Outline

• 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
  • Allowing 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 violating security policy

• Recovery
  • Stop attack, assess and repair damage
  • Continue to function correctly even if attack succeeds
Assumptions and Trust

• 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 or systems that carry out design
Example: SolarWinds

- SolarWinds provides widely used system management tools for network and infrastructure monitoring
  - Among the components is Orion, a performance monitoring system
  - Orion is used by over 30,000 public, private organizations, including government
- Attackers compromised system with Orion source code
- They then altered the source to create a back door
- At next upgrade of Orion, the rigged program was distributed
  - This gave the attackers access to organizations’ infrastructure
- FireEye spotted infected customers’ systems, then found they had been infected
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

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