SECURITY IN COMPUTING, FIFTH EDITION

Chapter 1: Introduction

Objectives for Chapter 1

- Define *computer security* as well as basic computer security terms
- Introduce the C-I-A Triad
- Introduce basic access control terminology
- Explain basic threats, vulnerabilities, and attacks
- 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)

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

- Individual applications

Unique; irreplaceable

Basic Terms

- Vulnerability
- Threat
- Attack
- Countermeasure or control

Vulnerabilities, Threats, Attacks, Controls

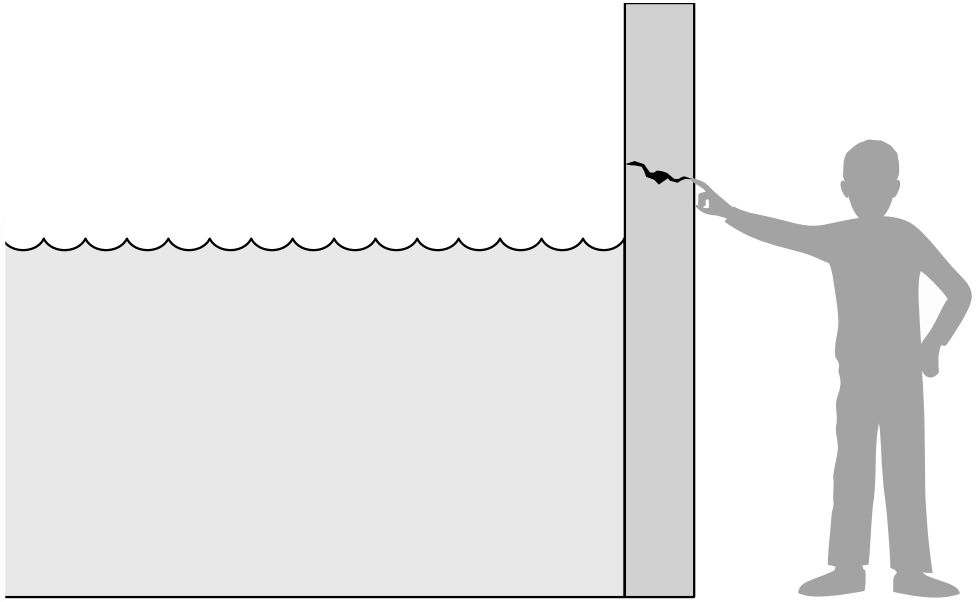
- **Vulnerability** is a weakness in the security system
  - (i.e., in procedures, design, or implementation), that might be exploited to *cause loss or harm*.
- **Threat** to a computing system is a set of circumstances that has the *potential to cause loss or harm*.
  - a potential violation of security
- A human (*criminal*) who exploits a vulnerability perpetrates an **attack** on the system.
- How do we address these problems?
  - We use a **control** as a protective measure.
  - That is, 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*.

