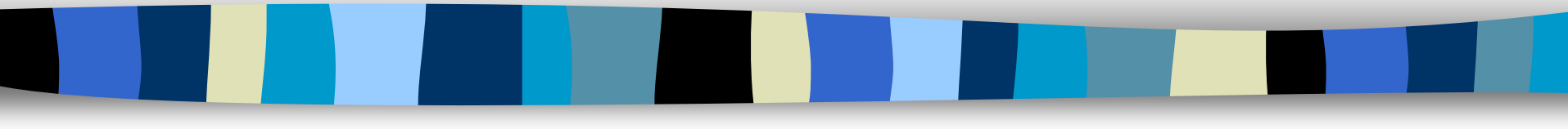
Chapter 1



Introduction to computer security

What is the security problem?

- Security is an increasingly prevalent problem in computer science. Why?
  - Increased connectivity
  - Large number of valuable assets online
  - Low threshold to access
  - Sophisticated attack tools and strategies available
  - Others…

What does IT security means?

IT security is commonly defined to have two aspects:

- *Computer security* which aims to preserve the computing resources against abuse and unauthorized use as well as to protect data from accidental or deliberate damage, disclosure or modification.
- *Communication security* which aims to protect data during its transmission in computer networks and distributed systems.

A security Paradox

- Organizations often choose not to investigate or prosecute intruders:
  - They don’t want to expose vulnerabilities in their systems
  - They want to protect their public image
  - Intruders are sometimes viewed as mere pranksters
  - Sometimes electronic assets are not viewed as valuable.

Characteristics of Computer Intrusion

- A **computing system**: a collection of hardware, software, data, and people that an organization uses to do computing tasks
- Any piece of the computing system can become the **target** of a computing crime.
- The **weakest point** is the most serious vulnerability.
- The **principles of easiest penetration** (p.5)

Security Breaches - Terminology (p.5)

- Exposure
  - a form of possible loss or harm
- Vulnerability
  - a weakness in the system
- Attack
- Threats
  - Human attacks, natural disasters, errors
- Control – a protective measure
- Assets – h/w, s/w, data

Types of Security Breaches (p 7, 8)

- **Interruption:** An asset of the system becomes lost, unavailable, or unusable.
  - Example: DOS (Denial of Service)
- **Interception:** An unauthorized party has gained access to an asset.
  - Peeping eyes
- **Modification:** An unauthorized part not only accesses but tampers with an asset.
  - Change of existing data
- **Fabrication:** An unauthorized party might fabricate counterfeit objects on a computing system.
  - Addition of false or spurious data

Security Goals (p 9-12)

Historically security has been defined to encompass:

- **Confidentiality**
  - The assets are accessible only by authorized parties.
- **Integrity**
  - The assets are modified only by authorized parties, and only in authorized ways.
- **Availability**
  - Assets are accessible to authorized parties.
- See Fig. 1-3 (p.11)

Security Goals (p 9-12)

Some experts (e.g. National Security Agency NSA) typically add to this list:

- Authentication: to make sure that a party is really the one which is claiming to be.
- Non Repudiation: to make sure that a party cannot deny sending or receiving an asset if done.

Computing System Vulnerabilities

- See Fig. 1-4 (p.13)
- Hardware vulnerabilities
- Software vulnerabilities
- Data vulnerabilities
- Human vulnerabilities ?

Software Vulnerabilities

- Destroyed (deleted) software
- Stolen (pirated) software
- Altered (but still run) software
  - Logic bomb
  - Trojan horse
  - Virus
  - Trapdoor
  - Information leaks

Data Security

- The **principle of adequate protection** *(p.16)*
- Fig. 1-5 (p.18)
  - Confidentiality: preventing unauthorized access
  - Integrity: preventing unauthorized modification (e.g., salami attack)
  - Availability: preventing denial of authorized access

Other Exposed Assets

- Storage media
- Networks
- Access
- Key people

People Involved in Computer Crimes

- Amateurs
- Crackers
- Career Criminals

Methods of Defense

- Encryption
- Software controls
- Hardware controls
- Policies
- Physical controls

Principle of Effectiveness

- Controls must be used to be effective.
  - Efficient
    - Time, memory space, human activity, …
  - Easy to use
  - appropriate