1. Security governance through principles and polices

CIA (Confidentiality, Integrity, Availability)

Confidentiality – (subject- user)

Management of the relationship between subjects and objects is known as access control. Confidentiality and integrity depend on each other.

Sensitivity – quality of information. which could cause harm if it is disclosed. **Discretion** – an operator can control disclosure in order to minimize damage. **Criticality** – Level to which information is mission critical**; concealment –** act of hiding or preventing disclosure. **Secrecy; privacy; seclusion -**storing something in an out of the way location. **Isolations**

Integrity – concept of protecting the reliability and correctness of the data. Prevents unauthorized alternations. It includes accuracy, truthfulness, authenticity, validity, non-repudiation, accountability, responsibility, completeness and comprehensiveness

Availability - it depends on integrity and confidentiality. usability, accessibility, and timeliness.

Five Elements of AAA services

- **Identification** – claiming an identity when attempting to access a secured area or system; **Authentication –** proving that you are that identity.
- **Authorization –** defining the permissions(allow/grant/deny) of a resource and object access for a specific identity.
- **Auditing-** recording a log of the events and activities related to the system and subjects.
- **Accounting-** reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions.

Protection Mechanisms

- **Layering –** also known as defense of depth- use of multiple controls in a series. Serial configurations are very narrow, but very deep. Parallel configurations are wide but very shallow.
- **Abstraction** – it is used for efficiency. Used to define what types of data an object can contain. Create group, classes and put data into it.
- **Data hiding** - security through obscurity makes sense here. Intentionally hiding or not revealing.
- **Encryption –** art and science of hiding meaning or intent of a communication to unintended recipients.

Security governance

collection of practices related to supporting, defining and directing the security efforts of an organization. Security governance is commonly managed by a governance committee or at least a board of directors. Security management planning ensures proper creation, implementation, and enforcement of **a security policy**. A **business case** is usually a documented argument or stated position in order to define a need to make decision or take some form of action. One of the most effective way is **top-down approach**. **Upper and senior management** is responsible for initiating and defining polices for the organization. It is the responsibility of **middle management to** flesh out the security policy into

standards, baseline, guidelines and procedures. **The operational managers or security professionals** to implement the security configuration prescribed in the security management document. finally **end users must** comply with all the security polices of the organization.

Security management is a responsibility of upper management.

Strategic plan – long term plan. Fairly stable -it defines the organization security purpose. It is useful for about five years if it is maintained and updated annually. **This also serves as the planning horizon.** Long term goals and visions for the future are discussed here. This plan should include a risk assessment.

Tactical plan -mid-term plan – it is for about a year- ad hoc based plans. Some examples are project plans, acquisition plans, hiring plans, support plans.

Operational plan - short term plan, highly detailed plan based on the strategic and tactical plan. Must be updated often (monthly or quarterly) it tells how to accomplish a task /goal of the organization. Specific plans with milestones, dates, and accountabilities provide the communication and direction to ensure that the individual projects are completed.

Security documentation should be concrete.

Organizational process- security governance needs to address every aspect of an organization .it includes acquisitions, Divestitures and governance committees. **acquisitions and mergers place an organization at increased level of risks. assets need to be sanitized to prevent data leakage**. **Storage media should be removed and destroyed as it doesn't guarantee against data remnant recovery. employees released from duty need to be debriefed. This process is often called exit interview**

Change management/change control and data classification are essential to strong security governance. one example of a change management is a parallel run.

Data classification – data is protected based on its need for secrecy, sensitivity or confidentiality.

To implement a classification system, we must follow 7 steps.1. Identify custodian and define their responsibilities .2. specify the evaluation criteria of how it will be classified and labeled. 3. Classify and label each source (owner does this and supervisor reviews it), 4. Document exception, 5. Select security controls that will be applied to each level .6. specify the procedure for declassifying resources and procedure for transferring custody of a resource to an external entity .7. create an enterprise-wide awareness program to instruct about classification system.

2 common classification system.

Government/military

Top secret is the highest and unclassified is the lowest.

- **Top secret** – highest level classification. It is on need-to-know basis. Should have top secret clearance. **Grave damage**
- **Secret** - used for data of a restricted nature. It might cause **critical damage** to national security if disclosure happens.
- **Confidential**- is used for data of a sensitive, proprietary, or highly valuable nature. It will have noticeable effects and **serious damage**. this classification is used between secret and sensitive.

- **Sensitive but unclassified** - used for internal purpose. privacy of individuals. Not technically a classification label.
- **Unclassified** - used for data neither sensitive nor classified .it doesn't compromise anything or cause any noticeable damage.

Easy way to remember is US CAN STOP TERRORISM (first letter lowest to top)

Items labelled as confidential, secret and top secrets are collectively known as classified. The term" classified" is generally used to refer to any data that is ranked above the unclassified level. All classified data is exempt from the freedom of information act as well as many other laws and regulations.

Commercial classification levels

- **Confidential** -Highest level- extremely high sensitive and used for internal purpose only. Proprietary is also called confidential. significant damage.
- **Private** – private personnel data. For internal purpose only. Significant damage
- **Sensitive** - used for data that is more classified than public data. A negative impact could occur for the company if sensitive data is disclosed.
- **Public** - lowest level. No impact

Roles & responsibilities.

- **Senior manager –** ultimate responsible for due care and due diligence. Must sign off security policy.
- **Security professionals**- functional responsibility and implementation. designing and implementing security solutions.
- **Data owner -**owner of the data who classified the data
- **Data custodian –** responsible for protecting data on behalf of owner.
- **User**- end user. Adhering to policy
- **Auditor-** reviewing and verifying that the security policy is implemented, and derived solution are adequate

Security control framework- one of the most important security planning steps is to consider the overall security control framework. More widely used security control framework is COBIT by ISACA. **CONTROL OBJETIVE FOR INFORMAITON RELATED TECHNOLOGY**. Mapping IT security ideals to business objectives

Five key principles are 1. Meeting stockholder needs ,2. covering the enterprise end to end. 3.applying a single, integrated framework 4. Enabling a holistic approach, 5. Separating governance from management.

COBIT is also a guideline for auditors

Other IT security standards are **OSSTMM (open-source security testing methodology manual**)- a peer reviewed guide for testing and analysis of a security infrastructure.

ISO/IEC 27002 (replaced ISO 17799)- For security and related management practices.

ITIL- initially crafted by British govt.

Due care – due care is using reasonable care to protect the interests of an organization- example- security policy, standards, procedures.

Due diligence - Due diligence is practicing the activities that maintain the due care effort. Example- continued application of security policy into infrastructure.

Security policy- is a strategic plan.

1. **Organizational security policy –** focuses on issues relevant to every aspect of an organization.
2. **an issue specific policy** focuses on specific department, function.
3. **system specific policy** focuses on specific systems like hardware, firewall, individual systems.

Regulatory – it is required whenever industry or legal standards are applicable to the organization.

Advisory – it discusses behaviors and activities that are acceptable and defines consequences of violations. Most policies are advisory.

An informative policy is designed to provide info or knowledge about a specific subject such as company goals, mission statements.

Standards – are tactical documents that define steps or method to accomplish the goals and overall direction defined by the security policy.

Baseline -minimum level of security. It is system specific. ex: ITSEC/NIST

Guideline – provides recommendations and servers as operational guide for user and security professionals. Can be customized

Procedure- final element of security policy. Detailed step on how to implement.

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

Microsoft uses SDL- Security development life cycle- supports security at each stage. This supports the mote of s**ecurity by design, security by default, secure in deployment and communication. It is also known as SD3+C. Goals are**

1. to reduce number of security related design and coding defects.
2. to reduce the severity of any remaining defects.

Proactive approach is also called as "defensive approach". this is based on predicting threats and designing in specific defenses during the coding and crafting process.

Reactive approach after the product has been created and deployed. This is known as adversarial approach. This technique is the core concept behind ethical hacking, penetration testing, source code review and fuzz testing.

Fuzz testing is a specialized dynamic testing that provides many different types of input to software to stress its limits and find previously undetected flaws. Provides invalid input wither randomly generated or specifically crafted to trigger known vuln.

Identifying threats.

1.Focused on assets, 2. Focused on attackers, 3. Focused on software.

Microsoft developed threat categorization scheme known as STRIDE threat model. It is used in relation to application and operating systems. It can also be used in other contexts.

Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. STRIDE is typically used to focus on application threats.

PASTA. - Process for attack simulation threat analysis- it is a seven-stage threat modeling technology. It is a risk centric approach that aims at selecting or developing countermeasures in a relation to the value of the assets to be protected.

Seven steps are

1. Definition of the objectives (DO) for the analysis of risks.
2. Definition of the technical scope (DTS)
3. Applications decompositions and analysis (ADA)
4. Threat analysis
5. Weakness and vulnerability analysis
6. Attack modeling and simulation (AMS)
7. Risk analysis and management (RAM)

TRIKE is another threat modeling methodology that focuses on risk-based approach. It provides a method of performing a security audit in a reliable and repeatable procedure it also provides consistent framework for communication and collaboration among security workers.

DREAD is another methodology (Disaster, reproducibility, exploitability, affected users and Discoverability

VAST (Visual, agile and simple threat (VAST) is a threat modeling methodology based on agile project management and programming principle. Goal is to integrate threat and risk management into an agile programming environment on a scalable basis. It is available from community groups, govt agencies and international associations.

To determine the potential attack, indication of data flow and privilege boundaries are used. The process of diagramming is also known as crafting an architecture diagram.

Performing reduction analysis – next step in threat modeling is this. reduction analysis is also known as decomposing the application, system or environment. Divide into smaller parts. And understand each.

5 key concepts in decomposing process

1. Trust boundaries – any location where the level of trust or security changes
2. Data flow paths- The movement of data between locations
3. Input points -Locations where external input is received

4. Privileged operations – Any activity that requires greater privileges than of a standard used account /process
5. Details about security stance and approach – The declaration of security policy, security foundations and security assumptions.

Prioritization and response

Probability x damage potential ranking (high, medium, low/DREAD system)

DREAD is designed to provide flexible rating solution by answering 5 main questions.

1. Damage potential -how severe it is?
2. Reproducibility – how complicated for attackers to re produce,
3. Exploitability – how hard it is to perform attack?
4. Affected users- how many users are likely to be affected?
5. 5.Disoverability -How hard for attacker to discover the weakness.

Supply chain or 3rd party assessment

1. Onsite assessment – visit the campus,

2. Document exchange and review -assess the reviews and reports,

3. Process/policy review,

4. Third party audit – as defined by American institute of certified public accountants (AICPA). Provide SOC reports (Service organization control).

SSAE (Standards on statement for attestation engagements) is a regulation that defines how service organization report on their compliance using various SOC reports. SSALE16 was replaced by SSAE18 as of May 2017. SOC1 audit focuses on description of security mechanism to access their suitability. SOC2 audit focuses on implemented security controls in relation to availability, security, integrity, privacy and confidentiality.

2. Personnel security and Risk management concepts.

Personnel security policies and procedures – Weakest link is people

Hiring steps- creating job description, classification of the job, screening, background verification, training. **Separation of duties** to prevent against collusion (Deterrence). **Collusion** is by two or more people together committing a fraud. **Job responsibilities** – Least privilege. **Job rotation**- to find fraud. Mandatory vacation is important. – cross training. Candidates hiring and screening- BG checks, education verification, checking police, govt records, polygraph test, drug testing and personality testing. **Non- Disclosure agreement (NDA)-** to accept org policies. **Non-compete agreement (NCA)-** prevent an employee with special knowledge from one company to another. It has time limit. **On boarding and termination process and offboarding**

Service level agreement (SLA)

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

Privacy policy requirements -personally identifiable, freedom from unauthorized access to information deemed personal or confidential. Freedom from being observed, monitored or examined without consent or knowledge

In Germany and other member countries of European union, IP and MAC addresses are considered PII in some situations.

Security governance - it is the collection of practices related to supporting, defining and directing the security efforts of an organization. **Third party governance** - by govt body or private auditor.

Documentation review- it takes before an onsite assessment take place. Failed to provide sufficient documentation will lead in loss and avoiding of “authorization to operate (ATO). Complete and sufficient documentation can often maintain existing ATO or temporary ATO(TATO). Once that TATO is lost, again reestablish the process.

RISK MANAGEMENT CONCEPTS –

The possibility that something could happen to damage, destroy or disclose data or other resources known as Risk. Primary goal of risk management is to reduce risk to an acceptable level. The process by which the goals of risk management are achieved is known as risk analysis

Asset- an asset is anything within an environment that should be protected.

Asset valuation – it is a dollar value assigned to an asset based on actual cost and nonmonetary expense.

Threats - any potential occurrence that could cause an undesirable or unwanted outcome for an organization.

Vulnerability – weakness or flaw in the system.

Exposure -it is being susceptible to asset loss because of a threat. There is a possibility that a vulnerability will be exploited by a threat agent or event. Another way of thinking is" what is the worst that could happen? EF- Exposure factor

Risk is the possibility or likelihood that a threat will exploit a vulnerability to cause harm to an asset. Risk= threat x vulnerability

Safeguard or countermeasure – that removes or reduces vulnerability

Attack- it is the exploitation of a vulnerability by a threat agent.

Breach- it is the occurrence of a security mechanism being bypassed by threat agent. Ex: gain access.

Risk assessment /analysis – initiative by upper management.

Quantitative risk analysis – it results in concrete probability percentages. 6 major steps.

1. AV- assign asset value
2. Calculate EF (Exposure factor) &SLE (Single loss expectancy),
3. Calculate ARO (Annualized rate of occurrence),
4. Calculate ALE (Annualized loss expectancy),
5. Research control for each threat,
6. Perform cost/benefit analysis.

ACS (annual cost of safeguard) = (ALE1-ALE2)-ACS

SLE (Single loss Expectancy) = asset value (AV) * exposure factor (EF)

ALE (Annualized loss expectancy) = single loss expectancy (SLE) * annualized rate of occurrence (ARO)

Or ALE = AV * EF * ARO

Quantitative Risk analysis Formula

Exposure factor (EF)	%
Single loss expectancy (SLE)	SLE = AV * EF
Annualized rate of occurrence	(ARO)# / year
Annualized loss expectancy (ALE)	ALE = SLE * ARO or ALE= AV * EF * ARO
Annual cost of the safeguard (ACS)	$ / year
Value or benefit of a safeguard	(ALE1 – ALE2) – ACS

Qualitative risk analysis – Scenario based. Delphi technique -Anonymous feedback & response

Risk response – Reduce or mitigate, assign or transfer, Accept, reject or ignore.

Residual risk = total risk – control gap

Total risk= threat * vuln * asset value

Selecting a control is based on cost/benefit analysis

Implementation of security control

- Technical control /logical control it uses technology
- administrative control – policies
- physical control- security guard

Types of control –

- **Deterrent** - which means discourage example CCTV camera.
- **Preventive control** - locks, fence.
- **Detective control** – job rotation, CCTV, audit logs,
- **Compensating control** -additional control to the existing control eg PII encrypted
- **Corrective control** – it helps to return to the normal state after an incident.
- **Recovery control** - to recover from an incident. extension of corrective control – ex- backup.
- **Directive control** – control or enforce compliance eg security policy.

Security control assessment (SCA) - Vulnerability assessment, pentest. Generally, SCA is a process implemented by federal agencies based on the NIST special publications 800-53A titled "Guide for assessing the security controls in federal information system

Monitoring and measurement, Asset valuation and reporting; continuous improvement

Risk frameworks – NIST Special publication 800-37. This provides guidelines for applying risk management frameworks (RMF)- 6 steps

1. **Categorize** – Information System
2. **Select** – security control
3. **Implement** - Security control
4. **Assess** - security control
5. **Authorize** - information system
6. **Monitor** - Security control

OCTAVE – Operationally critical threat asset and vulnerability evaluation,

FAIR - factor analysis of information risk

TARA - Threat agent risk assessment

Security awareness training program

3. Business continuity planning

The goal of BCP planners is to implement a combination of policies, procedures and process such that a potentially disruptive event has as little impact on the business as possible. BCP focuses on maintaining business operation with reduced or restricted infrastructure capabilities or resources.

Business continuity activities are typically strategically focused at a high level and center themselves on business processes and operations. Disaster recovery plans tend to be more tactical in nature and describe technical activities such as recovery sites, backups and fault tolerance.

The top priority of BCP and DRP is always people.

Four main steps in BCP process –

1. Project scope & planning,
2. Business impact assessment (BIA),
3. Continuity planning,
4. Approval and implementation

1 Project scope & planning - structured analysis of the business's **organization from a crisis planning point of view.** creation of BCP team with senior management approval. An assessment of the resource available to participate in business continuity activities. An analysis of the legal and regulatory landscape that governs an organization's response to **catastrophic event.**

Business organization analysis – first is to perform an analysis of the business organization to identify all departments and individuals who have a stake in the BCP process.

- Operational departments that are responsible for the core services the business provides to its clients.
- Critical support services, such as IT, facility, and maintenance.
- Corporate security team responsible for physical security.
- Senior executive and other key individuals essential for the ongoing viability of the organization.

BCP Team selection –

1. Representatives from each of the organization's departments responsible for the core services performed by the business.
2. Business unit team members from the functional areas identified by the organizational analysis.
3. IT subject matter experts with technical expertise in areas covered by the BCP.
4. Cybersecurity team members with knowledge of the BCP process.
5. Physical security and facility management teams responsible for the physical plant
6. Attorneys familiar with corporate legal, regulatory, and contractual responsibilities.

7. Human resources team members who can address staffing issues and the impact on individual employees
8. Public relations team members who need to conduct similar planning for how they will communicate with stakeholders and the public in the event of a disruption
9. Senior management representatives with the ability to set vision, define priorities, and allocate resources.

Once BCP team is selected, their first duty is to do business organization analysis again to check whether initial analysis done by the small group is good or not.

Resource requirements

BCP Development The BCP team will require some resources to perform the four of the BCP process (project scope and planning, business impact assessment, continuity planning, and approval and implementation), It's more than likely that the major resource Consumed by this BCP phase will be effort expended by members of the BCP team and the support staff they call on to assist in the development of the plan.

BCP Testing, Training, and Maintenance The testing, training, and maintenance phases of BCP will require some hardware and software commitments, but once again, the major commitment in this phase will be effort on the part of the employees involved in those activities.

BCP Implementation When a disaster strikes and the BCP team deems it necessary to conduct a full-scale implementation of the business continuity plan, this implementation will require significant resources. This includes a large amount of effort (BCP will likely become the focus of a large part, if not all the organization) and the utilization of hard resources for this reason, it's important that the team uses its BCP implementation powers judiciously yet decisively.

Legal and regulatory requirements – it is essential include company's legal counsel in the BCP process as they are familiar with legal regulatory and contractual obligations.

Business Impact Assessment (BIA) - BIA identifies the resources that are critical to an organization's ongoing viability and threats posed to those resources.

Quantitative decision-making – using numbers. Dollar value to the business

Qualitative decision-making – non-numerical factors such as reputation, customer confidence, workforce stability and other concerns. This results in categorizations (High, medium and low)

Identify priorities - list out all the critical assets- assign AV- asset value to each asset.

Second thing is, **develop (MTD) maximum tolerable downtime. It is also known as maximum tolerable outage (MTO)**. MTD is the maximum length of time a business function can be inoperable without causing irreparable harm to the business. MTD provides valuable information when you are performing both BCP and DRP Planning.

Next is **recovery time objective (RTO)** for each business function. This is the amount of time in which you think you can feasibly recover the function in the event of disruption. **RTO should be less than MTD. So that function it will never be unavailable beyond the MTD.**

RISK IDENTIFICATION – natural risks- man made risks**. The risk identification portion of the process is purely qualitative in nature. List out all the threats.**

Likelihood assessment - how frequently it will happen – ARO (Annualized rate of Occurrence)

Impact assessment - EF (exposure factor), SLE (single loss expectancy) and ALE (annualized loss expectancy)

SLE= AV*EF; ALE= SLE*ARO

Resource prioritization – Final step of BIA. – prioritize the allocations of business continuity resources to the various tasks that were identified and assessed in the tasks of BIA.

Continuity planning – focuses on developing and implementing a continuity strategy to minimize the impact.

Subtasks in continuity planning.

- **Strategy development –** this phase bridges the gap between BIA and continuity planning of BCP development. Decide which one to be accepted risk and which is to be added to the BCP Plan based on the MTD.
- **Provisions and process –** BCP team designs the specific procedures and mechanisms that will mitigate the risks deemed unacceptable during the strategy de**velopment stage. People, building/facilities, and infrastructure are 3 important assets to be protected.**
- **People -** people are important.
- **Buildings/facilities -** 2 areas to be considered – 1. **Hardening provisions –** protect existing facility. 2. **Alternate sites**
- **Infrastructure -**UPS to support computer systems. Alternate systems.

PLAN APPROVAL AND IMPLEMETATION –

- Plan approval - get top management signature to make it best to the people.
- Plan implementation – once approval received, schedule a plan for the implementation.
- Training and education – everyone in the organization should receive at least a plan overview.
- BCP Documentation –

Components of the written BCP plan –

1. **Continuity planning goals -** it remains unchanged throughout the life of the BCP.
2. **Statement of importance –** this reflects the criticality of the BCP to the organization's continued viability. If the letter has CEO signature, it will add weight to the visibility.
3. **Statement of priorities –** Listing the priorities of critical functions with statement to explain.
4. **Statement of organizational responsibility - everyone's responsibility.**
5. **Statement of urgency and timing –** the criticality of implementing the BCP, agreed by the upper management.
6. **Risk assessment-** all quantitative and qualitative figures should be included. It must be updated on a regular basis.
7. **Risk acceptance/mitigation –** it is the outcome of the strategy development portion of the BCP process. Why risk is accepted and why to mitigate details should be added in the section.

8. **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.
9. **Emergency response guidelines -**it should include immediate response procedures (security, emergency response agencies., notifications), list out the individuals who should be notified of the incident (CEO, BCP Team). Secondary response procedures that first responders should take while waiting for the BCP team to assemble. time is very important in BCP.
10. **Maintenance –** it must be living documents. Changes must have version control and older one should be physically destroyed to avoid confusions.
11. **Testing and exercise -** it is to ensure that the plan remains current, and all are trained to perform their duties.

4. Laws, regulations and compliance

Three types - Criminal Law, civil law, administrative law

Criminal law – computer fraud and abuse act, electronic communications privacy act and identity theft and assumption deterrence act provide criminal penalties for serious cases of computer crime.

