Chapter 1: Introduction

- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Assurance
- Operational Issues
- Human Issues

Basic Components

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources

Classes of Threats

- Disclosure
  - Snooping
- Deception
  - Modification, spoofing, repudiation of origin, denial of receipt
- Disruption
  - Modification
- Usurpation
  - Modification, spoofing, delay, denial of service

Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines "security" for the site/system/*etc*.
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

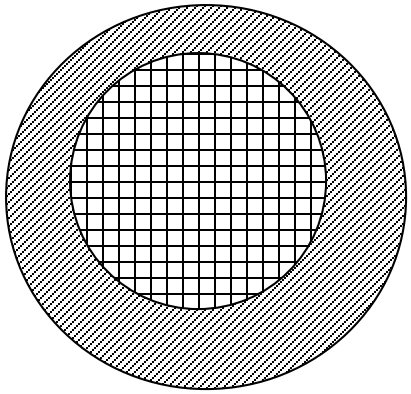
Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

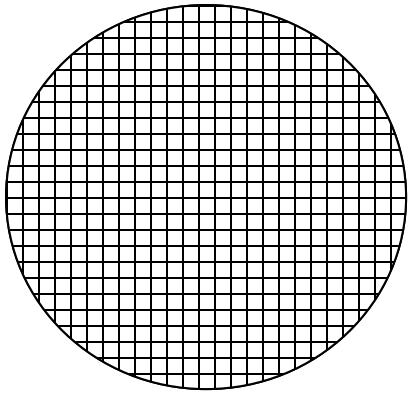
Trust and Assumptions

- Underlie *all* aspects of security
- Policies
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly

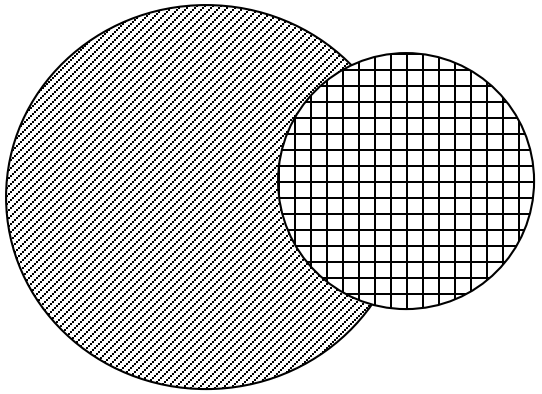
Types of Mechanisms



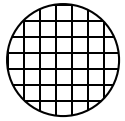
secure



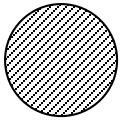
precise



broad



set of reachable states



set of secure states

Assurance

- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

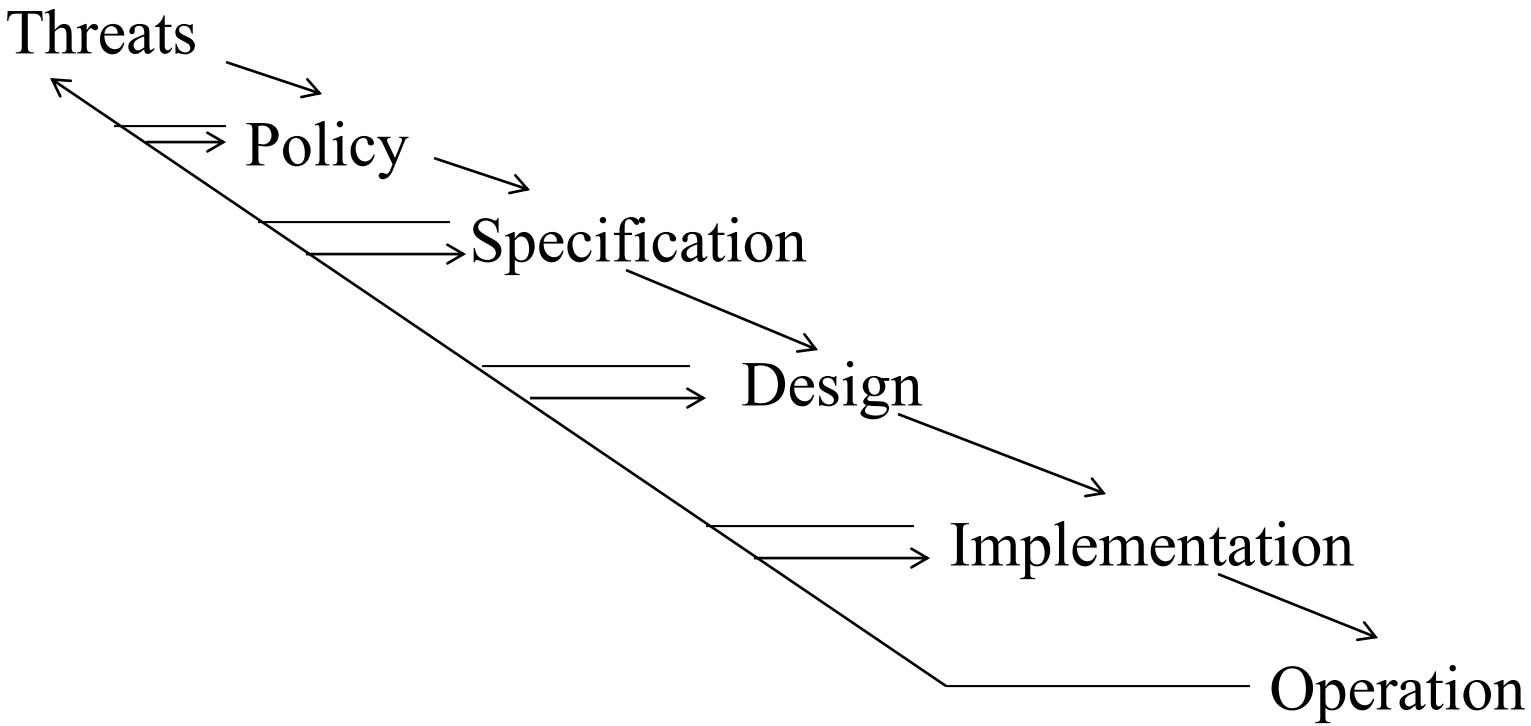
Operational Issues

- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect this thing?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?

Human Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
  - Social engineering

Tying Together



Key Points

- Policy defines security, and mechanisms enforce security
