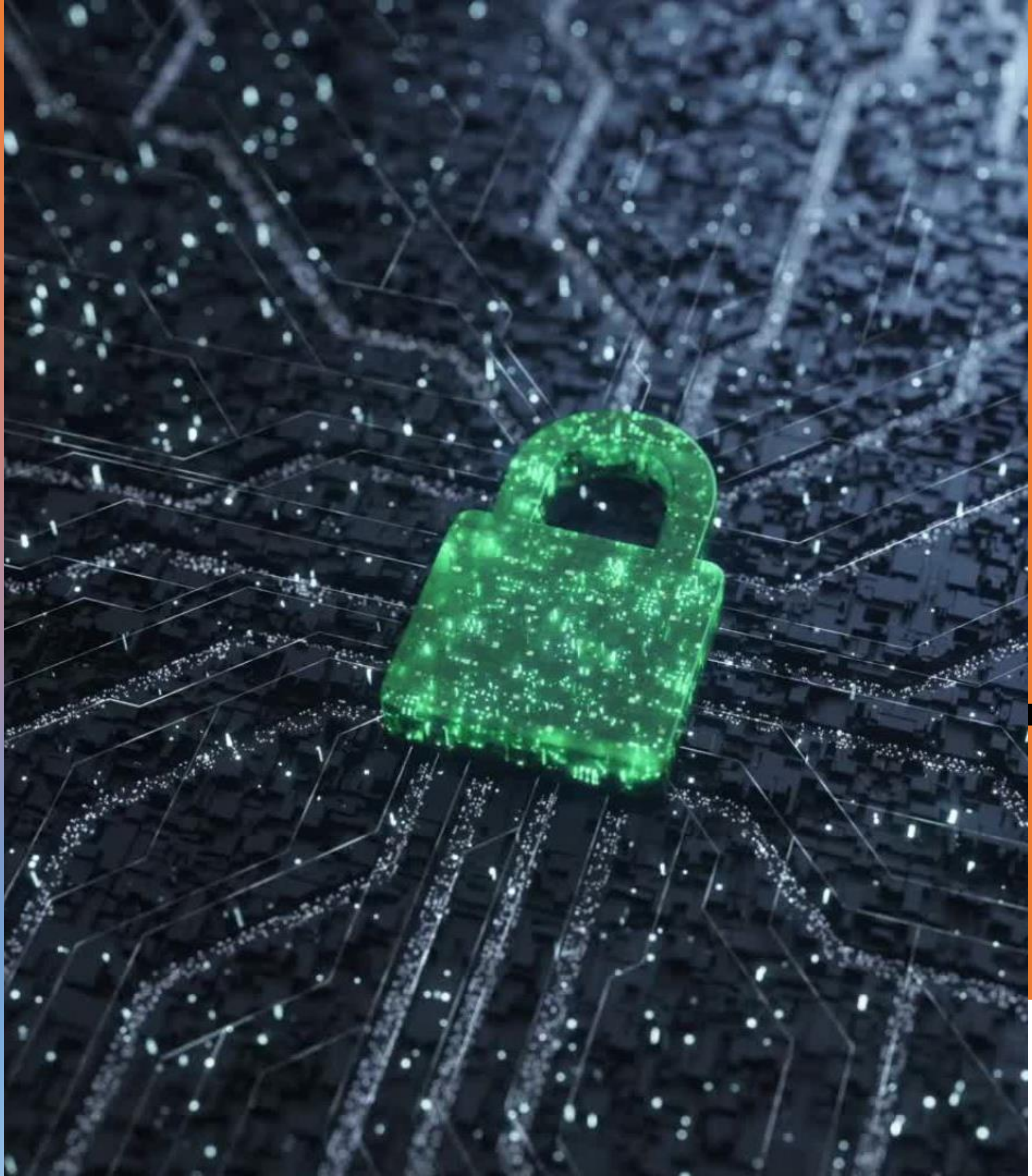


Computer Security
Course Code: COSC4035

Salale University, Department of Computer Science

Getahun

Chapter One

- Introduction to computer Security
  - Basic concepts of computer security
  - Threats, vulnerabilities and control risk
  - Goals of computer security
  - Security attack
  - Security policies and mechanisms
  - Prevention, detection and deterrence
  - Software security assurance