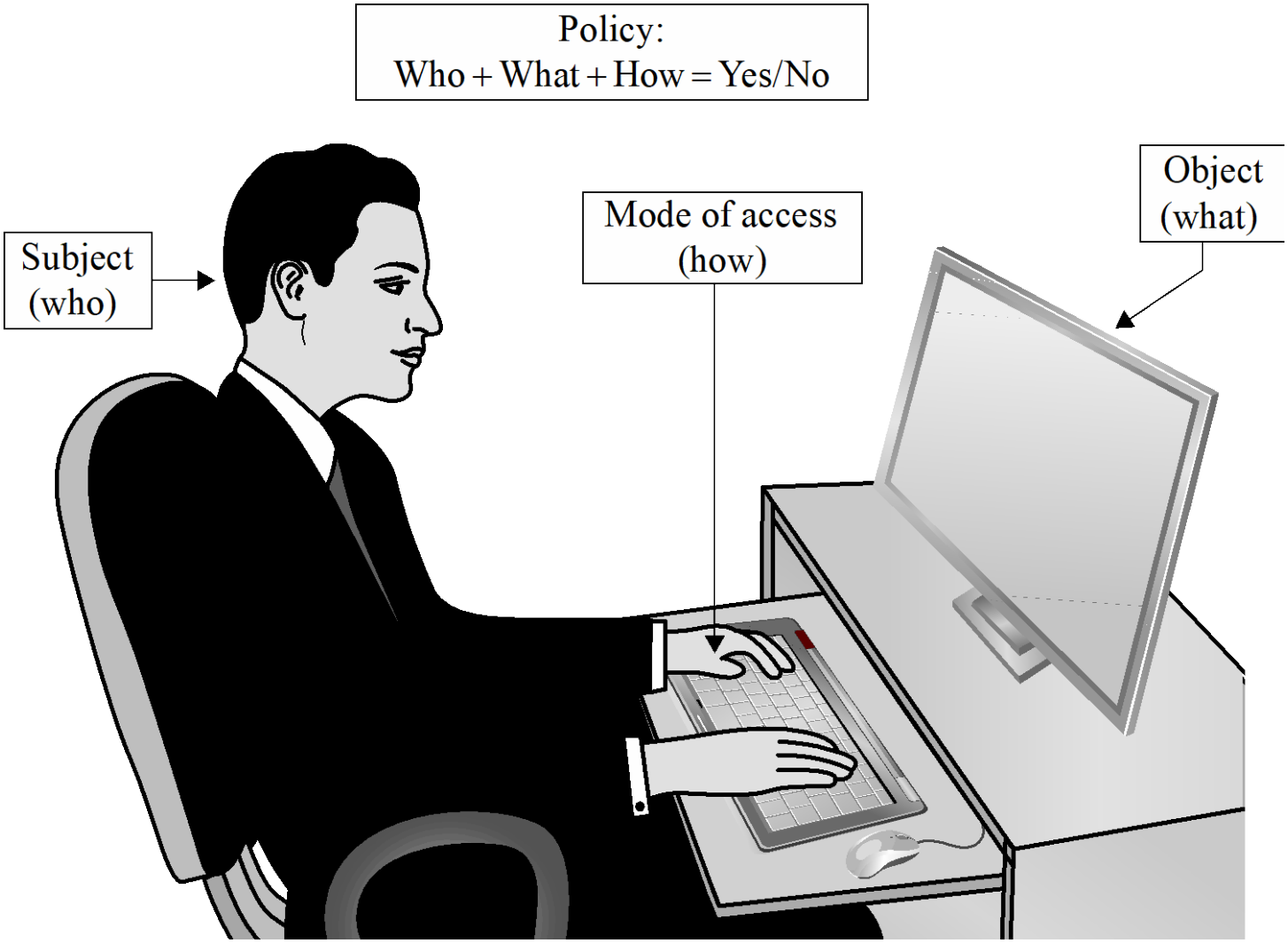
The fact that the violation might occur means that the actions that might cause it should be guarder against.



