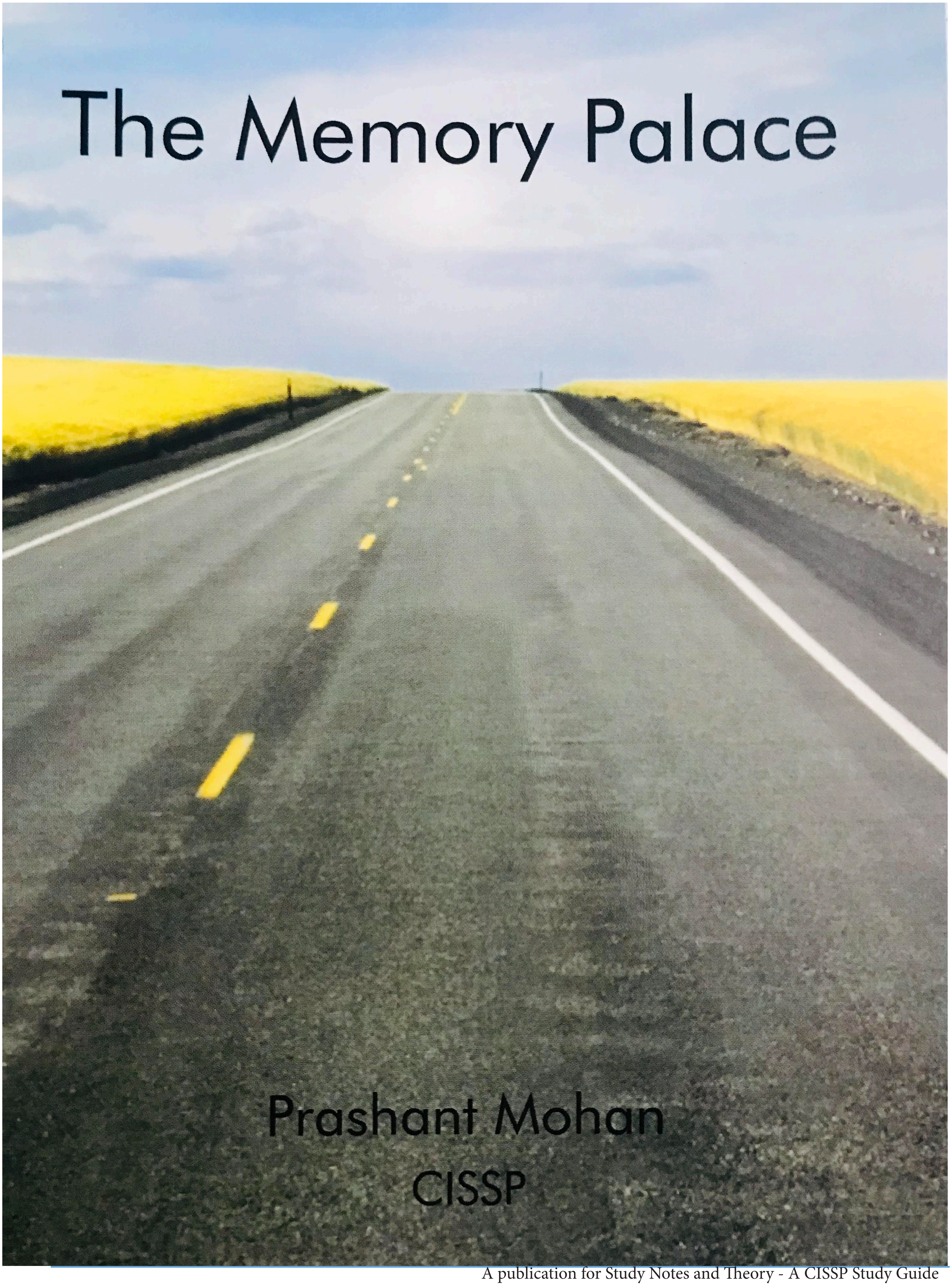


The Memory Palace

Prashant Mohan

CISSP

A publication for Study Notes and Theory - A CISSP Study Guide

A publication for *Study Notes and Theory - A CISSP Study Guide*

★ ★ ★ ★ ★

The Memory Palace - A Quick Refresher For Your CISSP Exam!

Fourth Edition

Written by Prashant Mohan, CISSP, CCSP

★ ★ ★ ★ ★

TABLE OF CONTENTS

Exam Breakdown

Domain	Percentage of exam
Domain 1: Security and Risk Management	15%
Domain 2: Asset Security	10%
Domain 3: Security Architecture and Engineering	13%
Domain 4: Communication and Network Security	13%
Domain 5: Identity and Access Management (IAM)	13%
Domain 6: Security Assessment and Testing	12%
Domain 7: Security Operations	13%
Domain 8: Software Development Security	11%
Total	100%

CISSP Exam Mindset

- Your role is a risk advisor, CISO, or Senior Management.
- Do NOT fix problems.
- Fix the process, not the problem.
- Who is responsible for security?
- How much security is enough?
- All decisions start with risk management. Risk Management starts with identifying/valuating your assets.
- Human life is always #1 priority.
- Security should be “baked in”, rather than “bolted on”.
- Layered defense!
- People are your weakest link.
- Always think about the overall risk and remediation steps for each technology, tools, components or solution.
- Think security? Think about CIA.
- Behave ethically.
- All controls must be cost justified (safeguards)
- Senior management must drive the security program (business proposal, positive ROI).

Preparing for Exam Day

- Refrain from studying too much 24 hours before exam day. It is good to have a clean head so that you can focus more on the day of the exam.
- Sleep early the day before exam and it’s advised to take at least 8 hours of good sleep. The exam needs you to be alert and focused.
- On the day of exam, have a good breakfast and reach your exam center at least 30 mins before the scheduled time. Please make sure you’re carrying all the necessary documents before leaving for exam center.
- Do read the NDA and agree within 5 minutes, as failing to do so will forfeit your exam and fees without a refund or appeal.
- Read the question, re-read the question and then read the given options. Please make sure you are totally convinced before submitting the response. The best way to prepare for this type of mindset is to do as many practice questions as possible. Understand why the choice is correct, and why the other choices are incorrect.
- Take breaks. It can’t be emphasized enough the significance of taking breaks during the exam. Make sure you re-channelize yourself and then come back.
- In the end, relax. Trust your preparation. If you’ve prepared well, it's all gonna end well! :)

Note From The Author

I would like to thank Radha Arora, CISSP for drafting and reviewing the document with me to make it a better version. I would also like to thank Luke Ahmed for allowing me to release the document on his CISSP platform and for assisting me in compiling it to produce a distributable format.

The Memory Palace

"It's a memory technique. A sort of mental map. You plot a map with a location. It doesn't have to be a real place. And then you deposit memories there. That, theoretically, you can never forget anything. All you have to do is find your way back to it." - *Sherlock*, BBC TV Series

Disclaimer

- This document is completely free for anyone preparing for their CISSP exam. It is not meant for sale or as part of a course. It is purely a contribution to align with the Fourth Canon of the ISC² Code of Ethics to "*Advance and Protect the Profession*".

- This book has been written with an objective to have all the CISSP concepts handy at one place. It is an original creation of the author. However, a few terms, concepts, tips, images, language(s) are a result of inspiration and derived from multiple sources (books, videos, notes). The intent is not to violate any copyright law(s). If the reader comes across any text, paragraph(s), image(s) which are violating any copyright, please contact the author at prashantmohan.cissp[at]gmail[dot]com so that this can be removed from the book.

- The content is completely on the guidelines of ISC² and I've tried my best effort to make them as simple as possible for others to understand. This document is not affiliated with or endorsed by ISC².

- The document is by no means a primary resource for the CISSP exam. Readers are expected to go through their primary materials first and then use this document as a quick reference.

Domain 1: Security and Risk Management

Confidentiality - Sharing of the information with the intended people. Data should be protected in all the states (At rest, in Process, in motion)

***Exam Tip**: To maintain confidentiality, you should always encrypt data. {In Motion - TLS} {At rest - AES - 256}

Examples of confidentiality requirements

- PII/PHI must be protected against disclosure using approved algorithms.
- Password and sensitive field should be masked.
- Password at rest must not be stored in clear text.
- TLS must be used for transmitting sensitive information.
- The use of unsecured transmission (e.g. FTP etc.) should not be allowed.
- Log files should not store sensitive information.

Integrity - Protection against system or software modification: System should perform as expected.

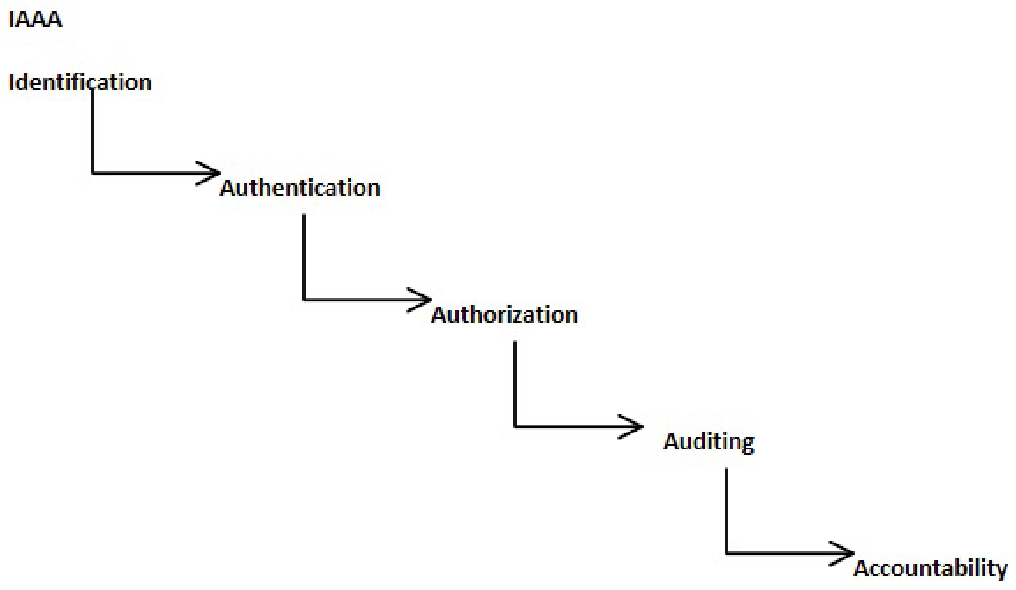
- Code injection can modify the database
- Input validation is a mitigation technique
- Data Integrity: Ensuring the accuracy and reliability of data
- CRCs, checksums, Message Digests, Hashes, MACs
- Internal and External consistency
- Some examples of Integrity Requirements:
- Input Validation should be used in all forms to ensure the data control language is not entered, and field size and data types are enforced.
- Published software should provide the user with a message digest so the user can validate the accuracy and completeness of the software.
- Subjects should be prevented from modifying data unless explicitly allowed.

Availability - Data should be available all the time whenever it’s required.

- Metrics Used:
    - MTD/RTO/RPO

Domain 1: Security and Risk Management

  - SLAs
  - MTBF/MTTR
- Examples of Availability requirements:
  - Software shall meet availability requirements of 99.999%, as specified in the SLA
  - Software should support access up to 200 users simultaneously
  - Software must support replication and provide load balancing
  - Mission critical function of the software should be restored to normal operations within 30 minutes



Identification: User should be uniquely Identified

Authentication: Validation of an entity's identity claim

Authorization: Confirms that an authenticated entity has the privileges and permissions necessary.

Auditing: Any activity in the application/system should be audited (Identify technical issues/ Breaches)

Accountability: Tracing an action to a subject

Domain 1: Security and Risk Management

Plans

Strategic - Longer (5 years)

Tactical - Mid/Short (6 months to 1 year)

Operational - Shortest (Days to weeks)

Primary goal of change management is to prevent security compromises.

Protection Mechanism:

1. Layering - Defense in depth (Series & Parallel)
2. Abstraction - Used for classifying data or assigning roles
3. Data Hiding
4. Encryption

Data Classification

Government	Private
Top Secret (Classified)	Confidential
Secret (Classified)	Private
Confidential (Classified)	Sensitive
Unclassified	Public

Top Secret---> Grave Damage

Secret--->Critical Damage

Confidential---> Serious Damage

Unclassified---> No damage

Domain 1: Security and Risk Management

Security Roles & Responsibilities

1. Senior Manager - Management (Ultimately responsible)
2. Security Professional - Information Security team
3. Data Owner - Classifies the data
4. Data Custodian - Takes care of day to day activity (performing backups)
5. User - End user
6. Auditor - Responsible for reviewing the data

   Control Frameworks

COBIT/COSO - Framework and Goals (What do we need to do?)
ITIL - How do we achieve those goals

Due Care - Doing the right thing / Prudent Man
Due Diligence - Practicing activities to maintain due care
Security Policy - Mandatory Document that defines the scope of security needed by the organization
Standards - Mandatory requirements
Baseline - Minimum security requirement
Guidelines - Optional. How Standards and Baselines should be implemented
Procedure - Step by step document. Maintain integrity of the business

Threat Modelling

It’s a security process where potential threats are identified, categorized and analyzed.

Proactive Measure: Design and development
Reactive Measure: Once the product has been deployed

Goal: (a) To reduce the number of security related design and coding defects
(b) To reduce the severity of any remaining defects

Overall result is reduced risk

Domain 1: Security and Risk Management

Identifying Threats:

1. Focused on Assets - Identify threats on valuable assets
2. Focused on attackers - Identify potential attackers and their goals
3. Focused on Software - Potential threat against developed software

STRIDE Model - Developed by Microsoft (purpose is to consider range of compromise concerns)

S - Spoofing
T - Tampering
R - Repudiation
I - Information Disclosure
D - Denial of Service
E - Escalation of privilege

DREAD Model - Designed to provide a flexible rating solution that is based on the answers of 5 main questions:

D - Damage potential (How severe the damage likely to be if the threat is realized)
R - Reproducibility (How complicated it is for the attacker to reproduce the exploit)
E - Exploitability (How hard it is to perform the attack)
A - Affected users (How many users are likely to be affected)
D - Discoverability (How hard it is for an attacker to discover the weakness)

Process for Attack Simulation and Threat Analysis (PASTA)

Stage I: Definition of the Objectives (DO) for the Analysis of Risks
Stage II: Definition of the Technical Scope (DTS)
Stage III: Application Decomposition and Analysis (ADA)
Stage IV: Threat Analysis (TA)
Stage V: Weakness and Vulnerability Analysis (WVA)
Stage VI: Attack Modeling & Simulation (AMS)
Stage VII: Risk Analysis & Management (RAM)

Domain 1: Security and Risk Management

Risk Management for Supply Chain

A supply chain is the concept that most computers, devices, networks, and systems are not built by a single entity.
Onsite Assessment
Document Exchange and Review
Process/Policy Review
Third Party Audit

<space reserved for future edits, corrections, or additions)

RISK Terminology

Asset Valuation - Value of an asset
Risk: Likelihood that a threat will exploit a vulnerability in an asset.
Threat: Has the potential to harm an asset.
Vulnerability: A weakness; a lack of safeguard
Exploit: Instance of compromise
Controls: Protective mechanisms to secure vulnerabilities

- Safeguards: Proactive
- Countermeasure: Reactive mechanism

Domain 1: Security and Risk Management

Total Risk: Amount of risk before the safeguard is implemented.

Secondary Risk: Risk event that comes as a result of another risk response.

Residual Risk: The amount of risk left over after a risk response.

Fallback Plan: “Plan B”

Workaround: Unplanned response (for unidentified risk or when other response does not work).

Risk Management

- Risk Assessment: Identify Assets, Threats, Vulnerabilities
  - Quantitative - $$
  - Qualitative - Experience (Delphi technique)
- Risk Analysis: Value of potential Risks (ALE, SLE)
- Risk Mitigation: Responding to Risk
- Risk Monitoring: Risk is FOREVER

SLE = AV*EF
ARO = Annual rate of occurrence
ALE = SLE * ARO

Cost Benefit Analysis (CBA) : ALE Before safeguard - ALE after implementing safeguard - annual cost of safeguard = Value of the safeguard to company

Risk Treatment: MAAT
M - Mitigate
A - Accept
A - Avoid
T - Transfer

*Exam tip: Primary goal of risk management is to reduce the risk to an acceptable level

Domain 1: Security and Risk Management

Controls

- Technical, Administrative, Physical
- Deterrent - Dogs
- Preventive - SoD (Protects against collusion)
- Detective - Job rotation (detects fraud)
- Compensating - Alternate control
- Corrective - Back up
- Recovery - Restore backups
- Directive - Security policy

- Personal Security policies and Procedures
- Separation of Duties: Preventive control (protects against collusion)
- Job Responsibilities: Access granted based on Least Privilege
- Job Rotation: Detective Control (Protects against Fraud)
- Candidate hiring and screening: Background check important
- Employment agreement and policies: Signing NDA and NCA
- On-boarding and termination process: IAM and UER
- Vendor, Consultant and Contractor Agreements and Controls: Contracts and SLA
- Compliance Policy Requirements: adhering to requirements (PCI-DSS)
- Privacy Policy requirement: Cannot monitor without consent

Documentation Review: Process of reading the exchanged material and verifying them against the standards and expectation

Domain 1: Security and Risk Management

Risk Management Framework

C - Categorize Information

S - Select security control

I - Implement security control

A - Assess the security control

A - Authorize Information system

M - Monitor security control

Awareness, Training & Education

- A prerequisite to security training is awareness. The goal of creating awareness is to bring security to the forefront and make it a recognized entity for users.
- Training is teaching employees to perform their work tasks and to comply with the security policy. Training is typically hosted by an organization and is targeted to groups of employees with similar job functions.
- Education is a more detailed endeavor in which students/users learn much more than they actually need to know to perform their work tasks. (obtaining CISSP certification for promotion or better job)

Business Continuity Management (BCM)

Business Continuity Planning

- Business Organization Analysis
- BCP Team
- Validate BOA

Domain 1: Security and Risk Management

- BIA
- Continuity Planning
- Approval and implementation
- Maintenance

Disaster Recovery

- Critical Systems
- MTD, RTO, RPO
- Offsite selection
- Recovery of critical systems
- Normal systems
- Get back to primary site

1. Process & Planning
   a. Business Organization Analysis
   b. BCP Team selection
   c. Validates BOA
   d. Resource requirement
   e. Legal and regulatory requirement

2. Business Impact Analysis
   a. Identify Assets and value
   b. Risk Identification (Threats)
   c. Likelihood estimation (ARO)
   d. Impact Assessment (Exposure Factor)
   e. Resource Prioritization (Analysis)

3. Continuity Planning
   a. Strategy planning - bridges gap between BIA and Continuity planning
   b. Provision and process - people, buildings & infrastructure (Meat of BCP)
   c. Plan Approval - (Senior Management support and approval : Very Important)
   d. Plan implementation
   e. Training and Education

Domain 1: Security and Risk Management

4. BCP Documentation
   a. Continuity plan goals
   b. Statement of importance
   c. Statement of priorities
   d. Statement of organization responsibility
   e. Statement of urgency and timing
   f. Risk assessment
   g. Risk acceptance/mitigation

*Exam tip: Human safety is your first priority. Data is second

Laws

Categories of Law

1. Criminal law: Law enforcement is involved (Murder)
2. Civil Law: Designed to provide an orderly society & govern matters which are not criminal. {United states code} (Law suite, defamation cases)
3. Administrative Law: Covers topics as procedures to be used within federal agency.

4. Comprehensive Crime Control Act (1984) - 1st Law against computer crime
   a. Unauthorized access of classified information
   b. Cause malicious damage to federal system excess $1000
   c. Modify medical resources

5. Computer Fraud and Abuse Act (1986): Amendment in CCCA. Creation of malicious code was introduced (1994)
6. Computer Security Act (1987): Amendment in CFAA
   a. NIST has been given responsibility to develop guidelines
   b. Mandatory periodic training
   c. Classified information to be dealt by NSA
   d. Unclassified information to be dealt by NIST

Domain 1: Security and Risk Management

7. Paperwork Reduction Act (1995): Office of Management Budget (OMB) - Approval before requesting information from public.
8. Government Information Security Reform Act (2000): Places burden of maintaining the security & Integrity of Government information.
9. Federal Information Security Management Act (2002): NIST develops FISMA implementation. It requires federal agencies implement an information security program that covers the agency's operations.

Intellectual Properties

1. Copyright: Original creation of author. Covers the expression of idea. It's covered till 70 years after the death.
    a. Digital Millennium Copyright Act (DMCA)
        i. Prohibition of attempts to break copyright.
        ii. Protection to ISP if internet is used as crime.
2. Trademarks: logos, way of packing. Granted for 10 years and then renewed for 10 years.
3. Patents: Protects the rights of inventor. 20 years from the date patent is applied.
4. Trade secret: If disclosed, business may be impacted. KFC, Coca cola recipe. No protection (By Law). Only way to protect is proper security control.
5. Licensing: Contractual - written by software vendors.
   Shrink wrap - written outside software packaging.
   Click through - During installation agreement of terms and conditions.
   Cloud - License agreement is displayed on the screen

Uniform Computer Information Transaction Act - Law against the breach of licensing.

Safe Harbor - Doing business outside EU.

Wassenar Agreement - Import/Export of encrypted goods.

Domain 1: Security and Risk Management

Privacy

US Privacy Law: 4th Amendment ---> Searching private property without search warrant
Agencies should only retain records which are used and destroy others.

a. Electronic Communication Privacy Act (1986): Invading electronic privacy is a crime.
b. Communication Assistance for Law Enforcement (1994): Wiretapping with proper orders is allowed.
c. Economic and Protection of Proprietary Information Act (1996): Theft of economic infor mation would be called as espionage.
d. Health Insurance Portability and Accountability Act (1996): Protection of PHI
e. Health Information Technology for economic and Clinical Health (2009): Business Assoc. (BA) and covered Entity should have agreement through Business Associate Agreement (BAA). It protects BA (Who handles PHI on behalf of HIPAA).
f. Children's online privacy protection act (2000): Protects information collection for children (under 13 years)
g. Graham-Leach-Bailey's Act (1999): Law for financial institutes, Banks
h. US Patriot Act (2001): Blanket approval for surveillance. Terrorist activity. Came after 9/11
i. Family Educational Rights and Privacy Act: Educational institutes receiving funding from government.
j. Identity Theft Act (1998)

European Union Privacy Law

Law giving directive outlining privacy measures that must be in place for protecting personal data processed by information system.

Criteria to be met:

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

Domain 1: Security and Risk Management

Key rights of individual about whom the data is held:

1. Right to access the data
2. Right to know the data's source
3. Right to correct the inaccurate data
4. Right to withhold consent to process in some situations
5. Right of legal action should these rights be violated.

European Union Global Data Protection Regulation - GDPR

Law applies to all organizations that collect data from EU residents or process that information on behalf of someone who collects it.

a. Breaches should be informed within 72 hours
b. Centralized data protection authorities
c. Individuals will have access to their own data
d. Data portability to facilitate the transfer of personal information between service providers.
e. Right to be forgotten - delete information if it's no longer required.

Task of Data protection officer

1. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions.

2. To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or proces-sor in relation to the protection of personal data, including the assignment of re-sponsibilities, awareness-raising and training of staff involved in processing oper-ations, and the related audits.

Domain 1: Security and Risk Management

3. To provide advice where requested as regards the data protection impact assessment and monitor its performance and cooperate with supervisory author-ity

4. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation and to consult, where appropriate, with regard to any other matter.

Contracting & Procurement: Any services or applications being on-boarded by an organization, should be reviewed properly before signing off the contract. Should ask appropriate questions before on-boarding the vendor:

a. What controls are in place to protect organization's information
b. What type of sensitive information is stored, processed, or transmitted by the vendor?
c. What type of security audits does the vendor perform, and what access does the client have to those audits?

Domain 2: Asset Security

Identify and Classify Assets

1. Define Sensitive Data
2. Defining Data and Asset classification
3. Determine data security controls
4. Understand Data states
5. Handling Information and Assets
6. Data Protection Methods

Define Sensitive Data

1. Personally Identifiable Information
2. Protected Health Information
3. Proprietary Data

Managing Sensitive Data

1. Marking - Labelling (protection mechanisms are assigned on the basis of data labels)
2. Handling sensitive data - secure transportation of data through entire lifecycle
3. Storing sensitive data - proper encryption (AES256)
4. Destroying Sensitive Data when no longer required.

Data Remanence: Left over data after deletion process is completed. (as magnetic flux)

Degaussing: Way to remove data remanence. Generates heavy magnetic field. (Only effective on magnetic media)
Note: it does not affect CD, DVD or SSD
Solid state drive (SSD): Uses integrated circuitry instead of magnetic flux.

Understanding Data States

1. Data in Motion
a. Protect using TLS 1.2, VPN etc.
2. Data at Rest
a. Protect using AES 256, masking, tokenization etc.
3. Data in Use
a. Isolation of memory location where sensitive data is being processed.

Domain 2: Asset Security

Methods of removing data.

a. Erasing: Simple deletion of file. Data can be overwritten and removed

b. Clearing (overwriting): Unclassified data is overwritten. Overwritten data can be retrieved in labs using some tools.

c. Purging: Intense form of clearing. Prepares a media to be reused in less sensitive environment. Data non-recoverable using known methods. High classified data is not purged (e.g. Top Secret)

d. Declassification: Process of using a media in an unclassified environment.

e. Sanitization: Combination of processes to remove data ensuring data cannot be recovered at any cost. (Destruction of media without physically destroying it) {factory reset, cryptoshredding}

f. Destruction: Final stage in the lifecycle of media. Most secure method of sanitization. Methods includes, incineration, crushing, shredding, disintegration and dissolving using chemicals.

Retaining Assets: Should be retained as per the business requirement and local laws and regulations. e.g. emails above 90 days should be deleted.

Identifying Data Roles:

1. Data Owners: Ultimately responsible for the data.
2. System Owners: Person who owns the system which processes the sensitive data.
3. Business Owners: Sales dept. head will be responsible for sales dept. However, systems being used in sales dept. will be owned by IT dept.
4. Data Custodian: Take efforts to protect the data, backup. (does task directed by owner)
5. Data processors: Person who processes personal data on behalf of data controller
6. Data Controller: Person who controls processing of data.
   *Company collecting employee information for Payroll - Data Controller
   *Company passing it to third-party for processing - Data Processor

California Online Privacy Protection Act (COPPA): Any website collecting PII, needs to protect the privacy.

Rules of behavior: Rules identified for the protection of data. It applies to the users not the system.

Domain 2: Asset Security

Pseudonymization: Pseudonymization refers to the process of using pseudonyms to represent other data. It can be done to prevent the data from directly identifying an entity, such as a person. (e.g. Agent 007 for James Bond)

Anonymization: Anonymization is the process of removing all relevant data so that it is impossible to identify the original subject or person.

Data Masking: Data masking is a method of creating a structurally similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training.

Security Baselines: Minimum set of security requirements that is needed for an organization to protect its assets.
Not all security controls would be relevant to us.

- Scoping: Scoping refers to reviewing a list of baseline security controls and se lecting only those controls that apply to the IT system you’re trying to protect. E.g. if a system doesn’t allow any two people to log on to it at the same time, there’s no need to apply a concurrent session control.
- Tailoring: Tailoring refers to modifying the list of security controls within a base line so that they align with the mission of the organization. E.g. Controls are needed for main office but not on remote locations so remote locations could have compensating controls.

Summary of Data classification process:

- Criteria are set for classifying data
- Data Owners are established for each type of data.
- Data is classified.
- Required controls are selected for each classification.
- Baseline security standards are selected for the organization.
- Controls are scoped and tailored.
- Controls are applied and enforced.
- Access is granted and managed.

Domain 3: Security Engineering

Cryptography

Encryption: Plain text + Algorithm + key = Cipher text

Caesar Cipher: Earlier Cipher a.k.a ROT3 (Substitution Cipher)

A --> D

B --> E

C --> F

ROT 12 A --> M

B --> N

Vulnerable to Frequency Analysis

Enigma Codes : German (Watch "The Imitation Game" movie)

Purple Machine: Japan

Goals of Cryptography: **P** - Privacy (Confidentiality)

A - Authentication

I - Integrity

N - Non-Repudiation

Key is also called crypto variables

Key Space: Range of values that are valid for use as a Key.

Key space = 2n where n us the bit size

e.g. AES 256 has the key space of 2^256

Kerckhoff Principle: Algorithm should be made public for examination and to test them.

Symmetric Key (aka Private Key/Secret Key)

Asymmetric Key (aka Public Key/Shared Key)

Domain 3: Security Engineering

Cryptography --> Art of converting plain text to cipher text

Cryptanalysis --> Art of breaking the cipher

Cryptology --> Science of Cryptography and Cryptanalysis

Cryptosystem --> Implementation of code/cipher in Hardware or Software

Cryptography Mathematics:

1. AND - X ^ Y (Both True then True)

X	Y	X ^ Y
0	0	0
0	1	0
1	0	0
1	1	1

2. OR - X V Y (Any one value True then True)

X	Y	X V Y
0	0	0
0	1	1
1	0	1
1	1	1

3. NOT - X ~ Y (Reverse the Input)

X	~X
0	1
1	0

4. Exclusive OR - X + Y (Only True if only ONE value is TRUE)

X	Y	X + Y
0	0	0
0	1	1
1	0	1
1	1	0

Domain 3: Security Engineering

Modulo Function: Remainder after the division

8 mod 6 = 2
6 mod 8 = 6
10 mod 2 = 0

One way function: The output cannot be reversed

Nonce: Random number to provide randomness to cryptographic function. Nonce must be unique number each time. {Initialization Vector (IV)}

Zero Knowledge proof: Sharing of proof without sharing actual knowledge.