Introduction to Computer Security

- The Protection of the Items You value called the asset of the computer or the computer system

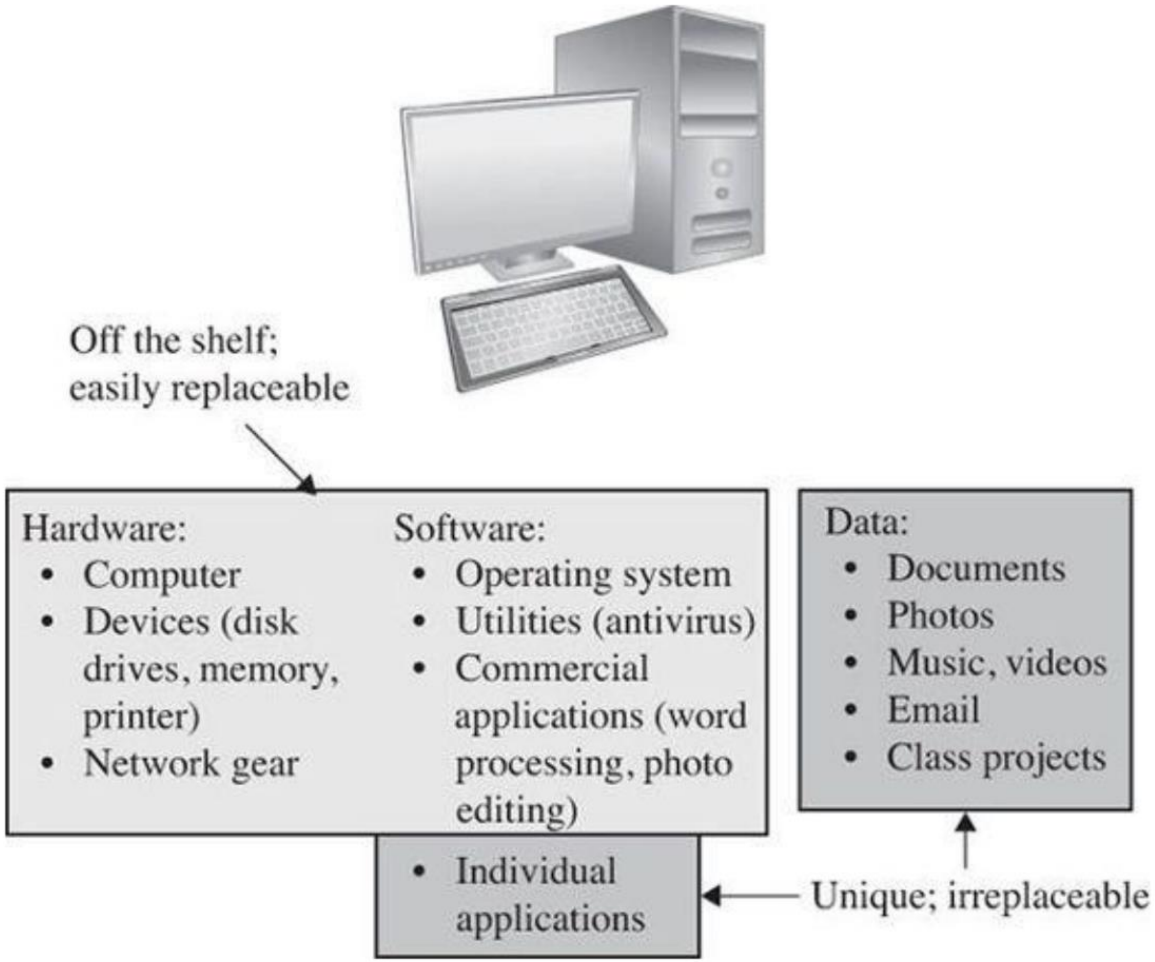
Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

Values of Assets

Assets' values are personal, time dependent, and often imprecise.