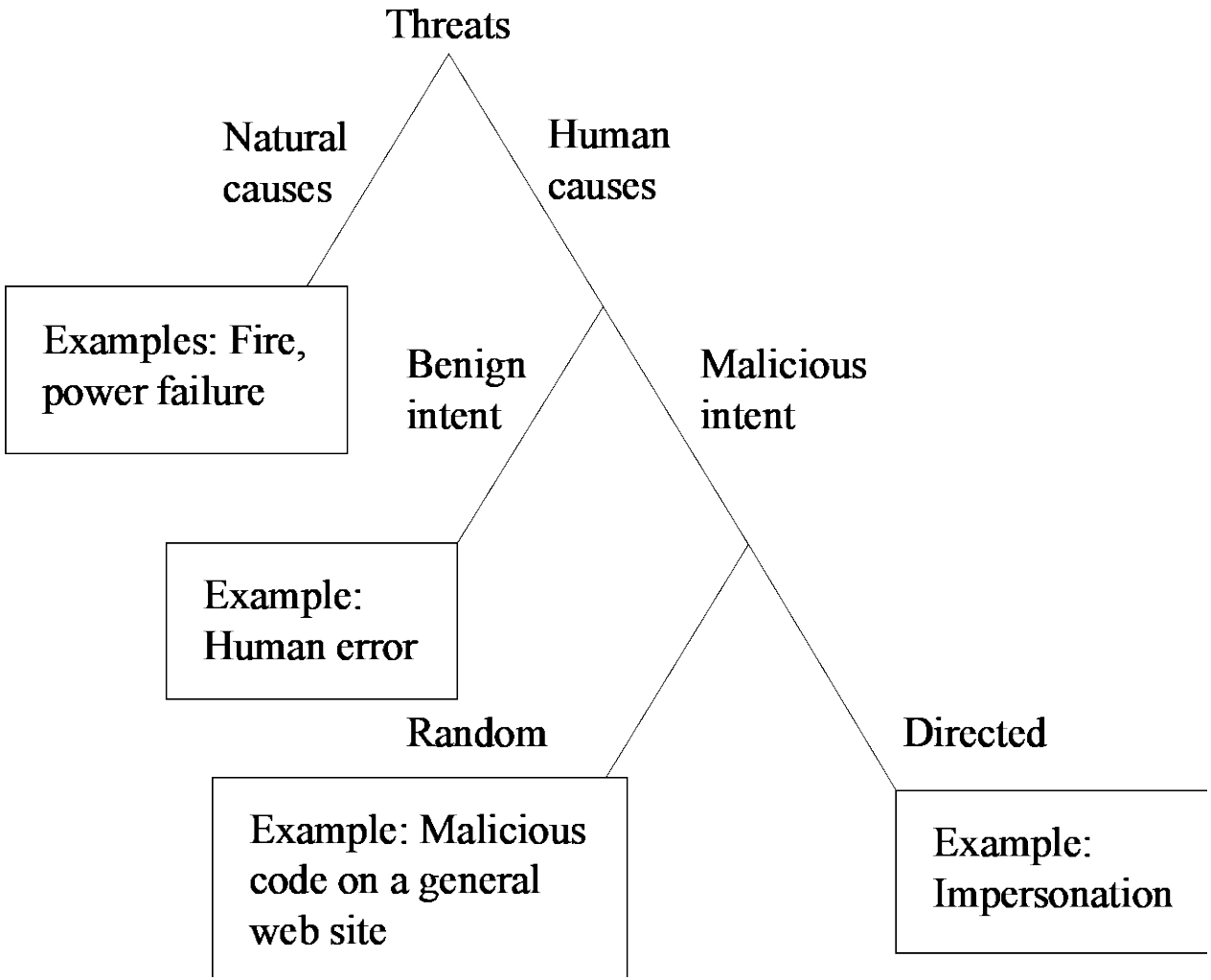
C-I-A Triad

- Confidentiality
- Integrity
- Availability
- 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



