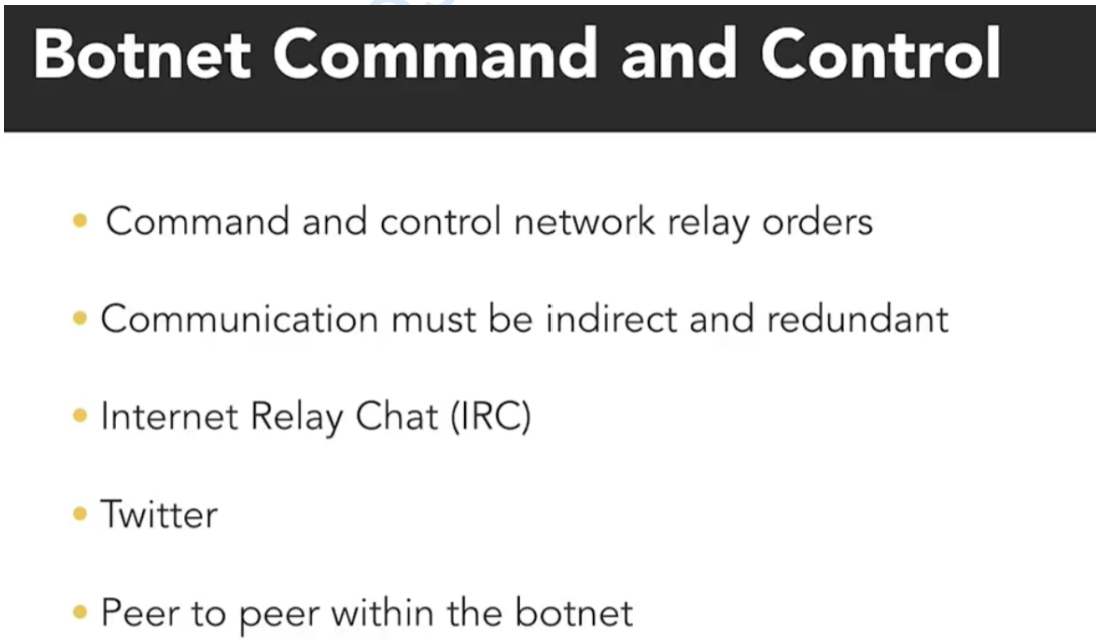
- Backdoors
- Botnet agents
- Adware/spyware
- Antitheft mechanisms



Fireless viruses, remains and operates in computer memory, it doesn't write any data to disks, seeks to avoid detection by antivirus software. Modern fileless viruses often execute as a JS code downloaded from a website, they write a copy of themselves in the windows registry to instruct windows to load them back into memory after reboots.

Botnets

Botnets are a collection of zombie computers that steal computing power, network bandwidth and storage capacity. Their objective is to create spam. DDOS attacks, mine crypto



Malicious script execution

A script if is a sequence of instructions written in a programming language to automate our work. Types:

- Shell scripts: run at the command line and integrate with the OS
- Application scripts: run within a software application and integrate with that application
- Programming languages: write code to carry out any task

Attackers can write scripts to create backdoors, modify files permissions, exploit systems

Scripting languages:

- Bash: used in Linux & Mac
- PowerShell: Windows
- Visual Basic for Applications: is the most common macro (task automation within an application) scripting language used in Office
- Python: general purpose language to write code to perform any task

TorosTechnology.com

Understanding attackers

Cybersecurity adversaries

- Unskilled attackers, lone individuals, also known as script kiddie, because they lack technical skills, they are defeated by basic security controls: patch management, endpoint security software, firewalls and IPS
- Hacktivist, they can be unskilled or posse advanced technical skills, they seek to use hacking tools to advance political and social agendas.
- Criminal syndicates, organised crime groups that use hacking tools such as ransomware for financial gain, they might possess advanced technical skills
- Corporate espionage, competitors may use hacking tools for espionage purposes to use proprietary information as a business advantage
- Nation state, are the most advanced skill attackers, well-funded, nation-state actors sponsor highly sophisticated APT (Advanced Persistent Threat) groups

Attacker motivations

- Data exfiltration, involves stealing sensitive information (intellectual property, employee data, financial records).
- Espionage, involves stealing data for the benefit of a government or corporation while covertly monitor the target system.
- Service disruption impedes the normal operation of systems

- Blackmail is an attempt to obtain a ransom from organizations trying to avoid legal or reputational damage due the sensitive information that was stolen
- Financial gain, steal credit cards, perform bank fraud, bank mining
- Philosophical or political beliefs to reveal sensitive information to the public
- Ethical hacking, authorised penetration of system by CS professionals
- Revenge attacks, often personal and targeted (disgruntled employees, business rivals)
- Chaos, some attackers just to create confusion and mistrust
- Cyberwarfare attacks, attacking other countries' critical infrastructure

Insider threats

Insider threat is the risk of current and former employees, contractors, and other insiders might exploit their privilege access to cause damage to the organization.

Shadow IT, is technology that is brought into the organization by individuals' employees without approval

TorosTechnology.com

Attack vectors

Are the pads that the attackers use to gain that initial access

- Images and other files with malicious code
- e-mails with malicious content and links
- SMS
- Voice calls
- Social media
- Flash drives
- Usb cables
- Card skimmers
- Cloud services (improperly secured content and systems)
- Tampering devices at the supply chain
- Wireless networks

Zero-day attacks

Zero-day vulnerability is when a vulnerability has been discovered by someone, but it hasn't been patched by the vendor yet, no ethical disclosure has been made.

Windows of vulnerability is the time lapse between the discovery of a zero-day vulnerability and a release of a security update

APTs (advanced persistent threats) usually carry out zero day attacks

Social Engineering attacks

Social engineering

Social engineering attacks use psychological tricks to manipulate people into information or an action that undermines information security. These attacks are successful because of:

- Authority people comply to authority
- Intimidation scaring people and something bad might happen
- Consensus herd mentality
- Scarcity making people believe that if they don't act quickly, they will lose an opportunity
- Urgency Time is running out (critical repair, etc)
- Familiarity being likeable

Impersonation attacks

Spam, unwanted commercial e-mails

- Phishing, a subcategory of spam, have the purpose of eliciting information

TarosTechnology.com

- Spear Phishing, targeted attack, it has higher success than generic phishing attacks
- Invoice scam, is a type of spear phishing where the attacker sends fake invoices
- Whaling, highly targeted to senior executives
- Pharming, they begin as a phish messages, but they have great links with fake websites that look legitimate, they might use typo squatting to pretend using a legit URL, or DNS poisoning to re-direct victims to a fake site.
- Vishing, voice phishing
- Smishing and SPIM (SMS and iMessages spam)
- Spoofing, faking identity of someone else.
- Brand impersonation, attacks to customers or third party that pretend to be from your organization

Identity fraud

Instead of targeting corporation attackers target individuals. Types:

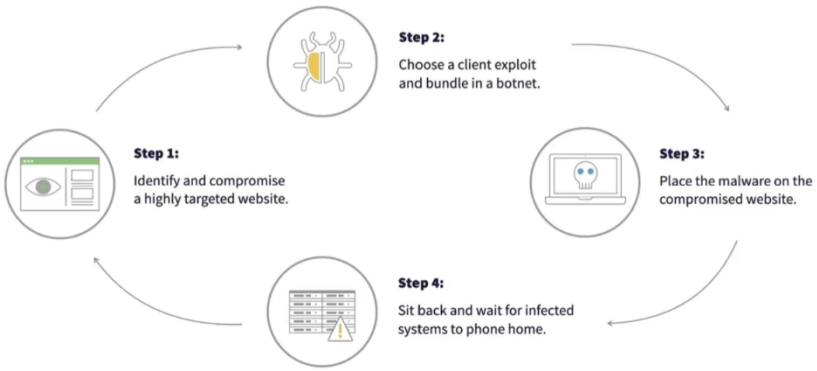
- Pretexting: the attacker contacts a company pretending to be the consumer

Watering hole attacks

Instead of the attacker trying to get inside of your network, they'll try to gain access to the system that you will access later on. We refer to this as a watering hole attack. That means the attacker will poison the watering hole and simply wait for you to visit.

These attacks usually prompt security warnings but the end users usually click ok because they trust the website

TorosTechnology.com



TorosTechnology.com

Physical social engineering

- Shoulder surfing
- Dumpsters diving
- Tailgating

Business e-mail compromise BEC

BEC involves spoofing to pose as an insider, or account takeovers using stolen accounts through password cracking or spear phishing to request fund transfers, they exploit a sense of urgency by pressuring the recipient to take action.

CEO fraud involves impersonating high ranking executives

Vendor e-mail compromise attacks use fake invoices to steal vendor payments.

Misinformation and disinformation

Misinformation false information that is spread unintentionally (social media echo chamber)

Disinformation false information that is spread intentionally with the goal to deceive others. (Propaganda, fake news, deep fake, SEO, State sponsor)

TorosTechnology.com

Password attacks

Password attacks

On Linux, password files contain user credentials with the password as a hash (stored as the shadow password file), to secure the system we need to remove the public accessible /etc/passwd file

Hash Function Criteria

- It must produce a completely different output for each input
- It must be computationally difficult to retrieve the input from the output
- It must be computationally difficult to find two different inputs that generate the same output

The birthday problem is when collisions occur when we have large samples

Common password attacks:

- Brute force: try all possibilities, can be offline against a stolen password or online by simple trying to logon to a system repeatedly
- Dictionary attacks: assume that people use words as passwords, trying English first
- Hybrid attacks: add variations to tries (numbers, years, letters)
- Rainbow table attack (precompute hashes)

TorosTechnology.com

Password spraying & credential stuffing

Password spraying: exploits commonly use passwords at the same time, best defense is to prohibit the use of common passwords to access control systems and MFA

Credential stuffing: exploit reused passwords, best way is to use password manager tools and MFA

Application attacks

SQL Injection

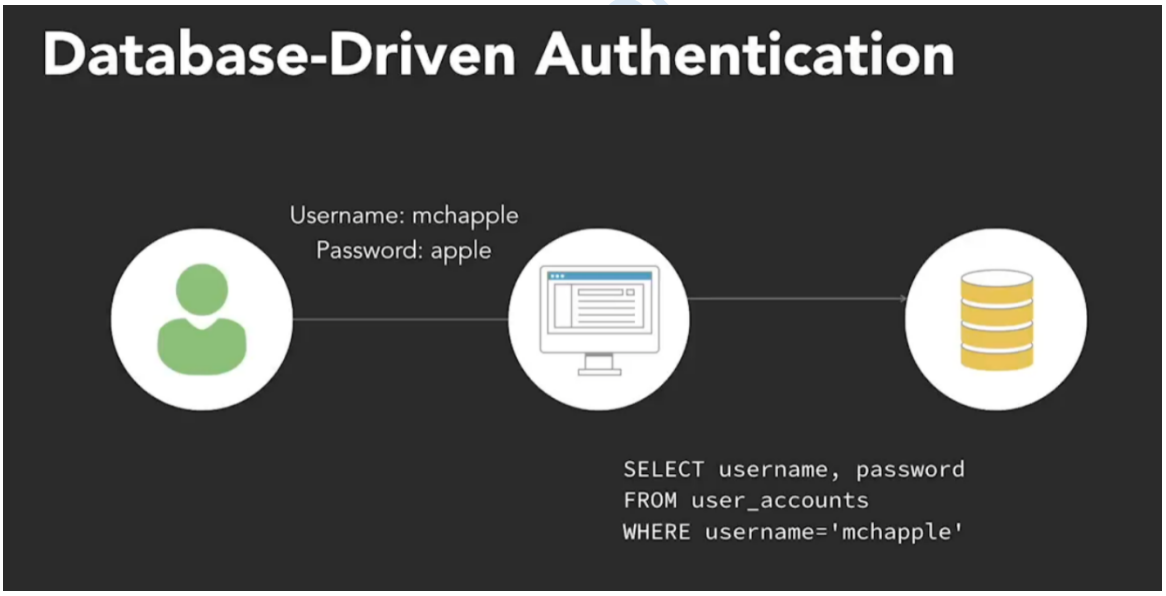
Dynamic web applications depend upon back-end databases

Applications request data from databases using Structured Query Language (SQL).

EXAM TIP: Learn how SQL injection works

Steps:

- Writing a SQL Query (in this example, retrieve a user's password from the database), semicolons separate commands is SQL, two dashes designate commands



Putting It All Together

```
SELECT username, password FROM
user_accounts WHERE username
='mchapple';

UPDATE user_accounts SET
password='hacked' WHERE
username='mchapple';

--'
```

There are 2 ways to defend again this attack

- Input validation protects against unsafe user input by checking it on the server before executing commands, input should never contain a single quote
- Parameterised SQL precompiles SQL code on the database server to prevent user input from altering query structure

Toros Technology

Cross-Site Scripting XSS

XXS occur when an attacker embeds malicious scripts in a third-party website (without permission) that are later run by innocent visitors to that site.

To prevent these attacks, we need to use input validation, not allowing <script> tags in user-supplied input

Cross Site Request Forgery attack (EXAM TIP: CSRF, XSRF, sea surf)

These attacks are similar to XSS, but they are even more dangerous.

Cross-Site Request Forgery

Cross-site request forgery (CSRF or XSRF) attacks leverage the fact that users are often logged into multiple sites at the same time and use one site to trick the browser into sending malicious requests to another site without the user's knowledge.

A client-side attack, most browsers have authentication cookies that enable us to automatically logon to websites we previously have logged on, XSRF usually happen when in web browsers you have a fake image tag that executes malicious commands

```
http://www.paybuddy.com/
transfer_funds.php?
amount=500&source=acct1230122&target=acct
9159284
```

Defending Against CSRF

- Rearchitect web applications
- Prevent the use of HTTP GET requests
- Advise users to log out of sites
- Automatically log out users after an idle period

Server-Side request forgery SSRF, manipulate servers into retrieving data from what it believes to be a trusted source

TorosTechnology.com

Overflow attacks

Buffer is an area of memory used to store data temporarily while it is being moved from one place to another.

Buffer overflow attacks, if the developer fails to check that the user content is larger than the area reserved for the buffer and overflow occurs.

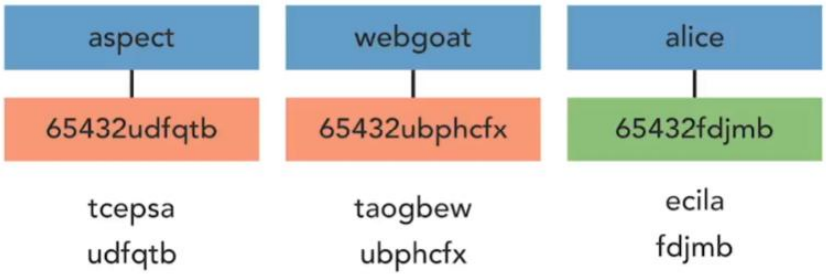
Cookies and attachments

Cookies track user activity on the web

Session hijacking

Cookies provide an easy shortcut for web authentication, once the user logs on to a website, the webserver provides a cookie so the end user doesn't need to authenticate the next time they request a webpage, the webpage will reference the latest successful logon.

Guessable cookies, this is possible if cookie values are not randomly generated



Session replay attacks, occurs when cookies are not encrypted in transit

To protect from these attacks, administrators should configure cookies with a secure attribute (over an encrypted connection)

Code execution attacks

The attacker exploits a vulnerability in a system that allows the attacker to run commands on that system, these commands are also known as arbitrary code execution, if taken place from a remote system is known as remote code execution.

Code execution objectives:

- Install malicious code
- Join a system to a botnet
- Steal sensitive information
- Create accounts for later access

We can prevent code execution attack by limiting administrative access (least privilege principle) and patch systems and applications.

Privilege Escalation Attack

Take on standard accounts and transform them into accounts with administrator rights. These attacks arise from buffer overflow issues. We can mitigate these attacks by:

- Performing input validation (that the expected input from end users has the right format and length)
- Patch OS platforms and apps
- Least privilege principle
- Use DEP (Data execution prevention) and ASLR (Address space layout randomization) technologies

OWASP Top ten

1. Broken access control occurs when developers fail to check the back end of an application to see if the user has the right access to a particular function of an application.

TorosTechnology.com

2. Cryptographic failures happen when insecure web apps accidentally expose sensitive information to eavesdroppers
3. Injection, when attackers insert unwanted code into a request sent to a website, and tricks that website to pass the code to a backend server where it's executed. (SQL Injection)
4. Insecure design, fails to meet security requirements
5. Security misconfiguration occurs because web apps depend on many complex systems, an error in any of those systems settings can jeopardize the security of the entire system
6. Vulnerable and outdated components
7. Identification and authentication failures (Session hijacking)
8. Software and Data Integrity failures, allows insertion of insecure code (lacking appropriate verification checks in the software pipeline)
9. Secure logging and monitoring failures (lack of logs)
10. SSRF Server-Side Request Forgery, attacker tricks a server into retrieve an URL that hasn't been validated

Application Security

Two types of software:

- Purchased software: acquired from vendors
- Developed Software: custom written to meet the needs of an organization

Application hardening:

- Using authentication
- Encrypting sensitive data
- Input validation
- Avoid and remediate known exploits
- Obfuscation and camouflage (hide source code)
- *Beware of malicious updates*

*Configuration baselines compare current settings of a system and the desired status

Application Configuration:

- Type and scope of encryption
- Users with access to the application

TorosTechnology.com

- Scope of access granted to each user
- Security of underlying infrastructure (networks, databases, servers)

TorosTechnology.com

Defending against directory traversal

Directory traversal attacks allow the attacker to manipulate the file system on a web server; they use directory navigation references (. ..) to search for insecure files.

