Topics Covered In The Course

- Security planning, security policies, security goals, security mechanisms, security principles, physical security, risk analysis and management, and hackers.
- Introduction to Cryptography.
- Authentication Functions.
- Symmetric Key-Exchange Protocols.
- Asymmetric Key-Distribution and Cryptography.
- Network Layer Security.
- Transport Layer Security.
- Wireless network security.

What is Security?

- *Security* is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable
- Security rests on confidentiality, integrity, and availability.

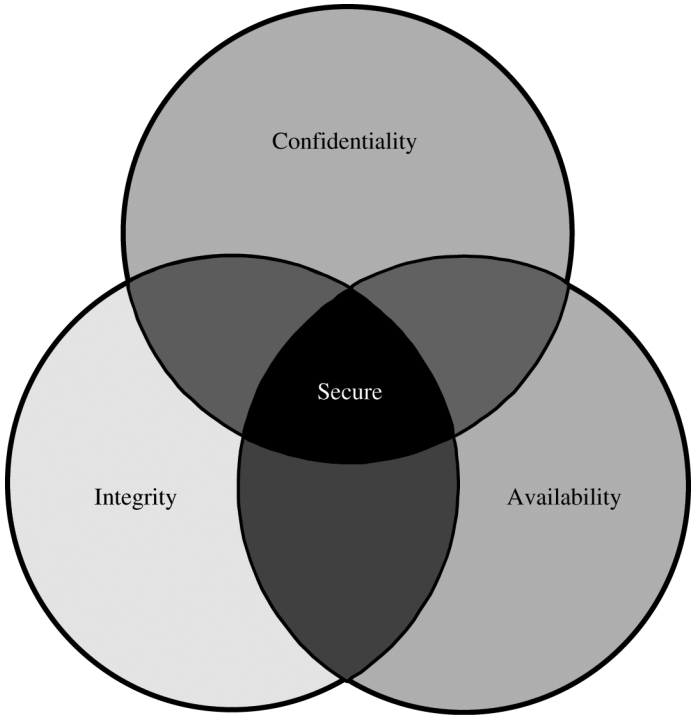


Figure 1-3 Relationship Between Confidentiality, Integrity, and Availability.

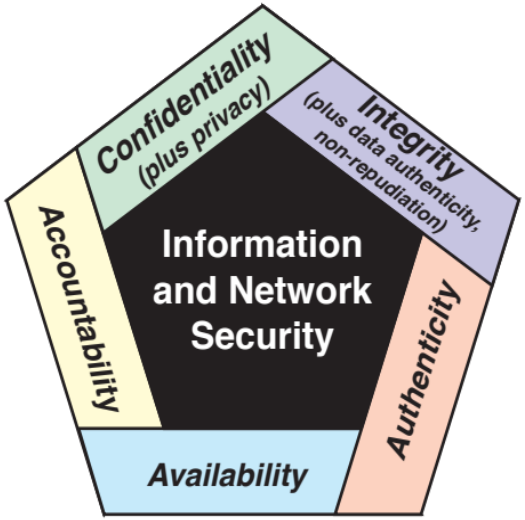


Figure 1.1 Essential Information and Network Security Objectives

Fundamental Security Services

- Confidentiality
  - guarantee that data is never available to unauthorized parties (in clear form).
- Integrity
  - guarantee that data can never be modified by unauthorized persons (or that it cannot be modified without being detected)
- Availability
  - guarantee of service
    - e.g., network bandwidth, disk space (for syslog, mail, ...)
- Everything else is a mechanism to achieve one of these services.

Fundamental Concepts/Terminology

- CompuSec – Computer Security (generally only access control, local authentication)
- ComSec – Communication Security (generally hardware-based crypto boxes)
- InfoSec – Information Security (a combination of CompuSec and ComSec)