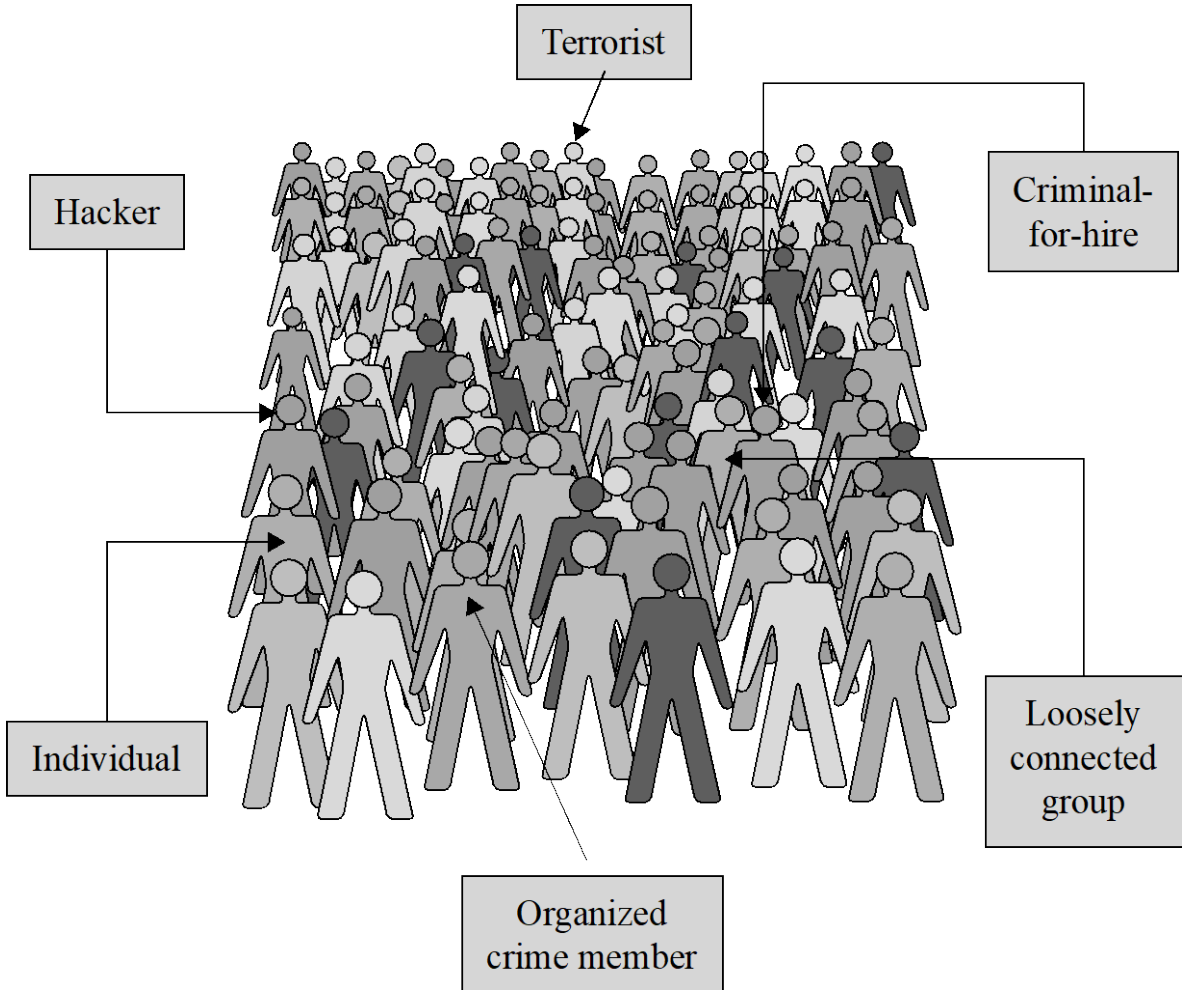
Types of Threats



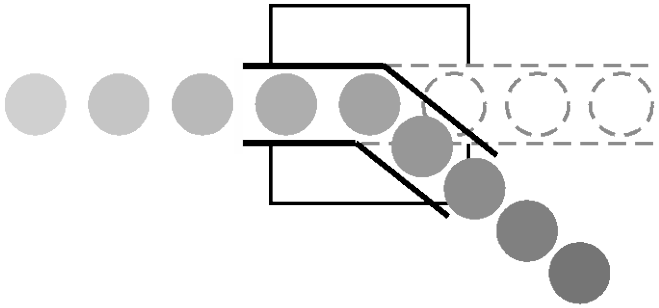
Advanced Persistent Threat (APT)