Off the shelf; easily replaceable

Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:

- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

- Documents
- Photos
- Music, videos
- Email
- Class projects

Unique; irreplaceable

Threats, Vulnerabilities and Control risk

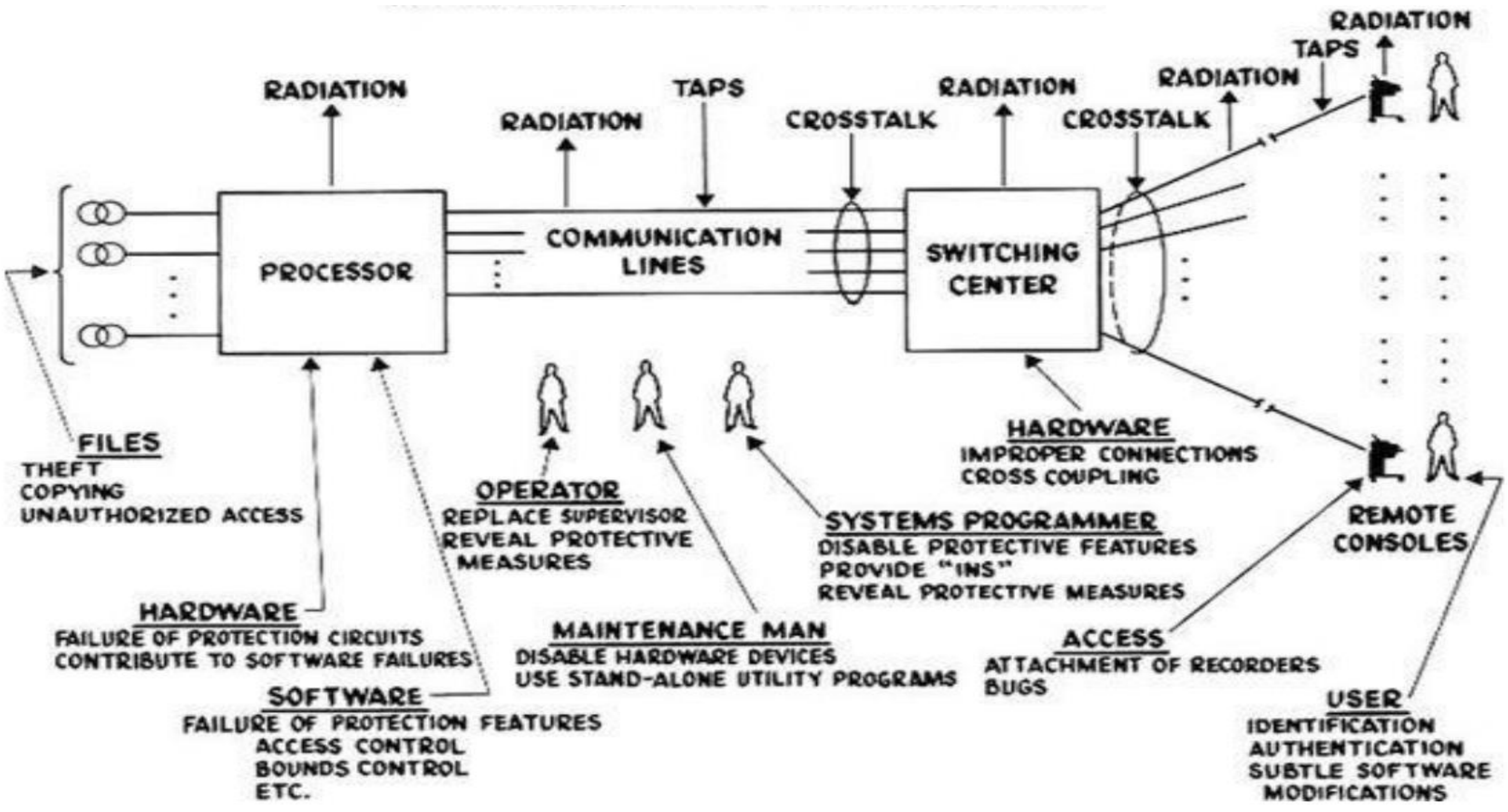
The goal of computer security is protecting valuable assets.

To study different ways of protection, we use a framework that describes how assets may be harmed and how to counter or mitigate that harm.