In the USA, legislative bodies at all the levels of government establish criminal laws through elected representative. At the federal level, both the house of representatives and senate must pass criminal law bills by a majority vote. Then it becomes federal law. It applies in all cases where the federal government has jurisdiction (mainly involve interstate commerce, cross state boundaries, cases that are offenses against the federal government itself. If federal Jurisdiction doesn't apply, state authorities handle the case.

Civil Law- contract disputes, real estate transactions, employment matters and probate procedures. at the federal level both **criminal and civil laws are embodied in the United States code (USC)**. The only role of the government in civil matters is to provide the judges, juries and court facilities used to hear civil cases and to play an administrative role in managing the judicial systems.

Administrative law - In the form of policies, procedures. It is published in the **code of federal** regulations (**CFR)**

Computer fraud and abuse act – first major piece of cybercrime specific legislation in the US. Before that congress had enacted CCCA (**comprehensive crime control act**) of 1984

Any computer used by the US Govt
Any computer used by a financial institution
Any computer used by the US Govt or financial institution when the offense impedes the ability of govt or institution to use that system.

Any combination of computers used to commit an offense when they are not all located in the same state.

Damage threshold raised from $1000(CCCA) **to $5000** (CFAA) Computer Fraud and Abuse Act. Last CFAA change was in 1986 include "federal interest". Then govt made changes in 1994 called **computer abuse amendments act of 1994** Included the following.

1. Creation of any types of malicious code that might cause damage to a computer system
2. Modified the CFAA to cover any computer used in interstate commerce rather than federal interest computer system

3. Allowed for the imprisonment of offenders, regardless of whether they intended to cause damage.

Computer Security Act (1987)

Federal sentencing guidelines - Released in 1991 provided punishment guidelines to help federal judges interpret computer crime laws. 3 major provisions guidelines.

1. **Prudent man rule –** which requires senior executives to take **responsibility for ensuring the due care.**
2. Minimized punishment for infractions by demonstrating **that they used due diligence** in the conduct of their information security policies.
3. 3 burdens of proof for negligence – legally recognized obligation - must have failed to comply with recognized standards - causal relationship between the act of negligence and subsequent damages.

National information infrastructure protection Act of 1996.

Broadens CFAA to cover computer systems used in international commerce in addition to systems used in interstate commerce. national infrastructure like rail roads, gas pipelines, electric power and tele communication circuits. Any international act that causes damages to national infrastructure.

Federal information security management Act (FISMA)

Passed in 2002. Requires that federal agencies implement an information security program that covers the agency's operations. FISMA replaced computer security act 1987 and government information security reform act of 2000.

NIST is responsible for developing the FISMA guidelines.

1. Periodic risk assessments, 2. Policies and procedures, 3. information security for networks, facilities 4. Security awareness training 5. Periodic testing of effectiveness of policies and procedures, 6. process for plan, implement, evaluate and document remedy actions. 7. Procedure for detecting, reporting, and responding to security incidents. ,8. Plans for continuity of operations

Federal cybersecurity Laws of 2014 – this is also called FISMA (Modernization act). It modified the 2002 FISMA. **Defense related cybersecurity issues remain the responsibility of the secretary of defense**. **Intelligence related issues remain with director of national intelligence**.

NIST Standards

NIST SP 800-53 – security and privacy controls. For federal information systems. Commonly used as cybersecurity benchmark

NIST SP 800-171 – protecting controlled unclassified information in **Nonfederal information systems**.

NIST CSF- Computer security framework is a set of standards designed to serve as a voluntary risk-based framework for securing information systems.

National cybersecurity protection Act is to serve as the interface between federal agencies and civilian organizations for sharing cyber security risks, incidents, analysis and warning.

Intellectual property - Intangible assets are collectively referred to as intellectual property. 4 major types

1. **Copyright - copyright and the digital millennium copyright Act** – Works by one or more authors are protected **until 70** years after the death of the last surviving author. works for hire and anonymous works are provided protection **for 95 years** from the date of first publications or **120 years from the date of creation, whichever is shorter.** Books, music work, algorithms. Mathematical functions.
   Digital millennium Copyright act also serves to bring US copyright law into compliance with terms of two world intellectual property organizations (WIPO) – protect copy prevention- CD, DVD. Penalties up to $ 1000000- and 10-years prison.
2. **Trademark – slogans, logos -** for period **of 10 years** and can be renewed for unlimited successive 10-year periods. Without registration TM symbol. With registration R symbol.
3. **Patents – rights of inventors** for 20 years from the date of application is submitted. Must be new, must be useful, must not be obvious.
4. **Trade secrets-** not disclosing the secrets. NDA must be in place to protect

Economic espionage act of 1996. -stealing trade secrets to benefit foreign govt will lead to 15 yrs prison and $500000 fine. For other $250000 and 10 years prison

Licensing - 4 types

- **Contractual license agreements –** written agreement between vendor and customer. This is for high priced software packages.
- **Shrink-wrap license agreements –** written outside of the software packaging. we acknowledge to the terms by breaking the shrink wrap seal. Once upon, it is ack'd. It does not require user ack.
- **Click through license agreement** - common. during the installation, click yes to the terms and agreements
- **Cloud services license agreement** – it does not require any form of written agreement. Simply flash legal terms on the screen for review. Simply click ok to continue the web service.

Import/Export – 2 sets of federal regulations

1.**ITAR (The international traffic in Arms regulations**) controls the export of items that are specifically designated as military and defense items, including technical information related to those items. It is listed on the list called **USML (united states munitions list), maintained in** 22 CFR 121.

2. **EAR (The export administration regulation**) cover a broader set of items that are designed for commercial use but may have military applications. **It is listed on commerce control list** (**CCL)** maintained by U.S. Department of commerce **EAR covers an entire category of information security products**

Computer export controls

US can export high performance computing systems to any country without receiving prior approval from the government except iron, north korea, cuba, sudan and syriya.

Encryption export controls.

The current rule is to submit the product for review by commerce department, it will take no longer **than 30 days**. Once review is done, company may freely export the products.

US Privacy Law.

Fourth amendment – without proper evidence and warrant, no search or arrest should be done.

Privacy Act of 1974 -it mandates that agencies maintain only the records that are necessary for conducting their business and they destroy the same when it is no longer needed. An individual can gain access to records the government maintains about them and to request that incorrect records be amended. **this act applies only to government agencies**.

Electronic communications privacy act of 1986 – it prohibits the interception or disclosure of electronic communication and define those situations in which disclosure is legal. It protects against the monitoring of email and voicemail communications. It is illegal to monitor telephone conversations. Punishment is $500 and prison 5 years.

Communications assistance for Law enforcement Act (CALEA) of 1994 – it amended electronic communication privacy act of 1986. It requires all communication carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology in use.

Economic espionage Act of 1996 – it extends the definition of property to include proprietary economic information. so that the theft of this information can be considered industrial or corporate espionage. No longer restricted by physical constraints.

Health Insurance portability and Accountability Act of 1996(HIPPA) – health maintenance organizations (HMO) handles health related data.

Health information technology for economic and clinical health Act of 2009(HITECH) – in 2009, HITECH was passed by congress. Updated many HIPAA's privacy and security requirements and was implemented through HIPAA omnibus rule in 2013. **Any relationship between a covered entity and a business associate must be governed by a written contract known as business associate agreement (BAA).** Under the new regulations, business associates are directly subject to HIPAA and HIPPA enforcement actions in the same manner as a covered entity. it must notify affected individuals when data breach happens and also notify secretary of health and human services and media when affects more than 500 individuals.

Children's online privacy protection Act of 1998 – in April 2000, it became the law (COPPA)

1.websites must have a privacy note that what information they collect and what is it used for, whether any information is disclosed to third parties. The privacy notice must also have the contact information of the operators of the site.

2. parents must be provided with the opportunity to review any information collected from their children and permanently delete it from the site's records.

3. parents must give verifiable consent to the collection of information about their children younger than the age of 13 prior to any such collection.

Gramm-Leach -Bliley Act of 1999 (GLBA)- became law in 1999. It is for financial institutions, banks and credit providers. GLBA relaxed the regulations concerning the service each organization could provide.

USA PATRIOT Act of 2001 – this is to intercept and obstruct terrorism. Major change is obtaining wiretapping authorizations. It allows authorities to obtain a blanket authorization for a person and then monitor all communications to or from that person under the single warrant.

Another change is that internet providers (ISP) may voluntarily provide the government with a large range of information. it also allows the govt to obtain detailed information on user activity through the use of a subpoena (as opposed to wiretap).

It amends CFAA to provide more severe penalties for criminal act. jail for up to 20 years. PATRIOT Act has a complex history. Many of the key provisions expired in 2015. Congress passed USA freedom act in 2015 which restored key provisions of the PATRIOT act.it remains until December 2019.

Family educational rights and privacy Act (FERPA) – it grants certain privacy rights to students older than 18 and the parents of minor students.

1. Parents/students have the right to inspect any educational records maintained by the institution.
2. Parents/students have the right to request correction of records.
3. Schools may not release personal information from student records without written consent, except under certain circumstances.

Identity theft and assumption deterrence Act – In 1998, it became a law. This makes identity theft a crime against the person whose identity was stolen, and penalties would be up to 15 years jail and $250000 fine for anyone found guilty violating this law.

European Union Privacy Law - Law effective from 1998. Must meet one of the following criteria.

1.Consent 2. Contract 3. Legal obligation 4. Vital interest of the data subject 5. Balance between the interest of the data holder and the interest of the data subject.

Key right of individuals – right to access, to know the data source, to correct inaccurate data, right to withhold consent to process data in some situations, rights of legal action should these rights be violated.

Organizations outside Europe must consider the applicability of these rules due to transborder data flow requirement. American companies doing business in EU can obtain protection under the privacy **shield agreement between** the EU and united states that allows **the department of commerce and the federal trade commission (FTC) to certify busine**ss that comply with regulations and offer them “safe harbor” from prosecution.

US companies doing business in Europe must meet 7 requirements for processing of personal information.

1. **Informing individual about data processing,**
2. **providing free and accessible dispute resolution –** response to complaints within 45 days.
3. **Cooperating with the department of commerce.**
4. **Marinating data integrity and purpose limitation.**
5. **Ensuring accountability for data transferred to third parties**
6. **Transparency related to enforcement actions,**
7. **Ensuring commitments are kept as long as data is held**

European union general data protection regulations (GDPR) -law passed in 2016. Effective from May 2018. It is to provide singe, harmonized law that covers data throughout the European union.

Key provisions

1. Data breach notification requirements- notified with 24 hrs for serious data breach.
2. The creation of centralized data protection authorities in each EU member state.
3. Individuals will have access to their own data
4. Data portability provisions that will facilitate transfer of personal data between service providers at the individual request
5. The "right to be forgotten" that allows companies to delete data when it is no longer needed.

Compliance

SOX for financial systems, PCI DSS for credit card processing systems.

5.Protecting security of assets.

Primary step in asset security is classifying information based on its value to the organization.

Identify and classify assets – first step; organization often include classification definitions within a security policy, then personnel assign labels to the assets. In this context assets include sensitive data, hardware used to process it and media used to hold it.

Defining sensitive data- sensitive data is any information that is not public or unclassified. It can include confidential, proprietary, protected or any other type of data that an organization needs to protect due to its value to the organization or to comply with existing laws and regulations.

Personally identifiable information (PII) – Any information that can identify an individual. NIST SP 800-122 provides formal definition.

Protected health information (PHI) - any health-related information that can be related to a specific person. HIPPA mandates the protection of PHI.

Proprietary data – any data that helps an organization maintain a competitive edge.

Defining data classifications- it is part of security policy or separate data policy. Data classification defines value of data to the organizations. It also defines how data owners can determine the proper classification. confidentiality and integrity will be protected by classifying the data.

US military – Top secret- exceptionally grave damage; secret – serious damage; confidential – damage

Within US, unclassified data is available to anyone and they have to request through **freedom of information act (FOIA).** Some non govt organizations use class 3, class 2, class 1 and class0 levels. Some use confidential, private, sensitive and public.

Sensitive information typically refers to any information that is not public or unclassified.

Defining asset classification- asset classification must match data classification. If a computer is processing top secrete data, the computer should also be given top secret level asset classification.

Determining data security controls –

Understanding data states – data at rest – any data stored in drive, tapes; data in transit- in motion through network. Data in use- when application using it/ temporary storage buffers. (Application cannot process encrypted data, it must decrypt it in memory)

Security administrators use the requirements defined in the security policy to identify security controls.

The identity theft resource center (ITRC) tracks data breaches.

Handling information and assets is important; Labeling/marking assets and data; Handling sensitive information and assets

Storing sensitive data- AES256 provides strong encryption at both file and disk level. Physical control should be there. Environmental control should be there (HVAC)

Destroying sensitive data – NIST SP 800-88 r1 (guideline for media sanitization) provides details (such as clearing, purging and destroying)

Eliminating data remanence – one way to remove data remanence is with a degausser. **degausser** generates heavy magnetic field which realign magnetic field in magnetic media such as traditional hard drives, magnetic tape, floppy disk drives. It is effective on magnetic media.

SSD's use integrated circuitry. So degaussing won't remove data in SSD's. the best of sanitizing SSD is destruction.

Erasing – performing delete operation. Actual data remains in drive. System eventually overwrites the erased data. Anyone can retrieve data using tools

Clearing/overwriting – ensuing that cleared data cannot be recovered using any traditional methods. When media is cleared, unclassified data is written over it.

Purging- more intense form of clearing and it prepares for reuse in less secure environments. It provides an assurance that original data is not recoverable using any known methods. Purging process will repeat the clearing process multiple times and may combine it with another method such as degaussing.

Degaussing – strong magnetic field to erase data. Mainly for magnetic tapes. It is not for CD, DVD & SSD

Destruction- methods are incineration, crushing, shredding, disintegration and dissolving using caustic and acidic chemicals.

Retention - record retention and media retention are most important element of asset retention. Organization has the responsibility of identifying laws and regulations that apply and complying with them for retention. Personnel retention refers to the knowledge that person gains while employed by an organization. NDA prevents this.

Data protection methods

Protecting data with symmetric encryption – the key size is much larger. AES uses key size of 128 or 192 bits. AES 256 uses 256 bits.

AES-Advanced encryption standard – **most popular symmetric algorithm**. NIST selected it as a replacement for old DES in 2001. Microsoft bitlocker uses AES, microsoft's encrypting file system (EFS) uses AES**. It is used till top secret level data by US govt. larger key size it.**

Triple DES /3DES – Replacement for DES. It used 56-bit keys. Newer implementation uses 112 or 168 keys. It is used in smart payment cards like VISA and in European standard cards. Combination of PIN and 3DES used while purchasing.

Blowfish – replacement for DES. It uses 32 to 448 bits. **Linux system use bcrypt to encrypt passwords.** Bcrypt is based on blowfish. It adds **128 additional bits as a salt to protect against rainbow table attacks.**

Protecting data with transport encryption – primary risk of sending unencrypted data over network is sniffing attack.

HTTPS uses TLS; VPN uses TLS and IPsec; L2TP with IPsec provides security for VPN. IPsec include AH (Authentication header) provides authentication and integrity. ESP (Encapsulating security payload) provides confidentiality.

SCP (Secure copy) and SFTP(Secure file transfer protocol) are used to send encrypted file over internal network.

Determining data ownership –

Data owners- ultimate owner. CEO or department head. Responsible for classifying data. NIST SP 800-18 outlines responsibility of data owner.

System/Asset owner – is the owner who owns the asset/system that processes sensitive data.

Business/mission owners – application owner. Who owns that particular system or application.

Data processors - any system used to process data. But in GDPR context it means a natural or legal person, public authority, agency or other body which processes personal data solely on behalf of the data controller. Data controller is the person or entity that controls processing of the data.

Ex company which collects personal information is data controller, the company which process the information is data processors. Violation of gdpr rule fine is 4 % of their global revenue. EU-US privacy shield program known as safe harbor program. US and Swiss created a framework called Swiss-US shield. These are administrated by US Department of commerce's international trade administration.

Privacy shield principles are

Notice; choice; accountability for onward transfer; security; data integrity and purpose limitation; access; enforcement.

Pseudonymization – it refers to the process of using pseudonyms to represent other data. For ex patient 123 refers to the all the information related to that particular patient. GDPR refers to **Pseudonymization as replacing data with artificial identifiers. Tokenization** is similar to pseudonymization. it uses tokens to represent other data.

Anonymization- masking data will help remove the original data.

Administrators is responsible for granting access to personnel using role-based access control.

Custodian helps protect the integrity and security of the data- day to day tasks.

Protecting privacy.

Security baseline – minimum security standard. NIST SP 800-53 outlines 5 security control baselines.

Scoping and tailoring – scoping refers to reviewing a list of baseline controls and selecting only those Controls that apply to the IT system we are trying to protect. Tailoring refers to modifying the list of controls with baseline, so that they align with org mission.

Selecting standards – pci dss, hippa, nist

6. Cryptography and symmetric key algorithms.

Cryptography provides confidentiality, integrity, authentication and nonrepudiation.

Caser cipher – developed by caser. earliest known system. **to encrypt - shifting 3 letters right** side. it is known as ROT3 (Rotate 3). This is substitution cipher (Mono alphabetic). **To decrypt, shift 3 letters to left.** This is vulnerable to **frequency analysis attack.**

American civil war – combination of substitution and transposition and series of flag signals.

Ultra vs enigma

German military adapted a commercial code machine nicknamed enigma for government use. It uses series of three to six rotor to implement extremely complicated substitution. the allied forces began ultra to attack enigma. Japanese used similar machine known as Japanese purple machine.

Cryptography basics

Two main types of cryptosystem enforce confidentiality. Symmetric and asymmetric

Symmetric uses shared secret key (private key) to all users of the cryptosystem

Asymmetric uses individual combination of private and public keys for each user of the system.

Data at rest (stored data) – data in motion (on the wire) – data in use (stored data in active memory of a computer system where it may be accessed by a process running on that system)

Message integrity is enforced through encrypted message digests, known as digital signatures. Integrity can be enforced by both public and secret key cryptosystems.

Authentication verifies the claimed identity of system users and is a major function of cryptosystem. Challenge response is used here. Reversing the word. Ex: apple becomes elppa.

Non-repudiation – provides assurance to the recipient that message was originated by the sender. it also prevents sender from claiming that they never sent message. Non-repudiation is offered only in public key or asymmetric cryptosystems. Not in shared secret key or symmetric key.

Cryptography concepts

p-plain text – cryptographic algorithm – cipher text C

All cryptography algorithm relies on Keys to maintain their security. A key is a number. It is a very large number. Every algorithm has specific key space. Key space is defined by its bit space. Bit size is nothing more than number of binary bits (0s 1s) in the key. Key space is the range of numbers from 0 to 2n where n is the bit size of the key. For example, 128-bit key can have 0 to 2(128). Key should be protected.

Kerchoff principle (security through obscurity). Everyone knows algorithm. Key should be protected.

Cryptographic keys are sometimes called crypto variables.

The art of creating and implementing secret codes and ciphers is known as cryptography. The study of methods to defeat codes and cipher is cryptanalysis. Together cryptography and cryptoanalysis is called cryptology. Specific implementation of code or cipher in hardware and software are known as cryptosystem. – FIPS 140-2

CRYPTOGRAPHIC METHAMATICS

Boolean mathematics- on -true; off- false.

Logical operation AND ^ (Multiplication). 000; 010; 100; 111

OR v (kind of addition) 000; 011; 101; 111.

NOT ~ !- reverse the value. 01; 10

Exclusive OR (XOR +) most important and most used in cryptography if both inputs are true or false, output will be false. 000; 011; 101; 110

Modulo function – mod % - ex 8 mod 6 = 2 ; 10 mod 2 =0 ; 6 mod 8 = 6

One-way functions – mathematical operation **that easily produces output values for each possible combination of inputs but makes it impossible to retrieve input values. Public key cryptosystems are all based on some sort of one-way functions.** there are 8363 five-digit prime numbers. This can be attacked by a computed and brute force algorithm.

Nonce – is a random number that acts as placeholder variable in mathematical functions. Adding randomness to the encryption process. IV- Initialization vector is an example of nonce, random bit string which is same length of block size and it is XORed with message.

Zero knowledge proof - user A doesn't want to disclose password. user b is watching user A accessing. So user b ensures that user A has valid password

Split knowledge - the example of this is **key escrow. using these cryptographic keys, digital signatures and digital certificates are stored in a special database called key escrow database. M of N control requires that minimum number of agent (M) out of the total number(N) of agents work together to perform high security tasks.**

Work function – we can measure the strength of cryptography system by measuring the effort in terms of cost/or time using work function /factor. The size of the work function should be matched against the relative value of the protected asset.

Code vs Ciphers

Code is a symbol that represent words or phrases. ex: the eagle has landed which means the arrival of an enemy aircraft.

Cipher is always meant to hide true meaning of a message. It works on individual characters and bits.

Transposition cipher – rearrange the letters. Apple becomes elppa.

Complicated can be done using **columnar transposition. Ex – the fighter will strike the enemy base at noon" using the keyword attacker.**

Assign number for ATTACKER

17823546

THEFIGHT……..

Output is based on numbers 1, 2, 3, on column wise.

Substitution cipher – replace each character or bit of the plaintext with different character. Caser cipher is the example. ROT3 cipher can be expressed in mathematical form

C=(P +3) MOD 26 ; P=(C-3) MOD 26

Polyalphabetic substitution ciphers use multiple alphabets in the same message to hinder decryption efforts. One of the example of this is **vigenere cipher.** Polyalphabetic substitution protects against frequency analysis attack but vulnerable to period analysis because of repeated use of key.

One-time pads - it is an extremely powerful type of substitution cipher. It uses different substitution alphabets for each letter. **K is the encryption key. function is C=(P+K) Mod 26. One time pad is also known as vernam ciphers**. **The one-time pad must be randomly generated. should not use dictionary words. Must be physically protected.** Cesar cipher uses key length of one, vigenere uses longer key (usually a word). One time pad uses key that is as long as the message itself.

Running key ciphers- also known as book cipher. The encryption key is as long as the message itself and is often chosen from a common book. Sender and receipt will agree in advance to use the text of a chapter from book as key.

Block cipher – operate on chunks or blocks. Apply the encryption algorithm to an entire message block at the same time. Transposition is the example of block cipher. Most modern encryption algorithm implement some type of block cipher.

Stream cipher – works on one character or a bit of a message at a time. Caser cipher is the example of stream cipher. One time pad also an example. stream cipher can also function as block cipher with real time data.

Confusion and diffusion

Confusion occurs when the relationship between plain text and key is complicated that an attacker cannot altering plain text and analyzing resulting cipher text to determine key. Diffusion occurs when a change in plaintext results in multiple changes spread throughout ciphertext. Substitution introduces confusion, transposition introduces diffusion.

