CISC 7310X

C13a System Security: Basic Concepts

Hui Chen

Department of Computer & Information Science

CUNY Brooklyn College

Acknowledgement

- These slides are a revision of the slides provided by the authors of the textbook via the publisher of the textbook

Outline

- An introduction to system security
  - The Security Problem
  - Program Threats
  - System and Network Threats
  - Cryptography as a Security Tool
  - User Authentication
  - Implementing Security Defenses
  - Firewalling to Protect Systems and Networks
  - Computer-Security Classifications
  - An Example: Windows 7

Defining Security for a System

- Security policy
  - Statement of *what is, and is not, allowed*
  - It defines "security" for a system, a network, or a site

Composition of Policies

- Mathematically, as a list of allowed (secure) and disallowed states
- In practice, policies often described in natural languages
- If policies conflict, discrepancies may create security vulnerabilities

Enforcing Security Policies

- Security mechanisms
  - Method, tool, or procedure for enforcing a security policy
  - Mechanism can be nontechnical
  - Procedural mechanisms often complement technical mechanisms
- Security vulnerabilities can also be the result of imperfect mechanisms

The Security Problem

- System **secure** if resources used and accessed as intended under all circumstances (i.e., security policies are strictly adhered to or perfectly enforced)
- Total security is unachievable

Vulnerabilities

- If policies conflict, discrepancies may create security vulnerabilities
- Security vulnerabilities can also be the result of imperfect mechanisms

Intruders, Threat, and Attack

- **Intruders** (**crackers**) attempt to breach security
- **Threat** is potential security violation
- **Attack** is attempt to breach security

- Attack can be accidental or malicious
- Easier to protect against accidental than malicious misuse

Security Violation Categories

- Security Violation ≡ Security Policy Violation
- Breach of confidentiality (which implies there is a confidentiality policy)
  - Unauthorized reading of data
- Breach of integrity
  - Unauthorized modification of data
- Breach of availability
  - Unauthorized destruction of data
- Theft of service
  - Unauthorized use of resources
- Denial of service (DOS)
  - Prevention of legitimate use

Security Violation Methods

- Masquerading (breach authentication)
  - Pretending to be an authorized user to escalate privileges
- Replay attack
  - As is or with message modification
- Man-in-the-middle attack
  - Intruder sits in data flow, masquerading as sender to receiver and vice versa
- Session hijacking
  - Intercept an already-established session to bypass authentication
- Privilege escalation
  - Common attack type with access beyond what a user or resource is supposed to have

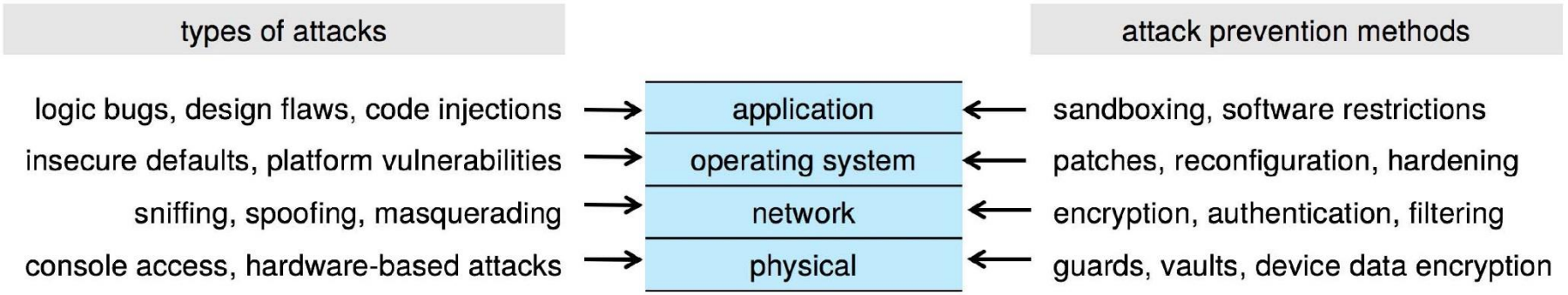
Security Measure Levels

- Impossible to have absolute security, but make cost to perpetrator sufficiently high to deter most intruders
- Security must occur at four levels to be effective:
  - Physical
    - Data centers, servers, connected terminals
  - Application
    - Benign or malicious apps can cause security problems
  - Operating System
    - Protection mechanisms, debugging
  - Network
    - Intercepted communications, interruption, DOS

Security Measures

- Security is as weak as the weakest link in the chain
- Humans a risk too via phishing and social-engineering attacks
- But can too much security be a problem?