Threat

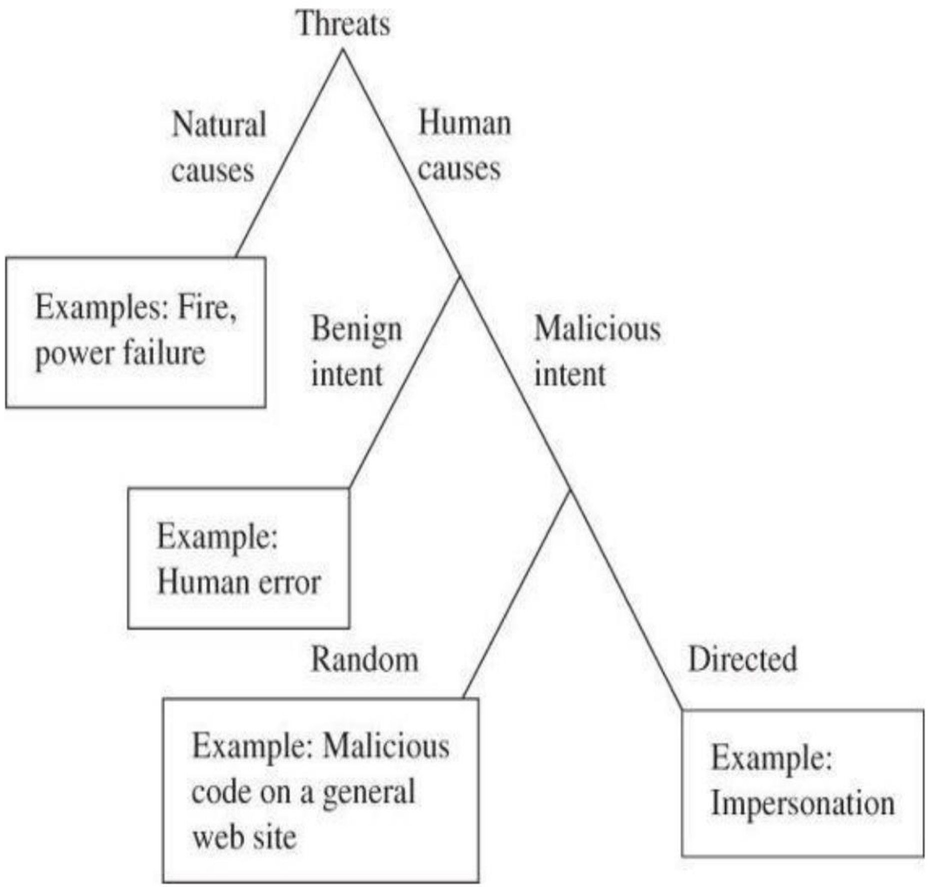
A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.

Threat



Types of Threat in Computer Network

Threat



Types of Threat in Computer Network

Vulnerability

Vulnerability is a weakness in the system

for example, in procedures, design, or implementation, that might be exploited to cause loss or harm.

For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user’s identity before allowing data access.

Control or Countermeasure

A control is an action, device, procedure, or technique that removes or reduces a vulnerability.

Controls prevent threats from exercising vulnerabilities.

Cont…

- We can consider potential harm to assets in two ways:
  - First, we can look at what bad things can happen to assets, and
  - Second, we can look at who or what can cause or allow those bad things to happen.
- These two perspectives enable us to determine how to protect assets.
- These three aspects, confidentiality, integrity, and availability, make your computer valuable to you.

Goals of Computer Security

- ***Availability***: the ability of a system to ensure that an asset can be used by any authorized parties
- ***Integrity***: the ability of a system to ensure that an asset is modified only by authorized parties
- ***Confidentiality***: the ability of a system to ensure that an asset is viewed only by authorized parties

Goals of Computer Security

Authentication: the ability of a system to confirm the identity of a sender

Non-repudiation of accountability: the ability of a system to confirm that a sender cannot convincingly deny have sent something