Modern cryptography.

DES used 56 bit key- no longer secure. Modern cryptography uses at least 128 bit key. The longer the key size, it is hard to break.

Symmetric key algorithms – (secret key cryptography)

Shared secret key. Used for bulk encryption. Faster. Provides confidentiality.

Weakness – 1. Key distribution. 2. It does not implement non-repudiation .3. the algorithm is not scalable. 4. Key must be regenerated often. Strength – 1. great speed.

Number of keys = n(n-1)/2, n is number of participants

Asymmetric key algorithms (public key cryptography)

Encrypt with receiver public key. Decrypts with receiver private key. It provides support of digital signatures.

Strength – addition of new user requires the generation of only one public key. User can be removed easily. Key generation is required only when user's private key is compromised. It can provide integrity, authentication and non-repudiation. Key distribution is simple process. No pre existing link needs to be exist.

Weakness – slow speed. Many applications use public key cryptography to establish a connection then use symmetric cryptography.

Hashing algorithms – each message will have separate hash value. If two message has same value then it is collision.

Symmetric cryptography.

DES, 3DES, IDEA, Blowfish, skipjack and AES.

DES- published in 1997 and superseded by AES in 2001. Des is no longer used. DES is a 64-bit block cipher that has five modes. The key used by DES is 56 bits long.

ECB- electronic code book – simplest mode and least secure. It is used only for exchanging small amounts of data such as keys. It will produce same encrypted block and eavesdropping will capture it to attack.

CBC- Cipher block chaining -each block of unencrypted text is XORd with the block of ciphertext immediately before encrypted using DES algorithm. It is error propagate. if one block is corrupted during transmission, it becomes impossible to decrypt that block and next block as well. It implements IV and XOR.

Cipher feedback mode- CFB- it is the streaming cipher version of CBC. It works against data produced in real time. It uses memory buffers of the same block size. As the buffer becomes full, it is encrypted and then sent to recipients. it uses an IV and it uses chaining.

Output feedback mode -OFB – DES XOR's the plaintext with a seed value and it does not propagate errors. There is no chaining and transmission errors.

Counter mode -CTR- stream cipher fashion. it uses counter that increments in each operation. do not propagate errors. This allows to break an encryption decryption operation into multiple independent steps which makes CTR mode well suited to use in parallel computing.

Triple DES-

There are four versions of 3DES . First is simply encrypts the plaintext three times using three different keys. K1,K2,K3 . It is known as DES-EEE3 mode. E(K, P) … E(k1,E(K2,E)K3,P)) effective key length of **168** bit

Second is DES-EDE3- also uses three different keys but replaces second encryption operation with decryption operation. E(K1, D(K2,E(K3,P)))

Third version is DES-EEE2 – uses only two keys E(K1,E(K2,E(K1,P))) – Key length 112 bits

Fourth version is DES-EDE2 uses two keys but uses decryption process in the middle E(K1,D(K2,E(K1,P)) 112 bits key length.

IDEA- block cipher it operates in 64 bit block of plaintext . it begins with 128 bit key and it is broken into 52 bit 16 keys. Subkeys act on input text using a combination of XOR. Capable of doing all five modes used by DES. Patented by swiss developers. It is now publicly available . IDEA is implemented in PGP secure email package.

Blowfish -block cipher 64-bit block text. Uses variable key length of 32 bits to 448 bits. Much faster than idea and des.

Skipjack -approved to use in federal information processing standard. 64-bit block of plain text. It uses 80 bit key and support same four mode supported by DES. It supports the escrow of encryption keys . portion of the key with two parties.

RC5 –(32,64,128 block) Key length(0-2040)

AES- Rijndael – three key strength 128,192 and 256. It allows only 128 bit blocks. 128 bit keys require 10 round of encryption; 192- 12 rounds and 256 – 14 rounds.

Two fish- block cipher. 128 block of data and keys upto 256 bits. AES finalists. Prewhitening involves XOR the plain text with separate subkey before first round of encryption. Postwhitening uses similar operation after the 16th round of encryption.

Symmetric key management

- Offline distribution – through mail, physical mode, telephone
- Public key encryption – use it only for key exchange

- Diffie hellman-key exchange algorithm. S RPC employs this for key exchange. Algorithm works on two large prime numbers 1<g(integer)<p(prime number)

Storage and destruction of symmetric keys - When employee leaves an org, key must be changed and encrypts data with new key,

Key escrow and recovery -fair cryptosystem- each portion of the key is given to different parties. **Escrowed encryption standard** -this provide government with technological means to decrypt ciphertext text. The standard is the basis behind skipjack algorithm.

Name	Block size	Key size
Advanced Encryption Standard (AES)	128	128, 192, 256
Rijndael	Variable	128, 192, 256
Blowfish (often used in SSH)	Variable	1–448
Data Encryption Standard (DES)	64	56
IDEA (used in PGP)	64	128
Rivest Cipher 2 (RC2)	64	128
Rivest Cipher 4 (RC4)	Streaming	128
Rivest Cipher 5 (RC5)	32, 64, 128	0–2,040
Skipjack	64	80
Triple DES (3DES)	64	112 or 168
Twofish	128	1–256

7.PKI and cryptographic applications.

RSA – most famous public key cryptosystem. Depends on computational difficulty inherent in factoring large prime numbers. Steps are 1. Choose two large prime numbers, approx. 200 digits each p&q . 2. Compute n=p*q 3. Select the number e , e should be less than n ; e and (p-1)(q-1) are relatively prime, that is two numbers have no common factors other than 1. 4. Find a number D such that (ed-1) mod(p-1)(q-1)=1, 5. Distribute e and n as public key to all cryptosystem users. Keep d secret as the private key.

Formula is C=Pe mod n ; to decrypt P=Cd mod n.

Merkle-Hellman knapsack is ineffective . it uses super increasing sets than large prime numbers.

RSA- 1024 Bits key length ; DSA – 1024 bits key length ; Elliptic curve – 160 bits key length.

EL GAMAL – did not get patent like RSA. It was freely available for public. Major disadvantage is it doubles the length of any message it encrypts. This takes time to encrypt long messages.

Elliptic curve (ECC)

Y2=x3+ax+b

1024 bits RSA key length is equivalent to a 160 bit ECC cryptosystem key.

Hash functions – they take potentially long message and generate a unique output value derived from the content of the message. This value is refereed as message digest/hash value/hash total/CRC, fingerprint/checksum/digital ID.

In most cases message digest is 128 bit or larger. Five basic requirements are 1. Input can be of any length 2. Output has fixed length. 3. Hash function is relatively easy to compute for any input. 4. Hash function is one way 5. It is collision free, difficult to find two message that produce the same hash value.

SHA- secure hash algorithm – SHA1,2,3, are government standard hash functions by the NIST. Specified in secure hash standard(SHS) also known as federal information processing standard(FIPS). It produces 160 bit message digest . process message in 512 bit blocks.

SHA2 has 4 variants - SHA 256 produces 256 bit MD using 512 block size ; SHA 224 uses truncated version of SHA 256 hash to produce 224 MD using 512 block size ; SHA 512 produces 512 MD using 1024 bit block size. SHA 384 uses truncated version of SHA 512 hash to produce a 384 MD using 1024-bit block size. SHA2 considered to be secure.

MD2 – created to provide secure hash functions for 8-bit processors. It pads the message, so that its length is a multiple of 16 bytes. It then computes 16-byte checksum and appends it to the end of the message .128-bit message digest is then generated by the entire original message along with the appended checksum. No longer is used as Collison may occur and it is not a one-way function

MD4 – to support 32-bit processors. Pads the message to ensure message length is 64 bits smaller than a multiple of 512 bits. It processes 512 block of the message in three rounds and final output is 128 bit digest. No longer used.

MD5 – it also uses 512-bit blocks of the message but using 4 rounds of computations. Subject to collision.

Digital signature – non-repudiation and integrity. It uses public key cryptography and hashing functions. Sender encrypts message digest with sender's private key. Receiver decrypts with sender's public key.

HMAC- hashed message authentication code – it implements partial digital signature. It provides integrity but not non-repudiation.

Digital signature standard –

FIPS 186-4 also known as DSS- Digital signature standard . it specifies that all approved digital signature algorithm must use SHA3 hashing functions. Approved encryption algorithms are DSA (digital signature algorithm) ; RSA and ECDSA(Elliptic curve DSA)

Public key infrastructure

Certificates – x.509 1.version of x.509 2. Serial number from the certificate creator .3 signature algorithm identifier (specifies the technique used by CA to digitally sign the content of the certificate) 4. Issuer name (identification of the CA that issued the certificate) .5. validity period (starting and ending date). 6. Subjects name (contains DN (Distinguished name) of the entity that owns the public key contained in the certificate. 7.subject's public key (actual public key the certificate owner used to set up secure communications).

The current version of X.509 is version 3

Certificate authorities

Registration authorities (RA) assist CA to verify users' identities prior to issuing digital certificates. Certification path validation (CPV) to verify links of certificates from root to end.

Certificate generation and destruction –

1. Enrollment – provide public key to the CA. CA will create x.509 digital certificate containing user's identifying information and a copy of user public key. CA sign with its private key.
2. Verification – to verify digital certificate of someone, check using CA's public key. Also check it is not revoked in CRL or online certificate status protocol (OSCP).
3. Revocation – when it is compromised; when it was mistakenly issued; when details of the certificate is changed ; when security association is changed.
4. CRL- to verify it is not revoked. Latency issue there as it needs to be downloaded
5. OCSP (Online Certificate status protocol)- To verify it is not revoked. Real time. No latency issues.

Asymmetric key management

HSM- hardware security module – to provide effective way to manage encryption keys.

Portable devices – Microsoft uses bitlocker and encrypting file system (EFS) ,MAC OS uses file vault encryption and TrueCrypt open source allows encryption of disks on linux, windows and MAC systems.

TPM- Trusted platform module -is a chip resides on the motherboard of the device. It provides OS with access to the keys and preventing someone from removing the drive from one device an inserting into another device to access the drive's data.

Email – if you need confidentiality, encrypt the message; if you need integrity, hash the message; if you need non repudiation, authentication , integrity, digitally sign the message ; if you need everything, you should encrypt and digitally sign the message.

Pretty good privacy -PGP – it secures email system. It is available in two versions. Commercial version uses RSA for key exchange; IDEA for encryption/decryption; MD5 for message digest. Freeware uses Diffie-Hellman key exchange and Carlisle adams(CAST)128 bit algorithm and SHA1 function.

S/MIME- secure multipurpose internet mail extensions protocol has emerged as de facto standard for encrypted email. it uses RSA encryption algorithms. Incorporated into Microsoft outlook, Mozilla ,mac os x mail , Gsuite enterprise edition. It uses x.509 certificates for exchanging keys. It is supported only by RSA. Supports AES and 3DES algorithms.

Web applications- SSL for HTTPS on 443. 1. On website access, Browser retrieves web server's certificate and extracts server's public key. 2. Browser creates random symmetric key, uses server's public key to encrypt it and sends encrypted symmetric key to the server. server decrypts encrypted symmetric key with its own private key and two system will start exchanging information's. POODLE attack on SSL in 2014. After which TLS was accepted by everyone.

Stenography and watermarking – to embed secret message within another message. It is often within pictures. Watermarking is used to protect intellectual property.

Digital rights management (DRM) – software uses encryption to enforce copyrights restrictions on digital media.

Music DRM-

movie DRM- 1. High bandwidth digital content protection (HBDCP)- protects content sent over digital connection. 2. **Advanced access content system (AACS)-** protect content stored on blu-ray and HD and dvd media.

Ebook DRM- most successful DRM. ADOBE offers ADEPT to provide DRM technology

Video game DRM-

Document DRM- commercial DRM products are vitrium, file open.

Networking –

Circuit encryption – 1. Link encryption protects entire communication by creating secure tunnel between two points. 2. End-end encryption protects communication between two parties and is performed independently of link encryption. Example is the use of TLS between a user and webserver.

Link encryption encrypts everything including headers. End -end doesn't encrypt headers, so it is faster , but susceptible to sniffers and eavesdroppers.

When encryption happen at higher OSI Layer, it is end to end encryption, at lower layer it is link encryption. SSH is an example of end-to-end encryption.

IPSEC- it uses public key cryptography to provide encryption, access control, non-repudiation and message authentication. Mainly for VPN. it can operate in transport or tunnel mode. It is commonly paired with layered 2 tunneling protocol -L2TP

It has two components – **AH** (Authentication Header) provides integrity and non-repudiation. It also provides authentication and access control and prevents reply attacks. **ESP** (Encapsulating Security Payload) provides confidentiality and integrity of packet contents. It provides encryption and limited authentication to prevent replay attacks. When IPsec is used in transport mode only the packet payload is encrypted, peer to peer communication. when it is used in tunnel mode, entire packet including header is encrypted. It is designed for gateway-to-gateway communication.

At run time, we set up an IPSEC session by creating security association (SA). It represents simplex connection. For both AH and ESP to be used for bi directional, we need 4 SA's.

ISAKMP- internet security association and key management protocol. It provides background supports for IPsec by negotiating, establishing security associations. SA's are managed through the use of ISAKMP. four basic requirements for ISAKMP are authenticate communicating peers, create and manage SA. Provide key generation mechanism, protect against threats.

Wireless networking-

WEP- Wireless equivalent privacy- it provides 64 and 128 bit encryption options to protect communication within wireless LAN. It is described in 802.11.

Wifi protected access- WPA- it improves on wep encryption by implementing TKIP-temporal key integrity protocol. Further WPA2 added AES cryptography. WPA does not provide end to end encryption.

IEEE 802.1X provides flexible framework for authentication and key management in wired and wirelss network. To use this client has to run piece of software known as supplicant. WPA is designed to authenticate with 802.1x authentication servers.

Cryptographic attacks-

1. **Analytic attacks**- algebraic manipulation. Focus on logic of the algorithm itself.
2. **Implementation attack** -exploits weakness in implementation, not just errors and flaws, also on methodology.
3. **Statistical attack** -floating point errors. vuln in hardware or operating system.
4. **Brute force** – every possible combination of key finding.
5. **Frequency analysis and ciphertext only attack** – on cipher text using transposition or substitution methods.
6. **Known plaintext** – attacker has both plain text and cipher text

7. **Chosen ciphertext** – attacker has the ability to decrypt chosen portion of encrypted cipher text message and use the decrypted portion to discover key.
8. **Chosen plaintext** – attacker has the ability to encrypt plain text message of their choosing and then analyze cipher text output of the encryption algorithm
9. **Meet in the middle** – to defeat encryption algorithm that use two rounds of encryption. attacker uses plain text message.
10. **Man in the middle** – the attacker sits in the middle.
11. **Birthday** -also known as collision attack or reverse hash matching. seeks to find flaws in one to one nature of hashing functions . substitute in digitally signed communication
12. **Replay** – attacker intercepts an encrypted message between two parties, then later replays the captured message to open a new session. Time stamp and expiration period will solve this issue

8.Principles of security models, design and capabilities.

IMPLEMENT AND MANAGE ENGINEERING PROCESS USING SECURE DESIGN PRINCIPLES

Much easier to build security to new system than add it to existing system.

Objects and subjects – transitive trust is a concept that if A trusts B and B trusts C, then A inherits trust of C through the transitive property. In mathematical way if A=B; B=C then A=C;

Closed and open system – closed system is designed to work well with a narrow range of other systems. Generally, all from same manufacture. The standards for closed system are often proprietary and not normally disclosed. Open systems are designed using agreed upon industry standards. open systems are much easier to integrate with systems from different manufactures that support the same standards.

Closed systems are hard to attack and find vulnerable. Open systems are easy to attack and find vulnerable.

Technique for ensuing confidentiality, Integrity and Availability.

Confinement – process confinement allows a process to read from and write to only certain memory locations and resources. It is also known as sandboxing. If a process attempts to initiate an action beyond its granted authority, that action will be denied, and logs will be logged. **Confinement can be implemented through process isolation and memory protection.**

Bounds – each process that run on a system is assigned an authority level. The authority level tells the operating system what the process can do. There are two levels. User and kernel. The authority level tells operating system how to set bounds for process. The bounds state the area within which a process is confined or contained. In most systems bounds are logical areas of memory for each process to use. It is the responsibility of operating system to enforce these logical bounds and to disallow access to other process. More secure systems may require physically bounded process, but it is expensive.

Isolation – when a process is confined through enforcing access bounds, that process runs in isolation. Process isolation ensures that any behavior will affect only the memory and resources associated with the isolated process. It is used to protect operating environment, the kernel and other application.

Controls –MAC- each subject possesses attributes that define its clearance or authority to access resources. Discretionary control differs from MAC. Based on identity subjects may be allowed to add or modify rules that define access to objects.

Trust and assurance – trusted system is one in which all protection mechanism work together to process sensitive data for many types of users while maintaining a stable and secure computing environment. Assurance is simple defined as the degree of confidence in satisfactory of security needs. Assurance must be continually maintained and updated.

Security models

Trusted computing base (TCB)- old standard known as orange book/TCSEC. TCB is a combination of hardware, software and controls that work together **to form a trusted base to enforce security policy. It should be as small as possible**. TCB is the only portion of the system that can be trusted to adhere to and enforce security policy. It is the responsibility of TCB to ensure that system behaves properly.

Security perimeter – it is an imaginary boundary that separates TCB from the rest of the system. F**or the TCB to communicate with rest of the systems, it must create secure channels, called trusted paths.**

Reference monitor and kernel – the part of the TCB that validates access to every resource prior to granting access requests is called reference monitor. Reference monitor is the access control enforce for TCB. It is a conceptual part of TCB. It doesn't need to be actual or stand alone or independent working system component.

The collection of components in TCB that work together to implement reference monitor function is called security kernel. The purpose of kernel is to launch appropriate components to enforce reference monitor functionality and resist all known attacks. Kernel uses trusted paths to communicate with subjects.

State machine model- always secure, no matter what state it is in. basis for many other security models. It is based on the computer science definition of a finite state machine (FSM). Transition occurs when accepting input or producing output. A transition always results in a new state (Called state transition).

Information flow model – focuses on flow of the information. It is based on state machine model. Bell lapadula and Biba are information flow models. Bell is concerned with preventing information flow from **high security level to low security. BIBA is concerned with low security to high security**. It also addresses cover channels by specifically excluding all non-defined flow pathways.

Non-interference model- it is based on the information flow model. But it is not concerned with flow of information. It is concerned with how subject at a higher security level affect the system state or the action of a subject at lower security level. Action of subject A (High) should not affect action of subject B. if it effects, it will create covert channel. This model can be imposed to provide form of protection against malicious programs such as trojan horse.

Cascading- input for one system comes from the output of another system; Feedback -one system provide an input to another system; Hookup – one system sends input to another system but also sends input to external entities.

Take-grant model – 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 – it is a table of subjects and objects that indicates actions or functions that each subject can perform on each object. Each column of the matrix is an ACL. **Each row of the matrix is called capabilities list and it is tied to subject. ACL is tied to object.** two things are important. 1. Constructing environment that can create and manage list of subjects and objects. 2. Crafting a function that can return the type associated with whatever object is supplied to that function as input.

Bell -lapadula model- DoD developed this model to protect classified information. It is a multilevel model. It states that a subject with any level of clearance can resources at or below its clearance level. A person with secret clearance can access secret, confidential, sensitive but unclassified, unclassified documents. But not top-secret documents. Also, to access documents within secret level, the person must have need to know for that document. By design this model prevents leaking information from classified to less secure clearance levels. This is accomplished by blocking lower levels from accessing higher levels. First mathematical model and it addresses only confidentiality. not integrity and not availability.

This model is built on state machine concept and information flow model. It also employs mandatory access control and lattice concept. Three basic properties. 1.**Simple security property states that subject may not read information at a higher level (no read up) 2. * star security property states that subject may not write information at lower level (no write down). This is also known as confinement property 3. Discretionary security property states that the system uses access matrix to enforce discretionary access control. There is an exception that "trusted subject" can write down. It doesn't cover covert channels.**

BIBA Model – state machine and information flow model. Focus on Integrity. 1. **Simple security property states that subject cannot read an object at lower level (No read down) 2. * star security property states that subject cannot modify an object at a higher integrity level(no write up).**

Biba was designed to address three integrity issues .1. prevent modification of objects from unauthorized subjects. 2. Prevent unauthorized modification by authorized subjects .3. protect internal external object consistency. it focuses on protecting objects from external threats. it thinks internal threats are taken care programmatically. It doesn't focus confidentiality and availability. It doesn't address access control management and it doesn't provide a way to assign or change an object's or subject's classification level. It doesn't prevent covert channel. Commercial organization prefer Biba model as their focus is on integrity.

Clark-Wilson Model - Integrity. approaches through small set of programs. It doesn't require lattice structure. It uses three-part relationship of **subject/program/object- known as triple or access control** triple. Subject cannot access objects directly. It can access only through programs. Two principles 1. Well-formed transactions 2. Separation of duties. This model provides an effective means to protect integrity. For commercial use.

Well-formed transactions take the form of programs, interface or access portal. Each program has limitation on what it can and what it cannot do to an object. This effectively limits subject capabilities. This is known as constrained interface. 1. CDI constrained data item- is any data item whose integrity is protected by the security model. 2. UDI unconstrained data item is any data item that is not controlled by the security model. 3. IVP integrity verification procedure is a procedure that scans data items and

confirm their integrity. 4. TP transformation procedure are the only procedure that is allowed to modify CDI. It uses security labels to grant access to objects , but only through TP and restricted interface model.

Brewer and Nash model (aka Chinese model) – it was created to permit access controls to change dynamically based on user's previous activity. State machine model. It seeks to create **security domains.**

Goguen -meseguer model – is an integrity model. This is the foundation of noninterference model. It is based on automation theory and domain separation. This means subjects are allowed only to perform predetermined actions against predetermined objects. Members of one domain cannot interface with another domain.

Sutherland model- integrity model. State machine and information flow model.it is based on the idea of defining set of system states, initial states and state transition. It prevents covert channel.

Graham- denning model – focused on the secure creation and deletion of both subjects and objects. Eight primary protection rules .1. create an object, subject, delete object, delete subject, provide access right, grant access right, delete access right, transfer access right.

Select controls based on system security requirements –

Rainbow series – 1. Trusted computer system evaluation criteria (TCSCEC). There were so many publications released with color covers- collectively known as rainbow series. European model called ITSEC. These two were replaced with common criteria. In TCSEC, functionality and security were combined, not separated. Orange book applies only to standalone systems.

