Computer Security

CS433

Objectives

Define	Define computer security as well as basic computer security terms
Introduce	Introduce the C-I-A Triad
Introduce	Introduce basic access control terminology
Explain	Explain basic threats, vulnerabilities, and attacks
Show	Show how controls map to threats

What Is Computer Security?

The protection of the assets of a computer system

- Hardware
- Software
- Data

Assets

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

Off the shelf; easily replaceable

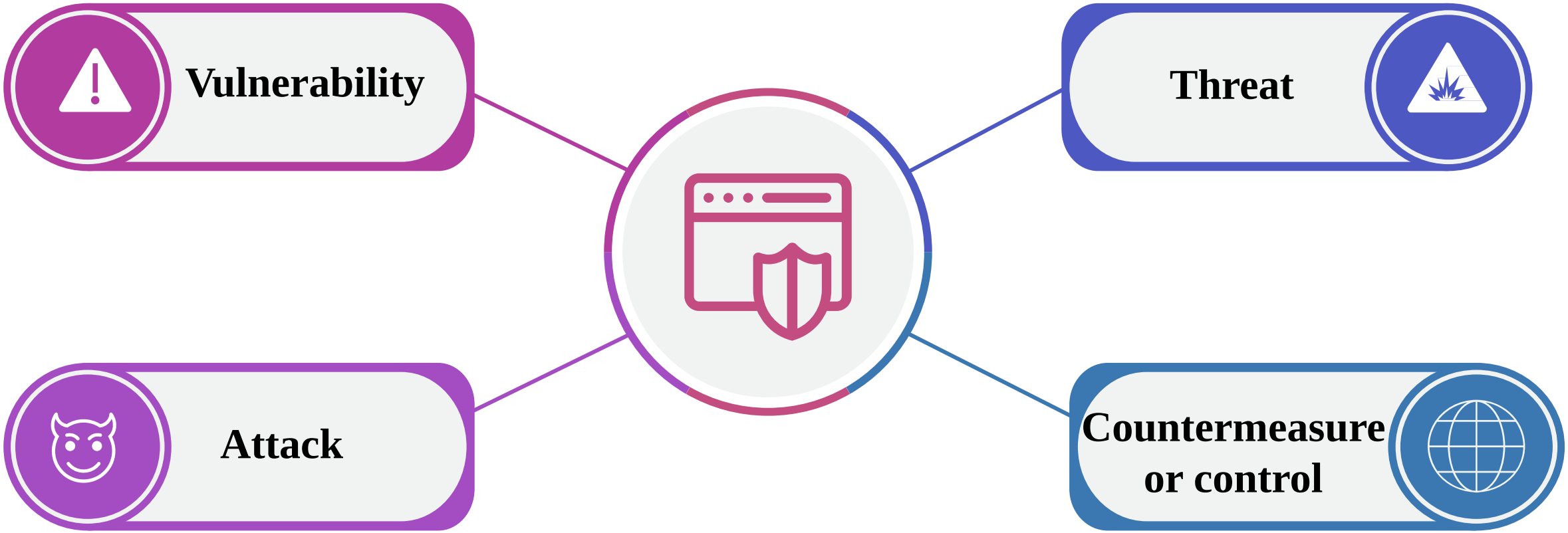
Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

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

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

Unique; irreplaceable

Basic Terms



Basic Terms

Vulnerability

A weakness in the system (i.e., in procedures, design, or implementation), that might be exploited to *cause loss or harm*.

Threat

A set of circumstances that has the *potential to cause loss or harm*.

- A potential violation of security.

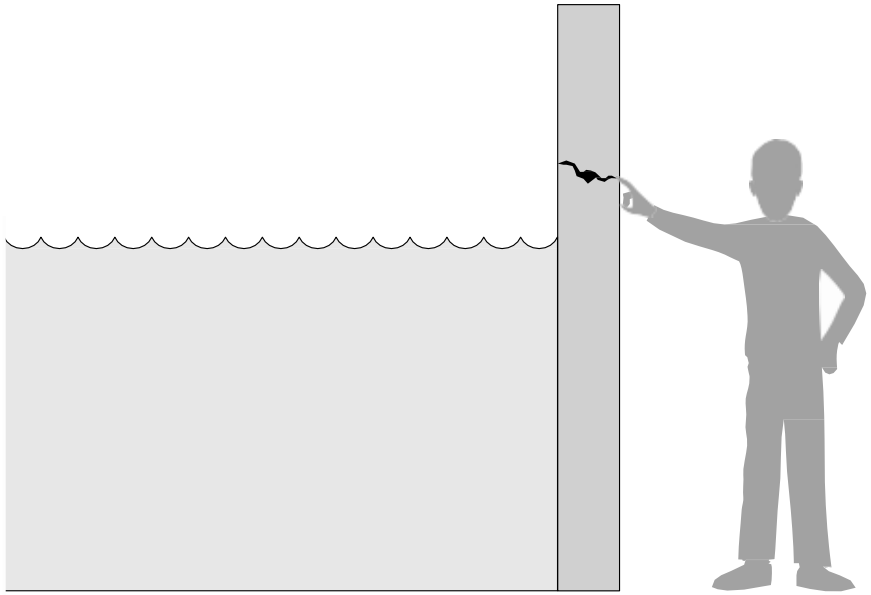
Attack

An attempt to break into a system to cause harm. A human (*criminal*) who exploits a vulnerability perpetrates an attack on the system

Countermeasure or control

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

Threat and Vulnerability



Relationship among threats, controls, and vulnerabilities:

- A threat is blocked by control of a vulnerability.
- To devise controls, we must *know as much about threats as possible*.

