Security in Computing

Chapter 1

Introduction

Chapter 1 overview

- Risks involved in computing
- Meaning of computer security
- Goals of secure computing
- Threats to secure computing
- Methods of defense

What risks are there?

- Losing the system.
- Losing control of the system
- Losing information in the system
- Information in the system gets “leaked”
- Information in the system gets changed

A Risk Classification

- Thus risks can be classified as:
  - Loss of confidentiality
  - Loss of integrity, or
  - Loss of Availability

Where Can Losses Happen?

- Data can be compromised while it is stored
- Data can be compromised while it is being transported
- Data can be compromised while it is being transformed.

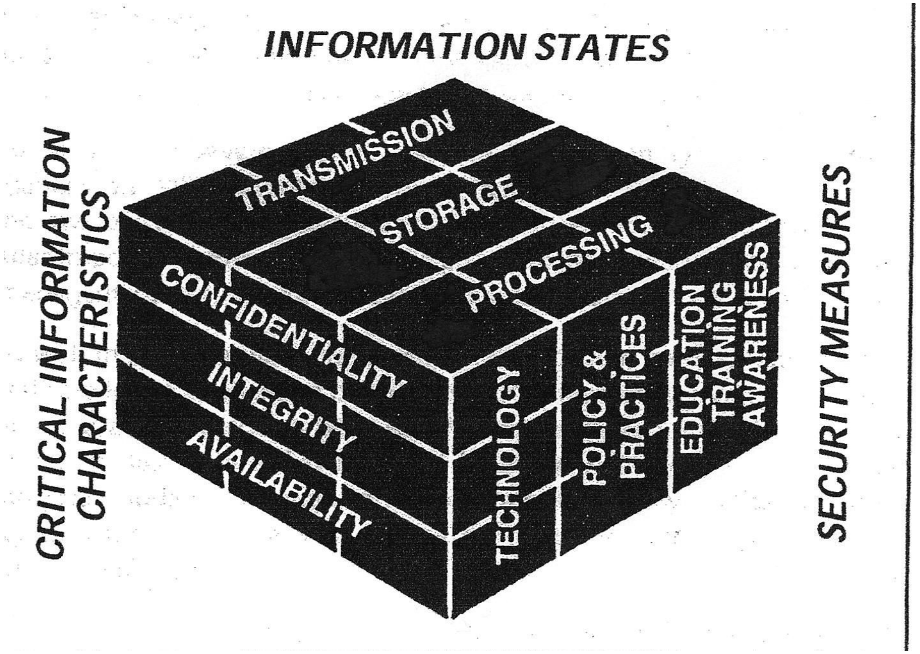
Principle of Easiest Penetration

An intruder will use any available means of penetration, probably the most devious, through the weakest point, and definitely where we least expect it.

What can we do?

