# Introduction

Jun Li
lijun@cs.uoregon.edu

# Risk is a fact of life

- Computing entails serious risks to the privacy and integrity of data, or the operation of a computer system.
- How to control the risks?
  - Learn the threats
  - Understand the vulnerabilities that cause the threats
  - Impose controls to reduce or block the threats
  - Balance security and risk

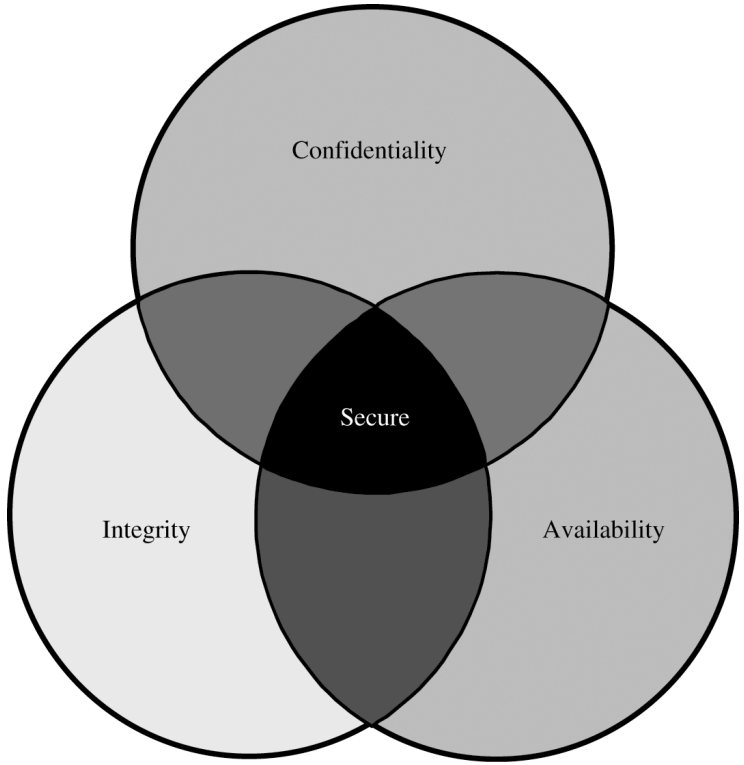
# Computing System and Security

- A **computing system** is a collection of hardware, software, data, and users.
- Any system is most vulnerable at its *weakest point.*
- **Principle of Easiest Penetration**
  - Attackers use any means they can.
  - Defenders must consider all possible penetration.
  - *Adversarial thinking*: Think like an attacker!