  - Confidentiality
  - Integrity
  - Availability
- Trust and knowing assumptions
- Importance of assurance
- The human factor

Chapter 1

Introduction

Objectives

- To define three security goals
- To define security attacks that threaten security goals
- To define security services and how they are related to the three security goals
- To define security mechanisms to provide security services
- To introduce two techniques, cryptography and steganography, to implement security mechanisms.

1-1 SECURITY GOALS

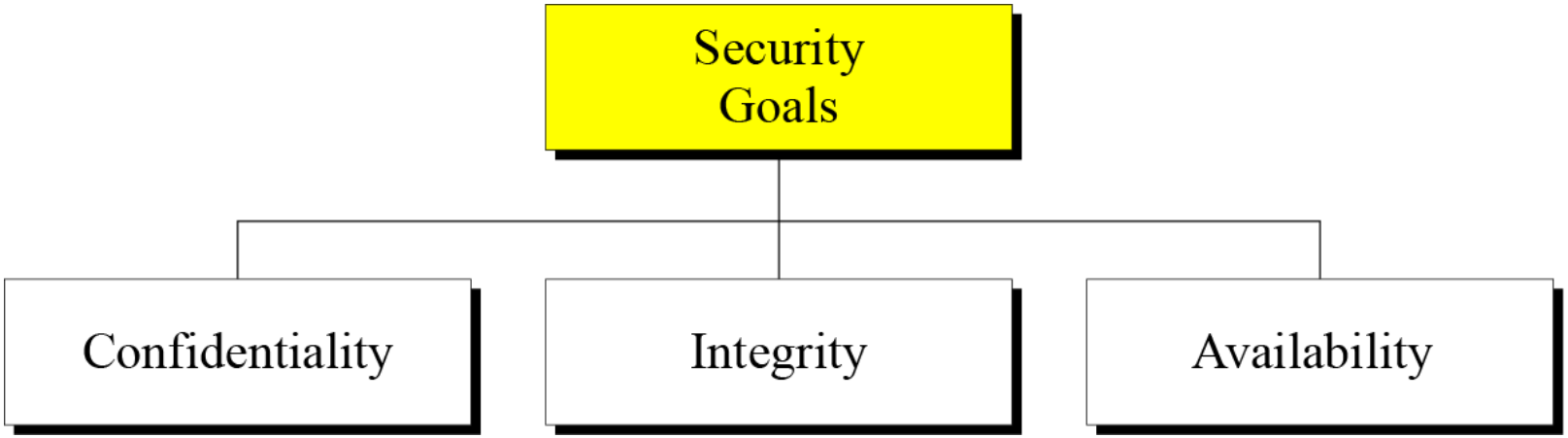
This section defines three security goals.