- Technology
- Policies and Practicies
- Education

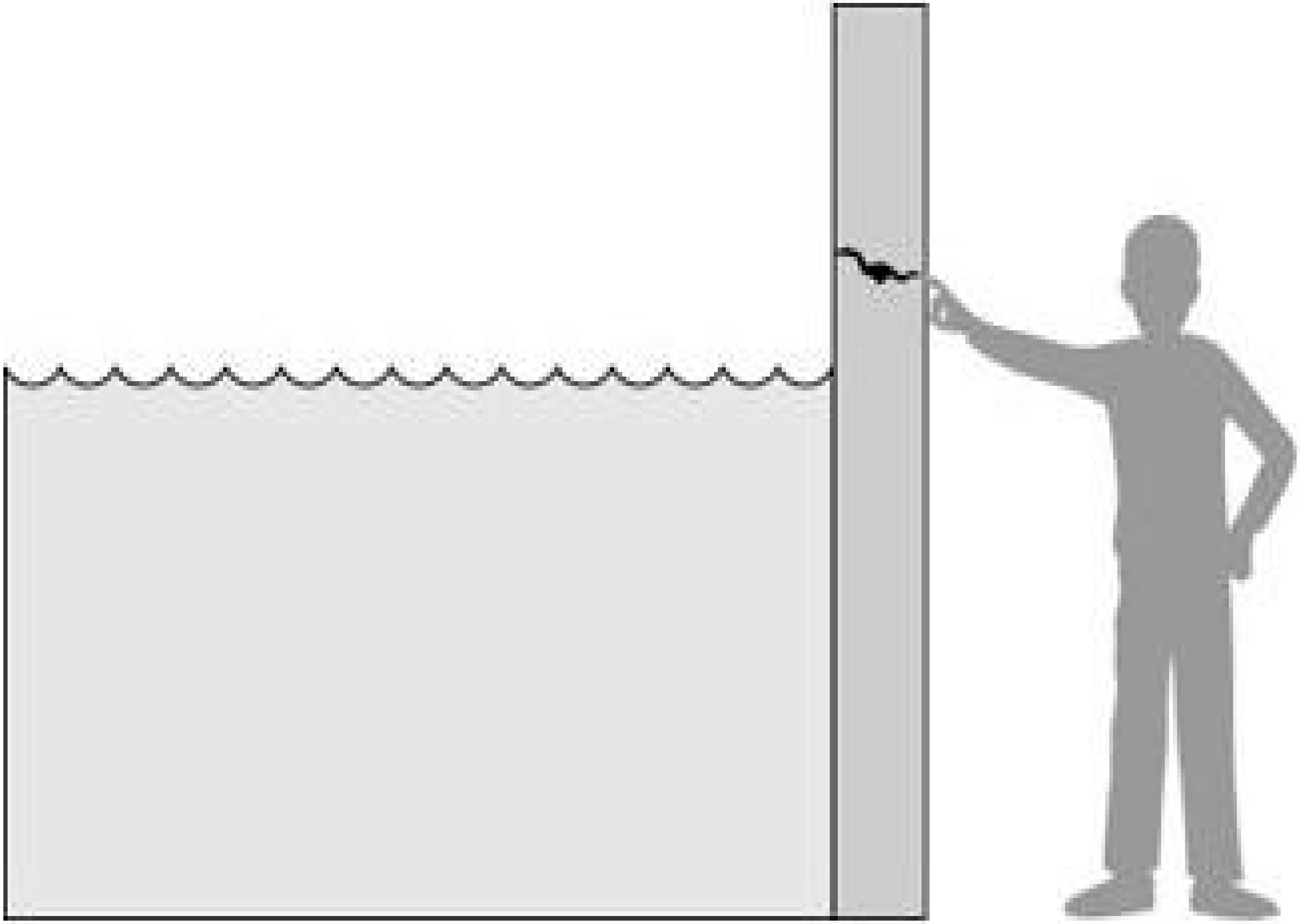
Information Security Cube Model



Some definitions

- Vulnerability: weakness in a system that can be exploited to cause harm.
- Threat: Set of circumstances that has a potential to cause harm.