TCSEC Classes and required functionality – functionality and assurance are combined. Applicable systems are standalone systems that are not networked. 4 categories. A,B,C,D ; Category A- Verified protection. The highest level of security; category B- Mandatory protection; category C- Discretionary protection; category D- Minimal protection. Reserved for systems that have been evaluated but do not meet requirements to belong to any other category.

A1- verified protection; B3-security domains; B2- structured protection; B1-labeled security. C2-Controlled access protection; C1-Discretionary protection; D-Minimal protection

Category C provides basic security controls. C1- Control access by user ID/groups. C2- stronger than C1. It enforces media cleansing to avoid remnant. Strict logon procedure must be in place.

Category B-This category of systems based on Bell-lapdula model. B1-labled security. It supports sufficient security to house classify data. B2- Structed protection- it ensures that no covert channel exist. Operator and administrator functions are separated, and isolation is maintained. B3- Security domain-separation and isolation of unrelated process. Difficult to attack. Focus on vulnerability. A1-verfired protection. each phase in the development is documented, tested, verified. Extreme security conscious. Assurance becomes more important. handle top secret data.

Other color is rainbow series- Red book – rates confidentiality and integrity. Address communication integrity. Address denial of service protection. Address intrusion protection and prevention. It is limited to networks.4 rating levels. None, C1,C2, B2

Green book –(password) ; yellow book(environment); tan book(audit) ; bright blue(product evaluation for vendors)

Issues with TCSEC- 1. Doesn't cover integrity, accuracy 2. Doesn't cover what user do with information 3. Does not cover procedural, policy matters. 4. Orange book only for standalone systems.

ITSEC Classes and required assurance and functionality

Functionality and assurance are separate. functionality rating states how well the system performs all necessary functions. Assurance rating states degree of confidence that system will work properly in consistent manner. ITSEC refers to any systems being evaluated as TOE target of evaluation. All ratings are expressed as TOE ratings in two categories. Functionality rating through F-D, assurance rating from E0-E6.

ITSEC covers integrity and availability in addition to confidentiality. It doesn't require that system's security components be isolated within TCB. ITSEC covers maintaining targets of evaluation after such changes occur without requiring a new formal evaluation.

Common criteria – Product evaluation model. ISO 15408(evaluation criteria for information technology security) it is based on two key elements. 1. Protection profile (PP). 2.Security target (ST).

PP specify the product to be evaluated (The TOE) the security requirements and protections, which are considered the security desires or "I want from customer".

ST specify the claims of security from the vendor that are built into a TOE.ST's are considered the implemented security measures or" I will provide" from the vendor. The PP is compared to various ST's from the selected vendor's TOE. The closest or best match is what the client purchases.

The client initially selects based on EAL-Evaluation assurance levels. CC is divided into three areas.

Part 1 -introduction and general model describes; part 2 – security functional requirements; part 3- assurance

- EAL1 - Functionally tested.
- EAL2 - Structurally tested.
- EAL3 - Methodically tested and checked.
- EAL4 - Methodically designed, tested and reviewed.
- EAL5 - Semi formally designed and tested.
- EAL6 - Semi formally verified, designed and tested.
- EAL7 - Formally verified designed and tested.

Certification – technical evaluation of each part of a computer system.

Accreditation – it is the formal declaration by the designated approving authority (DAA).

Two government standards are currently in place for the certification and accreditation of computing system. The current DoD standard is RMF. Risk management framework. Which replaced DIACAP which replaced DITSCAP. The standard for all other US govt executive branch departments is CNSS (committee on national security system) which replaced NIACAP.

1. Definition – creation of system security authorization agreement (SSAA).
2. Verification - system development activities and certification analysis.
3. Validation - certification evaluation of the integrated system, accreditation decision.

4. Post accreditation – includes maintenance; system operation; change management and compliance validation.

For system accreditation – major application or system is evaluated; for site accreditation – applications and system at specific location is evaluated; for type accreditation -system or application that is distributed to number of different locations is evaluated.

Security capabilities –

Memory protection – it is a core security component that must be designed and implemented into an operating system.

Virtualization-

Trusted platform module-TPM- it is used to store and process cryptographic keys. HSM- hardware security module-it adds tamper protection. TPM is one example of HSM. It provides 2048 but asymmetric encryption calculations and secure vault for key storage.

Interface – constrained interface- practical implementation of Clark Wilson model of security.

Fault tolerance -RAID.

The state machine model ensures that all instances of subjects accessing objects are secure. The information flow model is designed to prevent unauthorized, insecure, or restricted information flow. The noninterference model prevents the actions of one subject from affecting the system state or actions of another subject.

The Take-Grant model dictates how rights can be passed from one subject to another or from a subject to an object. An access control matrix is a table of subjects and objects that indicates the actions or functions that each subject can perform on each object.

Bell-LaPadula subjects have a clearance level that allows them to access only those objects with the corresponding classification levels. This enforces confidentiality. Biba prevents subjects with lower security levels from writing to objects at higher security levels.

Clark-Wilson is an integrity model that relies on auditing to ensure that unauthorized subjects cannot access objects and that authorized users access objects properly. Biba and Clark-Wilson enforce integrity. Goguen Meseguer and Sutherland focus on integrity. Graham-Denning focuses on the secure creation and deletion of both subjects and objects.

9.Security vulnerabilities, threats and countermeasures

The more complex the system, the less assurance it provides. Which means more areas for vulnerability exist and more areas must be secured against threats. Less trustworthy the system is.

Hardware – the collection of 0s and 1s that make up software and data stored within them.

Processor – Central processing unit CPU, generally called processor or microprocessor. It is the computer's nerve center. It is the chip that governs all major operations either directly or coordinate with other complex symphony of calculations. It is the responsibility of operating system and compliers to translate high level language into assembly language instruction that CPU understands. It allows CPU to perform computational and logical operation at blazing speed.

Execution types –

Multitasking – handling two or more tasks simultaneously. A single core multi-tasking system is able to juggle more than one task or process at any given time.

Multicore – today most CPU's are multi core which means a chip containing 2,4,8 or potentially dozens of independent execution cores that can operate simultaneously.

Multiprocessing – a computing system with more than one processor (CPU). For ex: database server might run on a system that contains four, six or more processors. If the db application receives a number of requests simultaneously, it might send each query to a separate processor for execution.

Two types of multiprocessing 1. A system containing multiple processors that are treated equally and controlled by single Operating system is called **symmetric multiprocessing (SMP**). Processors share not only OS, also common data bus and memory resources. 2. **Massive parallel processing (**MPP) it has 100's or 1000's of processors which has its own operating system and memory bus resources. Extremely

powerful. And expensive. Used in science research. SMP systems are for simple operations at extremely high rates, whereas MPP are for very large complex tasks.

Multiprogramming- it I similar to multitasking. It involves pseudo simultaneous execution of two tasks on a single processor co ordinated by the operating system 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 next process in line to begin. it is rarely found in today use.

Difference between multitasking and multiprogramming is multiprogramming takes place at large scale system such as mainframes, whereas multitasking takes place at personal computer, operating system such as windows and Linux. Multitasking is coordinated by operating system. Multiprogramming requires specially written software that coordinates its own activities and execution through the operating system.

Multithreading – it permits multiple concurrent tasks to be performed within single process unlike multitasking where multiple tasks take multiple process. Thread is a self-contained sequence of instructions that can execute in parallel with other threads that are part of the same parent process. It is often used in applications where frequent context switching between active process consumes excessive overhead and reduces efficiency.

Processing types.

Single state – it requires the use of policy mechanism to manage information at different levels. Security admin approves a processor and system to handle only one security level at a time.

Multistate – implements much higher level of security. These systems are certified to handle multiple security levels simultaneously by using specialized security mechanism. It will prevent crossing between two levels.

Protected mechanisms - Rings, Operational states and security modes.

Protection rings – though original multics implementation allowed up to seven rings (0 through 6), most modern operating system use a four-ring model (0 Through 3). Innermost ring 0 has the highest level of privilege and can basically access any resource, file or memory location. The part of operating system that remains resident in memory is called kernel. It occupies ring 0 and can preempt code running at any other ring. Remaining part of the operating system at ring 1. Ring 2 is also somewhat privileged in that I/O devices, drivers reside. Other applications at ring 3.

- RING 0- OS AND Kernel.
- RING 1- OTHER OS COMPONENTS (process switch and other operations.
- RING2 – DRIVERS, Protocols.
- RING 3- USER LEVEL PROGRAMS AND APPLIAITONS.

RING 0-2 Privileged mode or supervisory mode; ring 3 – user mode.

The essence of the ring model lies in priority, privilege and memory segmentation. The process associated with lowest ring number always run before process associated with highest numbered rings. Process in lowered ring number can access more resources and interact with the OS more directly than those in higher-numbered rings. Higher numbered process generally asks a handler or driver in a lower numbered ring for services they need. This is sometimes called **mediated access model.** Each ring has its

own associated memory segment. It enables operating system to protect itself from user and applications. System call is a term used to call another rings access.

Process states – also known as operating states. Various form of execution in which process may run. Operating system can be at one of the two modes. Supervisor state or problem state. Processes line up for execution in an operating system in a processing queue. Process consumes its entire chunk of processing time called time slice. Process scheduler usually selects highest priority process for execution.

Ready – a process is ready to resume or begin processing as soon as it is scheduled for execution. If CPU is available it will directly into running state, otherwise it will have to wait until its turn comes up. This means the process has all memory and other resources it needs to begin executing immediately.

Waiting – also called blocked state. A process is waiting for device or access request to be served before it can continue processing.

Running-also called problem state. Running process executes on CPU and keeps going until it finishes, its time slice expires or it is blocked for some reason. If time slice ends and the process is not completed, it will return to ready state. If the process blocks while waiting for a resource, it goes into waiting state.

Supervisory – when the process requires more privileges to execute will get into this state.

Stopped – when the process finishers or must be terminated duo to some reasons it gets into stopped mode. At this point operating system can recover all memory and other resources allocated to the process and reuse them for other process as needed.

A special part of the kernel, called program executive or process scheduler is always around, so that when a process state transition must occur, it can step in and handle the mechanics involved.

Security mode-

US govt approved four security modes for systems that process classified information. three specific elements must exist before the security modes themselves can be deployed.1. hierarchal mandatory access control (MAC) environment. 2.total physical control over which subject can access the computer console. 3. total physical control over which subject can enter into the same room as the computer console.

Dedicated mode - this is equivalent to single state. Three requirements are 1. Each user must have security clearance that permits access to all information processed by the system 2. Each user must have access approval for all information processed by the system 3. each user must have valid need to know for all information processed by the system.

System high mode - 1. Each user must have security clearance that permits access to all information processed by the system. 2. Each user must have access approval for all information processed by the system. 3. Each user must have valid need to know for some information processed by the system but not necessarily all information processed by the system.

Compartmented mode- 1. Each user must have security clearance that permits access to all information processed by the system. 2. Each user must have access approval for any information they will have access to on the system. 3. Each user must have valid need to know for all information they will have access to on the system. In a special implementation of this mode called compartmentalized mode workstations (CMW). CMW require two forms of security labels be placed on objects. Sensitivity levels

and information labels. Sensitivity level describe the level at which objects must be protected. Information labels prevent data over classification. Which assists in proper and accurate data labeling.

Multilevel mode – also known as "controlled security mode" 1. some users do not have security clearance for all information processed by the system. Thus, access is controlled by whether the subject's clearance level dominates the object sensitivity label. 2. Each user must have access approval for all information processed by the system. 3.each user must have valid need to know for all information they will have access to on the system.

Multilevel mode is exposed to the highest level of risk.

Operating modes

User mode – often process within user mode are executed within controlled environment called Virtual machine (VM).

Privileged mode also called supervisory, kernel, system mode.

Memory

Read only memory (ROM) Nonvolatile- it is a memory that PC can read but cannot change (no writing allowed). It often contains bootstrap information that computer uses to start up prior to loading an operating system from disk. This includes familiar POST Power on self-test, series of diagnostics that run each time you boot a PC.

Programmable ROM(PROM)- it is not burned at factory. It allows end user to burn in the chip's content. Once content is written to a PROM Chip, can't alter. this is like ROM. PROM provides software developers an opportunity to store information permanently on high speed. It is commonly used in hardware applications.

EPROM-erasable. Two types. **UVEPROM-** ultraviolet EPROM can be erased with a light. Once erased, it can be burnt again like a new one. **EEPROM**-Electronically erasable. A more flexible compared to UVEPROM. Which uses electric voltage delivered into the pins of the chip to force erasure.

Flash memory-derivative concept from EEPROM. It is a nonvolatile form of storage media that can be electronically erased and rewritten. EEPROM must be fully erased. Flash memory can be erased in blocks or pages. Most common type of flash memory is NAND flash.

Random access memory (RAM)Volatile. – readable and writable memory that contains information a computer uses during processing. Data will be wiped when the computer is shut down. It is only useful for temporary storage. critical data never be stored on RAM.

Real memory – also known as main memory or primary memory. Is typically the largest RAM storage resource available to computer. It is composed of dynamic RAM chips. Must be refreshed by CPU on periodic basis.

Cache RAM- for better performance. Temporarily storing it. Real memory often contains a cache of information stored magnetic media or SSD.

Dynamic RAM uses series of capacitors and it is cheaper. Static RAM uses logical device known as flip flop and runs faster than dynamic RAM.

Registers- CPU also includes limited number of onboard memory, known as registers. Any data that ALU is to manipulate must be loaded into register unless it is directly supplied as part of the instruction.

Memory addressing -

1. Register addressing – registers are small memory locations directly in the CPU. When CPU needs information from one of its registers to complete an operation, it uses register address. For example register1 to access its contents
2. Immediate addressing – it is not memory addressing, but rather a way of referring to data that is supplied to the CPU as part of an instruction. For example" add 2 to the value in register 1. It uses two commands. First is immediate addressing. The CPU is being told to add 2 to the value and does not need to retrieve that value from memory. Second is register addressing which instruct to retrieve the value from register 1.
3. Direct addressing -CPU is provided with actual address of the memory location to access. The address must be located on the same memory page as the instruction being executed. It is more flexible.
4. Indirect addressing – memory address contains another memory address. CPU reads the indirect address to learn where actual data resides and then retrieves the data from that address.
5. Base+offset addressing – it uses a value stored in one of the CPU's register as the base location from which to begin counting. CPU adds the offset supplied with the instruction to that base address and retrieves from the computed memory location.

Secondary memory- it is used to refer magnetic media or flash drive, CD/DVD/USB are secondary memory. Inexpensive. Can store massive information. Virtual memory is special type of secondary memory that operating system manages to make look and just act like a real memory. Page file is the most common type of virtual memory. This specially formatted file contains data previously stored in memory but not recently used. When OS needs to access address stored in the page file, it checks to see whether the page is memory resident to access directly or whether it has been swapped to disk. In which case it reads the data from disk back into real memory. This is called paging. Slow in processing, computer overhead. Larger banks of RAM and SSD can increase the performance

Memory security issues- should have proper control to prevent attacks.

Storage –

Primary (RAM)vs secondary (DVD, flash drive, other disks)

Volatile (RAM)- Loose data when power is off. Non volatile (other storage media)- doesn't loose data when power is off.

Random access storage allows OS to read from any point within the device by using some type of addressing system. Almost all primary storage devices are random access devices. Secondary devices are also random access.

Sequential storage devices have to scan physically. Magnetic tap drivers are the examples.

Storage media security – data remanence. theft. should encrypt the disks.

Input output devices –

Monitors – TEMPEST is a technology that allows the electronic emanations that every monitor produces (Van eck radiation) to be read from distance , this process is known as van eck phreaking. Another one is shoulder surfing.

Printers – sensitive copies may be there. Store data on drive.

Keyboard/mice – a simple device can be placed inside keyboard to intercept all the keystrokes. Wireless keyboard and mouse can be vulnerable to radio signal attack using blutooth.

Modems – improper config will lead to security issues.

Firmware -also known as microcode. Is a term used to describe software that is stored on ROM chip. There are two types of firmware 1. BIOS on motherboard and general internal and external device firmware.

Bios and UEFI- BASIC INPUT OUTPUT SYSTEM contains the operating system- independent primitive instructions that a computer needs to start up and load the operating system from disk. BIOS is contained in a firmware device that is accessed immediately by the computer at boot time. The BIOS is stored on EEPROM to facilitate version updates. The process of updating BIOS is known as “flashing the BIOS”. There is an attack called” Phlashing, in which malicious is installed to remote control. Most companies replaced the traditional BIOS with UEFI (unified extensible firmware interfaces).

Client based systems

Applets – applets are self-contained miniature programs that execute independently of the server that sent them. **Two examples are java applets and ActiveX control.**

Java applets – it is a short java program transmitted over the internet to perform operations on a remote system. Sandbox helps in preventing, but there are still vulnerabitlies.

Active x control – it uses proprietary Microsoft technology and therefore it can execute only on systems running Microsoft browsers. Active x controls are not subject to sandbox restrictions placed on java applets. They have full access to the windows operating system. Microsoft latest browser edge with windows 10 doesn’t support ActiveX

Local caches – local cache is anything that is temporarily stored on the client for future reuse. There are many local caches. 1. ARP Cache ,2. DNS cache,3. Internet file cache.

ARP cache poisoning is caused by an attack responding to ARP broadcast queries in order to send falsified replies. If the false reply is received by the client before valid reply, then false reply Is used to populate the ARP cache and the valid reply is discarded as being outside an open query. Dynamic content of ARP cache, whether poisoned or legitimate, will remain in cache until a timeout occurs (10 mins**). ARP is used to resolve IP to MAC address in order to craft the ethernet header for data transmission.**

Second form of ARP cache poisoning is to create static ARP entries. This is done via ARP command and must be done locally. This is easily accomplished by a script that gets executed on the client through trojan horse, buffer overflow or social engineering attacks. ARP is one means of setting up man in the middle attack.

Another man in the middle attack is through DNS cache poisoning. Similar to ARP, client receives response from DNS, and it will be cached for future use.

HOSTS File is the static file found on TCP/IP. Admin or hackers can add content to the HOSTS file that sets up a relationship between a FQDN (fully qualified domain name) and the IP address of choice. If an attacker is able to plant false information into hosts file, then when the system boots the contents of the hosts file will be read into memory where they will take precedence. unlike dynamic queries with time out, hosts file is permanent.

Authorized DNS server attack aims at altering primary record of a FQDN on its original host system, the primary authoritative DNS server. It hosts zone file or domain database. Attack on authoritative DNS gets noticed quickly, so most attackers focus on caching DNS servers instead.

DNS lookup address changing -it focuses on sending an alternate IP address to the client to be used as the DNS server that clients uses for resolving queries. DNS server address is typically distributed through DHCP, but it can also be assigned statically. Attacker may use script or compromise DHCP to alter IP. Once client has the wrong DNS server, they will be sending their queries to a hacker-controlled DNS server.

DNS query spoofing- this attack occurs when hacker is able to eavesdrop on client's query to a DNS server. Then attacker sends back false information to the client. If the client accepts false reply, then they will put that info in their local DNS cache.

Internet file cache will lead to split response attack and mobile script attack.

Organization should use split-DNS system. Which means separate DNS Server for public and internal systems. Should block 53 for TCP and UDP from outside to internal. TCP 53 is used for zone transfer and UDP 53 is for queries.

Server based systems –

A load balancer is used to spread or distribute network traffic load across several network links or network devices. A load balancer may be able to provide more control over data flow. The purpose of load balancer is to obtain more optimal infrastructure utilization, minimize response time, maximizing throughout, reduce overloading and eliminate bottlenecks. Techniques are random choice, round robin, load/utilization monitoring and preferencing. It is important to monitor for DOS attacks.

Database system security

Aggregation – SQL provides a number of functions that combine records from one or more tables to produce potentially useful information. This process is called aggregation. Aggregation attacks are used to collect numerous low-level security items or low value items and combine them to create something of a higher security level or value.

Inference- inference attacks combine several non-sensitive information to gain access to information that should be classified at higher level. It makes use of human's mind than mathematical ways. Database partitioning can help prevent this attack.

Datamining and data warehousing -many organizations use larger database, known as Datawarehouse. **Data dictionary** is commonly used for storing critical information about data, including usage, types,

sources, relationship and formats. DBMS reads data dictionary to determine access rights for users attempting access data

Data mining techniques allow analysts to comb through data warehouses and look for potential correlated information. Data mining techniques result in the development of data models that can be used to predict future activity. The activity of data mining produces metadata. **Metadata** is data about data. Meta data is valuable. It is stored in a secure container known as **data mart. Data mining can actually be used as security tool when it is used to develop baseline for statistical anomaly based intrusion deduction system.**

Data analytics – it is the science of raw data examination with the focus of extracting useful information out of bulk information set. It is also called "big data". Very difficult to maintain, transfer, process large amount of data. It needs high performance system to process.

Large scale parallel data systems – parallel systems or parallel computing is a computation system designed to perform numerous calculations simultaneously. It divides large task into smaller tasks and then distributing each sub element to different processing subsystem for parallel computation. Parallel data processing can be accomplished by using distinct CPUs or multicore CPUs using virtual system or any combination of these. There are many divisions .1 AMP Asymmetric multiprocessing and SMP symmetric multiprocessing. in AMP, the processors are often operating independently, each has its own OS or task instruction set. It is configured to execute only one specific code. It is called affinity.

In SMP, process share OS and common memory. It works collectively on a single task, code or project. A variation of AMP is massive parallel programming (MPP). SMP are linked together to work on single primary task.

Distributed system and endpoint security –

The concept of client server model is also known as distributed system or distributed architecture. Defense in depth is a multilayer security.

Cloud based systems and cloud computing

Cloud computing is a natural extension and evolution of virtualization, the internet, distributed architecture. It does have issues. The hypervisor also known as the virtual machine monitor (VMM) is the component of virtualization that creates manages and operate virtual machines. The computer running the hypervisor is known as host OS. And the OS running within a hypervisor supported virtual machine is known as guest OS.

A type 1 hypervisor is a native or bare metal hypervisor. In this configuration there is no host OS. Instead the hypervisor installs directly onto the hardware where the OS would normally reside. This is often used to support server virtualization. This allows for maximizations of the hardware resources while eliminating any risks or resource utilization caused by a host OS.

Type II hypervisor is a hosted hypervisor. In this configuration, a standard regular OS is present on the hardware and hypervisor is installed as another software application. It is used in relation to desktop deployment.

Elasticity refers to the flexibility of virtualization and cloud solutions to expand or contract based on need. In relation to virtualization, host elasticity means additional hardware hosts can be booted when

needed and then used to distribute the workload of the virtualized services over the newly available capacity.