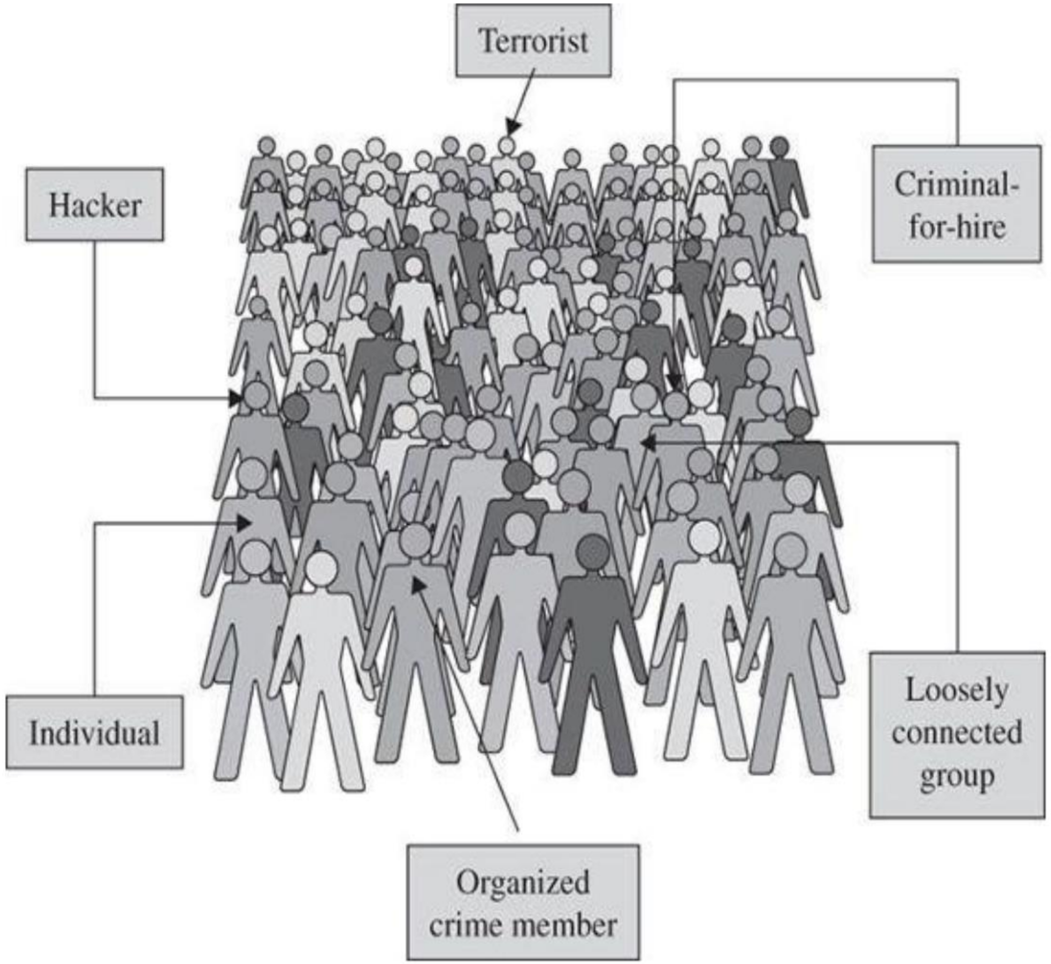
Auditability: the ability of a system to trace all actions related to a given asset

Security Attack

security attacks refer to the sets of actions that the threat actors perform to gain any unauthorised access, cause damage to systems/computers, steal data, or compromise the computer networks.

An attacker can launch a security attack from any location.

Security Attack



attackers look just like anybody in a crowd.

Security policies and mechanisms

- Security policies and mechanisms are two fundamental components of cybersecurity that work together to protect information systems and assets from unauthorized access, use, disclosure, disruption, modification, or destruction

Security Policies

- Clarity: Well-defined and easy to understand
- Comprehensiveness: Covers all aspects of information security
- Enforceability: Mechanisms in place to ensure compliance
- Regular Review: Updated as technology and threats evolve
- Prevent unauthorized access: Define who can access what and under what conditions
- Protect sensitive data: Establish safeguards to prevent data breaches
- Maintain system integrity: Ensure systems are not compromised or disrupted
- Promote responsible behavior: Guide users in using systems and data securely
- Access control policies: Define who can access what systems and resources
- Data classification policies: Classify data based on sensitivity and protection requirements

Security Policies

- Password policies: Establish rules for password creation, storage, and usage
- Acceptable use policies: Specify what is considered acceptable and unacceptable behavior on systems
- Incident response policies: Outline procedures for handling security breaches and incidents