- Organized
- Directed
- Well financed
- Patient
- Silent

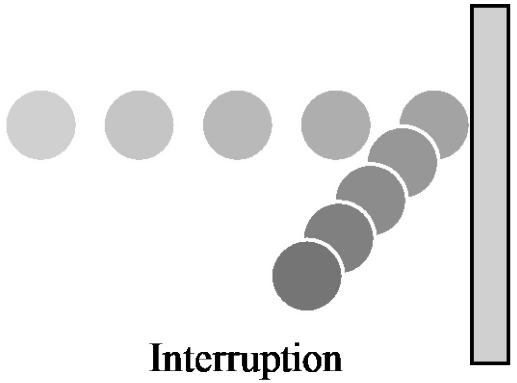
Types of Attackers



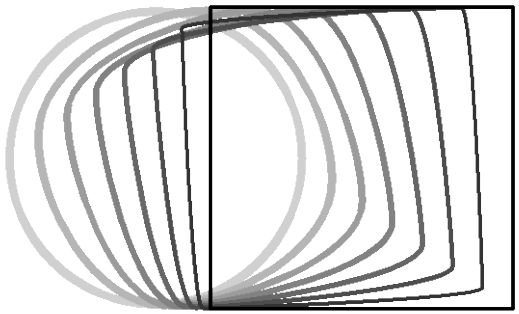
Types of Harm



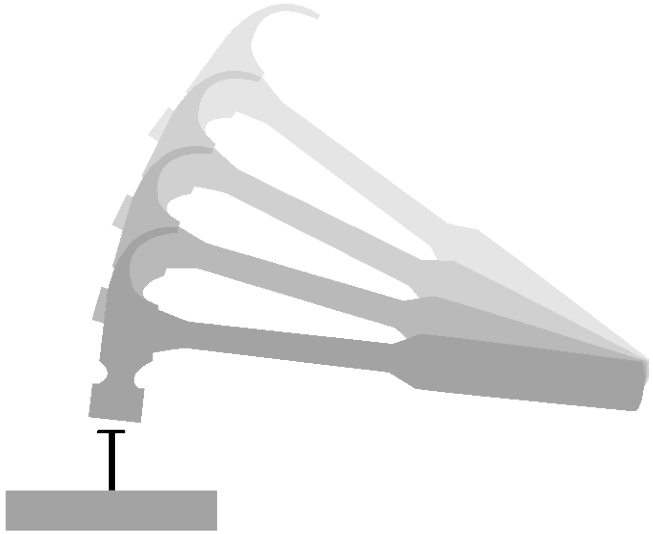
Interception



Interruption



Modification



Fabrication

Threats

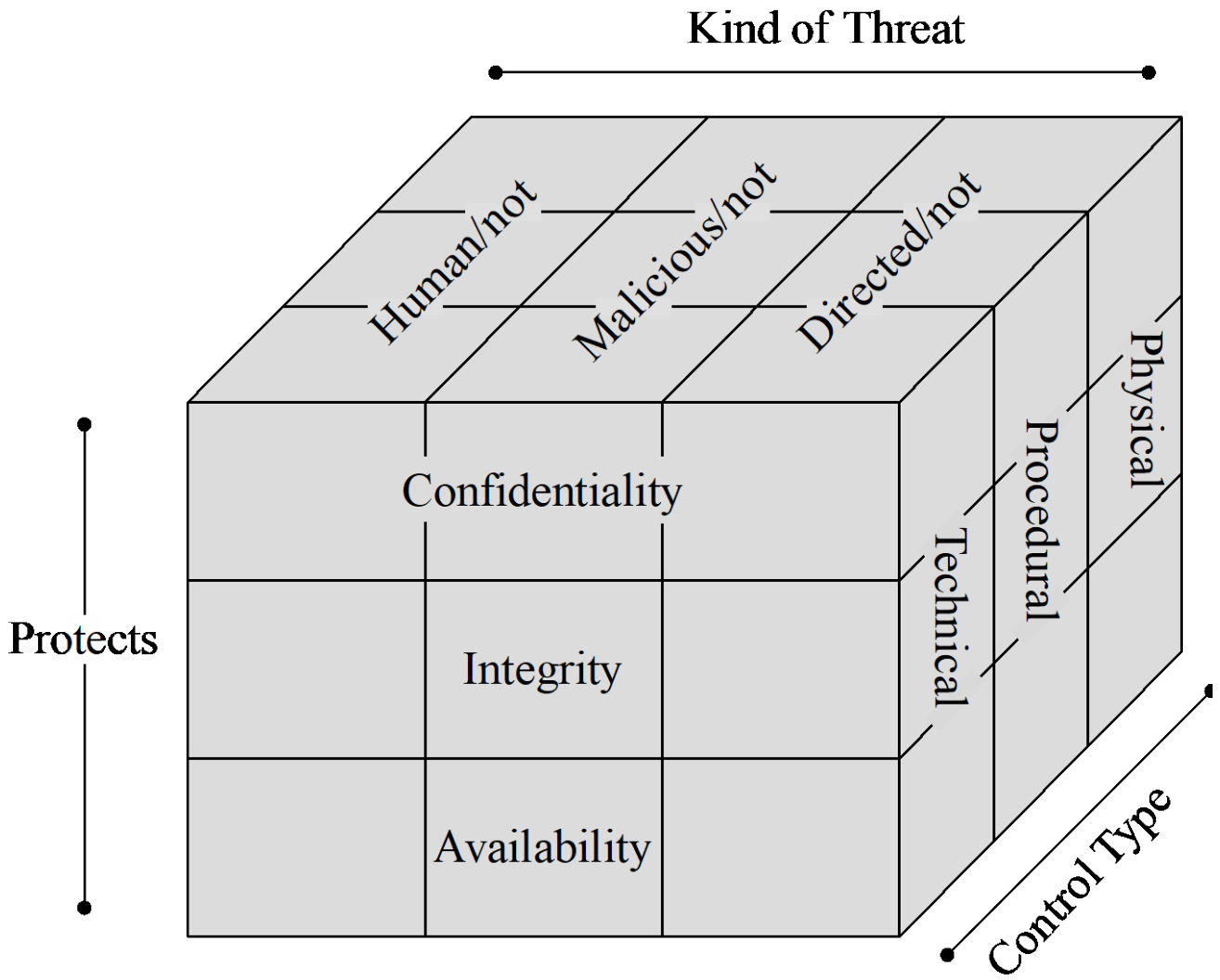
- In an **interception** means that some unauthorized party has gained access to an asset.
- In an **interruption**, an asset of the system becomes lost, unavailable, or unusable.
- If an unauthorized party not only accesses but **tampers** (forges) with an asset, the threat is a **modification**.
- Finally, an unauthorized party might create a **fabrication** of ***counterfeit*** objects on a computing system.