You can defend from these attacks by:

- Requiring input validation
- Strict files access controls to prevent the web server user to read sensitive files

Race condition vulnerabilities

A race condition is when two events happen at nearly the same time with an application, and the application doesn't consider that these two conditions may be operating simultaneously.
TOCTOU (This is a Time-Of-Check to Time-Of-Use attack) software checks whether an activity is authorised or not, but some time elapsed before the action of checking.
We can prevent race condition by adding a lock to prevent 2 users access the system at the same time

TorosTechnology.com

Cryptanalytic attacks

Brute force attacks (a.k.a ciphertext attacks)

Brute force attacks are the simplest form of attack against of a cryptographic system, the attacker repeatedly guess keys until they stumble the correct value for that key, it can a very long time if they ever succeed

Keyspace: is the set of all possible encryption keys usable with an algorithm

- 56-bit DES
  - 72,057,594,037,927,936 keys

Knowledge-based attacks

Frequency analysis the attacker does some statistical analysis to the ciphertext to detect patterns
Masking if the attacker has access to both the encrypted and unencrypted message could lead to a:
plain-text attack where the attacker uses his knowledge to crack the decryption key for other messages.
chosen plaintext attack occurs when the attacker creates an encrypted message of their choice
Birthday attack happens when there is a hash collision, two different of plain text that they produce the same hash

Limitations of encryption algorithms

Asymmetric algorithms are generally slower

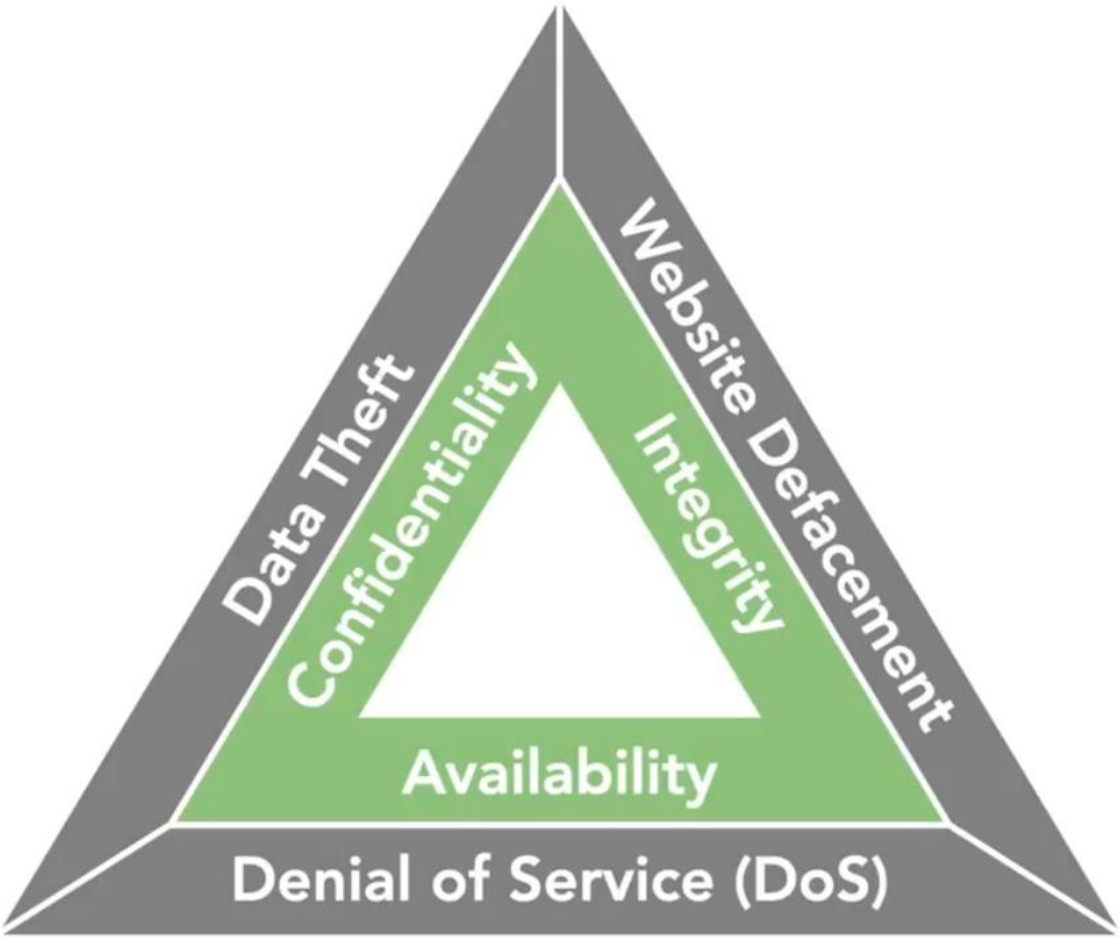
Longer keys are more secure, but they require more computing power
Cryptographic algorithms and keys have limited longevity

The ciphertext must exhibit a high level of entropy. If any elements of order from the plaintext persist, it will make the ciphertext vulnerable to cryptanalysis, and the algorithm can be shown to be weak

Downgrade attacks, the attacker tricks the parties into not encrypting their communication or using a weak form of communication (an example is the poodle attack to SSL implementations)

TorosTechnology.com

Network attacks



DOS attacks

Denial-of-service DOS attacks makes the system or resource unavailable to legitimate users. However, it has its limitations such as requiring large amount of bandwidth to send requests and the attack can be blocked by IP address.
Distributed denial-of-service DDOS attacks use botnets to overwhelm their targets.
Smurf attack, is a type of DDOS attack also known as amplified attack that uses a server as a bot to send ICMP echo request to the broadcast addresses (IP address that is used to send a communication signal to all devices present in the network) of third party servers with a forged sender

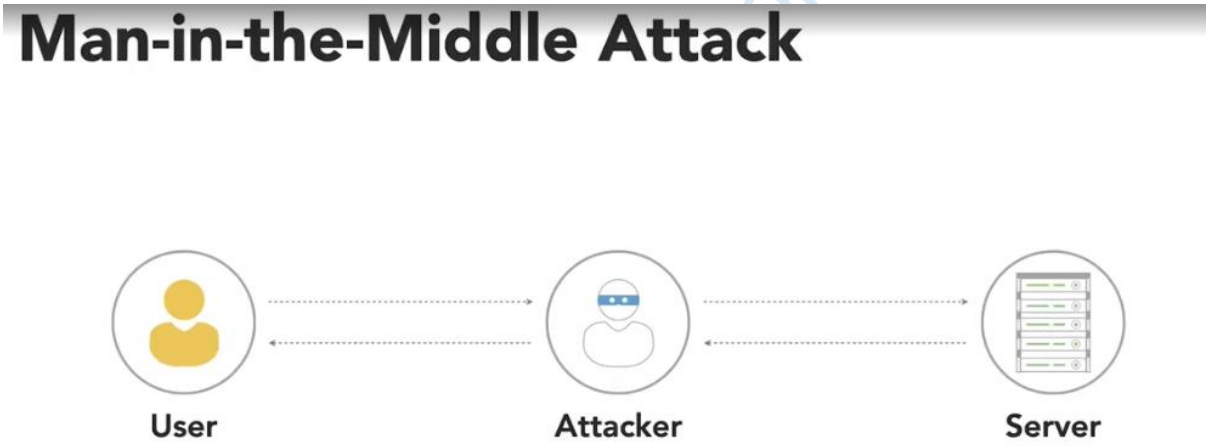
IP address (victim's Ip address) to overwhelm the victim with ICMP echo replies

Eavesdropping attacks

These attacks occur when the attacker has physical or logical access to a network, it relies on a compromised communication path (network device taping, DNS poisoning, ARP poisoning)

On-path attacks:

Man in the middle attack, instead of establishing communication with a legitimate server the sender communicates with the attacker



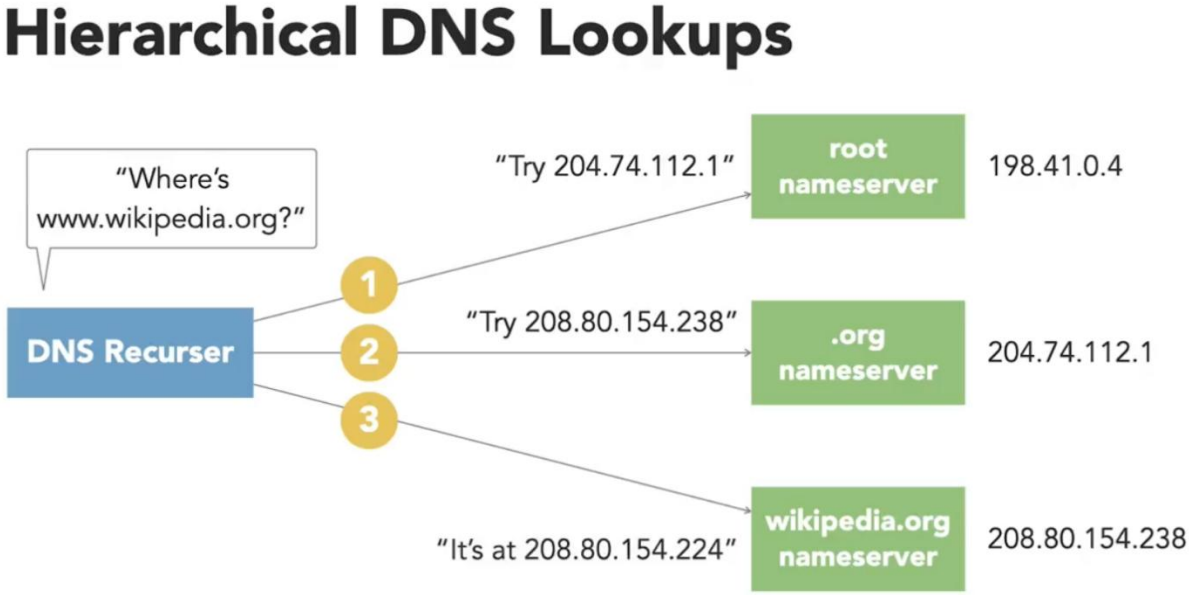
Man in the browser attack exploits flaws in browsers and browsers plugins

If the attacker is able to capture network traffic is what we know as a replay attack uses previous capture data (encryption token) to create a separate connection to the server that is authenticated but does not involve the real end user. Replay attacks can be defeated by using single session tokens or timestamps

SSL Stripping is a variation of eavesdropping attacks, tricks browser into using unencrypted communications

DNS Attacks

DNS Poisoning inserts incorrect DNS records at any point along the hierarchy to redirect traffic to the attacker's system



Typosquatting an attack that consists in registering domain names like official sites hoping that users will make a typo when trying to visit the site.

Domain Hijacking, the attack gains control of an organization's domain registration

URL Redirection, the attacker redirects traffic from a trusted site to a content hosted in a malicious site

Domain Reputation is a threat intelligence capability that identifies if the traffic is either benign or malicious

TerosTechnology

Wireless attacks

EXAM TIP WEP (Wireless Equivalent Privacy) is insecure because the attacker can capture the IVs (initialization vectors) that helps to get the connection established, these are sent without encryption because they are used to create the encrypted channel.
WPA (Wi-Fi Protected access), like WEP, relies on degauss

encryption standard but adds TKIP (Temporal Key Integrity Protocol) that makes the encryption key to change every time a packet is sent over the network. However, WPA is no longer secure due WPA hashing function

WPA2 and WPA3 are considered secure

WPS (Wi-Fi Protected Setup) has the purpose of making easy to connect new devices to a wireless network, however, the PIN needed to connect the devices can be guessed, a good practice is to disable the WPS.

- **There are two methods for establishing connection:**
  - Pressing buttons on devices
  - Using the eight-digit WPS PIN
- Though there are 10,000,000 possibilities, a flaw requires only 11,000 guesses

Propagation attacks

Powerful antennas can lead to attacks based upon radio propagation

Jamming and Interference attacks can lead to DOS of the Wireless Network due a powerful transmitter with a signal that overpowers the APs

Wardriving attacks, attackers go mobile, they cruise busy areas capturing information with software about WiFi networks

Warflying attacks take wardriving airborne by using aircraft, drones & UAV (Unmanned Aerial Vehicle)

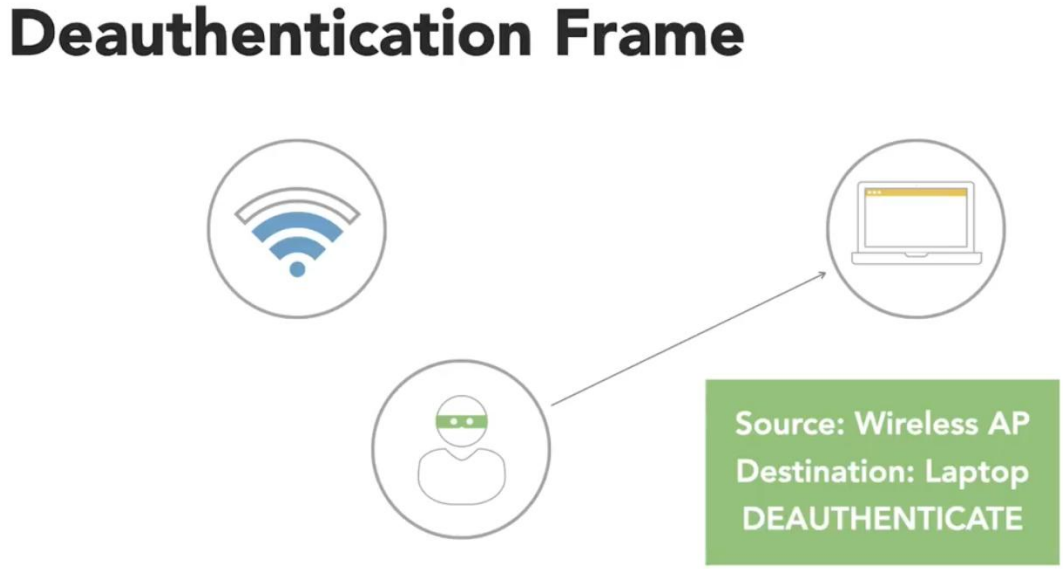
Rogue access points & Evil twins

Rogue access points occur when someone install an unauthorised AP to an enterprise network, they can bypass authentication, they possess interference

Evil Twins, a hacker sets up a fake access point with the SSID of a legitimate network

Disassociation attacks

Attackers use a disassociation capability in their favour called deauthenticate where the clients need to authenticate to the AP once or twice every hour to keep connected to the network, the attackers spoof the AP MAC and the client MAC to obtain cryptographic information and cause DOS to the client and the network.



Bluetooth attacks

Bluejacking occurs when an attacker sends Bluetooth spam to a user's device (not as common today)

Bluesnarfing occurs when an attacker exploits older implementations of Bluetooth firmware Ip

RFID

RFID chips are embedded in many items and may be read by RFID scanners

RFID Security Concerns

- Businesses want strong authentication and encryption to protect the integrity of RFID systems and prevent RFID cloning
- Consumers want privacy safeguards to protect their personal information

Attack indicators

- Account lockout
- Concurrent session use (user logged on from multiple locations simultaneously)
- Impossible travel time scenarios
- Blocked content
- Resource consumption (CPU, RAM, Bandwidth)
- Resource inaccessibility
- Out of Cycle logging
- Missing logs

DOMAIN 3- Security architecture

Cloud Computing

Cloud

Cloud computing: Delivering computing resources (network, storage, servers, applications, services) to a remote customer over a network

Cloud computing roles

Cloud Service provider: offers cloud computing services to third parties

Cloud Customer: purchases cloud computing services

Cloud Service Partner: provides add on services

Cloud Access Security mi (CASB): offer Identity and Management services to cloud customers

TorosTechnology.com

Drivers for Cloud computing

- On-demand Self-Service: available when you need it.
- Scalability: customer can increase or decrease capacity
- Horizontal scaling: add more servers to the pool
- Vertical scaling: more resources (CPU, RAM Storage)
- Elasticity: expanding and contracting capacity quickly
- Broad network access: connect form whenever you are
- Measured service: pay for what you consume

Multitenant Computing

Multitenancy: multiple customers sharing the same computing resources. The principle of Isolation should always be applied, and no customer should be seeing other's customer data.

Resource pooling: CPU and RAM is shared among users

Cloud considerations

Cost-benefit analysis:

However. There are cost factors we should be considering as well:

- Electricity costs
- Data center facility rental / acquisition / maintenance
- Training costs
- Consulting Services
- Staff Time

Some cloud migrations might come as a net loss to the organization, cost-benefit analysis should incorporate as well intangible benefits:

- Ease of deployment
- Risk transference
- Availability
- Resilience and ease of recovery
- Responsiveness

- Scalability and elasticity
- Capex vs OpEx

Managed Service Providers

MSPs: offer IT services to customers, some MSPs provide different services:

- Manage an entire security infrastructure
- Monitor system logs
- Manage firewalls or networks
- Perform identity and access management

EXAM TIP: Some MSSPs provide Security as a Service, a.k.a SECaaS

Cloud Access Security Broker (CASB): add a third-party security layer to interactions that users have with other cloud services.