Security Mechanisms

- Firewalls: Filter network traffic to control access and prevent unauthorized intrusions
- Intrusion detection and prevention systems : Monitor network activity for suspicious behavior and take action to block or mitigate attacks
- Encryption: Encodes data to protect its confidentiality and integrity during transmission and storage
- Authentication and authorization: Verify user identities and grant appropriate levels of access
- Data backups and recovery: Protect data from loss or damage and enable restoration in case of incidents
- Vulnerability scanning and patching: Identify and address system vulnerabilities to reduce attack surface

Relationship between Security Policies and Mechanisms

Security policies provide the guiding principles for information security, while security mechanisms implement and enforce those principles

Policies define what should be done, while mechanisms determine how it should be done

The corresponding security mechanism would be an authentication system that verifies user identities and grants access based on predefined permissions

Importance of Security Policies and Mechanisms

Effective security policies and mechanisms are essential for protecting information systems and assets from cyberattacks and data breaches

They provide a structured approach to managing security risks and ensuring the confidentiality, integrity, and availability of information

By implementing comprehensive security policies and mechanisms, organizations can significantly reduce their vulnerability to cyber threats and safeguard their valuable data and systems

Software security assurance

Access control: This involves using passwords, firewalls, and other tools to control who can access systems and data

Data encryption: This involves scrambling data so that it can only be read by authorized users

Vulnerability management: This involves identifying and fixing weaknesses in systems and software

Security awareness training: This involves educating users about security risks and how to protect themselves

Some common detection techniques include:

Intrusion detection systems : These systems monitor network traffic for signs of unauthorized access

Security information and event management : These systems collect and analyze data from multiple sources to identify security incidents

Log analysis: This involves reviewing logs of system activity to identify suspicious behavior

Threat intelligence: This involves gathering information about known threats to help identify and respond to attacks

Some common deterrence techniques include:

- Penalties for unauthorized access: This can include fines, imprisonment, or other legal consequences
- Public disclosure of security breaches: This can damage an attacker's reputation and make it more difficult for them to operate
- Security certifications: These demonstrate to customers and partners that an organization takes security seriously
- Security research and development: This helps to identify and fix vulnerabilities before they can be exploited

Here are some additional tips for preventing, detecting, and deterring cyberattacks:

KEEP YOUR SOFTWARE UP TO DATE

USE STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION

BE CAREFUL ABOUT WHAT LINKS YOU CLICK ON AND WHAT ATTACHMENTS YOU OPEN

BACK UP YOUR DATA REGULARLY

REPORT SUSPICIOUS ACTIVITY TO YOUR IT DEPARTMENT

Software security assurance

Threat modeling: Identifying and analyzing potential threats to the software

Requirements definition: Defining security requirements for the software

Design review: Reviewing the software design to identify and address security flaws

Code review: Reviewing the software code to identify and address security vulnerabilities

Testing: Performing security testing to identify and address security weaknesses

Deployment: Deploying the software securely

Maintenance: Maintaining the software securely over its lifecycle

Benefits of Software Security Assurance

Reduced risk of security vulnerabilities: SSA helps to identify and address security vulnerabilities before they can be exploited by attackers

Improved protection of data and resources: SSA helps to protect the data and resources that are contained in and controlled by software

Reduced costs of security breaches: SSA can help to reduce the costs of security breaches by preventing them from happening in the first place

Increased customer trust: SSA can help to increase customer trust by demonstrating that an organization takes security seriously

Implementing Software Security Assurance

Establish a security policy: A security policy defines an organization's commitment to security and outlines the organization's security requirements

Appoint a security champion: A security champion is responsible for promoting and overseeing SSA activities within the organization

Train employees on security: Employees need to be trained on security awareness and best practices in order to help protect the organization's systems and data

Use secure development tools and practices: There are a number of secure development tools and practices that can be used to help identify and address security vulnerabilities

Implementing Software Security Assurance

Implement a vulnerability management program: A vulnerability management program helps to identify, prioritize, and remediate security vulnerabilities

Monitor and audit systems and data: Organizations need to monitor and audit their systems and data to identify and address security incidents

Implementing Software Security Assurance

Open Web Application Security Project : https://owasp.org/

Software Engineering Institute Carnegie Mellon University: https://www.sei.cmu.edu/

National Institute of Standards and Technology : https://www.nist.gov/