The fact that the violation might occur means that the actions that might cause it should be *guarder against.*

C-I-A Triad

Confidentiality

Integrity

Availablity

C-I-A Triad

Sometimes two other desirable characteristics:

Authentication

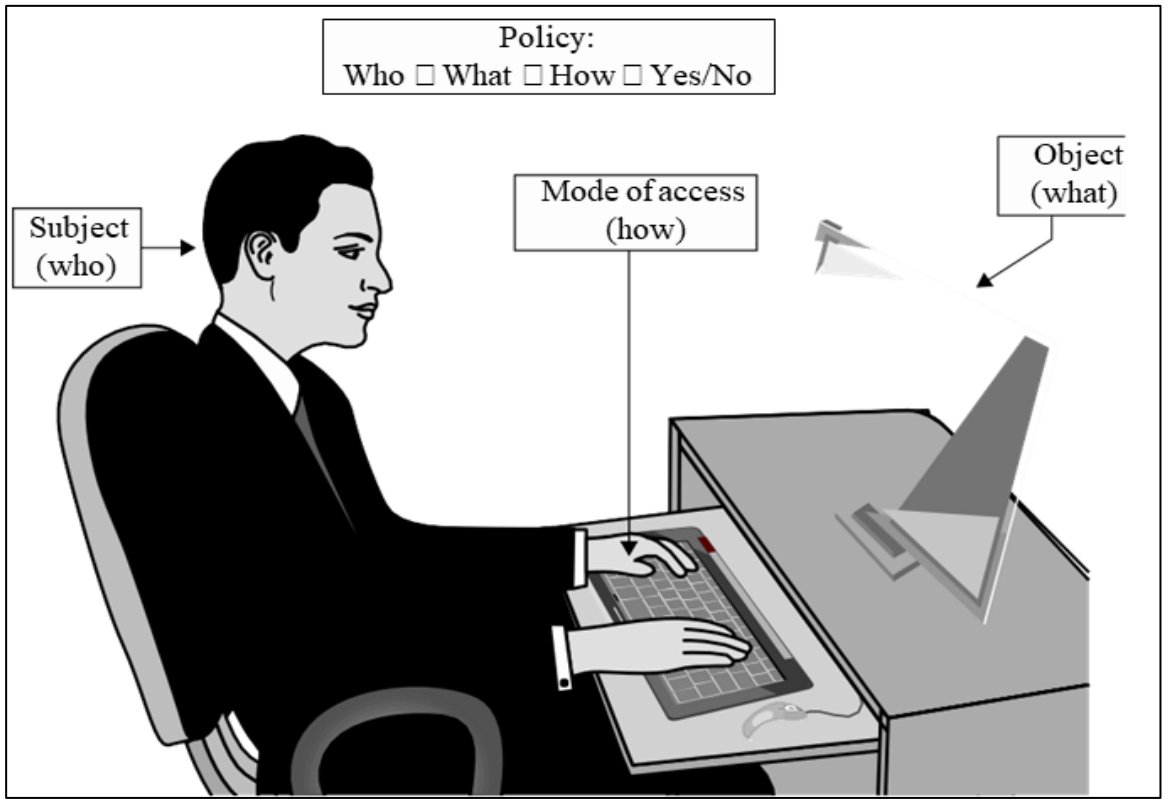
- The process or action of proving or showing something to be true, genuine, or valid.

Nonrepudiation

- Is the assurance that someone cannot deny something.
- i.e. **nonrepudiation** refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