Network Based CASB: Brokers intercept traffic between the user and the cloud service monitoring for security issues, broker can block requests

API-Based CASB: the broker queries the cloud service via API, might not be able to block requests

ToroTechnology.com

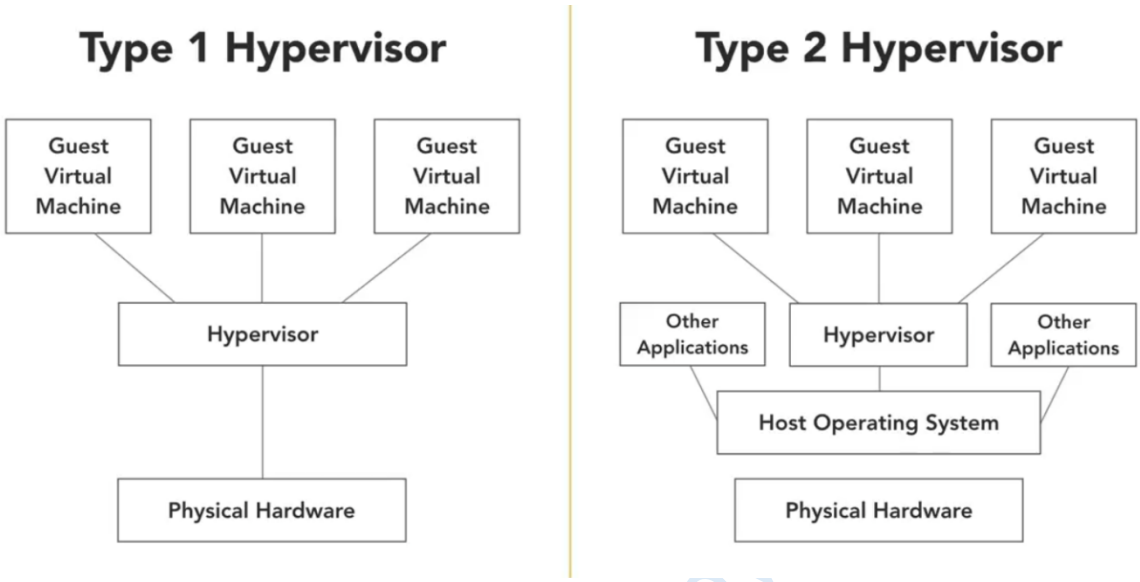
Virtualization

Virtualization

Virtualization, is the driver force behind cloud computing, allows many virtual servers use the same underlying infrastructure.

The host machine has special software known as hypervisor that manages guest VMs

- Type one Hypervisor (also known as bare metal) directly runs on physical hardware, commonly found in data centres
- Type 2 Hypervisor runs on the host OS; it's commonly used in personal computers.



Virtualization security:

- Virtual machine isolation is critical
- Each server should have access to his own resources
- VM escape attacks attempt to break out of the guest environment
- VMS should always be patches
- EXAM TIP: VM Sprawl: unused and unmaintained servers

Desktop and application virtualization

VDI Virtual Desktop Infrastructure provides network-based access to a desktop computing environment (if working from home though VDI you will be able to access company resources)

Application virtualization (Application streaming) streams applications to the user's desktop (Citrix ZenApp, VMware ThinApp, Microsoft App-V)

Cloud Building Blocks

Cloud Compute Resources

Virtual server run in cloud data centres.

- High availability: uses resources across zones insulating us against a possible failure in a single zone
- Instance awareness needs to be maintained (because is so easy to create VMs) to avoid VM Sprawl

Cloud Storage

After resources, Storage is the second most important building block of the cloud, we need to be able to store and archive data.

- Block Storage, we allocate a large chunk of storage such as a hard drive and partition it into volumes (C:/ or D:/ drive in Windows), it could be HDD or SSD
- Object Storage: we upload files or objects, and the Cloud Provider worries about where to place them, how to back them up and how to manage them over time. Less expensive than block storage, can be purchased with high availability or archival.

ForosTechnology.com

Cloud Storage Costs

- Object storage is much less expensive than block storage in the cloud
- Object storage costs are incurred only when used, while block storage must be allocated and paid for in drive-sized blocks

Cloud Networking

Cloud networking is the third most important building block

VPCs (Virtual Private Clouds) are the Amazon equivalent to VLANs

VPC Endpoints allows VPCs interconnection

SDN – Software defined Networking is a IaC approach that integrates the cloud provider API into our operations stack

SDV – Software defined visibility allows us to use the provider's API to gain visibility into the network traffic

"Virtual traffic" refers to network data flowing between virtual machines (VMs) within a virtualized environment, while "virtual NetFlow" is a method of monitoring and analysing that virtual traffic by capturing detailed information about each network flow, allowing administrators to see exactly how data is moving between VMs within a virtual network

Cloud Databases

Databases serve as a repository for information and are the backbone for transactional systems, the options are:

- Build databases on virtualized servers
- Managed database service (more expensive)
- Cloud native database platform (retooling existing applications)

Cloud Orchestration

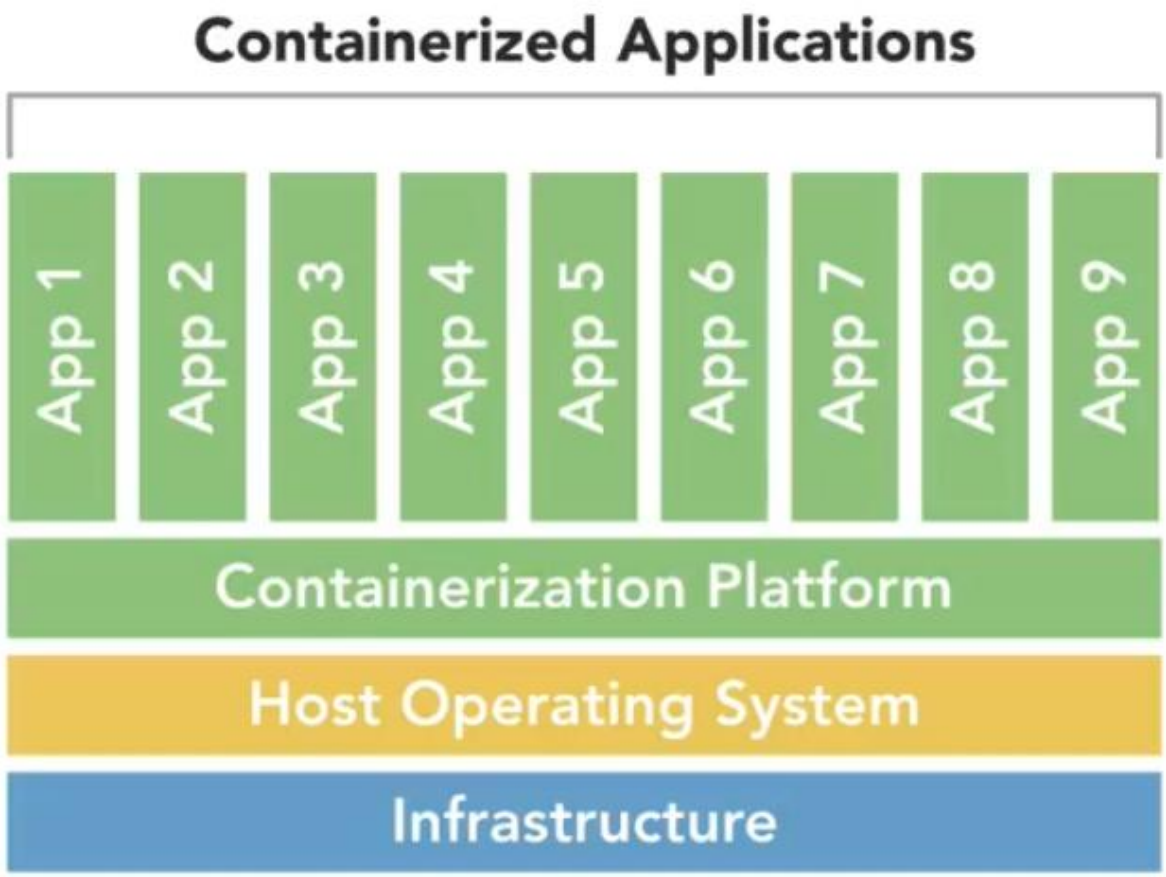
Cloud orchestration (IaaC) automates cloud environment, allowing administrators to easily create workflows.

Cloud providers and third-party vendors both offer orchestration solutions

TarosTechnology.com

Containers

Containers are lightweight way to package up an entire application and make it portable to move between different hardware, they are an alternative to virtual machines, they don't have their own OS, they use the host OS. Isolation is the most critical container security issue



Server Oriented Architecture (SOA)

SOA (commonly used by developers to integrate services from different vendors, example a sales system software different that the production management one) implies that customer don't need to know how the service provided to them works, they just need to know how to use it (Black-box nature)

Microservices are modern adaptations of SOA, they provide small and discreet function to other services

Cloud activities

Cloud activities and the cloud reference architecture

ISO- IEC 17789:2014 EXAM TIP Provides a useful framework, but they are just a starting point. It states customers, cloud providers and partner responsibilities, it also aligns with the **Cloud Security Matrix CCM** from the Cloud Security Alliance.

Cloud deployment models

EXAM TIP: No cloud model is superior to the other, it all depends on context.

Private cloud: Organizations use a dedicated cloud infrastructure, it provides flexibility, agility, scalability and cost effectiveness and do not want to share resources with other organizations.

Public cloud: Organizations use a multitenancy infrastructure, the same physical hardware is used by a few customers

Hybrid cloud: uses both private and public cloud

Community Cloud: not open to the general public but shared among related organizations (colleges, universities)

Cloud service categories

Shared Responsibility Matrix

IaaS	PaaS	SaaS
Data	Data	Data
Application	Application	Application
OS	OS	OS
Hardware	Hardware	Hardware
Data Center	Data Center	Data Center

Customer Responsibilities

Vendor Responsibilities

Xaas: Anything as a Service

Iaas: customer purchases servers to create customized solutions. (Azure, Aws)

Saas: customer purchases an entire application (e-mail, Dropbox)

Paas: customer purchases app platform (AWS Lambda)

Fass: function as a Service (run functions without worrying about servers – serverless computing)

Security and Privacy concerns in the cloud

C.I.A Triad

+

Privacy: protects the confidentiality rights of individuals whose information we store, process or transmit

In Cloud Computing, we might have Partners involved in our security planning work, bringing up 3 new concerns:

- **Governance:** oversight of cloud use in an organization, vetting potential vendors
- **Auditability:** the customer has the right to audit cloud service providers to ensure they are meeting security and operational obligations.
- **Regulatory: (**HIPAA, FERPA, PCI DSS) Cloud providers should remain complaint with obligations.

TorosTechnology.com

Data Sovereignty

Cloud service providers distribute data across multiple geographic locations as a security control. **Data Sovereignty c**oncept involves that local laws apply to the jurisdiction where the data is collected, stored or processed.

Operational Concerns

SLAs should include:

Availability, how much uptime is required?

Resiliency: the ability of Cloud Infrastructure to withstand disruptive events.

Performance, how much demand can be handled?

Reversibility, can we roll back to the state prior to a cloud transition?

Portability, can we move workloads between vendors?

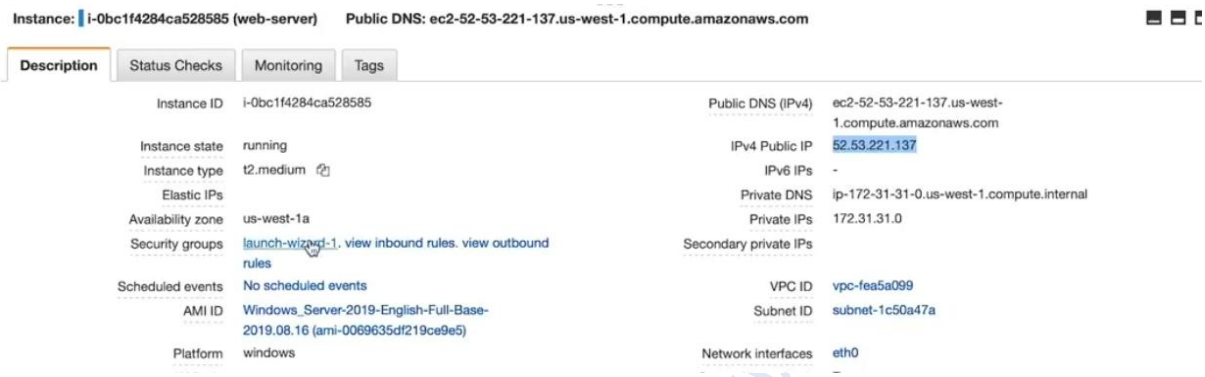
Interoperability, will our cloud solutions from different vendors work together?

TorosTechnology.com

Cloud Security Controls

Cloud firewalls considerations

Network security groups similar to firewall rules, serve as IaaS firewalls, they work at the Network, Transport and Session OSI layers



Cloud Application Security

Secure cloud applications require the integration of different services, **Defense in depth** requires the use of overlapping security controls:

- **Security groups** (Cloud firewalls)
- **TLS,** Encrypts data in transit
- **Full Disk Encryption,** encrypts data at rest
- **Application Virtualization services**
- **Secure Web Gateway**, serving as a Proxy filters web traffic

Cloud Provider security controls

Third party controls vendors offer security controls that integrate with different cloud providers

Resource Policy, limits cloud service usage

Transit Gateway, links on-premises and cloud networks

Secret Management, store keys and credentials

TarosTechnology

TCP/IP Networking

TCP/IP

The 2 main transport protocols are:

- **TCP**

- **UDP** (Voice and Video)

OSI Model:

Application Layer	User programs
Presentation Layer	Data translation and encryption
Session Layer	Exchanges between systems
Transport Layer	TCP and UDP
Network Layer	Internet Protocol (IP)
Data Link Layer	Data transfers between two nodes
Physical Layer	Wires, radios, and optics

IP addresses and DHCP

IPV6:

- Replaces IPv4 due to address exhaustion
- Uses 128 bits (compared to 32 for IPv4)
- Consists of eight groups of four hexadecimal numbers
- Example: fd02:24c1:b942:01f3:ead2:123a:c3d2:cf2f

Static IPs	DHCP
Static IPs are manually assigned to systems by an administrator. They must be unique and within the appropriate range for the network.	The Dynamic Host Configuration Protocol (DHCP) allows the automatic assignment of IP addresses from an administrator-configured pool.

DNS

Provides address resolution on the internet, DNS functions over UDP port 53

1. User types domain name into browser.
2. Computer sends a DNS query to the local DNS server.
3. DNS server responds with an IP address.
4. Computer contacts the server at that IP address.

DNSSEC adds digital signatures to DNS

Network ports

- 16-bit binary numbers
- 2^{16} or 65,536 possible values
- Start counting at 0
- Allowable range of 0–65,535

Ports 0-1023: well-known ports (assigned by Internet authorities)

Ports 1024-49151: registered ports (application vendor might register these ports to use them, e.g. 1433 is reserved for SQL database connections by Microsoft)

Ports 49152-65535: dynamic ports (temporary basis)

Services	Ports	Services	Ports	Services	Ports
FTP	21	SMTP	25	HTTP	80
SSH	22	POP	110	HTTPS	443
RDP	3389	IMAP	143		
NetBIOS	137–139				

ICMP

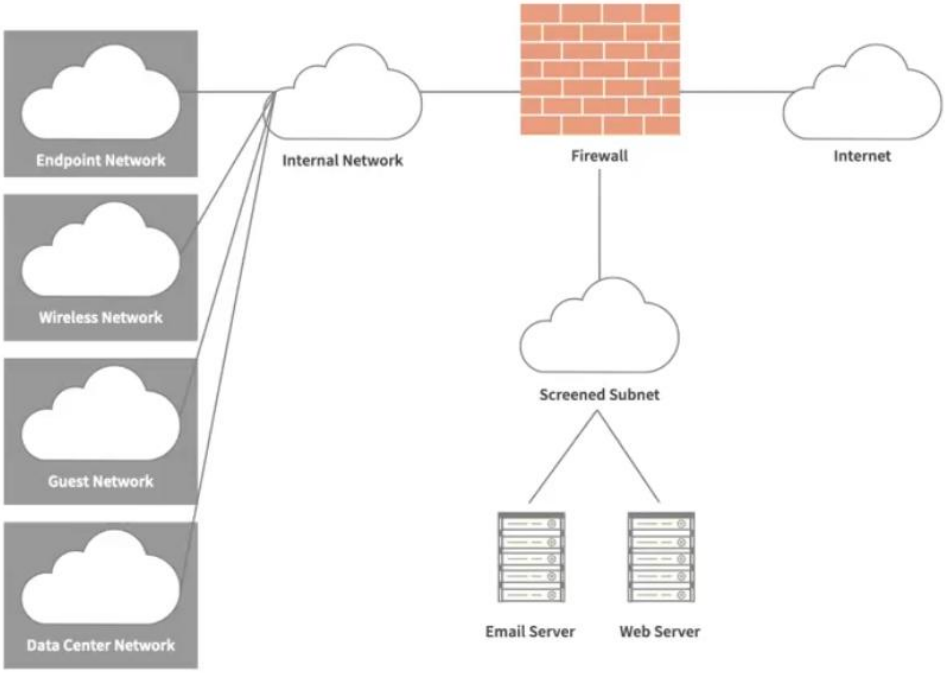
Performs a wide variety of administrative functions:

- **Ping:** Identify live systems
- **Traceroute:** Identify network paths

Secure Network Design

Security Zones

Firewalls segment networks into **security zones** to protect systems of different security levels. Below a Network Border Firewall with 3 zones: Internet, Screened Subnet (DMZ) and Internal Network:



Zero Trust: systems do not gain privileges based on solely network location.

