Diyala University
College of Engineering
Computer & Software
Engineering Department

Fourth Year 2012/2013

ENCRYPTION AND DATA SECURITY

CSE-405
6 UNITS

PRESENTED BY
DR. ALI J. ABBOUD

TEXTBOOKS

- **Applied Cryptography – 2nd edition**

  Bruce Schneier Available online.
- **Security In Computing – 4th edition**

  Pfleeger and Pfleeger.
- http://www.wikipedia.org/
- **Papers assigned for reading**

CLASS STRUCTURE

- Chapter 1: Introduction to encryption and Data security.
- Chapter 2: Encryption systems.
- Chapter 3: Secure encryption systems.
- Chapter 4: Security involving programs.
- Chapter 5: Protection Services for users of operating systems.
- Chapter 6: Data Base security.
- Chapter 7: Computer Network Security.
- Chapter 8: Communication Security.

Chapter 1: Introduction

Is There a Security Problem in Computing?

In This Chapter

- The risks involved in computing
- The goal of secure computing: confidentiality, integrity, availability
- The threats to security in computing: interception, interruption, modifications, fabrication
- Controls available to address these threats: encryption, programming controls, operating systems, network controls, administrative controls, laws and ethics

What Does "Secure" Mean?

- Are you Secure?
  - What makes you feel secure?
- Example: Banks
  - Yesterday – learning from the past
  - Today
- Protecting Valuables
  - Protecting Money Vs. Protecting Information
    - Size and Portability (large vs. small)
    - Ability to Avoid Physical Contact (lots vs. little)
    - Value of Asset (very high vs. variable)

Developing an Understanding

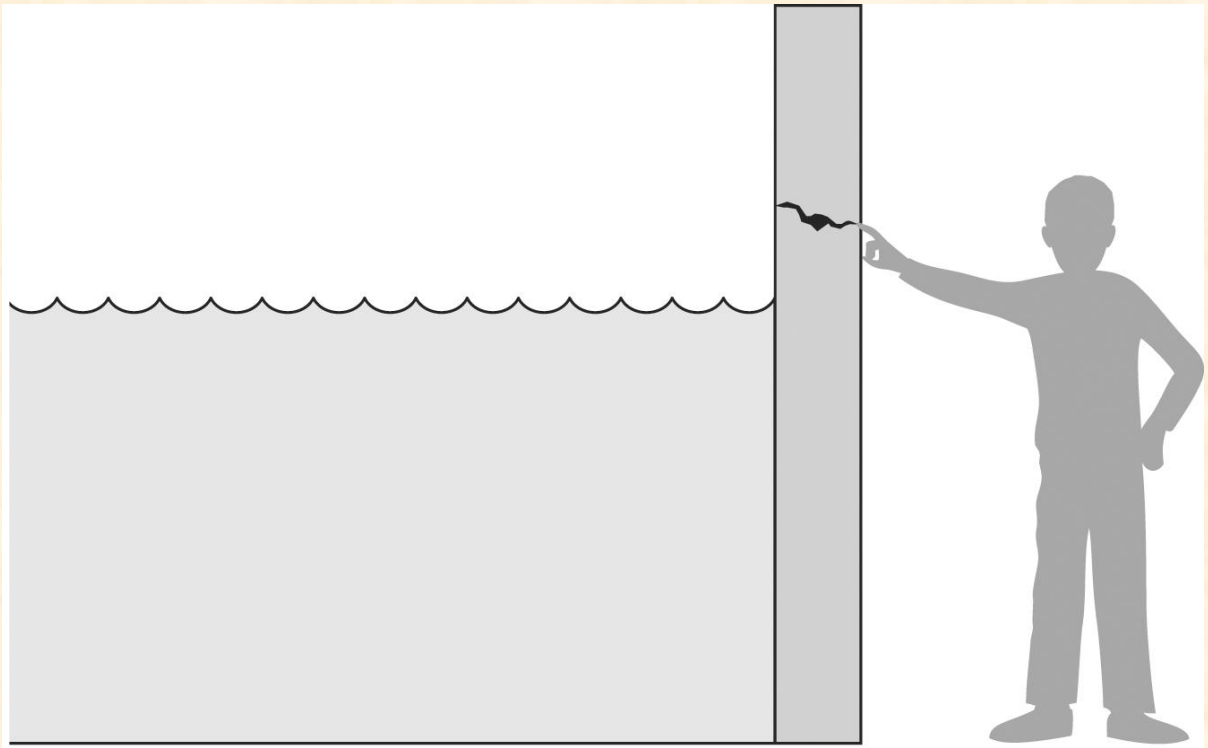
- Examine the risk of security in computing
- Consider available countermeasures or controls
- Stimulate thought about uncovered vulnerabilities
- Identify areas where more work is needed