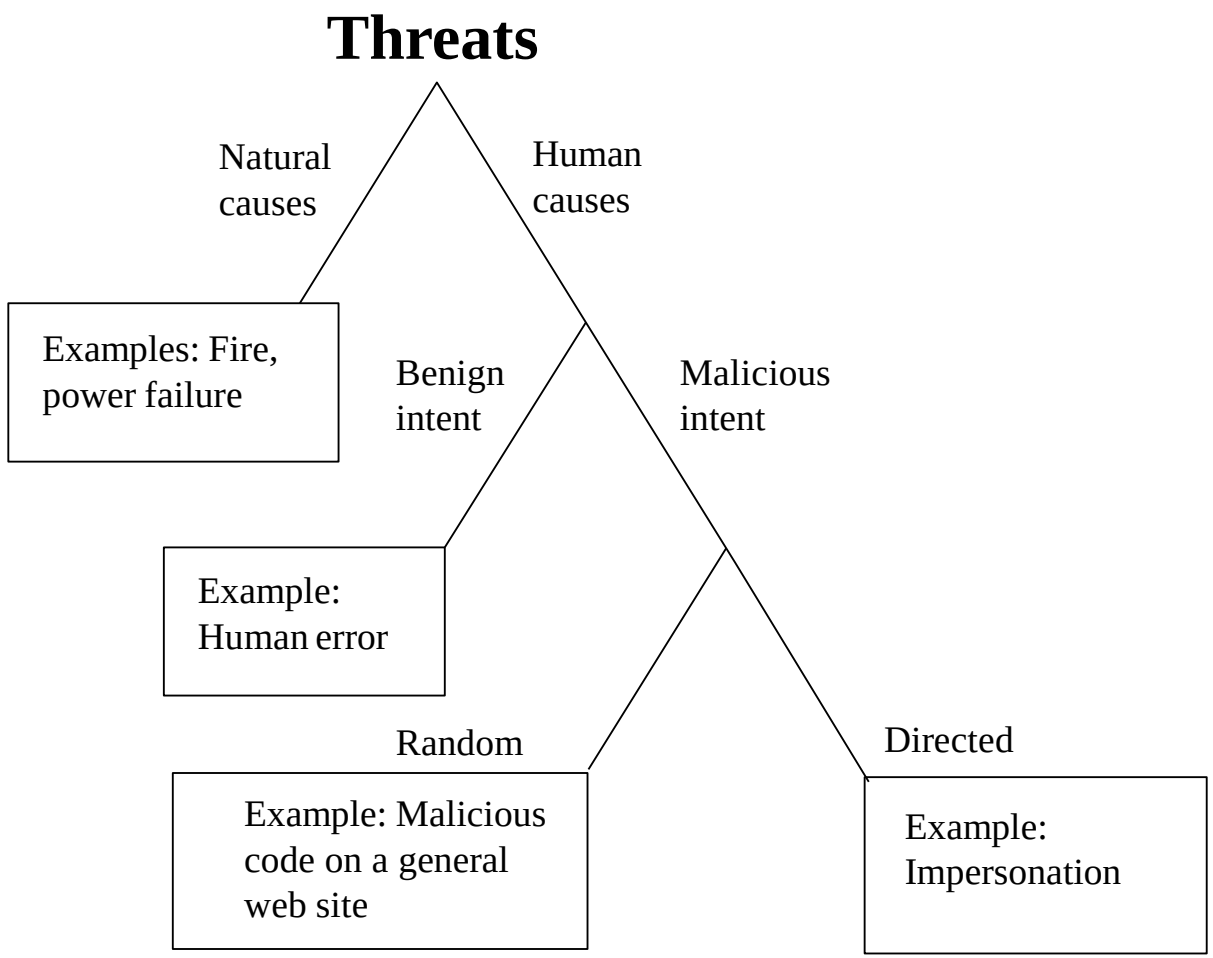
Access Control

Access control: limiting who can access what in what ways



- (Who)➔ Subjects: i.e: human users
- (What)➔ Objects: are things on which an action can be performed
  - i.e: Files, programs, hardware devices.
- (How) ➔ Access modes are any controllable actions of subjects on objects
  - i.e: read, write, modify, delete,