Split Knowledge: Separation of Duties and Dual Control

M of N control
M: Minimum number of people for task
N: Total number of people for task

Work Function: Time and effort required to break a cryptography (it also tells the strength of cryptography)

Code: Secret Codes {Words, Phrases}
Cipher: Converts plain text to cipher text

Transposition Cipher: Rearranging the letters of plain text

Substitution Cipher: Replace each character or bit with different character. e.g. Vigenere Cipher (Polyalphabetic Cipher)

Domain 3: Security Engineering

One Time Pads: Type of substitution cipher (aka Vernam Ciphers)

*Exam tip: When used properly, they are unbreakable

- One Time Pads must be randomly generated
- One Time Pads must be physically protected
- Each One Time Pad must be used only once
- Key length should be equal to length of the message

Running Key Ciphers: AKA Book Ciphers where Encryption key is equal to the length of the message. (Key is chosen from a common book or newspaper)

Block Cipher: Encrypts in huge block (Slow but secure)
Stream Cipher: Encrypts bit wise (Fast but not that secure)

Confusion: Complication in Substitution cipher
Diffusion: One change in plain text, change the cipher text in multiple ways.

Modern Cryptography

Cryptographic Keys: Keys are kept secret. Algorithms are made public to test them (Kerckhoff Principle)

*Exam tip: Key length directly relates to work function of cryptosystem

Symmetric Key: (Secret Key/Private Key) **P ~~A I N~~**
Same key is used to encrypt and decrypt the message.

- Key distribution is a challenge (Out of band)
- n(n-1)/2 = total number of keys required.
- Non scalable but great speed

Domain 3: Security Engineering

Asymmetric Key: (Public Key) **PAIN**

One key is used to encrypt and another key is used to decrypt

- Every user has a key pair (Public + Private)
- 2n = total number of keys required
- Scalable but very slow

Real World example: SSL/TLS uses Hybrid Cryptography. Encrypt message with symmetric key and encrypt the key using asymmetric key.

Symmetric Key	**Asymmetric Key**
Single shared key	Have key pairs
Out of band exchange	In band exchange
Not scalable	Scalable
Fast	Slow
Bulk Encryption	Small blocks, digital signature, Certificated, envelops
P~~AIN~~	**PAIN**

Hashing: Message Digest (Provides Integrity)

One way math

File changes --> Hash changes

Requirement for Hash

a. The input can be of any length

b. The output has a fixed length.

c. The hash function is relatively easy to compute for any input.

d. The hash function is one-way (meaning that it is extremely hard to determine the input when provided with the output).

e. The hash function is collision free (meaning that it is extremely hard to find two mes sages that produce the same hash value).

Domain 3: Security Engineering

Hash Algorithms:

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

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

Symmetric Key Algorithms: **P ~~A I N~~**

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

1. **DES (Data Encryption Standard)**:

    Block Size: 64 bits

    Key Size: 56 bits

    Rounds: 16

    a. Electronic Code Book (ECB): Least secure as it uses Secret key (static) Used for shortest transmission (data units are encrypted). No IV

    b. Cipher Block Chaining (CBC): It uses Block Cipher. Uses IV and it has chaining. As it uses chaining, it propagates errors during encryption process. Cipher Text is XORed with Plain Text of next block.

Domain 3: Security Engineering

c. Cipher Feedback Mode (CFB): It is a Stream Cipher. Uses IV and it has chaining. It propagates errors during the encryption process. (streaming cipher version of CBC)

d. Output Feedback (OFB): It is a Stream Cipher. No chaining hence it does not propagate errors.

e. Counter Mode (CTR): It is a Stream Cipher and helps in parallel computing. No chaining.

*Tip: To understand, OFB and CTR has no chaining hence it does not propagate errors.

2. Triple DES (3 DES):

Key Length: 3 * 56 = 168 bits

a. DES - EEE3 [E = Encryption; 3 = Number of keys used]

b. DES - EDE3 [E = Encryption; D = Decryption; 3 = Number of keys used]

c. DES - EEE2 [E = Encryption; 2 = Number of keys used (Key length: 2*56 = 112 bits)]

d. DES - EDE2 [E = Encryption; D = Decryption; 2 = Number of keys used (Key length: 2*56 = 112 bits)]

3. **IDEA (International Data Encryption Algorithm): PGP uses IDEA (PGP is a good IDEA)**

Bit Block: 64 bits

Key length: 128 bit (works on DES principle)

4. **Blowfish**: Bit block - 64 bits; Key length: 32-448 bits. Much faster than IDEA and DES

5. **Skipjack**: Bit block = 64 bits; key = 80 bits. Supports key escrow. Retained by NIST and Dept. of Treasury.

Domain 3: Security Engineering

6. **RC5**

   Block = (32, 64 or 128); Key length = 0-2040 bits

7. **Advance Encryption Standard (AES)**:

   Bit Block = 128 bits

   Key: 128 bits (10 rounds)

   Key: 192 bits (12 rounds)

   Key: 256 bits (14 rounds) *Exam tip: Best encryption for Data at rest AES 256

8. **2 Fish**

   Bit block = 128 bits; Key = 256 bits

*Exam tip: Key management is essential part

Creation & Distribution of keys:

- Offline - Out of band
- Public Key encryption - Uses public key to establish communication link
- Diffie Hellman - Key exchange

Storage and Destruction of Keys:

- Keys and encrypted data should be stored in different system
- For sensitive key, use split knowledge

Key Escrow & Recovery: Secret key is divided into 2 halves and given to 3rd party. When government obtain legal authority, can combine 2 keys to create secret key. (Fair cryptosystem)

Cryptographic Life cycle: All cryptographic system has a life span (except One-time Pad).

*Exam tip: Each key should be changed periodically

Domain 3: Security Engineering

Asymmetric Key Algorithms: **P A I N**

1. RSA
2. DSA

(Remember: SA Brothers)

3. ECC
4. Elgamal

(Both starts with “E”)

5. Diffie Hellman - First Asymmetric Algorithm
6. Knapsack

1. **Rivest, Adi Shamir, and Leonard Adleman** (RSA): It’s still the worldwide standard today.

   Based on factorization of 2 large prime numbers.

   N = P * Q

   Key Length = 1024-2048 bits

2. **Elgamal: Based on Diffie Hellman** (Key exchange)

   Encrypted message is double the length of plain text. Not recommended for long mes sages.

   Plain Text= 4 bit

   Cipher text= 8 bit

3. **Elliptic Curve Cryptography (ECC)**: Key length is 160 bit. However, due to the mathe matical complexity of the algorithm, it is considered as more effective and secure than RSA.

4. **Diffie Hellman**: Used for Key Exchange

*Exam tip: Key length is perhaps the most important security parameter. Key length determines the amount of time taken to break the algorithm. Considering computing powers changes, it is advisable to keep on changing the key length.

Domain 3: Security Engineering

Core Principles of Public Key Cryptography

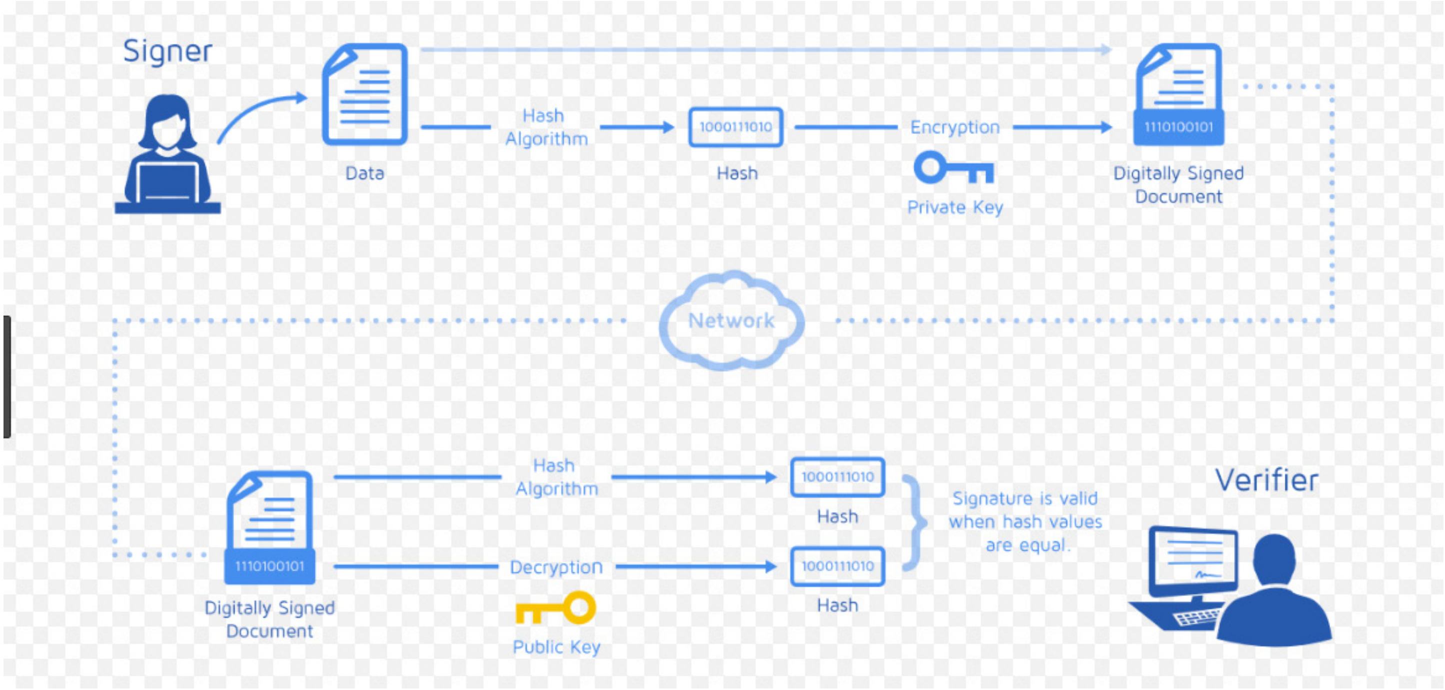
Purpose	**Method**
To Encrypt Message	Receiver's Public Key
To Decrypt Message	Own Private Key
To Digitally Sign	Own Private Key
Verify Signature	Sender's Public Key

Hash Function: **~~P~~ A I ~~N~~**

One-way mathematics. File changes-----> Hash changes

2 different message ---> same hash (collision) {Birthday attack}

Digital Signature: **~~P~~ A I N**



Domain 3: Security Engineering

Hashed Message Authentication Code (HMAC):

Hashing + Symmetric Key. **PAI~~N~~** (It provides partial authenticity)

Public Key Infrastructure (PKI):

Communication between parties previously unknown to each other. Standard: X.509 for Digital Certificates

Symmetric + Asymmetric + Hashing + Digital Certificate ----> **PAIN**

Components of PKI:

1. Certificates: Provides assurance between the parties that they are verified by CA and they are who they claim to be.

2. Certificate Authority: Authority that verifies identities and provides certificates.

3. Registration Authority: Assists CA in verification.

4. Certification Path Validation: Each certificate is valid from root till end.

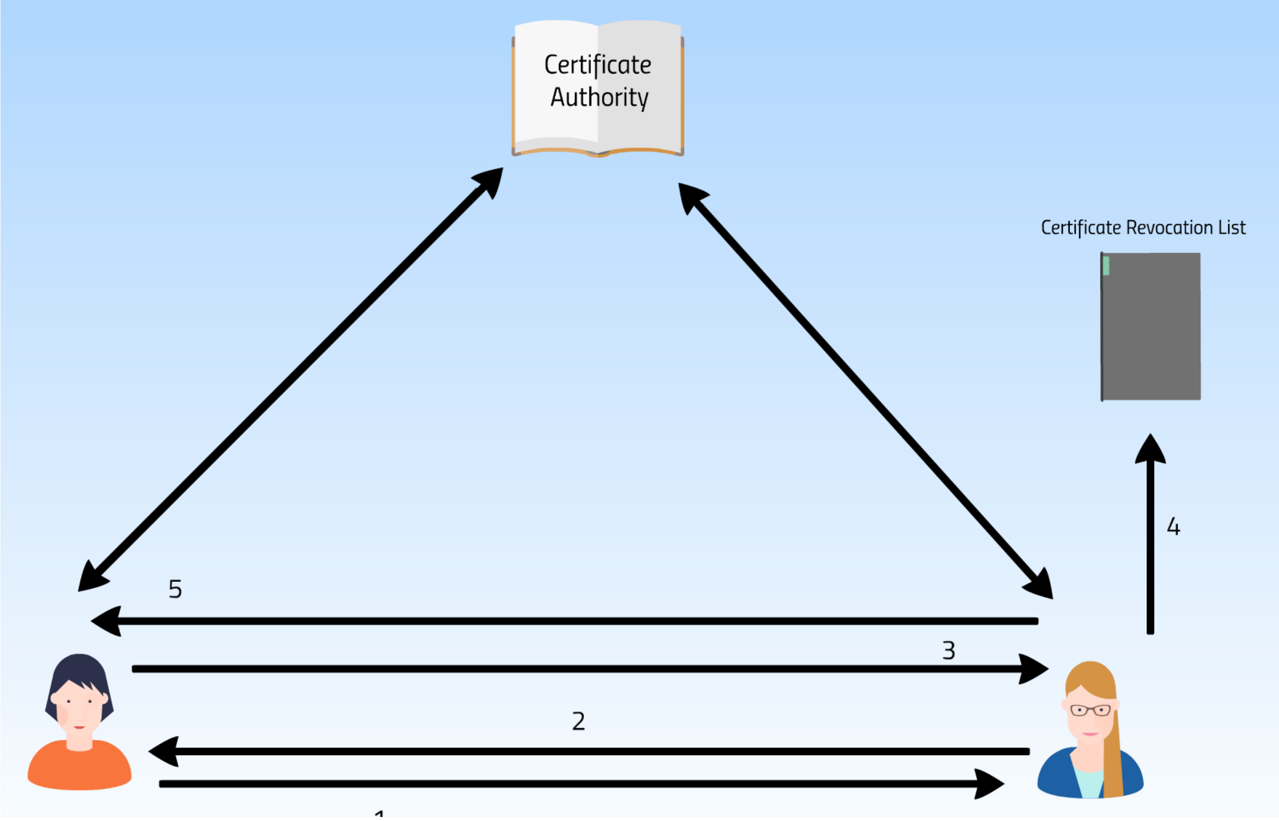
5. Certification Revocation List: List of the revoked certificates. Causes Latency

6. Online Certificate status protocol: Just query the certificate online and result would be valid, invalid or unknown.

Stages of Certificate: Enrollment -----> Verification -----> Revocation

Domain 3: Security Engineering

PUBLIC KEY INFRASTRUCTURE



1. Hey! Can we connect?
2. I don’t know you. (Trust issues...)
3. Here’s my certificate. I know our common friend CA.
4. I’ll reach out to CRL just to check if your certificate is still valid.
5. OH yes! We can connect now.

Certificate generation process:

1. Prove your identity to CA
2. Once verified, provide your public key to CA
3. CA will make a copy of public key and put in a certificate.
4. CA will digitally sign the certificate using own private key and give it to you.
5. You can distribute the certificate to the users.

Domain 3: Security Engineering

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best-known example of quantum cryptography is quantum key distribution which offers an information-theoretically secure solution to the key exchange problem.

1. Quantum Key Distribution
2. Uses Quantum Bits (Qbits)
3. Prevents from Man in The Middle Attack. Photons change state even if observed.

Applied Cryptography

1. Portable devices: MS bitlocker and encrypting file system (True Crypt)
2. Email: **P** - Encrypt
   A - Digitally Sign
   I - Hash
   N - Digitally Sign

PGP - IDEA

S/MIME - RSA

3. Web Application - SSL/TLS
4. Steganography/Water marking
5. Digital Rights Management (DRM) - Protection of music, movie, game, e-book and documents.

Circuit Encryption:

1. Link Encryption: Encrypts everything (Tunnel). Slow but secure. Works on low OSI layers
2. End to End Encryption: Encrypts on Payload (TLS/Transport). Fast but less se cure. High on OSI layers.

IPSec:

Works on Layer 3. Standard Architecture for VPN. (**P A I N**)
Setting up secure channel between 2 parties.

Modes:

a. Tunneling: Whole Packet is encapsulated (Security)
b. Transport: Only Payload is encapsulated (Performance)

Domain 3: Security Engineering

Authentication Header (AH): **~~P~~ A I N**. Prevents against replay attack

Encapsulated Security Payload (ESP): **P A I ~~N~~**

Security Association: Unique Identifier of a secure connection.

Destination address + secure parameter index

It has simplex connection ---> 2-way channel needs 2 security association.

Note: ESP also provides some limited authentication, but not to the degree of the AH.

ISAKMP: Internet Security Association Key Management Protocol

a. Authenticate

b. Create and Manage SA

c. Provide key generation mechanism

d. Protect against threat

Oakley: Used for key management (uses Diffie Hellman)

Wireless:

1. Wired Equivalent Privacy: Provides 64 & 128 bit encryption.
2. Wi-Fi Protected Access: Uses TKIP which overcomes the weakness of WEP
3. WPA2: Uses AES. Most secure

Cryptographic Attacks:

1. Analytic: Algebraic weakness
2. Implementation: Exploits the weakness in implementation.
3. Statistical Attack: Statistical weakness (generating randomness)
4. Brute Force
5. Frequency Analysis: ROT3
6. Cipher text Only: Cipher text is known
7. Known Plain text: Cipher text + Plain Text is known
8. Chosen Cipher text: Key is discovered. Decrypts the chosen cipher text.
9. Chosen Plain text: Encrypts the plain text to see the output
10. Meet in the middle attack: Attack has known plain text. DES, 3DES
11. Man in the middle attack
12. Birthday (Collision attack): Hashing
13. Replay: Keep the intercepted message and replay later.

Domain 3: Security Engineering

Security Modes, Designs, Architecture and Capabilities

Security should be at every phase of development. Should be baked in rather than bolted on.

Transitive Trust: A trust B and B trust C, then A trust C
(Proxy systems are based on transitive trust)

Open System: Anyone can access the source code.
Closed System: Proprietary systems

Zero Trust: The traditional way of saying "trust but verify" now needs to be modified to ZERO Trust. This is a manifestation of defense in depth where users (both internal and external) need to be authenticated, authorized at each and every network segment before they are able to access any resource.

Basic requirements for Zero Trust:

- Granular Access Control (Implementing Attribute Based Access control)
- Micro-segmentation of the network
- Implementing control layer/management plane to monitor any access point

Security By Design: Developers need to incorporate security at the very beginning phase and they should make security an integral part of their development process.

Requirements for security by design principles are:

- Asset classification: It's important to know what to protect. Without classification, controls cannot be implemented.
- Minimize attack surface: Always perform the threat model to know your potential threats.
- Principle of Least Privilege: Access to the system should always be limited based on least privilege.
- Principle of Defense in Depth: Never rely on one security control. Always implement layered security.
- Fail Securely: There would be several reasons the system would fail. However, when it fails, do not let any user/process gain more privileges.
- Trust but verify: It's totally okay to trust your users but always ensure to verify just to avoid any unauthorized impact on CIA.

Domain 3: Security Engineering

- Secure defaults: Establishing secure defaults means there should be strong security rules for how user registrations are handled, how often passwords must be updated, how complex passwords should be and so on.
- Separation of Duties: Ensuring no single person should be able to complete a critical task alone.
- Privacy by design: It's equally important to consider privacy at the design phase. Considering the system will be subject to processing PII data, it's important to design the controls to protect it.
- Keep it simple: More complex the design of the system will be, it will be difficult to protect.

Confinement: Read and Write are allowed only from a certain memory area (Restricted).
E.g. Sandboxing.

Bounds: State the area where process is confined.

(Limits of memory which process cannot exceed)

Isolation: When process is confined through bound, it runs in isolation

Controls: Access rules to limit access of subject to an object.

Trusted Systems: All protection mechanism work together to process sensitive data.

Fundamental concepts of Security Models

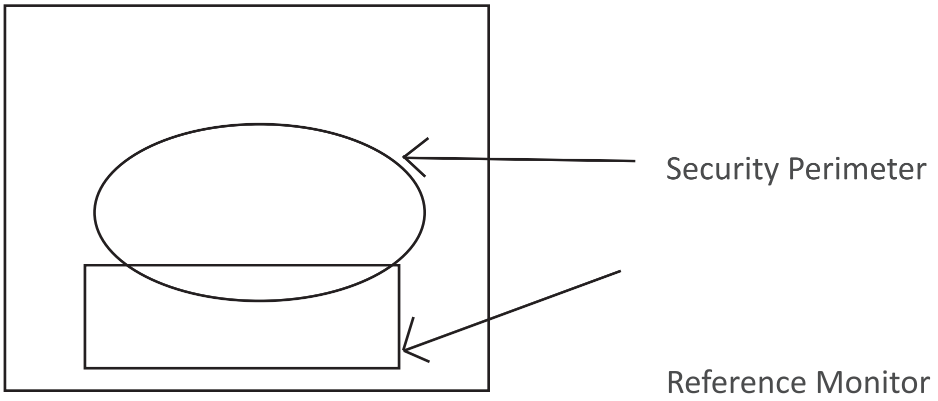
Token: Separate object that is associated with a resource and describe its security attributes.
Capability list: Rows of security attributes for each controlled object.
Security label: Permanent part of Object
Trusted Computing Base (TCB): Hardware + Software + Firmware

Domain 3: Security Engineering

Security Perimeter: Imaginary boundary that separates TCB from rest of the system.

Reference Monitor: Mediated access between subjects and objects (Access Control)

Kernel: Implements the concept of Reference Monitor



State Machine Model: System is always secure irrespective of its state.

Information Flow Model: Prevent unauthorized flow of information between different level of security.

Non Interference Model: Action taken by subject A should not affect or be noticed by subject B

Composition Theories:

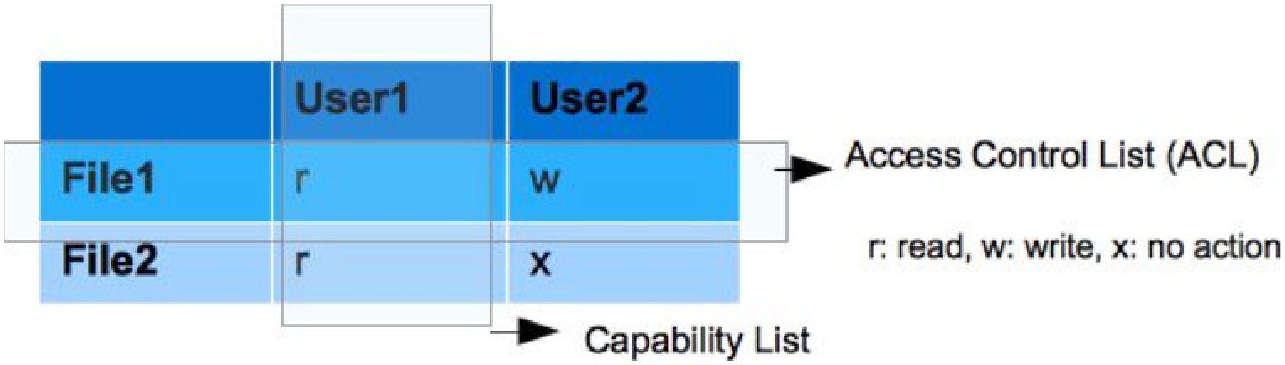
1. Cascading. Output of System A is input of System B
2. Feedback: Output of System A is input of System B and vice versa
3. Hookup: Output of System A is input of System B and other System C

Domain 3: Security Engineering

Take Grant Model: To dictate how rights can be passed from one subject to another or from a subject to an object

Take rule: Allows a subject to take rights over an object
Grant rule: Allows a subject to grant rights to an object
Create rule: Allows a subject to create new rights
Remove rule: Allows a subject to remove rights it has

Access Control Matrix: Table which shows which single subject and can take a specific action on another specific object



	User1	User2
File1	r	w
File2	r	x

Access Control List (ACL)
Capability List

r: read, w: write, x: no action

Domain 3: Security Engineering

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

Simple Rule: No Read Up
Star (*) Rule: No Write Down

Note: Covert Channels are not addressed.

Biba Model: Deals with Integrity. Information Flow Model

Simple Rule: No Read Down
Star (*) Rule: No Write Up

Maintain internal and external object consistency. Does not address Covert Channel.

*Exam tip: Simple ---> Read; Star ---> Write

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

- Prevent authorized subjects from making undesirable changes
- Transaction by authorized changes to be evaluated by another party before they are committed.
- Maintains internal consistency.
- Constrained Data Interface: When integrity is protected by Security Model
- Unconstrained Data Item: When Integrity is not protected by Security Model
- Integrity Verification Procedure: Procedures that scan data items and confirms the integrity.
- Transformation Procedure: Procedures which are allowed to modify CDI.

Brewer Nash Model: Chinese wall. Protects the conflict of interest.

Domain 3: Security Engineering

Goguen and Meseguer Model: Deals with Integrity. Non-Interference Model. Predetermined actions against predetermined objects.

Sutherland Model: Deals with Integrity. Focus on preventing interference in support of integrity. Based on State Machine and Information Flow Model. Prevents covert channel.

Graham Denning Model: Secure creation and deletion of objects and subjects

Controls Based on Security Evaluation Models

1. Evaluation is preferred to ensure system's security capabilities meet criteria of intended use.
2. System is compared if its design and security criteria and its actual capabilities and performance.

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

a. Orange Book: Standalone system
b. Red Book: Network Security
c. Green Book: Password Management

Level	Requirement
D	Minimum Protection
C1	Discretionary Protection (DAC)
C2	Controlled Access Protection (Media cleansing for reusability)
B1	Labelled Security (Labelling of data)
B2	Structured Domain (Addresses Covert channel)
B3	Security Domain (Isolation)
A	Verified Protection (B3 + Dev Cycle)

Domain 3: Security Engineering

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

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

C. Common Criteria: ISO: 15408 - Globally accepted evaluation criteria. Based on following key elements to test Target of Evaluation (TOE) {The product for evaluation}

a. Profile Protection: What customer needs

b. Security Targets: Vendor’s claim of the security in the system.

Structure of Common Criteria:

1. Introduction: Being familiar with the TOE.

2. Security Functional Requirement: Describes various functional requirements in terms of security audits, communications security, cryptographic support for security, user data protection, identification and authentication, security management etc.

3. Security Assurance: Covers assurance requirements for TOEs in the areas of configura tion management, delivery and operation, development, guidance documents, and life-cycle support plus assurance tests and vulnerability assessments.

Domain 3: Security Engineering

Level Assurance Level

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 designed, verified and tested
EAL7	Formally designed, verified and tested

Certification: Technical Evaluation. Internal verification trusted by your internal organization.
Accreditation: Formal Acceptance by the management. Performed by third party and accepted by everyone.

*Exam tip: Whenever change happens, system needs to be recertified again.

Memory Protection: Prevent process from interacting to the other area not allocated to it.

Virtualization: Guest OS's running on single OS. (Hypervisor is a component enabling virtualization)

Trusted Platform Module: Crypto processor chip used to store and process cryptographic keys for the purpose of a hardware supported/implemented hard drive encryption system.
Hardware Security Module (HSM) is a crypto processor used to manage store digital encryption keys, support faster digital signature and improve authentication.

Fault Tolerance: RAID, server cluster

Security Vulnerabilities Threats & Counter Measure

Hardware: Tangible parts of computer

Domain 3: Security Engineering

Processor: CPU - process the input to give the output. Capable of performing limited set of computational and logical operation.

Execution Types:

1. Multitasking: Two or more tasks at the same time. (Performed by OS)

2. Multi programming: Performing 2 or more programs at the same time. (Performed by special software)

3. Multi-processing: CPU harness more than one processor. (Dual Core, Octa Core)
    a. Symmetric Multiprocessing (SMP): All processors have single OS
    b. Massively Parallel Processor (MPP): All processors have their own OS

4. Multi-Threading: Multiple tasks to be performed within single process

High-Performance Computing
High-performance computing (HPC) is the ability to process data and perform complex calculations at high speeds. One of the best-known types of HPC solutions is the supercomputer.
Main components for HPC:

- Compute
- Network
- Storage

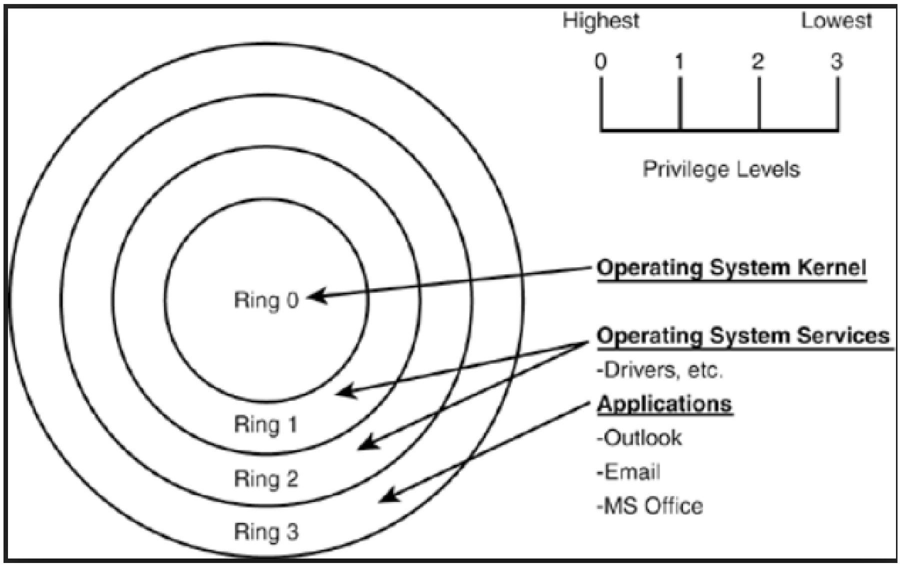
To build a high-performance computing architecture, compute servers are networked together into a cluster. To achieve high-availability, HPC clusters could be useful.
Processing Types:

1. Single State: System handle only ONE security level at a time.
2. Multi State: Handles multiple security levels at a time.