Characteristics of Computer Intrusion

- Any computer system can be a target:
  - Hardware, Software, Storage, Data, People/User
- Any system is most vulnerable at its weakest point.
- **Principle of Easiest Penetration** - An intruder must be expected to use any available means of penetration. Penetration may not necessarily be by the most obvious means, nor via the one we have the most defense against.
  - Consider all the means of penetration
  - Checked repeated times
  - Don’t underestimate the attacker/think like an attacker
  - Strengthening one thin might weaken another

Attacks

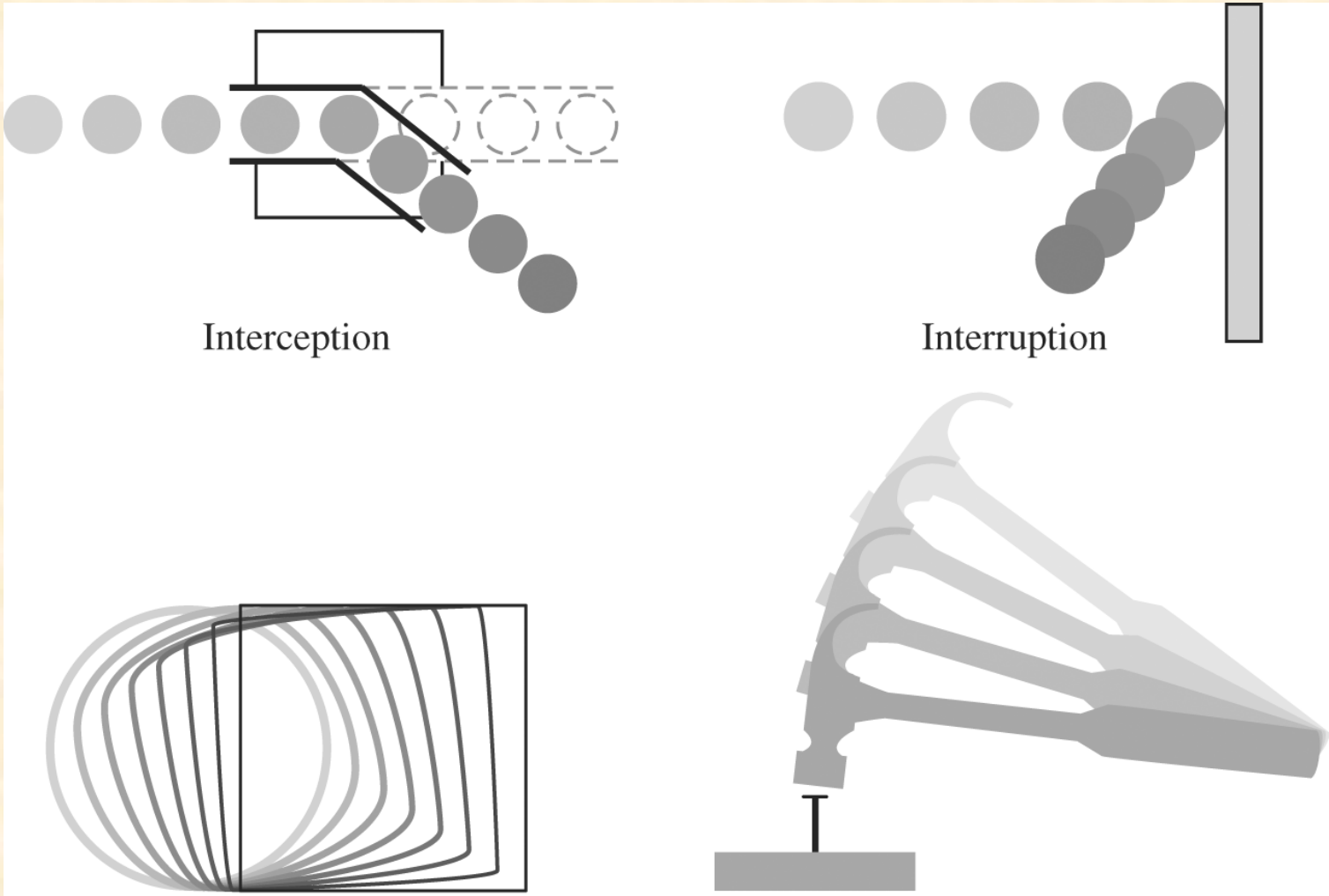
- **The components to attack**:
  - Hardware
  - Software
  - Data
- **Vulnerability** – a weakness in the security system that could be exploited to cause harm or loss.
- **Threat** – a set of circumstances that has the potential to cause loss or harm.
- **Wall holding back water**
  - Threat to get wet
  - Vulnerability is a crack in the wall