Method—Opportunity—Motive (MOM)

Method, Opportunity, and Motive

- A malicious attacker must have **three things (MOM)**:
  - *method:* the **skills**, **knowledge**, **tools**, and other things with which to be able to pull off the attack
    - Knowledge of systems are widely available
  - *opportunity:* the **time** and **access** to accomplish the attack
    - Systems available to the public are accessible to them
  - *motive:* a **reason** to want to perform this attack against this system

Controls/Countermeasures

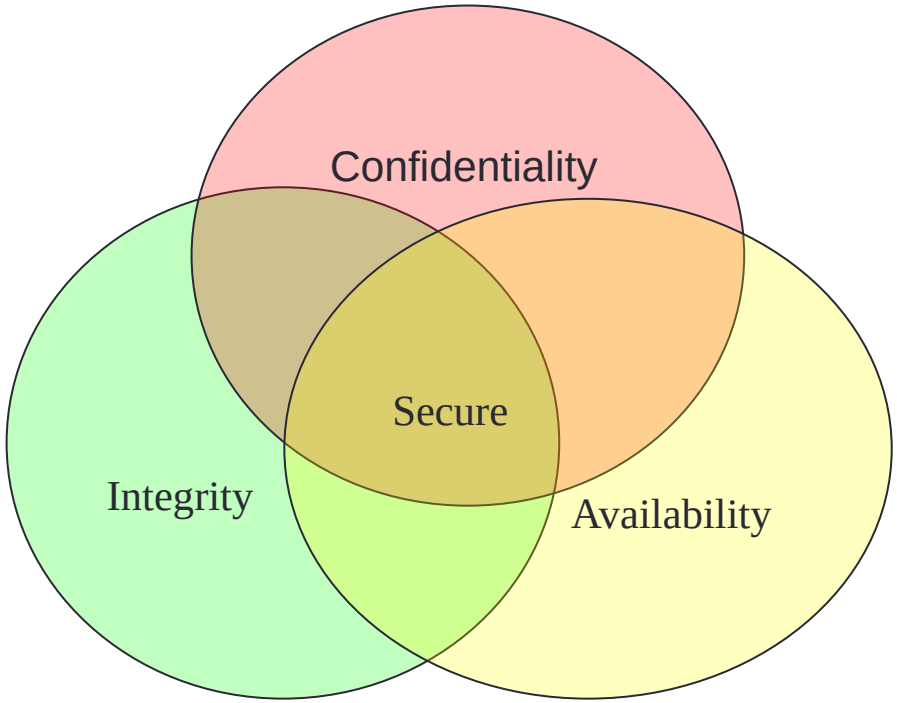


Security Goals

- 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.



Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

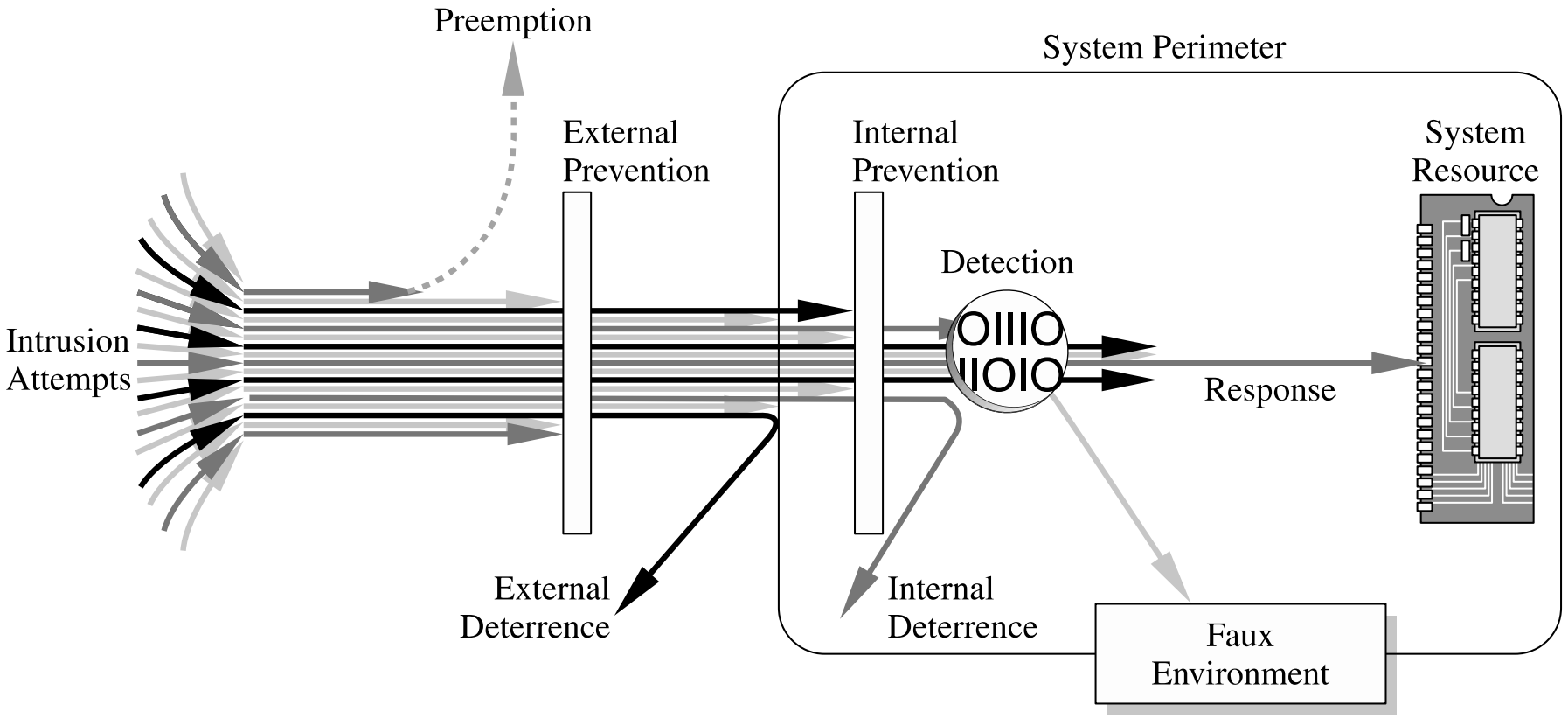
Trust and Assumptions

- Trust underlies *all* aspects of security

- Policies
  - Unambiguously partition system states
  - Correctly capture security requirements

- Mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly

Different Types of Controls



Countermeasures types (controls)

- Prevention
  - Removal of vulnerabilities
- Deterrence
  - Removal of motivations
  - Increasing costs and risks for attackers
- Deflection
  - Showing a more convenient target
- Detection
  - Well DOH!
- Recovery
  - Ok, it happened, what now?

Controls Available

- **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.*

Controls Available

- **Encryption** does **not solve all** computer security problems, and other tools must complement its use.
  - if encryption is not used properly, it may have no effect on security or could even degrade the performance of the entire system.

- **Weak encryption** can actually be **worse than no encryption** at all,
  - because it gives users an unwarranted sense of protection.

- *Therefore, we must understand those situations in which encryption is most useful as well as ways to use it effectively.*

Controls Available

- **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.

- **Program controls include the following:**
  - **Internal program controls**: parts of the program that enforce security restrictions,
    - i.e. *access limitations in a database* management program
  - **Operating system and network system controls**: *limitations enforced by the operating system* or network to protect each user from all other users
    - i.e. chmod on UNIX: (Read, Write, Execute) ***vs***. (Owner, Group, Other)
  - **Independent control programs**: application programs,
    - i.e. *password checkers*, intrusion detection utilities, or *virus scanners*, that protect against certain types of vulnerabilities

Controls Available

- **Development controls**:
  - quality standards under which a program is **designed**, **coded (implementation)**, **tested**, and maintained to prevent software faults from becoming exploitable vulnerabilities
    - i.e. **Penetration testing** (pen testing or ethical hacking), is the practice of testing a computer system, network or web application to *find security vulnerabilities that an attacker could exploit*.

- Software controls frequently affect users directly ?
  - i.e. when the user is interrupted and asked for a password before being given access to a program or data.
  - Because they influence the usability of the system, software controls must be carefully designed.
    - Ease of use and capabilities are often competing goals in the design of a collection of software controls.

Controls Available

- **Hardware Controls**
  - Numerous hardware devices have been created to assist in providing computer security. These devices include a variety of means, such as
    - hardware or smart card implementations of encryption
    - locks or cables limiting access or deterring theft
    - devices to verify users' identities
    - firewalls
    - intrusion detection systems
    - circuit boards that control access to storage media

Controls Available

- **Policies and Procedures**
  - Sometimes, we can rely on agreed-on procedures or policies among users rather than enforcing security through hardware or software means
    - i.e. frequent changes of passwords
  - We must not forget the value of community standards and expectations when we consider how to enforce security.

- **Physical Controls**
  - i.e. locks on doors,
  - guards at entry points,
  - backup copies of important software and data, and
  - physical site planning that reduces the risk of natural disasters.

Effectiveness of Controls

- **Awareness of Problem**
  - People using controls must be convinced of the need for security. That is, people will willingly cooperate with security requirements only if they understand
    - why security is appropriate in a given situation.

Effectiveness of Controls

- **Likelihood of Use**
  - Of course, no control is effective unless it is used
  - **Principle of Effectiveness:**
    - Controls must be used properly to be effective.
      - They must be efficient, easy to use, and appropriate.
    - This principle implies that computer security controls
      - must be efficient enough, in terms of time, memory space, human activity, or other resources used,
      - using the control does not seriously affect the task being protected.
      - Controls should be selective so that they do not exclude legitimate accesses.

Effectiveness of Controls

- **Overlapping Controls**
  - Several different controls may apply to address a single vulnerability.

- **Periodic Review**
  - Just when the security specialist finds a way to secure assets against certain kinds of attacks, the opposition doubles its efforts in an attempt to defeat the security mechanisms. Thus, judging the effectiveness of a control is an ongoing task.

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