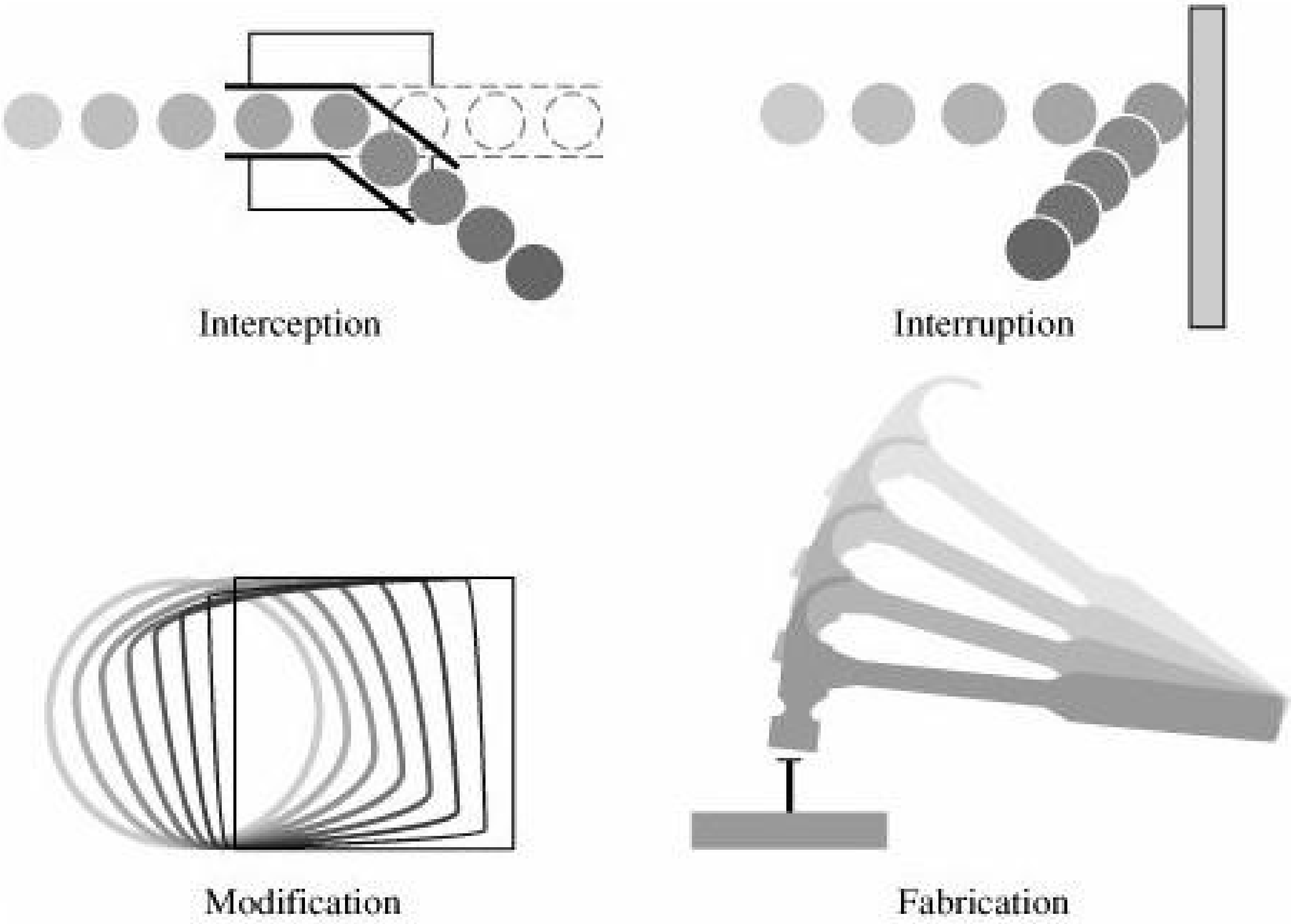
Figure 1-1. Threats, Controls, and Vulnerabilities.



Some more concepts

- Attack: action taken by a person exploting a vulnerability. Sometimes, a system may attack another, but ultimately, a person is in control. (Threat + vulnerability)
- Controls are protective measures against attacks. There are four kinds of attacks for each of which we must devise a different family of controls:

Figure 1-2. System Security Threats.