Three other special purpose networks:

- **Extranet:** Intranet segment to business partners.
- **Honeypot:** Devoy network designed to attract attackers
- **Ad Hoc Network:** Temporary network that may bypass security controls (Security Risk)

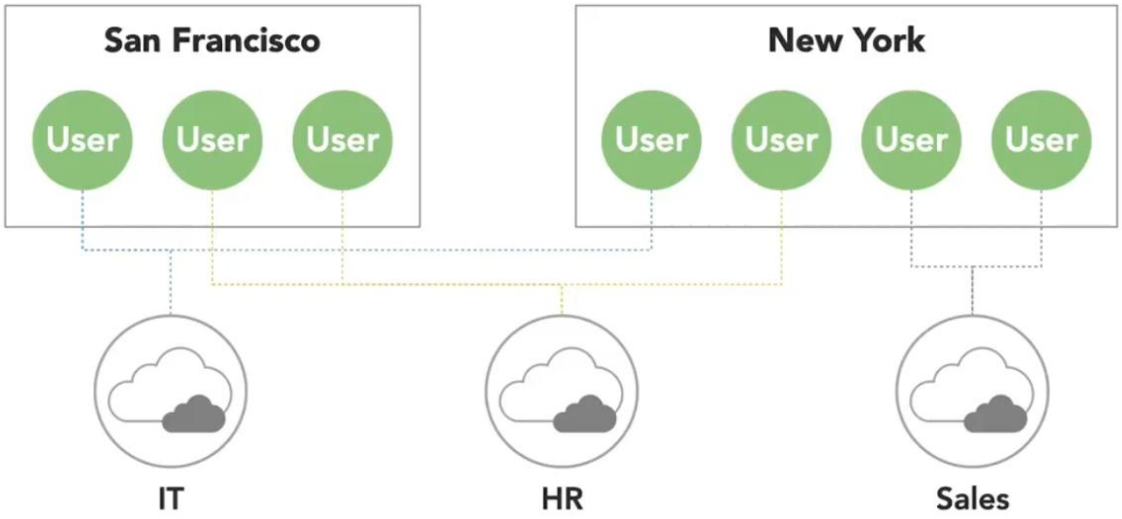
Types of traffic on a network:

East-west traffic: network traffic between systems in the same data center.

North-South Traffic: network traffic between systems in the data center and systems on the internet.

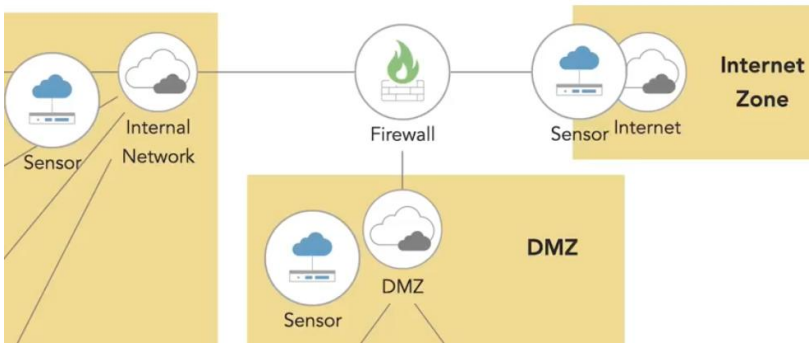
VLANs and Network Segmentation

VLANs separate systems on a network into logical groups, VLANs extend the broadcast domain allowing users in the same VLAN interact to each other as if they were connected in the same switch



Security device placement

- **Firewalls** should be placed at any place where we want to implement security boundaries.
- **Sensors with IDS and IPS, network TAPs and port mirrors** should be placed in the network segments where they should be collecting the information from



- **SPAN (Switched Port Analyzer)** allows network administrators to capture network traffic from specified ports in the switch to an analyzer host.

- **Port mirroring** allows the monitoring of network traffic on a single switchport.
- **Proxy Servers and content filters** usually belong in the DMZ, especially if they need to initiate connections to the outside world.
- **SSL Accelerators** (offloads the SSL handshake from a web server to a separate device) and **Load Balancers** belong to the DMZ
- **VPN Concentrators a**re hardware devices used to aggregate inbound network connections from employees and other users that require remote access, they are usually place in their own VLAN
- **DDoS Mitigation Services** should be bought from ISP

Software-defined networking SDN

SDN treats the network functionality and implementation details separately

- **Control Plane,** responsible for making routing and switching decisions, how network devices interact with each other.
- **Data Plane,** carries out the instructions of the control plane

Network Security Devices

Routers, Switches, Bridges

- **Switches** connect devices to the Network
- **WAPs** connect to switches and create Wi-Fi networks
- **Routers** connect to each other creating networks
- **Bridges** operates at Layer 2, and connects 2 or more network segments based on mac addresses

Firewalls

- **Firewalls** work at the network perimeter; they analyse the traffic in the network.

TorosTechnology.com

- **Stateless Firewall (**older firewalls) evaluates each packet separately when they arrive to the firewall

- **Stateful Inspection firewalls**, also known as a layer 4 firewalls, because it works and the transport layer of the OSI model, allows to keep track of established connections.

Firewall Rule Contents:

- Source address
- Destination address
- Destination port and protocol
- Action (allow or deny)
- **Implicit Deny/ Default Deny,** any traffic that is not explicitly allowed by a firewall will be blocked.

Next Generation Firewalls (NGFWs) incorporate contextual information (identity of the user, nature of the application and time of the day) into their decision-making, also known as **layer 7 firewalls.**

Other firewall roles:

- NAT Gateway
- Content and URL firewall
- Web application firewalls know how the HTTP protocol works, and they can look for SQL injections, cross-site scripting.

TorosTechnology.com

Web application firewalls

WAFs know how the HTTP/ HTTPs protocol works, and they can look for, SQL injections, cross-site scripting, directory traversal, buffer overflows, privilege escalation, cookie-based attacks.

They can be:

- **Hardware WAF** (Physical device)
- **Software WAF** (Software running in the web server)

- **Cloud-based WAF** (effective against DDoS attacks die the wide bandwidth)
- XML Firewalls (filter access to REST APIs)

TorosTechnology.com

Proxy Server

Proxy servers connect to websites on behalf of end users. Proxy servers provide:

- Anonymization
- Performance boosting (due the cache)
- Content filtering

Forward Proxies, work on behalf of clients, in the client's network.

Reverse Proxies, work on behalf of servers, in the remote network.

Transparent Proxies (a.k.a inline proxies or forced proxies), work without the client's or server knowledge

Load Balancers

Load Balancers distribute work among servers, they can also provide SSL certificate management, URL filtering.

- **Load Balancers also Round-Robin scheduling,** which makes decision about routing requests to servers maintaining an equal share.
- **Session Persistence**: some applications require end user's requests to be routed to the same sever to maintain session persistence
- **Autoscaling,** as demands increases, administrators can add or remove servers.

Organizations should maintain load-balancers in **high availability mode**, an **active-active** approach where two or more load balancers handling network traffic.

Active-passive approach, one load balancer handles all traffic while the second monitors activity in case the primary one fails.

VPNs and VPNs Concentrators.

- **Site to Site VPNs** allows secure interconnection between remote networks

TorosTechnology.com

- **Remote access VPNS**, provides access to remote workers

VPN Concentrator are very efficient when setting up VPNs and can manage high bandwidth with ease.

IPsec (IP Protocol Security) (layer 3) often used for static site-to-site VPN connections is become less common for Remote User VPNs, if the administrator wants to also run VPNs connections at the data link layer they can use L2TP (Layer 2 Tunnel Protocol) over an IPsec connection

Remote user VPNs **(SSL/TLS VPNs**) are configured at the application layer over TCP Port 443

HTML5 VPNs works within the web browser and allows users to work with internal resources

VPN Traffic **types:**

- **Full-tunnel VPN**, all traffic leaving the connected device is routed through VPN
- **Split-tunnel VPN,** (most security experts recommend not to use split-tunnel VPNs) only traffic destined for the corporate network is sent through VPN tunnel, other traffic is routed over the internet.
- Always on VPN, connects automatically to the VPN whenever they are powered on

TomsTechnology.com

Network intrusion detection and prevention

- **IDS** sit in the network and monitors traffic searching for signs of malicious activity (SQL Injections, malformed packets, unusual logins, botnet traffic)
- **IPS** performs IDS functions + takes immediate action to block the malicious activity, they can be deployed **Inline** (active - device sits in the path of network communications and blocks suspicious activities) or **Out-of-band** (passive – device connects to SPAN or TAP port in a switch and reacts after suspicious traffic enters the network)

Both systems perform **signature detection**, detecting signatures that are known to be associated with malicious activity, they have a low false positive rate, the downside: can fail to detect brand new attacks

False positive errors: IDS & IPS detect an attack that did not take place

False negative errors: IDS/ IPS fails to trigger an alert when an actual attack occurs.

Anomaly detection systems build models of normal activity and reports anomalies, also known as behaviour-based detection and heuristic detection

Protocol Analyzers

They allow deep inspection of traffic, troubleshoot network issues and investigate security incidents, in the wrong hands could be used to eavesdrop communications.

- **Wireshark** is the most common protocol analyzer. Uses l**ibpcap** library
- **Tcpdump** is a command line protocol analyzer. Uses **libpcap** library
- **Tcpreplay** allows editing and replaying traffic

UTM

Unified Threat Management UTM combines multiple security functions in a single appliance.

- Firewall functions
- VPN connectivity
- IDS
- IPS
- URL filtering
- Content inspection
- Malware inspection
- Email and spam filtering

Security is a design element

Security is a design element, “Bolt-on" security rarely works. When designing a system, we need to define how the system will behave in the event of failure:

- Fail open: if security controls fail, they automatically bypassed (security risk)
- Fail closed: block access

TorosTechnology.com

Network Security Techniques

Restricting Network access

Security professionals must restrict access no networks, we can restrict access based on rules, roles, time, location.

Perimeter security: keep unwanted remote users out of the networks through UAC and firewalls.

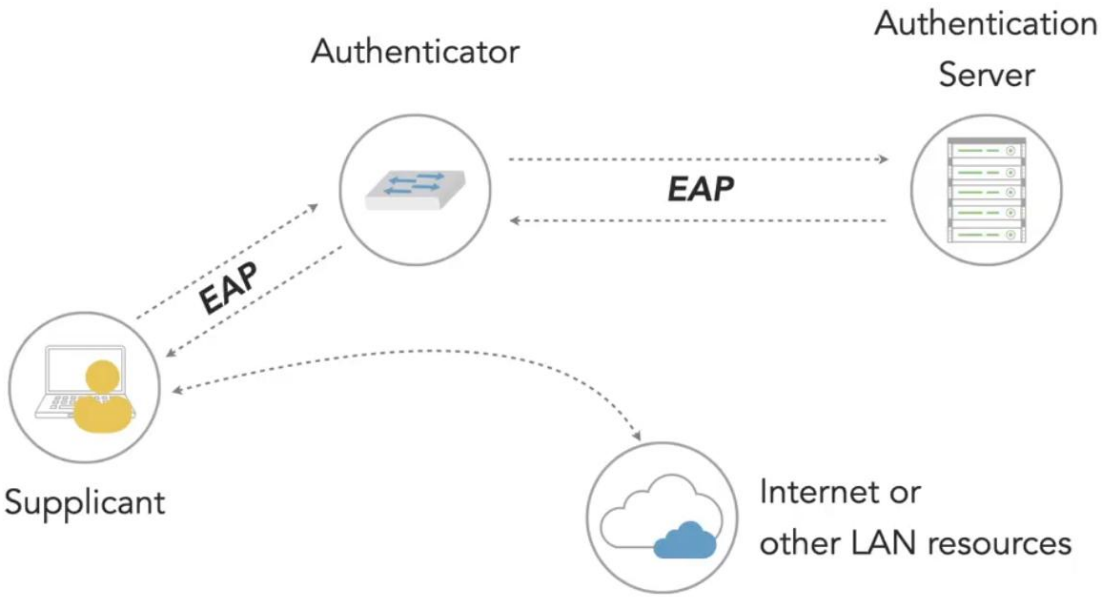
Net

work Access Control: limit physical network access to authorized individuals and devices.

Network Access Control

NAC intercepts traffic coming from unknown devices and verifies that the system and user are authorized before allowing further communication. NAC uses the **802.1X Authentication**

NAC can also perform **Role-based access** (example students and professor in different VLANs) and **posture checking** (devices that connect to the network need to be compliant with organization policy, if devices failure posture checking they are placed in a **Quarantine VLAN** without accessing Internal Recourses)



rosTechnology.com

Routers

They perform basic filtering reducing the load in firewalls, for example **Cisco Routers** support **ACLs:**

Standard: block inbound traffic based on source IP address

```
access-list[number]      [permit/deny][source][mask]
# access-list 1          deny    10.3.1.00.0.0.255
```

Extended: can block source and destination addresses based on source and destination addresses, ports and protocols

Switch

Switches are spread all over the place, they should be locked away because someone could gain physical access and control part of the network. This can be avoided by implementing:

VLAN Pruning: limit the exposure of VLANs by limiting the number of switches that are trunked.

VLAN trunk negotiation should be denied avoiding **VLAN hoping attacks**.

Port Security: limits the mac addresses that may connect to a switch port, this can be **static** (manually configure valid MACs for each port) or **dynamic or sticky mode (**switches memorise the first MAC address they see on each port and limit access to that address)

DHCP Snooping blocking malicious DHCP traffic by checking that is coming from authorised DHCP servers.

Network availability

Flooding attacks (DoS) overwhelm network devices with traffic:

- **Syn Flood**, the attacker creates thousands of half open tcp connections to a device, this Syn packets will never be able to create the three-way handshake.

TorosTechnology.com

- **MAC Flooding** fills switch's MAC Address table with many entries causing to flood traffic on all ports.

We can protect this by:

- **Flood Guad technology**, they control the number of open connections each source system may have.
- **Port Security**

Routing Loops various physical paths between 2 network devices allowing **broadcast storms,** the best way to prevent this issue is by **STP** that help us keeping our networks loop free, it uses **BPDUs** (**Bridge Protocol Data Units)** that are network packets that are used to exchange information between switches, the **BDPU Guard** security feature disable ports that receive BDPUs from unauthorised devices.

Network monitoring

Firewall logs contain information about attempted connection, timestamps and the relevant firewall rule that authorised or denied the connection.

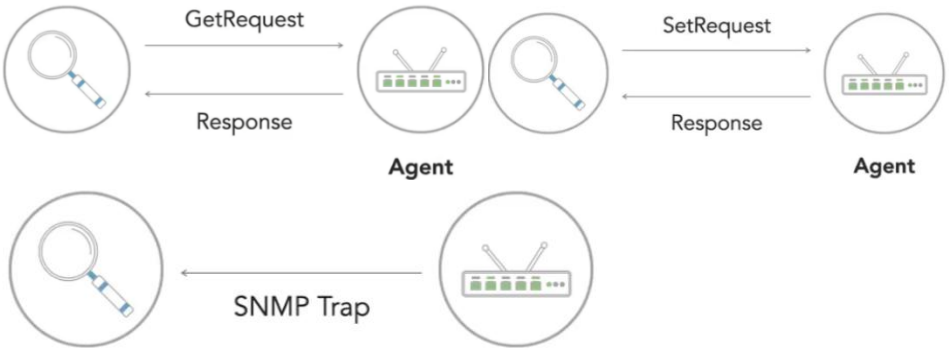
Network Flow Data (NetFlow) captures connection details, src-dest systems, ports, timestamps and amount of data.

SIEM (System Information and Event Management) are network security systems that automate the collection and analysis of logs from different systems (firewalls, network devices, servers and applications)

TorosTechnology.com

SNMP

SNMPv3 Simple Network Management Protocol provides network administrators with the automation of network monitoring and management tasks, **early versions of SNMP have security flaws**



TorosTechnology.com

Isolating Sensitive systems

Network Segmentation is a security control; sensitive servers may be placed in their own physically isolated security zone also known as **air-gapped system.**

Jump Servers, allows administrators to jump or connect to those different security zones

Zero Trust Networking

Organizations should be trusting individuals (through **IAM** Identity Access Management) rather than networks shifting away the focus of perimeter protection, **SIEM** and **SOAR** platforms facilitate the monitoring of the network activity.

CASB Cloud Access Security Brokers enforce security policy in the cloud.

EDR Endpoint Detection and Response platforms remediate endpoint security issues.