Protection Mechanism:
Prevents information from crossing between two security levels.

Domain 3: Security Engineering

Protection Ring: Organize code and components in an operating system (as well as applications, utilities, or other code that runs under the operating system's control) into concentric rings.

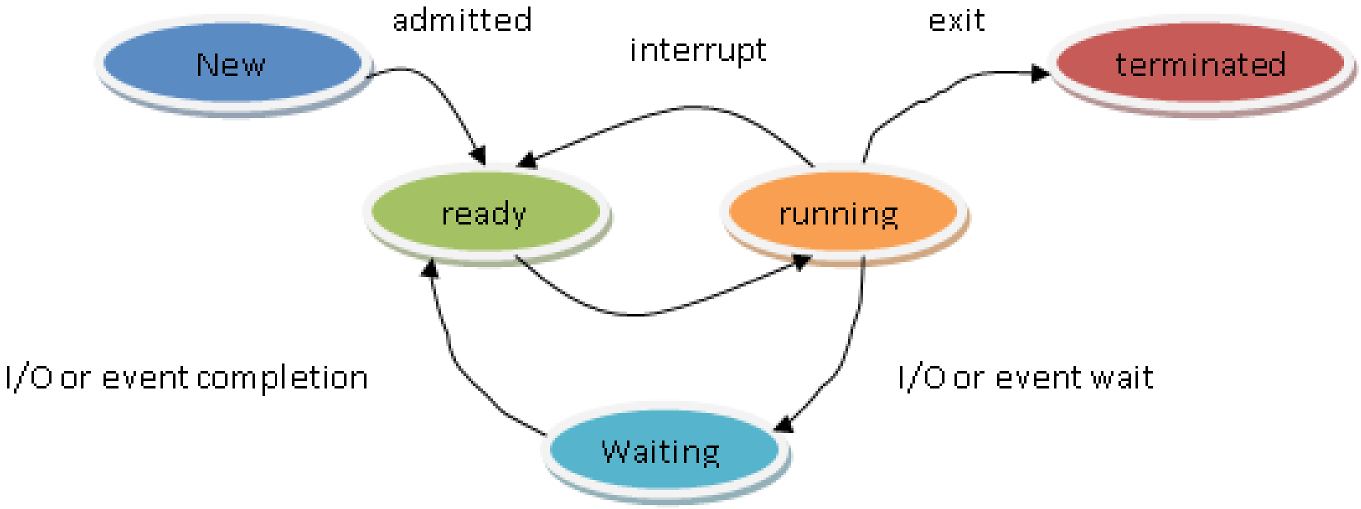


Privilege Mode: Supervisory State

User Mode: Problem State

If outer ring needs to communicate with inner rings, then it needs to make request by System Call.

Process State:



Domain 3: Security Engineering

Ready: Ready to begin or resume

Waiting: Waiting for the resources

Running: Ongoing activity

Stopped: When process finishes or terminates.

Security Modes: (**S.C.A.N.**)

	Signed NDA	**C**learance	**A**pproval	**N**eed to Know
Dedicated	All	All	All	All
System High All	All	All	All	Some
Compartmentalized	All	All	Some	Some
Multilevel	All	Some	Some	Some

Memory:

1. Read Only Memory (ROM): No writing allowed
2. Programmable ROM (PROM): Can be written only once
(Used for hardware application)
3. Erasable PROM (EPROM): Special Ultra violet lights can erase the content
4. Electrically EPROM (EEPROM): Electric voltage delivered (Used in BIOS)
5. Flash Memory: Similar to EEPROM, just needs to be deleted in blocks.
6. Random Access Memory: Readable and writable memory
7. Real Memory: Also called as primary.
Largest RAM storage resource available to a computer.
8. Cache Memory: Faster RAM
9. Dynamic RAM: Capacitor (Slow)
10. Static RAM: Flip flops (Fast)
11. Synchronous DRAM: Clock Cycle

Registers: Temporary memory of CPU holding initial instructions.

Domain 3: Security Engineering

Memory Addresses:

1. Register Addressing: Address of the CPU register used in instruction (e.g. register 1)
2. Immediate addressing: Provide immediate instructions to CPU
3. Direct Addressing: Actual address of the memory location.
4. Indirect addressing: Memory address contains other memory address. (Reference)

Secondary Memory: Tapes, Optical disks etc.

Virtual Memory: Special type of secondary memory which OS manages to look like real mem ory. (less expensive but slow)

Storage:

Primary VS Secondary: RAM VS ROM
Volatile VS Non-Volatile: RAM VS HDD
Random VS Sequential: Random search (Fast) VS Sequential Search (slow)

*Exam tip: Threat to storage media ----> Data Remanence

Input/output structures:

1. Memory mapped I/O: Manage I/O
2. Interrupt RQ: When device needs to supply I/P to CPU, it sends signal to assign IRQ.
3. Interrupt Conflict: When two devices have same IRQ number.

4. Direct Memory Access: When device needs to make direct access with other device it uses “DMQ” (DMA Request). Till the time CPU blocks the memory location. DACK (DMA Acknowledgement) is when the task is completed, device sends DACK.

Firmware: Software in the ROM chip.
BIOS: Base Input Output System are the instructions that a computer needs to startup and load the OS from the disk. (attack on BIOS is called phlashing attack)

Domain 3: Security Engineering

Client Based:

1. Applet: Mini programs that server sends to client system. Processing burden is on client. Remote code execution can happen.

2. Java Applet: Short java programs transmitted over internet.
    a. Sandbox: Isolates Java program

3. ActiveX: Similar to Java Applet. Product of Microsoft. Can run only on MS browsers and MS proprietary.

4. Local Caches:
    a. ARP Cache Poisoning: Intruding the ARP cache where IP to MAC table is main tained. (can lead to MITM attack)
    b. DNS Poisoning: Intruding the DNS cache.
    c. Local cache: Temporary internet files.

Server Based: Data flow management = Efficiency + minimum delay + throughput + Confidentiality.

Database Security:

1. Aggregation: Collection of non-sensitive information to create sensitive information.
2. Inference: Requires deduction. Gain access to higher level. Countermeasure ---> Poly instantiation
3. Data Ware housing: Collection of data from multiple databases for the purpose of analysis.
4. Data Mining: Analysis on the data obtained by data warehousing.
5. Data Dictionary: Storing data usage, type, source, relationship & format.
    - Activity of Data mining produces metadata. Metadata is stored in a more secure container “Data Mart”
6. Data Analytics: Extraction and making meaningful data.
7. Large scale parallel Data Systems: Performs numerous calculations in parallel.
8. Distributed systems: Multiple thin clients with processing capabilities. (Tip: Trust is an issue with distributed system)

Domain 3: Security Engineering

Cloud Computing:

1. Virtualization
    a. Type 1 Hypervisor - Directly interacts with hardware. More secure
    b. Type 2 Hypervisor - Less secure as OS introduces larger attack surface area
2. Elasticity
3. Resource Pooling
4. Cloud Storage

Cloud Services

1. Software As A Service: Fully functional applications accessed via browsers. e.g. Gmail, Office 365. Max. responsibility is with CSP. On demand access to applications.

2. Platform As A Service: CSP provides platforms like OS, Hardware. Customer simply builds the applications over those platforms. CSP is responsible for maintenance of underlying infrastructure.

3. Infrastructure As A Service: Provides basic computing resources. All the maintenance is performed by the consumers. Full control over virtualized Hardware, memory & storage.

Cloud Deployment Model

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud
4. Community Cloud

Grid Computing: If a computer is ideal, its resources are utilized for other projects. (Like searching aliens ;-))

Peer to Peer: VOIP service e.g. Bit torrent, Skype etc.

Domain 3: Security Engineering

Internet of Things

The Internet of Things (IoT) is a new subcategory or even a new class of smart devices that are Internet-connected in order to provide automation, remote control, or AI processing to traditional or new appliances or devices in a home or office setting.

- The security issues related to IoT are about access and encryption.
- Best Practice is to isolate the IoT devices from primary network.

Edge Computing

It is a part of a distributed computing topology in which information processing is located close to the edge – where things and people produce or consume that information. (Similar to CDN). Development of Edge computing was because of significant growth in IoT devices and expectation is to process the information on the devices rather than transmitting through the data center. Security and Privacy should be considered in a similar way as incorporated in Cloud environment. Shift of ownership would be on end users instead of service providers.

Microservices

Service-oriented architecture (SOA) is an enterprise-wide approach to software development that takes advantage of reusable software components, or services. Each service is comprised of the code and data integrations required to execute a specific business function—for example, checking a customer's credit, signing in to a website, or processing a mortgage application. Like SOA, microservices architectures are made up of loosely coupled, reusable, and specialized components. However, rather than being adopted enterprise-wide, microservices are typically used to build individual applications in a way that makes them more agile, scalable, and resilient.

Containerization

Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS). A container is essentially a fully packaged and portable computing environment:

Domain 3: Security Engineering

•Everything an application needs to run – its binaries, libraries, configuration files and dependencies – is encapsulated and isolated in its container.
•The container itself is abstracted away from the host OS, with only limited access to underlying resources – much like a lightweight virtual machine (VM).
•As a result, the containerized application can be run on various types of infrastructure: bare metal, within VMs, and in the cloud—without needing to refactor it for each environment.

Industrial Control system:
An industrial control system (ICS) is a form of computer-management device that controls industrial processes and machines including manufacturing, fabrication etc.
Forms of ICS:
Distributed Control System (DCS): It's for large scale industries. Controls are distributed.
Programmable Logic Control (PLC): Focused on computers. E.g. Used in systems are assembly line.
Supervisory Control and Data Acquisition: It can operate as a stand-alone device, be networked together with other SCADA systems.

1. Distributed Control System (DCS): It's for large scan industries (Digital and Analog)
2. Programmable Logic Control (PLC): Focused on computers. (Digital)

(Stuxnet ---> Rootkit for SCADA systems)

OWASP:
XSS (Persistent, Non-persistent, DOM based) {Input Validation}
SQL Injection {Input Validation, Limit Access Privileges, use stored procedures)
CSRF {Session authentication, terminate inactive sessions}
XML Exploitation: Falsify information being sent to a visitor.
Broken Authentication: Vulnerabilities in authentication systems
Sensitive Data Exposure
Broken Access Control
Security Misconfiguration
Using Components with Known Vulnerabilities
Insufficient Logging and Monitoring

Vulnerabilities of mobile system: Eaves dropping, malicious code.

Domain 3: Security Engineering

Mobile Security:

1. Full Device Encryption
2. Remote wiping
3. Lock out
4. Screen locks (swiping, pattern, pin, password etc.)
5. GPS
6. Application control (Limits which application can be installed)
7. Storage segmentation (for isolation)
8. Asset tracking
9. Inventory control
10. Mobile Device Management: Improves security of mobile devices
11. Device Access Control (Strong password, MDM)
12. Removable storage
13. Disabling unused feature

Application Security:

1. Key Management (Randomness)
2. Credential Management (Storage of credentials)
3. Authentication
4. Geo Tagging
5. Encryption
6. Application Whitelisting (Only authorized application can be installed)

BYOD Concerns: It is important to sign off BYOD policy

1. Data Ownership: Data isolation is important. Device owner should backup data.
2. Support ownership
3. Patch Management
4. Antivirus Management
5. Forensics
6. Privacy
7. On-boarding/Off-boarding
8. Adherence to Corporate Policy
9. User Acceptance (Policy acceptance)

Domain 3: Security Engineering

10. Architecture/Infrastructure consideration (Load on network)
11. Legal Concerns
12. On-board Camera/Video

Embedded Devices: The Internet of Things (IoT) is a new subcategory or even a new class of smart devices that are Internet-connected in order to provide automation, remote control, or AI processing to traditional or new appliances or devices in a home or office setting. The security issues related to IoT are about access and encryption. Best Practice is to isolate the IoT devices from primary network. (Homeland Web series has a great example of IoT breach.) e.g. Robotic surgery, car sensors, Smart home appliances.

Methods for security:

1. Network Segmentation (Isolation)
2. Security Layers
    a. Logical Isolation (Classification)
    b. Physical isolation (Network segments)
3. Application firewalls
4. Manual Updates
5. Firmware version control ---> Updates should be manual
6. Wrappers ---> Encapsulation
7. Control Redundancy and Diversity ---> Defense in Depth

Essential Security Protection Mechanism: No software should be trusted.

***Exam tip**: Primary focus of OS is to keep the computing environment stable and keep process isolated from each other

1. Technical Mechanism
    a. Layering: Ring Model (Ring 0---> Privilege; Ring 3 ---> User)
    b. Abstraction: Transparent to how objects work
    c. Data hiding: Cell suppression
    d. Process Isolation: Protects integrity & prevent unauthorized data access
    e. Hardware segmentation: Physical isolation

Domain 3: Security Engineering

2. Policy Mechanism
    a. Principle of least privilege: right + Permission
    b. Separation of privilege
    c. Accountability: System should capture logs

Common Architecture Flaws:

1. Covert Channels: Communication over unauthorized channel. Opposite is known as Overt Channel (communication through authorized channel)
    a. Covert Timing Channel: Modify resource timing (Difficult to detect)
    b. Covert storage channel: writing data to a common storage for other process to read it.
    Defense: Proper Code Review, Auditing

2. Backdoors: Deliberate entry point left so that system can be accessed without access control

3. Maintenance hook: Developers leave the backdoor to fix production issues. (Trapdoor)

4. Trusted Recovery: If system fails, it should make an attempt to recover to a state prior to failure. All controls remain intact.

5. Buffer Overflow: Bound checking

6. Salami: small amounts are stolen assuming it will go unnoticed

7. Data Diddling: Small change in data during processing, storage, input/output transaction

8. TOC-TOU (Time of check-Time of Use)
    a. TOC: Subject checks the object
    b. Subject decides to use the object

Between TOC & TOU, there is a time difference which is exploited. (Race condition)

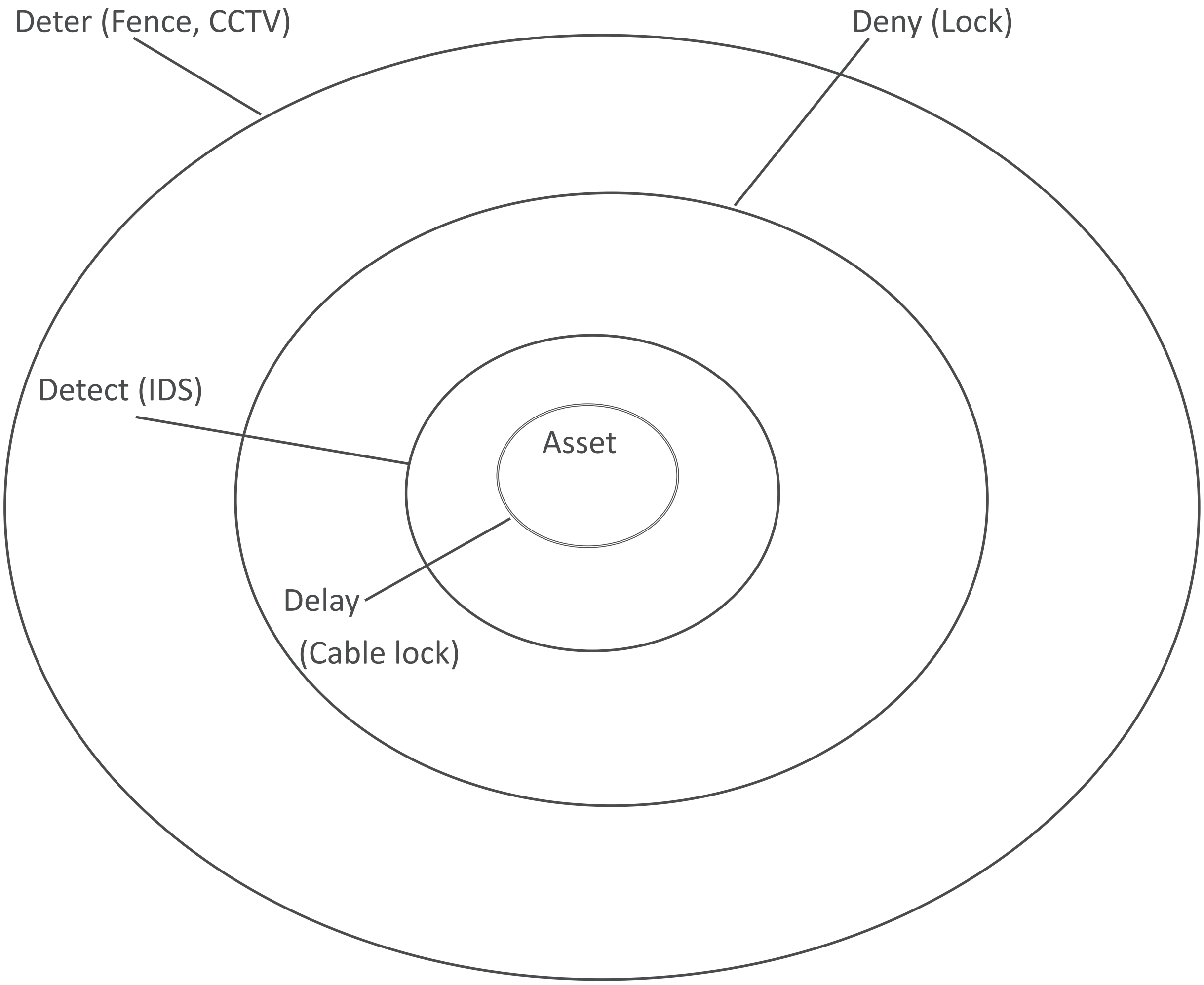
Domain 3: Security Engineering

Service Oriented Architecture: Constructs new apps out of existing apps. Web based and distributed computing.

Tempest:

1. Faraday Cage: Special enclosure to protect electromagnetic emissions from leaving the enclosure.
2. White noise: Generating random signals causing too much interference which makes difficult to retrieve data.
3. Control Zone: Faraday cage + White noise

Physical Security



Defense in Depth

Domain 3: Security Engineering

Physical Security are the first line of defense. People are the last.

Critical Path Analysis: First thing to do before outlining security. Systematic effort to identify relationship between mission critical applications and all necessary supporting elements.

Technology Convergence: Tendency for various technologies solution to evolve and merge overtime.

Wiring Closet: Premises wire distribution room

Smart Cards: Have chip in it to process information (used for multi-factor authentication)

Memory cards: Can store information (credit cards)

Proximity readers: Passive device --> Magnet with specific properties (anti-theft)

Field Powered: card readers for access card (generates magnetic field)

Transponder: Self powered and transmits a signal (garage door opener)

Intrusion Detection system: Alarm system. If the line of alarm system fails, heartbeat sensor helps in line supervision. (A heartbeat sensor is a mechanism by which the communication pathway is either constantly or periodically checked with a test signal.)

Access Abuse: Masquerading, Piggybacking

Domain 3: Security Engineering

Emanation Security:

1. Faraday Cage: Special enclosure to protect electromagnetic emissions from leaving the enclosure.

2. White noise: Generating random signals causing too much interference which makes difficult to retrieve data.

3. Control Zone: Faraday cage + White noise

Utilities & HVAC: UPS, Surge Protectors (Prevent power fluctuations)

Fault: Momentary loss

Black out: Complete loss

Sag: Momentary low voltage

Brown out: Prolonged low voltage (8% drop between power source and meter and 3.5% drop between meter and power outlet)

Spike: Momentary High voltage

In-rush: Initial surge

Noise: Steady power fluctuation

Transient: Short duration of line noise

Clean: Non fluctuation power

Ground: Wire which is grounded

Domain 3: Security Engineering

Noise:

1. Electromagnetic Interference (EMI):
    a. Common Mode: Difference between Hot and Ground wire.
    b. Traverse Mode: Difference between Hot and Neutral wire.
2. Radio Frequency Interference: Appliances and fluorescent lights, electrical cables generates RFI.

Temperatures, Humidity & Static:

Computer Rooms: 15°C - 23°C (Temperature)
40 - 60% (Humidity)

Static Voltage	Damage
40	Destroy Circuits
1000	Scrambling monitor display
1500	Destroy stored data
2000	System shut down
4000	Printer jam
17000	Permanent circuit damage

Water Issues ----> Leakage, flooding
Positive Drain ----> Water goes out

Fire prevention, Detection and Suppression

1. Water ----(**Suppress**)----> Temperature
2. Soda Acid, Dry Powder ----(**Suppress**)----> Fuel Supply
3. CO2 ----(**Suppress**)----> Oxygen
4. Halon ----(**Stops**)----> Chemical Reaction

Domain 3: Security Engineering

Four stages of Fire:

1. Incipient: Air ionization but no smoke
2. Smoke: Smoke visible
3. Flame stage: Flame Visible
4. Heat: Intense Heat visible

Fire Extinguisher -- **C L E M** (Tip to remember)

Class	Type	Suppression Material
A	**C**ommon Combustible	Water, soda acid
B	**L**iquid	CO2, Halon, Soda acid
C	**E**lectrical	CO2, Halon (FM-200)
D	**M**etal	Dry Powder

*Note: Montreal Protocol is a reference to ban of Halon as it depletes Ozone Layer

Water Suppression System:

1. Wet Pipe (closed headed): Always filled with water
2. Dry Pipe: Contains compressed air
3. Deluge: Dry pipe with large pipes which deliver huge volume of water. (not suitable for environments with computer or electronic items)
4. Preaction: Combination of dry and wet pipe. Most suitable for computer rooms with humans

Damage:

Temperature	Damage
100°F	Storage Tapes
175°F	Hardware (RAM, CPU)
350°F	Paper products

Domain 3: Security Engineering

Perimeter Security:

Single Entrance ----> Better Security

Multiple Entrance ----> Better Evacuation

Fence:

1. 3-4 feet ---> casual trespasser
2. 6-7 feet ---> most intruders
3. 8+ feet ---> Determined intrude

Turnstile --> Prevents tailgating

Man Trap --> Prevents Piggy Backing

Lightening --> Most common perimeter security (2 candle feet of power is the unit of lightening)

Security Guards --> Most expensive. Used where judgement is required. Not reliable.

Dogs --> Expensive with liability

Internal Security:

1. Locks: Inexpensive control --> preset locks (house hold locks) {attack is called shimming}

2. Programmable locks --> Multiple valid access combination (smart cards, cipher device)

3. Electronic Access Control --> Electro Magnet, Credential reader, sensor (Access cards in offices)

4. Badges --> Used for identity & Authentication/Authorization

Domain 3: Security Engineering

Motion Detectors:

1. Infrared --> changes in infrared light pattern
2. Heat Based --> changes in heat level
3. Wave Pattern --> changes in the ultra-sonic or high microwave signal
4. Capacitance --> changes in the electric or magnetic field
5. Photoelectric --> changes in the visible light
6. Passive audio motion --> Listens abnormal sound

Intrusion Alarms: Deterrent, Repellant, Notification

Local Alarm system: Must be audible by 400 feet
Central station system: Silent locally, but offsite monitoring agents are notified

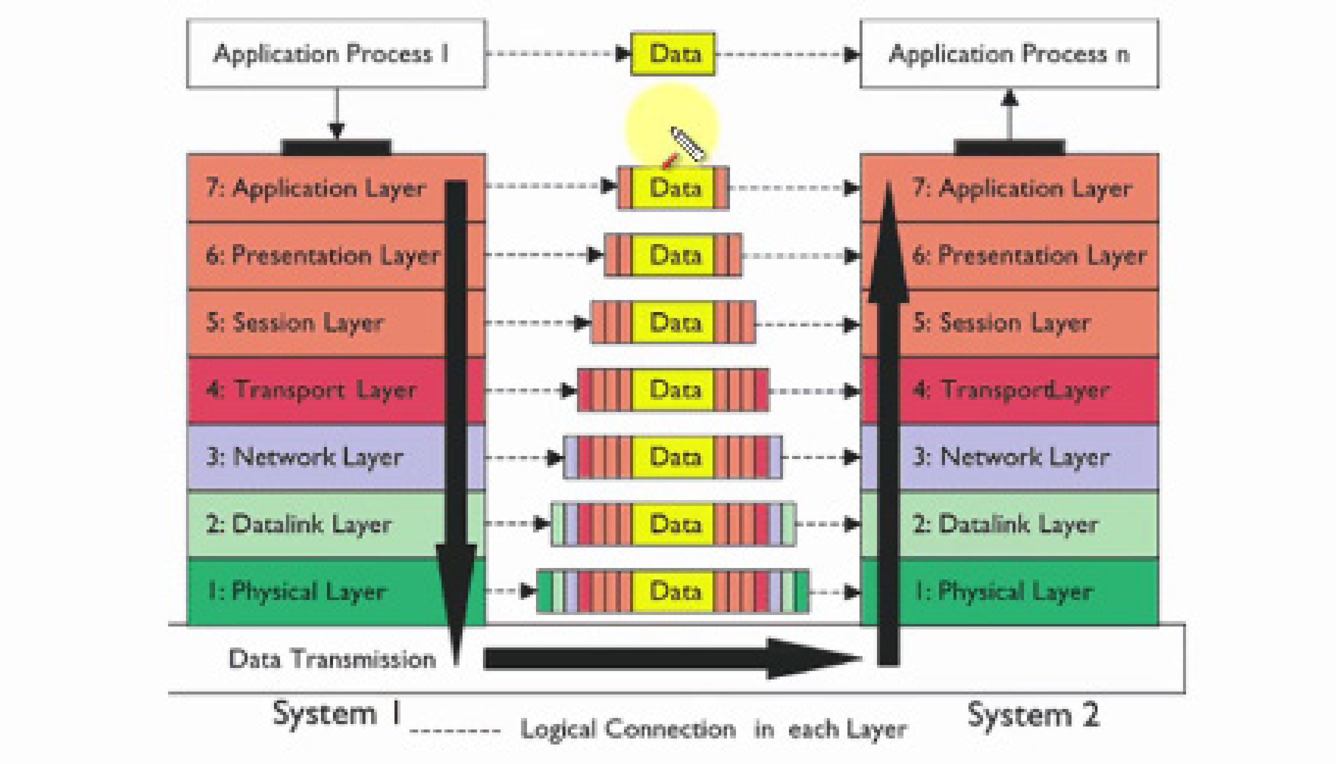
Auxiliary station: Emergency services are notified
Secondary verification: CCTV + 24x7 monitoring

*Exam tip: Within organization, area should be compartmentalized or separated based on the sensitivity.

Environment & Life safety: Human life is first priority (Occupant Emergency Plan)

Domain 4: Network Security

OSI Reference Model: Developed by ISO (ISO 7498) --> This model gave a framework on how two systems should communicate with the protocols.



*Hint: Please Do Not Touch Steve's Pet Alligator {way to remember 7 layers starting from Physical to Application}

Encapsulation ---> Packaging : When the payload (message) has the headers and footers add ed as the message goes down to layers in OSI model.

Decapsulation ---> De-packaging : Unwinding the message as it goes up to the layers of OSI Model.

Domain 4: Network Security

Layer	**Data known as**
Application	Data Stream
Presentation	Data Stream
Session	Data Stream
Transport	**S**egment (TCP)/Datagram (UDP)
Network	**P**acket
Data Link	**F**rames
Physical	**B**its

*Hint: Some People Forget Birthdays

Layer 1 (Physical): Accepts frames from Data link and coverts them into bits (encapsulation) and it also converts physical bits to frames at the receiving system (Decapsulation).

Cable, voltage, HUB, signals.

Cables:

a. Twisted Pair --> Least secure. Cheap and easy installation

b. Fiber Optics --> Most secure. Expensive and hard to work with.