Interception

Interruption

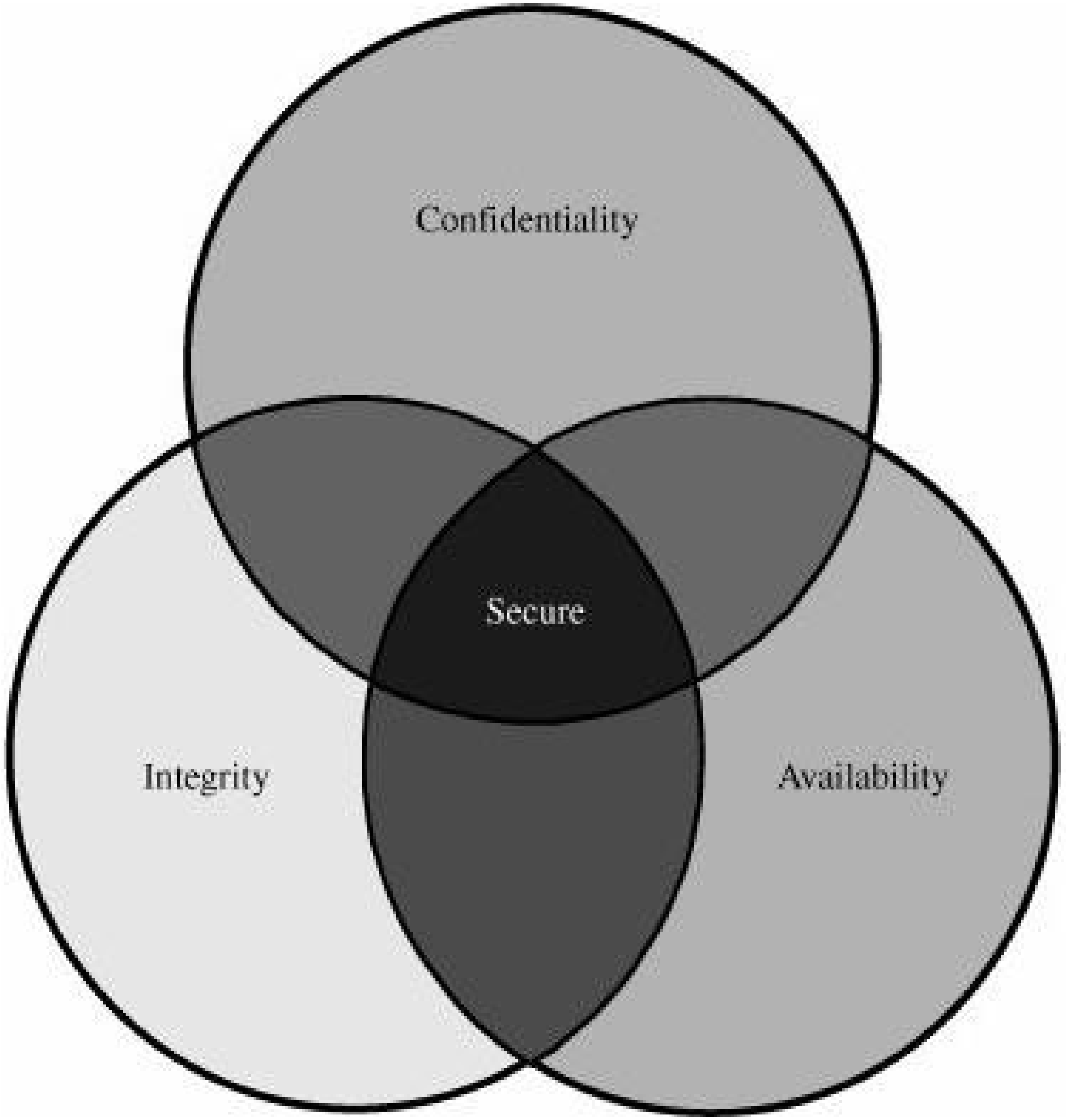
Modification

Fabrication

Crime 101

- In order for a crime to be committed, the criminal needs:
  - A method: skills, knowledge, tools, etc
  - Opportunity: time and access
  - Motive: a reason
- Cyber-crime is no different.

Figure 1-3. Relationship Between Confidentiality, Integrity, and Availability.