Brief History of Computer Security

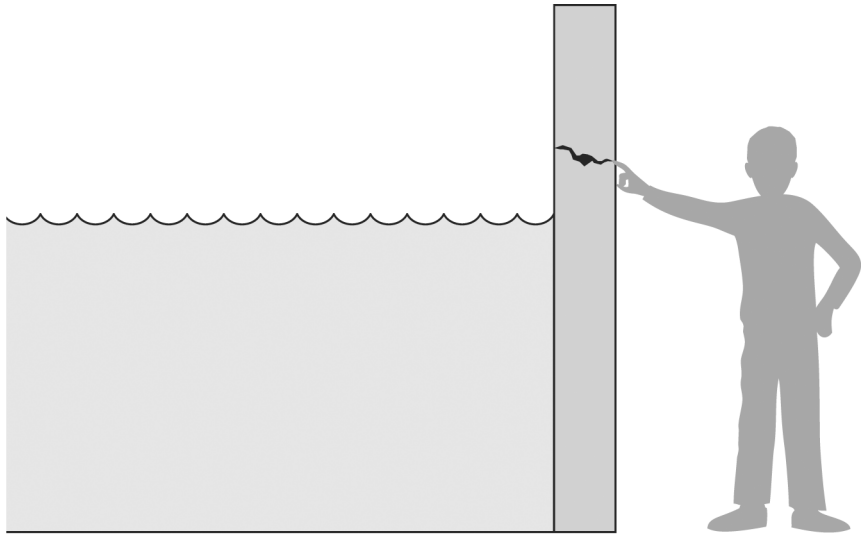
- **Security starts as a DoD-only problem**
  - only to those who really care
  - Only to those who have budget for custom solutions
- **Multics**
  - origin of automated "multi-level" security policy
- **Orange Book**
- **Rainbow Series**
- **DoD Efforts**
  - SComp
  - Blacker
  - Lock
- **Commercial Efforts**
  - DEC's A1 VAX Architecture
  - Compartmented Mode Workstations
  - TMach

1990s: Security is Everyone's Problem

- DoD cannot/will not afford custom solutions
- Power grids
- Stock market
- Internet (infrastructure)
- e-commerce, privacy, liability
- from risks:
  - ATM screen shows "C:\exe>"
  - youth released from jail in Baltimore

Vulnerabilities vs. Threats

- **Vulnerability: any property (generally a weakness) of the system that could lead to the loss of one of the basic services**
  - **e.g. not checking string lengths**
- **Threat: the chance for someone to exploit a vulnerability.**
  - **e.g. the Morris worm**
- **Evaluating the security of a system is a process of evaluating the threats against a system, the probability of exploiting each of those threats, and the consequences of exploitation.**
- **Securing a system is the process of trading off the security of potential system designs, with the cost of addressing "Risk Management."**