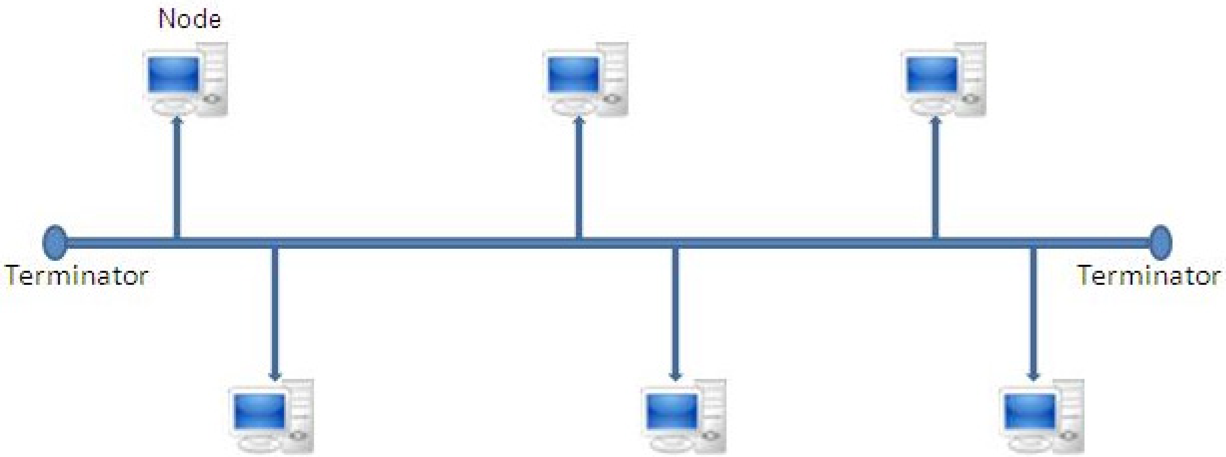
Network topology:

1. Bus:

a. No central point of connection

b. Difficult to troubleshoot

c. One break in cable takes down whole network

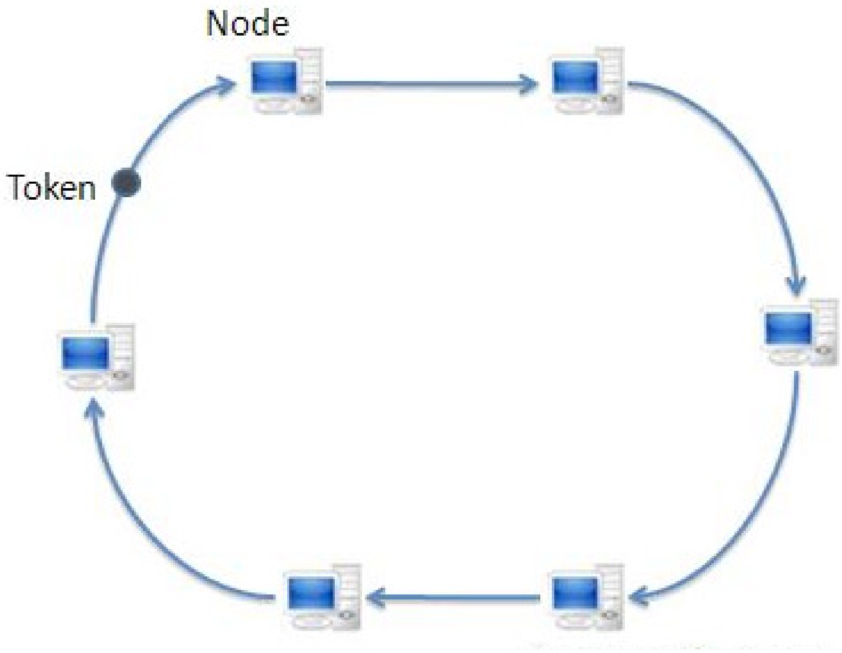


Domain 4: Network Security

2. Ring:

    a. No central point of connection

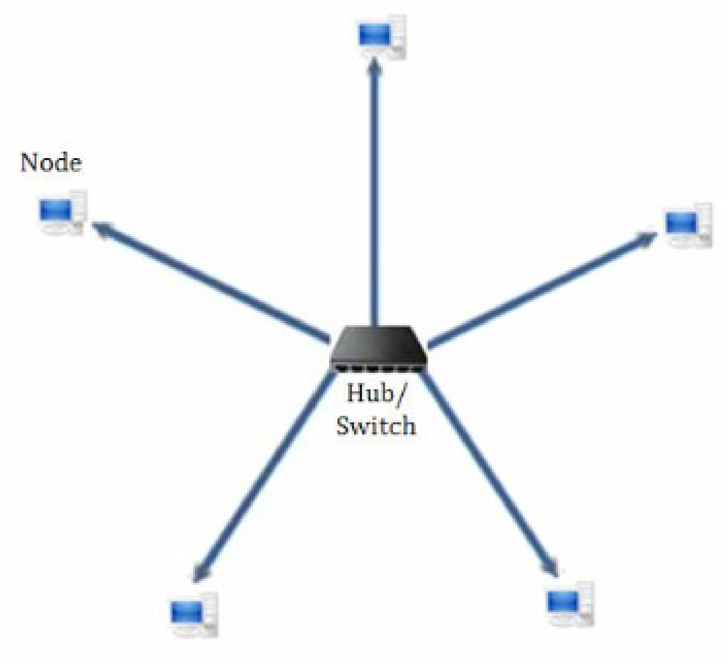
    b. Implemented with MAU (Media Access Unit) for fault tolerance.



3. Star:

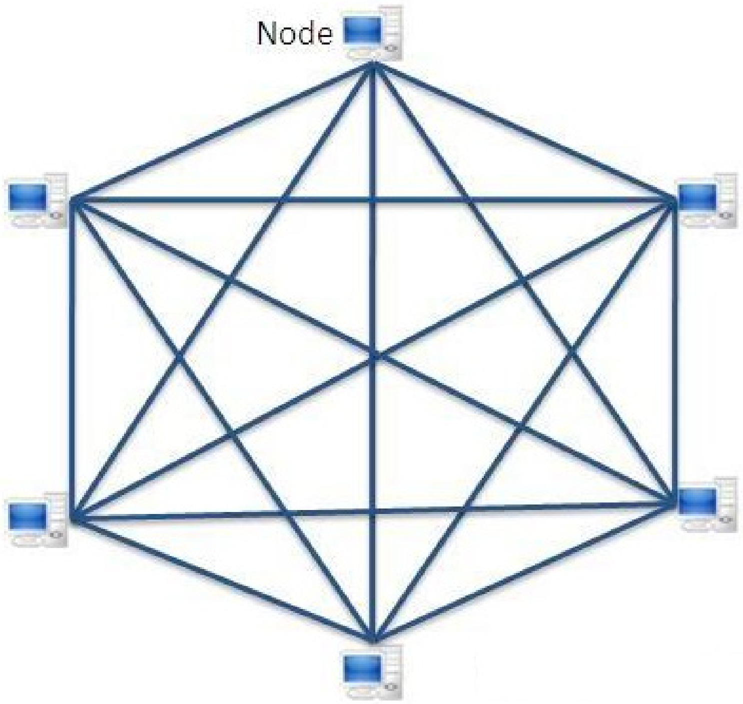
    a. Offers Fault Tolerance

    b. Switch is a single point of failure



Domain 4: Network Security

4. Mesh:
    a. Most fault tolerant
    b. Fully redundant
    c. Partial mesh is used to spare cost as its very costly



HUB: Sends all data to all ports. No addressing and less expensive. (Layer 1)

Modem: Modulator Demodulator. Converts digital to analog signals and vice versa

Router: Routers are networking devices used to move traffic based on IP addresses. They are located at Layer 3 of the OSI Model.

Bridges: These devices connect two different networks within a LAN and works at Layer 2.

Gateways: Also known as Gateway routers. These devices are used to connect 2 different networks using different protocols.

Switch: Uses MAC address to direct traffic. Acts as a police officer directing traffic to respective ports. Reduces collision. Associate VLANs with switches.

Wireless Access Point: Provides wireless devices a point of connection to the wired network.

Domain 4: Network Security

Layer 2 (Data Link): Converts packet into proper format for transmission (frames)
Logical Link Control (LLC): Error detection
Media Access Control (MAC): Physical address

Address Resolution Protocol (ARP): Maps IP address to MAC address
Reverse Address Resolution Protocol (RARP): Maps MAC address to IP address

ARP poisoning: ARP keeps the list of MAC address to its cache memory. If an attacker changes the legitimate address to some other address.

Unsolicited reply: Response to the query which ARP never asked

Media Access Control:

1. CSMA/CD: Carrier sense multiple access with collision detection (IEEE 802.3) Ethernet
2. CSMA/CA: Carrier sense multiple access with collision avoidance (IEEE 802.11) Wireless
3. Token Passing: 24 bit control frame passed around the network environment with the purpose of determining which system can transmit data. No collision as system can't communicate without token.

Baseband vs Broadband

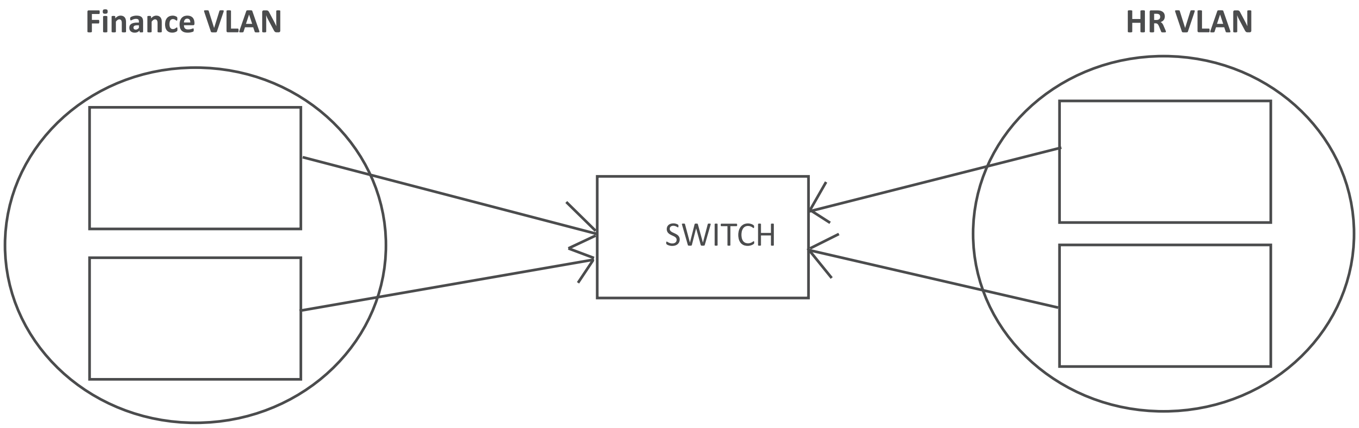
1. Baseband technology can support only a single communication channel. Baseband is a form of digital signal. Ethernet is a baseband technology.
2. Broadband technology can support multiple simultaneous signals. Broadband is a form of analog signal. Cable television and cable modems, ISDN, DSL, T1, and T3 are examples of broadband technologies.

Broadcast, multicast, and unicast technologies determine how many destinations a single transmission can reach:

1. Broadcast technology supports communications to all possible recipients.
2. Multicast technology supports communications to multiple specific recipients.
3. Unicast technology supports only a single communication to a specific recipient.

Domain 4: Network Security

Layer 3 (Network): Adds routing and addressing information to data. Network layer adds information but doesn’t guarantee delivery of the packet. It is done by transport layer.
Routers isolate traffic into broadcast domain and uses IP addressing to direct traffic. As routers are expensive, broadcast isolation is done through switch.



- Routers are expensive
- Broadcast isolation is done through VLAN
- Layer 3 switch is necessary for inter VLAN communication
- Layer 2 switch provides proper VLAN isolation

*Exam tips: Most of the protocols which starts with “I” is a layer 3 protocol. IP, ICMP, IGMP, IGRP, IPSeC, IKE, ISAKMP. IMAP being an exception as it works at layer 7

Domain 4: Network Security

SNMP V3: Simple Management Network Protocol is a standard protocol used to interact with various network devices to obtain status information, performance data, statistics, and configuration details.

ICMP: Internet Control Message Protocol is used to determine the health of a network or a specific link.

Any attack with 'ping' exploits ICMP.
ICMP attacks:

- Loki (Covert channel)
- Ping of death (Violates maximum transmission unit)
- Ping of flood
- Smurf

Distance Vector: Direction and distance in hops (BGP, RIP, IGRP)
Link state: Determines shortest path (OSPF)

Layer 4 (Transport): Provides end to end data transport services & establish a logical connection between 2 computer system.
Protocols used at layer 4:

1. SSL/TLS (from layer 4 to 7)
2. TCP (connection oriented --> slow)
3. UDP (Connectionless)
4. SPX (sequenced packet exchange)

SYN flood and Fraggle (Layer 4 attack)
Streaming, gaming uses UDP

Domain 4: Network Security

Layer 5 (Session): Responsible for establishing connection between 2 applications.

Simplex: system A communicates to system B
Half Duplex: system A communicates to system B and B communicates to A but only one at a time
Full Duplex: Bi-directional and both systems can communicate simultaneously.

Create ---> Transfer ---> Release

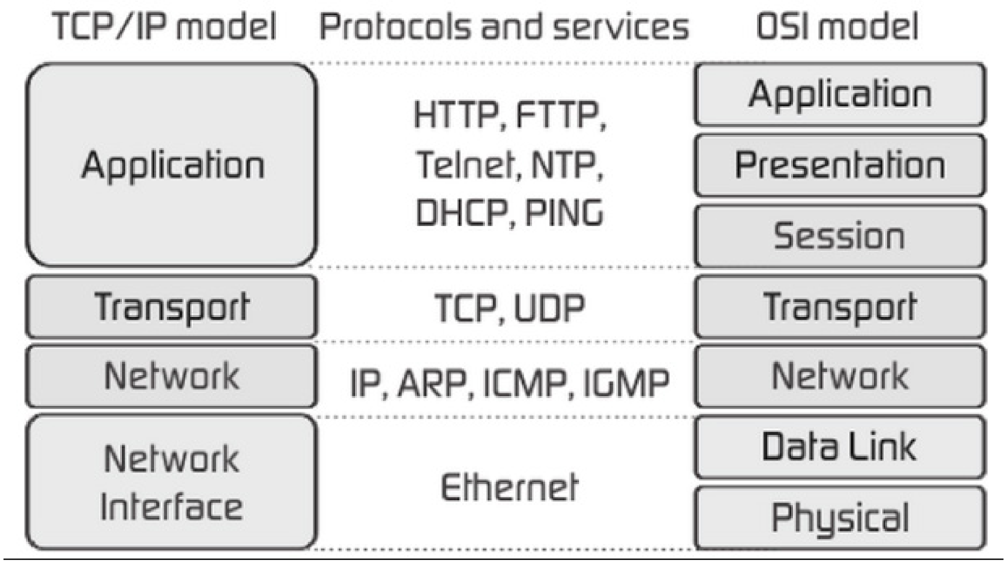
Remote procedural call, NFS, SQL are the protocols working at layer 5.

Layer 6 (Presentation): Present the data in a format that all computer can understand.

- Formatting (JPEG, GIF, MP3)
- Encryption
- Compression (removing redundancy)

*No protocols

Layer 7 (Application): Defines a protocol (way of sending data) that 2 different programs or application understand.
HTTP, HTTPS, FTP, TFTP, SMTP, etc.



Domain 4: Network Security

TCP Wrapper: Application like a Firewall restricting access to ports and resources based on user IDs and system IDs (Port based access control)

Port (0 - 1023) - Known ports
Port (1024 - 49151) - Registered software ports
Port (49152 - 65536) - Random/Dynamic

Converged Protocols: Merging of specialty protocols with standard protocols majorly done for cost saving.

1. Fiber Channel over Ethernet (FCoE): Works as network data storage solution. Allows high speed (16 Gbps) fiber channel over ethernet. Works at Layer 3

2. Multi-protocol Label Switching (MPLS): High performance, high throughput which directs data on short path labels.

3. Internet small computer system interface (iSCSI): Used to enable location independent file storage, transmission and retrieval over LAN, WAN. Used as cheap alternative of Fiber Channel.

4. VOIP: Tunneling mechanism used to transport voice & data over TCP/IP network.

5. Software Defined Network: Separates Infrastructure layer from Control Layer (Network Virtualization)

6. Content Distribution Network (CDN): Collection of resources deployed in data center across internet in order to provide low latency and High performance. (Layer3)

Domain 4: Network Security

Threats to Network Security

Common attacks:

1. Virus: Malicious code which is created to infect systems.
2. Worms: Malicious code which propagates itself
3. Logic Bomb: Execute the code on April 1 2020. (time based/event based)
4. Trojan: Executable file which resembles like a legitimate file which infects the system.
5. Backdoor: Entry point in an application which is not authorized.
6. Salami: Stealing small amounts to avoid getting noticed and accumulating it to bigger amount (salami slices)
7. Data diddling: Altering raw data just before it is getting processed by a computer.
8. Sniffing: Listening to the traffic being transmitted
9. Session Hijacking: Capturing authentication session to identify credentials.
10. War dialing: Dialing the random numbers to identify the modem running behind.
11. DDoS: Sending packets beyond the bandwidth capacity
12. Syn Flood: sending syn packets in 3 way handshake process without completing the handshake.
13. Smurf: Sending ICMP packets (DDoS)
14. Fraggle: Similar to smurf just uses UDP packets.
15. Loki: Covert channel
16. Teardrop: Sending fragmented packets in an order which cannot be re-arranged.

Network Access Control

Network Access Control (NAC) is a concept of controlling access to an environment through strict adherence to and implementation of security policy. The goals of NAC are as follows:

- Prevent/reduce zero-day attacks
- Enforce security policy throughout the network
- Use identities to perform access control

NAC can be implemented with a preadmission philosophy or a postadmission philosophy, or aspects of both:

- The preadmission philosophy requires a system to meet all current security requirements (such as patch application and antivirus updates) before it is allowed to communicate with the network.

- The postadmission philosophy allows and denies access based on user activity, which is based on a predefined authorization matrix.

Domain 4: Network Security

Firewalls: Allow/Block traffic (RuBAC). Hardware or Software based.

1. Packet Filter Firewall: aka 1st Generation Firewall
    - a. Uses ACL (rules that firewall applies)
    - b. Not state full (Looks at network and transport layer packets -- IP, ports etc.)
    - c. Do not look into applications. Can't block virus
    - d. Do not support anything advanced or custom.
    - e. Works on Layer 3 (Decision on source/destination, IP address & Port information)

2. Application Level Firewall: aka 2nd Generation Firewall
    - a. Also called as proxy firewall
    - b. Adds extra security in the architecture
    - c. Can have logging, auditing and access control feature.
    - d. Extra processing degrades the performance as it examines each packet.
    - e. Works at layer 7

3. Circuit Level Firewall: aka 2nd Generation Firewall
    - a. Used to establish communication session between trusted partners
    - b. Monitor TCP handshake
    - c. Also called as Circuit proxies.
    - d. SOCKS (socket secure) is a common implementation.
    - e. Works at layer 5

4. State full Firewall: aka 3rd Generation Firewall
    - a. Knowledge of who initiated the session. Blocks unsolicited replies (ARP poisoning)
    - b. Router keeps a track of connection in a table. It knows which connections are active.
    - c. More complex, can launch DoS against itself by trying to fill up all the entries in state table.
    - d. If rebooted, can disrupt conversation that had been occurring.
    - e. Content dependent access control
    - f. Works at layer 3 and 4

Domain 4: Network Security

5. Deep Packet Inspect Firewall

    a.Deep packet inspection (DPI) firewalls is a filtering mechanism that operates typically at the application layer in order to filter the payload contents of a communication rather than only on the header values.

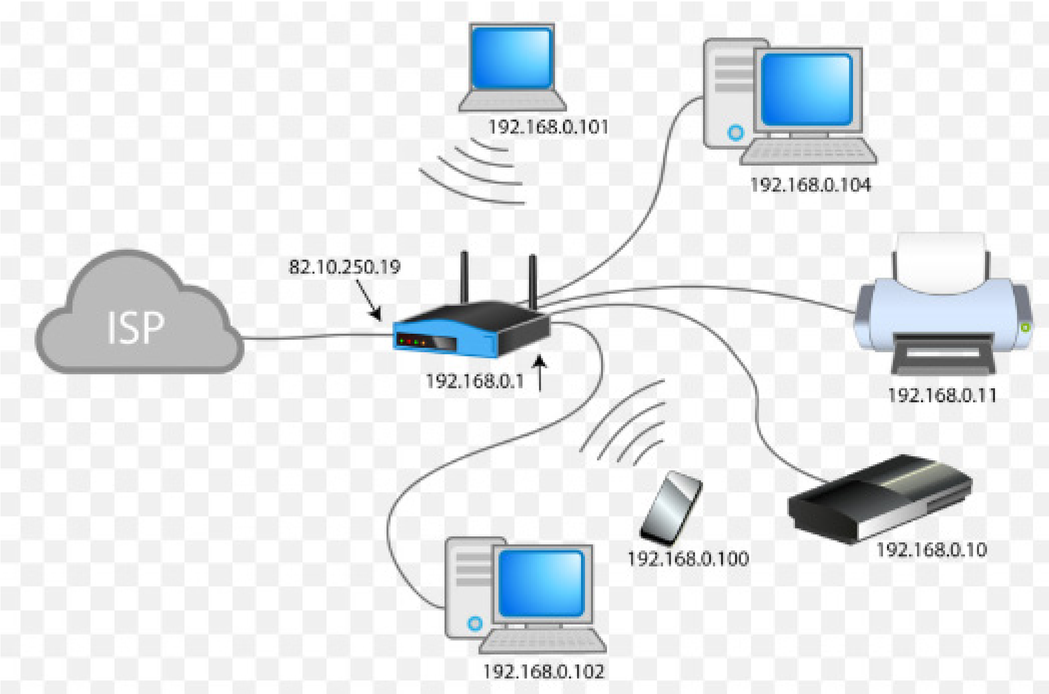
    b.DPI filtering is able to block domain names, malware, spam, or other identifiable elements in the payload of a communication.

6. Next Gen Firewall: A next-gen firewall is a multifunction device (MFD) composed of several security features in addition to a firewall; integrated components can include an IDS, an intrusion prevention system (IPS), a TLS/SSL proxy, web filtering, QoS management, bandwidth throttling, NATing, VPN anchoring, and antivirus.

Bastion Host: Hardened Server (Takes all abuse)

Screened Subnet: Area between 2 firewalls

Network Address Translation (NAT): Purpose of NAT is to hide internal IP address {Layer 3}



Domain 4: Network Security

Internal IP Address Ranges:

10.x.x.x (Class A)
172.16.x.x-172.31.x.x (Class B)
192.168.x.x (Class C)

Port Address Translation (PAT): Allows many internal IP address to share one Public IP address.
Disadvantage: Single Point of Failure

1. State full NAT: Maintains the information of the session between clients and external systems
2. Static NAT: ONE internal IP maps to specific external IPs.
3. Dynamic NAT: multiple internal IP maps to few external IP. (Many to Many)

Automatic Private IP Addressing (APIPA) aka Link Local address assignment: Assigns IP address to system in case of DHCP failure.

Loopback address ---> Used for Software entity (127.x.x.x)

Circuit Switching: Dedicated channel is created between 2 communicating parties. Once the connection is established, link remains the same (consistent connection). All data follows the same path. PSTN, ISDN, DSL, T-carriers

Disadvantages are backdoor, slow, war-dialing.
Defense: Dial-back, Caller ID restriction, user authentication, Modem tone should be after 4 or more rings.

Packet Switching: Message is broken in small segments and each packet search its own way to destination.

Technologies: X.25, Frame Relay, ATM, VOIP, MPLS, cable modems (Very high speed, shared bandwidth)

Domain 4: Network Security

Permanent Virtual Circuit (PVC): Dedicated Lease line. Waiting for customer to send data. (Radio Walkie Talkie)

Switched Virtual Circuit (SVC): Dial-up connection. Connection needs to be established before transmission (Ham Radio)

1. X.25: Uses packet switching. Low performance
2. Frame Relay: PVC uses frame relay packet switching. Uses Committed Information Rate (CIR) which means minimum bandwidth guaranteed. Requires DTE/DCE
3. Asynchronous Transfer Mode: Cell switching (53 byte cells). Connection Oriented packet switching.
4. Switched Multimegabit Data Service: Connectionless packet switching. Connects mul tiple LAN to MAN or WAN

Specialized Protocols:

1. Synchronize Data Link Control (SDLC): Permanent Physical connection for mainframe. Uses polling (Layer 2)
2. High-level Data Link Control (HDLC): supports full duplex, PPP. Uses polling (Layer 2)
3. High Speed Serial Interface (HSSI): Uses DTE/DCE. Defines how multiplexors and rout ers connect to high speed network carrier

Multiplexor ---> Transmits multiple signals over single line.

*A data circuit-terminating equipment (DCE) is a device that sits between the data terminal equipment (DTE) and a data transmission circuit. Usually, the DTE device is the terminal (or computer), and the DCE is a modem.

WAN Technologies:

- LAN: High speed. Small Physical area
- WAN: Used to connect LAN’s. Generally slow using serial links
- MAN: Connect sites together within a medium range (city)

Domain 4: Network Security

1. Dedicated Line: Reserved for specific customer. (Digital signal Level 0/1/3, Cable Mo dem)
2. Non Dedicated Line: Connection needs to be established before transmission. (DSL, ISDN)

Integrated Service Digital Network (ISDN): A fully digital telephone network that supports both voice and high-speed data communications.

- Basic Rate Interface (BRI): 2 B channels and 1 D channel
- Primary Rate Interface (PRI): 23 B channels and 1 D channel (Not for personal use)

*Exam tip: Asymmetric Digital Subscriber Line (ADSL) faster than ISDN

MPLS: Multi-Protocol Labeled Switching (Layer 3) --> Cost effective, provides QoS for VOIP, more secure than public network as it can create a VPN.

VOIP: Voice over IP --> Converts analog to digital signals. No security (lacks authentication mechanism leading to Toll fraud).
Security issues for VOIP: Eaves dropping, vishing, SPIT
Performance issues: Latency (Fixed delay), Jittering (Variable delay)

General Wireless Concepts: Wireless communications employ radio waves to transmit signals over a distance.

Spread Spectrum: communication occurs over multiple frequencies at the same time. A message is broken into pieces, and each piece is sent at the same time but using a different frequency.
Frequency Hopping Spread Spectrum – Sent in Series
Direct Sequence Spread Spectrum – Sent in Parallel
Orthogonal Frequency Division Multiplexing – Signals are perpendicular

Domain 4: Network Security

Wireless Component:

802.11 Family

1. 802.11 a : 54 Mbps/ 5 GHz/ 8 channels
2. 802.11 b : 11 Mbps/ 2.4 GHz (same as home network)
3. 802.11 g : 54 Mbps/ 2.4 GHz
4. 802.11 n : 200+ Mbps/ 2.4 GHz or 5 GHz
5. 802.11 ac : 1 Gbps/ 5GHz

*Exam tip: The b/g/n amendments all use the same frequency, so are backwards compatible

Wireless Security Issues:

- Unauthorized access
- Sniffing
- War Driving
- Unauthorized Access Points (MITM)
- Air Snarfing (Wireless Sniffing)

Transmission Encryption:

1. Wired Equivalent Protocol (WEP)
   a. Shared Authentication Passwords
   b. Weak Initialization vector (24 bits)
   c. IV transmitted in clear text
   d. RC4 (Stream Cipher)
   e. Easily crack able
   f. Only option for 802.11 b
2. Wi-Fi Protected Access (WPA)
   a. Stronger IV
   b. Introduced Temporal Key Integrity Protocol (TKIP)
   c. Still uses RC4
3. WPA 2
   a. AES (Block Cipher)
   b. CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
   c. Not backward compatible
   Uses 802.1X/EAP authentication to have individual passwords for individual users.

Domain 4: Network Security

Bluetooth

- Discovery Mode should be disabled
- Automatic pairing should be turned off

○ Attacks:

§ Blue Jacking --> Sending SPAM

§ Blue Snarfing --> Copies information of the remote device

§ Blue Bugging --> More serious. Allows full use of phone, make call and can eaves drop on calls.

Li-Fi

- LiFi, which stands for Light Fidelity, is a wireless communications technology that uses visible light to transmit data in real time. It is up to 100 times faster than standard Wi-Fi.
- LiFi is a mobile wireless technology that uses light rather than radio frequencies to transmit data. The technology is supported by a global ecosystem of companies driving the adoption of LiFi, the next generation of wireless that is ready for seamless integration into the 5G core.
- Though it has short range as light cannot cross walls but its immune to electromagnetic interference which was common in radio frequency communications.

Zigbee

- Wondering how smart bulbs, cameras, smart appliances talk to each other? Its challenging to sync up all the smart devices as it requires a common protocol to bind together from different manufacturers.
- Zigbee is the answer to this problem. Zigbee uses the IEEE's 802.15.4 personal-area network (PAN) standard to communicate with other Zigbee devices. These can talk up to a maximum range of 300+ meters with a clear line of sight, which works out to between 75-100 meters indoors with obstacles such as walls.
- Ensure the network is isolated, properly encrypted and hardened to achieve maximum security.

Domain 4: Network Security

Secure Communication and Network Attacks

1. Simple Key Management for IP (SKIP): Layer 3. Protect session less datagram protocol. Replaced by IKE
2. Software IP Encryption (SwIPe): Layer 3 P A I N (remember Privacy, Authentication, Integrity, Non-repudiation from Domain 3)
3. Secure Remote Procedural Call: Authentication service. Prevents unauthorized code execution remote system.
4. SSL: Protect communication between web server and web browser
5. TLS: Similar to SSL. (stronger authentication and encryption protocols). Supports 2-way authentication using digital certificate.

    ----> can be implemented at layer 3 (Open VPN)

    ----> can encrypt UDP and Session Initiation Protocol (SIP)
6. Secure Electronic Transaction: Uses RSA & DES used to secure credit card transaction

Authentication Protocol:

1. Challenge Handshake Authentication Protocol: Used over Point to Point Protocol (PPP). Encrypts userID and passwords. Protects against replay attack. Reauthenticates.
2. Password Authentication Protocol: Transmits userID and password in clear text. Just transports credentials.

    *Exam tip: There are no attacks against PAP as everything is in cleartext.
3. Extensible Authentication Protocol: This is a Framework for authentication which can be incorporated with any type of authentication.

    a. Protected EAP: EAP itself doesn't provide any security so it encapsulates EAP in TLS tunnel.

    b. Lightweight EAP: Cisco Proprietary but it was broken with ASLEAP attack.

Secure Voice Communication (VOIP)

Attacks:

- VOIP Phishing and Spam over internet telephony (SPIT)
- Host OS attacks and DDoS attacks
- MitM
- VLAN and VOIP hopping

Domain 4: Network Security

Direct Inward System Access (DISA): Used to manage external and internal access to PBX systems but was exploited by phreakers

- Black Box: Manipulate line voltage
- Red Box: Makes a sound of coin
- Blue Box: Generates 2600 Hz tone
- White Box: Dual tone mobile frequency (DTMF) - control over phone

Manage Email Security (X.400)

1. POP3: Downloads emails from the server
2. IMAP: Gives option to user if they want to download or simply delete from the server

Security Goals: **P A I N**
*Exam tip: Spamming, mail bombing are some common issues which are hard to stop as addresses are spoofed.