Four-layered Model of Security



Goals of Security

- Given a security policy (specifying "secure" and "nonsecure" actions), prevent and detect attacks or recover from attacks via security mechanisms
  - Prevention
  - Detection
  - Recovery

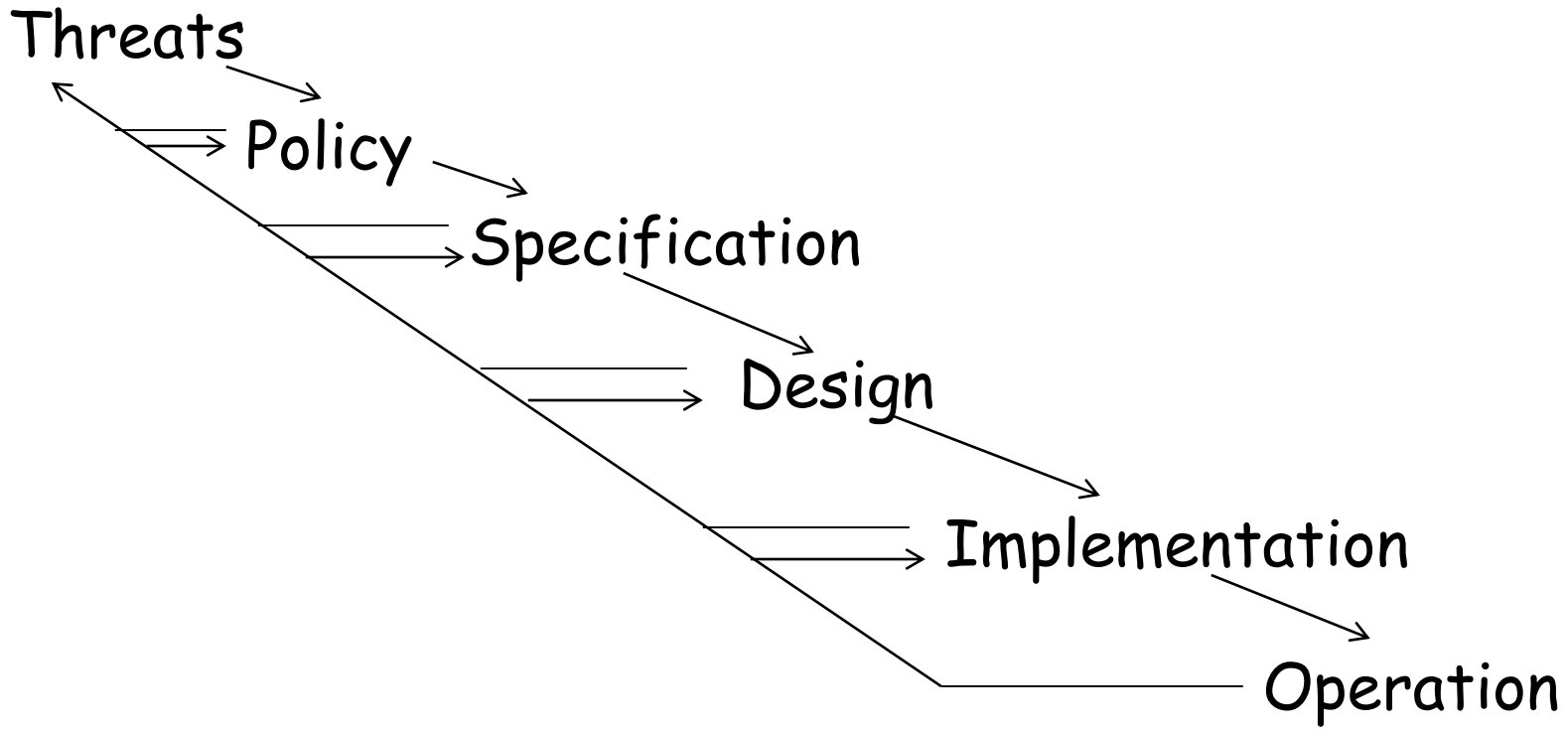
Trust and Assumptions

- Underlie *all* aspects of security
- Policies: assume or trust policies to
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms: assume or trust mechanisms to
  - Assumed to enforce policy
  - Support mechanisms work correctly
- Total security is unachievable

Assurance

- Determine "how much" to trust a system
- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

Tying Together



Operational Issues

- Cost-Benefit Analysis
  - Is it cheaper *to prevent* or *to 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*

Questions?

- Policy vs. mechanism
- Vulnerabilities,
- Intruders, threads, and attacks
- Layered model of security measures/mechanism
- The security problem and the goal of security
- Trust, assumptions, and assurance
- Operational issues and human issues