Cyber Security

ICT 3156

IPSITA UPASANA

Syllabus

- Course Objectives
- Course Outcomes
- Books

Books

1. Pfleeger C. P., Pfleeger S. L. and Margulies J., Security in Computing (5e), Prentice Hall, 2015.

2. Akhgar B., Staniforth A. and Bosco F., Cyber Crime and Cyber Terrorism Investigator's Handbook (1e), Syngress Publishing, 2014.

3. Hubbard D. W. and Seiersen R., How to Measure Anything in Cybersecurity Risk, John Wiley & Sons, 2016.

4. Mitnick K. D. and Simon W. L., Art of Intrusion, Wiley Publishing Inc. 2005.

5. Singer P. W. and Friedman A., Cybersecurity and Cyber war- What Everyone Needs to Know, Oxford.

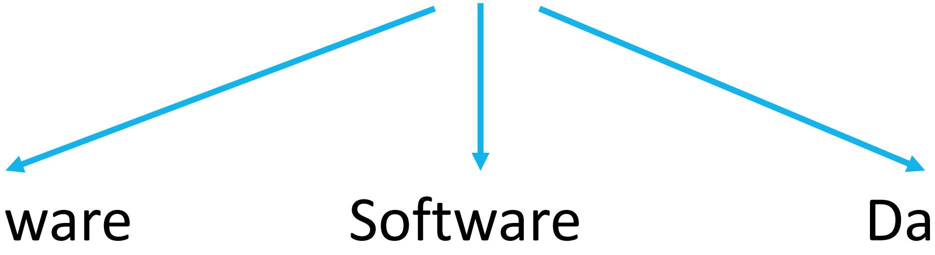
Introduction

- What is Security?
- Why do we (human beings) need security?

Introduction to Computer Security

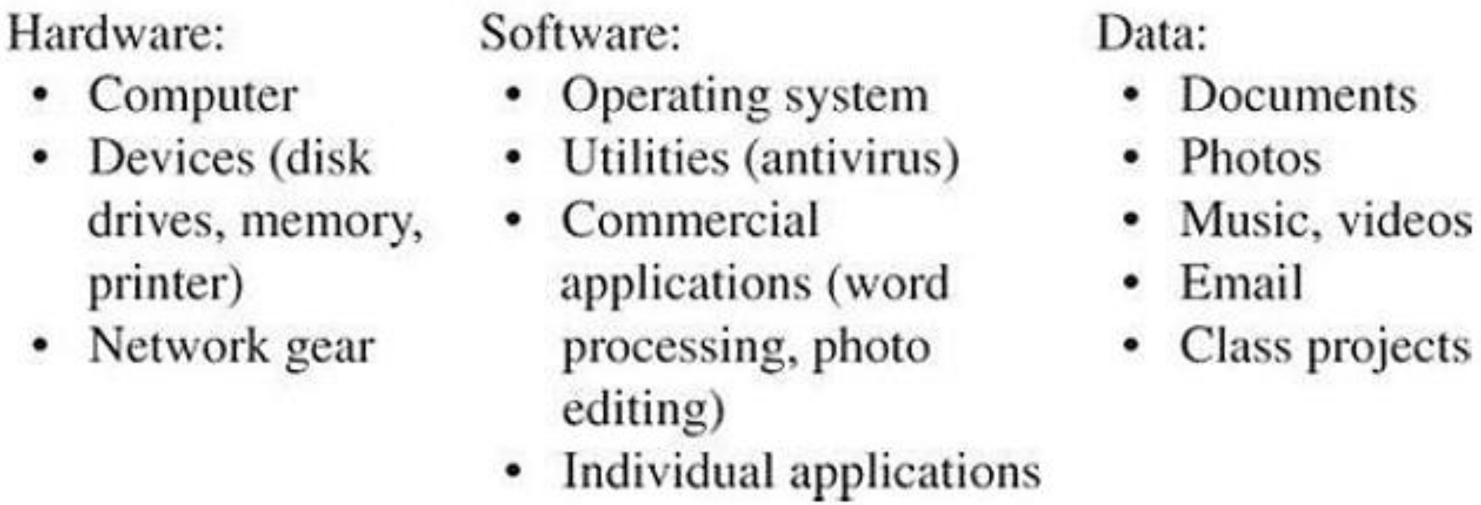
- The protection of the **ASSETS** of a computer system.

What makes the assets worthy of protection?


Hardware

Software

Data


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

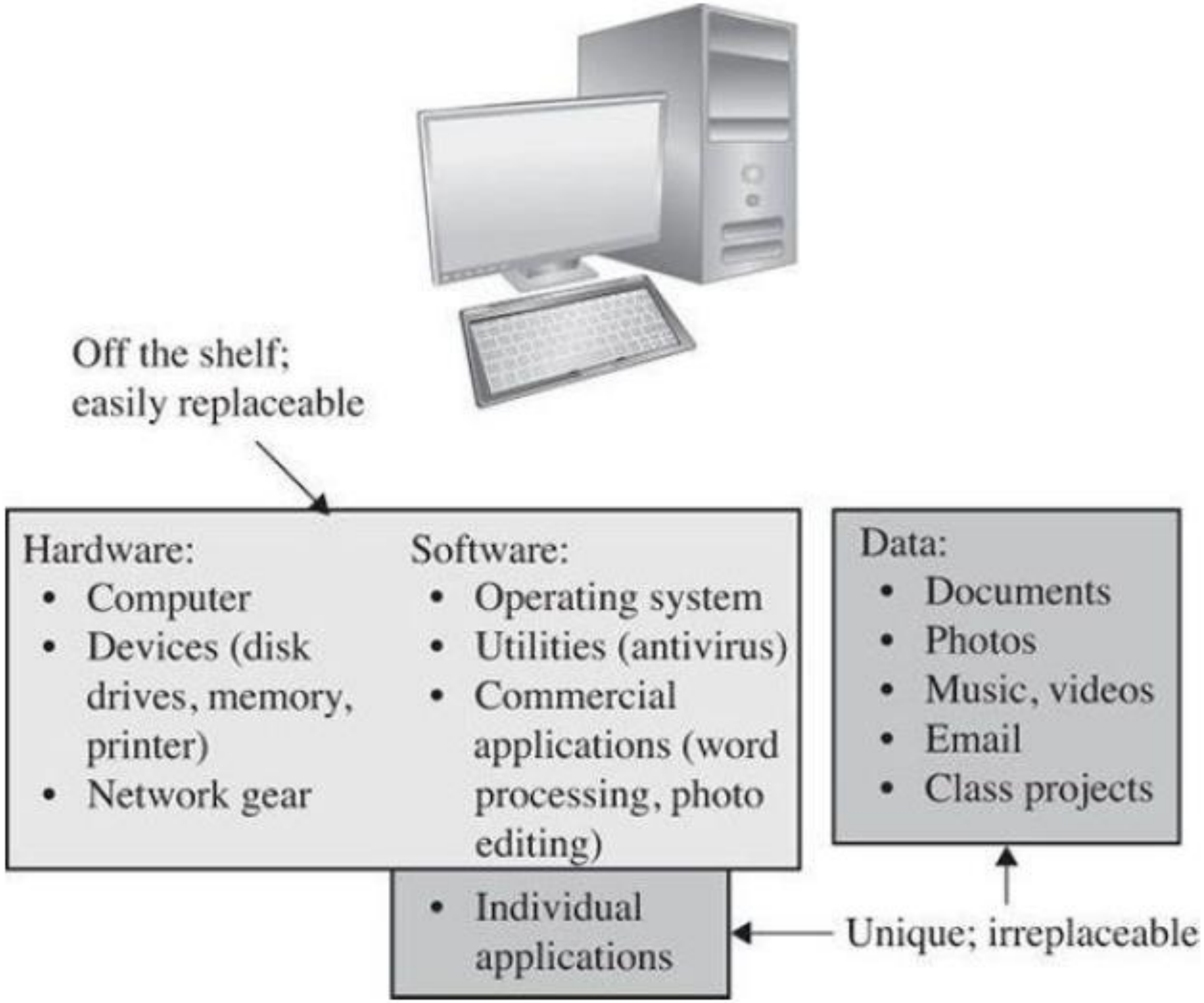
Represent intellectual endeavor or property.