Solutions:

1. Secure Multipurpose Internet Mail Extension (S/MIME): **P A ~~I N~~**
    a. X.509:
        i. Signed: **~~P~~ A I N**
        ii. Enveloped: **P A I ~~N~~**
2. MIME Object security Services (MOSS): Uses RSA, DES and MD2/MD5 (**P A I N**)
3. Privacy Enhanced Email (PEM): Uses RSA, DES and X.509 (**P A I N**)
4. Domain Key Identified Mail (DKIM): Email validity is performed if it has been sent through domain name
5. Pretty Good Privacy: Uses International Data Encryption Algorithm (IDEA) {PGP is a good IDEA}

Fax security: Fax encryptors, Link encryptors, activity logs and exception reports.

Domain 4: Network Security

Remote Access Security Management

Client Based:

- Using modem to Dial up
- Internet through VPN

Terminal Server:

- Connecting to terminal server

*Exam tip: POTS/PSTN can be used as back up of broadband failure

Remote Access Techniques:

1. Service Specific: Connect and interact with one service
2. Remote Control: Remotely connecting a system
3. Screen Scraper/scraping: Screen at target machine is showed to remote user.
    a. Scraping: tool to interact with human interface
4. Remote Node Operation: Dial up connectivity

Remote connectivity technology: DSL, ISDN, Modem, Satellite

Transmission Protection: VPN, TLS, SSL, SSH, L2TP, IPSeC

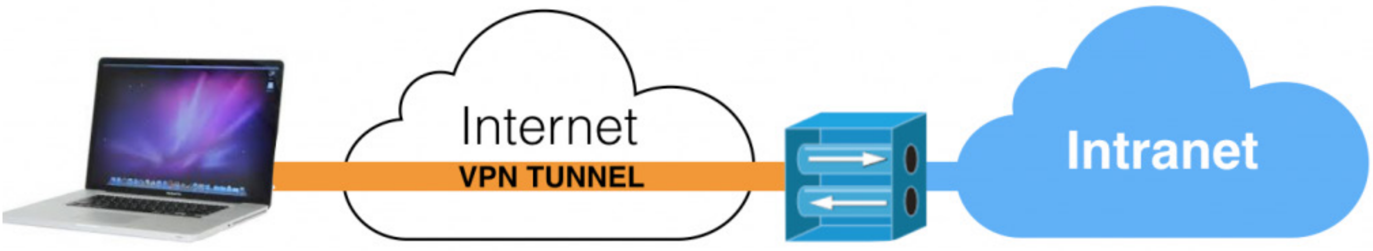
Authentication Protection: EAP, PAP, CHAP, RADIUS, TACACS+

Remote User Assistance:

1. Dial-up protocol
    a. PPP: Full Duplex. Uses CHAP and PAP. Allows multi-vendor interoperability. Replaces SLIP.
    b. SLIP: Provides no error correction/detection

2. Centralized Remote Authentication
    a. RADIUS
    b. TACACS+
3. Virtual Private Network (C I A)

Domain 4: Network Security



Tunneling: Think about sending email through post. Data inside cannot be read using SSL or TLS. Uses more than one protocol at a time.

Common protocols: PPTP, L2TP, L2F, IPSeC

Protocol	**Authentication**	**Data Encryption**	**Protocols**	**Dial-up**	**# of connection**
PPTP	Yes	No	PPP	Yes	Point to Point
L2F	Yes	No	PPP/SLIP	Yes	Point to Point
L2TP	Yes	No	PPP	Yes	Point to Point
IPSec	Yes	Yes	IP	No	Multiple

IPSec

- Authentication Header (**~~P~~ A I N**)
- Encapsulating Security Payload (**P A I ~~N~~**)

Note: ESP also provides some limited authentication, but not to the degree of the AH.

Virtual LAN: Logically segment a network without altering physical topology.

Virtualization: Guest OS running on single OS. Hypervisor is a component used for virtualization.

*Exam tip: Scalability, quick recovery are few advantages of virtualization. However, threats like malicious codes which compromise virtual OS are also there.

Domain 4: Network Security

Virtual Desktop Technology

- Remote Access
- Larger Display
- Extension of virtual application concept.

Virtual Networking

- Storage Area Network
- Software Defined Network (makes organization vendor independent)

Virtual Extensible LAN (VXLAN)

Datacenters have rapidly increased their server virtualization over the past decade, resulting in dramatic increases in agility and flexibility. Virtualization of the network and decoupling the virtual network from the physical network makes it easier to manage, automate, and orchestrate.

VXLAN is a technology that allows you to segment your networks (as VLANs do) but also solves the scaling limitation of VLANs and provides benefits that VLANs cannot.

- You can theoretically create as many as 16 million VXLANs [24 bit VNID] in an administrative domain (as opposed to 4094 VLANs [12 bit VNID]).
- You can enable migration of virtual machines between servers that exist in separate Layer 2 domains by tunnelling the traffic over Layer 3 networks.
- It allows you to dynamically allocate resources within or between data centers without being constrained by Layer 2 boundaries or being forced to create large or geographically stretched Layer 2 domains.

SD-WAN

Software Defined WAN or SD-WAN is the technology which simplifies the management and operation of WAN technologies by decoupling the control plane and data plane very similar to SDN. The existing WAN technology requires expensive ways (like MPLS) to connect the Head Quarters to Branch offices. SD-WAN products are designed to address these issues by replacing the traditional networking devices with virtualization appliances making it possible for organizations to become vendor independent, simplify the configuration and choose less expensive solutions.

Domain 4: Network Security

Security Control:

1. Transparency: Invisible to user
2. Verify Integrity: Hashing
3. Transmission Mechanism: Logs the transmission records (auditing)

Security Boundaries: A security boundary is the line of intersection between any two areas, subnets, or environments that have different security requirements or needs.

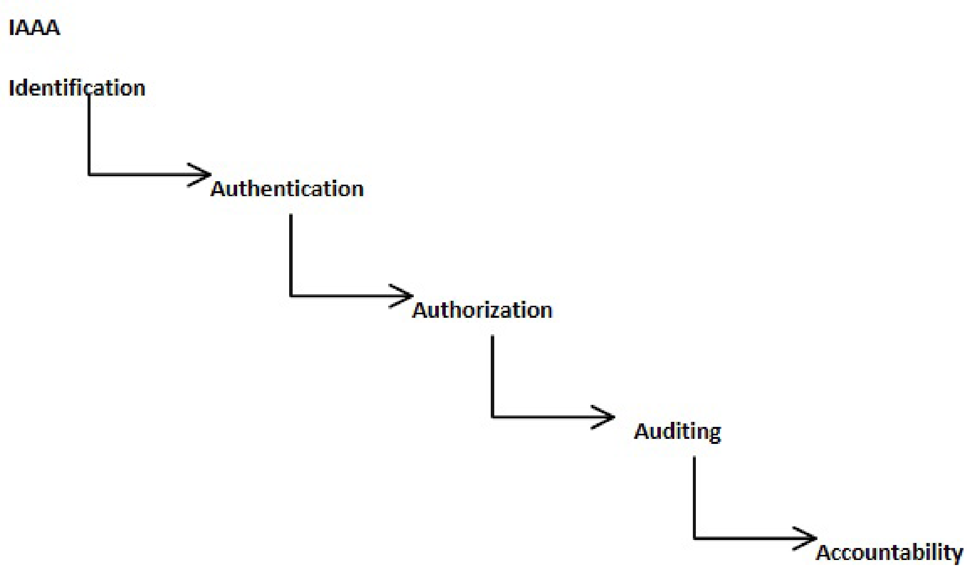
It is created with the help of classification, logical boundaries.

Network Attack:

Attack	Countermeasure
DDoS	Firewall, third-party vendor, load balancer, null route
Eaves Dropping	TLS, SSH
Impersonation/ Masquerading	One Time Pads/Token Authentication
Replay Attacks	One Time Authentication
Modification Attack	Digital Signature, Packet checksum, verification
ARP spoofing	Monitoring ARP cache, IDS
Hyperlink Spoofing	Verify the hyperlink before clicking

DNS Poisoning, Spoofing and High Jacking (Pharming) : Also known as resolution attacks.
Poisoning: IP address resolves to malicious DNS
Spoofing: Attacker sends false replies instead of DNS server.
The resolution is to keep upgrading DNSSEC.

Domain 5: Identity and Access Management



Identification: User should be uniquely Identified

Authentication: Validation of an entity's identity claim

Authorization: Confirms that an authenticated entity has the privileges and permissions necessary.

Auditing: Any activity in the application/system should be audited (Identify technical issues/ Breaches)

Accountability: Tracing an action to a subject

Identity & Authentication is must for accountability but not authorization.

Domain 5: Identity and Access Management

Type1: Something you know (password, pin)

Type2: Something you have (smart card, token)

Type3: Something you are (biometric)

Type4: Somewhere you are (location)

Passwords are not stored in clear text. It is hashed using algorithm such as Password Based Key Derivation Function 2 (PBKDF2)

**Retina scans are the most accurate form of biometric as it scans the blood vessel behind the eyes. Although it's not acceptable as it reveals the health condition of the person (BP, Pregnancy). It needs to be protected as it contains PHI details.

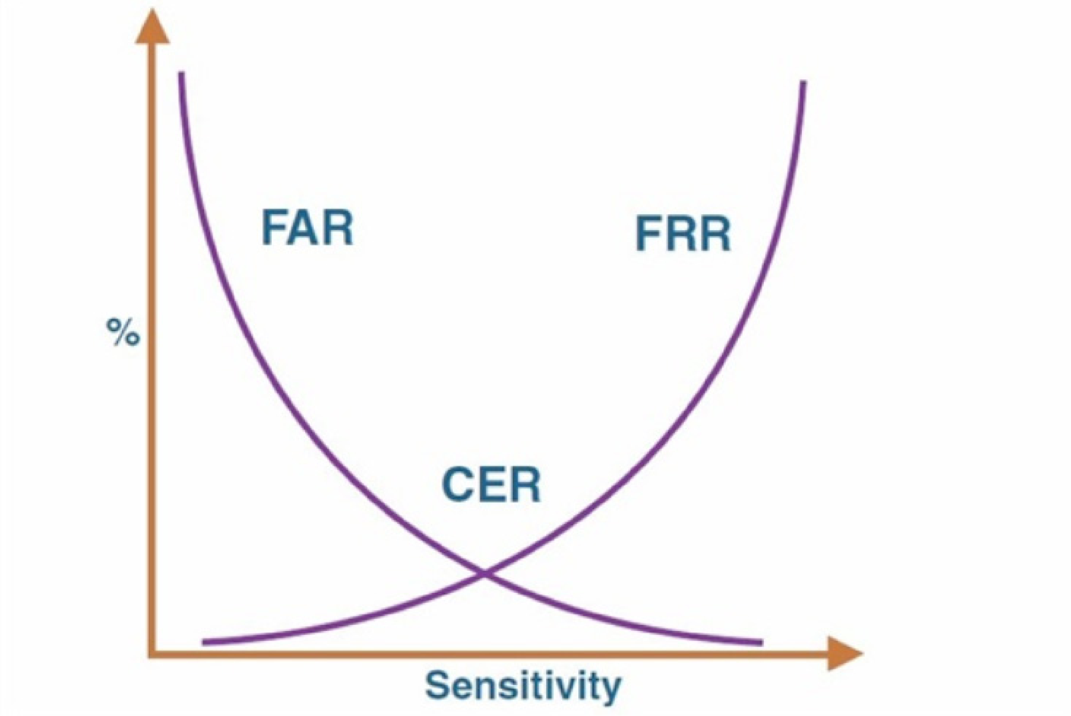
**Iris Scan is the second best and mostly accepted form of authentication.

Type1 error: False Rejection Rate (FRR)

Type2 error: False Acceptance Rate (FAR)

Cross over error rate (CER): It’s the meeting point of FAR and FRR

*Exam tip: Type 2 Error is FAR from Type 1 error



*Exam tip: For Biometric Authentication, ENROLLMENT must take place first. Enrollment time over 2 mins is unacceptable

Domain 5: Identity and Access Management

Throughput time: Amount of time taken for a biometric device to scan the subject.

NOTE: Where BYOD is allowed, device registration is must.

Identity Management:

a. Centralized---> SSO, Directory Service

b. Decentralized

Identity Assurance Level: Identity Assurance Level (IAL) refers to the identity proofing process. A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.
IAL 1: If any are self-asserted or should be treated as self-asserted.
IAL 2: Either remote or in person identity proofing is required. It requires identity proofing to have been verified in person or remotely.
IAL 3: In person identity proofing is required. Identifying attributes must be verified by the authorized Credential Service Provider (CSP) representative through examination of physical documentation.

Smart Cards & Tokens:

Smart Card: A credit-card sized ID/badge that has integrated circuit chip embedded in it which is used for identification and/or authentication. (Mostly used as Multi-Factor Authentication)

Tokens: A password generating device which users can carry with them. This authentication method can be used along with other factor (password).

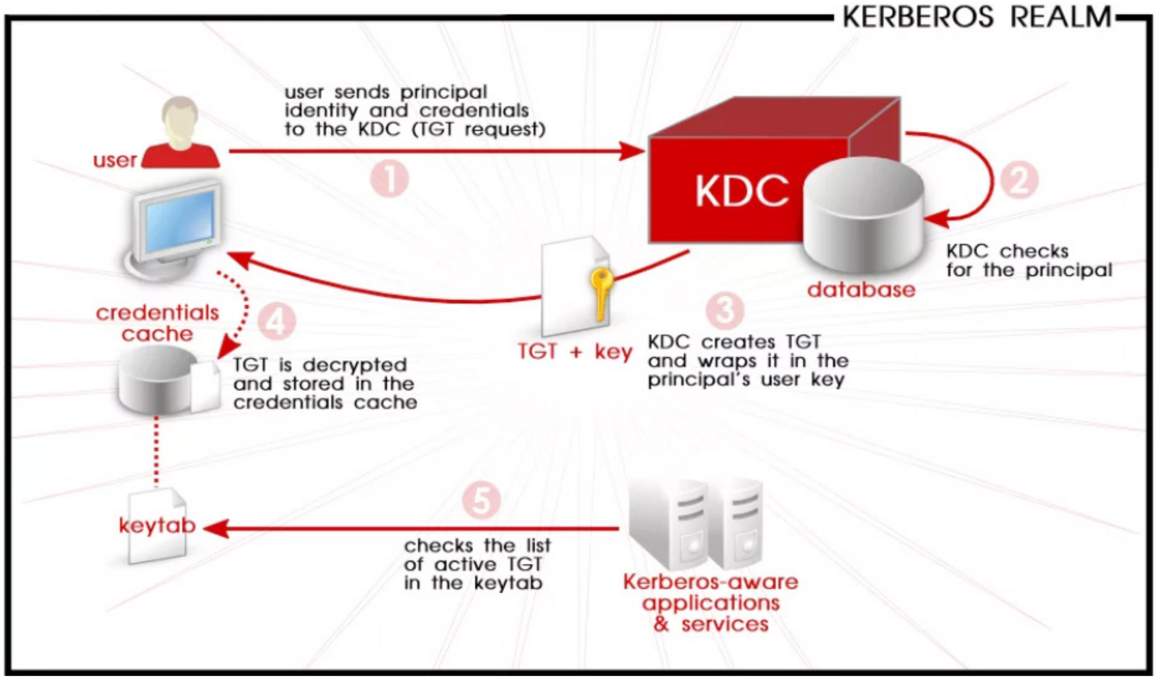
1. **Synchronous Password Tokens:** Hardware tokens that create synchronous dynamic passwords are time-based and synchronized with an authentication server. They generate a new password periodically, such as every 60 seconds.

2. **Asynchronous Password Tokens:** Generates password based on algorithm and an incrementing counter. it creates a dynamic onetime password that stays the same until used for authentication.

Domain 5: Identity and Access Management

Kerberos

1. Key Distribution Centre: The KDC is the trusted 3rd Party that provides authentication services. Kerberos uses symmetric key cryptography to authenticate clients to servers. All clients and servers are registered with the KDC, and it maintains the secret keys for all the members.
2. Authentication server: It verifies or rejects the authenticity and timeliness of tickets.
3. Ticket Granting Ticket: TGT provides proof that a subject as authenticated through a KDC and is authorized to request tickets to access other objects. TGT is encrypted and includes symmetric key, expiration time and the user's IP address. Subjects present TGT while accessing the Object.
4. Ticket: Ticket is an encrypted message that provides proof that a subject is authorized to access an object.


KERBEROS REALM
user
user sends principal identity and credentials to the KDC (TGT request)
1
KDC
2
KDC checks for the principal
database
3
KDC creates TGT and wraps it in the principal's user key
TGT + key
credentials cache
4
TGT is decrypted and stored in the credentials cache
keytab
5
checks the list of active TGT in the keytab
Kerberos-aware applications & services

1. 3rd Party Authentication (version 5 is the latest)
2. Provides confidentiality and Integrity
3. Uses Symmetric Key Cryptography (AES) to encrypt the ticket granting ticket.
4. KDC is the single point of failure

Domain 5: Identity and Access Management

Pass the Hash (PtH)

A Pass-the-Hash (PtH) attack is a technique whereby an attacker captures a password hash (as opposed to the password characters) and then simply passes it through for authentication and potentially lateral access to other networked systems. Although it affects almost all the platforms but mostly in Windows.

In order to succeed, the attacker has to gain local administrative rights.

- Principle of Least Privilege
- Password Management solution (frequent rotation/challenge response)
- Separation of privileges

Federated Identity Management & SSO

Organizations share the credentials within federated domain. It uses SAML (Security Assertion Markup language) and SPML (Service Provisioning Markup Language).

**Exam tip: Think about booking a flight for your holidays and you get an option to book hotel on the same site. The moment you login to hotel site, it won't ask for your credentials again as the site for flight booking and hotel booking are under Federated Domain.*

SAML: Based on XML and is used to exchange authentication & Authorization between federated organization.

SPML: Based on XML specifically designed for exchanging user information for federated identity single sign on purposes.

XACML: Extensible Access Control Markup Language is used to define access control policies within an XML format and it commonly implements RBAC.

Other SSO methods:

a. Scripted Access: Establish communication links by providing an automated process to transmit logon credentials at the start of logon session.

b. SESAME: Secure European System for Application in a Multivendor Environment, implemented to overcome the weakness of Kerberos. New version of Kerberos superseded.

c. Krypto knight: Time based authentication system by IBM

d. Open ID & OAuth: OpenID is for authentication and OAuth is for authorization.

**Exam tip: SAML is for enterprise use and OAuth is for commercial use (by us)*

Domain 5: Identity and Access Management

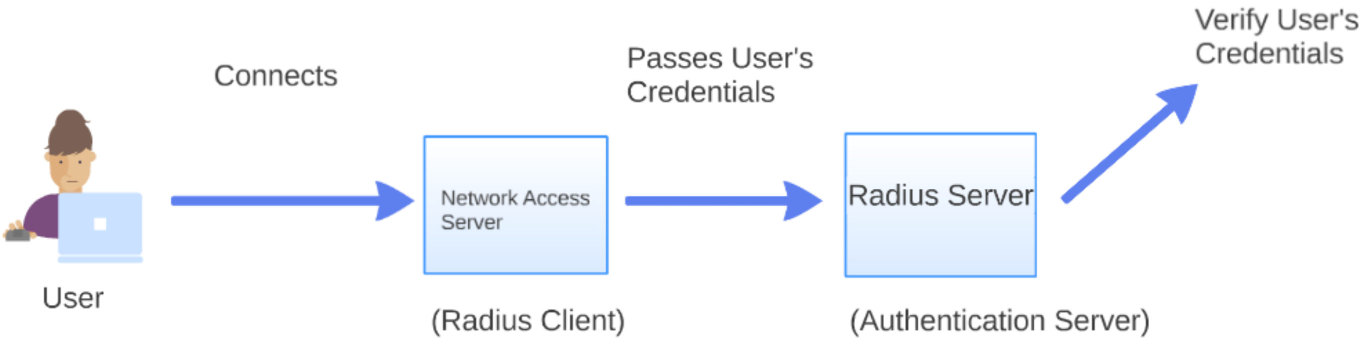
Credential Management: Place to store credentials in encrypted format (mainly when SSO is not working)

IdaaS (Identity as a Service): e.g. Google, login to google once and use multiple google products without authenticating. Okta is an example for IdaaS.

Just in time Access

- Using the just-in-time (JIT) access methodology, organizations can give elevate human and non-human users in real-time to provide elevated and granular elevated privileged access to an application or system in order to perform a necessary task.
- It ensures that access is granted only when a subject is about to access instead giving implicit access.
- It helps organizations improve their overall cybersecurity posture by significantly reducing the risk of privileged access abuse and lateral movement by threat actors. Significant approach towards implementing Zero Trust Architecture.

AAA protocols: Protocols that provide Authentication, Authorization and Accounting are referred as AAA protocols. These provide centralized access control with remote access systems such as VPN. Common protocols are RADIUS, TACACS+ and Diameter.



RADIUS: Remote Authentication Dial-in User Services is a centralized authentication service for remote connection. RFC 2865. Uses UDP on Port 1812.

TACACS+: Terminal Access Controller Access Control System was introduced as an alternative to RADIUS. CISCO introduced extended TACACS (XTACACS). TACACS+ was created as open public documented protocol and most commonly used among three. Uses TCP on Port 49.

Domain 5: Identity and Access Management

RADIUS

- Uses UDP in transport layer. Must have extra code to detect transmission errors.
- It encrypts only password while communicating between RADIUS client & server. User ID and sessions are sent in clear text and vulnerable to Replay attack.
- Combines AAA
- Appropriate for simple environment like ISP.
- Supports IP only.

TACACS+

- Uses TCP and does not need any extra precaution.
- It encrypts everything.
- Separates AA & A
- Used for more sophisticated environment like corporate.
- Supports IP, Apple, NetBIOS, Novell, X25

Diameter: Enhanced version of RADIUS. Not backward compatible. Supports wide range of protocols (IP, mobile IP, VOIP). Uses TCP on port 3868 or Stream Control Transmission Protocol (SCTP) Port 3868. Supports IPSec and TLS.

Authentication

a. PAP, CHAP, EAP

b. End to End protection

c. Replay attack protection

Authorization

a. Redirect secure proxies

b. State reconciliation

c. Re-Auth on demand

Auditing

a. Reporting & event monitoring.

Domain 5: Identity and Access Management

Permission: What can you do with your access (READ, RW etc.)

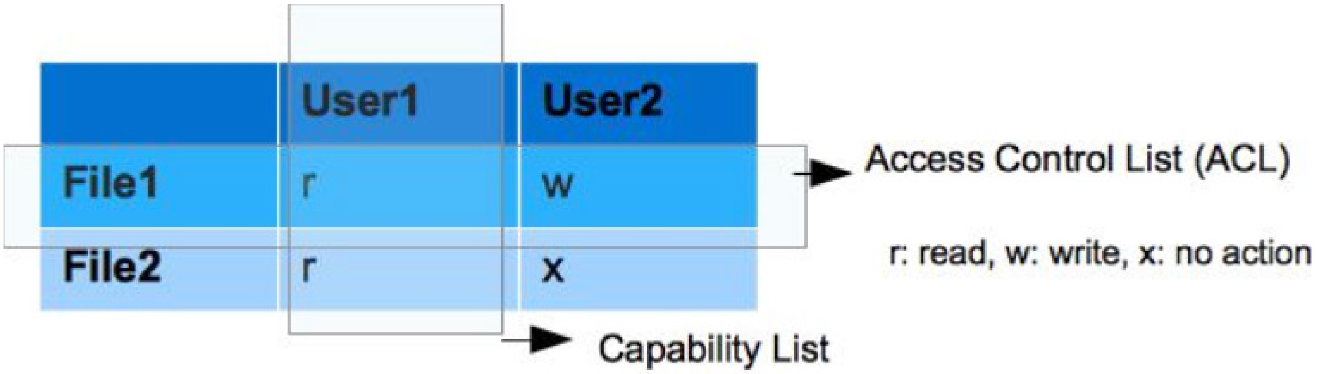
Rights: Ability to take action on the object (changing system time)

Privilege: Combination of permission and rights

Implicit Deny: Access is denied unless explicitly granted (Deny All).

*Exam tip: Implicit deny should be a default configuration for any component.

Access Control Matrix:



	User1	User2
File1	r	w
File2	r	x

Access Control List (ACL)

r: read, w: write, x: no action

Capability List

Access Control List: Object Focused

File1: ((read, {user1}), (write, {user2}))

File2: ((read, {user1}), (write, {}))

Capability Table: Subject Focused

User1: ((read, {file1,file2}), (write, {}))

User2: ((read, { }), (write, {file1}))

Constrained Interface: Access control on interface. E.g. Access to modify would be visible, however, it would be greyed out if not authorized.

Content Dependent: Database Views. Depends on the content of the Object

Context Dependent: Require specific activity before granting access. E.g. Payment needs to be made before downloading online media.

Domain 5: Identity and Access Management

Need to know: Access granted only to data resources they need to perform. (Permission)

Least Privilege: Access granted to the privileges necessary to perform an assigned task. (Security clearance)

Separation of Duties: No single person is allowed to perform end to end critical task alone. (Preventive control)

Threat Modelling

It's a security process where potential threats are identified, categorized and analyzed.

Proactive Measure: Design and development
Reactive Measure: Once the product has been deployed

Goal: (a) To reduce the number of security related design and coding defects
(b) To reduce the severity of any remaining defects

Overall result is reduced risk
Identifying Threats:

1. Focused on Assets - Identify threats on valuable assets
2. Focused on attackers - Identify potential attackers and their goals
3. Focused on Software - Potential threat against developed software

Risk Management Process:

a. Identify Assets
b. Identify Vulnerability
c. Identify Threat and see if it can exploit the vulnerability
d. Calculate Risk
e. Identify Control

Access Aggregation Attack: User gather chain of less sensitive information and aggregate it to make more sensitive information.

Domain 5: Identity and Access Management

Access Control Models:

1. **Discretionary Access Control**: Owner, creator or custodian define access to the objects. Uses Access control list (known as Identity based access control)
2. **Non-Discretionary Access Control**: Centrally managed by administrators. (Hint: Any model which is not DAC, can be called as Non-DAC)
3. **Role Based Access Control**: Access is defined based on the role in an organization and subjects are granted access based on their roles. Normally it is implemented in the organizations with high employee turnover.
4. **Rule Based Access Control**: There are set of rules. e.g. Firewall. Global rules are applied to all users equally.
5. **Mandatory Access Control (Lattice Based)**: Implemented in high secure organizations such as Military. It is compartment based.
   a. **Hierarchical** - Clearance of Top secret gives access to Top secret as well as Secret
   b. **Compartmentalized** - Each domain represents a separate isolated compartment.
   c. **Hybrid** - Combination of both
6. **Attribute Based Access Control**: Rules that can include multiple attributes. e.g. working hours, place of work, type of connection etc.
7. **Risk Based Access Control:** Risk-based Access Control uses real-time intelligence to gain a holistic view of the context behind each login. When a user attempts to sign in, a risk-based authentication solution analyses factors such as:

•Device. Is the user on a known computer? Or is the user on a mobile device that has never logged in before?
•Location. Is the user in the same building that houses the server? Or is the person in another time zone?
•Network. Is the person logging in from a familiar IP address? Or is that data foreign?
•Sensitivity. Is the requested file crucial for the company? Or is it a relatively unimportant piece of information?

Based on all of these factors, the system makes a decision. The user can either:
•Enter normally. The person uses a familiar system, such as a password, to gain access.
•Offer proof. The person must provide some other form of verification to gain entry.

Domain 5: Identity and Access Management

Advanced Persistent Threat: Advanced Persistent Threat (APT) is referred to the group of hackers who are highly skilled and motivated who would not give up until they successfully breach the system. Most of the times, they are government sponsored attacks.

Common Access control attacks:

1. **Access Aggregation attacks**: Collecting several non-sensitive information and combining them to make sensitive information. Need-to-know and least privilege are the common countermeasure for this attack.

2. **Password attacks**: Password is considered as the weakest form of authentication and easiest form of password attack is to just guess them. It is always good practice to keep your password long and with the combination of alpha-numeric, upper case, lower case and special character.

3. **Dictionary attack**: Dictionary attack is an attempt to discover your password by using every possible word present in the dictionary and compare against your credentials. It also combines the upper-case and lower-case while attacking. The best way to prevent this attack is to avoid common dictionary words as your password.

4. **Brute Force Attacks**: Brute force attack is when there is an attempt to discover password by using all the possible combination of letters, numbers and symbols. It is also called as the last resort of the hackers. However, this attack is going to take a long (very, very long) time to identify the actual password. However, considering the computing capabilities and increase in processing power, brute force is able to gain momentum. It is always advisable to keep your passwords long and complex to deter the brute force attack as it requires cost and computing powers.

5. **Birthday attacks**: It's a type of password attack which focuses on finding collision (hash values).

6. **Rainbow Table Attacks**: If an attacker successfully gains access to password file/database, it might not still be useful as the passwords are hashed. Rainbow table helps in comparing the hashes against the database of precomputed hash which reduces the time and effort for the attacker. The best way to protect this attack is to salt your hashes to add randomness.