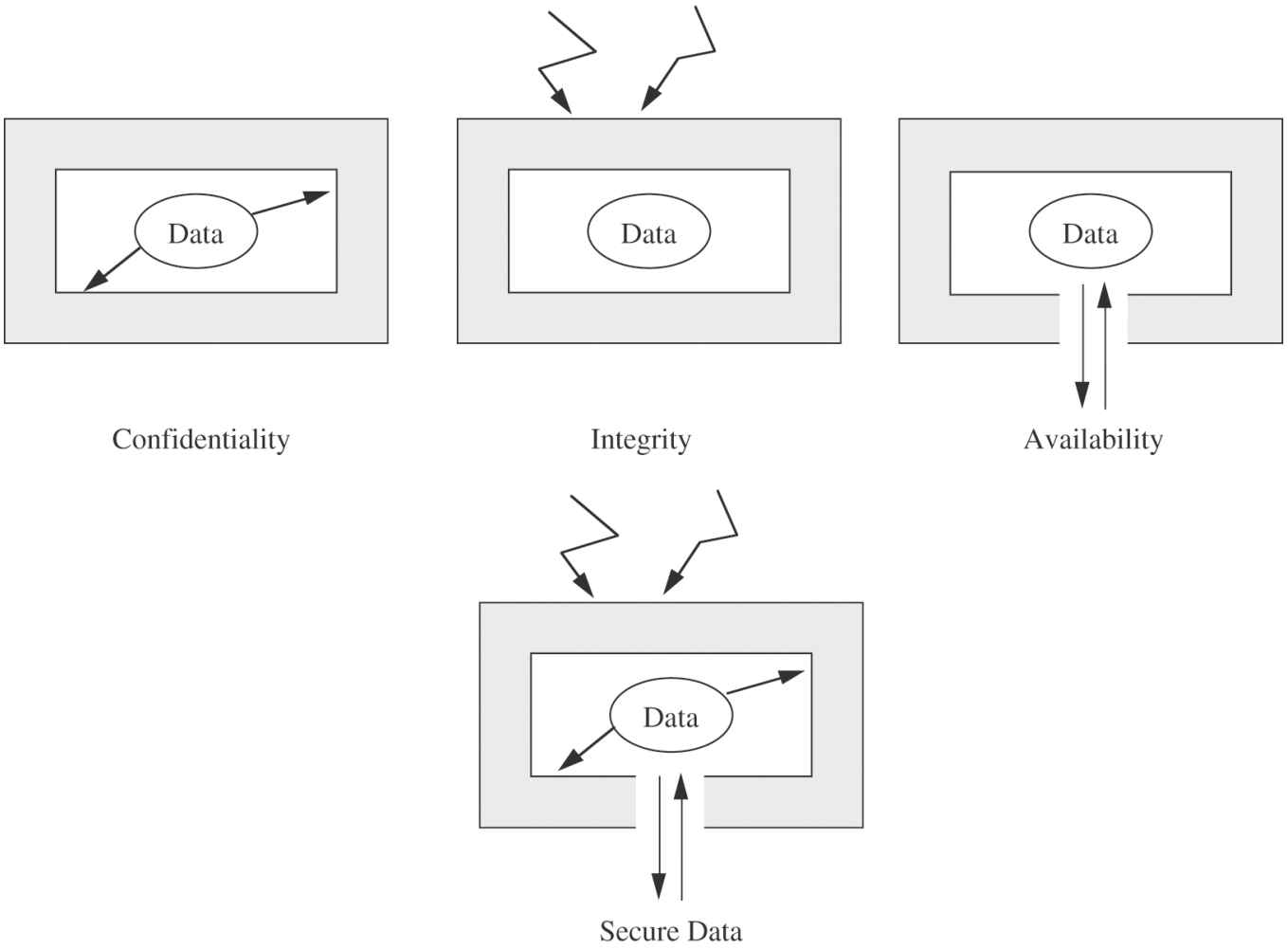
# Meaning of Computer Security

- Confidentiality
- Integrity
- Availability

- *Authentication*
- *Accountability*



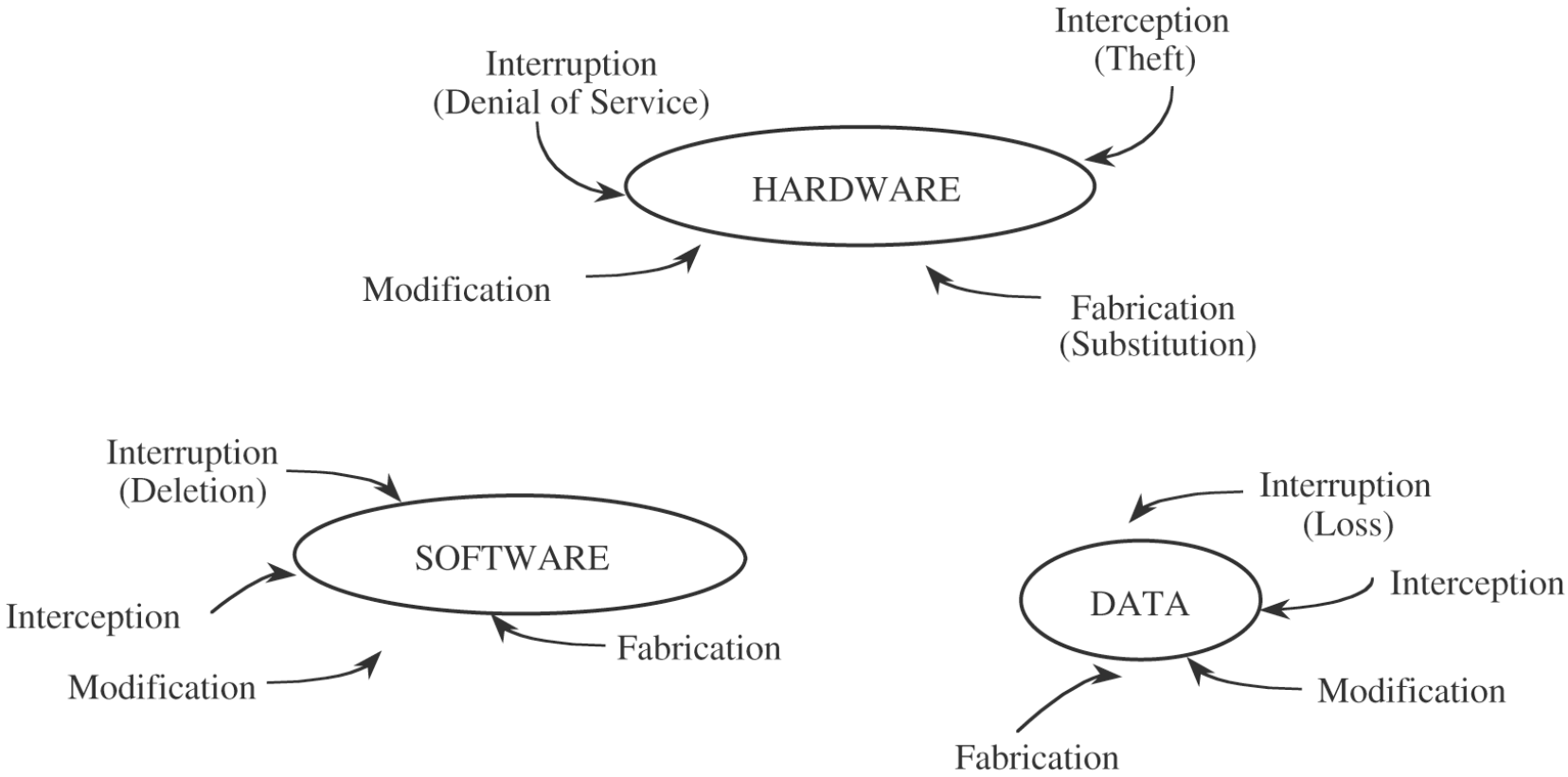
# Data Security



# Vulnerability, Threats, Attacks

- **Vulnerability**: a weakness in a computing system that may be exploited to cause loss or harm.
- **Threat**: a set of circumstances that has the potential to cause loss or harm.
- **Attack**: A human who exploits a vulnerability launches an attack on the system.

# Vulnerabilities



# Computer Criminal and Attackers

- Method
- Opportunity
- Motive

- Amateurs
- Crackers or malicious hackers
- Career criminals
- Terrorists

# What is Computer Security About?

- It's about attack and defense
- It's about the protection of hardware, software, data, and user
- It's about confidentiality, integrity, and availability (plus authentication and accountability as new desired properties)

# Methods of Defense

- Prevent
- Deter
- Deflect
- Detect
- Mitigate
- Recover

# Controls

- Encryption
- Physical controls
- Hardware controls
  - Hardware implementation of encryption
  - Circuit boards that control access to storage media
  - Authentication device
  - Intrusion detection systems (IDS)
  - Firewalls

# Controls (cont'd)

- Software controls
  - Independent control programs (e.g., IDS, virus scanner, password checker)
  - Operating system and network system controls
  - Internal program controls
  - Development controls
- Policies and procedures
  - This is usually the starting point!

# Effectiveness of Controls

- **Principle of Effectiveness:** Controls must be used—and used properly—to be effective. They must be efficient, easy to use, and appropriate.
- **Principle of Weakest Link:** Security can be no stronger than its weakest link.

# Discussion Questions

- What is the relationship between the **Principle of Easiest Penetration** and **Principle of Weakest Link**?
- Which method(s) of defense do you prefer the most?
- Vulnerability, threat, and attack: which one(s) would you handle first to protect a computing system?
- What is your definition w.r.t. what computer security is about?