Topics discussed in this section:

1.1.1 Confidentiality
1.1.2 Integrity
1.1.3 Security

1.1 Continued

Figure 1.1 *Taxonomy of security goals*



1.1.1 Confidentiality

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

1.1.2 Integrity

Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

1.1.3 Availability

The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

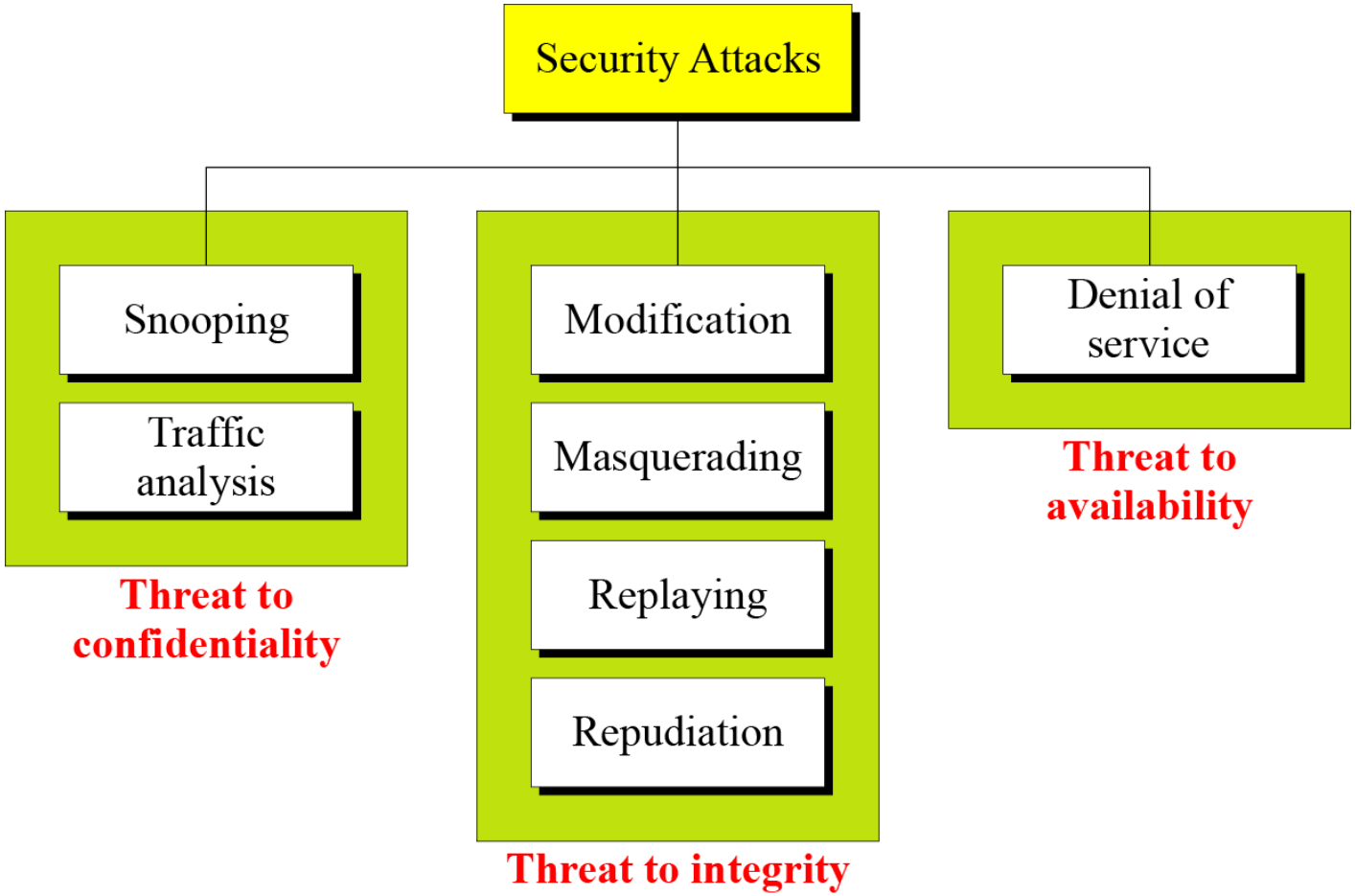
1-2 ATTACKS

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

Topics discussed in this section:

1.2.1 Attacks Threatening Confidentiality
1.2.2 Attacks Threatening Integrity
1.2.3 Attacks Threatening Availability
1.2.4 Passive versus Active Attacks

Figure 1.2 *Taxonomy of attacks with relation to security goals*



1.2.1 Attacks Threatening Confidentiality

Snooping ***refers to unauthorized access to or interception of data.***

Traffic analysis ***refers to obtaining some other type of information by monitoring online traffic.***

1.2.2 Attacks Threatening Integrity

Modification ***means that the attacker intercepts the message and changes it.***

Masquerading ***or*** ***spoofing*** ***happens when the attacker impersonates somebody else.***

Replaying ***means the attacker obtains a copy of a message sent by a user and later tries to replay it.***

Repudiation ***means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.***

1.2.3 Attacks Threatening Availability

Denial of service ***(DoS) is a very common attack. It may slow down or totally interrupt the service of a system.***

1.2.4 Passive Versus Active Attacks

Table 1.1 *Categorization of passive and active attacks*

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

1-3 SERVICES AND MECHANISMS

ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..

Topics discussed in this section:

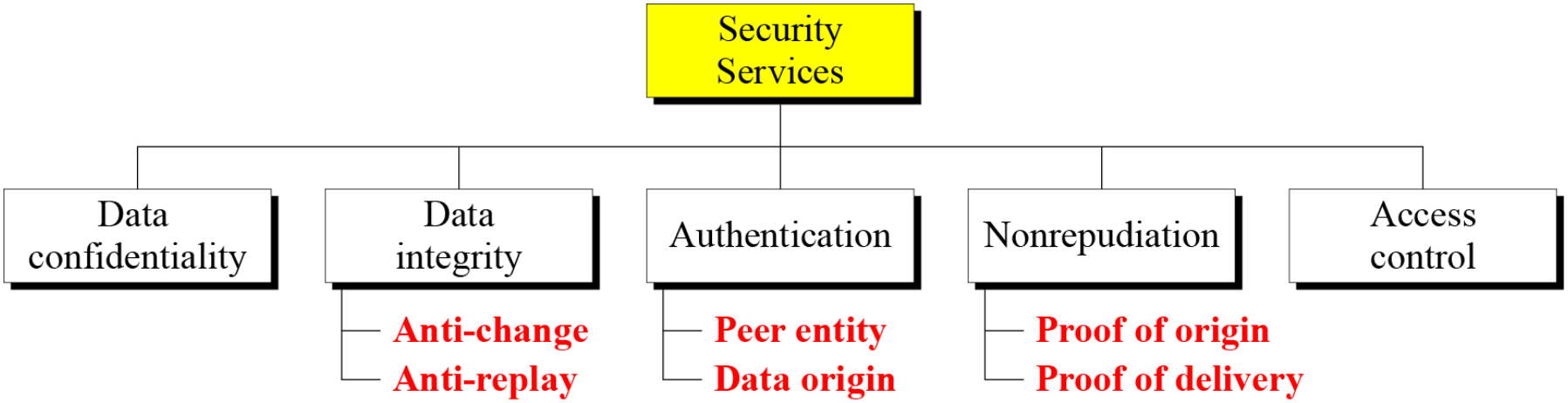
1.3.1 Security Services

1.3.2 Security Mechanism

1.3.3 Relation between Services and Mechanisms

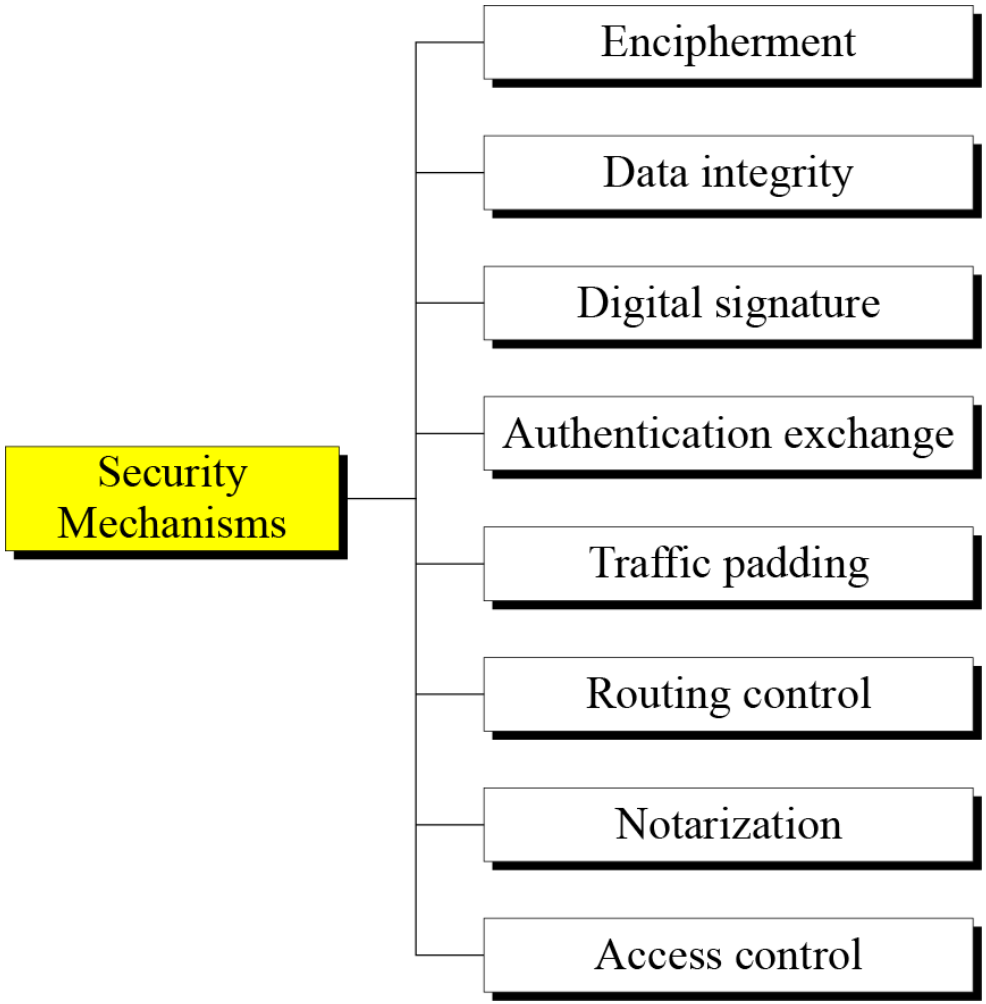
1.3.1 Security Services

Figure 1.3 *Security services*



1.3.2 Security Mechanism

Figure 1.4 *Security mechanisms*



1.3.3 Relation between Services and Mechanisms

Table 1.2 *Relation between security services and mechanisms*

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

1-4 TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.

Topics discussed in this section:

1.4.1 Cryptography

1.4.2 Steganography

1.4.1 Cryptography

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

1.4.2 Steganography

The word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing."

Example: covering data with text

This book is mostly about cryptography, not steganography.

□ □□□ □ □ □ □ □□

0 1 0 0 0 0 1

1.4.2 Continued

Example: using dictionary

A	friend	called	a	doctor.
0	10010	0001	0	01001

Example: covering data under color image

01010011	10111100	01010101
01011110	10111100	01100101
01111110	01001010	00010101

1-5 THE REST OF THE BOOK

The rest of this book is divided into four parts.

Part One: Symmetric-Key Enciphermen

Part Two: Asymmetric-Key Encipherment

Part Three: Integrity, Authentication, and Key Management

Part Four: Network Security