Domain 5: Identity and Access Management

7. **Sniffer Attacks**: Sniffing is a technique referred to look into the packets which are being sent over the network. Wireshark is a common tool which does that. Best way to protect against this type of attack is encryption.
(*Exam tip: TLS 1.2 is a technique to encrypt data in transit)

8. **Spoofing Attacks**: Also known as masquerading attacks, is a technique when an attacker pretends to be someone else. Most common techniques are email spoofing, caller ID spoofing, IP address spoofing. This is done to conceal the real identity and impersonate as someone or something else. Best method to protect yourself from spoofing attacks is a common saying "Trust, but verify"

9. **Social Engineering attacks**: Social Engineering is referred to a technique where attacker doesn't have to apply any technical knowledge to attack a system or a person. e.g. best way to hack a password is to simply ask for it. Common examples are phishing attacks. Countermeasure is to always verify about the person who he/she is claiming to be.

10. **Phishing**: It is a technique where attacker tricks the victim by sending an email which looks like a legitimate email or through a legitimate source (spoofing email) which contains malformed link. The link will take the user to an infected page (created by attacker) which normally asks for sensitive information like credentials, credit card details etc. It is always recommended to verify the source and be diligent before clicking on any suspicious link.
    a. **Spear Phishing**: When a specific person or group of users are targeted.
    b. **Whaling**: When the target is a CXO or someone who belong to higher management.
    c. **Vishing**: It's a technique referred to trick user over voice call.
    d. **Smishing**: When a phishing attempt is done via SMS.

Summary of Protection Methods

a. Control physical access to systems
b. Control electronic access to files
c. Create strong password policy
d. Hash and salt passwords
e. Use password masking
f. Deploy multi-factor authentication
g. Use account lockout controls
h. Use last logon notification
i. Educate users about security

Domain 6: Security Assessment and Testing

Test Program

SECURITY TEST: verify that a control is functioning properly

SECURITY ASSESSMENT: comprehensive review of the security of a system, application or the tested environment and perform risk assessment, find vulnerabilities and make remediation recommendation.

SECURITY AUDITS: similar to security assessment but it's performed by auditor

	Performed by	**Intended Audience**
Internal Audits	Internal team (Audit staff)	Internal stake holders
External Audits	External Auditors(Big 4)	Internal stake holders, Regulators

CARTE BLANCHE: *Complete Access*

Security Content Automation Protocol

The security community depends upon a common set of standards to provide a common language for describing and evaluating vulnerabilities. NIST provides the community with the Security Content Automation Protocol (SCAP) to meet this need. SCAP provides this common framework for discussion and also facilitates the automation of interactions between different security systems. The components of SCAP include the following:

- Common Vulnerabilities and Exposures (CVE) provides a naming system for describing security vulnerabilities.
- Common Vulnerability Scoring System (CVSS) provides a standardized scoring system for describing the severity of security vulnerabilities.
- Common Configuration Enumeration (CCE) provides a naming system for system configuration issues.
- Common Platform Enumeration (CPE) provides a naming system for operating systems, applications, and devices.
- Extensible Configuration Checklist Description Format (XCCDF) provides a language for specifying security checklists.
- Open Vulnerability and Assessment Language (OVAL) provides a language for describing security testing procedures.

Domain 6: Security Assessment and Testing

VULNERABILITY ASSESSMENTS

VULNERABILITY SCANS: Automatically probe systems weakness which can be exploited by attackers.

a. Network Discovery: discover ports and services

1. TCP SYN Scanning: sends a packet with SYN flag.
   If system responds, its set as SYN ACK
   (Also called as 'Half Open' Scanning)
2. TCP Connect Scanning: opens a full connection to a remote system on a specified port
3. X-Mas Scanning: sends packet with FIN, PSH, URG flags

NMAP is used for N/W discovery

Open: Port is open and application is actively accepting connections

Closed: Port is accessible , no application is accepting connection on that port

Filtered: Unable to determine if port is open or closed

b. Network Vulnerability Scanning: Go deeper than discovery scans (Nessus)
By default, un-authenticated scans are done.
To avoid FPs and FNs, authenticated scans are done.

Important Ports:

FTP – 21
SSH – 22
Telnet - 23
SMTP – 25
DNS – 53
HTTP – 80
POP3 – 110
NTP – 123
HTTPS – 443
MS SQL – 1433
Oracle – 1521
H.323 – 1720
PPTP – 1723
RDP – 3389

Domain 6: Security Assessment and Testing

c. Web Scanning: special purpose tools that probe web applications for known vulnerabilities.

   a. Detection
   b. Validation
   c. Remediation

PENETRATION TESTING: Exploits the identifies vulnerabilities through vulnerability scanner

1. Planning (Scope of the test, Management approval)
2. Information Gathering (Network discovery scan, enumeration)
3. Vulnerability Scanning (Network/Web vulnerability scan)
4. Exploitation
5. Reporting

Breach Attack Simulation

It allows enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means.

WHITE BOX TESTING: knowledge of target (crystal box)
GREY BOX TESTING: partial knowledge of target (partial knowledge test)
BLACK BOX TESTING: no knowledge of target

CODE REVIEW & TESTING

Code Review: must happen (peer review)
Fagan Inspection: Highly restrictive environment where code flaw would be catastrophic
P – Planning
O – Overview
P – Preparation
I – Inspection
R – Rework
F – Follow up

Domain 6: Security Assessment and Testing

1. **STATIC TESTING**: source code analysis
2. **DYNAMIC TESTING**: testing done on runtime . SQL injection & CSRF are identified
3. **FUZZ TESTING**: Different types of inputs are sent to application to test the behavior, stress testing

i. **Mutation** (Dumb) Fuzzing – Previous input values are mutated (changed) and passed to the application

ii. **Generational** (Intelligent) Fuzzing – Develops data model & creates new input.

SYNTHETIC TRANSACTION: Test results are compared against expected result

BIT FLIPPING: Process of slightly changing the input (ZUFF TOOL used for mutation fuzzing)

a. **Interface Testing**
   i. API – Code that interacts with outer world
   ii. User Interface – GUI and Command line
   iii. Physical Interface – Logic controllers

b. **Misuse Case Testing**: Exploiting the software's known risk (Abuse Case Testing)

TEST COVERAGE ANALYSIS: use cases tested / total number of use cases

Website Monitoring:

1. Passive Monitoring Analysis: It analyses actual network traffic sent to a website by cap turing it as it travels over the network or reaches the server. Real User Monitoring (RUM) is one of the variants.
2. Synthetic Monitoring (or active monitoring): performs artificial transactions against a website to assess performance.

IMPLEMENTING SECURITY MANAGEMENT PROCESS

i. **Log reviews**: Should be done periodically (SIEM)

ii. **Account Management**: Privileged account should be reviewed, if they do not have un necessary access (UER)

iii. **Backup Verification**: Process function effectively meets organization's data protection needs

iv. **KPI**: Should be published by management

Domain 7: Security Operations

Primary purpose is to safeguard the information assets

Permission: Am I allowed to access the object? (accessing file)
Rights: What actions I can take on these objects? (changing system time)
Privilege: Permission + Rights

Need to know: Access granted only to data resources they need to perform. (Permission)

Least Privilege: Access granted to the privileges necessary to perform an assigned task. (Security clearance)

Entitlement: Amount of privileges granted to user.

Aggregation: Amount of privileges that user collect overtime.

Transitive Trust: A trust B and B Trust C, then A trust C. (Happens on the domains)

SoD: No single person is allowed to perform end to end critical task alone. (Preventive control)

Collusion: 2 people committing fraud together.

Job Rotation: Movement from one role to another (Detective control)
Mandatory vacation: Sending an employee to vacation. (Detective control)

*Exam Tip: Least Privilege and SoD helps in prevent violation
Monitor helps in Deter or detect violation

Managing Information Life Cycle
Create--->Classify--->Storage---->Use--->Archive--->Destroy

SLA: Financial stipulation is involved
MOU: No financial stipulation is involved. (Same as SLA)

Duress System: Alone guard raises alarm in case of threat or emergency.

Domain 7: Security Operations

Hardware inventory: Should have labels (Barcode, RFD), unused memory devices should be sanitized or destroyed.

Software licensing: Prevents downloading unauthorized applications. Protects piracy.

Protecting Physical Assets: Locks, doors, bollards, CCTV

Depth of Field (Focal Length) ‘f’
Field of view: Entire area is captured by camera lens.

Managing Virtual Assets

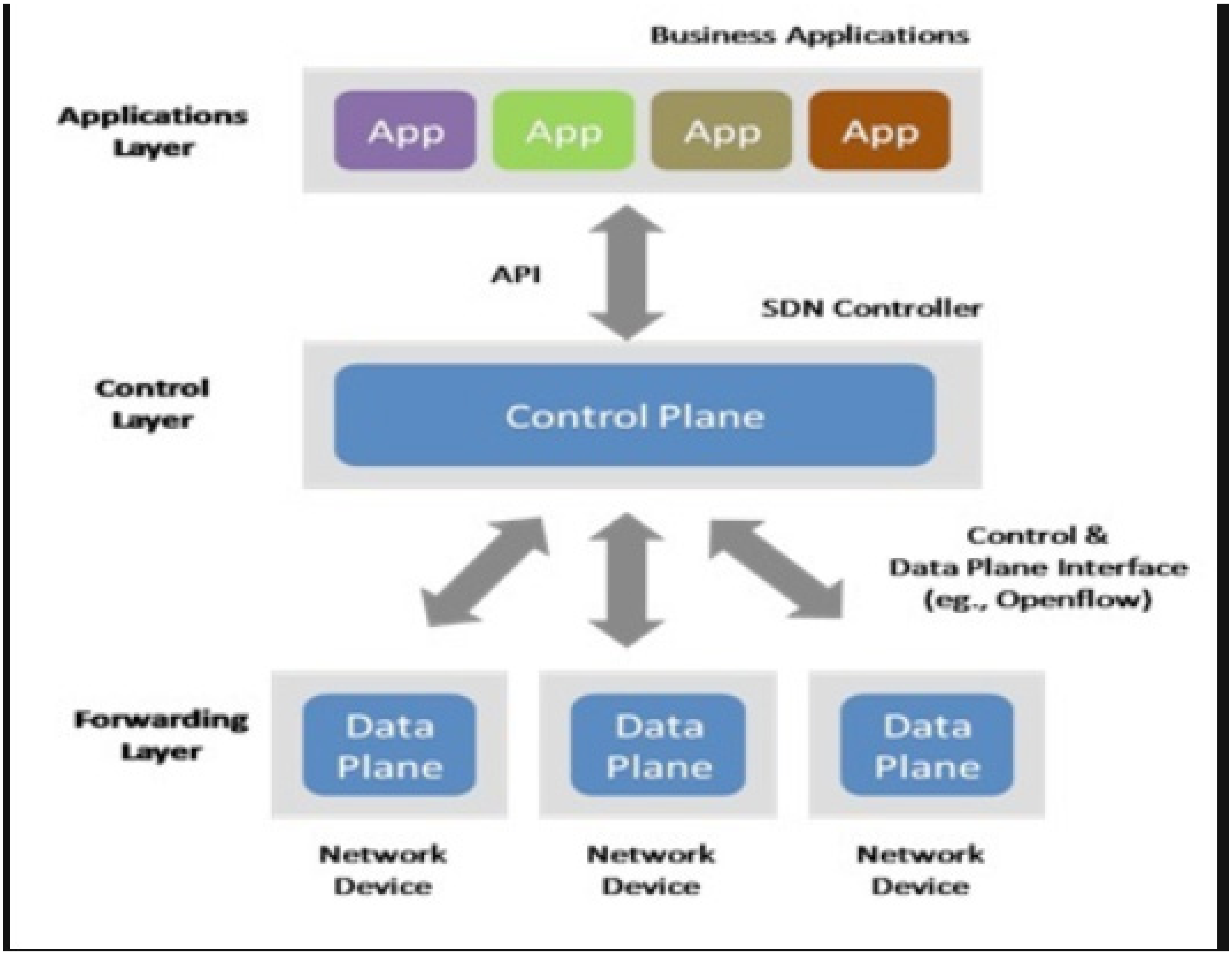
Virtual Machine: Guest OS running on physical machines. (Hypervisor)

Software Defined Network: Decouple control plane from the Data plane

Control Plane: Where to send traffic?

Data Plane: Identifying the path to forward the data

Domain 7: Security Operations

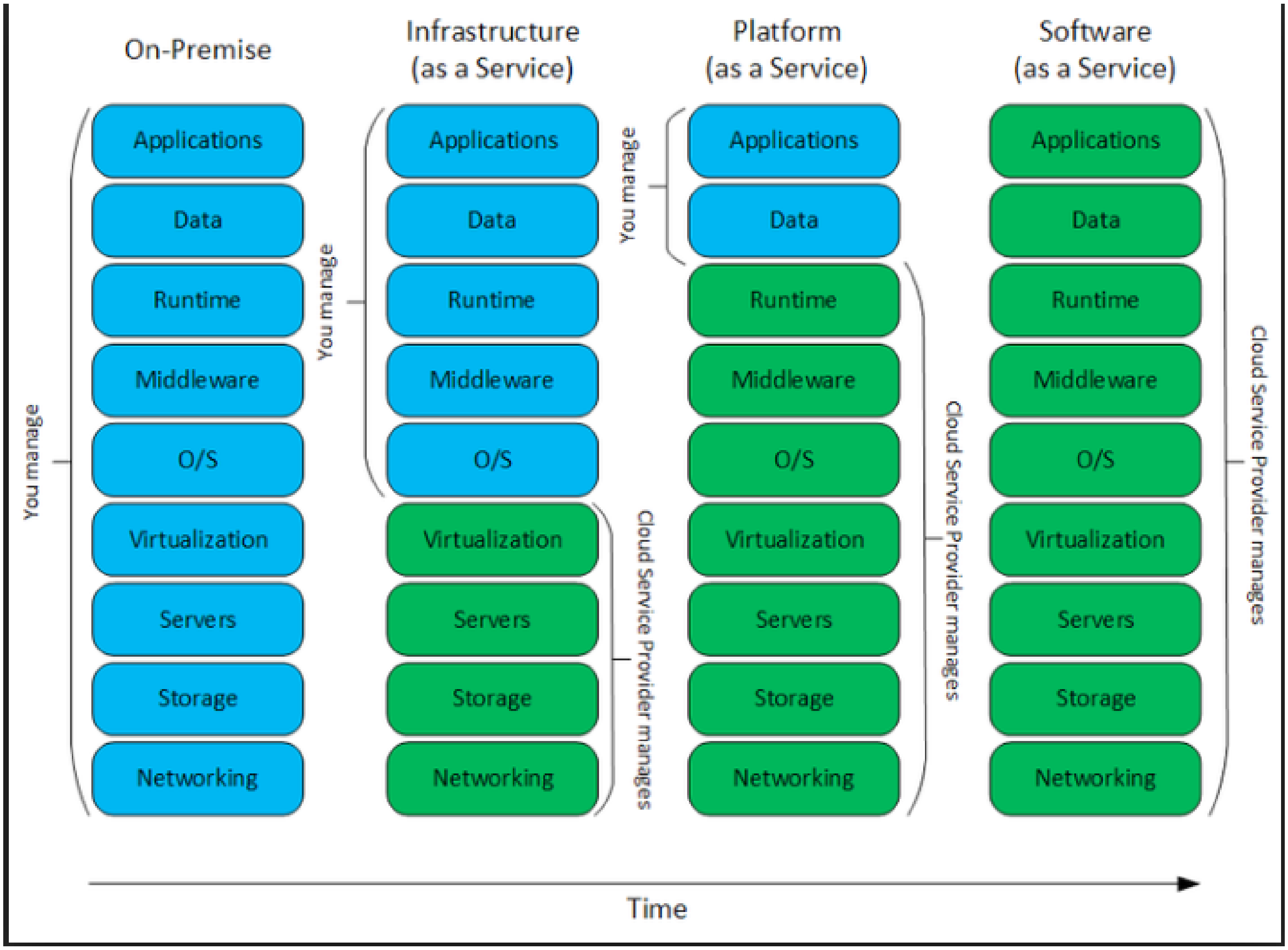


Virtual SAN: High-speed network to Host multiple devices. (Hypervisor is used for virtualization)

Managing Cloud based assets: Risk Management is difficult as resources are outside the direct control.

a. **Software As A Service**: Fully functional applications accessed via browsers. e.g. Gmail, Office 365. Max. responsibility is with CSP.
b. **Platform As A Service**: CSP provides platforms like OS, Hardware. Customer simply builds the applications over those platforms. CSP is responsible for maintenance of underlying infrastructure.
c. **Infrastructure As A Service**: Provides basic computing resources. All the maintenance is performed by the consumers.

Domain 7: Security Operations



Public Cloud: Anyone can rent the services. (Org A uses PaaS, Org B uses SaaS and Org C uses IaaS)

Private Cloud: Services for Single Organization

Community Cloud: Services for 2 or more organizations with similar objectives. (all tenants opting for SaaS)

Hybrid: Public + Private

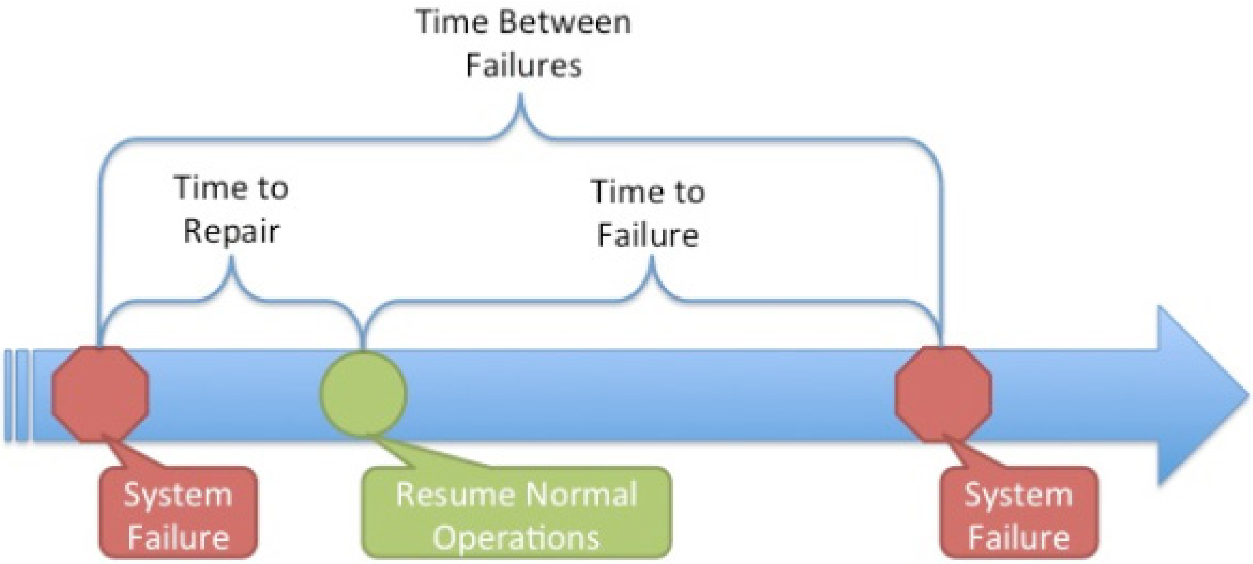
Media Management: 1. Tapes should not be kept in high magnetic field. This can result in degaussing.

2. Always try an restore the data to avoid last minute surprise.
3. Encryption should be done. (AES 256)

Mobile Devices: Screen Lock, Remote Wipe etc.

Domain 7: Security Operations

Differentiating Between Failure Metrics



MTTR, MTTF, MTBF

Baselining ----> New Systems -----> Baseline Created

New Systems with Baselines--------> Image created for every new systems--------> Image is used for further baselining.

Change Management: Any changes in the system should undergo change management process.

*Exam tip: Any unauthorized change in the system impacts Availability of CIA triad.

Domain 7: Security Operations

1. Request Change: Request is made by the team who would like to make changes in the system
2. Review the change: Requirement is reviewed by the designated person.
3. Approve/Reject: Based on the review, the change will be approved/rejected
4. Test: Once the change is approved, it should be tested in non-prod environment
5. Schedule for implementation: Mainly on off hours (weekends)
6. Document: All the findings should be documented. Versioning of document is also important.

*Exam tip: it's important to remember the above sequence of steps

Patch Management:

1. Evaluate --> Release Patches
2. Test--> Test on isolated systems
3. Approve--> Use of change management to approve
4. Deploy--> Deployment of patches on affected systems.
5. Verify--> Verify if patches are deployed.

Vulnerability Management = Vulnerability Scans + Vulnerability Assessment

Scans: What's in the signature will be found
Assessment: Will try to analyze the finding.

CVE - Common Vulnerability Exposure (Gives you the score of the vulnerability based on several factors)

Domain 7: Security Operations

Preventing And Reporting Incidents

Incident Response Steps: DRM Rep Rec Rem LL

Detect-->Response--->Mitigate--->Report--->Recover--->Remediate--->Lesson Learned
(Contain) (Mgt. & Media) (RCA)

Implementing Preventive measures

- Keep systems and applications up-to date
- Remove or disable unneeded services and protocols
- User intrusion detection and prevention systems
- Use up-to date anti malware software
- Use Firewalls
- Implement configuration and system management processes

<space reserved for edits, corrections, and additions>

Domain 7: Security Operations

Detect: Not every incident needs to be reported or escalated (Identify FPs)

Response: Respond to the true incident immediately and effectively

Mitigate: Ensure no further damage is caused. (Contain)

Report: It should be reported to the senior management and concerned people. (Only designated person should be allowed to speak with media)

Recover: Build the system at least as secure as it was prior to the incident

Remediate: Identify the root cause of the incident.

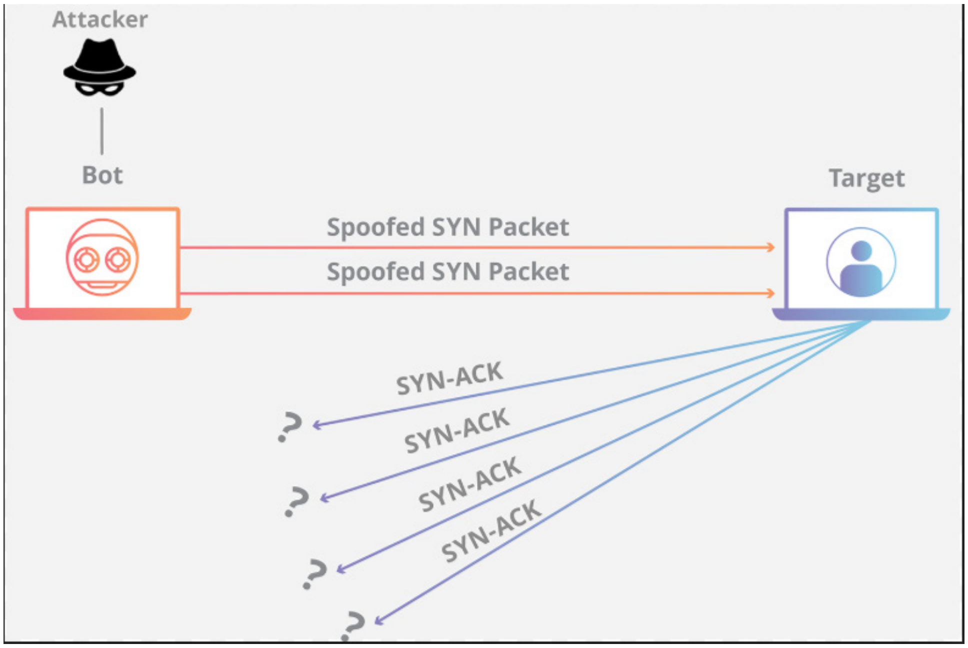
Lesson Learned: What can be improved from the past experience.

*Exam tip: It is best to be familiar with the sequence of incident response

Attacks:

Denial of Service: Utilization more than capacity (DDoS)

Syn Flood: 3 way handshake is not completed



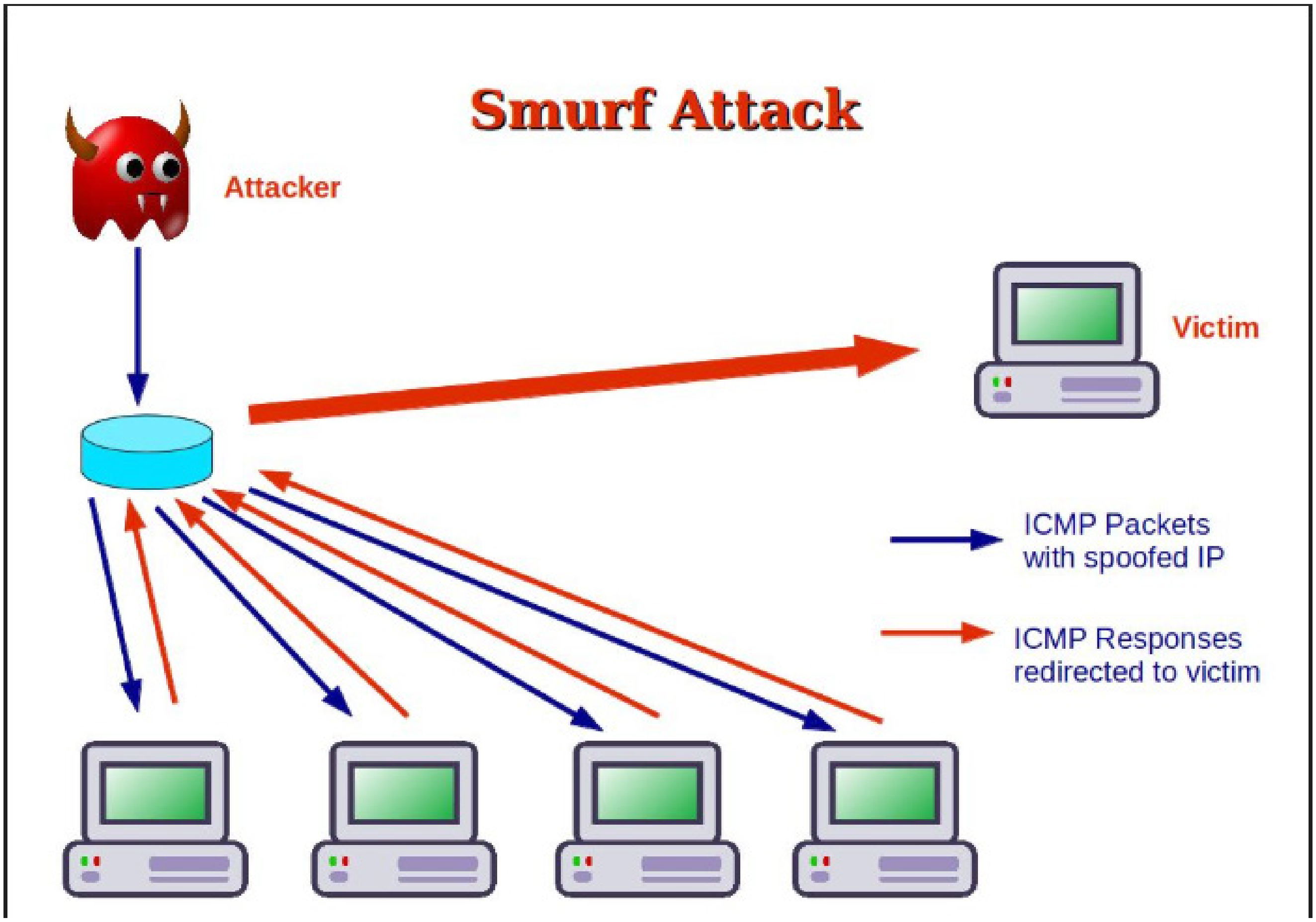
Domain 7: Security Operations

Syn cookies, RST packet, Time bound ACK are the countermeasure.

Smurf and Fraggle Attack: Attacker pings with spoofed source address of victim.

Smurf: ICMP packets

Fraggle: UDP packets

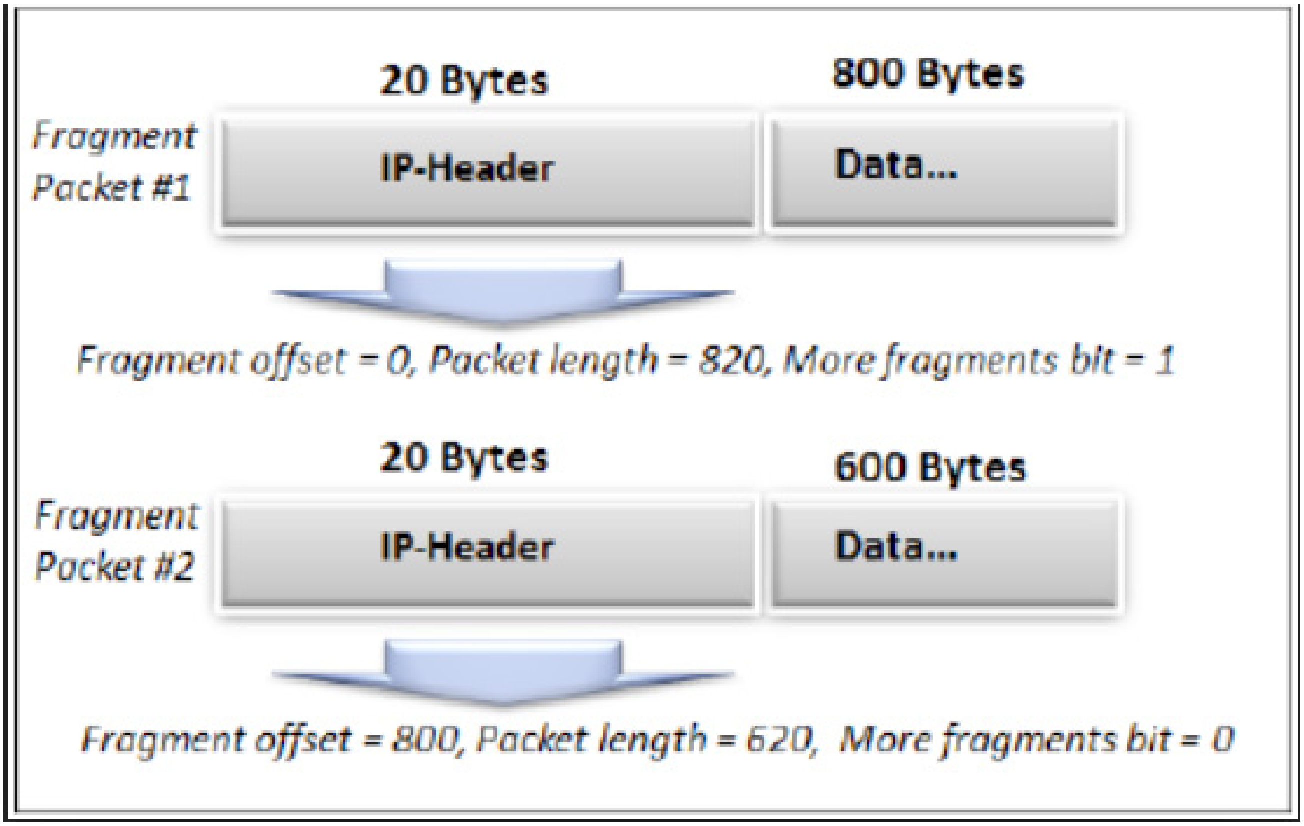

Smurf Attack
Attacker
Victim
ICMP Packets with spoofed IP
ICMP Responses redirected to victim

Botnets: Infected machines helps in attacking victims.