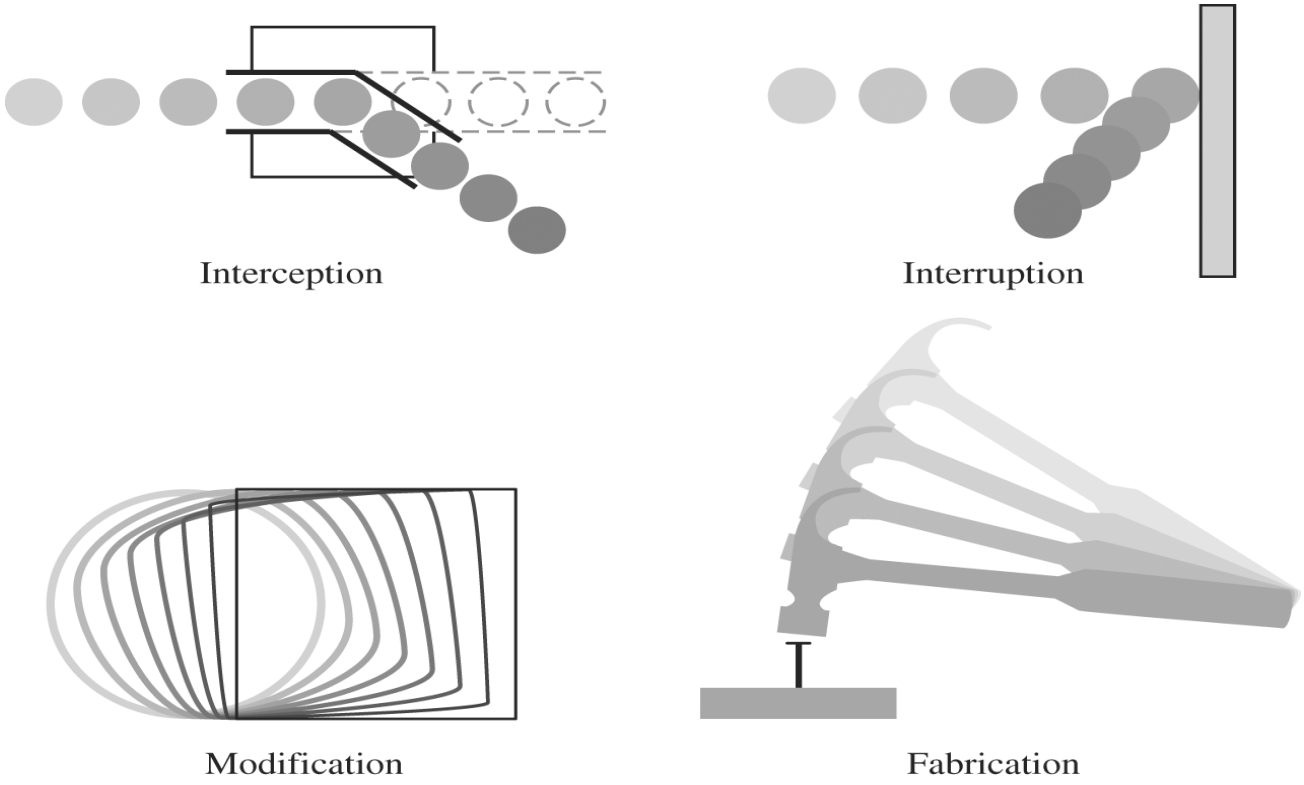


Pfleeger/Pfleeger Fig. 01-01

Figure 1-1 Threats, Controls, and Vulnerabilities.