Pfleeger/Pfleeger Fig. 01-01

Definitions

- **Attack** – human who exploits a vulnerability
- **Control** – a protective measure against an attack
- ***A threat is blocked by control of vulnerability***
- Type of System Security Threats in computing
  - Interception
  - Interruption
  - Modification
  - Fabrication



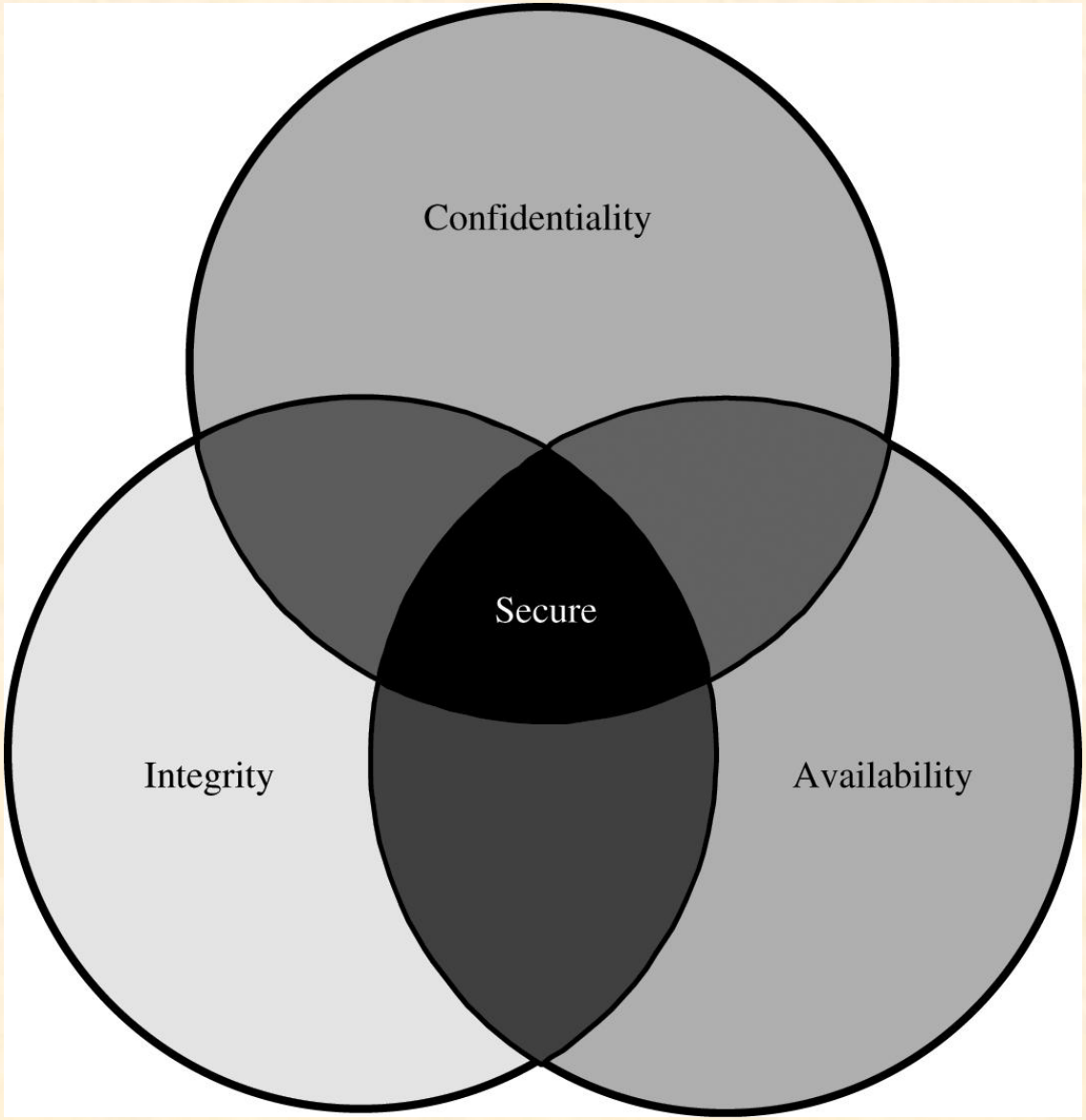
Pfleeger/Pfleeger Fig. 01-02

Method, Opportunity & Motive

- Why? Who? What? When? Where?
- Attacker must have three things:
  - Method – the skill, knowledge and tool
  - Opportunity – the time and access
  - Motive – a reason to want to perform an attack