Values of Assets

- The value of an asset depends on the asset owner's or user's perspective.
- Assets' values are **personal**, **time dependent**, and often **imprecise**.

The goal of computer security is **protecting** valuable assets.

1. How can assets be harmed?
2. How to control it?



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

- Vulnerability
- Threat
- Attack
- Control

Basic Terms

- Vulnerability

  A vulnerability is a weakness **in the system** that might be exploited to cause loss or harm.

  in procedures, design, or implementation, and so on.

- Threat
- Attack
- Control

Basic Terms

- Vulnerability
- Threat

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

- Human-initiated
- Computer-initiated
- Natural Disasters

- Attack
- Control

Basic Terms

- Vulnerability
- Threat
- Attack

  A human who exploits a vulnerability perpetrates an **attack** on the system. An attack can also be launched by another system.

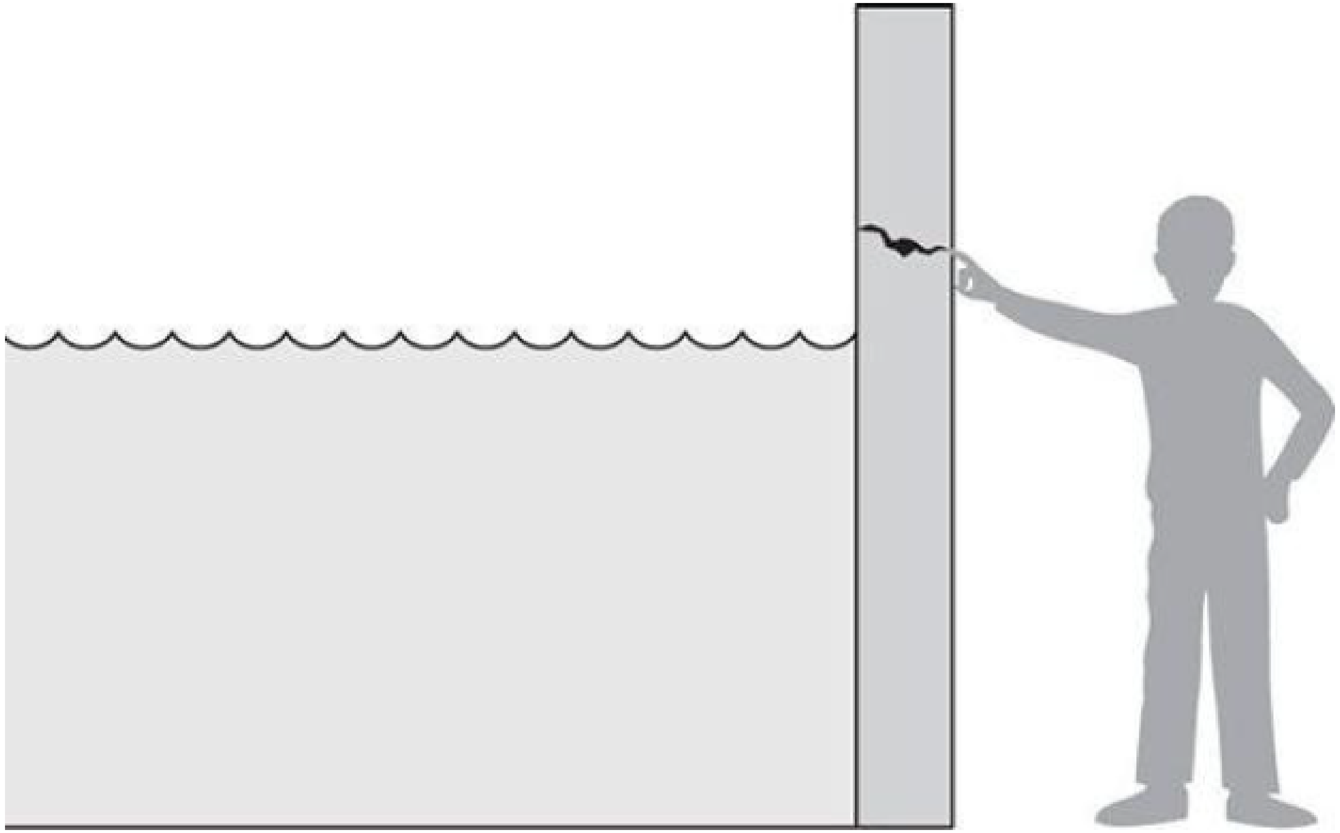
- Control

Basic Terms

- Vulnerability
- Threat
- Attack
- Control

A **control** is an action, device, procedure, or technique that removes or reduces a vulnerability. We use a **control** or **countermeasure** as protection.