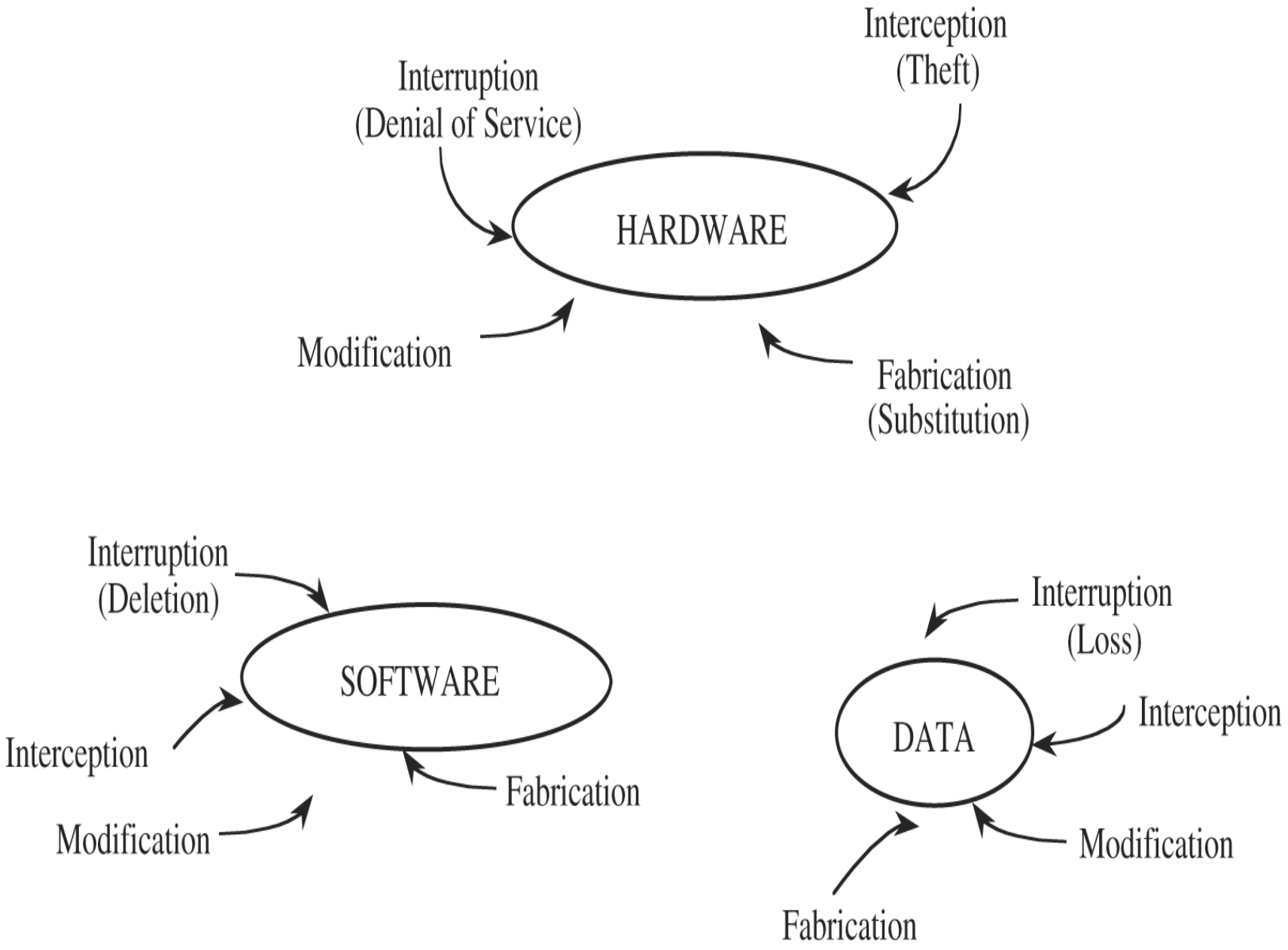
Threats

- Interception
  - Unauthorized parties obtain access to assets
- Interruption
  - Assets of a system becomes lost, unavailable, or unusable
- Modification
  - Unauthorized parties tamper assets
- Fabrication
  - Unauthorized parties create counterfeit objects to cheat a system



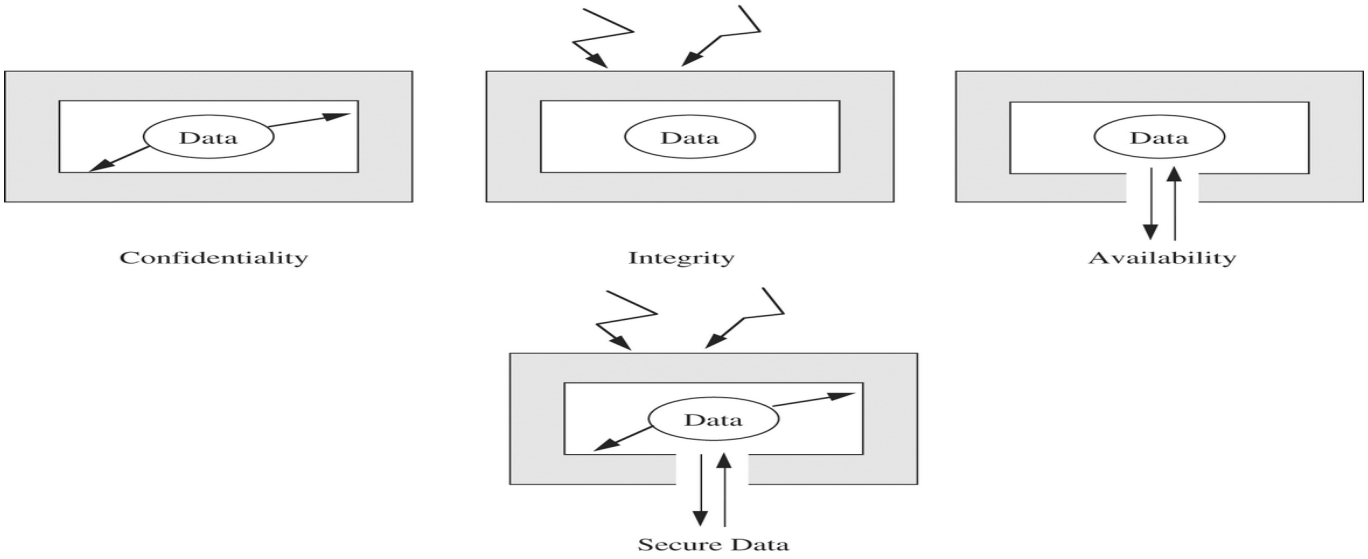
Pfleeger/Pfleeger Fig. 01-02

Figure 1-2 System Security Threats.


