CSS Unit 1 Short Notes

Basic Concepts of Computer Security

- Confidentiality : The Act of Keeping Data and Resources hidden to prevent unauthorized access to sensitive data , Cryptography is one example mechanism that helps in maintaining the confidentiality of the Data

- Integrity : The Act of Ensuring the correctness and consistency of the data by preventing unauthorized data tampering. Threats may arise due to Unauthorized sources or authorized personnel modifying the data

+ Data Integrity : Correctness of the info

+ Source Integrity : Correctness of the Source from where the info is received

Detection Mechanisms can only detect if the integrity of the data is no longer trustworthy , there is no way to prevent it

- Availability : The Act of Ensuring all required data and resources are available all the time without any disruptions or overload , Denial of Service Attacks are most common threats to the Availability of data

Four Classes of Threats

- Disclosure : The Action of Unauthorized Access Or Exposure of Sensitive Information , impacting the confidentiality of the data

EG : Snooping : listening to communications or browsing through files etc

- Deception : The Action of Falsifying or modification of data , compromising all three components of security

EG : Modification , MITM , Denial of Receipt

- Disruption : The Action of Disrupting the flow of information or causing Delays impacting the availability of Data

EG : DDos

- Usurpation : The Action of taking Unauthorized control over a system and manipulating information , affecting all three components of security

EG : Spoofing

Some Common Threats :

- Snooping : Listening to communication channels passively and browsing through files of the Target System

- Modification : Altering data to manipulate system behavior and cause havoc

- Spoofing : Pretending to be someone else in the network and accessing sensitive info

- Repudiation of Origin : Denying the existence of receipts after sending them

- Denial of Receipt : Denying that you didn't receive a product after receiving it

- Delay : Forcing the computer to take more time for an action than regular to cause delay

- Denial of Service : Overloading Or Flooding a Server to Restrict Availability of data

- Distributed Dos : Dos with a lot of computers

Policies & Mechanisms

- Policies : They are Rules and Regulations about what actions are allowed and prohibited in a network , Eg : Identity Check before Password Changing , Disallowing viewing or copying files from another computer in the connected Network etc

- Mechanisms : They are responsible for enforcing the policies in the network

Goals of Security :

- Prevention : Prevention of an attack from happening by using safety mechanisms like closely monitoring user actions to make sure they are not allowed to do things that shouldn't be done in the network

- Detection : Detection of an attack aims at providing all required information about an attack if a breach or cyber attack takes place , although it may not help in preventing the attack , it will prompt a trigger to necessary countermeasure mechanisms

- Recovery : Recovery is the roll back of computer's state to before the attack happened , it can be of two types

+ First Type , Identifies and stops the attack , analyzes the damage and repairs the system to it's original state , the system may halt , It also identifies vulnerabilities and fixes them to prevent future attacks , sometimes involving legal actions or retaliations

+ Second Type , The System doesn't stop functioning even when being attacked, using fault tolerance and security mechanisms , this kind of recovery is hard to implement and often used in safety critical systems , This recovery might disable some non essential functions

Trust and Assumptions :

- Assumptions : There are 2 main assumptions

+ The Security policies correctly partitions the entire system into secure and unsecure states

+ The Security Mechanisms make sure the system won't enter into an unsecure state

- Trust : 4 Trust on security mechanisms

+ Each Mechanism is designed to Implement one or more parts of the security policy

+ Union of Mechanisms implement the security policy completely

+ Mechanisms are Tamperproof

+ Mechanisms are implemented correctly

Additional : Security Mechanisms Fall into 3 Categories :

R - States Allowed by the Mechanisms

Q - All Secure States

+ Secure if R is a Subset of Q

+ Precise if R = Q

+ Broad if R is a Subset of Q But also Contains unsecure states

Assurance : It is the Basis for determining How much you can trust your computer with the help of 3 factors :

- Specification : Defining Correct and Incorrect Behavior of the System , If the Specification correctly figures how the system will function then the system has passed