Threat versus Vulnerability



The Vulnerability–Threat–Control Paradigm

Control prevents Threats from exercising Vulnerabilities

- A threat is blocked by control of a vulnerability.

- To protect the assets, or to devise controls, we need to know the kinds of harm we have to protect them against.

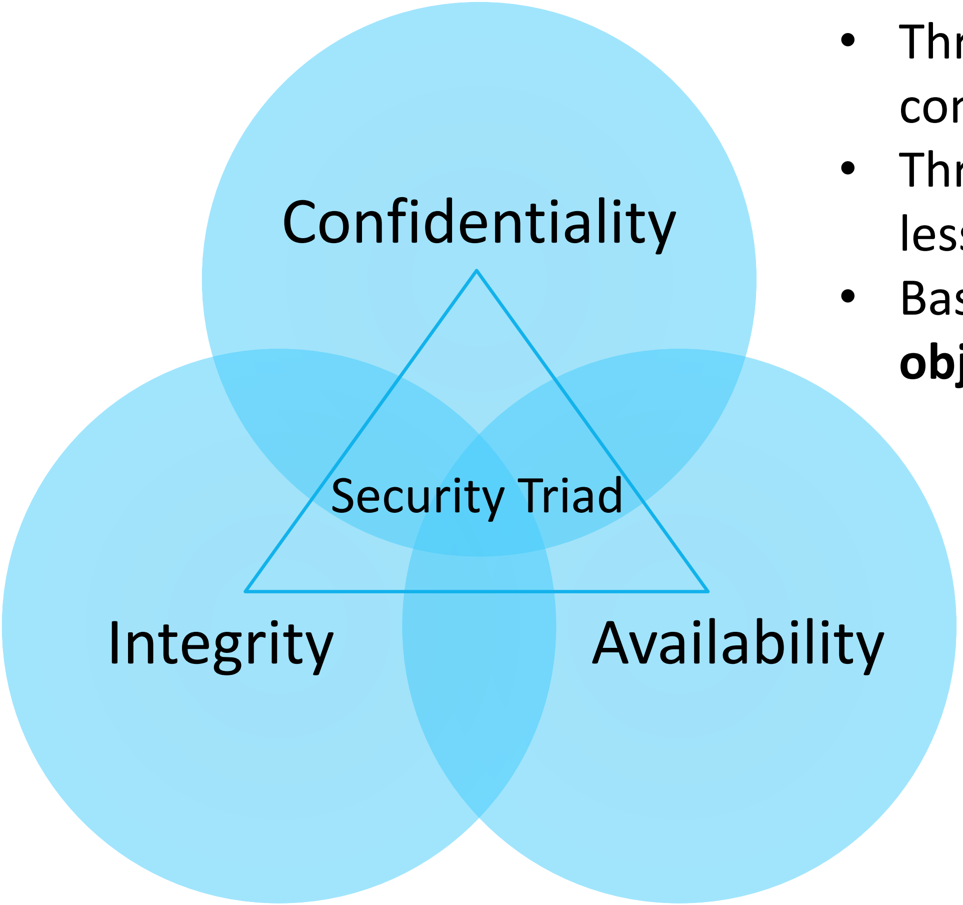
- We must explore more about threats to valuable assets.

Threats

- Potential harm to assets:
  - What bad things can happen to assets.
  - Who or What can cause or allow those bad things to happen.

- These two perspectives enable us to determine how to **protect** assets.

The CIA Triad : Hallmarks of solid security



- Three aspects to make your computer valuable to you.
- Three possible ways to make it less valuable, to cause you harm.
- Basic **security properties** and the **objects of security threats**.

CIA5

- Confidentiality
- Integrity
- Availability

Foundation for thinking about security.

- Authentication
- Accountability/ Non-repudiation

Extend security notions to network Communications.