Platform as a service – is the concept of providing a computing platform and software solution stack as a virtual or cloud-based service. It provides all the aspects of a platform (that is OS and complete solution package). The primary attraction of PaaS is the avoidance of having to purchase and maintain high end hardware and software locally.

Software as service – it provides on demand online access to specific software applications or suites without need for local installation. Pay and get service (Office 365) or free like Google doc, Gmail.

Infrastructure as service - it is next level to Pass. It provides you complete outsourcing solution. This can include dynamic scaling, policy implementation, managed filter connectivity. It allows an enterprise to scale up new software or data-based services/solutions.

An on-promise solution is a traditional deployment concept that organization owns own hard ware, licensed software and operate, maintains the system on its own usually within their own building.

A hosted solution deployment concept is where organization owns license software, operate and maintain, but hosting provider owns hardware that supports organization software.

A cloud solution is a deployment concept where an organization contracts with third party cloud provider. The third party owns, operates, maintain the hardware and software. Companies pay monthly fee to use cloud solution. It can be in the following methods.

1. Private – it is within corporate network and isolated from internet it is for internal use only
2. Public – it is accessible to the general public over internet. May be for pay or free. Data is kept isolated from other customers.
3. Hybrid – it is a mixture of private and public. For example, private cloud can be accessible by public and business partners
4. Community – sharing cloud by group of people. Cost saving

Snapshots are backup of virtual machines.

CASB Cloud access security broker is a security policy enforcement solution that may be installed on premises, or it may be cloud based. The goal of this is to enforce and ensure that proper security measures are implemented between a cloud solution and a customer organization.

SECaaS- security as a service – is a cloud provider in which security is provided to an organization through or by an online entity.

Grid computing- is a form of parallel distributed computing processing that loosely groups a significant number of processing nodes to work toward a specific processing goal. Members of the grid can enter and leave the grid at random intervals.

Peer to peer – are networking and distributed application solutions that share tasks and workloads among peers. There is no central management system for this

IOT-Internet of things - the security issues related to IOT are access and encryption. One possible secure implementation is to deploy a distinct network for the IoT equipment which is kept separate and isolated from primary network. This configuration is known as three dumb routers.

Industrial control systems (ICS)- is a form of computer management device that controls industrial processes and machines. There are several form of ICS including **distributed control system (DCS), Programmable logic controllers (PLC) and supervisory control and data acquisition (SCADA).**

DCS can be analog or digital. Gathering data from various locations. It is used in a location where the need to gather data and implement control over a large-scale environment from a single solution is essential.

PLC units are single purpose or focused purpose digital computers. It is deployed for automation of electromechanical operations.

SCADA system can operate as a stand-alone device. It is designed with minimal human interface. Often, they use mechanical buttons or knob or simple LCD screen interface. Networked SCADA may have more complexed remote-control software interfaces. Stuxnet delivered the first ever rootkit to a SCADA system located in nuclear facility. Still SCADA and ICS systems are poorly secured.

Assess and mitigate vulnerabilities in web-based systems-

OWASP is a nonprofit security project focusing on improving security for online or web-based applications. Any security evaluation should start with reconnaissance or information gathering. This step is to collect as much information as possible about the target. Next is to evaluate authentication and session management.

Few of the OWASP top ten web risks are injection, XML exploitation, cross site scripting (XSS), XSRF.

SQL injection attacks are riskier than XSS attack as it attacks the database. Two methods to protect sql injection is 1. Perform input validation, 2. Limit account privileges.

LDAP injection is a variation of an input injection attack. The focus on the back end of an LDAP directory service rather than a database server. Sanitization of input and defensive coding are essential to eliminate this threat.

XML injection is another variant of sql injection, where the back-end target is an XML application, again input sanitization is necessary to eliminate this threat.

Directory traversal/Command injection – the attack enables the attacker to jump out of the web root directory structure and into any other part of the file system hosted by the web server's host OS. The attack is against IIS 4.0. the attack uses modified URL to directory traverse out of the web root. This attack can be stopped using metacharacter escaping or filtering.

XML exploitation – it is a form of programming attack that is used to either falsify information being sent to a visitor or cause their system to give up information without authorization. One area of growing concern in regard to XML attacks is SAML. SAML abuses are often focused on web-based authentication.

SAML is used to provide web based SSO-single sign on between security domains.

XSS-Cross site scripting- attacking webserver. inject can be via CGI common gateway interface, web server vulnerabilities and many other ways. to protect this attack, patching web server, using web application firewalls, using HIDS and performing server-side input validation for length, metacharacter and malicious content.

Cross site request forgery -XSRF- it is similar to XSS, but it is focused on web browser. This is tricking the user to perform some action. Malicious file will hide in user system and wait for the webpage to be visited to execute. Stealing money using this attack is common. To protect this attack, two factor authentications is required or CAPATCHA and to add randomization string called nonce to each URL request and session establishment.

Assess and mitigate vulnerabilities in mobile system.

Device security

1. **Full device encryption**
2. **Remote wiping**
3. **Lock out**
4. **Screen locks- NFC attacks include man in the middle, eavesdropping, data manipulation and replay attack.**
5. **GPS (Global positioning system)**
6. **Application control-**
7. **Storage segmentation –**
8. **Asset tracking**
9. **Inventory control**
10. **Mobile device management-**
11. **Device access control.**
12. **Removable storage**
13. **Disabling unused features**
14. **Application security**
15. **Key management**
16. **Credential management**
17. **Authentication**
18. **Geotagging**
19. **Encryption**
20. **Application whitelisting – it prohibits unauthorized software from being able to execute. It is also known as deny by default or implicit deny**
21. **Blacklisting – allow by default or deny by exception.**

BYOD concerns – there are several alternatives to a BYOD policy including COPE, CYOD, corporate owned and VDI.

COPE- Concept pf company owned, personally enabled – companies purchase device and give to the employees.

CYOD-choose your own device – user can purchase from the approved list of devices.

Company owned mobile strategy is only for company purpose and not for personal work.

VDI- Virtual desk infrastructure – this has led to virtual mobile infrastructure.

Data ownership; support ownership

Patch management; anti-virus management ; forensics ; privacy ; on boarding/ off boarding ; adherence to corporate policy ; user acceptance ; architecture /infrastructure consideration ; legal concerns ; acceptable use policy ; on board camera video

Assess and mitigate vulnerabitlies in embedded devices and cyber physical systems.

Static systems/environment is a set of conditions, events and surroundings that don't change.

Cyber physical systems are essentially key elements in robotics and sensor network.

Methods of securing embedded and static systems-

1. Network segmentation –
2. Security layers
3. Application firewall; network firewall
4. Manual updates
5. Firmware version control
6. Wrappers -it is something used to enclose or contain something else. Configured to reject updates and changes.
7. Monitoring-
8. Control redundancy and diversity

Essential security protection mechanism.

Technical mechanism – Layering, Abstraction, data hiding, process isolation, hardware segmentation

Security policy and computer architecture-

Common architecture flaws and security issues-

1. **Covert channels**- it is a method used to pass information over a path that is not normally used for communication. **Overt channel** is an authorized controlled mode of communication**.**
   Covert timing channel is, it conveys information by altering the performance of a system component or modifying a resource's timing in predictable manner.
   Covert storage channel is, it writes data to a common storage where another process can read it.

Attacks based on design and coding flaws and security issues-

Trusted recovery – it will protect the system even during crash.

Input parameter checking-

Maintenance hooks and privileged programs- maintenance hooks are entry points into a system that are known only by the developer of the system.

Incremental attacks – some attacks are slow and gradual increments. Two such attacks are data diddling and salami attack. Diddling attack is doing small changes, it is more often done by insiders than outsiders. It is an active attack.

Salami attack- small amounts of money deducted from accounts regularly. Proper separation of duties will protect this issue.

Programming

TOC- Time of check is the time at which the subject checks on the status of the object. The difference between TOC and TOU is sometimes attacker use to replace original object with another object. TOCTOU attacks are often called race conditions. It is also known as state attacks.

SOA- service oriented architecture constructs new applications or functions out of existing, but separate and distinct software services.

Electromagnetic radiation – easiest way to eliminate EM radiation interception is to reduce emanation through cable shielding or conduit and block unauthorized personnel and device from getting close to equipment. And also reduce signal strength.

Several TEMPEST technologies will provide protection against EM issues. **A faraday cage is a special enclosure that acts as an EM capacitor. when it is used, no EM signal can enter or leave the enclosed area.**

Jamming or noise generators in use, it is difficult to retrieve the signal. Use control zone to protect signals.

10.Physical security requirements

Apply security principles to site and facility design

Physical control is the first line of defense.

Secure facility plan outlines the security needs of the organization and emphasis methods or mechanism to employ to provide security. Such plan is developed through a process known as critical path analysis. It is a systematic approach to identify relationship between mission critical applications, process and operations and all necessary supporting elements. Technology convergence is the tendency for various technologies, solutions and systems to evolve and merge over time.

Site-selection: security should be taken care while selecting the site.

Visibility- should have clear visibility. camera should be installed, Natural disasters

Facility design- secured architecture, called crime prevention through environmental design (CPTED)

Implement site and facility security controls.

Administrative control; technical control; physical control

When designing physical security for an environment focus on the functional order

1. Deterrence

2. Denial
3. Detection
4. Delay

Equipment failure – aging hardware should be scheduled for replacement and to repair. It should be based on mean time to failure (MTTF) and mean time to repair (MTTR). MTTF is expected typical functional lifetime of the device. MTTR is average time to repair that device. Schedule to replace the devices before MTTF expires. MTBF- mean time between failure is, between first and subsequent failures. If MTTF and MTBF are same, manufacture will list only MTTF.

Wiring closets – also called as premises wire distribution room and intermediate distribution facilities (IDF) common copper based twisted cable length is 100 mtr. Wiring closet are just one element of "cable plant management policy" it includes following

1. Entrance facility – also known as demarcation point. This is the entrance point to the building where the cable from the provider connects the internal cable plant.
2. Equipment room – this is the main wiring closet for the building, often connected to or adjacent to the entrance facility.
3. Backbone distribution system – this provides wired connection between equipment room and telecommunication rooms including cross floor connections.
4. Telecommunication room – also known as wiring closet. this serves as the connection needs of a floor or a section of a large building, also serves as the interconnection point between the backbone distribution system and the horizontal distribution system
5. Horizontal distribution system – this provides connection between telecommunication room and work areas, cable trays, cable hangers.

Server room/Data centers should be protected.

Smartcards – credit card size card embedded with magnetic strip, bar code or integrated circuit chip. Used for identification/authentication purpose. It is known by identity token containing IC chip, a processor IC card and IC card with ISO 7816 interface.

Memory cards are machine readable ID cards with a magnetic card. It holds data but unable process data like smart cards.

Proximity readers – it is a passive device, a field powered device or transponder

Intrusion detection systems – physical intrusion detection systems are called burglar alarms. Heartbeat sensor for checking signal.

Access abuses – masquerading is using someone else's security ID to gain entry into a facility. Piggybacking is flowing someone through secured doorway without being identified or authorized personally.

Emanation security – faraday cage; white noise and control zones. (TEMPEST countermeasures called)

Media storage facilities –Evidence storage –

Restricted and work area security – SCIF- Sensitive compartmented information facility used by government and military contractors to provide secure environment.

HVAC Considerations –

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 secondary. **Noise –** steady fluctuation**; transient -**a short duration of line noise disturbance**; clean –** non fluctuating pure power**; ground –** wire in an electrical circuit is grounded**.**

Noise - there are two types of electromagnetic interference (EMI). **Common mode** and **traverse mode**.

Common mode noise is generated by a difference in power between hot and ground wires of a power source or operating electrical equipment. Traverse mode noise generated by a difference in power between hot and neutral wires of a power source or operating electrical equipment.

RFI-radio frequency interference is another source of noise and interference that can affect many of the systems as EMI.

Temperature, Humidity and static- rooms intended to keep computers should generally be kept between 60-75 degree Fahrenheit (15-23 degree Celsius). Humidity in computer room should be maintained between 40-60 percent. **Too much humidity can cause corrosion. Too little humidity can cause static electricity.**

- **Static voltage damages**
- **40 destruction of sensitive circuits and other electrical components**
- **1000 scrambling of monitor displays**
- **1500 destruction of data stored on hard drive**
- **2000 abrupt system shutdown**
- **4000 Printer jam or component damage**
- **17000 Permanent circuit damage**

Water issues –

Fire prevention, detection and suppression –

Water suppresses temperature; soda acid and other dry powders suppress the fuel supply; CO2 suppress oxygen supply ; halon and other non-flammable gases interfere with the chemistry of combustion and suppress the oxygen supply.

Fire stages – step 1 incipient step 2- smoke step 3- flame step 4- heat.

Fire extinguishers

Class A - common combustibles – water, soda acid (dry powder or liquid chemical)

Class B - liquids – CO2, halon, soda acid

Class C - electrical – CO2, halon

Class D - metal – Dry powder.

Fire detection systems

Fixed temperature detection systems trigger suppression when a specific temperature is reached. Rate of rise detection systems trigger suppression when the speed at which the temperature changes reach a specific level. Flame-actuated systems trigger suppression based on infrared energy of flames. Smoke actuated systems use photoelectric or radioactive ionization sensors as triggers.

Water suppression systems

1. **Wet pipe**- also known as closed head system is always full of water. Water discharges immediately when suppression is triggered.
2. **Dry pipe** -it contains compressed air, when suppression is triggered, air escapes, opening water valve that fill the pipe and discharge water
3. **Deluge system** is another form of dry pipe that uses larger pipes and delivers larger volume of water. This is inappropriate for the environment which has computers, electrical equipment.
4. **Preaction system** – is a combination of dry /wet pipe systems. It exists as dry pipe during initial stages of fire and then pipes are filled with water. The water is released only after sprinkler head activation triggers are melted by sufficient heat. manual intervention can also be applied. this is the most appropriate system for the environment that has both people and equipment.

Gas discharge systems

CO2, halon and FM200(HALON replacement) --- gas systems shouldn't be used in people environment as it takes way oxygen.

100-degree temperature can damage storage tapes, 175 degree damages CPU, hardware. 350-degree damages paper product.

Implement and manage physical security

Perimeter security controls –

Fence – 3 to 4 feet high deter casual trespassers; 6 to 7 feet high are too hard to climb easily and deter most intruders. fence 8 ft more high with three strands of barbed wire deter even determined intruders.

Mantrap is a double set of doors protected by guard. if the subject is not authorized, gates remain closed. This is called delay feature. It prevents piggybacking and tailgating.

Lighting – 2 candle feet of power.

Internal security controls –

A lock is a crude form of identification and authentication to enter. Key based locks are the most common and inexpensive physical access controls. These are known as preset locks. This is subject to picking, attacks called shimming.

Electronic access control (EAC) incorporates three elements 1. An electromagnet to keep the door closed, 2. credential reader to authenticate subject and to disable electromagnet and 3. sensor to reengage the electromagnet when the door is closed. Eg. Badges.

Motion detectors

1. **Infrared** - monitors significant or meaningful changes in the infrared lighting pattern of a monitored area.
2. **Heat based** – changes in the heat levels and patterns
3. **Wave pattern** - transmits low ultrasonic or high microwave frequency signal to check the changes or disturbance.
4. **Capacitance motion** - senses changes in electrical or magnetic field.
5. **Photoelectric** - senses changes in visible light levels. It is installed in rooms that have no window and kept dark.
6. **Passive audio motion** - listens for abnormal sounds in the monitored area.

Intrusion alarms-

1. Deterrent alarms - to avoid further access/damages
2. Repellant alarms – triggers lights and sound to discourage intruders
3. Notification alarm -silent alarm
4. Local alarm system -upto 120db sound
5. Central station system- silent, but central team notifies
6. Auxiliary systems – to notify policy, fire station and medical service.

CCTV is a preventive measure and reviewing recorded events is a detective measure.

OEP- Occupant Emergency Plan - guides how to minimize threat to life. It doesn't address IT issues or BCP. Just personnel. BCP and DR addresses IT issues.

11. secure network architecture and securing network components

OSI Model

Encapsulation – Top layers to bottom layer. De encapsulation -Bottom to top layer. Presentation layer encapsulates the message by adding information to it, called header, at times end of the message, called footer.

Application layer (layer 7)- data stream until it reaches transport layer (layer 4). In transport layer it is called segment or datagram (TCP protocols) UDP; In network layer (layer3) it is packet. In datalink layer (layer 2) it is frame. In physical layer -bits.

Physical layer- bits to frame and frame to bit conversion. SONET, HSSI, V.24 and V.35, x.21, EIA/tia232,449, NIC at physical layer, hubs, repeaters, concentrators, and amplifiers.

Data link layer- packets to frame through Ethernet (IEEE 802.3), token ring (IEEE 802.5), ATM (Asynchronous transfer mode), FDDI(fiber distributed data interface), copper DDI. Ethernet is in use today. Protocols in this layer are SLIP, PPP, ARP, L2F, L2TP, PPTP, ISDN. The hardware address is MAC, media access control which is a 6byte -48 bits binary address. The first 3 bytes denote the vendor or

manufacture of the physical network interface. This is known as organizationally unique identifier (OUI). Last 3 bytes represent unique number to that interface by the vendor.

EUI-48 extended unique identifier. ARP used to resolve Ip address into MAC Address.

LLC- Logical link control – and MAC sublayer. Switches and bridges are at data link layer.

Network layer – ICMP, RIP, OSPF, BGP, IGMP, IP, IPSEC, IPX, NAT, SKIP. This layer is responsible for routing information but doesn't guarantee verifying. Verifying is the role of transport layer. Network layer manages error detection/traffic control. Routers and bridge routers work at network layer.

Non-IP protocols are IPX, Appletalk and NetBEUI.

Two routing protocols – **Distance vector** -it maintains the destination networks along with metrics of direction, distance and hops. **Link state** maintain topography map to find shortest path to the destination. RIP and IGRP are distance vector protocols. OSPF is Link state.

Transport layer – responsible for managing the integrity of the connection and controlling the session. It accepts a PDU (Payload data unit). It converts PDU from session into segment. It establishes logical connection between devices and provides end to end transport service to ensure data delivery. This includes segmentation, sequencing, error checking, controlling the flow of data, error correction, multiplexing and network service optimization. Protocols are TCP, UDP, SPX, SSL and TLS.

Session layer – responsible for establishing, maintaining and terminating communication session between two computers. Simplex, half -duplex and full duplex. Simplex is one way communication; half duplex is two-way communication but only one direction can send data at a time. Full duplex is two-way communication in which data can be sent in both directions simultaneously. Protocols are NFS, SQL, RPC.

Presentation layer -is responsible for transforming data received from application layer into a format that any system following the OSI model can understand. Standard structure. It is responsible for encryption and compression. Thus, it acts as an interface between network and application. Standard formats are ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI.

Application layer- is responsible for interacting with user and applications. HTTP, FTP, LPD, SMTP, Telnet, TFTP, EDI, POP3, IMAP, SNMP, NNTP, SET. Gateway works at application layer.

TCP/IP Model – also called DARPA or DOD model. Consists of four layers. 1. Application (also known as process), 2 Transport (host to host) ,3 Internet (internetworking), Link (network interface)

TCP/IP is a platform independent protocol based on open standards.

VPN protocols are PPTP, L2TP, SSH, OPEN VPN(TLS/SSL) and IPSEC. TCP wrapper is an application that can server as a basic firewall by restricting access to ports and resources based on user IDs or user system IDs. Using TCP wrappers is a form of port-based protocol.

Transport layer protocols -TCP is full duplex and UDP is simplex. Each have 65536 ports. 0- 65535. The combination of IP address and port is known as Socket. The first 1024 ports are called well known ports 0-1023. Ports 1024- 49151 are known as registered ports.49152- 65535 are random or dynamic or ephemeral ports.

TCP Three-way handshake

1. Client sends syn packets to the server
2. Server send syn/ack
3. Client sends ack.

Fin to finish the session. RST for immediate abrupt session. TCP transmissions are tagged with a sequence number. No of packet transmitted before ack packet sent is known as transmission window. Data flow is controlled through a mechanism called sliding window. TCP header is 20 -60 bytes long. TCP field value is 6.

UDP field value is 17. Four parts, source, destination address, message length and checksum.

Network layer protocols and IP networking basics-

Similar to UDP, IP is connection less and unreliable. IPV4 use 34 bit addressing scheme. IPV6 uses 128bits.

IP classes – Class A 0- 126; 127 is a loopback address; class B-128-191; Class C-192-223; Class D-224-239, Used for multicasting; class E-240-255 is reserved for future use.

A default subnet mask 255.0.0.0 CIDR /8; B 255.255.0.0 /16; C 255.255.255.0 /24.

ICMP (Internet Control Message Protocol)- is used to determine health of the network or a specific link. It is utilized by ping, traceroute, pathping. Smurf attack, ping of death, ping floods is by using ICMP. ICMP field value is 1.

Codes – 0 echo reply, 3- destination unreachable, 5-redirect, 8-echo request ,9- router advertisement, 10- router solicitation, 11- time exceeded.

IGMP (Internet Group Management Protocol) -it allows system to support multicasting. Field value for IGMP is 2.

ARP-

Common application layer protocols – telnet TCP 23, FTP -20(Passive data),21(control connection), TFTP -UDP 69, SMTP -TCP 25, POP3- tcp 110, IMAP- tcp 143 , DHCP -UDP 67,68(Source) , HTTP -TCP 80, SSL-TCP 443, LPD(Print jobs) TCP 515 , Xwindow-tcp 6000-6063 , NFS- TCP 2049, SNMP-UDP 161, 162(Trap).

TCP/IP is a multilayer protocol. **Vlan hopping attack- is performed by creating a double encapsulated IEEE 802.1Q Vlan tag.**

DNP3- distributed network protocol. Primarily used in the electric and water utility and management industries.

TCP/IP Vulnerabilities –

Domain name system-DNS. FQDN has three parts 1. Top level domain/TLD (com) ,2. Registered domain name(google) ,3. Subdomain(www). Total length of FQDN can't exceed 253 characters. Any single section can't exceed 63 characters. Primary authoritative name server hosts the original zone file for the domain, secondary authoritative server used to host read only copies of zone file. A zone file is the collection of resource records or details about specific domain.

DNSSEC- Domain name system security extensions.

DNS poisoning – 1. Deploy a rogue DNS sever (also known as DNS Spoofing or DNS Pharming)

Domain hijacking –

Converged protocols – For proprietary services.