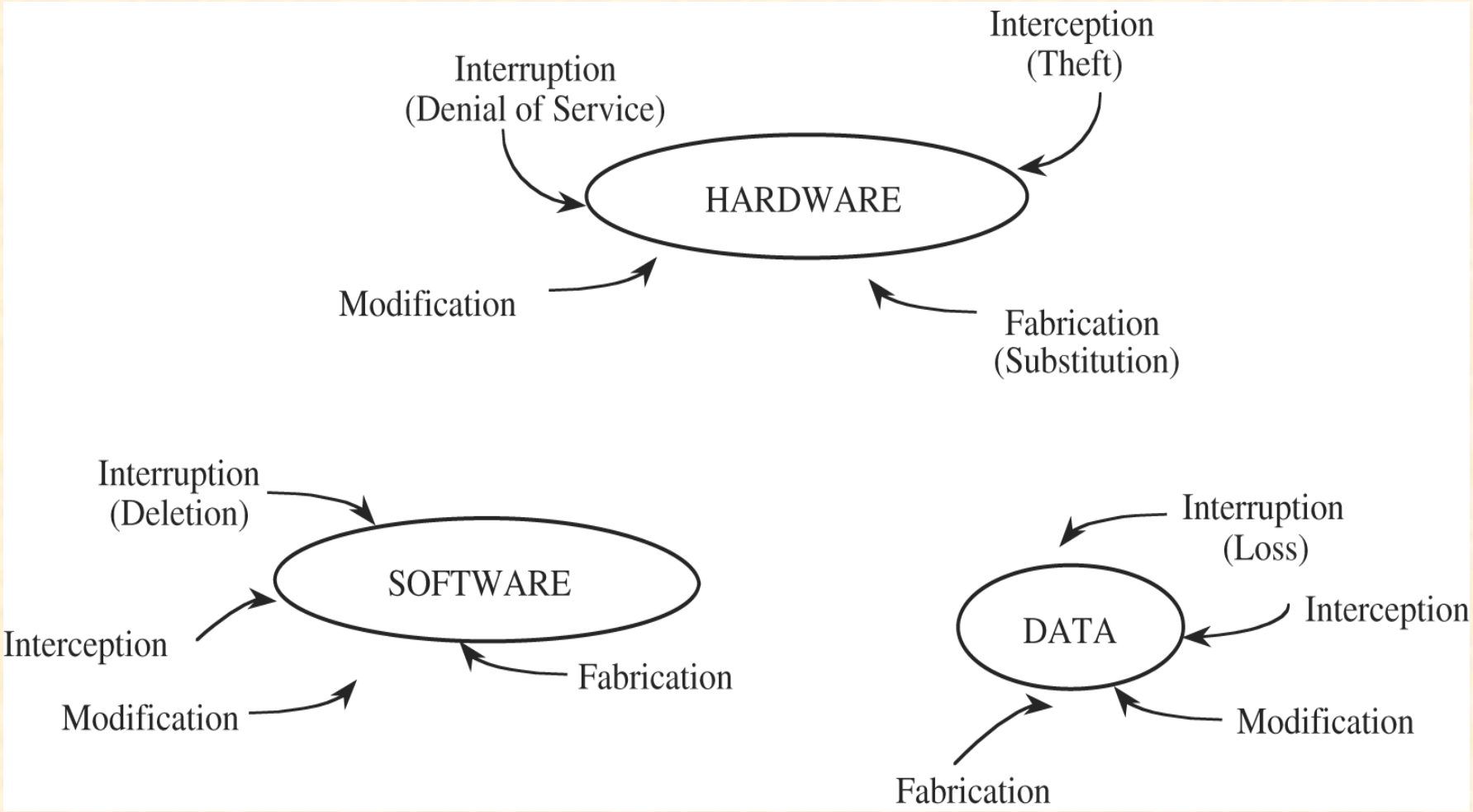
Security Goals

- Secure is:
  - **Confidentiality** (Secrecy or Privacy)- assets accessed only by authorized parties
    - Not only reading but viewing, printing or knowing about the asset
  - **Integrity** – assets modified only by authorized parties
    - Includes writing, changing, changing the status, deleting or creating
  - **Availability** – assets are accessible to authorized parties at appropriate times.
    - Denial of Service