Ping of Death: Sending oversized packets.

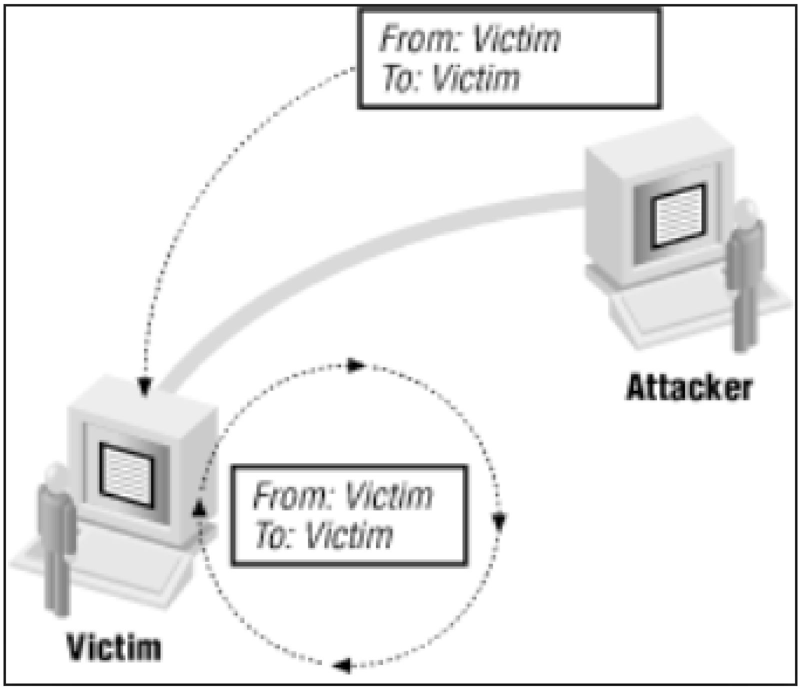
Tear drop: Packets are fragmented and can’t be put together.

Domain 7: Security Operations


20 Bytes
800 Bytes
Fragment Packet #1
IP-Header
Data...
Fragment offset = 0, Packet length = 820, More fragments bit = 1
20 Bytes
600 Bytes
Fragment Packet #2
IP-Header
Data...
Fragment offset = 800, Packet length = 620, More fragments bit = 0

Land Attack: Loop

Attacker spoofs the source address of victim and sends the SYN Packets. Victim's system ends up responding to SYN/ACK to its own and DoS itself.



Domain 7: Security Operations

Zero Day: Vulnerability which has not been reported or found by vendor.

Malicious Code: Drive by download (Most common method for system infection)

Man in the middle attack (MITM) - When an attacker sits in between the 2 legitimate parties and tries to sniff through the communication.

War dialing: Dialing the phone numbers to get the modem tone. Keeping the modem tone after longer number of rings is the countermeasure.

Sabotage: Destruction caused by inside people

Espionage: Spying

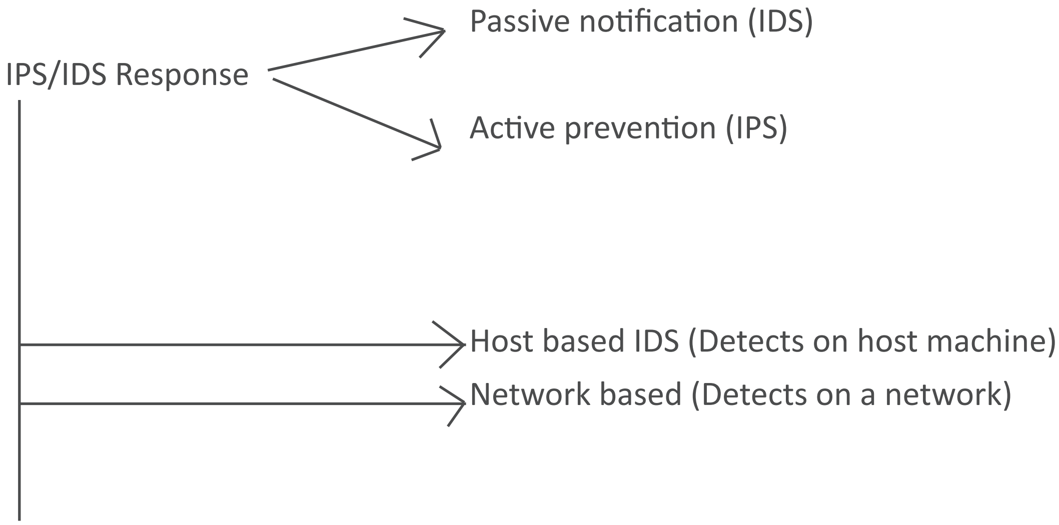
Intrusion Detection and Prevention Systems: Effective method to detect DoS attacks.

Primary purpose is timely and accurate response.

Types:

a. Knowledge Based (Signature/Pattern): Detects what signatures are updated.

b. Anomaly (Behavioral/Statistical/Heuristic): IDS is kept in an environment to learn. (Best for Zero day attacks)


Passive notification (IDS)
IPS/IDS Response
Active prevention (IPS)
Host based IDS (Detects on host machine)
Network based (Detects on a network)

Domain 7: Security Operations

Darknets: Networks present with no sensitive content. They help in capturing attacks.

Honey Pot: Temp attacker to attack. (Trap) Detects the type of attack. Network of honeypot is known as Honey Net.

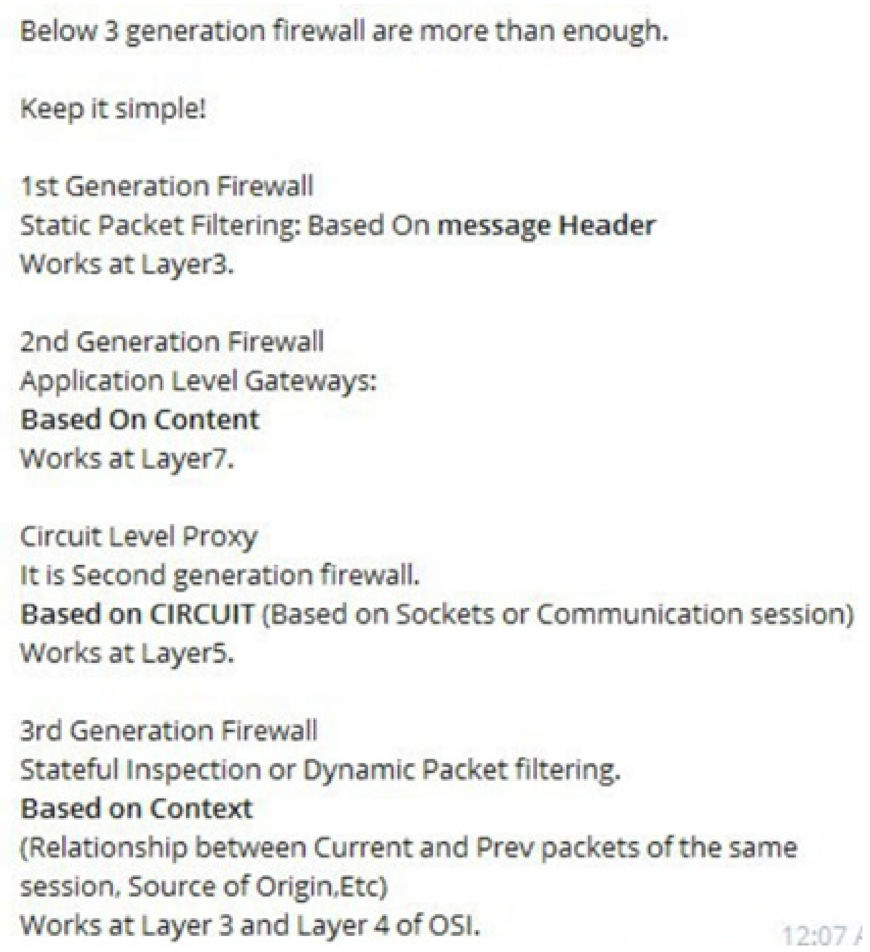
Enticement -- Legal
Entrapment -- Illegal (Deliberate attempt to lure an attacker and then reporting against it)

Pseudo Flaws: Intentional flaws to tempt attackers.

Padded Cell: Similar to Honey Net. Once attacker attacks, IDS transfer the attacker to padded cell without letting the attacker know.

Warning Banners: Administrative Deterrent control.

Firewalls:



Below 3 generation firewall are more than enough.

Keep it simple!

1st Generation Firewall
Static Packet Filtering: Based On **message Header**
Works at Layer3.

2nd Generation Firewall
Application Level Gateways:
Based On Content
Works at Layer7.

Circuit Level Proxy
It is Second generation firewall.
Based on CIRCUIT (Based on Sockets or Communication session)
Works at Layer5.

3rd Generation Firewall
Stateful Inspection or Dynamic Packet filtering.
Based on Context
(Relationship between Current and Prev packets of the same session, Source of Origin,Etc)
Works at Layer 3 and Layer 4 of OSI.

Domain 7: Security Operations

Sandbox: Isolate Java apps from interacting with other apps.

*Exam tip: Logs and reports should be preserved. One way is to access remotely.

Logging & Monitoring: Uses of SIEM
Audit Trail: Detective Control (Passive)

Sampling: Statistical method-- portion of samples
Clipping Level: Setting Threshold (Non-Statistical)
Other Monitoring tools: CCTV, Keystroke, traffic analysis, Trend Analysis
Egress Monitoring: Protecting outgoing data (DLP, Watermark)
Ingress Monitoring: IDS, IPS, Firewall

Threat Intelligence - Threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace. Threat intelligence sources include open source intelligence, social media intelligence, human Intelligence, technical intelligence or intelligence from the deep and dark web.
Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network.

Types of Threat Intelligence:
There are three overarching types of threat intelligence:

- Tactical: technical intelligence (including Indicators of Compromise such as IP addresses, file names, or hashes) which can be used to assist in the identification of threat actors
- Operational: details of the motivation or capabilities of threat actors, including their tools, techniques and procedures
- Strategic: intelligence about the overarching risks associated with cyber threats which can be used to drive high-level organizational strategy

Domain 7: Security Operations

Benefits of Threat Intelligence:

Cyber threat intelligence provides a number of benefits, including:

- Empowers organisations to develop a proactive cybersecurity posture and to bolster overall risk management policies
- Drives momentum toward a cybersecurity posture that is predictive, not just reactive
- Enables improved detection of threats
- Informs better decision-making during and following the detection of a cyber intrusion

User and Entity Behavior Analytics

- User and entity behavior analytics, or UEBA, is a type of cyber security process that takes note of the normal conduct of users. In turn, they detect any anomalous behavior or instances when there are deviations from these “normal” patterns. For example, if a particular user regularly downloads 10 MB of files every day but suddenly downloads gigabytes of files, the system would be able to detect this anomaly and alert them immediately.
- UEBA uses machine learning, algorithms, and statistical analyses to know when there is a deviation from established patterns, showing which of these anomalies could result in a potential, real threat.

Auditing to Assess Effectiveness:

1. Perform User Entitlement Review, Managing High level privileges.
2. Security Audit ---> Due Care
3. Technical logs used to evaluate the effectiveness of the system
4. Audit reports should be assigned a classification label.
5. External Audits is a regulatory requirement.

Disaster Recovery

Natural Disaster: Earth Quake, Floods, Avalanche, storms, fire.

Manmade disaster: Fire, terrorism, hacking, bombing, explosion, power outage

Insurance agencies have started insuring against terrorism.

Other failures: Hardware/Software failures

*Exam tip: For zero downtime, redundant failover systems are required.

Strikes, loots, vandalism are some forms of disasters. (Insurance is required to protect against these events)

Domain 7: Security Operations

System Resilience & Fault Tolerance

Single Point of Failure: Failure of component that can cause issues. (e.g. the only Server processing online banking requests crashes)

System Resilience: Ability of a system to maintain an acceptable level of service during an adverse event.

1. Failover---> Switching to redundant service at the event of failure
2. Failback--->Switching back to primary service
3. Cluster---> Appears to be single server to the end user (Server farm) {listens to the heartbeat of the servers. Any server fails, peer servers picks up the request}
4. Redundant Server---> Server kept in case of failure of primary server. In case of zero downtime. (Expensive)

Protecting Hard drives

Redundant Array of Inexpensive Disks (RAID)

RAID 0 ---> Striping ; Great performance (Speed). No redundancy
RAID 1---> Mirroring; 2 disks, both holds same data. Fault tolerance
RAID 5---> Striping + Parity; Fault tolerance + High Speed. 3 or more disks are used
RAID 10---> Combination of RAID 1 and 0; At least 4 disks are used. Striping + Mirroring. Even number of disks.
*Exam tips: Hardware disks are more reliable & expensive.

Protecting Servers

- Failover---> Switching to redundant service at the event of failure
- Failback--->Switching back to primary service
- Cluster---> Appears to be single server to the end user (Server farm) {listens to the heart beat of the servers. Any server fails, peer servers picks up the request}
- Redundant Server---> Server kept in case of failure of primary server. In case of zero downtime. (Expensive)

Domain 7: Security Operations

Hot Swap: Replacing Faulty disk without power down

Cold Swap: Need to power down the system to replace faulty system

Power Back up: UPS, Generators

Spike: Sudden rise in voltage

Sag: Sudden reduction in voltage

Surge: High Voltage for long time

Brownout: prolonged low voltage

Transient: Power Noise

Trusted Recovery: Assurance that system is as secure as it was before disaster.

Manual Recovery: Manual intervention is required

Automated recovery: Systems which performs trusted recovery itself.

Automated recovery with undue loss: Similar to automated recovery. Additionally, specific objects are protected to prevent their loss.

Functional Recovery: Automatic recovery of a specific function. Or the system will be able to roll back to secure state

Fail Secure: After failure, system secures itself. (Blue screen of death)--- where security is important

Fail Open: System will grant access to all after failure--- Where Availability is important

Fail Safe-- Human Safety

Fail Secure-- System safety and doors of server room

Recovery Strategy: Actual Cash Value (ACV) = compensation on the market value on the day of loss (minus) Depreciated value since the time of purchase.

Actual Loss: Loss of data

Potential Loss: Loss of opportunity & future business.

Best Practice: Try to restore 50% of highest priority systems and then move on to lower priority units to achieve minimum operating capacity.

Domain 7: Security Operations

Crisis Management: Continuous training. Should know how to handle situation at the time of emergency.

Emergency Communication: Should be prepared with alternate communication links.

Off sites

1. Cold Site: Low in cost. No actual systems, just the basic infrastructure e.g. building, air conditioning etc. takes weeks to activate.
2. Hot Sites: Most expensive. Very quickly available (within hours). Same level of protection as primary sites. People just needs to be moved along with data restoration is required.
3. Warm site: Available within 12 hours. Transportation of backup media is required.
4. Mobile Sites: Easily relocated units.
5. Service Bearers: Company that leases computer time. Owns large server farms and workstations.
6. Mutual Assistance Agreement/ Reciprocal Agreement: 2 organizations share computing facilities.

Characteristics: a. Hardware and software compatibility is an issue

b. Non-enforceable

c. Cost-effective

7. Redundant site: 2 sites running in parallel. Highly expensive. Majorly for organizations with ZERO downtime.

*Exam tip: Always make sure your off site is at an optimum distance so that any disaster should not affect both the sites.

Domain 7: Security Operations

Database Recovery:

a. Electronic Vaulting---> Transfer data in bulk. Not real time transfers.
b. Remote Journaling---> Transaction logs are being transferred. Frequent transfers.
c. Remote Mirroring: Real time data is transferred. Exact data sync is there. Very expensive.

*Exam tip: A disaster plan should contain a call tree (list of the people to be contacted) handy. Once the disaster team reaches at site, first task is to assess the situation.

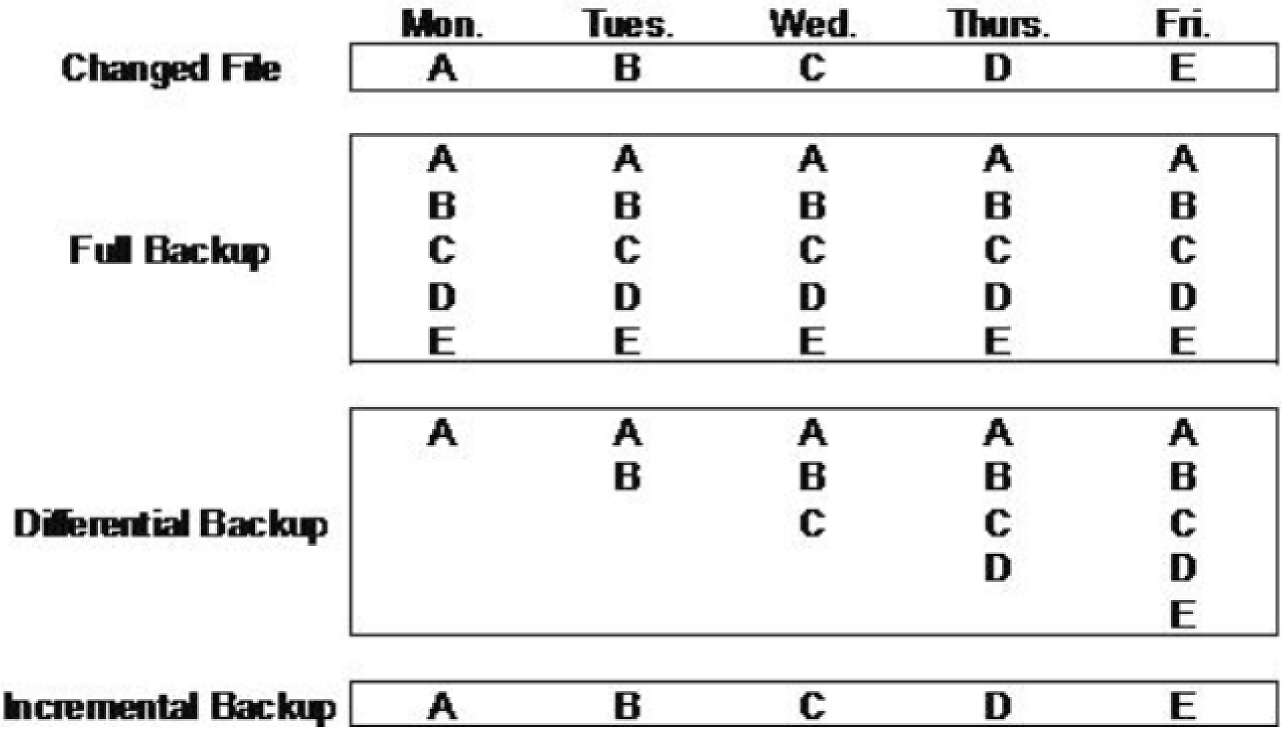
Backups:

Archive Bit: If it has any value, it means archive of the file is due or backup is not yet taken. Once the backup is done, archive bit is reset or made to 0 (zero).

1. Full Backup: Complete Back up. Archive bit is set to 0.

2. Incremental Back up: Backs up only files which have changed after full backup. Archive bit is set to 0.

3. Differential Backup: Backs up everything after last full backup.



	Mon.	Tues.	Wed.	Thurs.	Fri.
Changed File	A	B	C	D	E
Full Backup	A B C D E	A B C D E	A B C D E	A B C D E	A B C D E
Differential Backup	A	A B	A B C	A B C D	A B C D E
Incremental Backup	A	B	C	D	E

Domain 7: Security Operations

	Full	Incremental	Differential
Backup Time	3	1	2
Restoration Time	2	3	1

3 - Highest

2 - Medium

1 - Lowest

*Exam tip: Back up should be done during low peak time. You should always test the restoration of the backups to avoid last minute surprises.

Software Escrow: If a vendor who has developed the software goes out of the business, it gives the source code to 3rd Party which can be accessed by the client.

Recovery Team: Which moves to the alternate site. Most critical data are moved first.
Salvage team: Which moves to the primary site. Least critical data is moved first.

Recovery: Bringing back business operation to working state
Restoration: Bringing back business facility to workable state.

Exam tip: Disaster Recovery plan should be classified as extremely sensitive document. Should have only one copy.

Testing of Disaster Recovery Plan:

1. Read through test: Copies of the DR plan is distributed.
2. Structured walkthrough: aka Table Top; scenario is discussed in a room over a table
3. Simulation Test: Scenarios are performed and responses are developed.
4. Parallel test: Conducted at offsite but primary site is still operational
5. Full interruption test: Main site is shut down.

Domain 7: Security Operations

Incidents and Ethics

Investigation Types

1. Operational: Resolving operational issues. Conduct RCA
2. Criminal: Conducted by law enforcement. Murder, kidnapping, terrorism
a. Evidence: Beyond a reasonable doubt. (Making it concrete for conviction)
3. Civil: Legal team (issues inside and outside company), family matter, real estate etc.
a. Evidence: Preponderance of evidence (convincing enough to justify the claim)
4. Regulatory: Violation of administrative law (staying in a country despite of expiration of Visa). It is conducted by regulators.

e-Discovery: Evidence extraction from electronic media. Following are the steps for e-Discovery:

1. Information Governance ---> Information is well organized
2. Identification ---> locating information
3. Preservation---> preserving the evidence is must to avoid any deviation
4. Collection---> collection of evidence should be done by the trained professional
5. Processing ---> should get rid of irrelevant information
6. Review ---> examines the remaining information
7. Analysis ---> perform deeper inspection
8. Production---> produce a format which can be shared
9. Presentation ---> presented to court

<u>Evidence</u>

Admissible: Relevant, material to the case, must be obtained legally

Domain 7: Security Operations

Types:

1. Real Evidence: Which can be brought into court. (murder weapon)
2. Documentary: Written evidence (agreements etc.)

a. Best---> Original copy of document. (copies of the original document are called secondary evidence)

b. Parol---> Written agreement between parties.

3. Testimonial: verbal witness (Gawaah ;-))
4. Hearsay: Indirect (Whispers)

Chain of custody: proper chain of evidence collection should be maintained. Who handles evidence at what moment should be properly documented. Any break in COC makes the evidence inadmissible. (Very Important)

<u>Evidence Collection and Forensic Procedure</u> (International Organization on Computer Evidence) IOCE

1. Action taken on evidence should not change evidence
2. Person should be trained for this purpose
3. All activity must be documented, preserved, and reviewed.
4. An individual is responsible while evidence is in its possession
5. Agency seizing the evidence is responsible for compliance.

*Exam tip: Best method is to work on the copy of the evidence

Media Analysis: Involves identification and extraction of information from storage media
Network Analysis: Activity took on the network during the incident.
Software Analysis: Looking for logic bombs, back doors etc.
Hardware Analysis: PC, smartphones etc.

Investigation Process: Clearly outline the scope of investigation. Roles, responsibilities and Rule of engagement (Different phases of investigation)

Domain 7: Security Operations

Phases:

1. Calling Law enforcement
2. Interrogating suspects
3. Collecting evidence
4. Disrupting access.

*Exam tip: Never hack back the attacker.

Major Attacks

1. Military & Intelligence: Obtain classified data (APT)
2. Business Attacks: Corporate espionage
3. Financial attacks: Obtain financial gain
4. Terrorist attack: Disrupt normal life
5. Grudge attack: Personal attack against individual or organization (Employee is the biggest threat)
6. Thrill Attack: Attack for fun (script kiddies). Hacktivist (political belief, thrill of hacking)

Common Incidents

1. Scanning: Very common form of incident. It allows us to buy some time for investigation.
2. Compromise: Hardest to detect
3. Malicious code: Reported by users
4. DDoS: Easiest to detect

Incident Response (As per NIST)

1. Detection and Identification
2. Response and Report
   a. Isolation & Containment
   b. Evidence Gather
3. Recover & Remediate
   a. Restoration
   b. Lesson Learned

Domain 7: Security Operations

Interview: Gather information to assist with investigation

Interrogate: Question the suspect

Gather Evidence:

1. Search warrant
2. Surrender
3. Subpoena

*Exam tip: All evidence must be secured. Remote login to preserve any evidence. Incidents should be properly reported and documented.

Ethics (Personal Conduct): These rules are not laws. Minimum standards for personal behavior.

ISC2 code of Ethics: (Very Important)

Preamble: Safety. Welfare of society common good
Canons:

1. Protect society, the common good, necessary public trust and confidence, and the infrastruc ture (Social Responsibility)
2. Act honorably, honestly, justly, responsibly, and legally (Maintain Integrity)
3. Provide diligent and competent service to principals (Protect organization you are working for)
4. Advance and protect profession (Don't share exam questions)

Ethics & Internet: Internet Advisory Board (IAB) RFC 1087

1. Unauthorized access
2. Disrupts the internet
3. Wastes resources
4. Destroys integrity
5. Compromise privacy

Domain 8: Software Development Security

Security should be considered at every phase of system development.

0,1 : Machine Language (Low Level)

C, C++ : High level Language (Programming)

1st Gen : All Machine Language

2nd Gen : All Assembly Language

3rd Gen : All Compiled Language

4th Gen : Natural Language like SQL

5th Gen : Allows programmer to create own visual interface

OBJECT ORIENTED PROGRAMMING :

Object: Accounts, Account holder, employee

Method: Actions on Object (Add Fund)

Sub Class: Saving account, Current account

Behavior: Result exhibited by an Object

Class: Collection of common methods from a set of Object

Polymorphism: Object that responds with different behavior to same message

Cohesion: Strength of relationship between methods of same class (HIGH)

Coupling: Interaction between Objects (LOW)

Assurance: Degree of confidence that security control mechanism built in the system will work effectively throughout the life cycle (TCB)

Fail Secure: Disaster happen, System secure itself (Confidentiality Important)

Fail Open: Disaster happen, access is allowed to system (Availability Important)

SYSTEM DEVELOPMENT LIFECYCLE (SDLC)

1. Conceptual Definition: High level statement agreed by all stake holders
2. Functional Requirement: Specific functionalities are used and how parts will inter operate
3. Control Specification Development: Security in the system is designed (Access Control, ensuring CIA)

Domain 8: Software Development Security

4. Design Review: How various parts of system will inter operate (Architecture)
5. Code Review: Once the code is written, peer review should happen with different individuals.
6. UAT: End users tests if the product meets the given requirement.
7. Maintenance and Change Management: Any further change in the system should go through change management process.

SOFTWARE DEVELOPMENT LIFECYCLE

1. **Requirement Gathering**: Functional requirements are gathered. Security and Privacy risk assessments are performed.

2. **Design**: Various components of application are defined which will be used. Attack surface Analysis and Threat Modelling is performed in this phase.

3. **Develop**: Codes are written and a peer review is done.

4. **Test**: Various testing and validation are performed. Unit (done by developers), integration (combining the modules), regression (when code is tested after changes have been performed) and UAT (performed by end users to test the functionality).

5. **Operation** and Maintenance: Once the code is deployed, production support is given and further changes are done through change management process.