1. **Fibre channel over ethernet (FCoE)**- it is a form of network data storage solution (SAN/NAS). That allows for high speed file transfer upward of 128 GBps. It requires its own infra, however it can be used at existing infra as well. It is used to encapsulate fibre channel communication over ethernet networks. It is layer 3 protocol.
2. **MPLS-Multiprotocol label switching** – high throughput and high performance. It also supports T1/E1, ATM, Frame relay, sonnet and DSL.
3. **Iscsi- Internet small computer system interface**- network storage standard based on IP. Low cost compared to fCoe. used in LAN and Wan.
4. **Voip**- used for voice/data via Tcp/ip.
5. **SDN- software defined networking** – it is for network virtualization. Multiple vendor product can be used. SDN control layer handles data transmission paths, communication decision trees and flow control

CONTENT DISTRIBUTION NETWORKS

CDN- lower latency and high performance as it is distributed across locations and accessible via internet. Akamai, amazon are examples.

Wireless networks - Data emanation occurs when EM signals travel. Tempest is the solution to this.

Securing wireless access point – 802.11 is a standard for wireless network communications.

- **802.**11 2 mbps 2.4 GHZ FREQUENCY
- **802.**11a 54mbps 5ghz
- **802.**11b 11 mbps 2.4ghz
- **802.**11g 54 mbps 2.4ghz
- **802.**11n 200+mbps 2.4 or 5 ghz
- **802.**11ac 1gbps 5 ghz

Wireless access points should be configured to work in infrastructure mode (2 Nic cannot interact directly), not ad hoc mode(2 Nic interact direct).

Stand-alone – connecting two wireless clients; **wired extension** – when the wireless access point act as a connection point to link the wireless clients to wired network. An **enterprise extended** – when multiple wireless access points are used to connect large physical area to the same wired network. **Bridge mode** is used when wireless connection connects two wired networks.

Securing SSID- SSID is broadcast by the WAP via special transmission called a beacon frame. Use WAP2 to secure. Conducting site survey is the process of investigating strength, presence.

Using secure encryption protocols

IEE 802.11 standard supports two methods 1. OSA Open system authentication, no authentication required 2. SKA shared key authentication, auth must. WEP, WAP and WAP2.

WEP- wired equivalent privacy- it provides protection from packet sniffing and eavesdropping.it uses predefined shared secret key. WAP doesn't use same static key to encrypt instead it negotiates a unique key set with each host. WEP use RC4.

WPA – wifi protected access. it was temporary fix until 802.11i. WPA is based on LEAP and TKIP and employs secret passphrase for authentication.

WPA2 – it uses Countermode cipher block chaining message authentication code protocol (CCMP). Which is based AES encryption.

802.1x/EAP- both WPA and WPA2 supports enterprise authentication known as 802.1X/EAP. EAP is an authentication framework.

PEAP- Protected extensible authentication protocol. It encapsulates EAP methods within a TLS tunnel that provide authentication and potentially encryption. EAP usually not encrypted as it was designed for physical network. PEAP provides encryption for EAP methods.

LEAP – Lightweight extensible authentication protocol is a cisco proprietary alternate to TKIP and WPA. EAP TLS should be used as an alternate to LEAP.

Mac filter – allow traffic based on mac address. It is very complex

TKIP- temporal key integrity protocol. it combines IV with secret root key.

CCMP- it uses 128 bit key. AES encryption. In use today. No attacks found against this. 802.11i

Determining antenna placement – if a base station has omnidirectional antennas, it must be positioned pointing straight up vertically. If a directional antenna used, it must be positioned the point toward the area of desired use.

Antenna types – the standard straight and pole antenna is omnidirectional that can send and receive signal in all directions. It is also called rubber duck antenna. Directional antenna are yagi, cantenna , panel and parabolic.

WPS- WIfi protected setup is a security standard for wireless networks. It should be disabled.

Using captive portals – authenticated technique that redirects a newly connected wireless web client to a portal access control page. Mostly used in public places like hotels, airports.

General wifi security procedure-

Wireless attacks – 1. War driving – someone looking for wireless networks that they aren't authorized to access. 2. War chalking. 3. Replay attacks. 4.IV – When IV is short, it can be attacked. 5. Rogue access points – 6. Evil twin- connect to different network in clear text.

Secure network components

Network access control (NAC) – is a concept of controlling access to an environment through strict adherence to and implementation of security policy. The goals are prevent/reduce zero-day attacks. Enforce security policy throughout the network, use identities to perform access control. Preadmission checks the requirements before allow, postadmission is based on user activity.

Firewalls –

1. **Static packet filtering –** first generation firewalls, operate at layer 3. They can also be called screening routers.
2. A**pplication-level gateway-** it is also called proxy firewall. Second generation firewall. Operate at layer 7.
3. **Circuit level gateway-** between trusted partners. operate at session layer 5. SOCKS is a common implementation. Also known as circuit proxies. Second generation firewall.
4. **Stateful inspection firewall –** also known as dynamic packet filtering. third generation firewall, at network and transport layers 3 and 4.
5. **Deep packet inspection firewall –** at application layer in order to filter payload contents of a communication. Also known as information extraction. It is able to block domain names, malware spa. It is often integrated with application layer firewalls or stateful inspection firewall.
6. **Next gen firewall –** is a multifunction device it can include IDS, TLS, Qos, web filtering.

Multihomed firewall – it has more than one interface. Also known as dual homed firewall. **A bastion host is a computer or appliance exposed on internet and has been hardened by removing all unnecessary elements such as services, programs, protocols and ports.**

a screened host is a firewall protected system logically positioned inside private network. It acts as proxy.

Single tier **-** internet-router-firewall-private network

Two tier 1**-** internet- router- firewall -Private network and DMZ

Two tier 2 – internet-router-firewall – DMZ- firewall -Private network

Three tier 1 – internet -router -firewall -DMZ-firewall- Transaction subnet -Firewall-Private network

Three tier 4 -Internet -router -firewall-DMZ- transaction subnet -firewall-private network

Endpoint security-

Repeaters, concentrators and amplifiers – used to strengthen communication signal over cable segment. Work at layer 1. Same collision and broadcast domain.

Hub – layer 1– used to connect multiple system that use same protocol. It ensures traffic reach intended host. Same collision and broadcast domain

Modems

Bridges – layer 2- used to connect two networks together. It forwards traffic. Same collision and diff broadcast domain

Switches – layer 2. it forwards to the exact destination. Create separate Collison domains and improve overall throughput of data. diff collision and same broadcast domain

Routers – layer 3- used to connect similar networks and control traffic flow. diff collision and diff broadcast domain

Brouters – combination of router and bridge – it routes first, if it fails, then it acts as bridge.

Gateway – it connects two different networks. responsible for transferring traffic from one network to another. also known as protocol translators. Operate at layer 7.

Proxies – Form of gateway that does not translate across protocols.

LAN extenders.

Cabling, topology and transmission media technology

Common private circuit technologies include dedicated or leased lines such as PPP, SLIP, ISDN and DSL Connections. Packet switching technologies such as x.25, frame relay, ATM, SDLC, HDLC.

Transmission media

Coaxial cable – core of copper wire surrounded by a layer of insulation. it allows two-way communication. Resistant to EMI. Support high bandwidth. Used in audio connections. It offers longer usable length then twisted pair. Two types. Thinnet also known as 10Base2- 185 meters and 10Mbps throughput. Used for connecting to backbone trunks of thicknet.

Thicknet also known as 10Base5, 500 meter and 10Mbps throughput

Baseband and broadband cables.

Twisted pair – extremely thin and flexible. Four pair of wires that are twisted around each other and sheathed in a PVC insulator. if there is a metal foil, it is called STP, Shielded twisted pair. It provides additional protection. Without foil is known as UTP. UTP is often referred as 10baseT, 100BaseT or 1000BaseT.

UTP categories are cat1- voice only, cat 2 – 4mbps, cat 3 10 mbps , cate4 -16 mbps, cat5-100 mbps, cat 6- 1000 mbps, cat 7-10 gbps.

Conductors & 5-4-3 rule –

Topology

Ring – connected to each system in ring shape. It is a unidirectional transmission loop. Traffic management is performed by a token. If one system is broken, all goes wrong.

Bus – each system connects through trunk or backbone cable. can transmit data simultaneously which can result in collisions. all system hear the data. If one system is broken, no issue with other system. Trunk line is the single point of failure. Linear employs single trunk line. tree employs single trunk line with branches.

Star – employs centralized device. This can be simple hub or switch. Hub is a single point of failure. It uses less cabling. Ethernet is a bus-based technology. Token ring is a ring based.

Mesh- connects using numerous paths. It provides redundant connections.

Wireless concepts

Spectrum techniques

1. **FHSS- frequency hopping spread spectrum-** not in parallel. It is in serial, changing the frequency frequently.
2. **DSSS- Direct sequence spread spectrum –** in parallel. This provides higher rate of data throughput than FHSS.
3. **OFDM-Orthogonal frequency division multiplexing –** it employs digital multicarrier modulation scheme. Signals are perpendicular.

Cellphone

Bluetooth 802.15 – bluejacking- allows an attacker to send SMS to your device. **Bluesnarfing** allows hacker to connect your Bluetooth devices without your knowledge and extract information. **Bluebugging** is an attack that grants hackers remote control over the feature and function of Bluetooth device. This can turn on microphone to use the phone as an audio bug. Generally, Bluetooth range is 30 ft some have 100 meters.

RFID- Radio frequency identification – to track

NFC- Near field communication –

Cordless phones- Mobile devices –

LAN Technologies

Ethernet – supports full duplex, uses twisted pair. Often deployed on star or bus topologies. based on 802.3. individual units of ethernet data are called frames. Fast ethernet supports 100 MBps. gigabit ethernet supports 1000Mbps or 1GBps, 10 gigabit supports 10 Gbps throughput

Token ring- employed in ring or star. rarely used today.

FDDI (Fiber distributed data interface)- high speed token passing technology that employs two rings with traffic flowing in opposite directions. Expensive, used in backbone. Less expensive and slower is called CDDI that uses twisted pair cable. CDDI is vulnerable to eavesdropping and interference.

Analog and digital –

Digital signals are more reliable than analog.

Synchronous (Timing based /timestamp) and asynchronous (start/stop based- pstn is the example)

Baseband (support only single channel, uses direct current apply to the cable. ethernet is a baseband technology)

Broadband can support multiple channels. It uses frequency modulation. Suitable for high throughput. Analog signal. ISDN, T1, DSL, T3 are examples.

Broadcast to all recipients; multicast to multiple recipients; unicast to single communication to a specific recipient.

LAN media access-

CSMA- carrier sense multiple access – it listens and transmits and wait for ack. It doesn't address collision.

CSMA/CA- with collision avoidance – two connection inbound and outbound. Appletalk and 802.11 are examples.

CSMA/CD- collision detection -it listens for collision. If detected it transmits jam signal.

Token passing -using digital token. it prevents collision.

Polling -using master -slave configuration. SDLC uses polling. Primary systems ask secondary system whether to transmit data.

12. Secure communication and network attacks

Network and protocol security mechanism

Secure communication protocols

Simple Key Management for Internet Protocol (SKIP)

Software IP Encryption (swIPe)

Secure Remote Procedure Call (S-RPC) - authentication service

Secure Electronic Transaction (SET)

IPSEC- it uses public key cryptography to provide encryption, access control, non-repudiation and message authentication. Primary for VPN. It can operate in transport or tunnel mode.

Kerberos -offers single sign on solution for users.

SSH- good example of end-to-end encryption technique.

Signal protocol - this is a cryptographic protocol that provides end to end encryption for voice communications, videoconferencing, and text message services. It is a nonfederated protocol.

SSL- 128 bit key, session-oriented protocol that provides confidentiality and integrity.

TLS- it uses stronger authentication and encryption protocols. When it is implemented at layer 3 for VPN, it is called OpenVPN. It is also used in UDP to encrypt and in session initiation protocol connections. **SIP** is a protocol associated with VoiceIP.

Authentication protocols

CHAP- Challenge handshake authentication protocol- used over PPP links. It encrypts user name and password. It performs challenge response dialog that cannot be replayed. It keeps reauthenticating.

PAP-Password authentication protocol – standard protocol for PPP. It transmits username and password in clear text.

EAP- extensible authentication protocol- this is a framework for authentication instead of an actual protocol. It allows for customization.

Secure voice communication

Normal PBX or POTS/Public switched telephone network voice communications are vulnerable to interception, eavesdropping, tapping and other issues.

VOIP- caller ID can be falsified by hacker. hacker can perform VoIP phishing or SPIT (Spam over Internet Telephony) attack. Vuln to DOS attacks. man in the middle attacks by spoofing call managers. Secure real time transport protocol (SRTP) is used in many VOIP communications.

Social engineering –

Fraud and abuse – attackers known as phreakers abuse phone systems in much the same way that attackers abuse computer networks. Deploy direct inward system access (DISA) technologies to reduce PBX fraud. Some of the phreaker tools are **black box** – manipulates line voltages to steal long distance services. **Red box** is used to stimulate tones of coins being deposited into a pay phone. **Blue box** is used to stimulate 2600 Hz tones to interact directly with the phone network trunk systems. **White box** is used to control the phone system. It is a dual tone multifrequency generator (DTMF)

Manage email security – clients retrieve email from their server-based inboxes using POP3 or IMAP. Internet compatible email systems relay on x.400 standard. Sendmail is the most common for SMTP server for unix systems. Exchange is most common for Microsoft systems.

When sufficient numbers of messages are directed to a single user's inbox or through a specific SMTP server, a DOS attack can result. this is called mail bombing.

Email security solutions –

S/MIME-Secure multipurpose internet mail extension - it is an email security standard that provides authentication and confidentiality to email through public key encryption and digital signatures. Authentication is provided through x.509 digital certificates. Privacy provided through use of public key cryptography standard (PKCS) encryption. Two types of messages can be formed using SIMME. 1. Signed

message ,2. secured enveloped message. Singed message provides integrity, sender authentication and non-repudiation. enveloped message provides integrity, sender authentication and confidentiality.

MIME Object security services (MOSS)- it employs MD2 and MD5 algorithms.RSA public key and DES. It provides integrity, confidentiality, authentication and non-repudiation.

Privacy enhanced mail (PEM) – it uses RSA, DES and X.509. provides integrity, confidentiality, authentication and non-repudiation

Domainkeys identified mail (DKIM)- it is to assert that valid mail is sent by an organization through verification of domain name identity.

Pretty good privacy (PGP)-is a public-private key system that uses a variety of encryption algorithms to encrypt files and email messages. The first version used RSA and second version used IDEA, but later version offered spectrum of algorithm options. PGP is not a standard, but rather an independently developed product that has wide internet support.

Opportunistic TLS for SMTP Gateway – TLS support for SMTP

Sender policy framework – to protect against spam and email spoofing. It will check the mail whether to allow or not.

Remote access security management –

Dial up protocols –

Point to point protocol (PPP)- full duplex protocol used for transmitting TCP/IP packets over various non-LAN connections, such as modem, ISDN, VPN, frame relay. Protection is through CHAP and PAP.PPP is a replacement for SLIP

SLIP- Serial line internet protocol -older technology developed to support TCP/IP over asynchronous serial connections. It requires static IP and no error detection or correction.

Centralized remote authentication services

RADIUS – used to centralize authentication of remote dial up connections. remote access server pass logon credential to radius server for authentication. It uses UDP 1812 and TCP 2083 over tls.

TACACS+ - TACACS integrate authentication and authorization process. XTACACS keeps authentication authorization and accounting process separate. TACACS+ improves by adding two factor authentication and it is the most current version. it uses TCP 49.

VPN &Tunneling –

VPN Protocols – PPTP, L2F, L2TP are operating at datalink layer.

PPTP is an encapsulation protocol developed from the dial up point to point protocol. At data link layer and used for IP networks. It creates point to point tunnel between two systems and encapsulates packets. it offers protection through MS-CHAP, CHAP, PAP, EAP, SPAP. PPTP doesn't support radius and TACACS+.

Layer 2 forwarding and L2TP- cisco developed its own protocol called layer2 forwarding. It doesn't offer encryption. L2TP supports radius and tacacs+. IPSEC is commonly used as a security mechanism for L2TP.

IPSEC- it is both standalone VPN protocol and also the security mechanism for L2TP. AH- provides authentication, integrity and non-repudiation. ESP provides confidentiality. It works at layer 3. In transport mode, IP packet is encrypted but not the header. In tunnel mode , entire IP packet is encrypted.

VLAN- Vlan 1 very typically is the designated management traffic Vlan. Vlan are created by switch at layer 2.

Virtualization –Virtual software-

Virtual networking –

SDN- Software defined networking – it aims at separating the infrastructure layer from control layer. This also removes the traditional networking concepts of IP addressing, subnets, routing. It offers new network design that is directly programmable from a central location, is flexible, open standard based. Virtual SAN-storage area network combines multiple individual storage devices into a single consolidated one.

NAT- network address translation

NAT maps one internal IP to one external IP. PAT maps one internal IP to an external IP with port number combination.

Private IP address

10.0.0.0- 10.255.255.255 (Full A class 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- it maintains the information about the communication sessions between client and external system.

Static and dynamic NAT. NAT Traversal was designed to support IPSEC.

Automatic private IP addressing (APIPA)- from the range 169.254.0.1 to 169.254.255.254. if dhcp addressing fails.

Switching technologies –

Circuit switching – it employs permanent, physical connections.

Packet switching – logical transmission technology. Not permanent link. Bursty traffic. Variable delays, connectionless, sensitive to data loss, used for any type of traffic.

Virtual circuit -also called communication path is a logical pathway or circuit created over packet switched network between two specific endpoints. 1. PVC (permanent virtual circuit)- always

available .2 SVP (Switched virtual circuit)- it is more like a dial up connection and one way. Multiple paths may exist. Pvc is a two-way communication.

WAN Technologies

Dedicated line/leased line – always available. T1, T3, E1, E3 and partial T1.

Nondedicated line- standard modems, DSL and ISDN are example of this.

DSL line can be upto 5000 meters. ISDN support both voice and high-speed data communications. There are two classes. 1. BRI- Basic rate interface – it offers connection with two B channels and one D channel. B channel for data with 64kbps throughput and D channel for call with 16kbps. Total throughput is 144 kbps. 2. PRI- Primary rate interface -it offers multiple b Channel connection with 64kbps and single D channel with 64kbps. So total 192kbps and upto 1,544 mbps.

WAN Connection technologies

The border connection device is called channel service unit/data service unit-CSU/DSU. Which will convert LAN signal to the format used by WAN carrier network and vice versa. CSU/DSU contains data terminal equipment and data circuit terminating equipment (DTE/DCE) which provides actual connection. CSU/DSU acts as translator.

X.25 -is an older packet switching technology it uses permanent virtual circuit. Lower performance

Frame relay -packet switching technology that also uses PVC's. it supports multiple PVCs over single wan carrier service connection. A key concept here is CIR- Committed information rate. It is a connection-oriented packet switching technology.

ATM- asynchronous transfer mode is a cell switching WAN communication technology. Fixed length 53-byte cells. Very efficient and high throughputs. It can use wither PVC or SVC.

SMDS-Switched multimegabit data service - is a connectionless packet switching technology. It is often used to connect multiple LAN to create MAN. Preferred connection mechanism for linking remote LANs that communicate infrequently. It fragments data into small transmission cells. High speed traffic is supported.

Synchronous digital hierarchy and synchronous optical network

SDH and SONET are fiber optic high speed networking standards. SDH was by International telecommunication and SONET by American national standard. High speed duplex communications. Supports speed of 51.48 Mbps which supports STS of SDH and STM of sonnet. Both support mesh and ring topologies.

Specialized protocols –

SDLC- Synchronous data link control- for permanent physical connection. It uses polling. Layer 2.

HDLC- high level data link control – supports full duplex it also uses polling, layer 2. It offers flow control and error detection and correction.

High Speed Serial Interface (HSSI) – DTE/DCE interface standard defining how multiplexor and routers connect to high-speed network eg Atm.

Dial up encapsulation protocol

PPP is an encapsulation protocol.

Verify integrity transmission -Checksum hash total used to verify integrity of transmission. Hash total added to end of message is called message digest.

Security boundaries

DOS- the attacker installs remote control tools called, bot, zombies or agents. Disable echo replies, block broadcast feature on border systems.

Eavesdropping – listening to communications.

Impersonation/Masquerading – pretending to be someone. Prevention Kerberos

Replay attacks – attempts to reestablish the connection. Prevent by using onetime authentication and sequenced identification

Modification attack- captured packets are altered then played against a system. Prevent by using digital signature verification and packet checksum verification.

ARP Spoofing – DNS poisoning, spoofing, hijacking. – prevent DNSSEC (Domain name system security Extension)

hyperlink spoofing (alter the hyperlink or redirect)

13.Managing identity and authentication.

Controlling access to assets – information, system, devices, facilities and personnel.

Subjects - active entity. users, programs.

Object – passive entity. that provides information to subject. Files. Databases.

Types of access control

Preventive access control; detective access control; corrective access control

Deterrent, recovery, directive, compensating, administrative, logical/technical controls, physical control.

Identification and authentication

Identification and authentication always work together, identity username and authenticate password

Registration and proofing of identity

Authorization and accountability – accountability relies on strong identification and authentication, not authorization.

Authentication factors

- Type 1- something you know (PIN)
- Type 2 – something you have (smartcard)
- Type 3- something you are or do (fingerprint)

Context aware authentication – based on geolocation, time and type of device

Passwords- static password is the weakest form of authentication. MD5 have vulnerabilities and should not be used to hash passwords.

Strong password- maximum age ; password complexity(NIST 800-63B) ; password length(minimum 8 characters) . 32 bits used to be used in salts; password history

Password phrases –

Cognitive password- a series of questions asked.

Smart cards and tokens – type 2 . example is credit card. It uses asymmetric cryptography to encrypt data. It is tamper resistant. It provides both identification and authentication.

Common access card or personal identity verification (PIV) cards are like badges.

Tokens

It displays 6-8 digit number. Hardware token device use dynamic onetime password.

Synchronous dynamic password tokens- time based. Valid for specific time

Asynchronous dynamic password token – challenge based nonce

Two step authentications

HOTP -HMAC (Hash message authentication code) includes hash function used by HMAC OTP . it is like challenge based. It is valid till used.

TOTP- time based. Time frame is there to use it.

Biometrics – type 3

Finger prints; face scans; retina scan (blood vessals at the back of the eye); iris scan (color area around pupil, 2nd most accurate biometric method, which never changes in life); palm scans (vein scan) ; hand geometry ; heart/pulse patterns , voice patterns recognition.

Signature dynamic and keystrokes are behavioral bio metrics methods.

Keystroke- flight time how long it takes between key presses and dwell time how long key is pressed.

Bio metric factor error ratings

Type 1 – valid subject not authenticated. False rejection rate (FRR)- Ratio of type1 error to valid authentication. False negative.