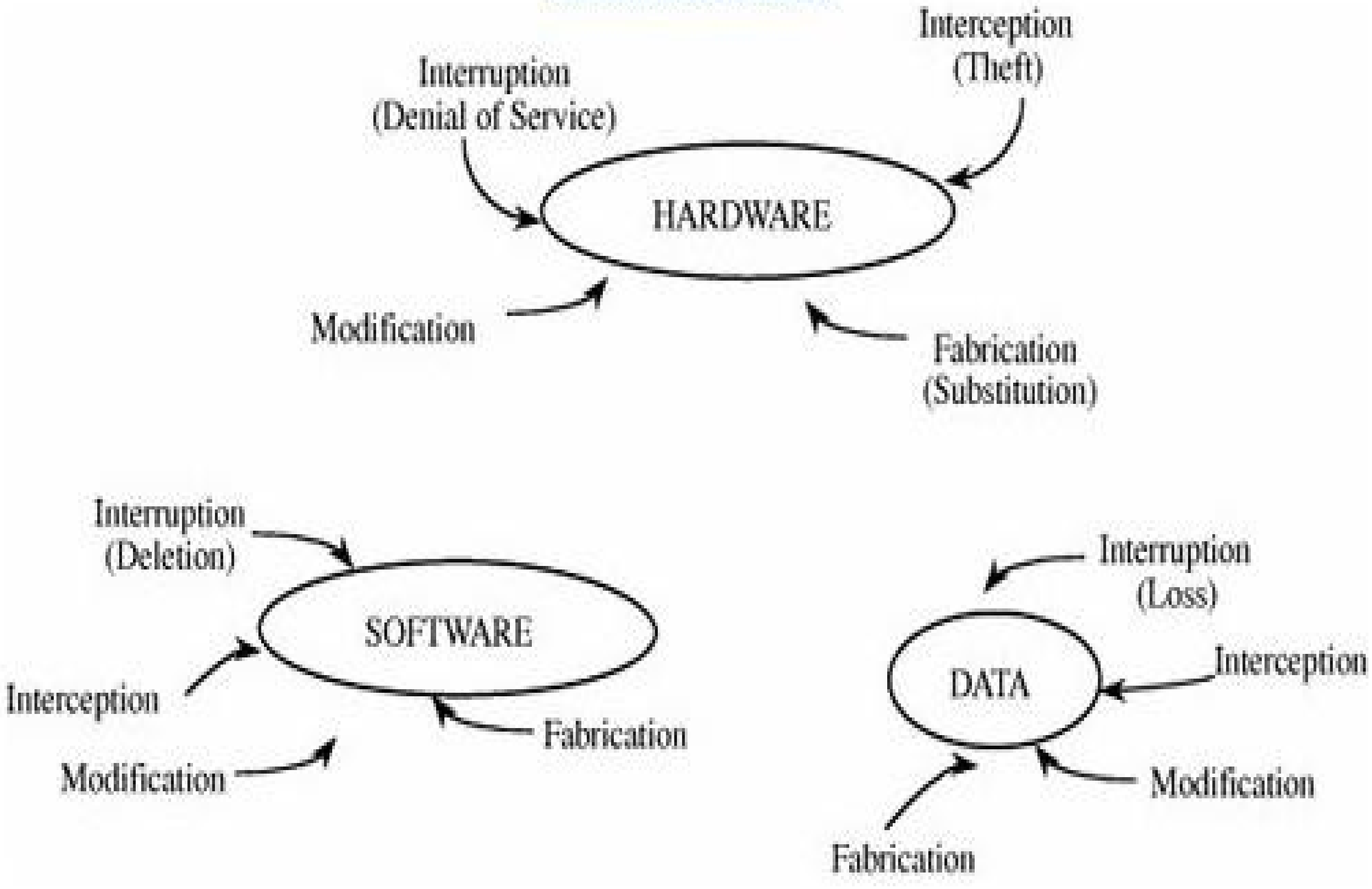


What are we protecting?

- Hardware
- Software
- Data

Figure 1-4. Vulnerabilities of Computing Systems.

[View full size image]



Attacks and attackers

- Attacks
  - Malicious, nonmalicious, from nature
  - Accidental or intentional
- Attackers:
  - Need
    - Method, opportunity, motivation
      - Typical motivations include financial, ego, challenge, revenge.
  - Work factor: difficulty in pulling off attack, measured in time, skill, resources.

Confidentiality

- Privacy
- Sensitive information
- Protection of classified information

Integrity

- Precision, accuracy
- Internally consistent
  - What is recorded is what was entered
  - When an update is entered, it is propagated as far as appropriate.
- Meaningful and usable
  - Readable
  - Not protected against legitimate access (availability)

Possible ways to protect integrity

- Not modified
- Only in acceptable ways, for example:
    - Can add fields but not change or delete any existing ones.
    - Can increment salary by no more than 10%
    - Each change is logged
    - Each change contains valid data (e.g. A date)
    - frequency

More possible ways to protect integrity

- Only by certain people
  - List of people
  - Roles
- Only by certain processes/programs
  - Database management systems
  - Check certain kinds of validity
  - Check that certain other actions have occured

Availability

- Usable
- Sufficient capacity (bandwidth, sharable, copied as needed, etc)
- Is making progress.
- Not hung (time constraints)
- May be limited by
  - Confidentiality restrictions
  - Integrity control slowdowns

Kinds of Vulnerabilities

- Interruption:
  - breaking a pathway, deleting/destroying
- Interception:
  - “stealing”
- Modification
- Fabrication

Possible Targets:

- Hardware/Firmware
- Software
- Data and Information
- Access, Time, bandwidth, network resources
- People
- Supplies

Computer Attackers run a gamut:

- Unintentional, non-malicious (but not necesarily less deadly!)
  - Caused by insiders.
  - Security awareness and general education is the most effective and least expensive tool
- Amateurs
  - Often insiders with priviledges
  - Outside probers, tinkerers
- Crackers
- Criminals

Crackers

- When does a prober/tinkerer become a cracker?
- Intention to undermine or circumvent security controls
- Motivations: challenge, ego, curiosity, adventure, experimentation, impatience.
- Nonmalicious attacks are still attacks