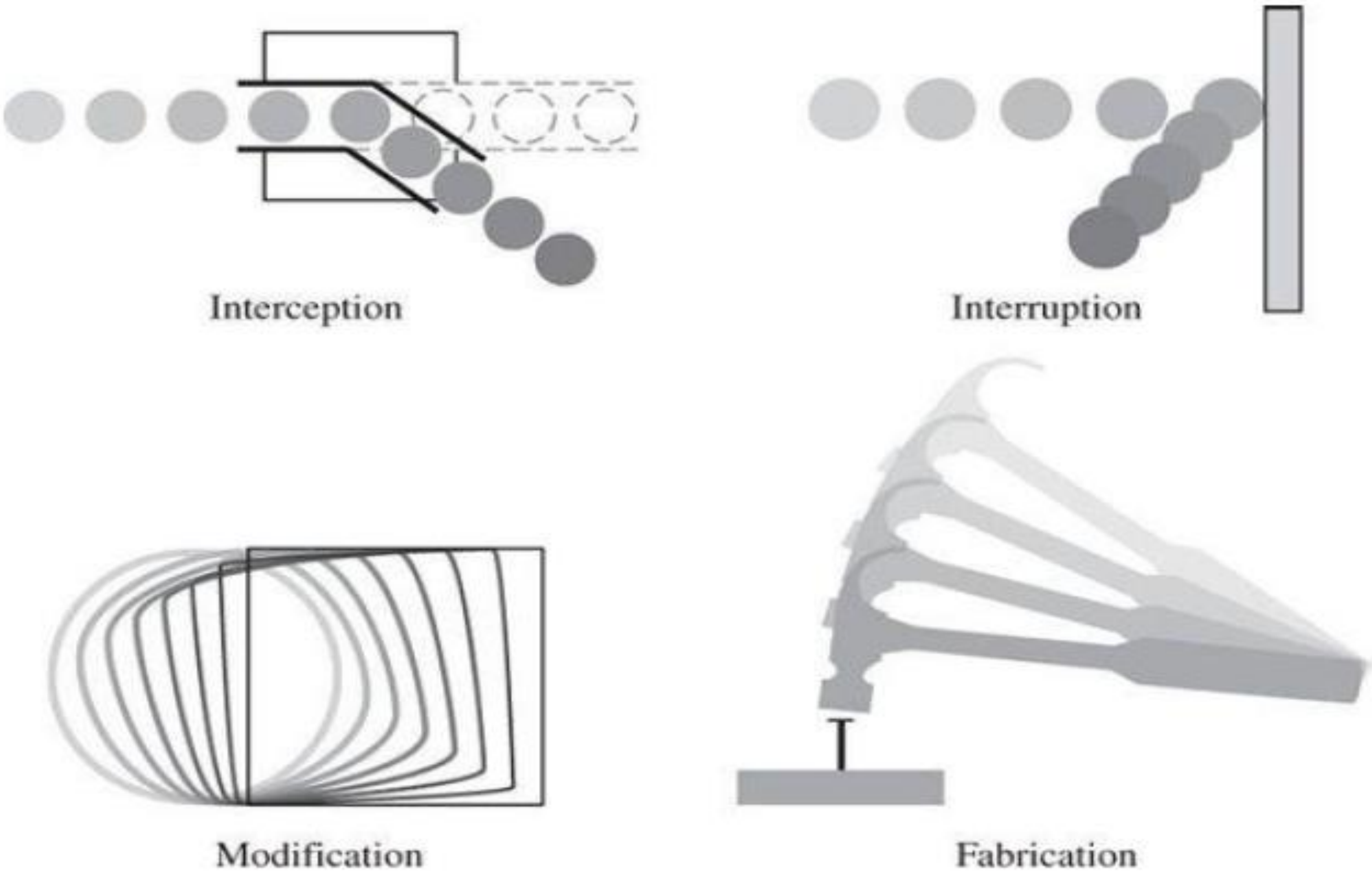
- Auditability

Important in establishing individual accountability for computer activity.

- Authorization

CIA Triad: Four Acts to Cause Security Harm

- Thinking of these four kinds of acts can help determine what threats might exist against the computers under protection.



Confidentiality

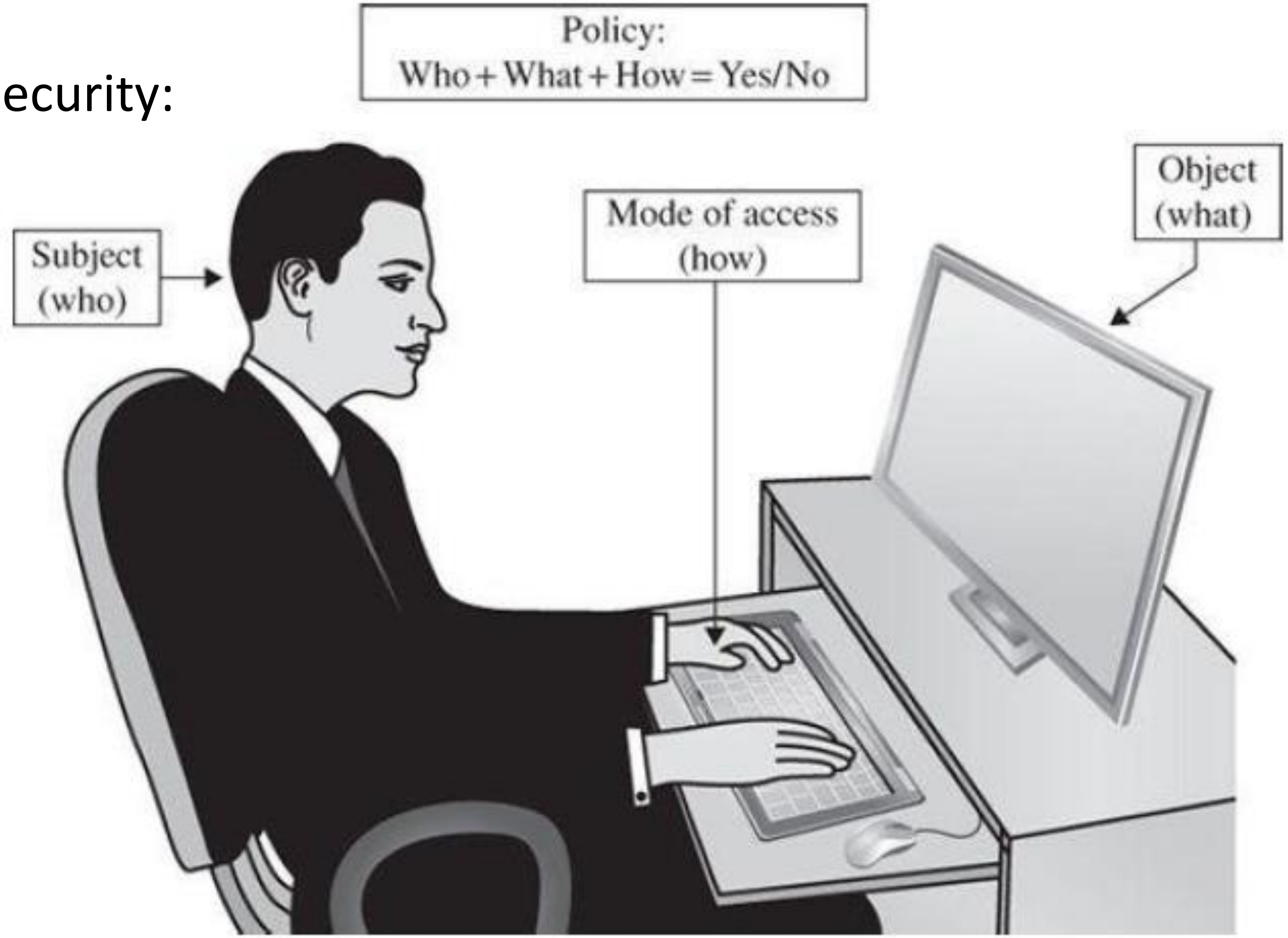
- Only authorized people or systems can **access** protected data.

- Who grants access?
- What all can be accessed?
- Does access permits disclosure?

- Properties that could mean a failure of data confidentiality:
  - An unauthorized **person** accesses a **data item**.
  - An unauthorized **process** or **program** accesses a **data item**.
  - A **person authorized** to access certain data accesses other **data not authorized**.
  - An unauthorized **person** accesses an **approximate data value**.
  - An unauthorized **person** learns the **existence** of a piece of **data**.

Fundamental aspects of computer security:

- Subject,
- Object,
- Policy, and
- Mode of Access.



Confidentiality and view.