Type 2 – invalid subject authenticated. False acceptance rate (FAR) - Ratio of type2 error to valid authentication. False positive.

CER- Crossover error rate also known as ERR (Equal error rate). Device with lower CER is more accurate.

Biometric registration – enrollment must take to register. Stored data is the reference profile. Also known as reference template. Throughput rate is how much time system use to scan a subject and approve or deny access.

Multifactor authentication

Device authentication - secureauth identity provider is used for device authentication. Bring your own device concept. MDM solutions use context aware authentication method to identify access. 802.1x is port-based method used sometimes.

Service authentication – service accounts

Implementing identity management

Centralized and de centralized access control system

Single sign on- centralized access control technique.

LDAP and centralized access control - trust are established between domains to create security bridge.

PKI uses LDAP when integrating digital certificates into transmissions.

Kerberos

Most well-known Ticket system is called Kerberos. It **offers single sign on solution for users and provide protection for logon credentials. Current version is 5 and it is symmetric key cryptography (secret key). It uses AES. It provides confidentiality and integrity . helps protecting end to end security and protect against eavesdropping and replay attacks.**

KDC- Key distribution center. All clients and servers are registered with KDC. It provides authentication service. it maintains all secret key for all network members.

Kerberos authentication server – it hosts the functions of KDC. TGS (Ticket granting service) and authentication service (AS). Authentication service verifies the ticket to approve or reject. This server is called KDC.

Ticket granting ticket -TGT- it provides proof that a subject has authenticated through KDC and is authorized to request ticket to access other objects. TGT is encrypted and includes symmetric key, an expiration time and user IP address. Subject present TGT when requesting tickets to access objects.

Ticket – it is an encrypted message that provides proof that subject is authorized to access an object. It is sometimes called service ticket (ST). Kerberos issues ticket. Tickets has specific time limit. Once it expires, subject has to renew it or get new ticket.

For request steps - Client/user type username/pass; KDC checks the database, then KDC creating a symmetric key with hash of the user's password. then creating TGT with time stamp. Then sending this to client. Clients installs TGT and decrypts the key using hash of user's password.

For object access - Client send TGT back to KDC for requesting access to an object. KDC verifies TGT is valid and send service ticket to client. Client send ST to the requested server. the server checks the validity of the ticket with KDC then open up connection to use.

Kerberos works over LAN, Remote access and client server resource. KDC is single point of failure.

Federated identity management and SSO – SSO over internet. Multiple organization come together in FIM. It uses SAML(Security assertion markup language) and SPML- service provisioning markup language.

HTML – It was derived from SGML (Standard generalized Markup Language) and GML.

XML- used for exchanging information by importing and exporting.

SAML (Security Assertion Markup Language) – Xml based used to exchange authentication and authorization info b/w federated org. SSO for browser access.

SPML (Service Provisioning Markup Language) is based on directory service markup language (DSML). Used for exchanging info. Which can display LDAP based directory service in XML format

Extensible access control ML(XACML)- used to define access control polices within XML format. It implements attribute based and role based access control.

Oauth 2.0 – open standard used for access delegation.

OpenID – it provides decentralized authentication . allowing users to log in to multiple unrelated web sites with set of credentials maintained by third party service . open id is also known as relaying party .

Open id connect – it is an authentication layer using 2.0 framework. It uses java script notation(JSON) web token.

Scripted access can be used to implement SSO where true SSO solution is not available .

Credential management system – password safe is the example. and storing credentials in browser.

Integrating identity services. Identity as service (IDass).

AAA protocols – authentication, authorization, accounting

RADIUS- remote authentication dial in service – centralized authentication for remote connection. it uses UDP. And encrypts only the exchange of password. it doesn't encrypt entire session.

TACACS+ Terminal access controller access control system(TACACS) -open publicly documented protocol. It separates authentication, authorization and accountability. It encrypts entire information. it uses TCP PORT 49. Tacacs and xtacacs uses UDP.

Diameter – enhanced version of radius is diameter. It uses IP, mobile IP, VOIP. Preferable where roaming support is required such as wireless device and smartphones. It uses TCP 3868 or scream TCP. It also supports IPSEC and TLS.

Identity access provisioning – often called enrollment.

Account review – to prevent excess privilege over time. Which is called privilege creep.

Account revocation – should be revoked when no longer is needed.

14.Controlling and monitoring access

- Permission - Access granted for an object and what you can do with it like open, read etc.
- Rights - ability to take an action on object eg. modify sys time etc.
- Privileges -combination of rights and permission. For example administrator will have full privileges.

Authorization mechanism

Implicit deny – a basic principle of access control is implicit deny and most authorization use it. which means explicit deny is not required. If the administrator doesn't provide specific permission to user, he will not have access. Though administrator explicitly deny it, user might not have access if it is not permitted.

Access control matrix- it is a table that contains subjects, objects and assigned privileges. It will show the exact permission authorized by each user for each file. It covers more than ACL. Each file has a separate ACL that lists authorized users and their assigned permissions.

Capability tables – it is subject based. They are different from ACL. In this capability table created for accounting role will have list of all objects that accounting role can access. In contrast, ACL focus on objects.

Constrained interface restricting access in application. It hides the feature if the user doesn't have permission to access it.

Content dependent control database view is the content dependent control. View retrieves specific columns from table creating a virtual table.

Context dependent control it requires specific activity before granting user an access. Accessing page by page . for ex: first cart, then purchase then payment. It also based on date and time.

Need to know access is given based on what they have to access.

Least privilege only what is required to access.

Separation of duties and responsibilities activities are performed by two or more employees to prevent fraud.

Security policy -Implementing defense in depth – it uses multiple layers

Access control models –

Discretionary access control model - Owner grant or reject access. NTFS on windows uses DAC model, uses ACL on objects.

Non-DAC model – admin centrally administered. Any models except DAC is non-discretionary model

Role based – RBAC- access will be given to the role/group. Microsoft windows uses this. administrator determine privileges based on the roles,

Rule based – uses set of rules or restriction or filters. Ex : firewall. Based on rules.

Attribute based – it uses multiple attributes. Much more flexible than rule based. Software defined networks use this model. Admin guys create a rule within policy like" allow managers to access WAN".

Mandatory access – based on labels. It is referred as lattice-based model. Prohibitive than permissive.

Another method related to RBAC is TBAC- Task based access control. The focus is on task by controlling access, not on the identity.

Classification with MAC model is **hierarchy environment –** from low to medium to high levels. Access is provided to that level and below that level. Top secret access can access secret level as well. But not higher level. **Compartmentalized environment** no relationship between one security domain and another. Each domain is isolated. To access an object, subject should have clearance for its security domain **hybrid environment** it combines both hierarchy and compartment. It provided granular control over access. Difficult to manage.

Risk – possibility or likelihood a threat will exploit vulnerability resulting to harm or loss. **Threat** – potential occurrence resulting undesirable outcome. **Vulnerability** – Any type of weakness. **Threat modeling** – process of identifying, understanding and categorizing potential threats.

Common access control attacks

Once attackers gain access credentials, they can launch an online **impersonation** attack by logging in as user.

Access aggregation attacks – collecting multiple piece of non-sensitive information and combining them to learn sensitive info. Reconnaissance attacks are aggregation attacks like port scanning, IP details. Need to know, lease privilege , defense in depth are controls to prevent this attack.

Password attacks – password should be in SHA-3, not in clear text. **Dictionary attacks**

Brute force attacks – attackers have tool to run possible character to find credential. Hybrid attacks attempt dictionary attack then brute force attack. Attackers analyze hash and crack the password. this is also known as comparative analysis.

Birthday attacks – it focuses on finding collisions. we can prevent by using salt. SHA 3 is collision free and safe to use against birthday attacks.

Rainbow table attacks – attacker guess the password and hash the password, then put both into rainbow table. Then compare every hash in the rainbow table . Bcrypt and password based key derivation function 2(PBKDF2) are two commonly used algorithms to salt password. adding pepper to salt can increase security. A pepper is large constant number stored somewhere else.

Sniffer attacks – capturing network traffic to find the credentials.

Spoofing attacks also known as masquerading. pretend to be someone else/something. Email spoofing and **phone spoofing**

Social engineering attacks – shoulder surfing, phishing, spear phishing – specific group or employee; whaling – high level executives; vishing – via VOIP. Over phone system. Smart card attacks

A side channel attack is the passive, noninvasive attack intended to observe the function of the device.

15.Security assessment and testing.

Security testing - it verifies the control. Automated scans, tool assisted pen test

Security assessment -It includes risk assessment, threat analysis, providing non-technical report to management.

NIST 800-53A- assessing security and privacy controls. It has 4 components. 1. Specification documents (Policy, procedures) 2. mechanism (control to meet the specification), 3. Activities (Actions by people Ex: backup,) 4. Individuals are who implement specification, mechanism and activities.

Security audits – must be performed by independent auditors. Reports to board of directors, govt regulators. Internal audit; external audit by EY, PWC and other companies. Third party audits – another organization audits.

SSAE16- Statement on standards for attestation engagements document 16. This is used by auditors for service organizations . it provides 2 different reports.

1. Type 1 – provides description of the control provided by the audited org and auditor opinion based upon that description . this does not include the actual testing of the control by the auditor.
2. Type II- it covers minimum 6-month period and also opinion from the auditor on the effectiveness of the control based upon actual test by the auditor. this report is much more reliable .

Auditing standards
COBIT – conducting audits and assessment ;
ISO 27001- Information security management system
ISO 27002- detail on specific security controls.

Performing vulnerability assessment – security test.

- **SCAP-** security content automation protocol
- CVE- Common vulnerabilities and exposures – naming system for vulnerabilities
- CVSS- common vuln scoring system – to describe severity
- CCE- Common configuration enumeration – naming system for system config issues
- CPE-Common platform enumeration -naming system for OS, application and devices
- XCCDF- extensible configuration checklist description format – provides language for specifying security checklist
- OVAL- open vulnerability and assessment languages- provides language for describing security testing procedures

Vulnerability scans – network discovery scan, network vulnerability scan web application vulnerability scan

TCP SYN SCANNING - also known as half open scanning. Packet is sent with syn flag, if it receives the response, it is moving to next phase in three-way handshake.

TCP connect scanning -it opens full connection.

TCP ACK scanning -send a packet with ACK flag set indicating that it is part of an open connection.

Xmas scanning - send a packet with FIN, PSH and URG flag set.

Nmap- open, closed or filtered (unable to determine) - Open- open port available and application is actively accepting connections. Closed- port is accessible, firewall is allowing the access, but no application accepting connections on port. Filtered Nmap is unable to determine whether a port is open or closed due to firewall interference.

Banner grabbing is used to identify the variant and version of the service running on a system.

Network vulnerability scan- for wireless network- air crack is the tool for VA

Web vulnerability scan- acunetix, open-source scanner- Nikto and wapiti and Burp suite proxy.

Database vulnerability scan- sql-nmap is commonly used tool to scan- open source.

Port – smtp:25, dns:53, pop3:110, ntp:123, Microsoft sql server:1433, oracle:1521,H.323:1720,PPTP:1723

Pentest- Consider using OWASP testing guide, OSSTMM, NIST 800-115, FedRAMP pen test guide

Code review is the foundation of software assessment programs. Most formal code review process known as Fagan inspections has 6 steps. Planning, overview, preparation, inspection, rework and follow up

Static testing - without running. Reviewing source code. Using automated tools to detect flaws.

Dynamic testing – by running it, pentest, VA, sql injection. May include the use of synthetic transactions to verify system performance

Fuzz testing- dynamic testing used by many different types of input. Fuzz testing is useful to test coverage analysis. Two types

Mutation(dumb) fuzzing – takes previous input from actual operation and alter it to create a fuzzed input.

Generational (intelligent) fuzzing – develop data models that create new fuzzed input. The **zzuf tool. slightly changing the input is called bit flipping.**

Interface testing- 3 types, Web 2.0 world combines interfaces**.**

- **API-** standard way of code modules to interact and may be exposed to the outside world through web services.
- **User interface** GUI and command level interfaces.
- **Physical interface** eg machine controllers

Misuse case testing - manual or automated test to test known misuse cases.

Test coverage analysis = number of use case tested/ total number of use cases.

Website monitoring-

Passive monitoring – real user monitoring (RUM).

Synthetic monitoring/active monitoring – performs artificial transactions against a website to assess performance.

Log reviews - SIEM logs are useful during security incidents.

16.Managing security operation

Need to know and least privilege – need to know focuses on permission and ability to access information. least privilege focus on privilege. Need to know commonly associated with clearance. Proper job description is required to know about privileges

Entitlement – it refers to the amount of privileges granted to users. When it is first provisioning an account. Least privileges should be given.

Aggregation – when employee keeps moving from one department to another, they get additional access which would help them to get information.

Transitive trust – relationship between two security domain allows subjects in one domain to access objects in another domain. If the trust is non transitive, they cannot access another domain. A nontransitive enforces the principle of least privilege and grant the trust to a single domain at a time.

Separation of duties.

Separation of privileges – least privilege for different users and service accounts.

Segregation of duties - similar to separation of duties, but it also combines the principle of least privileges. SOX specially requires segregation of duties.

Two-person control- also called two-man rule. Two persons access required to perform an action

Split knowledge – combines separation of duties and split knowledge.

Job rotation (deterrent and deduction mechanism); mandatory vacations (deterrent and deduction mechanism); Privileged account management

Managing information lifecycle –

Creation /capture – when file is created or captured, Classification – classify the data, Storage - store with adequate controls, Usage – any data in use or transit, Archive – archives and backups often stored off site. Protection to be given. Destruction or purging.

Service level agreements -SLA – In addition to SLA, some companies use MOU-memorandum of understanding or ISA- interconnection security agreement. MOU is less formal and doesn't include monetary penalties. if two parties plan to transmit sensitive data, they can use ISA to specify technical requirements of the connection.

Addressing personnel safety and security

Duress – security guard will use duress system to notify to monitoring team about attackers.

Travel – sensitive data should not be there. No free wifi should be used

Emergency management & Security training and awareness.

Managing hardware and software assets –

Hardware inventories – bar code is used. RFID- Radio frequency identification tags are used. RFID is more expensive, but less time to perform inventory search.

Software licensing – configmgr or sccm finds the softwares on the network

Managing virtual assets – SDx- software defined.

Virtual machines (VM's) – vm run as guest OS on physical servers.

Software defined network(sdn)- it decouple control plane from data plane. Control planes uses protocols to decide where to send traffic and data plane decides whether traffic will be forwarded. SDN

Controller handles traffic using simpler network devices that accept instruction from the controller. This eliminates some complexity related traditional networking protocols.

Virtual storage area networks (VASNs)- SAN is a dedicated high-speed network that hosts multiple storage device. But it is complex. VSANs bypass this complexity with virtualization. Primary component in virtualization is a **hypervisor.** Hypervisor manages the VM's, virtual data storage and virtual network components.

Managing cloud-based assets

Software as service (Saas)- provide fully functional applications. Ex: Gmail. Google is responsible for maintenance. consumers don't manage or control.

Platform as service (Pass) – provide computing platform, hardware, OS and applications. Consumers can install applications from the list provided by CSP. Consumers manage their application and some config settings. But CSP is responsible for maintenance of the host and underlying cloud infra.

Infrastructure as service (Iaas) – provide servers, storage, networking resource. Consumer can install OS and application and manage it. CSP maintains the cloud-based infrastructure.

NIST SP 800-145 for cloud computing.

4 cloud models are public, private, community and hybrid.

Managing media lifecycle – reusable media is subject to meantime to failure (MTTF).

Change Management – 1. Request the change 2. review the change 3. approve/reject the change 4. Schedule and implement the change 5. document the change.

Systems to manage – patch management – evaluate patch; test patch, approve, deploy and verify patches are deployed.

IN 2016, malware named "mirai" took control of IOT devices.

MITRE maintains CVE database. It is founded by US government.

17.Preventing and responding to incidents.

The primary goal of incident response is to minimize the impact on the organization. NIST 800- 61 for security incident.

Incident response steps –

Detection- response- mitigation -reporting -recovery -remediation- lessons learned.

Botnet - the computers in botnets are like robots, sometimes called bots or zombies. Multiple bots in a network form a botnet. Bot herder controls the bot in botnet. Bot herders instruct the bots within botnet to launch a wide range of attacks. Computers are joined botnet after being infected with some type of malicious code

Denial of service attacks – it will prevent system from processing or functioning. multiple systems attack a single system. attackers commonly use botnet to launch DDOS attacks.

DRDos- distributed reflective denial of service – it doesn't attack the victim directly, instead manipulates traffic so that attacks are reflected back to the victim from other sources. DNS poisoning and smurf attacks are examples.

SYN FLOOD ATTACK- it is a common Dos attack. It disrupts standard three-way handshake used by TCP. To initiate communication sessions. Syn – syn/ack- ack is the 3-way handshake process. In this attack, attacker never ack. Using SYN cookies is one method of blocking this attack. Another method is to reduce server wait time to block this attack.

Tcp reset attack – spoofing IP address in RST packet to re-establish

Smurf attack – DOS attack. Another type of flood attack using ICMP echo packets. It is a spoofed broadcast ping request using the IP address of the victim as the source IP address. **Ping uses ICMP**

Fraggle attack uses UDP packets over port 7 and 19 and similar to smurf except udp.

Ping flood – sending too many ICMP packets- disabling icmp will resolve this issue.

Ping of death – ping packets normally 32 or 64 bytes. This changes the size of ping packets which will not be handled by system. above 64kb, system can't handle.

Teardrop – system can't put back packets together. Modification done in packets. Keep system up to date will solve this.

Land attacks – spoofed syn packets with same source and destination IP address.

War Dialing – use modem to search system that accepts inbound connection attempts.

Sabotage – employee sabotage is criminal act of destruction committed against an organization.

Espionage – malicious act of gathering confidential information from companies and selling outside.

IDS and IPS - NIST SP 800-94, Knowledge based (signature based); behavioral based (anomaly/statistic)

SIEM Systems - IDS Passive response(notification); active response(block). Host and network-based IDS

Darknet – portion of allocated Ip addresses within a network that are not used.

Preventing measures –

Honeypots – individual computers created as trap for intruders. **Honeynet is** more than one computer as honey nets.

Pseudo flaws -are false vulnerabilities in the honeypot system to tempt attackers.

Padded cells – like honeypot but intrusion isolation by transfer the attacker to padded cells to fake systems/network.

Whitelisting – list of authorized application to run **blacklisting** – list of unauthorized application not to run

Firewalls – ACL ends with implicit deny rule. Second generation firewall add additional filtering capabilities. A**pplication-level** gateway filters traffic based on application. **Circuit level gateway firewalls** filter based on communication circuit. Third generation also called stateful inspection/dynamic packet filtering filter based on its state within stream of traffic. Next generation firewall function as UTM (unified threat management)- combining filter capabilities.

Sandbox- provides security boundary for application and prevents the application from interacting with the application

Penetration testing – NIST SP 800-115

Logging, monitoring and auditing

1. security logs- it logs user's access to a file. Open, modify and delete actions
2. system logs- it stores when system start and stops
3. application access – store for specific applications
4. firewall logs- stores firewall logs
5. proxy logs-
6. change logs

Sampling /data extraction – is the process of extracting specific elements from a large collection of data to construct a meaningful representation of the whole. Statistical sampling uses mathematical functions to extract

Clipping level- **non statistical sampling**. It selects only events that exceed a clipping level. Which is a predefined threshold for the event. It is discretionary sampling.

- Keystroke monitoring- monitoring keyboard. using keylogger.
- Traffic analysis and trend analysis – sometimes called network flow monitoring.
- Egress monitoring – monitoring out going data. DLP (Data loss Prevention) can help in monitoring.
- DLP-Network based and end point based
- Steganography -embedding a message within a file eg image
- watermarking- embed image or pattern in paper that isn't readily perceivable.

auditing to assess effectiveness – user entitlement audit/user access audits

interim report - reports about any observed security weakness in org that demand immediate attention.

18. Disaster recovery planning (DRP)

DRP is a technical complement to the business focused BCP exercise. DRP should also be designed to reduce decision making activities during a disaster as much as possible.

Natural disasters – Earthquake – san-andreas location poses significant risk of earthquake. 82% of the states in US are earthquake possibilities.

FEMA- federate emergency management agency.

flood – flash floods (Excessive water in short time) - according to govt statistics, flooding is responsible for **approximately $8 billion** in damage to business and homes each year in the United States.

FEMA's national flood insurance program is responsible for completing a flood risk assessment for the entire united states and providing this data to citizens in graphical form.

System resilience and fault tolerance - it affects availability. the primary goal of system resilience and fault tolerance is to eliminate **single point of failure (SPOF)**

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

System resilience refers to the ability of a system to maintain an acceptable level of service during an adverse event. It refers to the ability of system to return to a previous sate after an adverse event. For example, if a primary server in a failover cluster fails, fault tolerance ensures that the system fails over to another server. it also implies to get back to the original server once it is repaired.

Protecting hard drives

RAID 0 – This is also called striping – uses two or more disks and improves the performance – doesn't provide fault tolerance.

RAID 1 – This is also called mirroring – uses two disks, both hold the same data. **If one disk fails**, another one continues to operate. it may continue to operate without intervention or manually need to use.

RAID 5- This is called striping with parity – it uses three or more disks with the equivalent of one disk holding parity information**, if one disk fails** it will continue to operate, but it will be slower.

RAID 10 – This is known as RAID 1+0 or stripe of mirrors .it is configured as RAID 1 and RAID 0. Uses at least 4 disks but can support **more. it will continue to operate even if multiple disks fail**

Software RAID require OS to manage and inexpensive. it can reduce overall system performance

Hardware RAID is expensive. More efficient and reliable. it includes spare drives that can be logically added to the array. For ex: RAID5 will have two spare disks. It also supports hot swapping. It doesn't need to shut down the systems to replace failed disks. Cold swappable RAID requires system to be powered down to replace faulty drive.

A failover cluster includes two or more servers and if one of the servers fails, another server in the cluster can take over its load in an automatic process called failover.

Fault tolerance can be added for power sources with UPS. It lasts for 5hr 30 mins. **Quick high voltage** is called **spike,** if it **stays for long time, it is called surge,** quick **reduction in voltage is called sag** and if it stays for long **time, it is called brownout**. if power line has **noise on them called transients**.

Basic UPS provides surge protection and battery backup. Line-interactive UPS include a variable - voltage transformer that can adjust to the overvoltage and undervoltage events without draining battery.