Types of Threats

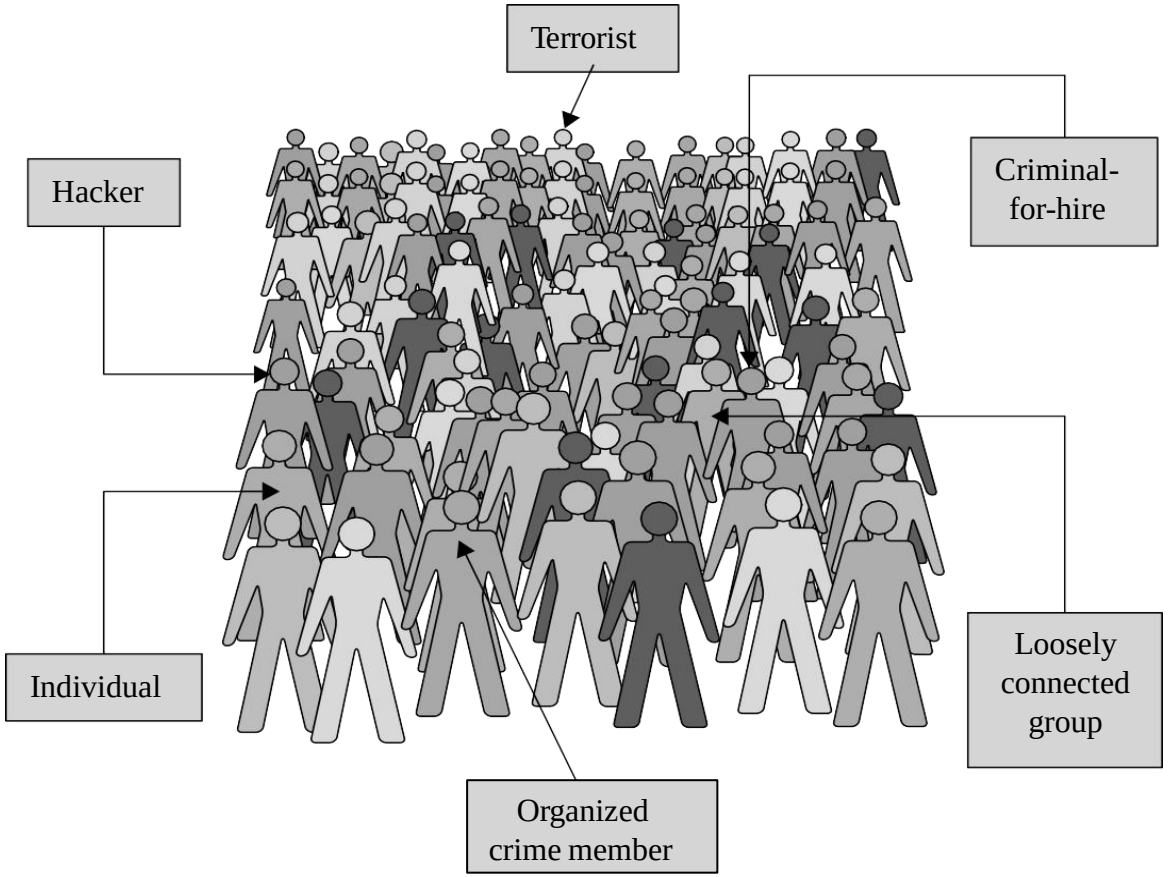


(APT): Advanced Persistent Threat

- APT is a special type of threat that has only been taken seriously by the broad security community over the past decade.
- Security experts believe that no one who becomes a high-priority target can truly be safe from APT.

APT has the following characteristics:				
Organized	Directed	Well financed	Patient	Silent

Types of Attackers



- Each of these attacker types is associated with a different set of *resources*, *capabilities*, and *motivations*.
- Understanding the different types will help in considering threats.

Method, Opportunity, and Motive

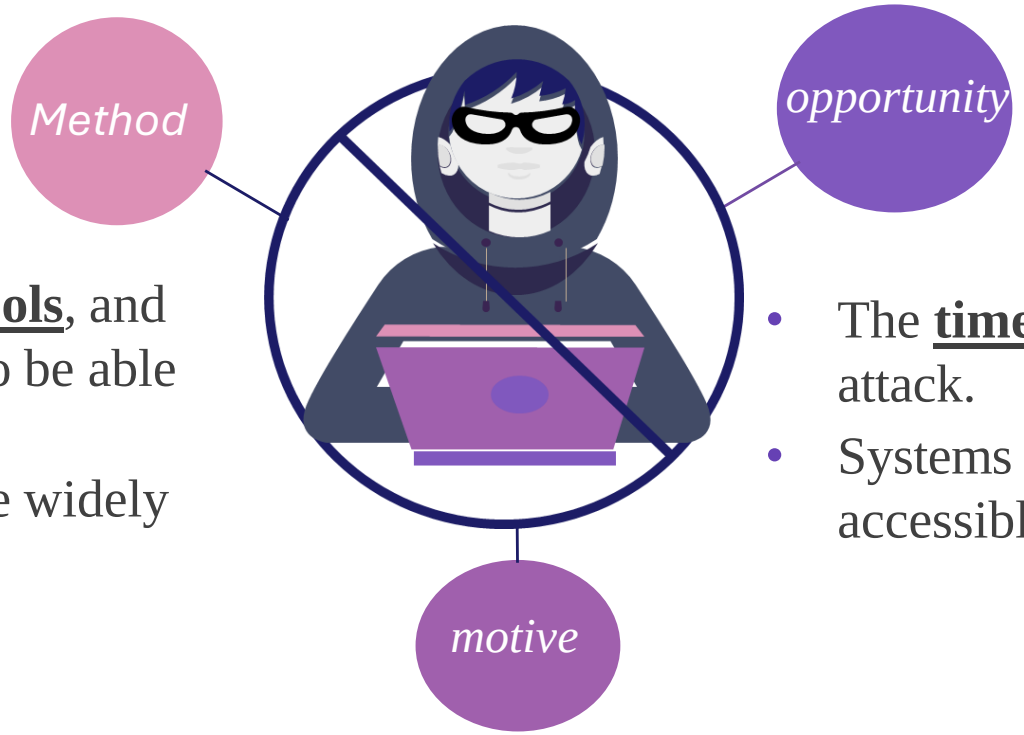
Opportunity

Motive

Method

Method, Opportunity, and Motive

A malicious attacker must have **three things (MOM)**:



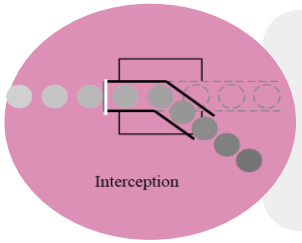
- The **skills**, **knowledge**, **tools**, and other things with which to be able to pull off the attack
- Knowledge of systems are widely available.