Integrity

- Integrity is harder to pin down than confidentiality.
- Preserving the integrity of an item may mean that the item is
  - precise
  - accurate
  - unmodified
  - modified only in acceptable ways
  - modified only by authorized people
  - modified only by authorized processes
  - consistent
  - internally consistent
  - meaningful and usable

Three particular aspects of integrity—authorized actions, separation and protection of resources, and error detection and correction.

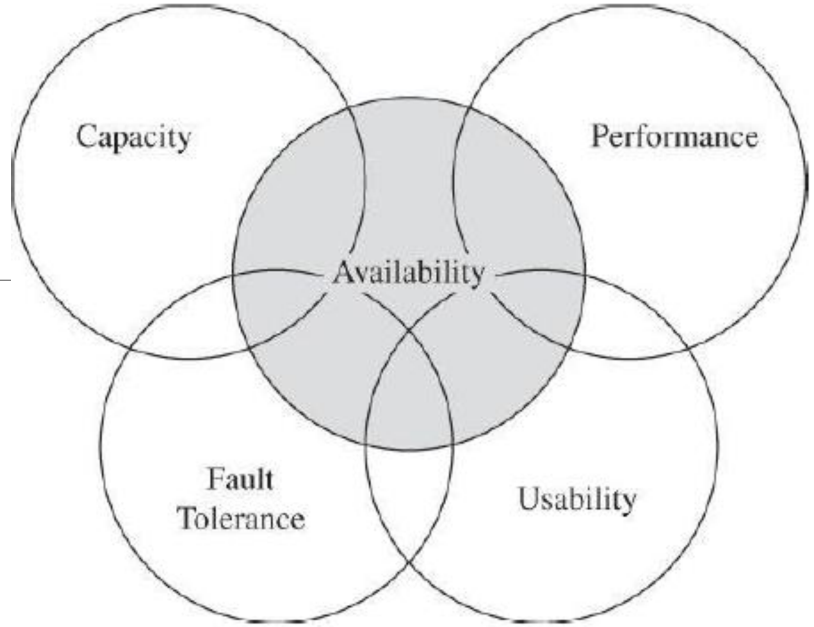
Availability

- Availability applies both to data and to services.
- An object or service is thought to be available if the following are true:

Goals

  - It is present in a **usable** form.
  - It has **enough capacity** to meet the service's needs.
  - It is **making clear progress**, and, if in wait mode, it has a bounded waiting time.
  - The service is **completed** in an **acceptable period of time**.

Availability



- Some criteria to define availability.
  - There is a timely response to our request.
  - Resources are allocated fairly
  - Concurrency is controlled;
  - Philosophy of fault tolerance, whereby hardware or software faults lead to **graceful cessation** of service or to work-arounds.
  - The service or system can be used easily and in the way it was intended to be used.

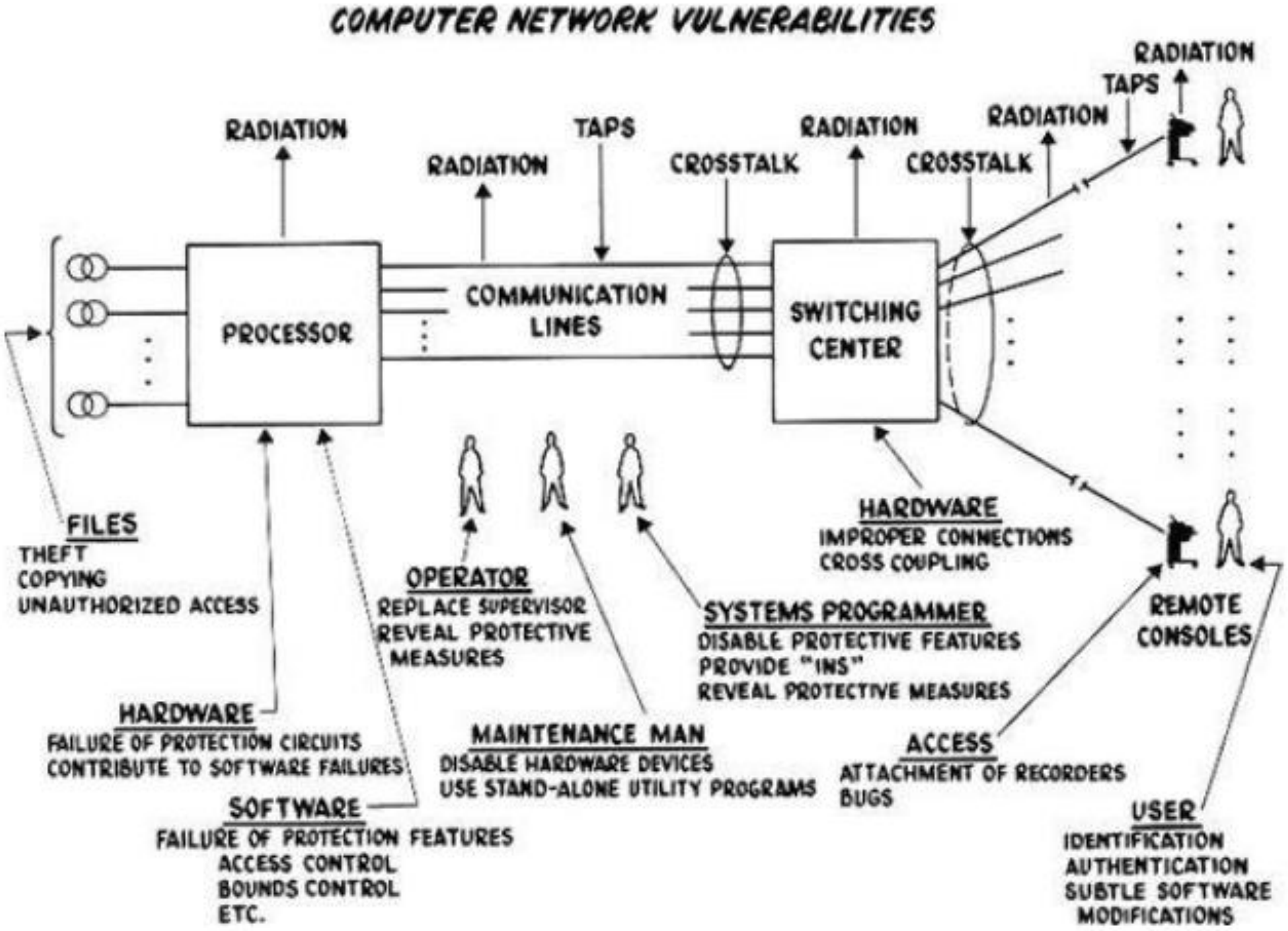
Access Control

- To implement a **policy**, computer security controls all accesses by all **subjects** to all protected **objects** in all **modes of access**.
- A small, centralized control of access is fundamental to preserving confidentiality and integrity, but it is not clear that a single access control point can enforce availability.