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. Recovery may be automated or require manual intervention. In either case it should be secured. **Fail-secure will block all the access, making sure to secure state (Security). Fail-open will grant all access which is open state - availability. In physical security fail safe term is used for fail-open.**

2 elements – failure preparation. It includes fault tolerance and system resilience; second one is a process of system recovery. The system should be forced to reboot into single user, non-privileged state.

Manual recovery – if a system fails, it doesn't fail in secure state, it requires administrator to manually perform actions to implement secure state

Automated recovery – automated trusted recovery for ex RAID for hard drive, but not for server.

Automated recovery with undue loss – it includes additional protection mechanism to restore corrupted files, rebuild data from transaction logs and verify the integrity of key system and security components.

Function recovery – This is for specific functions. Automatically recover functions. It is either complete the recovery or roll back to the changes to return to a secure state.

Quality of service(qos) it protects the integrity of data networks

1. Bandwidth -the network capacity available to carry communications.
2. Latency – the time it takes a packet to travel from source to destination
3. Jitter – the variation in latency in different packets.
4. Packet loss – some packets may be lost between source and destination, requires retransmission
5. Interference -electrical noise, faulty equipment and other factors may corrupt the content packets.

Recovery strategy

Valuable paper insurance coverage provides protection for inscribed, printed and written documents and manuscripts and other printed business records, it does not cover damage to paper money and printed security certificates.

Business unit and functional priorities. – based on MTTR (Mean time to recovery) and MTO (maximum tolerable outage) – this is the maximum amount of time that the business can withstand the unavailability of a service without experiencing significant disruption.

Alternate processing sites

Cold sites - Equipped with appropriate electrical and environmental support systems. Ex: empty office building; need to install hardware, computers. Least expensive. It takes week time to activate the site completely.

Hot site – most expensive. Exact replication of primary site. Everything is ready. Shared hot site can also be used

Warm site- this is between cold and hot. It takes 12 hours to activate. Equipment's will be there, but back up should be restored and activate the links. Shared warm site is also possible. Make sure to see "no lock out" which guaranteeing the availability even during high demand.

Mobile sites via air, sea, rail. Anywhere in the world. Best for workgroup recovery strategy.

Service bureaus – it is a company that leases computer. can have a contract in place to supply IT support during disaster.

Cloud computing- ex amazon web service, Microsoft azure, they can keep data in cloud, cost effective.

Mutual assistance agreements – it is also called reciprocal agreements. Company mutually agrees to share their space during disaster. Issues are trust is required, vulnerability may be there, confidentiality data will be there.

Database recovery –

Electronic vaulting - database are moved to a remote site using bulk transfer. There may be a delay in transfer to the remote site. Data may be available only till before the disaster occurred. updated data won't be available.

Remote journaling – data are moved on frequent basis, usually every hour. It transfers transaction logs.

Remote mirroring- most advanced database backup solution. Most expensive. Live database is maintained in remote site. It copies the db modifications at the same time they are applied to the production server at primary site. Popular for hot site.

Recovery plan development

Disaster recovery plan document – 1. Executive summary providing high level overview of the plan 2. department specific plans, 3. Technical guides for IT personnel responsible for implementing and maintaining critical backup systems. ,4. Checklist for individuals on the disaster recovery team. 5. Full copies of the plan for critical disaster recovery team members.

Emergency response- Most essentials tasks should be put on the first in the check list.

Personnel communications- the DRP plan should include key members of the DRP team as well as personnel who execute critical disaster recovery tasks. It should have alternate personnel, contact details like mobile number.

3 types of Backups

Full backups – full backup duplicates every file when it is modified. Archive bit is turned off or set to 0.

Incremental backup – it stores only those files that have been modified since the most recent full or incremental back up, those with archive 1 are duplicated then all the files are set to 0

Differential backup – it stores all files that have been modified since most recent full backup. It doesn't change the archive bit. Those with Bit 1 are duplicated.

Full and differential don't take much time to restore than incremental. But it takes time to create it.

Restoring incremental backup in chronological order.

Disk to Disk backup- many backup technologies are designed around the tape paradigm**. Virtual tap library (VTL) support** the use of disks with this model by using software to make disk storage appear as tapes to backup software. Those who adopt disk to disk approach must maintain geographical diversity. Some of the disks have to be located offsite.

Back up best practices

Murphy's law dictates that a server never crashes immediately after a successful backup. It is always crashing before next backup begins. To avoid such issues, we need to have real time continuous back up such as RAID, clustering or server mirroring.

Tape rotation – The grand father-son (GFS) strategy, the tower of Hanoi strategy and the six-cartridge weekly backup strategy. these are very complex. It can be implemented manually or automated software HSM. Hierarchical storage management, it is an automated robotic backup jukebox consisting of 32 or 64 optical or tape backup devices. It is configured as single drive array like RAID.

Software escrow arrangements – it is a tool used to protect a company against the failure of a developer to provide support for its product. Developer provides a copy of source code to the independent third-party organization. When failure to meet SLA, the third-party organization releases the code to the company to fix the issues.

External communication- during disaster, it is not sound to use CEO as spokesperson. Media liaison should be hired and trained.

Utilities – water, electric power- should have contact information of those suppliers.

Recovery vs restoration - A disaster recovery team may be assigned to implement and maintain operations at the recovery site. And salvage team is assigned to restore the primary site to operational capacity.

Recovery- business operations back to working state; restore: business facilities back to work state.

Training, awareness and documentation

1. Orientation training for all new employees
2. Initial training for employees taking on a new disaster recovery role for the first time.
3. Detailed refresher training for disaster recovery team members.
4. Brief awareness refreshers for all other employees.

Testing & Maintenance:

1. **Read-through test(checklist)-** simplest and most critical test. Distributing DRP plan copies to the member of the DRP team for review. It ensures all are aware of their responsibility and knowledge. Opportunity to review plans to see if any modification needed. It helps to identify if any of the DRP member has resigned and need to allocate the roles to someone else.
2. **Structured walk-through –** it is also called as table-top exercise. members gather in a room and role play disaster scenario. the exact scenario is known only to the test moderator who presents the details at the meeting. Team members refer to their copies and discuss appropriate responses to that disaster.
3. **Simulation test –** disaster scenarios are presented to the members to develop plan. This may involve noncritical business activities and some operational personnel.
4. **Parallel test-** the employees are relocated to the site to perform disaster recovery responsibilities. there won't be any interrupt in the primary site.
5. **Full-interruption test -** shutting down primary site and shifting them to recovery site. Extremely difficult to manage.

Maintenance – DRP is a living document. A Disaster recovery planner should refer to the BCP plan as a template for its recovery efforts.

19.Investigations and Ethics.

Investigation types –

Administrative investigations – it is internal investigations that examine either operational issue or violations of org polices. Technical troubleshooting or HR procedures may get involved. Main goal is to resolve the issue. No evidence is collected. Root cause analysis will be performed to identify what was the reason and to prevent similar incidents in future.

Criminal investigations- typically conducted by law enforcement personnel. It must meet the "beyond **a reasonable doubt" standard** of evidence. No other logical conclusions. Strong evidence must be collected.

Civil investigations – involve legal team to prepare evidence to submit in civil court to resolve the dispute between two parties. It uses "weaker **preponderance of the evidence "**standard .

Regulatory investigations- violation of industry regulations. Ex pci dss, HIPPA.

Electronic discovery – it facilitates the processing of electronic information for disclosure. electronic discovery reference model has nine steps. 1 . Information governance ensures that information is well organized for future eDiscovery efforts. 2. Identification locates the information that may be responsive to a discovery request when the org believes that litigation is likely 3. Preservation ensures that discoverable information is protected against alteration and deletion .4. collection gathers responsive information centrally for use ibn the eDiscovery process 5. Processing does the rough cut of collected information and reducing amount of information 6. Review examines what information is responsive to the request and removing any info protected by attorney client privilege. 7. Analysis performs deeper inspection of the content. 8. Production places the information into a format that can be shared with others.9. Presentation displays the info to the court and other parties.

Evidence- NIST 800-86

Admissible evidence – it must be relevant to the fact; it should be material ; it must be competent which means it should have obtained legally .

Types of evidence – 3 types

Real evidence – also known as object evidence. knife, weapon, hard disk from attacker are examples. it can also be conclusive evidence.

Documentary evidence - any written items. it must be authenticated. For ex- logs with administrator to the court. Two additional rules apply here. 1.Best evidence rule which means Original documents should be submitted in the court. 2. Parol evidence rule which means all the terms should be in agreement and no verbal agreements to modify the written agreement.

Testimonial evidence – direct witness in the court. Court won't accept expert in certain field. In that case witness may offer expert opinion-based points. Testimonial evidence must not be hearsay evidence which means what someone else told the witness outside the court.

Chain of evidence – all details must be collected and labeled.

Evidence collection and forensic procedures - It should be done only by forensic technicians. **IOCE- International organization on computer evidence** outlines six principles 1. All the general forensic and procedural principles must be applied .2. upon seizing digital evidence, action taken should not change that evidence .3. when it is necessary for a person to access original evidence, that person should be trained for the purpose. 4. all activities must be documented, preserved and available for review .5. individual is responsible for all actions taken with respect to digital evidence while in their possession. 6. Any agency collecting doing activities with digital evidence is responsible for compliance.

Media analysis a branch of computer forensic analysis involves the identification and extraction of information from storage media. it may include tape, hard disk, CD, DVD, RAM. Technique used are 1. "Recovery of deleted files from unlocated sectors of physical disk.2 Live analysis of storage media connected to a computer .3. static analysis of forensic image of storage media.

Network analysis – IPS /IDS logs, monitoring system, packet capture, logs from firewall during the incident.

Software analysis – application analysis, code review, sql injection logs analysis.

Hardware/embedded device analysis - personal computers, smart phones, tablet.

Investigation process

Gathering evidence – first thing is, the person who has the evidence should voluntary surrender it. second is, ask court to issue a subpoena to order to surrender. There will be a possibility to alter evidence if the time is enough. Last option is search warrant.

Calling in law enforcement – specialized experts will come and do the investigation.

Conducting the investigation – never conduct investigation on compromised system. take a backup and work on it. never attack the attacker. Contact private consultant or law enforcement.

Interviewing individuals – if you suspect the person, it is called interrogation.

Data integrity and retention – make sure the evidence is not altered.

Reporting and documenting investigations –

Computer crime - Military and intelligence attacks, financial attacks, Terrorist attacks, Grudge attacks

Business attacks – the gathering of competitors confidential information, also called corporate espionage or industrial espionage

Thrill attacks -these types of attacks are called script kiddies. They run programs .

ISC2 CODE OF ETHICS – 4 RULES.

1. **1.Protect society and common good,**
2. **Act honorably, honestly**
3. **Provide diligent and competent service to principles.**
4. **advance and protect the profession.**

IAB- Internet advisory board.

20.Software development security.

Software development – security should be considered every step of system development, including software development process.

Programming languages –

Computer understands 0s and 1's which is called machine language. Assembly language is an alternative that used by CPU. Programmers use high level language(c++,vb). Some languages are compiled languages like C, JAVA AND FORTAN. they use compliers to convert high level into exe file.

Python, R, JAVA SCRIPT AND VB SCRIPT are interpreted languages. source code is shared to people to execute it. they can see the source code.

Object oriented languages – from security view, OOP provides black box approach to abstraction.

Message – a communication or input of an object; **Method** – an internal code that defines an action an object performs in response to the message; **Behavior** -output of the message; **Class** – a collection of common methods; **Instance** -object are instances or classes that contains methods; **Inheritance** – from one class to another; **Delegation** -forwarding the request to another object; **Polymorphism** – different behavior. **Cohesion**- describes the strength of the relationship between the purpose of methods within the same class; **Coupling** – level of interaction between objects. Low coupling means less interaction and provides better software design.

Input validation should be done. When the code checks the input whether it falls within range is called limit check. Input validation routine can transform the input to remove risky characters and replace with safe values. Which is called escaping point.

Input validation should be done at server side, not browser side as user can manipulate the input.

Authentication and session management – multifactor authentication and session should expire.

Error handling – detailed error message should be disabled on server and application side. which is also called debugging mode

Logging – applications should send detailed logging of errors to the centralized repository

OWASP has list of things to check; Fail secure and fail open.

System development life cycle

Conceptual definition - purpose of the application and general requirements. High level statements. Should not be longer than two paragraph.

Functional requirements determination – input, behavior and output.

Control specification development - access controls and Security controls discussed here.

Design review – Code review walkthrough – user acceptance testing –maintenance and change management

Life cycle models

Waterfall model – developed by Winston Royce in 1970. iterative model. It has 7 stages. it can go back to previous stage to correct defects; it is called feedback loop characteristic of the waterfall model. First model.

System requirements -software requirements -preliminary design – detailed design – code and debug-testing -operations and maintenance.

Spiral model - developed by barry boehm. This encapsulates another model into it. it is known as meta model or model of models.

Determine objectives, alternatives and constraints – evaluate alternatives -develop and verify next level -plan next phase …. P1, P2, P3. this model helps developers to return to the planning stages to add customer requirements changes as demands.

Agile software development -

Individuals and interaction over process and tools; working software over comprehensive documentation; customer collaboration over contract negotiation; responding to change over following a plan. 12 principles -

It has many variants like scrum, agile unified process(aup), dynamic system development model (DSDM) and extreme programming (XP)

Software capability maturity model (SW-CMM) - stages

- **Initial** - no development process found here
- **Repeatable** – codes are reused, and minimal documents are found here like requirements documentation.
- **Defined** – organization level process documents, peer review
- **Managed** – quantitative process and qualitative process management
- **Optimizing** – continuous improvement, change management

IDEAL MODEL - Five phases

- **Initiating** – appropriate infrastructure put in place
- **Diagnosing** – analyzing the current situation and provide suggestion
- **Establishing** – develops plan to improve
- **Acting** – stop talking and implementing actions, tests
- **Learning**- continues to improve and learnings

Gantt charts – bar chart, between scheduling and projects, tracking tasks.

Pert (program evaluation review technique) – project scheduling tool. Used for improving project management and software,

Change and configuration management –

1. **Request control –** to request modifications
2. **Change control –** changing, testing,

3. **Release control-** once changes are finalized, they must be approved for release. It must go through acceptance testing.

Configuration management

- **Configuration identification** – admin guys document the configuration
- **Configuration control** – changes of config are updated here by authorized people
- **Configuration status accounting** – formalized procedures are used to keep track of all authorized changes
- **Configuration audit** – auditing frequently.

DEVOPS APPROACH

Combination of software development, quality assurance and operations. It is closely aligned with agile model.

Application programming interface (API)

Software testing-

Reasonableness check - it ensures that values returned by software matches specified criteria that are within reasonable bounds.

White box test – analyzing the code line by line

Black box test- from user perspective. They don't have access to internal code. Final acceptance testing is an example of black box test.

Gray box test- combines both tests. Popular for input validation, from user perspective.

Static testing – using automated tools to test without running it. analyze source code.

Dynamic test – in runtime environment. Example web application scanning.

Code repositories

Central place to save source code. GitHub, bitbucket and source forge are some of the code repositories.

In SaaS environments, security responsibility rests with the vendor.

Database management system architecture

Hierarchical and distributed database – hierarchical is in logical tree structure. It may have one to many data model. Distributed model is many to many. data is stored in more than one database.

Relational database

It consists of flat two-dimensional tables made up of rows and columns. One to one mapping. Table is also known as relation. Each table has attributes/fields. The **number of rows in the table is referred to as cardinality. Number of columns is degree**.

Candidate keys- column heading.

Primary key- unique key to refer. Each table has one primary key

Foreign key or referential integrity- used to refer in another table.

Normalization: 1NF, 2NF, 3NF. To be in 2NF, a table must be 1NF compliant; to be in 3NF, must be complaint with 2NF.

DDL- Data definition language – used for creating and modifying database structure, known as schema.

DML- Data manipulation language – allows users to interact with schema.

Database transactions - ACID MODEL

- **Atomicity -** all or nothing. If any part of the transaction fails, it must roll back.
- **Consistency -** all rules must be consistent after every transaction
- **Isolation -** one after another transaction.
- **Durability -** they must be preserved. Backup mechanism, transaction logs.

Security for multilevel database

Mixing data wit**h different classification levels/need to know requirement is known as database contamination.**

Views is the best security for database. Restricting views to the users.

Concurrency (Preventive)– it ensures that database is always correct, and integrity and availability protected. Used for single level or multi-level database. it uses lock and unlock while changes.

1. Lost updates – cannot update when two transactions happen at the same time
2. Dirty reads – if it cannot rollback to previous state when crashes occur.

Other security mechanism

Semantic integrity is common security feature of DBMS. It ensures that user activity doesn't violate any structural rules. It also checks all stored data types are within domain range and logical values exist.

Time and date stamps often appear in distributed database system.

Content dependent access control – it is based on content. Increases process overhead. Another security feature is **cell suppression. Suppression is the concept of hiding individual database fields or cells.**

Context dependent access control – it evaluates big picture to make access control decisions. Key factor is how much each object or packet, or field relates to the overall activity or communication.

Database partitioning is splitting a single database into multiple parts

Polyinstantiation occurs when two or more rows in the same relational database table appear to have identical primary key elements but contain different data. It is often used as defense against inference attack.

When false info inserted into table is called noise or perturbation.

Open database connectivity – ODBC Connection between database and application. NOSQL databases are a class of database that use models other the relational model to store data. 3 major classes of NOSQL.

1. **Key/value stores**- they store information in key/value pairs. Key is an index used to uniquely identify a record. Useful for high-speed applications.
2. **Graph database** – it stores data in graph format using **nodes to represent objects and edges to represent relationships. Useful for social network, geographic locations.**
3. **Document stores** are similar to key values. But here XML AND JAVESCRIPT OBJECT NOTATION(JSON) Used here.

Storing data and information.

Types of storage –

Primary memory is directly available to a system's CPU. It is called random access memory (RAM). It is volatile. It is usually the most high-performance storage resource.

Secondary storage -Nonvolatile – CD/DVD, USB, Hard disk, tape drives.

Virtual memory allows a system to simulate additional primary memory resources through use of secondary storage.

Virtual storage allows system to simulate secondary storage resources through use of primary storage. No recovery ability.

Sequential access storage – magnetic tape is the example of sequential access storage. searching from beginning to locate specific address.

Volatile storage loses its content once powered off. RAM is the example.

Nonvolatile storage doesn't lose content. Magnetic media and non-volatile RAM(NVRAM) are examples.

Covert channel attacks pose the threat against storage resources.

Understanding knowledge-based systems

2 types – expert systems and neural networks.

Expert system

It has 2 components. Knowledge base and inference engine. **Knowledge system** based on rules known by the system. **Inference engine** gets input from user and do fuzzy technique to arrive the conclusion. They don't judge by emotion.

Machine learning – 2 categories

Supervised learning -it uses labeled data for training .it uses dataset. **Unsupervised learning** -it uses unlabeled data for training. Dataset provided to the algorithm does not contain correct data.

Neural networks- Commonly referred to as deep learning or cognitive system. biological reasoning process. The algorithm works backwards from decisions to determine the proper weights for each node in the chain. This is known as delta rule or learning rule.

21.Malicious code and application attacks.

Virus – earliest form of malicious code .it spreads from one system to another. it has two function. Propagation and destruction.

Virus propagation techniques

Master boot record viruses (MBR) – earliest virus.it attacks the portion of bootable media (CD/DVD/USB/HARD DISK). Mbr is extremely small (512 bytes). It stores majority of the code in another location. When the system reads infected MBR, it executes the code stored in alternative location.

File infector virus – files end with .exe or .com in windows. It may slightly alter the code of the file or replace the entire file. a variation of the file infector virus is the companion virus. it will have the same name as original. For ex: if you have game.exe and when you type game in command prompt, it will execute game.com. to avoid this always type full file name instead of shortcuts.

Macro virus – using VBA script.

Service injection virus – injects themselves into runtime process. winlogin.exe. to prevent this, have to update current security patches.

Antivirus mechanism – signature based detection.

Virus technologies

Multipartite virus – it uses more than one propagation technique in attempt to penetrate the system.
stealth virus – they hide themselves by actually tampering with the OS to fool antivirus.
Polymorphic virus – it modifies their own code as it travels from system to system.
Encrypted virus -it uses cryptographic techniques. **It uses a short segment of code known as virus decryption routine.**

Hoaxes – information through social media circulating.

Logic bombs -it is launched by time or program. It resides in the system, most of the logic bombs are coded into an application.

Trojan horses – downloading application from internet will infect the computer. Ransomware is one of the types. Most famous one is crypto locker.

Botnets – collection of system is called botnet.

Worms – they propagate themselves without human intervention. **Code red worm –** it randomly chose IP address to see vulnerability on those machines to exploit it.

Stuxnet - searching for unprotected administrative shares of systems on the local network. exploiting zero-day vuln. Connecting to system using default database password. spreading by shared infected USB.

Spyware -spyware waits for us to enter username and password and transfer the information the remote system which created this spyware.

Adware shows up ad on the screen, when it is clicked, it infects or observing web search and taking it to the competitor websites.

Zero day attacks - no remediation.

Password guessing attacks; dictionary attacks, social engineering attacks

Spear phishing targets at an individual; **whaling** attacks high position targets like vice president; **vishing** uses telephone communication. **Dumpster driving**- searches info through dustbin.

Application attacks

Buffer overflow- it happens when the user input is not properly validated. Parameter checking is important. It modifies system memory

Time of check to time of use – checks access too far before resource requests.

Backdoors – developers use backdoors during development and leaves it .

Escalation of privilege and rootkits -they again access to system and increase access level from normal to admin access using rootkits.

Web application security –

Cross site scripting (XSS) – injecting scripts in input box. To prevent input validation must be performed

Cross site request forgery – XSRF or CSRF attacks. it will redirect to sub links. To avoid this secure token should be used or it can navigate only from main webpage.

SQL injection - attacking database

Dynamic web applications - web pages are created dynamically using database query.

Protecting against sql injection – 1. Use prepared statements – stored procedures to store sql statements. 2. **Perform input validation –** whitelist validation; 3. **Limit account privileges to the web application to the database.**

Reconnaissance attacks –

IP Probes also called IP Sweep or ping sweep. Nmap is used for this. disable ping service to avoid this.

Port scans -next step is after IP probe is to do port scan on the active system. using port scanner, they get ports details. Unnecessary ports should be disabled to prevent.

Vulnerability scans

Masquerading attacks- impersonate someone who does have access permission. Two attacks are IP spoofing and hijacking.

IP spoofing – to avoid this. packets with internal IP don't enter from the outside. Packets with external IP don't exit the network from inside. packets with private IP don't pass through the router in either direction.

Session hijacking – capturing credential between client and server. using cookies data which is not closed properly. Anti -replay authentication and expiring cookies will resolve this issue.