- The **time** and **access** to accomplish the attack.
- Systems available to the public are accessible to them

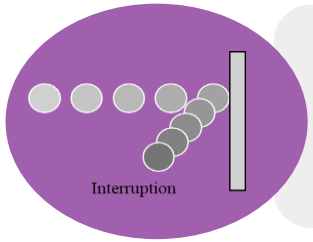
A **reason** to want to perform this attack against this system

MOM are all necessary for an attack to succeed; deny any of these and the attack will fail.

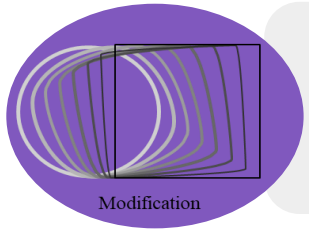
Types of Harms/ Threa



In an **interception** means that some unauthorized party has gained access to an asset.



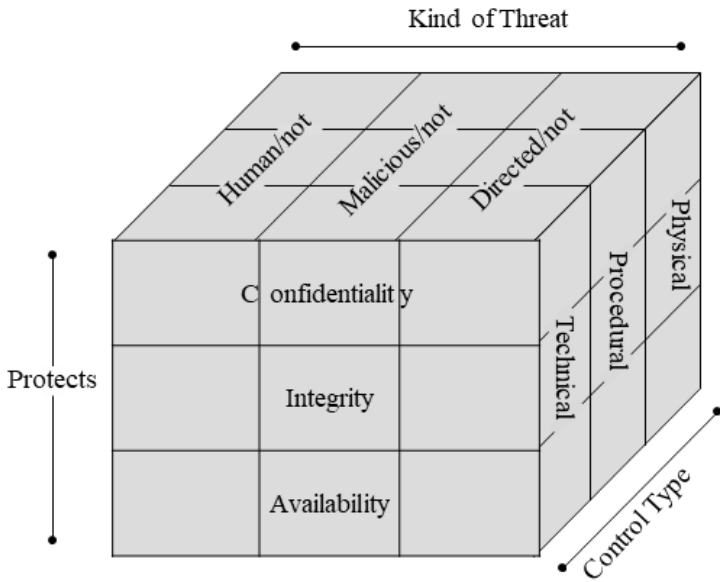
In an **interruption**, an asset of the system becomes lost, unavailable, or unusable.



If an unauthorized party not only accesses but **tampers** (forges) with an asset, the threat is a **modification**.

An unauthorized party might create a **fabrication** of ***counterfeit*** objects on a computing system.

Controls/Countermeasures



This representation shows the three dimensions by which a control can be categorized.

Thinking about controls in this way enables you to easily map the controls against the threats they help address.

Control Type

- Physical
- Procedural
- Technical

Protects

- Confidentiality
- Integrity
- Availability

Kind of threat

- Human/not
- Direct/not
- Malicious/not

Security Goals

When we talk about computer security, we mean that we are addressing three important aspects of any computer-related system: confidentiality, integrity, & availability (CIA)

confidentiality

- ensures that computer-related assets are accessed only by authorized parties.
  - **i.e**. reading, viewing, printing, or even knowing their existence
  - Secrecy or privacy

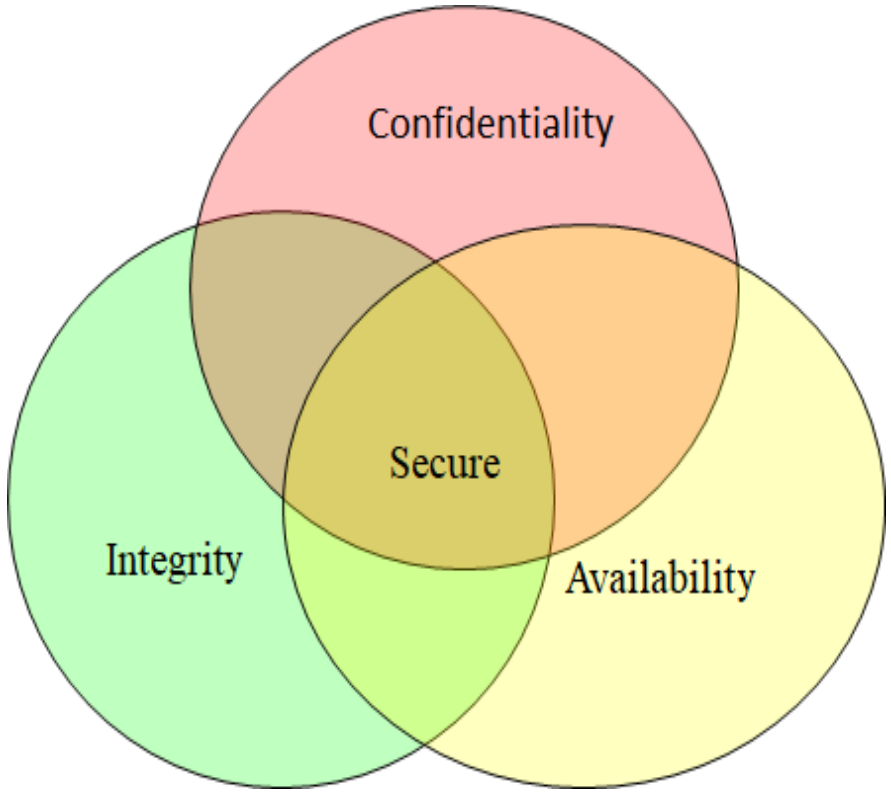
integrity

- means that assets can be modified only by authorized parties or only in authorized ways.
- **i.e**. writing, changing, deleting, creating

availability

- means that assets are accessible to authorized parties at appropriate times.
- **i.e.** often, availability is known by its opposite, denial of service.