- Design : Checking if the Software and Hardware Components adhere to the specifications

- Implementation : Checking if the Computer Functions Correctly

(Build More Stories if wanted)

Operational Issues : This Involves Balancing the Security Benefits with the Implementation costs for the Securities by subjective risk assessment and Cost Benefit Analysis

+ Cost Benefit Analysis : To Check the Data being protected actually requires high level security or not , Cheaply replenishable data don't require costly securities

+ Risk Analysis : To assess if a data is actually under a threat of being attack and requires protection , High Risk and High Impact Data should be given top priority in securities ,

Additional : Analysis Paralysis is a state which occurs to an organization if it spends too much time evaluating potential risks instead of implementing risk protection strategies

Human Issues : Human Related Struggles to Implement Security Measures

- Organizational Problems :

1) Security is considered as an expense until the company is attacked

2) Security is not given higher priority

3) Security is seen as slowing down processes

4) Lack of security Professionals

5) Unwillingness to spend more resources into security

- People Problems :

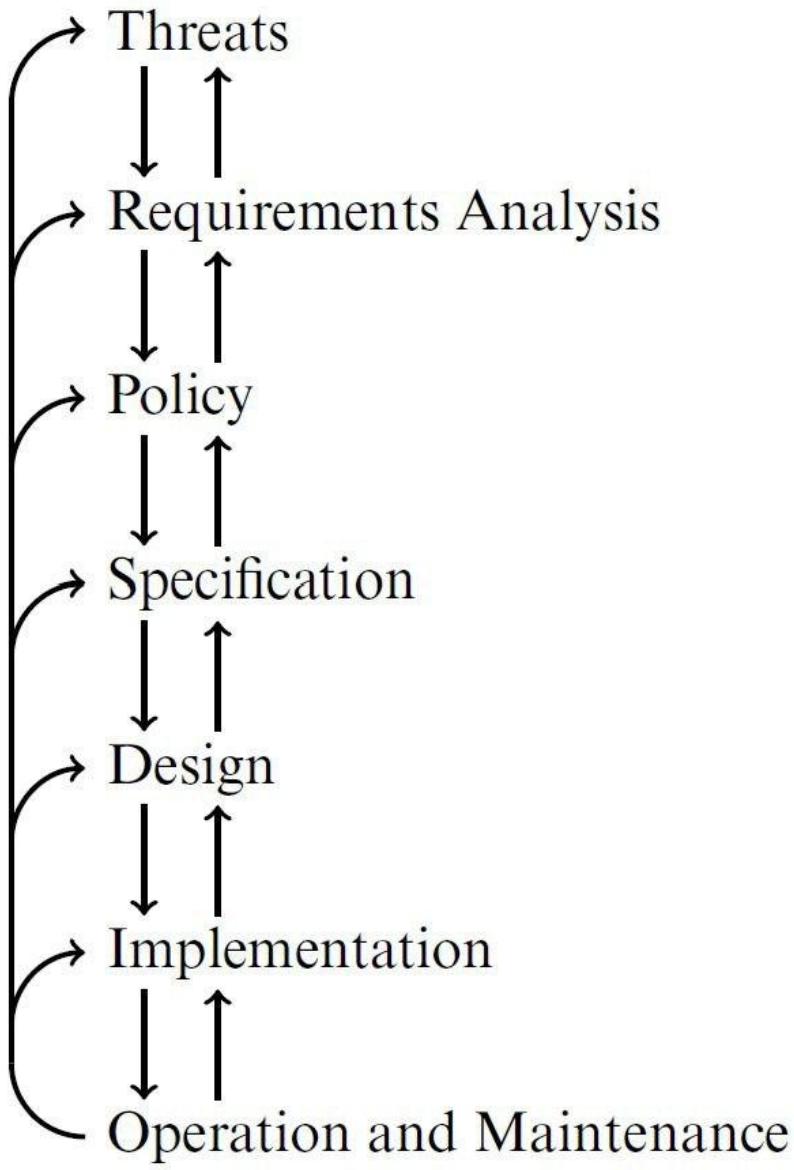
1) Insider Threats by employees through sharing of passwords etc

2) Untrained Personel not following security protocols properly like not backing up data

3) Misconfiguration and wrongly set security policies by the Administrator

4) Social Engineering to manipulate employees to reveal sensitive information

Security Life Cycle :



1. Threats

Identifying potential risks, vulnerabilities, and attack vectors.