Computer security seeks to prevent unauthorized viewing (**confidentiality**) or modification (**integrity**) of data while preserving access (**availability**).

Types of Threats

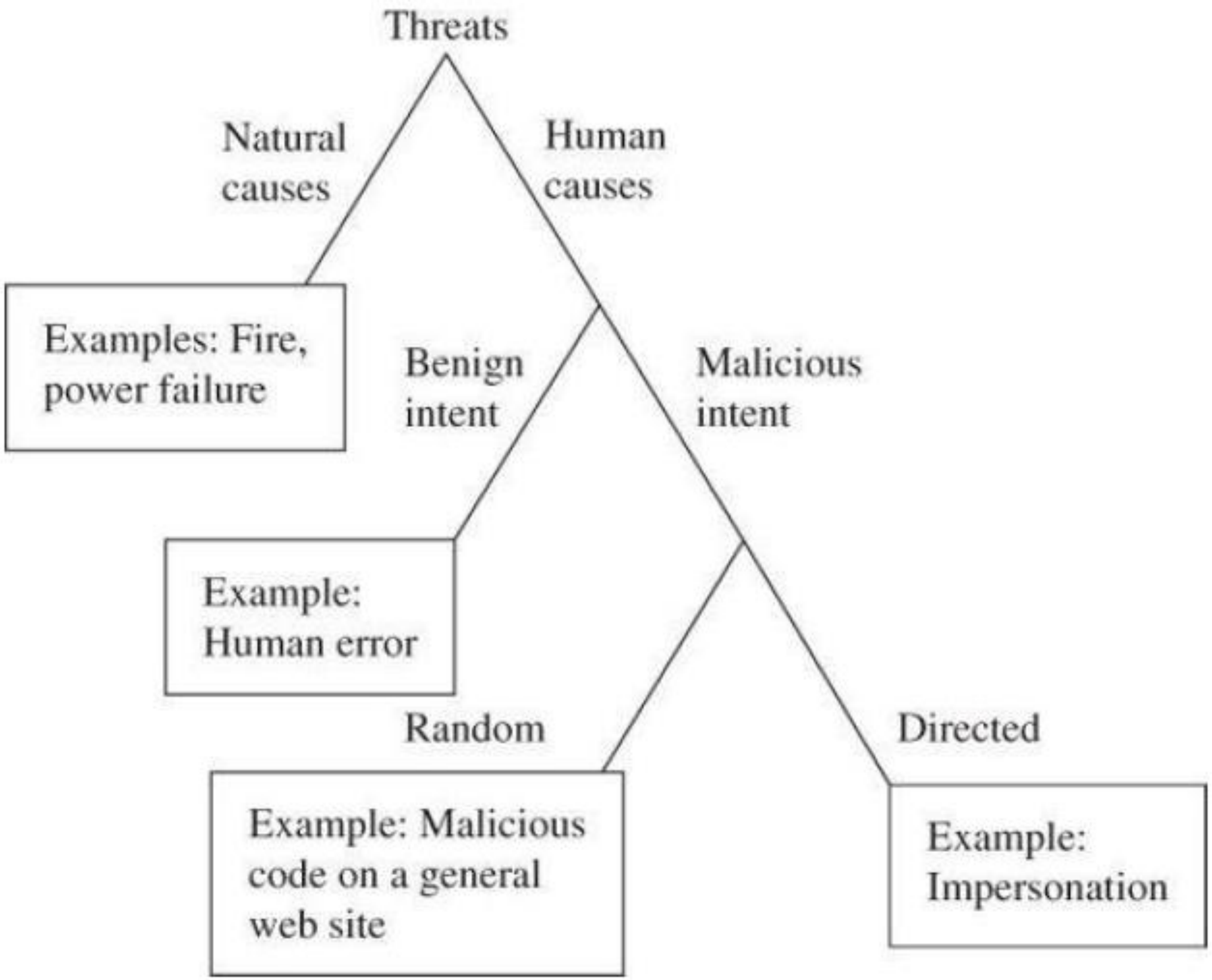
Taken from Willis Ware's report [WAR70].



Types of Threats

- Sometimes the nature of an attack is not obvious until the attack is well underway, or perhaps even ended.
- Two retrospective lists of known vulnerabilities:

1. The Common Vulnerabilities and Exposures (CVE) list.
2. The Common Vulnerability Scoring System (CVSS).



Advanced Persistent Threat

- Advanced persistent threat attacks come from organized, well-financed, patient assailants.
- They carefully select their targets, crafting attacks that appeal to specifically those targets.
- Typically the attacks are silent, avoiding any obvious impact that would alert a victim.

Types of Attackers

- Individuals
- Organized, Worldwide Groups
- Organized Crime
- Terrorists

Harm

- Harm occurs when a threat is realized against a vulnerability.
- Protection against threats is done in order to reduce or eliminate harm.
- **Risk management** involves **choosing** which threats to control and what resources to devote to protection.
    - Value of an asset depends on perspective.
    - The value of many assets can change over time, so the degree of can change, too.
- The risk that remains uncovered by controls is called **residual risk**.
- Spending for security is based on the **impact** and **likelihood** of potential harm—both of which are nearly impossible to measure precisely.

How? When? Why?

MOM : Method–Opportunity–Motive

Three factors that determine feasibility of an attack or harm.

- **Method**

  The skills, knowledge, tools, and other things with which to perpetrate the attack.

- **Opportunity**

  The time and access to execute an attack.

- **Motive**

  Reason to want to attack.

- Method, opportunity, and motive are all necessary for an attack to succeed; deny any of these and the attack will fail.