Geofencing: Alerts when a device leaves a defined area

SASE

ZTNA Zero Trust Network Access applies least privilege to network access based on **IAM.** ZTNA is a **medium-term** objective

SASE Security Access Service Edge delivers a fully integrated network with ZTNA, SASE combines SDN, ZTNA, CASBs, FWaaS to provide a cloud-bases secure network. Is a **long-term goal**

TonosTechnology.com

TorosTechnology.com

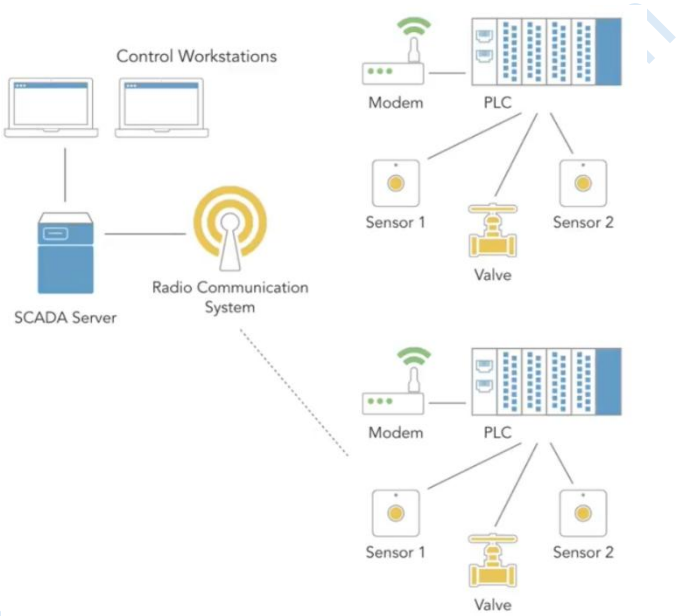
Embedded Security Systems

Industrial Control Systems ICSs

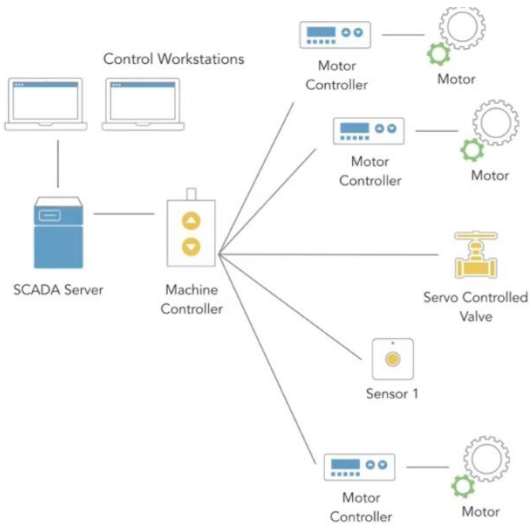
ICSs control industrial production and operation, an attack to a ICSs could result in dramatic implications

ICS Types:

SCADA Supervisory control and data acquisition: common in systems that require **remote monitoring** (gas pipelines, power production, water supply systems), they have **remote telemetry** units that provide reports back to the Server



DCSs Distributed Control Systems: common in wastewater treatment and distribution systems, refineries, food products



PLCs Programmable Logic Controllers are designed to handle specialised output and input systems; it uses **Modbus Protocol** to communicate over the serial interfaces.

Internet of Things IoT

Smart devices are computer and network controlled, IoT security challenges:

- Difficult to update software and OS
- They connect to our home network
- They connect back to a cloud command control

Securing Smart Devices

- Check for weak default passwords
- Regular security updates
- Firmware version control
- **Security wrappers:** when is not possible to patch vulnerabilities organizations must take this approach where the device is not accessible over the network but through a wrapper system that monitors input and output for security issues.

TorosTechnology.com

Secure networking for Smart Devices

- **Segmenting** embedded devices in an isolated DMZ increases security.
- **Application Firewalls** provide added protection, when placed in front of the embedded system, monitors inbound traffic looking for malicious activity

Both security controls are effective for old **mainframes systems**

Embedded Systems

IoT devices are embedded systems, a full system embedded inside another larger one (i.e. a multifunction printer, cameras, drones)

Embedded systems have 2 main technologies:

- **System on a Chip SoC:** combines processor, memory, networking in a single chip (XoGo, Raspberry PI)

- **Field-programmable gate arrays FPGAs** are chips that allow dynamic reprogramming (**IBM eFUSE** technology allows this)

Other technologies:

- **RTOs Real-time operating systems** provide reliable and secure computing for IoT devices
- **Controller Area Network CAN Bus**, replacing TCP/IP to communicate IoT devices

TorosTechnology.com

Data Protection

Data Security

- Clear procedures covering the appropriate use of data and its security
- Encryption to protect sensitive information
- File system permission restrictions
- Geographic restrictions
- Network Segmentation

Data Types

Data Inventory Contents, please bear in mind that we also need to include **non-human-readable** information in the inventory:

- PII (including binary formatted files including PII)
- PHI
- Financial Information
- Intellectual Property
- Legal information
- Regulated Information

FurosTechnology.com

Data Anonymization

Deidentification is the process of reviewing a dataset and removing obvious identifiers, this includes: zip code + DOB + Gender which the 3 combined are %87 unique.

Anonymization removes the possibility of identification

Data Obfuscation

Data obfuscation is the process of transforming PII into a form that is no longer possible to tie it to an individual person, by using:

- **Hashing**, replacing sensitive fields with hash values, although could be subject of **Rainbow Table attacks.**
- **Tokenization**, replaces sensitive fields with a random identifier using a lookup table, this lookup table has to be maintained secure

- **Masking** redacts PPI, replaces sensitive information with blanks

Information classification

Is the backbone of data government efforts to help employees understand security requirements, splits information to categories based on low, medium or high sensitivity levels. **Labelling requirements** help identifying sensitive data, and we also need to **securely dispose** information when is no longer needed.

Military Classification
Top secret
Secret
Confidential
Unclassified

Business Classification
Sensitive
Restricted
Private
Public

ToroTechnolo

Resilience and Recovery

Business Continuity Planning BCP

Set of controls designed to keep business running in the face of adversity, whether natural or man-made. Also known as **COOP** Continuity of Operations Planning. It goes along with the CIA triad pillar: **Availability.**

BCP Scope is usually done after a **BIA (Business Impact Assessment)**:

- What business activities will the plan cover?
- What systems will it cover?
- What controls will it consider?

When it comes to **BCP in the cloud**, involves a partnership between the cloud provider and customers

Business Continuity Controls

Redundancy protects against the failure of a single component.

Single Point of Failure Analysis SPOFs identifies and remove SPOF from systems. IT Contingency Scenarios:

- Bankruptcy of a key vendor
- Insufficient storage or compute capacity
- Utility service failure

High Availability

HA uses multiple systems to protect against failures

Fault Tolerance makes a single system resilient against technical failure, the most common points of failure are: **storage, network and power supplies.** Best way to provide fault tolerance is:

- **Power supplies** UPS with 2 power sources and containing to UPS in case one of them fails
- **Storage**, RAID allow us to use mirroring or stripping which is EXAM TIP a fault tolerance technique, not a backup strategy (we still need to regularly back up our data)
- **Networking**, use 2 or more ISPs, using 2 NICs (NIC teaming), multipath approach between servers and storage

Multicloud strategy adds resilience to operations

TorosTechnology.com

Disaster Recovery

Disaster Recovery allow us to restore a business to normal operations as quickly as possible.

- **Initial response** allows us to contain the damage caused by the disaster and recover those capabilities that need to be restored, employees will be working in different jobs from their assigned duties (team members should be trained in a regular basis)
- **Disaster communications**: initial activation of the disaster recovery team, regular status updates, tactical communications
- **Assessment mode:** after the danger passes, is time to triage the damage to the organization and implement a recovery plan. The metrics are:

1. **RTO recovery time objective** max time that it should take to recover a service after a disaster
2. **RPO recovery point objective** max time period from which data may be lost as a result of a disaster
3. **RSL Recovery Service Level** is the percentage of a service that must be available during a disaster

- EXAM TIP: Disaster Recovery efforts end only when the business operations are back to normal in their primary environment

Backups

Backups are the most component of a disaster recovery plan because business are built on their data. Types:

- Tape backups
- Disk-to-Disk backups (including the backups sent to SAN & NAS)
- Cloud backups

We can also classify backups based on the type of data they include:

- **Full backups:** copy of all data.
- **Snapshots** create back up disk image, common on VMs.
- **differential backup** includes all data modified from last full back up,
- **incremental backups** include all data modified since last full or incremental back up.
- **journaling** records logs changes made to files or databases.

TorosTechnology.com

Restoring Backups

The most common reason that we restore backups are because of human error or a technical error, backups provide a fail-safe role in protecting against accidents. For large-scale recovery process the order of restoration is important.

- Non-persistence allows us to back up only unique data
- Last known configuration (Windows 7) allowed to restore from the latest known configuration, Windows 10 and 11 offers safe mode only.
- Live boot media loads the OS from the USB Drive and allows us to recover media from the SSD/ / HDD

Disaster Recovery Sites

- **Hot sites**, primary form of disaster recovery, fully operational data centers that have all data required to handle operations ready to run. (Expensive)
- **Cold sites**, they are empty data centres, they just have core racks, cabling, network connections, inexpensive and they take a few weeks to be operational.
- **Warm sites,** stocked with all equipment and data with similar hardware than a hot side but not equally maintained and updated and operations might take a few days to be run.
- **Offsite storage** is geographically dispersed; they can be online (ready to restore) or offline (restore to a point)

Disaster Recovery Testing Goals

- **Tabletop exercises**, gathers the team together for a formal review of the disaster recovery plan
- **Simulations** gather the team but also discuss how to respond in a specific scenario
- **Parallel processing tests** activates the DR plan (an alternative cloud or a physical operating environment)
- **Failover test,** the most effective test but the most disruptive to normal operations (simulating a disaster)

Toros Technology.com

Capacity planning

- **Technology,** must be robust and scalable (Prevent DDOS attacks)
- **Infrastructure**, redundancy (data centres)
- **People** must be trained and adaptable

DOMAIN 4- Security operations

Data Security Controls

Developing Security baselines

Security baselines are generic, and they provide a set of minimum standards for computing systems. For Windows users GPO & AD are used to automate baselines allowing administrators easier monitoring. Organizations follow 3 steps:

- **Establish** the baseline for the organization
- **Deploy** the baseline to systems throughout the organization
- **Maintain** the systems

Leveraging Industry Standards

- Vendors
- Windows (Security Compliance Toolkit and Baselines)
- Independent organizations (CIS Center for Internet Security)

Customizing Security Standards

Organizations scope and tailor de standards to meet their requirements

TorosTechnology.com

Host Security

Operating system security

- Limit administrative access (GPOs)
- Patch management (Patch management tools make the job easier)
- System hardening (analysis default settings of the OS and eliminating services, OS components, unnecessary software, lock down firewall)

Malware

Malicious software that disrupts the CIA of systems, types.

- Viruses (malicious code objects spread after human action: USB sticks, email attachments)
- Worms (similar to viruses, but they spread by themselves)
- Trojan horses (pretend to be legitimate software)
- Spyware (gathers information, keystroke loggers)

Antivirus software uses 2 mechanisms to protect against malicious software:

- **Signature detection** (watches for known patterns of malware activity)
- **Behaviour detection** (watches deviations from normal patterns of activity)

Endpoint detection and response **(EDR)** & Extended detection and response **(XDR)** use behaviour detection, as well as **sandboxing** to test executables before allowing them on the protected system. XDR Systems usually incorporate AI and machine learning algorithms.

Spam filtering filters unwanted emails, usually built in in Gmail and m365

TorosTechnology.com

Application Management

Application control restricts what software may run, it should send logs to our SIEM or log repository for analysis. 2 types of control:

- **Allow lists,** more restrictive and more effective
- **Deny lists**, less effective control, there could be some applications that should be restricted

Host Software Baselining identifies expected system software, allowed unwanted software in our environment.

Firewalls

Firewalls restrict network traffic, monitoring attempts to start communication and only allowing those that match the enterprise security policy.

Firewalls follow the **default deny rule,** any connection that is not explicitly allowed is blocked.

Firewall types:

- **Network firewalls,** are those that sit between the organization's network and the internet.
- **Host based firewalls,** they are software components of an OS, they limit connection to a server (Windows Firewall)
- **Next generation firewall (NGFW),** incorporates advanced security features such as contextual information about the user and applications, as well as their past behaviour into firewall decisions

For IDS and IPS organizations must purchase a third-party security software package

- **Intrusion Detection System IDS**, they alert administrators to suspicious activity
- **Intrusion Prevention Systems IPS**, IDS capabilities + block the suspicious activity

File Integrity Monitoring FIM

Defense-in-depth strategies require the use of diverse and overlapping security controls to detect intrusions even when other systems fail.

FIM, watch the file system of an endpoint or server in a periodic basis for unexpected changes, making sure that the hash values have not changed, they do it though **hash function** (one way function that transform variable length input to a unique fixed-length output). **Tuning** is critical, administrator need to tune FIM to the organization needs

TonesTechnology.com

Data loss prevention DLP

DLP technology search for systems and monitor networks for unsecured sensitive information and provide the ability to remove the information, block the transmission or encrypt the stored data. 2 types:

- **Host-based DLP** uses software agents installed on a single system, and search that system for sensitive information such as SSN, it also monitors system configuration and user actions (such as stopping users from using USBs)
- **Network-based DLP** protect network connections for sensitive information blocking traffic or applying encryption to that information

DLPs have 2 mechanisms of action:

- **Pattern Matching**, recognising patterns of sensitive information, such as SSN
- **Watermarking,** identifies sensitive information using electronic tags

Data encryption

Key Management System (KMS) manages the creation, distribution management and disposal of encryption keys in a secure manner.

AES Crypt is an open source file encryption software

Full-disk encryption (FDE) protects an entire drive

Hardware Security Module (HSM), the best option, it uses dedicated hardware to perform encryption and decryption operations and store encryption keys.

Trusted Platform Modules (TPMs) is a specialized HSM found in many computer systems, allows FDE minimizing the system performance of a device.

Self-Encrypting Drives (SED) it performs self-encryption automatically

Hardware and Firmware security

Trusted Execution Technology is the process of combining elements to provide a trusted execution ***root of trust > UEFI > TPM > Secure Boot***

BIOS lightweight OS stored in firmware that loads the OS

Unified Extensible Firmware Interface (UEFI) replaces BIOS with a flexible alternative. Features:

1. **Secure Boot:** verifies that the OS is loaded by UEFI is a legitimate OS from a trusted manufacturer, the process:

- Read boot loader from disk
- Compute the hash of the boot loader
- Decrypt the boot loader's digital signature
- Verify that the signature is accurate, if the signature is not accurate it will prompt a violation prompt:

TorosTechnology.com

2. **Remote attestation** sends a compliance report to an external server to provide assurance that the computer is no running malicious code
3. **Measured boot** each device in the boot chain measures the trust of the next device in the chain, trusted hashes are stored in the TPM.

Root of Trust verifies firmware integrity by storing the keys used to validate UEFI firmware

Bus Encryption protects inter-component communications

Secure enclaves provide hardware-based encryption key management (iPhones)

Processor Security Extensions allow applications to request their own protected areas of memory.

Atomic Execution ensures that transactions that are meant to be completed as a ser are entirely executed or not executed at all.

Electromagnetic Interference (EMI) can cause disruption to nearby electronic equipment

Electromagnetic pulses EMPs are extreme bursts of EMI (nuclear explosion)

TorosTechnology.com

Linux File System Access Commands

chown changes a file or directory user owner

chgrp changes a file or directory group owner

chmod changes the permissions on a file directory. Example: ***chmod o+r publicfile***

```
chmod [ownership][+/-][permissions] [file]
```

File permissions	File Ownerships
Read	User Owner
Write	Group owner
Execute	Others

Web content filtering

- **Agent-based** install a filtering agent directly on end users' devices
- **Centralized proxy** routing all website requests though a centralized proxy server that performs the filtering

URL scanning analyses URLs to identify those that are harmful or unwanted

Administrators can also restrict websites by **categories** (Adult, social media, etc) or block rules for **individual websites.**

Site reputation helps with content filtering decisions

Configuration Enforcement

Change management

Change management, ensures that an organization follows a standard process for requesting, reviewing, approving and implementing changes to information systems.

To implement change management: **Request for Change (RFC)** includes:

- the description of the change
- expected impact
- risk assessment
- rollback plan
- identity of those involved
- proposed schedule
- affected configuration items

The **RFC must be approved** by relevant authorities, although routine changes may be pre-approved.

Configuration Management

Configuration management tracks the way that devices are set up

- **Baselines** provide a configuration snapshot at a given time; it helps to assess if the system has been changed in comparison to approved RFCs.
- **Versioning** assigns numbers to each version of the system software. For example: **9.1.2** where the **first number** represents major version of the

TorosTechnology.com

software, **second number** the major update, and the **third number** minor updates
- **Diagrams** serve as configuration artifacts

Physical Asset Management

Hardware inventory is part of asset management; it should show us the device **lifecycle** (request, approval, asset tag, configure device, check out device, check in device) data updates are critical to hardware inventory it help us to keep track the assigned user and the device location, **device enumeration** allow us to find devices that are not actively managed. **Media management** tracks highly sensitive data.

Disposal and decommissioning

Erasing a file doesn't completely remove data from the disk, the OS maintains file system information known as **metadata** that contains the name of the file, creation data, access permissions, location (Windows: master file table / Linux: Inodes).

When you delete the file, the OS only removes the Inode or MFT, the raw data still contains file information. Before deleting data make sure you comply with data retention policies

- **Data sanitization** programs overwrite the data stored in the disk, in a cloud environment overwriting is performed by the cloud provider.
- **Crypto-shredding** deletes all decryption keys, is essential to destroy all copies.
- **Physical destruction** can also be used if the device is no longer needed

TorosTechnology.com

Mobile Device Security

Mobile connection methods

- **Cellular networks** are available in most urban and suburban areas, cover distances of 20+ miles away (4G, 5G)
- **WiFi networks** cover shorter distances with higher bandwidth, can be **point-to-multipoint** that connects a single base station to many clients, or **point-to-point** which connects two fixed-base stations to each other.
- **Bluetooth** cover distances of around 30 ft

- **Near Field Communication (NFC)** cover distances measured in centimetres using electromagnetic induction

Mobile device security

- **Passcode**: 4 digits passcode does not provide strong security, use an alphanumeric passcode instead.
- **Biometric authentication**, offers a convenient alternative
- **Full-device encryption** android and apple automatically encrypt the contents of the devices when you enable **password protection.**
- **Remote wiping** in case you lose the phone
- **Push notifications** are used in multifactor authentication

Mobile device management MDM

MDM manage settings across many mobile devices from a central console, such as:

- **Application block lists**
- **Application allow lists**
- **Storage segmentation** separating sensitive information
- **Content filtering and management**

ForosTechnology.com

Mobile device tracking

Inventory control with **asset-tracking software** manage device inventories and can also track the device location though **geolocation**.