Relationship between Confidentiality Integrity and Availability



In fact, these three characteristics can be independent, can overlap, and can even be mutually exclusive.

Confidentiality, Integrity, and Availability

Ensuring confidentiality can be difficult.

For example, who determines which people or systems are authorized to access the current system? By "accessing" data, do we mean that an authorized party can access a single bit? the whole collection? pieces of data out of context? Can someone who is authorized disclose those data to other parties?

We understand confidentiality well because we can relate computing examples to those of preserving confidentiality in the real world.

Confidentiality, **Integrity**, and Availability

Integrity is much harder to pin down.

Integrity means different things in different contexts.
• Precise, unmodified, modified only in acceptable ways, modified only by authorized people, modified only by authorized processes, consistent, meaningful and usable

Integrity can be enforced in much the same way as can confidentiality: by rigorous control of ***who or what can access which resources in what ways***.

Confidentiality, Integrity, and Availability

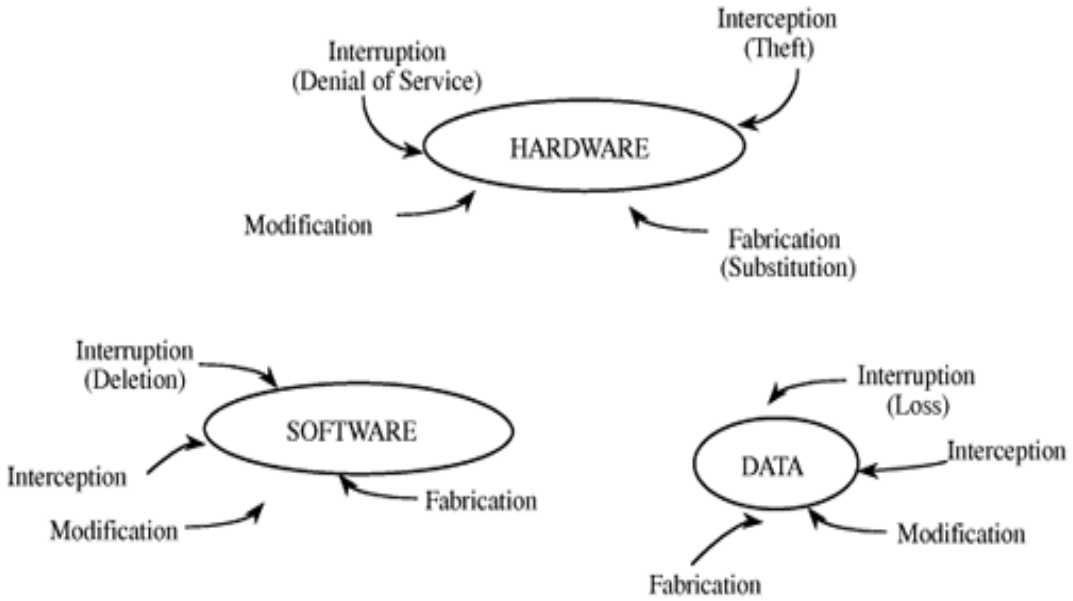
Availability applies both to data and to services

That is, to information and to information processing. We say a data item, service, or system is available