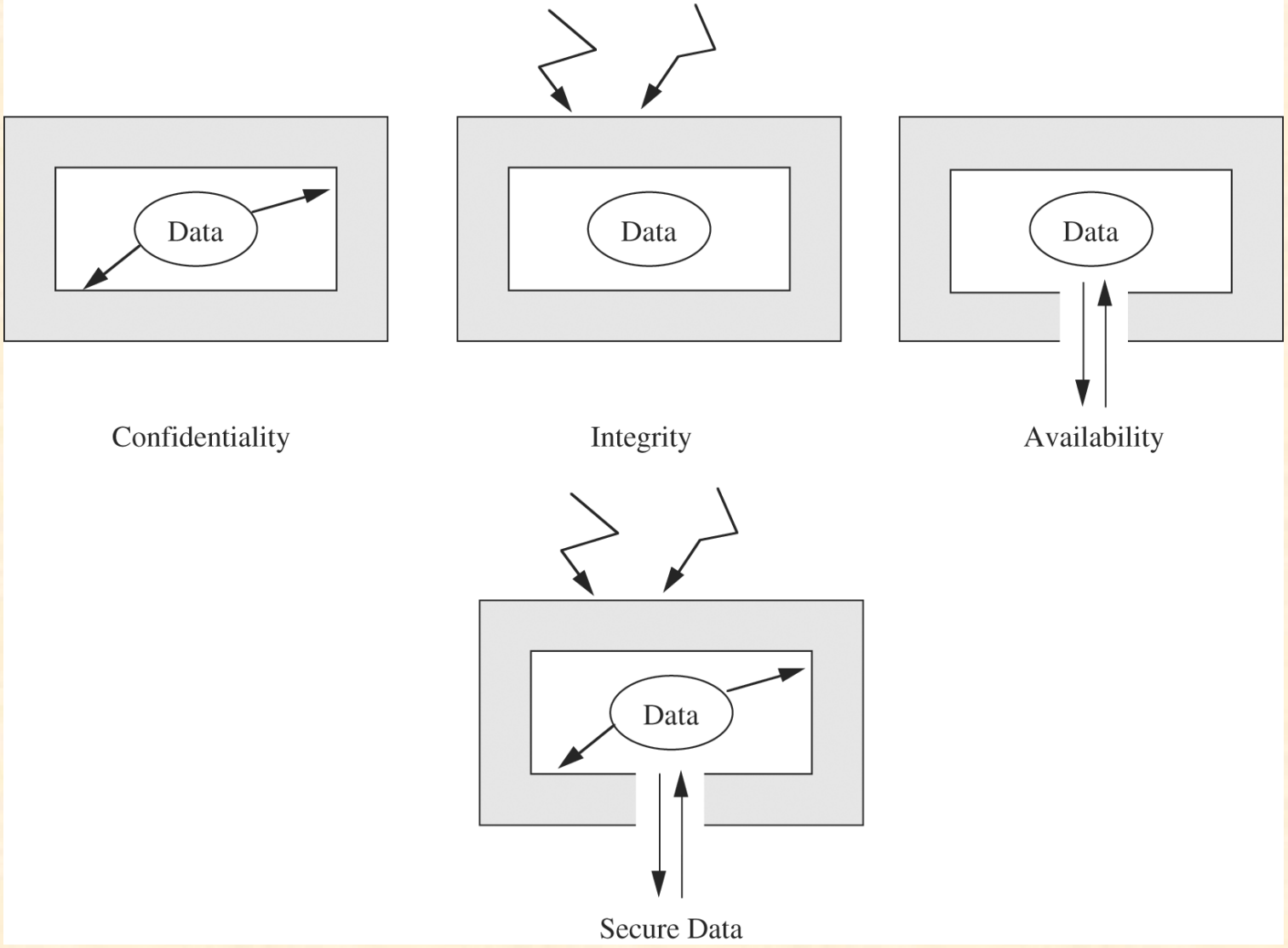

Confidentiality
Secure
Integrity
Availability

Vulnerabilities

- Hardware
  - It is very visible
  - Easy to attack
  - Water, burned, frozen, gassed and electrocuted, dust, time, rodents, environment
  - Voluntary Machine Slaughter or Machinicide
- Software
  - Software Deletion
  - Software Modification
  - Software Theft


Interruption
(Denial of Service)
Interception
(Theft)
HARDWARE
Modification
Fabrication
(Substitution)
Interruption
(Deletion)
SOFTWARE
Interception
Modification
Fabrication
Interruption
(Loss)
DATA
Interception
Modification
Fabrication

- Malicious Modification of Software
  - Logic Bomb
  - Trojan Horse
  - Virus
  - Trapdoor
  - Information leaks
- Data Vulnerabilities
  - Effects everyone
  - Data is more than just an electronic file
  - **Principle of Adequate Protection** – Computer items must be protected only until they lose their value.
  - Data Confidentiality
  - Data Integrity
- Other Exposed Assets
  - Networks
  - Access
  - Key People


Data
Data
Data
Confidentiality
Integrity
Availability
Data
Secure Data

Computer Criminals

- Amateurs
- Crackers or Hackers
- Career Criminal
- Terrorists

Methods of Defense

- Harm occurs when a threat is realized against a vulnerability
- **Risk** – the possibility of harm
- 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)
  - Detect it: either as it happens or some time after the fact
  - And Recover from its effects

Controls

- **Control** – attempt to prevent the exploitation of a vulnerability
- Computer Security has lots of controls
  - Simple or Difficulty
  - Inexpensive or Expensive