Geofencing alerts when a device leaves a defined area

Mobile application security

Application process sensitive data and must have strong security controls, they should require:

- **Authentication** (passwords, social media should be reviewed as a way to authenticate)
- **Encrypt Sensitive Information** (in transit, at rest, strong key management)

- **Geotagging** (May disclose sensitive locations, some camera apps geotag the photos with the gps coordinates)

Mobile security enforcement

Third-party apps stores might contain unsafe code, installing apps from unofficial sources is known as **sideloading.**

Jailbreaking involves a user loading a custom version of an OS firmware

Over-the-air OTA are updates pushed down to the mobile device by the OS when they're ready (automatically)

Device unlocking (**carrier unlocking**) allows portability among service providers

Restrict features use: cameras, SMS, external media, USB, Microphone, GPS tagging, Wi-Fi usage, tethering, mobile payments

BYOD

BYOD Policy issues: who? What devices? How will the security be managed?

Mobile Deployment models

- **Choose your own device CYOD**: the user selects the devices
- **Corporate-Owned Personally Enabled COPE** allow personal use of corporate devices
- **Virtual Desktop infrastructure** desktops in the cloud or data center.

ForosTechnology.com

Wireless Networking

Wireless Networking

Wi-Fi is the most common wireless network, is regulated by the IEEE. WiFi devices replace network cables with radio transmitters and receivers.

Wireless access points WAPs connect wireless network to wired networks and the internet

WiFi standards:

- **802.11n (2009) WiFi 4** allows 600Mbps
- **802.11ac (2014)** allows 6.9 Gbps
- **802.11ax (2019)** allows 9.6 Gbps

Wireless Encryption

- **Wireless Equivalent Privacy (WEP)** is vulnerable
- **WiFi protected access (WPA)** replaced WEP in 2003, uses **TKIP** to rapidly rotate encryptions keys, no longer considered secure
- **WPA2 (2004)** uses AES (advanced encryption standard), uses the **CCMP** protocol, still considered secure although there are some potential security issues.
- **WPA3 (2020)** supports CCMP and adds **Simultaneous Authentication of Equals SAE** for key exchange

TorosTechnology.com

Wireless Authentication

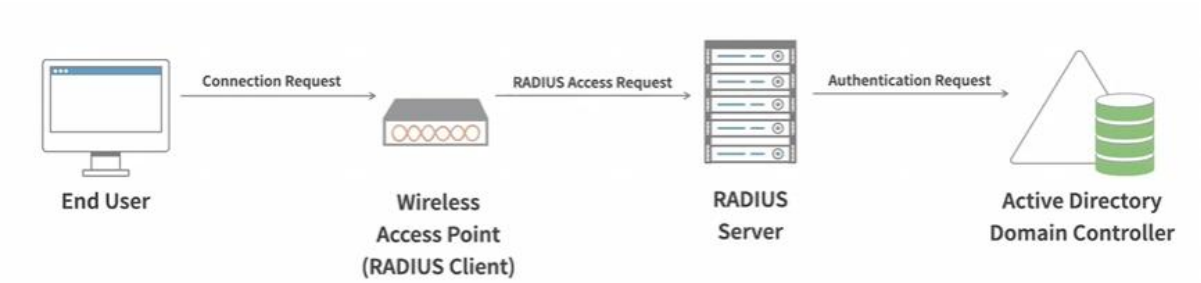
- **Pre-shared keys** (WiFi passwords using ASCII characters) are the simplest form of wireless authentication.
- **Enterprise authentication** users authenticate to a RADIUS server with their credentials using the Leap protocol, which has 3 versions:
  1. **Lightweight EAP (LEAP) protocol:** insecure protocol created by Cisco
  2. **EAP:** is a broad framework with secure and insecure variants
     EAP-TLS secure
     EAP-TTLS secure
     EAP-FAST secure
     EAP-MD5 insecure
  3. **Protected EAP (PEAP):** Tunnels EAP inside an encrypted TLS session

- **Captive portal** redirect users to an authorization page

RADIUS

RADIUS Remote Authentication Dial In User Service provides AAA, in the example below, WAP is the radius client.

RADIUS disadvantages: uses UDP, most of the data sent in a radius connection is unencrypted



Wireless Signal Propagation

- **Omnidirectional antennas** send a signal in all directions
- **Directional antennas** direct all the power from an AP to a single direction
- **Beamforming** is an 802.11ac feature that send the signal in direction of client devices by using Multiple antennas

Site Survey is ideal for optimal AP placement (heat maps)

Avoiding **channel overlaps** reduces interference from nearby networks

Power levels modify wireless signal range

Wireless Networking Equipment

FAT access points contain all the hardware and software needed to operate a wireless network

Thin access points rely on a WLC for configuration

Wifi analysers search for rogue networks and test wireless security

Code Security

Code review

Use peer analysis to assess code, the most formal process of code review is the **Fagan inspection** with its 6 steps:

- Planning (pre work)
- Overview (assign roles to participants)
- Preparation (review the code)
- Meeting (formal inspection)
- Rework (correct any errors)
- Follow up (the leader confirms all defects were corrected)

Software testing

- **Software model validation** is where the software produced meets the original business requirements.
- **Software verification** occurs in the development process
- **Stress testing or Load testing** developers simulate real world activity in the system to test the maximum capacity
- **User Acceptance Testing UAT (Beta testing)** ensures software will work for users in a testing environment.
- **Regression testing** verify that the changes don't have any side effects

Toros Technology.com

Code security tests

- **Static tests** use automated techniques to analyse the code for errors without executing it.
- **Dynamic tests** executed the code to verify that functions correctly and doesn't have security flaws.
- **Synthetic transactions** supply inputs to code with expected outputs for each code

Fuzzing

Fuzzing is a software testing technique that provides valid and invalid input to software in attempt to make the software entering an unpredictable state or disclose confidential information.

Acquired Software

- **Commercial off the Shelf COTS** purchased from third-party vendors and run on systems managed by the consumer
- **Software as a Service**, software developed by vendors that runs in the cloud on vendor managed services
- Apply **security updates**, also known as security patches, hotfixes, critical updates, major and minor releases
- **Open-source software** also requires careful management

Package Monitoring

Third party libraries and packages could save time but also represents a security risk. Package monitoring tracks third-party code

Threat Intelligence

Threat Intelligence

Threat intelligence allows organizations to stay up-to-date on current risks. A way to stay up-to-date is through open-source intelligence:

- Security websites
- Vulnerability databases
- News Media
- Social media
- Code Repositories

Timeliness: how promptly is threat intelligence delivered?

Accuracy: is the data correct?

Reliability: is the provider consistent?

Intelligence Sharing

Information Sharing and Analysis Centres ISACs are organizations that gathers and analyse information about threats, there is almost one for each industry.

TerosTechnology.com

Threat hunting

Is a systematic approach to seek indicators of network compromise using expertise and analytic techniques. Steps:

- Establish a hypothesis
- Indicators of compromise (anything unusual)
- After discovering a compromise, we move into incident response

Vulnerability Management

Vulnerability Management

The **Linux Kernel** manages input, output, memory management, CPU management, it contains over 24 million lines of code. Vulnerability Patching Process help administrators to handle the vulnerability complex process:

- Company learns of a vulnerability
- Developers analyse the issue and develop a patch
- The company releases the patch to customers
- Customers apply the patch to remediate the vulnerability

Vulnerability management has many reasons that make them essential, among them:

Payment Card Industry Data Security Standard PCI DSS Requires quarterly internal and external vulnerability scans, new scans after significant changes, use approved scanning vendor, remediate and rescan until you achieve a clean report.

Agencies from the US Government are subject to **FISMA Federal information Security Management Act** enforces agencies to follow the security controls from NIST Publication 800-53

Types of vulnerability scans:

- **Network Vulnerability scans**
- **Application scans** test the code running in devices
- **Web Application scans** (SQL injection cross site scripting)

TorosTechnology.com

Scan targets

Vulnerability Management Steps:

- Develop requirements (company or regulatory requirements)
- List specific network and systems we want to scan (asset inventory) then prioritise assets based on: **impact** (highest data classification), **likelihood** (network exposure, how likely? what services?), **criticality.**

Scan configuration

Most Vulnerability scans tools also allow uploading assets from asset management tools.

When creating a scanning program, we can organise in confidential, sensitive, and highly sensitive. Specify the frequency of the scans

Scan perspective

Network location affects scan results, placing the scanner in:

- DMZ: give us the clearest picture of vulnerabilities on the target system
- Internet: give us an attacker view of the network

Scanner types:

- **Server based scanner** reaches out devices over the network
- **Agent-based scanner** installs software on each target device
- **Credential scanning** use passwords to logon into systems, is important to give the scanner read only permissions and not and admin account

Terminology

SQL Injection, web application vulnerability and input validation flaw usually refers to the same.

Same as for several, critical and urgent refers to the same.

- **SCAP Security Content Automation Protocol** help us to use the same language

TorosTechnology.com

- **CVSS Common Vulnerability Scoring Systems**

CVSS scores vulnerabilities on a 10-point scale based on 8 metrics.

1. **Attack Vector AV** type of access that an attacker must have to exploit a vulnerability (**P**hysical, **L**ocal, **A**djacent Network (LAN access), **N**etwork = remote)
2. **Attack Complexity AC** how difficult it is to exploit a vulnerability (**H**igh, **L**ow)
3. **Privileges Required PR** (**H**igh, **L**ow, **N**one)
4. **User Interaction UI** requires the user take some action (**R**equired, **N**one)

+

5,6,7. Impacts to the **CIA** triad (High, Low, None)

8. **Scope** if exploiting the vulnerability can affect other resources (**C**hanged, **U**nchanged)

- **CCE Common Configuration Enumeration**
- **CPE Common Platform Enumeration** product names and versions
- **CVE Common Vulnerabilities and Exposure**
- **XCCDF Extensible Configuration Checklist Description Format** provides a language for creating and sharing checklists
- **OVAL Open Vulnerability and Assessment Language**

Toros Technology.com

Analysing Scan Reports

First, we need to do a **Vulnerability Validation,** asses the results:

true positive (when the scanner finds a vulnerability and it does exist),

false positive (reports a finding and the vulnerability doesn't exist),

true negative (if the there is no finding and there is no vulnerability)

false negative (no finding but there is vulnerability)

Then when analysing scan reports when need to focus on:

- Vulnerability severity
- System criticality
- Information Sensitivity
- Remediation Difficulty

- Environmental variables

Correlating Scan Reports

Correlate scan results with others source of information, such as:

1. **Industry standards:**

PCI DSS CVSS

CVSS Score	Severity Level	Scan Results
0.0–3.9	Low	Pass
4.0–6.9	Medium	Fail
7.0–10.0	High	Fail

2. **Technical Information Sources:**

- Configuration management systems
- Log repositories
- Other data sources

3. **Trend analysis:**

Compare to other vulnerability trends

Vulnerability Response and Remediation

Spotting the vulnerability involves a response:

- Patch affected systems
- Segment the network (a compensating control)
- Exception? Exemption?

Penetration Testing

Penetration testing

Penetration testing place professionals as attackers, their goal is to defeat security controls. When meeting up with the company doing the test we need to clarify the permitted scope of the testing (the target systems and the techniques) in the **Rules of Engagement** formal document.

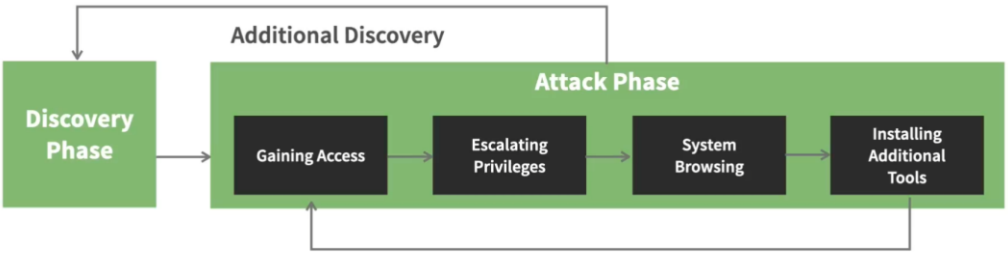
Types:

- **Physical** penetration testing (example: penetrating to the building)
- **Offensive** penetration testing (acting as attackers)
- **Defensive** penetration testing (assessing the effectiveness of security policies)
- **Integrated** (combines offensive and defensive)

Environment information:

- **Known environment**
- **Partially known environment**
- **Unknown environment**

Penetration testing phases:



Discovery phase: may include active and passive reconnaissance (using tools such as: Open-Source Intelligence, foot printing, wardriving, war flying, UAVs)

Attack phase: gain access to the system, escalate privileges, system browsing (lateral browsing), install additional tools to gain deeper access to the network.

Pivot: after exploiting a vulnerability in the system attackers use that system as a base to target (to pivot) other systems.

Persistence: after exploiting a vulnerability attackers install tools on the system to allow future access.

Responsible Disclosure

Zero-day vulnerability when a researcher discovers a vulnerability that no one else has discovered. The **windows of vulnerability** begins with the initial discovery of an issue and ends with a successful patch.

Vulnerability disclosure options:

- Share privately with the vendor
- Publicly disclose with the security community
- Keep it secret for personal use or sale

Responsible disclosure: share newly discovered vulnerabilities with the vendor first, provide a deadline to the vendor otherwise it will be publicly disclosed.

Bug Bounty

Bug bounty allows attackers to exercise their skills and monetise their findings in a completely legal and legitimate manner. Apart from in-house programs, there are vendors that specialise designing bug bounty programs:

Fully managed: the vendor validates and provide analysis to the customer

Self-managed: is the customer that validates and analyse results

TorosTechnology.com

Security alerting, monitoring, and automation

Logging security information

- **Network logs (NetFlow)** tells us about the systems on a network and the amount of information they exchanged
- **DNS logs**, provides information about network names lookups providing information about possible communication with external systems.
- **System logs**, information about the inner working of the OS (security events)
- **Application logs**
- **Authentication logs**
- **VOIP logs** provide insight of the traffic of the network using SIP (Session initiation protocol)
- **Dump files**
- **Vulnerability scans**

Syslog is a protocol that supports **text-based** log monitoring (Linux), its versions: syslog is the original standard and rarely used today, **syslog-ng** added security and delivery enhancements in 1998, **rsyslog** further enhancements 2004, **journalctl binary journal format**

Syslog has 4 components:

- **Header**: time stamp, source address
- **Facility**: source of the message (facility 0: kernel, facility 1: user message, facility 2: mail service)
- **Severity**

Severity	Description
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

- **Message**

Tagging allows us to facilitate searching, filtering and analysis

NXLog centralizes the management of disparate logs

TorosTe

SIEM

Security Information and Event Management SIEM have 2 major functions in an enterprise network:

Central, secure collection for logs across of the organization (firewall logs, web server logs, data server logs, router logs)

Source of AI: SIEMs detect patterns of malicious activity

SIEM provides this information through **dashboards**

SOAR Security Orchestration Automation and Response go beyond SIEM capabilities to further automate security operations and respond in 2 ways:

- **Playbooks** are processed focused response to security events including both human and automated actions
- **Runbooks** are automated responses to security events

Monitoring Activities

- **Monitoring**: continuous observing activities for irregularities
- **Alerting**: notifies personnel of anomalies
- **Scanning**: automatically seek vulnerabilities
- **p** consolidates monitoring, alerting and scanning into data

If the system is believed to be compromised:

1. **Quarantine**: isolates the system
2. **Alert Tuning**: adjust parameters of the alerts to reduce the noise

Endpoint monitoring

- A single end point device can serve as the jumping off point for a broader attack.
- Unusual file system activity can be a **data exfiltration attempt**
- Behaviour monitoring can detect exploit techniques, is good to have **behaviour baselines**
- **User and Entity Behaviour Analytics (UEBA) compares** user to behaviour to normal standards using machine learning.