Criminals

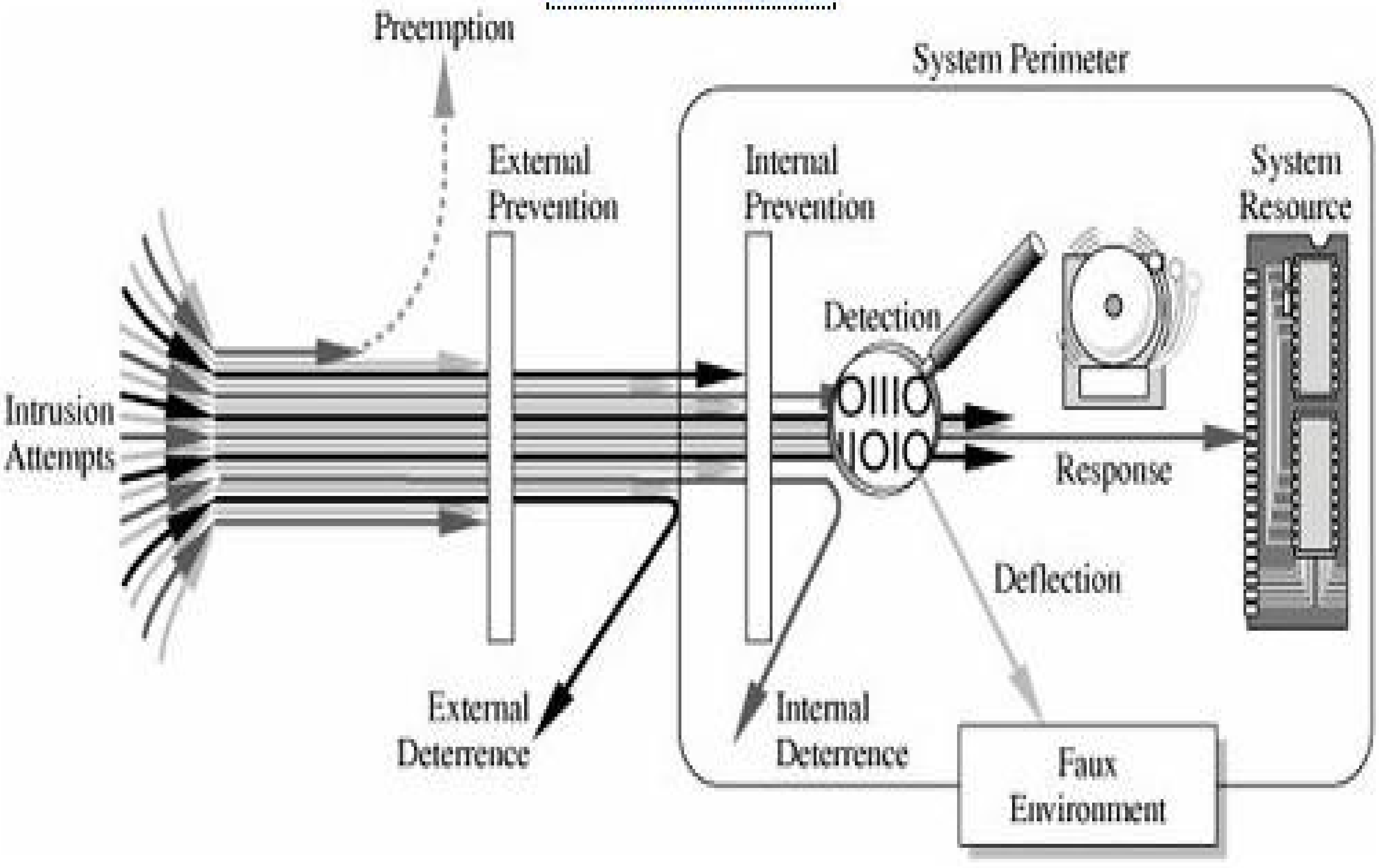
- Motivation: payoff, revenge, competition
- Rapidly growing
- Financial reward potential
- Organized crime is becoming involved
- Definition of “computer crime” not precise,
  - “Malicious act” vs “crime"
  - “using a computer” vs “depending on a computer”
  - Count network vs individual computers
- Morale: beware of statistics (Disraeli)

Defense Objectives

- Prevent Harm: Block attack
  - Not always possible: insiders, unknown vulnerabilities, weakened defenses.
- Deter Harm: Make attack more difficult
- Deflect Harm: Push attacker to another target: honeypots.
- Detect Harm. (help in other objectives)
- Recover From Harm: Resume normal operation – increase defenses, deal with data los/exposure.
- Cost effectiveness of the above for all possible attacks.

Figure 1-6. Multiple Controls.

[View full size image]


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