Computer Security Overview

Dr. Ahmad Almulhem

Computer Engineering Department, KFUPM

Spring 2008
Basic Components

Confidentiality: Keeping data and resources hidden

Integrity: Preventing unauthorized modification
  - Data integrity (integrity)
  - Origin integrity (authentication)
  - Integrity mechanisms: Prevention vs Detection

Availability: Enabling access to data and resources
Threats

Definition (Threat)
A threat is a potential violation of security

Definition (Attack)
An attack is a threat executed by an attacker

- confidentiality, integrity, and availability are used to counter threats and attacks
Classes of Threats

1. **Disclosure** (unauthorized access to information)
   - snooping, sniffing, wiretapping
   - Confidentiality services counter this threat

2. **Deception** (acceptance of false data)
   - Modification, spoofing, repudiation of origin, denial of receipt
   - Integrity services counter this threat

3. **Disruption** (interruption or prevention of correct operation)
   - Modification
   - Integrity services counter this threat

4. **Usurpation** (unauthorized control of some part of a system)
   - Modification, spoofing, delay, denial of service
   - Availability services counter this threat
Policies and Mechanisms

Definition (security policy)
A security policy is a statement of what is, and what is not, allowed.

Definition (security mechanism)
A security mechanism is a method, tool, or procedure for enforcing a security policy.

- Policy says what is, and is not, allowed (formal or informal)
- 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

1. **Prevention**
   - Prevent attackers from violating security policy

2. **Detection**
   - Detect attackers violation of security policy

3. **Recovery**
   - Stop attack, assess and repair damage
   - Continue to function correctly even if attack succeeds
Assumptions and Trust

- Underlie all aspects of security
  - example: Opening a door lock requires a key?

- Assumptions about policies
  - Unambiguously partition system states
  - Correctly capture security requirements

- Assumptions about mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly
Types of Mechanisms

- **Secure**
- **Precise**
- **Broad**

- Set of reachable states
- Set of secure states
Assurance

**Definition (Assurance)**

A basis of “how much” one can trust a system

- **Specification**
  - Requirements analysis
  - Statement of desired functionality

- **Design**
  - How system will meet specification

- **Implementation**
  - Programs/systems that carry out design
Operational Issues

- Policies and mechanisms must consider factors other than protection
- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis (Attack trees)
  - 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**
  - No financial benefits (how about break-ins!)
  - Security conflicts with usability, free access, performance

- **People problems**
  - Outsiders and insiders
  - Social engineering

(src: http://www.ranum.com/)
Tying Together

The security life cycle

- Threats
- Policy
- Specification
- Design
- Implementation
- Operation
Key Points

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