TorosTechnology.com

Automation and Orchestration

Security Orchestration, Automation, and Response (SOAR) automate tasks (repeatable and do not require human interaction) that cross multiple systems, improves the use of threat intelligence (by bringing information about threats into the SOAR platform)

Scripting (Python, Bash and PowerShell) can automate repetitive tasks such as user provisioning, resource provisioning, guardrails, security groups. However, over relying in automation could lead to a **single point of failure**

Secure Protocols

TLS & SSL

Digital certificates allow the secure exchange of public encryption keys. **TLS** uses digital certificates to facilitate secure communication using **session keys (ephemeral keys)** over the network, is a protocol that uses other cryptographic algorithms, depends on **cipher suits** (pairing of encryption and hash functions)

- **SSL (Secure Sockets Layer)** is insecure and predecessor to TLS
- **OpenSSL** is a TLS open-source project although some vulnerabilities had been discovered
- **SSL Inspection** performs a friendly man in the middle attack to inspect network traffic

IPSec

IPsec adds security capabilities to TCP/IP using **security association SA** to allow systems to communicate the cipher suites they support to each other, can be used in **tunnel mode** in **site-to-site VPNs** encrypting the traffic in the tunnel, or in **transport mode** in end-user VPNs clients to connect individual PCs to a remote network, IPsec secures the entire payload in encrypted communications using 2 protocols:

- **Encapsulating Security Payload ESP** provides confidentiality and integrity
- **Authentication header AH** ensures no changes are made to the header or payload while is on transit

TorosTechnology.com

Securing Common Protocols

- **HTTPS** adds **TLS** to web browsing
- **Telnet** is insecure, all data sent back and forth is unencrypted
- **SSH** TCP 22 is secure and exchanges sessions keys same as TLS
- **FTP** is insecure
- **TFTP (Trivial)** is insecure
- **FTPs** add TLS
- **sFTP** adds SSH
- **SCP Secure Copy** provides secure cmd file transfer over SSH
- **SRTP Real Time Protocol** is used for secure VoIP
- **NTP Network Time Protocol** synchronises system clocks is **insecure**
- **NTPSec** is secure

- **POP 110** Insecure **POP3 995** secure
- **IMAP 143** Insecure **IMAPS 943** secure
- **SMTP 35** Insecure **SMTP over TLS 587** secure
- **S/MIME** secure messages and attachments on emails at application layer
- **DNSSEC** add digital signatures to **DNS** verifies that DNS records are authentic
- **DHCP** runs without authentication but in Windows you can limit the servers allowed to run DHCP services
- **LDAPs** is secure for Directory Service communications

SPF, DKIM, DMARC

Sender Protection Framework (SPF) allows mail owners to specify the mail servers that are allowed to send messages from the domain.

DKIM Domain Keys Identified Mail uses digital signature technology to allow mail servers to digital sign legitimate outbound messages. DKIM uses a **public-private key pair**, the public key is the DNS records (DKIM record) so everyone can find it and the private key is kept secret. The **e-mail signature** is added to the **e-mail header.**

DMARC Domain Message Authentication Reporting and Conformance is a protocol that ties together SPF and DKIM.

ToroisTechnology.com

Email gateways

An **Email Gateway** is a system designed to monitor and filter inbound and outbound traffic; malicious e-mails are intercepted before they reach end user. They also enforce an organization's data-sharing policies.

Identification

Identification, Authentication, Authorization, Accounting

The access control process consists of three steps:

1. **Identification**, an individual **claims** their identity (username)
2. **Authentication**, the individual **proofs** their identity (password, MFA)
3. **Authorization**, the individual is **allowed** to access the system (ACLs) & **Accounting** tracks the user activity.

Usernames and access cards

Identification mechanisms uniquely identify each user in a system

1. **Username**: identification
2. **Access Cards:** identification, proof of employment, may perform authentication

- **Magnetic stripe cards** can be easily duplicated and are considered **insecure**
- **Smart cards** contain an integrated circuit chip reader to proof the authenticity of the card
- **Card readers** interact with the card's chip
- **Proximity cards**, an antenna in the card communicates with the reader, **passive cards** must be placed into or close to the reader and they receive power from the reader that energizes the chip, so they last forever, **active cards** contain batteries and transmitters (tolls transponders)

Biometrics

Uses something you are (fingerprints, face ID), they are identification and authentication tool.

Registration and Identity Proofing

Registration and Identity proofing help us create an individual's system account. Steps: *Request* > *Approval* > *Identity Proofing by HR* photo identification, fingerprints, background checks > *Issuance*

TorosTechnology.com

Authentication

Authentication factors

- **Something you know**: password
- **Something you have:** MFA, key fob
- **Something you are**: biometrics, fingerprints
- **Somewhere you are**: physical location

Errors in authentication:

- **False acceptance**: (serious) system misidentifies an individual as an authorised user, measured by the **false acceptance rate FAR**

- **False Rejection:** system fails to recognise an authorized user, measured by the **false rejection date FRR**
- Errors should be measured using the **crossover error date CED** (where FRR and FAR meets)

Multifactor authentication

MFA combines 2 or more different authentication methods.

Something you have

- **Physical tokens** are rarely used today, **HOTP (hardware OTP**) technology
- **Smartphones (soft token technology)** replaced physical tokens, they provide **OTP One-time passwords** generated by **TOPT (Time OTP)** uses time in conjunction with a shared secret
- **SMS and phone calls** provide weak security
- **Push notifications** through a smartphone app
- **Static codes** provide backup authentication
- **Smart cards**

TonosTechnology.com

Passwords

Most common authentication form, in terms of password complexity **NIST** says that users should be allowed but not required to use a variety of complex characters if the organization uses MFA. NIST also recommends that passwords should not expire.

Passwords Managers

Password managers encrypt passwords

Passwordless authentication

Passwordless authentication is used among others with security keys (public key / private key). It provides phishing resistance, however losing the key can lockout the account

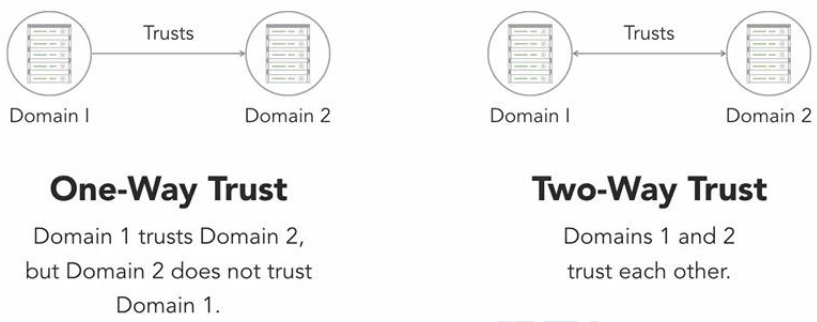
Federation and SSO

Federation occurs when logging to a website using google, Facebook, apple account.

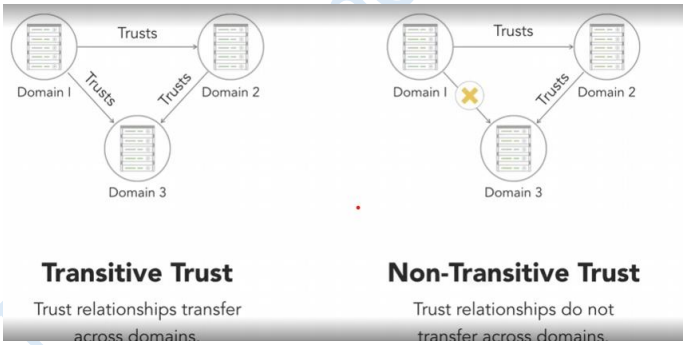
Single Sign On SSO authentication systems that shares the session across multiple systems, just need the users to logon once a day.

Trust relationships across different authentication domains are described in terms of:

- **Direction** (one way or two way)

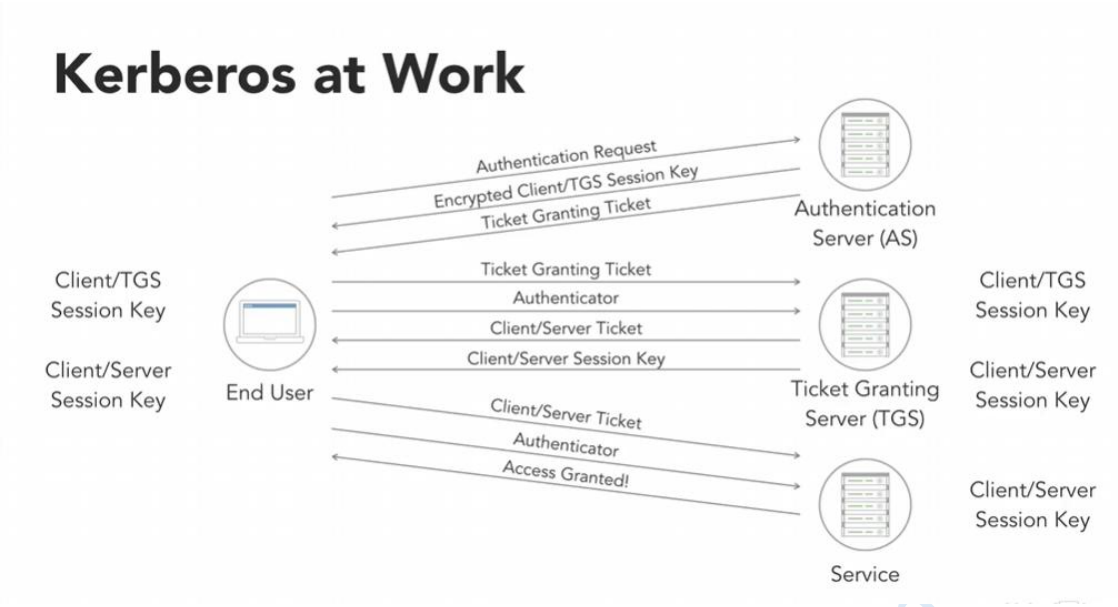


- **Transitivity** (transitive or nontransitive)



Kerberos and LDAP

Kerberos (88) is one of the core protocols for Microsoft Active Directory, provides authentication and authorization in Windows and Linux. Kerberos is a ticket-based authentication system that allows user to authenticate to a centralized service and then use tickets to gain access to distributed services



LDAP 389 (LDAP Secure 686) allows services on a network to share information about users and their authorizations in an open format.

Active Directory uses LDAP in combination with Kerberos. Kerberos handles authentication, LDAP allows to query information stored in the directory service

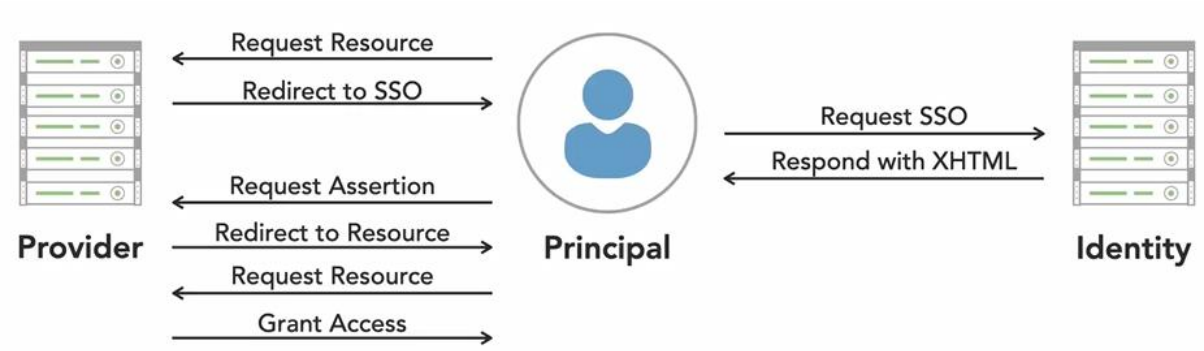
NTLM Authentication, is an older Microsoft technology also known as **NT LAN Manager** before Kerberos, uses weak encryption, can be susceptible to **pass the hash** attack

ToroisTechnology.com

SAML

Security Assertion Markup Language SAML allows **SSO** within a web browser across various systems. 3 actors:

1. **End user** (a.k.a principal) that wants to use a web-based service
2. **Organization** (Identity Provider) providing proof of identity
3. **Web service** (service provider) that the end user wishes to access



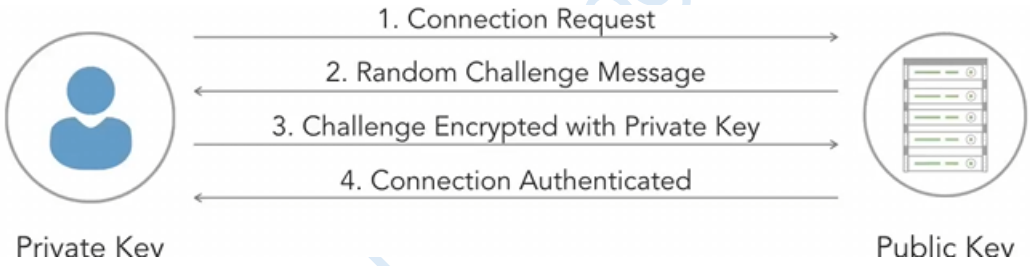
OAuth and OpenID Connect Users

OAuth and OpenID are related protocols, provide a federated SSO for the web, LinkedIn, Google, Facebook use these protocols.

OAuth is an authorization protocol; OpenID Connect is an authentication protocol

Certificate-based authentication

Certificate-based authentication is used for server-to-server communication using SSH, smart cards, network access. Digital Certificates can be used for authentication, provide a trusted copy of a public key to third parties. **Key-based authentication:** first you create a public-private key pair retaining the private key as secret and sharing the public with the server



Authorization

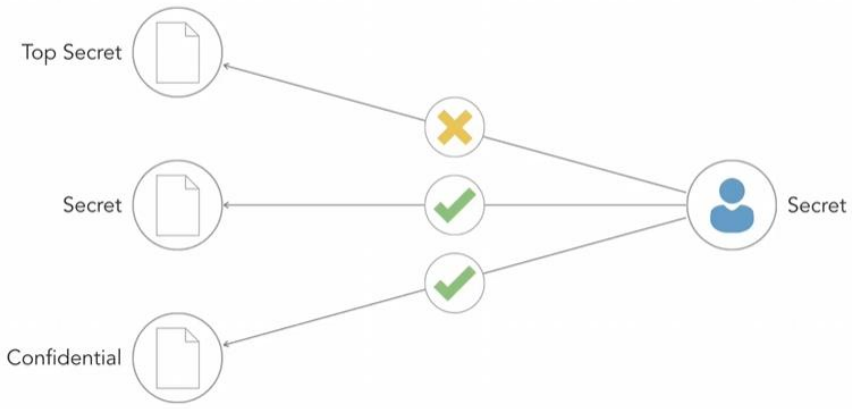
Authorization

Authorization has 2 principles that leads to strong security:

1. **Least privilege,** just necessary permissions to do the job, need to be aware of **privilege creep** that occurs when users accumulate excess permissions after shifting job responsibilities, to avoid privilege creep is necessary to do **accounts review**
2. **Separation of duties** any critical business function should have 2 or more individuals

Mandatory Access Control (MAC)

MAC systems are the most stricter access control; the OS itself restrict the permissions granted to users and processes on system resources. Users can't modify these permissions. The US government uses MAC to protect classified information with labels to systems and users such as **top secret, secret and confidential.** The most common example of and OS implementing MAC is **SELinux (Security Enhanced Linux)**



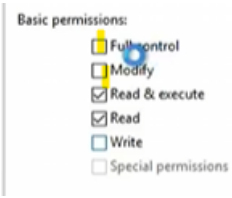
Discretionary Access Control (DAC)

Offers a flexible approach to authorization, permissions may be set by the file owners, computers, and other resources (full control, read and write, read only)

NTFS New Technology File System permissions are an example of DAC

Access Control Lists

Resource owners set DAC permissions using ACLs (f**ull control, read and write, read** (read only, won't be allowed to run .exe files)**, read and execute** read and execute the file if it's .exe)**, modify** goes beyond read and write and let users delete files)



Advanced Authorization Concepts

- **Implicit Deny (Default Deny)** any action that is not explicitly allowed must be denied. Example Firewalls.
- **RBAC Role-based access control**, permissions are grouped together into functional roles and users are assigned to those roles
- **ABAC Attribute-based access control**, more generalized that RBAC, admins write security policies based on the attributes of a user, object and situation. For example, managers allowed to check an employee salary if under his management
- **Location-based control,** limits access based upon physical geographic location
- **Time of day restriction**

TorosTechnology.com

Account Management

Understanding account and privilege management

Account administrators must implement **Least privilege & Separation of duties** principles, also, some companies implement **job rotation** to prevent job fraud, **mandatory vacation** where employees no access to systems.

Account administrators must implement **naming convention** and **account management life cycle** (provisioning, modifying roles, modifying permissions, deprovisioning)

Privileged access

Privileged access management **PAM** monitors the activity of privileged users, also provides:

- **Password vaulting** (stores administrative passwords)
- **Command proxying** (send commands to the system on behalf of the privileged user)

- **Monitoring** (logs administrative user activity)
- **Credential Management** (Rotates passwords and access keys)
- **Ephemeral (temporary) accounts** grant temporary access (**Sudo** command)

Privileged account management solutions should provide an **emergency access workflow** in case the user needs to bypass the account manager and access a system with admin privileges.

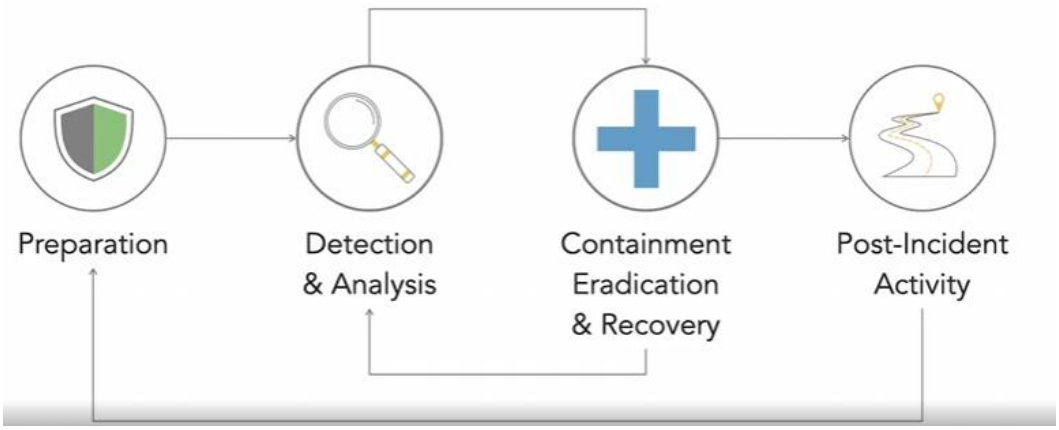
Provisioning and Deprovisioning

- Provisioning = onboarding
- Deprovisioning = offboarding
- **Routine workflow,** disable accounts on a scheduled basis for planned departures.
- **Emergency workflow**, immediate suspends access when user is unexpectedly terminated.