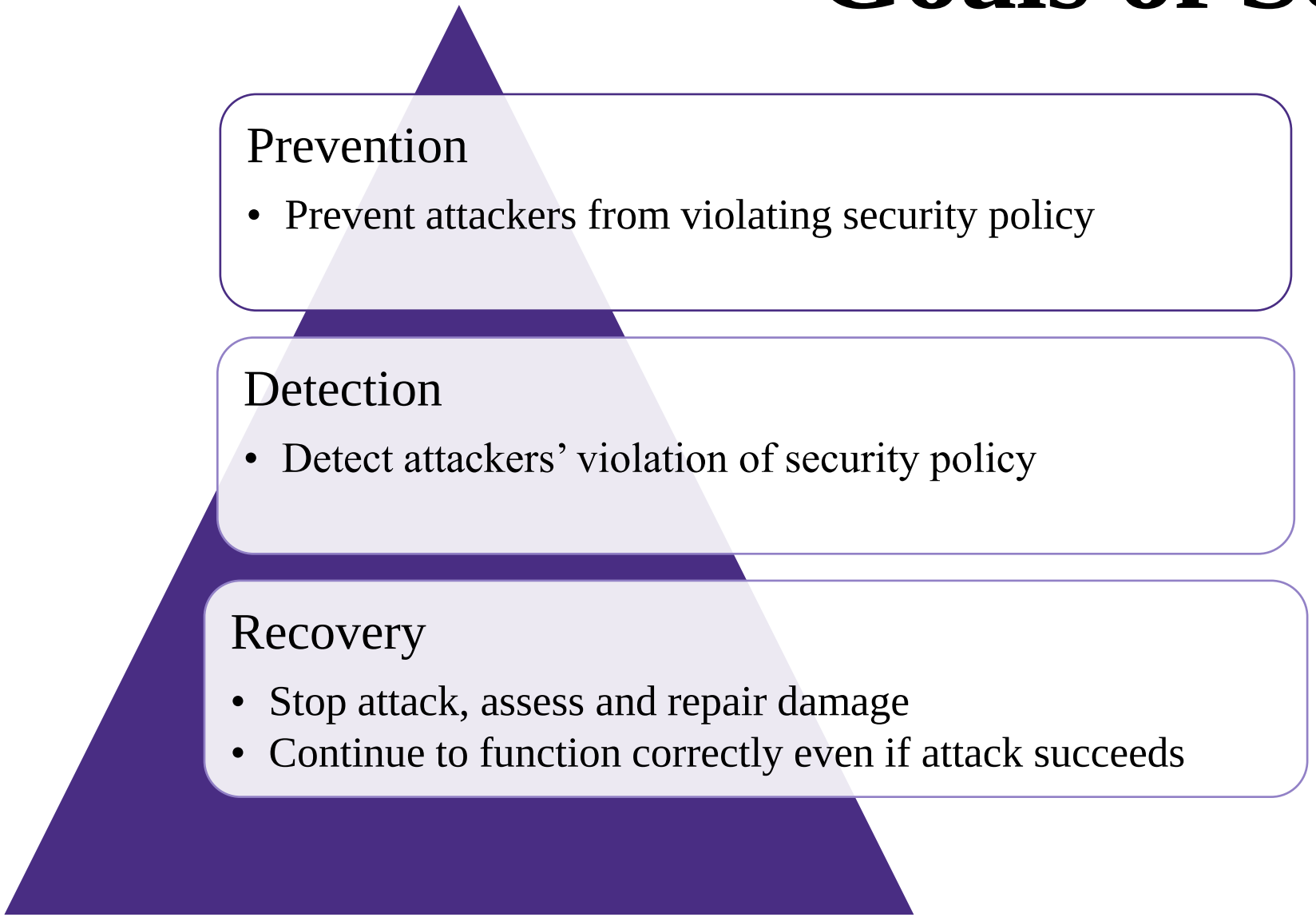
The service or system involved follows a philosophy of fault tolerance, whereby hardware or software faults lead to graceful cessation of service or to work-arounds rather than to crashes and abrupt loss of information.

Security Testing: Vulnerabilities and Threats

- When we prepare to test a system, we usually try to **imagine how the system can fail**;
  - we then look for ways in which the requirements, design, or code can enable such failures.
  - Imagine **the vulnerabilities** that would prevent us from reaching one or more of our three security goals.



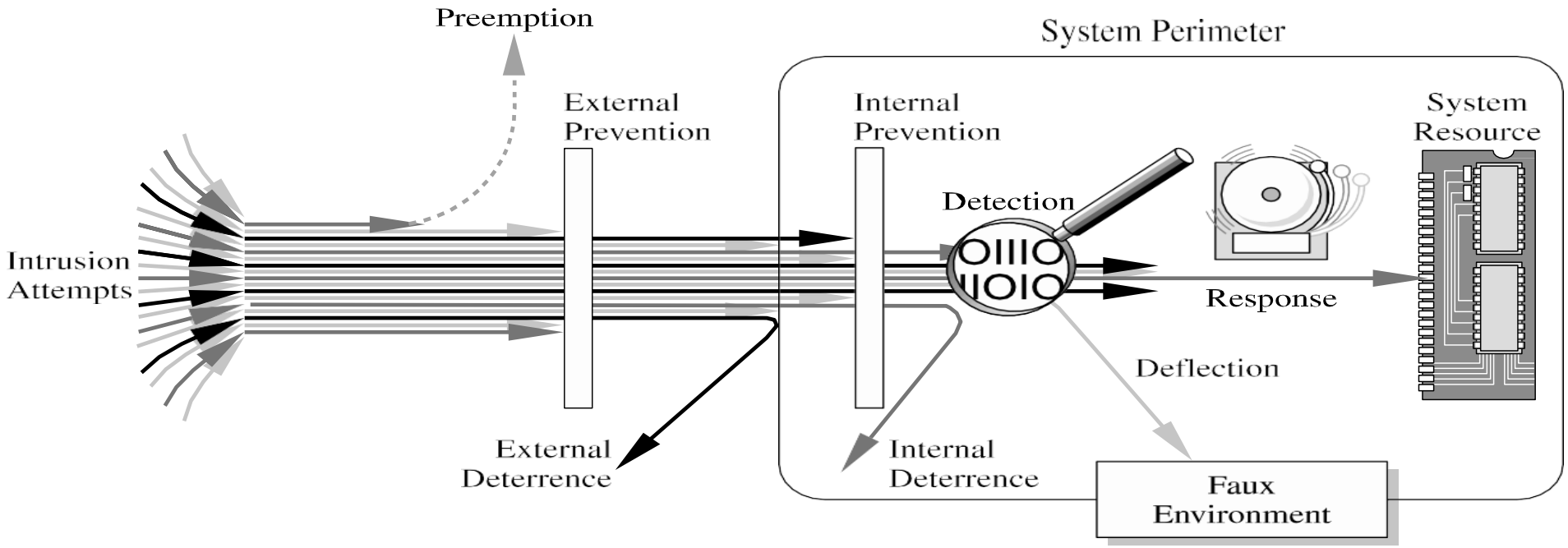
Goals of Security



Different Types of Controls

The figure illustrates how a combination of controls can be used to secure valuable resources.