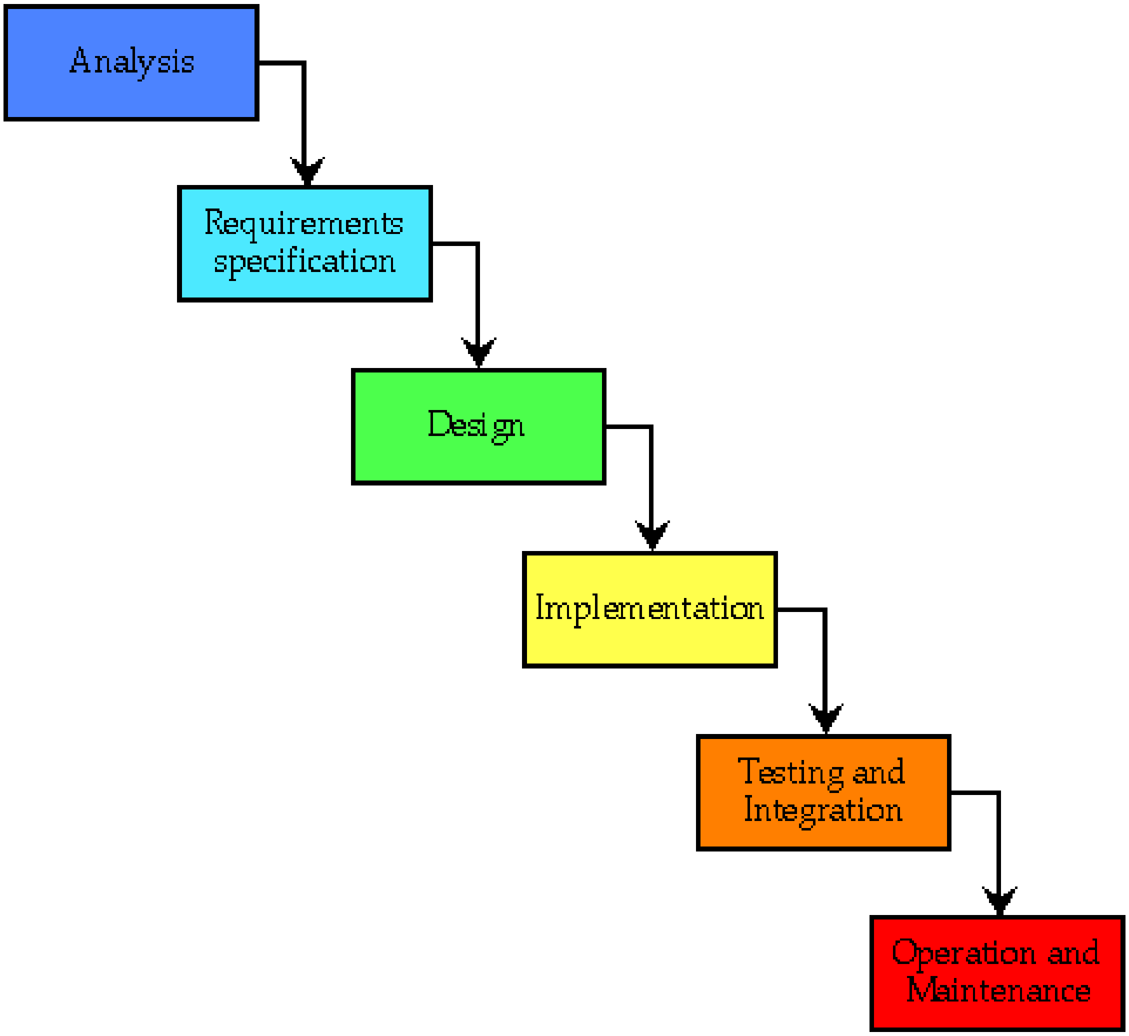
Domain 8: Software Development Security

LIFE CYCLE MODELS:

1. Waterfall: 7 Stages. Also called Feedback Loop. Allow one step back.

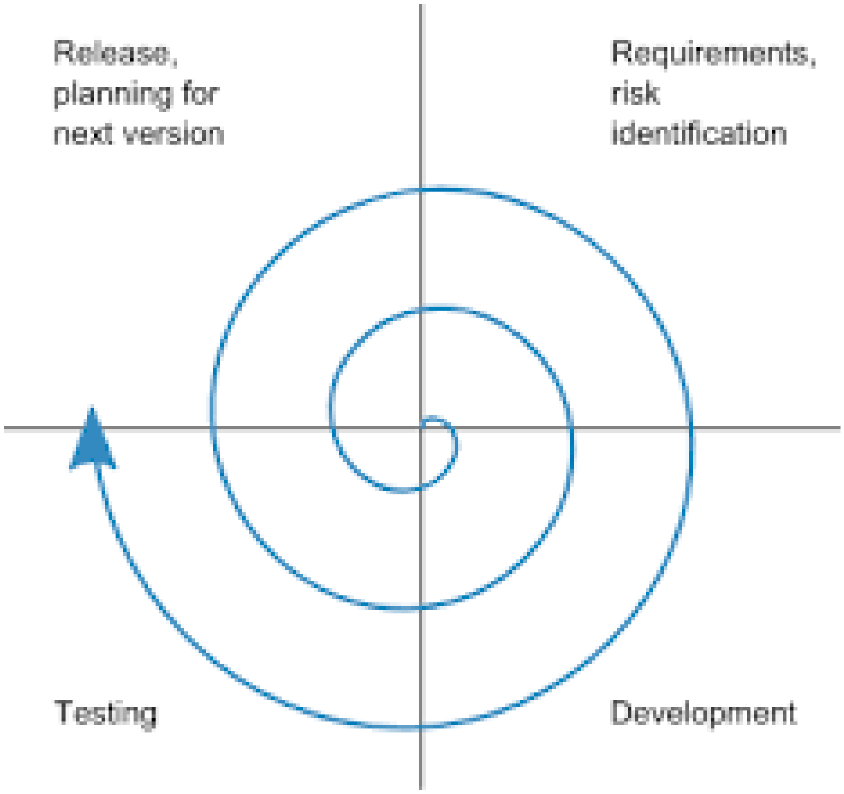
   Verification – Evaluates against specification

   Validation – Evaluates if the product meets the real world requirements.



Domain 8: Software Development Security

2. Spiral Model: Prototype is created, tested, and then re-created.
   Matures as it gets feedback by end user.


Release, planning for next version
Requirements, risk identification
Testing
Development

3. Agile:

    Very popular, scalable, flexible

    Business developers work together.

    Customer satisfaction is topmost priority.

    Scrum, AUP, XP, DSDM

   Core Values of Agile:

    Individuals and interactions over processes and tools

    Working software over comprehensive documentation

    Customer collaboration over contract negotiation

    Responding to change over following a plan

Domain 8: Software Development Security

S/W CMM (IRDMO)

Initial: Disorganized, no process

Repeatable: Life cycle management process is introduced, Repeatable results. S/W project planning, tracking, Quality Assurance etc.

Defined: S/W developers operates with formal procedure. More organized.

Managed: Detailed understanding of development. Quantitative process & Quality Management.

Optimized: Sophisticated S/W development process is there. Feedback oriented. Change Management.

IDEAL MODELS

Initiating: Business reason for the change is defined.

Diagnosing: Analyze current state of organization

Establishing: Takes general recommendation from diagnosing phase

Acting: Develops solution, test and refine them.

Learning: Must continue to improve

GANTT CHART: Project scheduling is done

PERT CHART (Project Evaluation Review Technique): Size of the product and standard deviation of Risk assessment is calculated.

CHANGE & CONFIGURATION MANAGEMENT:

(1) **Request Control**: Users request modification

(2) **Change Control:** Developers create code, testing happens & sent for manager's approval

(3) **Release Control**: Once UAT is complete & manager has approved, code is deployed

CONFIGURATION IDENTIFICATION: Document the configuration of covered software.

CONFIGURATION CONTROL: Ensures changes are done as per change management

CONFIGURATION STATUS ACCOUNTING: Keeps track of all authorized changes

CONFIGURATION AUDIT: Ensures no unauthorized changes have taken place

Domain 8: Software Development Security

DEVOPS APPROACH: Combines development, operations & quality assurance
Based on Agile, deploy codes several times a day.

Continuous integration (CI) and continuous delivery (CD) embody a culture, set of operating principles, and collection of practices that enable application development teams to deliver code changes more frequently and reliably. The implementation is also known as the CI/CD pipeline.

APPLICATION PROGRAMMING INTERFACE (API) : Social media API. Post Status, Follow user, like Post.
Web Service interacts with other web services.
Developers should protect API Keys (similar to password)

SOFTWARE TESTING
White Box: Have full access to code & system. AKA Crystal Box
Black Box: No access to code & system
Grey Box: Partial knowledge of code

Static Testing: Code Review (Buffer Overflow)
Dynamic Testing: Testing on runtime (XSS, SQL Injection)

CODE REPOSITORIES: Place to keep code, make sure it is protected
SERVICE LEVEL AGREEMENT (SLA): Whenever an agreed service is not provided, financial & contractual remedies are invoked

Software Acquisition: Most of the software used by enterprises is not developed internally but purchased from vendors. Some of this software is purchased to run
on servers managed by the organization, either on premises or in an infrastructure as a service (IaaS) environment. Other software is purchased and delivered over the internet through web browsers, in a software as a service (SaaS) approach (In SaaS, most of the responsibility is with service providers)

Domain 8: Software Development Security

Assess Security Impact of Acquired Software

Software Assurance: Defined as having high level of confidence that software is free from vulnerabilities, either intentionally designed into software or accidently inserted at anytime during its life cycle and it functions in the intended manner.

Phases:

- Planning: Developing requirement, creating acquisition strategy, identifying risk and an evaluation plan.
- Contracting Phase: Creating RFPs, evaluating and negotiating terms and addressing software risks.
- Monitoring and acceptance phase: Establishing contract work schedule, implementing change control, accepting software deliverables.
- Follow on phase: Sustainment (Risk Management, change management & assurance management), decommissioning.

Commercial Off the Shelf (COTS): Commercial off the shelf products are ready-made, doesn't need any customization and available to purchase. Some Summary Observations on Buying and Using COTS Code:

- 1)Adopt a broad definition of COTS and learn to recognize it when you see it.
- 2)Consider security as part of the purchase process.
- 3) Research security from all available directions.
- 4)Assume the software is insecure until proven otherwise.
- 5)Consider the environment in which the COTS system will operate; what may be secure in one instance, may not be in another.
- 6)Protect yourself—legally and physically. Request guarantees from COTS vendors and, if possible, indemnification. Where testing or risk indicate, wrap the software with a package that validates input and/or output. Protect against failure.
- 7) Track changes and adapt the security strategy accordingly.
- 8)Build in monitoring systems to detect failure.

Domain 8: Software Development Security

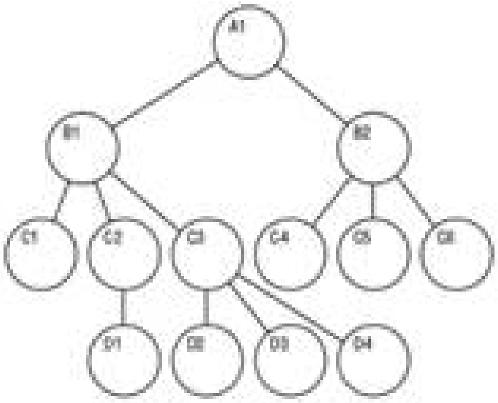
Security issues on COTS

- COTS software is an attractive attack target because of organizational dependency on them as well as their high profile in the marketplace.
- It is difficult to verify the security of COTS products because they are black boxes to their customers.
- The COTS software vendors have limited liability as designated by the end-user license agreement (EULA) that the user must agree with prior to software use.
- COTS is typically designed without consideration for your specific security control requirements. While this is not universally true, COTS products are usually developed to be standalone products.

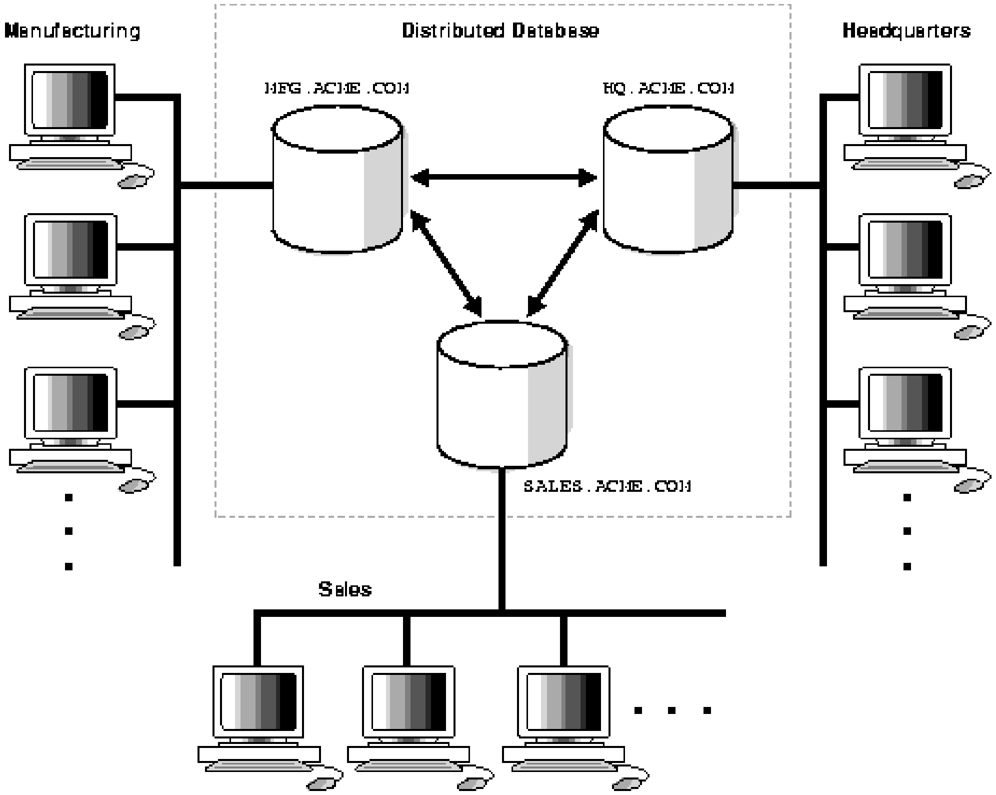
SOAR (Security Orchestration, Automation, and Response): It refers to a collection of software solutions and tools that allow organizations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation

DATABASES (DBMS or RDBMS)

(1) Hierarchical : One to Many



Domain 8: Software Development Security



(2) Distributed: Data stored in more than one databases

(3) **Relational**: 2D (Rows & Column)
Row – Tuple , Cardinality
Column – Attribute, Degree

PRIMARY KEY: Value which can be used to uniquely identify a record in table

CANDIDATE KEY: Uniquely identify any record in table

FOREIGN KEY: Referential Integrity. Enforce relationships between two tables

Domain 8: Software Development Security

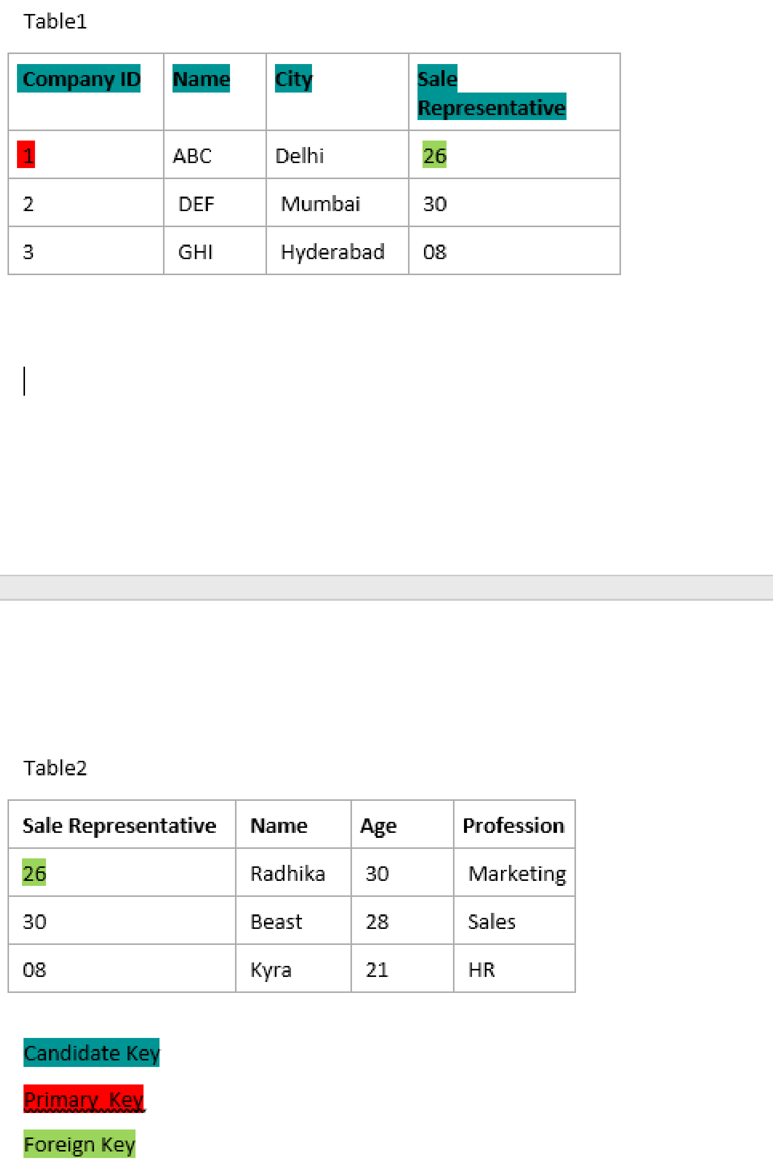


Table1

Company ID	Name	City	Sale Representative
1	ABC	Delhi	26
2	DEF	Mumbai	30
3	GHI	Hyderabad	08

Table2

Sale Representative	Name	Age	Profession
26	Radhika	30	Marketing
30	Beast	28	Sales
08	Kyra	21	HR

Candidate Key

Primary Key

Foreign Key

NORMALIZATION: Making Data Base into normal forms

1st Normal Form

2nd Normal Form

3rd Normal Form

Reduce redundancy, housekeeping activity

Before DB become 2nd Normal Form, it has to be compliant with 1st Normal Form (cumulative)

Domain 8: Software Development Security

DATABASE TRANSACTION

Committed: Once a transaction is successfully completed

Rollback: If a transaction fails, must be rolled back to previous state.

ACID

Atomic: All or nothing. Either every transaction is completed or nothing.

Consistency: Transaction should be consistent to database rules

Isolation: Should not affect other transactions

Durability: Once its committed, it should be preserved

Database Contamination: Mixing data with different classification

Database Views: Way to restrict access to database. Classified information

Concurrency: Preventive mechanism. Protects integrity & availability. Uses lock & unlock feature.

Cell Suppression: Way of hiding a cell

Polyinstantiation: Two or more rows in same relational table have identical primary keys. Defense against Inference attack.

Perturbation (Noise): Meaningless data to protect confidentiality

ODBC: Dictates how application communicate with databases. Act as proxy.

Expert Systems: Knowledge Base + Inference Engines

Knowledge Base: If/Else , Set of rules

Inference Engine: Judgement of previous experience. Useful in Emergency Solution. Doesn't effect emotion.

*Exam tip: Expert Systems are as good as the data in the Knowledge Base.

Machine Learning: Machine learning techniques use analytic capabilities to develop knowledge from datasets without the direct application of human insight. The core approach of machine learning is to allow the computer to analyze and learn directly from data, developing and updating models of activity.

NEURAL NETWORK: Chain of computational units used to imitate human brain.

Benefits – Linearity, I/O Adaptivity & mapping

Voice recognition , weather prediction

Delta rule, Learning rule

Domain 8: Software Development Security

DECISION SUPPORT SYSTEM (DSS) : Knowledge base application that analyses business data & present in a way to make business decision easier.
N IDES : Next Generation Intrusion Detection Expert System

MALICIOUS CODES:
Virus:

- Propagation Technique
- Destruction

PROPAGATION TECHNIQUES:
(1) Master Boot Record Virus (MBR): Affects boot sector
(2) File Infection: Replaces original file with corrupted
(3) Macro Virus: Easy to write(VBA), very lethal Ex. I Love you
(4) Service Injection: Injecting into trusted runtime process.

ANTIVIRUS: Signature Based
(1) Disinfect
(2) Quarantine
(3) Delete

Tripwire : Integrity check (Defacement attacks)

VIRUS TECHNOLOGIES:
(1) Multipartite Viruses: More than one propagation technique
(2) Stealth Viruses: Hide themselves from getting detected
(3) Polymorphic Viruses: Modify their own code as they travel from system to system
(4) Encrypted Viruses: Use cryptographic techniques
Short segment code – decryption routine
(5) Hoax: Circulating misleading information.
(6) Logic Bomb: Triggers on a logic (time based or event based)
(7) Trojan Horse: S/W that appears legitimate but carries malicious payload
(8) Ransomware: Encrypts documents & asks for ransom to decrypt it

Domain 8: Software Development Security

WORMS: Spread without human intervention

(1) Code red:

Step1- Select IP range to target
Step2- Deface web pages
Step3- Places logic bomb
(Specially on Microsoft IIS)

(2) Robert Tappan Morris (RTM):

- Send email
- Password attack
- Finger vulnerability
- Trust relationship

(3) Stuxnet

- Zero day
- Windows service
- Spread through USB
- Causes physical damage. Targets siemens products

(4) Spyware & Adware: Spyware monitors your actions and transmits important details to a remote system that spies on your activity. Adware uses a variety of techniques to display advertisements on infected computers.

Zero Day Attack: Many forms of malicious code take advantage of zero-day vulnerabilities, security flaws discovered by hackers that have not been thoroughly addressed by the security community. Should include a strong patch management program, current antivirus software, configuration management, application control, content filtering, and other protections.

COUNTER MEASURE

(1) Client System: Updated antivirus
(2) Server System: Updated antivirus
(3) Content Filters: Should be able to read SMTP traffic (mails)

Domain 8: Software Development Security

Tripwire: Integrity check

Sandbox: Isolates java application

ActiveX: Uses digital signature

Whitelisting of apps used in organization

PASSWORD ATTACK

- Password guessing
- Dictionary attacks
- Social Engineering

Counter Measure: Training & Awareness

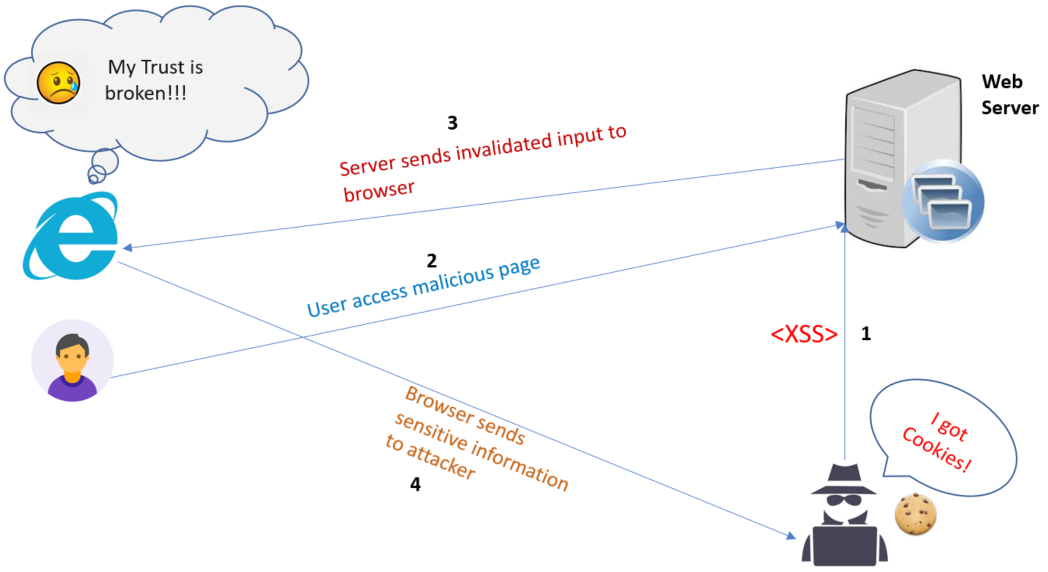
UNIX: Password shadowing / etc / shadow

APPLICATION ATTACKS:

- Buffer Overflow (Bound Check)
- Time of Check to Time of Use
- Back door
- Rootkit and Escalation of Privilege

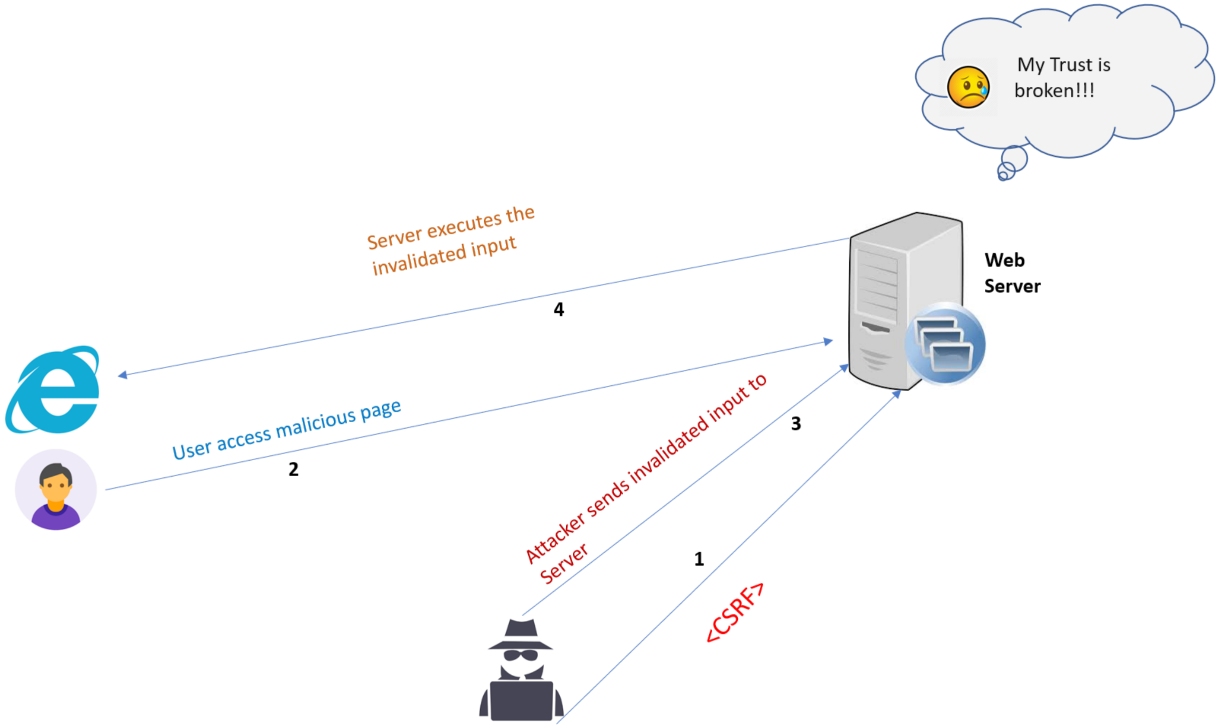
WEB APPLICATION SECURITY

- XSS (Persistent, Non-persistent, DOM based) {Input Validation}


My Trust is broken!!!
Web Server
3
Server sends invalidated input to browser
2
User access malicious page
<XSS>
1
Browser sends sensitive information to attacker
4
I got Cookies!

Domain 8: Software Development Security

- SQL Injection {Input Validation, Limit Access Privileges , use stored procedures)
- CSRF Cross-site Request Forgery (CSRF Token, custom header, cookies)


My Trust is broken!!!
Web Server
Server executes the invalidated input
4
User access malicious page
2
Attacker sends invalidated input to Server
3
1
<CSRF>

RECONNAISSANCE ATTACKS

- IP Probes
- Port Scans (Nmap)
- Vulnerability Scan (Nessus)
- Dumpster Diving

MASQUARADING ATTACK

- IP Spoofing
- Session High jacking

Copyright Credits

Digital Signature: https://medium.com/@meruja/digital-signature-generation-75cc63b7e1b4

Access Control Matrix: https://prosuncsedu.wordpress.com/2014/08/21/comparing-object-centric-access-control-mechanisms-acl-capability-list-attribute-based-access-control/

Protection Ring Model: https://asmed.com/cissp-security-mechanisms/

Process state: http://www.hexainclude.com/process-state-diagram-and-pcb/

OSI Model: https://community.arubanetworks.com/t5/Mobility-Hero-Tutorials/OSI-Layers/ta-p/178558

Topology: https://www.ianswer4u.com/

TCP/IP Model: https://clinetworking.wordpress.com/2018/06/09/1-1-compare-and-contrast-osi-and-tcp-ip-models/

NAT: https://en.wikibooks.org/wiki/A-level_Computing/AQA/Paper_2/Fundamentals_of_communication_and_networking/Network_Address_Translation_(NAT)

VPN: https://netbeez.net/blog/monitoring-vpn-connections/

CER: https://pen-testing.sans.org/blog/2015/10/08/whats-the-deal-with-mobile-device-passcodes-biometrics-part-1-of-2

Kerberos: https://www.infotechno.net/kerberos

SDN: http://www.thetech.in/2012/12/sdn-architecture.html

Cloud Responsibilities: http://www.bigdatapump.com/blogs/2016/4/4/cloud-services-trend-in-2016

Copyright Credits (Continued)

MTBF: https://blog.fosketts.net/2011/07/06/defining-failure-mttr-mttf-mtbf/

SYN flood attack: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

Smurf Attack: https://www.thesecuritybuddy.com/dos-ddos-prevention/what-is-smurf-attack/

Tear Drop: https://www.researchgate.net/figure/An-example-of-Teardrop-attack-packets_fig7_271497120

Land Attack: https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch04_08.htm

Cybrary.it

Back up methods: https://www.electronicdiscoveryblog.com/data-backup-systems/

Waterfall Model: http://fseassignments.blogspot.com/2011/06/waterfall-model.html

Spiral Model: https://mixmastamyk.bitbucket.io/pro_soft_dev/models.html

Hierarchical Database: https://mariadb.com/kb/en/library/understanding-the-hierarchical-database-model/

Distributed Database: https://docs.oracle.com/cd/B10501_01/server.920/a96521/ds_concepts.htm

CISSP Official Study Guide - Sybex 8th Edition

CISSP All In One -Exam Guide 8th edition

https://us-cert.cisa.gov/bsi/articles/best-practices/legacy-systems/security-considerations-in-managing-cots-software

https://gdpr-info.eu/art-39-gdpr/

https://www.rapid7.com/solutions/security-orchestration-and-automation/