Incident Response

Incident Response Plan

NIST SP 800-61



Recommends that every organization should have an incident response plan that provides structure during cybersecurity incidents, its elements:

- **Statement of Purpose** (reason for the plan and its scope, incident types)
- **Strategies and goals** for incident response

- **Approach to incident response** roles and authorities
- **Communication with other groups**
- **Senior leadership approval**

Incident Identification

SIEM Security Incident and Event Management is a security centralised solution that collects information from different sources, analyses it for signs for security incidents and retains it for later use.

- **First step: First responder must act quickly isolating the affected systems** quarantine the system
- Incident response should be integrated with **threat intelligence programs**
- **Counterintelligence hinders** adversary abilities to gather intelligence

Escalation and Notification

Second step: After containment (quarantine) move into escalation and notification mode. It evaluates the incident severity, escalate response to appropriate level, notifies management. Triaging incidents:

- **Low impact**, usually handled by first responders
- **Moderate impact**, significant impact that triggers the whole response team activation, requires notification to management
- **High Impact,** may cause critical damage to information or systems, immediate full response needed

Mitigation

Third step: Mitigation allow us to contain the damage and loss caused to the organization by performing a full range of incident containment activities, **mitigation ends with stability**, business functioning without danger. NIST suggest 6 criteria: damage potential, evidence preservation, service availability, resource required, expected effectiveness, length of time for the solution to be in place

TorosTechnology.com

Containment techniques

- **Segmentation** is a network security technique (Quarantine VLAN)
- **Isolation** takes segmentation to the next level, instead of moving compromised systems to a different VLAN, they move it to a network disconnected from the rest of the network
- **Removal,** completely disconnects the quarantine network

Incident eradication

Eradication
& Recovery

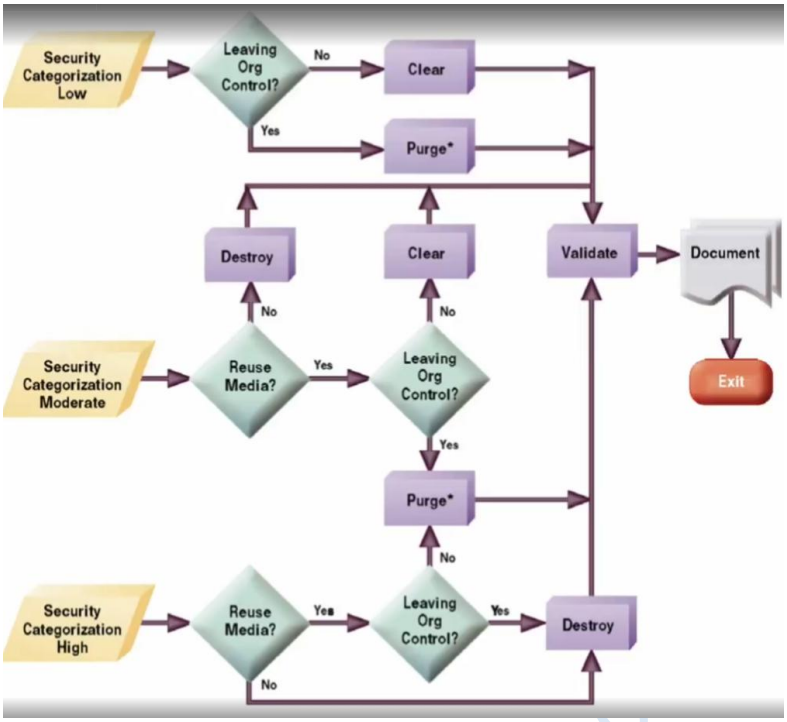
The goal of **eradication** is to remove all traces of an incident from system and networks. **Recovery:** restores normal operations. To rebuild an affected system is necessary re-image the machine or factory reset network devices and appliances, is also necessary to correct the security issues that led to the incident in first place (apply security patches, strong user passwords).

Endpoint security practices: whitelisting, blacklisting, quarantine, ACLs

Enterprise security controls: firewall rules, MDM, DLP, URL and content filtering, update or revoke digital certificates

Sanatization techniques: clearing (overwriting sensitive information), **purging** (cryptographic functions, degaussing techniques), **destroying.**

TorosTechnology.com



Post incident activities

- **Lessons learned** reflects in their role during the incident response efforts and offer feedback (what happened? What time? Performance? procedures adequate? Improvements? Corrective actions?)
- **Report** (lessons learned and recommendations)
- **Change Management Process** (update incident response plan as needed)
- **Incident Summary Report** (**root cause analysis** will help making similar mistakes, retain **evidence**)

Incident Response Training and Testing

Train your incident response ream to keep skills sharp, **tabletop exercises** gather the team together, **simulation test** (how will you respond in a specific scenario)

Forensics

Digital Forensics

Digital forensics investigate techniques that collect, preserve, analyse and interpret digital evidence. Investigations must never alter evidence.

- **Volatility:** evidence may not last long. **Volatility order**: N*etwork traffic* > *Memory contents* > *System Config and process data* > *files* (including temporary files) > *logs* > *archived records*
- **Time offset:** check precise time by comparing the time stamps with a reliable source
- **Video Recordings**
- **Witness statements**

System and file forensics

Never work with the original evidence unless necessary, better to create copies or images**. Write blockers (forensic disk) controllers** prevent accidental modification of disks when imaging.

Hashing protect evidence, hashes are unique, and a **digital signature** can be added to provide non-repudiation.

File metadata contains information about the file creation, last modified, time stamps.

Other forensic sources**: screenshots, memory contents, process table, OS Configuration** if they encounter a system in a running state

Chain of Custody

Provides a paper trail of evidence. Physical evidence should be **labelled** and **sealed**, including **log** events. Evidence logs must be available to present in court.

TerosTechnology.com

E-discovery and evidence of production

E-discovery is a legal mechanism to gather digital data in legal proceedings; it has 3 steps:

- **Preservation**, sys admins must prevent automatic deletion of relevant logs
- **Collection** Security teams often assist in collection efforts (file servers, endpoint systems, email messages, enterprise systems and cloud services)

(if the dispute moves forward, attorneys must review documents = production)

- **Production** produce evidence

Investigation data sources

Logs: firewall logs, application logs, endpoint logs, OS logs, IDS / IPS logs, network logs.

Other data sources: metadata, vulnerability scans, automated reports (done by security tools), dashboards (to preset data), packet captures

ToroisTechnology.com

DOMAIN 5 – Security Program Management and Oversight

Security Policies

Security Policy framework

Written documents that have 4 different types of documents

- **Policy** describes security expectations, **mandatory**
- **Standards** provide **specific** details of security controls, **mandatory**
- **Guidelines** provide **advice**, including best practices, **not mandatory**
- **Procedures** step by step **instructions,** depending in the procedure could be **mandatory or optional**

Security Policies

- **Data storage policies**: appropriate storage locations, ACLs, encryption, encryption requirements, appropriate data transmission and its mechanisms.
- **Data Lifecycle policies:** describe end of life for data, data retention policies (minimum, maximum), data disposal policies
- **Acceptable Use Policies AUPs** provide appropriate ways to use computing resources
- **Business Continuity and disaster recovery policies**
- **Incident response policies** (identifying, containing, communicating, eradicating, recovering, learning from the incident)
- **Software development lifecycle SDLC** formalize security requirements for software development
- **Change Management** review, approve and implement proposed changes to information systems

Teres Technology.com

Security Standards

Security standards provide technical and operational requirements to an organization. Types:

- **Passwords standards** (length, reuse, complexity)
- **Access control standards** (active use and decommissioning; credential for devices, admin and root devices)
- **Physical security standard** (access control systems)
- **Encryption standards** (in transit and at rest)

Security Procedures

Step by step documentation:

- Change management
- Onboarding & offboarding
- Playbook (actions of the incident response team when specific accidents occur)

Policy monitoring

Policy framework should be careful monitored and revised. Example:

- **Regular reviews**
- **Laws and regulations**

Policy considerations

- **Regulatory and Legal**, not adhering could result in non-compliant penalties.
- **Industry**, each industry has their own set of security standards
- **Location** local, national and regional policies

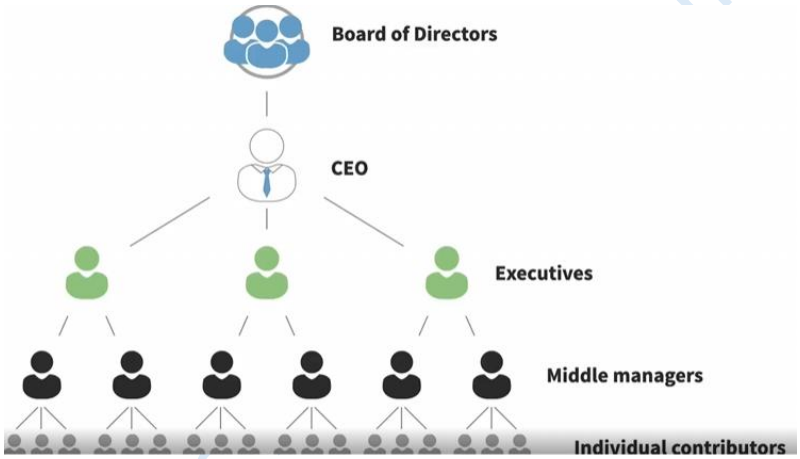
TorosTechnology.com

Security Governance

Security Governance structures

Governance ensures that all parts of an organization remain aligned with its strategic goals. Shareholders elect a **board of directors** (often major shareholders with expertise in corporate governance) to represent them although the majority of board members should be independent. They meet monthly or quarterly.

The board appoints a **CEO (Chief Executive Officer)** to lead the organization and lead day to day operations. The CEO delegates Security to a **CISO Chief Information Security Officer**



Governance types:

- **Centralized Governance: top-down** approach where a central authority creates policies and standards.
- **Decentralized Governance**: **bottom-up** approach where individual business units are delegated the authority to achieve cybersecurity objectives
- May include **internal committees**, subject matter experts such as regulatory agencies

Data Security Roles

- **Data controllers** determine the reasons and methods for processing PII
- **Data Processors**, are service providers that process PII on behalf of data controllers

Roles:

- **Data owner (highest):** business leaders that make final decisions and are responsible for the data privacy
- **Data Stewards:** handles of the day-to-day governance activities, delegated from the data owner, ensure data protection (encryption, backups, ACLs)
- **Data Custodians:** store and process information (usually IT)
- **Data subjects** are the individuals whose data are being processed

Organizations subject to **European Union General Data Protection Regulation GDPR** requires the formal designation of a **Data protection officer DPO**

Risk Analysis

Risk Assessment

Identify and Prioritise risks to spend precious resources based in **likelihood** of occurrence and **impact** in the organization. Key terms:

- **Threats:** external force jeopardizing security (natural occurring, human made such as hacking or terrorism).
  EXAM TIP: **Theat Vector,** are methods that an attacker uses to exploit a vulnerability
- **Vulnerabilities:** weakness in security controls that a threat may exploit to undermine CIA of information or systems.
- **Risks:** are the combination of a vulnerability and a corresponding threat

TorosTechnology.com

Risk assessment timing types:

- **One-time risk assessment** when implementing a new system or implementing significant changes to an existing one
- **Ad-hoc risk assessment** responds to immediate and unforeseen needs
- **Recurrent risk assessment:** scheduled at regular intervals, used automated tools

Categories of techniques:

Qualitative risk assessments use subjective ratings to evaluate risk likelihood and impact (low, medium, high)

Quantitative risk assessment uses numeric ratings to evaluate risk likelihood aids data-driven decision-making, Security professionals perform a quantitative risk assessment for a single risk asset pairing at a time. Variables values:

- **Asset Value AV** (original cost or depreciated cost or replacement risk)
- **Exposure Factor EF** expected percentage of damage to an asset
- **Single-Loss Expectancy SLE** actual damage if a risk materialises one tie **AV x EF = SLE** (SLE give us impact, but we also need likelihood of a risk)
- **Annualized Rate of Occurrence ARO** is the number of times a risk is expected to occur each year
- **Annualized Loss Expectancy ALE** amount of money we expect to lose each year from that risk asset pairing. **ARO x SLE = ALE**

When it comes to non-repairable and repairable assets:

- **MTTF (Mean time to Failure)** average time for the asset to fail (non-repairable)
- **MTBF (Mean time between Failures)** time gap between failures of a repairable asset
- **MTTR (Mean time to Repair)** amount of time the asset will be out of service to repair

TorosTechnology.com

Security Impact Analysis

Cost-Benefit Analysis, is the cloud worth it? Or on premises?

Cost factor at large Scale: electricity costs, data center facility costs, training costs, consulting services, staff time.

Intangible benefits: increased productivity, scalability, capex to opex, agility, faster access to emerging technologies.

Risk Treatment options

Risk Management/ Treatment analyses potential responses to each risk and implement strategies to control those risks. Strategies:

- **Risk avoidance** (relocate data center because of flooding)
- **Risk Transference** (shift the risk to another organization such as insurance)
- **Risk Mitigation** (reduce likelihood and impact)
- **Risk acceptance** (accepts the risk, dealing with the aftermath)

Every organisation has a **risk profile** (set of risks facing an organization). Level of risks:

- **Inherent risk** (the initial risk)
- **Residual risk** (leftover risk after applying controls)
- **Control risk** (control themselves may introduce some new risks)

Risk appetite describes how much risk an organization is willing to accept. Residual and control risk should be below risk appetite. Types:

- **Expansionary:** willingness to take on higher level of risks (higher rewards)
- **Neutral:** moderate
- **Conservative:** focused on stability

Risk Threshold the level a risk becomes unacceptable

Risk Tolerance, ability to withstand risks and continue operations without impact

ToroTechnology.com

Risk Visibility and Reporting

Risk Visibility and Reporting techniques document and track risks over time. **Risks register (Risk logs)** centralised document with each risk facing an organization. Risk register **contains**: description, categorization, risk owner, risk assessment, risk rating, risk management actions. Information sources: risk assessment results, audit findings, team member output & **threat intelligence** shares risk information between organizations

Ongoing Risk Assessment

Risk Management is an ongoing process:

- **Risk control assessment:** single point in time analysis
- **Control assessment**: test control effectiveness
- **Routine control effectiveness** (technical and operational)

Security Metrics

Metrics evaluate security program effectiveness:

- **KPIs:** mutually agreed measurements, they look back and evaluate the success of the program
- **KGIs Key Goal Indicators:** measure progress towards defined goals
- **KRIs Key Risk Indicators:** they look forward, they measure how much risk exists

ITIL KPIs: decrease in breaches, decrease in breach impact, increase strong SLAs, number of new controls, time to implement controls, number of incidents, training events.

KRI Criteria: business impact, implement measure and support the indicator, reliability, sensitivity

TonsTechnology.com

Supply Chain Risk

Managing vendor relationships

Vendors play a crucial role in the IT supply chain. Ensure vendor security policies are at least the same level of effectiveness as your own.
Lifecycle: *Vendor Selection>Onboarding>Monitoring> Offboarding*

Managing agreements

- **NDAs Non-Disclosure Agreements** protects the confidentiality of information
- **SLRs Service Level Requirements** that a customer has for any aspect of a vendor's performance (response time for example) SRLs are documented in **SLAs**
- **N a** Document aspect of the relationship, no legal binding.
- **MOA** Formal document, outlines terms and details of an agreement between parties
- **BPA Business partners agreements** 2 or more companies join and develop a project
- **MSA** if the joint companies are involved in more than one project, including all key terms
- **SOW** if a new project comes to the MSA can be included through a SOW

TorosTechnology.com

Vendor Information Management

Agreements should contain clear data ownership language. Prohibit sharing data with third parties

Privacy and Compliance

Legal and compliance risks

Global, national, territory, state local and regional laws protect sensitive information. **PCI DSS Payment Card Industry Data Security Standard** applies worldwide. Noncompliance may include fines, sanctions loss of license.

Compliance Monitoring and reporting

- **Internal Reporting:** regular updates to management, gap analysis, recommendations. **Internal monitoring** uses internal audits, reviews and checks to verify compliance
- **External compliance:** reports and evidence submitted to regulatory authorities. **External monitoring** involves third party assessments
- **Automation:** assists with compliance monitoring efforts
- **Due Diligence:** understanding legal and regulatory requirements
- **Due care:** controls are effective and maintained. **Acknowledgement** states that employees and business are aware of regulatory requirements. **Attestation** state that their practices adhere to these policies

Audit and Assessments

Audits and Assessments verify that security controls are functioning properly protecting CIA.

Audits follow a formal standard and use planned tests, they have a cleared defined scope; **internal auditors** work for the organization but report independently, **external auditors** independent third party firms.

- **User access reviews:** assessors validate rights and permissions granted to a user
- **Gap analysis:** road map

TerosTechnology.com