- Type of Control
  - Encryption – formal name for the scrambling process
    - deals with confidentially and integrity
    - Does not solve computer security problems.
      - Cleartext
      - Ciphertext
      - Protocols

- Software Controls
  - Programs must be secure to prevent attacks
  - Program Controls:
    - Internal Program Controls
    - Operating System and Network System Controls
    - Independent Control Programs (virus checker)
    - Development Controls (quality standards in construction)
  - Software controls effect the user
- Hardware Controls
  - Smart cards, locks, devices to ID users, firewalls, intrusion detection systems, circuitry control
  - Policies and Procedures
    - Policies – an agreement of way things are done
    - Must be written and training provided
  - Physical Controls – locks/security officer/backups

Effectiveness of Controls

- Controls must be properly used!
- Awareness of Problem
- Likelihood of Use
  - **Principles of Effectiveness** - Control must be used- and used properly- to be effective. They must be efficient, easy to use, and appropriate.
- Overlapping Controls (good)
- Periodic Review – controls are not permanent
  - **Principle of Weakest Link** – Security can be no stronger than its weakest link.

Conclusion

- The risks involved in computing
- The goal of secure computing: confidentiality, integrity, availability
- The threats to security in computing: interception, interruption, modifications, fabrication
- Controls available to address these threats: encryption, programming controls, operating systems, network controls, administrative controls, laws and ethics