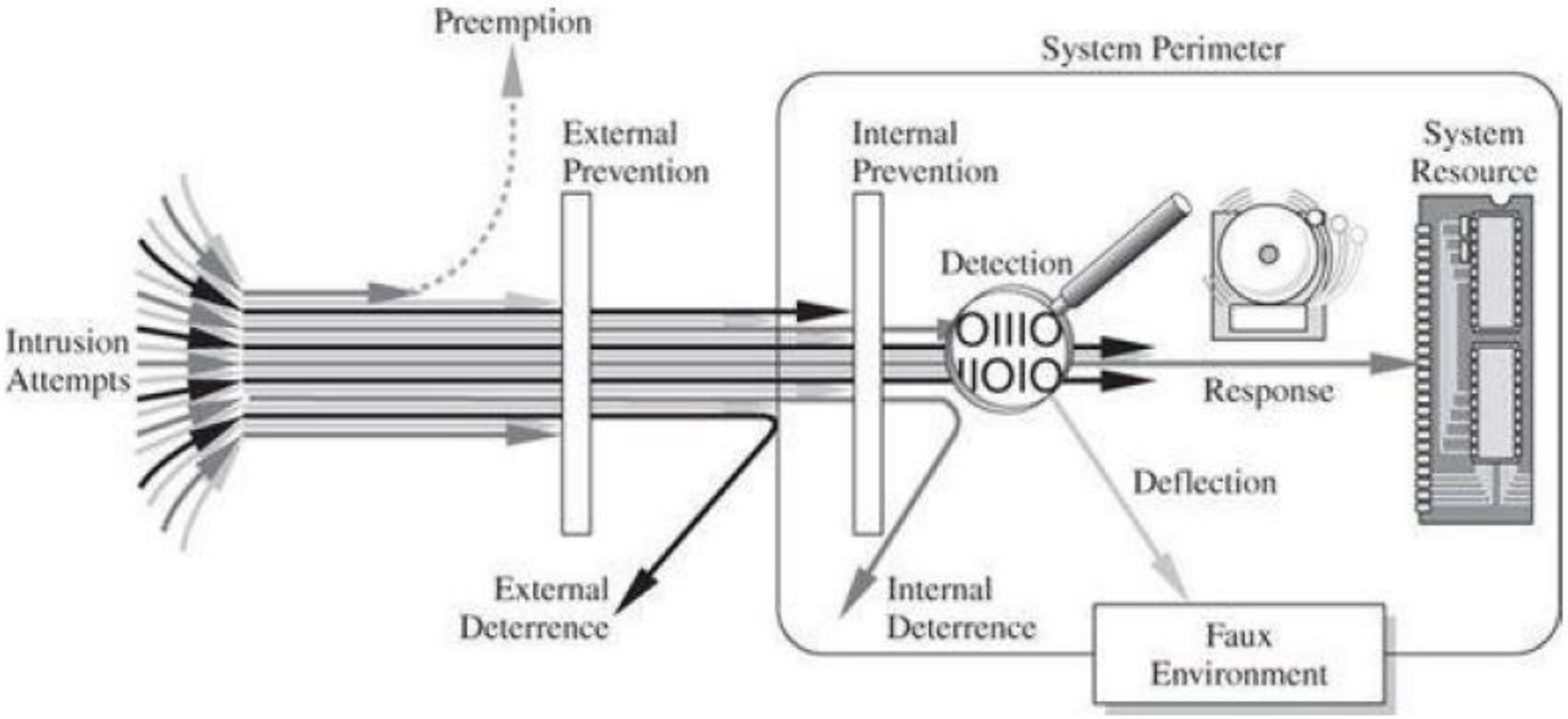
Vulnerabilities

- Vulnerabilities are weaknesses that can allow harm to occur.
- Examples: weak authentication, lack of access control, errors in programs, finite or insufficient resources, and inadequate physical protection.
- System's **attack surface**
  - System's full set of vulnerabilities—actual and potential.
- Thus, the attack surface includes physical hazards, malicious attacks by outsiders, stealth data theft by insiders, mistakes, and impersonations.

Controls

- To protect against harm, then, we can neutralize the threat, close the vulnerability, or both.
- Several ways of dealing with harm:
    - **Prevent** it, by blocking the attack or closing the vulnerability
    - **Deter** it, by making the attack harder but not impossible
    - **Deflect** it, by making another target more attractive (or this one less so)
    - **Mitigate** it, by making its impact less severe
    - **Detect** it, either as it happens or some time after the fact
    - **Recover** from its effects.
- Security professionals balance the cost and effectiveness of controls with the likelihood and severity of harm.

Controls


Preemption
System Perimeter
External Prevention
Internal Prevention
System Resource
Detection
OIIIO
IIOIO
Intrusion Attempts
Response
Deflection
External Deterrence
Internal Deterrence
Faux Environment