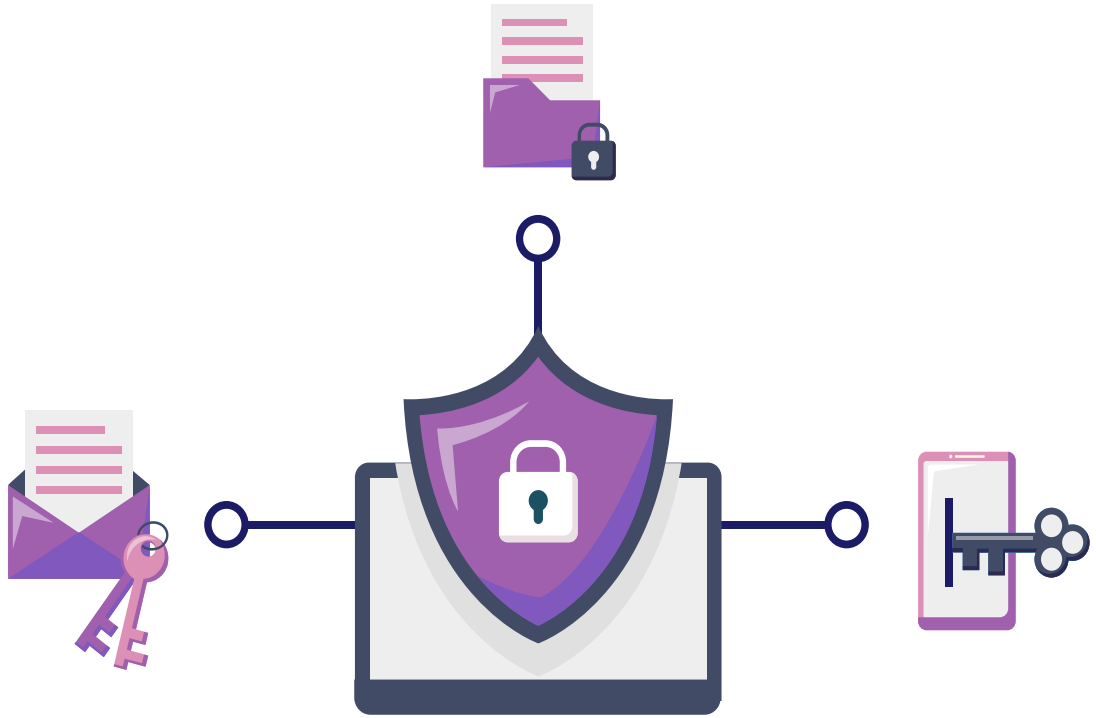
- In this simple representation of a networked system, it is easy to see all the touch points where controls can be placed, as well as some different types of controls, including deterrence, deflection, response, prevention, and preemption.



Control Available

Policies and Procedures

Physical Controls



Technical Control

Control Available

Technical controls
counter threats with technology (hardware or software)

Encryption

- We take data in their normal, unscrambled state, called:
  - **cleartext** or **plaintext**, and transform them so that they are unintelligible to the outside observer;
  - The transformed data are called **enciphered** text or **ciphertext**.

- **Encryption** clearly addresses the need for **confidentiality** of data.

- Additionally, it can be used to ensure **integrity**;
  - data that cannot be read generally cannot easily be changed in a meaningful manner.

Control Available

Technical controls
counter threats with technology (hardware or software)

Software/Program Controls

- Programs must be secure enough to *prevent outside attack*
- They must also be developed and maintained so that we can be confident of the programs' dependability.

Development controls:

- Quality standards under which a program is **designed**, **coded (implementation)**, **tested**, and maintained to prevent software faults from becoming exploitable vulnerabilities

Hardware Controls

- Numerous hardware devices have been created to assist in providing computer security.

Control Available

Policies and Procedures

use a command or agreement

Physical Controls

Stop or block an attack by using something tangible

Principle of Weakest Link

Security can be no stronger than its weakest link !!!

Whether it is the power supply that powers the firewall or the operating system under the security application or the human who plans, implements, and administers controls, a failure of any control can lead to a security failure.

Summary

- Vulnerabilities are weaknesses in a system;
  - threats exploit those weaknesses;
  - controls protect those weaknesses from exploitation
- Confidentiality, integrity, and availability are the three basic security primitives
- Different attackers pose different kinds of threats based on their capabilities and motivations
- Different controls address different threats; controls come in many flavors and can exist at various points in the system