Understanding the impact of different types of threats (e.g., cyberattacks, insider threats, natural disasters).

2. Requirements Analysis

Assessing security needs based on the identified threats.

Gathering security requirements from stakeholders, regulations, and industry standards.

3. Policy

Defining security policies and rules to protect the system.

Establishing guidelines for access control, authentication, encryption, and incident response.

4. Specification

Translating security policies into detailed technical specifications.

Defining security mechanisms such as firewalls, intrusion detection systems, and encryption standards.

5. Design

Creating a secure system architecture.

Incorporating security best practices into the design phase.

Ensuring security is integrated from the beginning rather than as an afterthought.

6. Implementation

Developing and deploying security controls according to the design.

Configuring firewalls, authentication systems, and monitoring tools.

Conducting security testing to identify vulnerabilities.

7. Operation and Maintenance

Monitoring the system for security incidents.

Updating security controls and policies as new threats emerge.

Conducting regular security audits and patch management.

Feedback Loops in the Model

The arrows in the diagram indicate a continuous feedback loop between different phases.

If new threats emerge, organizations may need to revise their policies, update specifications, or redesign security mechanisms.

Access Control Matrix : It is the Most Efficient Way to visualize the Protection State of a Network Or Server etc

Access Control Algebra : It is a mathematical Framework used for definition of Access Control Policies, Uses Logical Operators such as AND OR NOT etc

Eg : if ROLE is Manager OR CEO AND Request is for Payroll Data > Access Granted

Protection State Transitions : Modifications can be made in the Access Control Matrix using the Primitive and Conditional commands

+ Primitive :

create object/subject

destroy object/subject

enter (access) into A[subject, object]

delete (access) from A[subject, object]

+ Conditional :

if (condition)

then

Access Control Models : These Models Define how access to data is provided and managed within a system

1) Discretionary AC : The Owner has All Permissions and can easily grant and revoke permissions to individual users (MORE SUITABLE FOR HANDLING PERSONAL FILES)

2) Mandatory AC : A Central Authority decides who has access to what based on the secrecy level of the data and authority of the subject

(MORE SUITABLE FOR HANDLING SENSITIVE INFORMATION)

3) Role Based AC : An Access is granted based on the Role of the Subject , it is easier to manage when there are large number of subjects (MORE SUITABLE FOR CORPORATE ENVIRONMENT)

4) Task Based AC : An Access is Granted Based on the Task assigned to the Subject , Permissions are automatically revoked after the Task is completed (MORE SUITABLE FOR GRANTING PERMISSIONS FOR TEMPORARY TASKS)

Additonal :

- Unified Model : It a combination of several access control models used by an organization for specific tasks

- Temporal Models : Time Based Access , Eg : You can access information after working hours

- Spatio Temporal : Time and Location Based , Eg : you can access office files only from office computers during office hours

ADDITIONAL :

Access Control List : It is an Object Centric List Prepared using the ACM for visualizing the subjects and their access levels to a specific object in the ACM , used in centralized systems like file servers and databases

EG :

file 1 :

sub 1 : read

sub 2 : write

Admin : read , write

Capability Ticket : It is a Subject centric list prepared using the ACM for visualizing the objects and access levels of a Subject in ACM , used more in distributed systems like Cloud Computing

EG :

sub 1 :

File 1 : read

File 2 : read, write