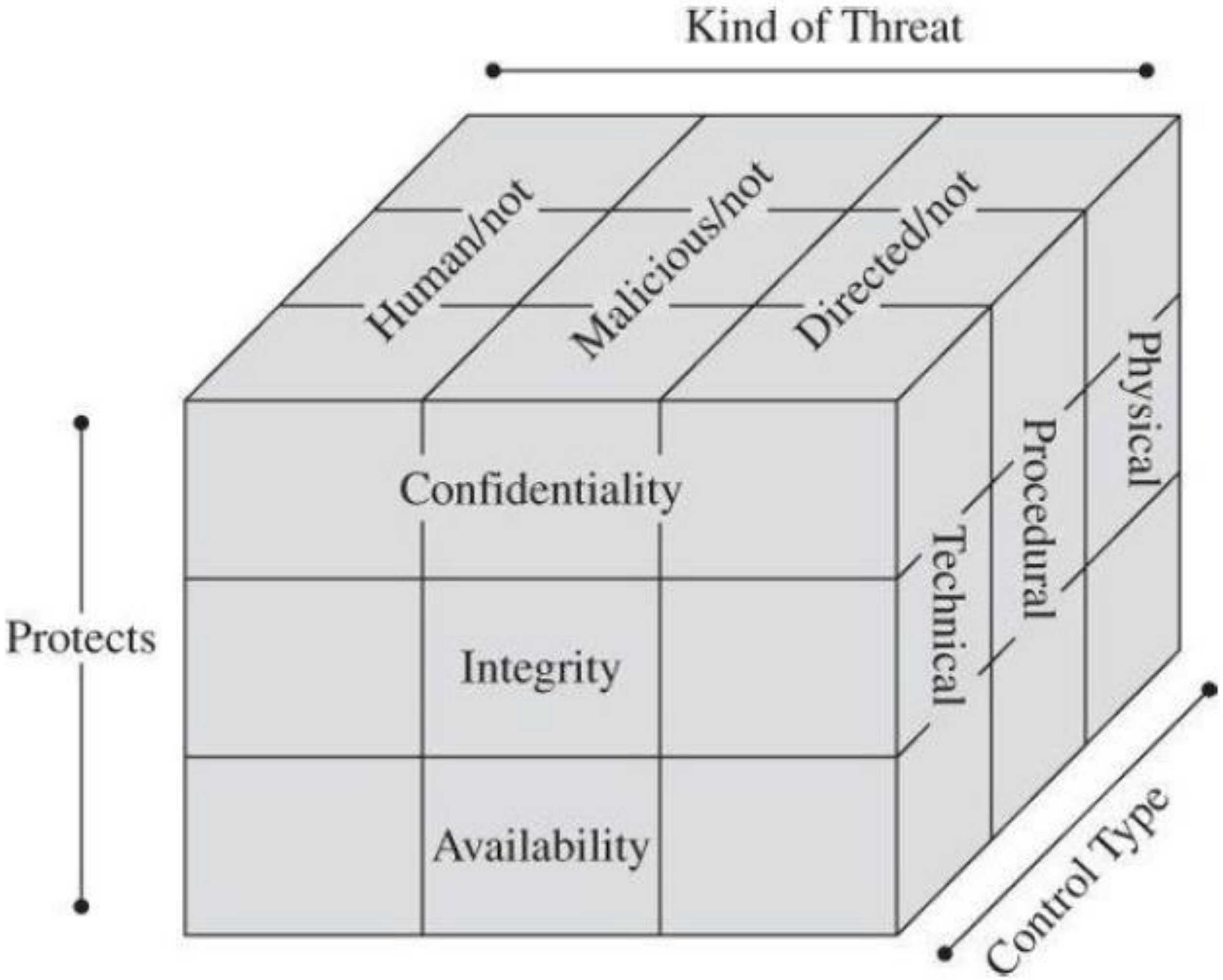
Controls

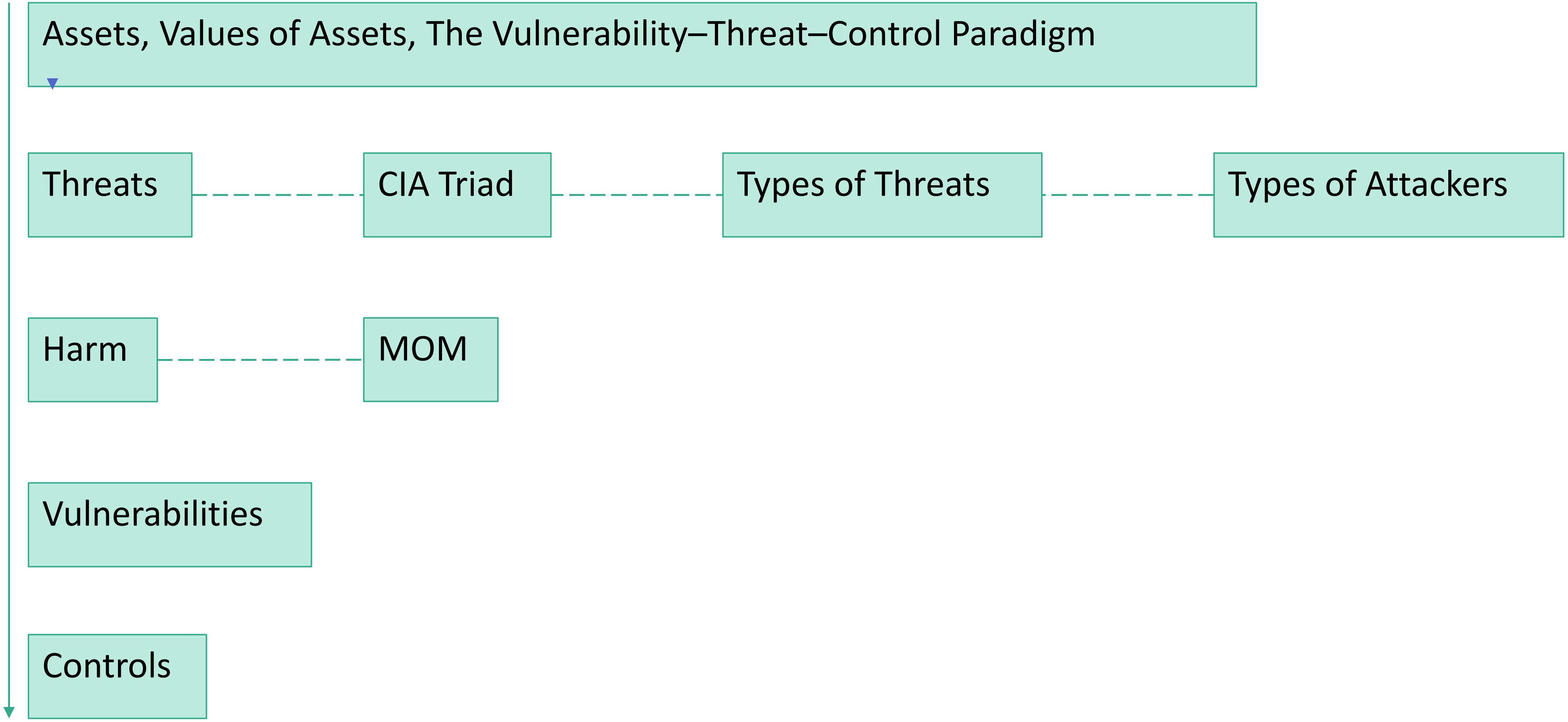
Controls can be grouped into 3 largely independent classes:

- **Physical** controls stop or block an attack by using something tangible.
- **Procedural** or **administrative** controls use a command or agreement.
- **Technical** controls counter threats with technology (hardware or software).

Controls

- The **property** to be protected and the **kind of threat** when you are choosing appropriate types of **countermeasures**.
- It can be effective to use **overlapping** controls or **defense in depth**: more than one control or more than one class of control to achieve protection.





Assets, Values of Assets, The Vulnerability–Threat–Control Paradigm

Threats

CIA Triad

Types of Threats

Types of Attackers

Harm

MOM

Vulnerabilities

Controls

Book

- Pfleeger C. P., Pfleeger S. L. and Margulies J., Security in Computing (5e), Prentice Hall, 2015, Chapter 1.