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

Three Goals of Data Security

- Data Confidentiality
  - to prevent unauthorized disclosure of data
- Data Integrity
  - to prevent unauthorized modification on data
- Data Availability
  - to prevent authorized access to data



Security Policies

- Discretionary Security Models
- Access Control Lists
- Unix rwx bits/groups
- Mandatory Policies (i.e., not at discretion of users)
- Lattice-based Policies
- Miscellaneous Policies

Mandatory Security Policies

- **Intransitivity: Type Enforcement, Domain Type Enforcement**
  - **Subjects are in domains, objects have types**
  - **Table of access rights (subject domain X object type)**
  - **Enforcement of "Least Privilege"**
    - **constrain malicious code**
    - **trusted pipelines**
    - **can't run everything you can read**
    - **can't mod what you can execute**

Lattice-based Policies

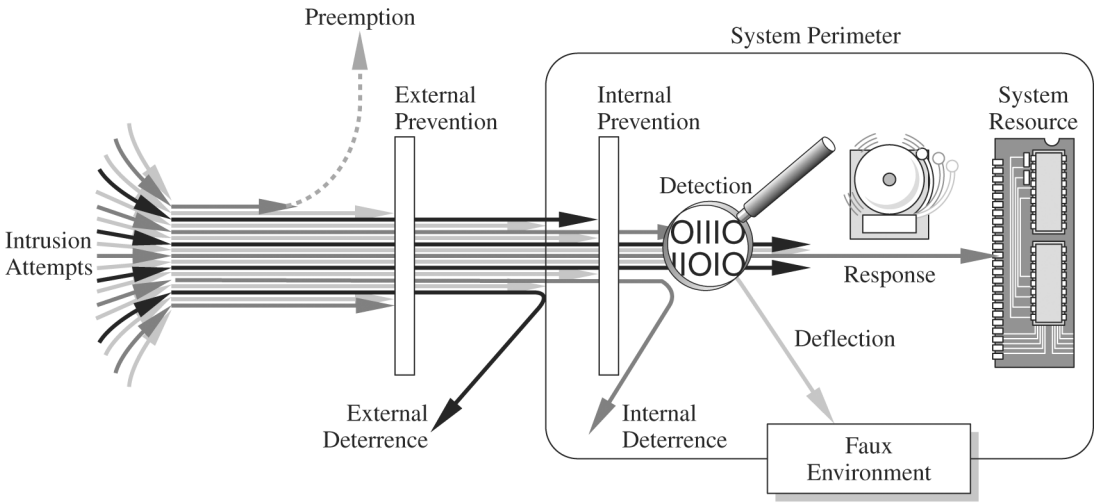
- **MLS (Multi-level security)**
  - **subjects, objects**
  - **top secret, secret, etc.**
  - **Confidentiality**
- **Lattices are partial orders**
  - **transitive; x >> y & y >> z -> x >> z**
  - **reflexive; x dominates x**
  - **anti-symmetric; x >> y & y >> x -> x = y**
- **Information Flow Policies**
  - **Non-interference/covert channels**

Miscellaneous Policies

- **Role-based access control**
- **Time-based access control**
- **Separation of Duty**
- **Conflict of Interest**
- **Trust**
  - Amount of faith placed in another person/computer to obey certain policies
  - should always be with respect to something else

Methods of Defense

- Prevention
  - to block attacks or to close the vulnerability
- Deterrence
  - to make it more difficult to attack
- Deflection
  - to lure attacks to fake objects
- Detection
  - to discover attacks or intrusions
- Recovery
  - to recover a compromised environment



Pfleeger/Pfleeger Fig. 01-06

Figure 1-6 Multiple Controls.

Evaluating System Security (Criteria)

- Orange Book Ratings
  - D -- No Security (Free!)
  - C1, C2 -- Discretionary Access Controls/Audit
  - B1, B2, B3 - Mandatory Access Controls, Audit, Covert Channel, ...
  - A1 -- Formally proven design
- UK/Canadian Criteria