Introduction to Computer Security

ECS 153 Spring Quarter 2021

Module 1

Basic Components

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

McCumber Cube

Critical Information Characteristics

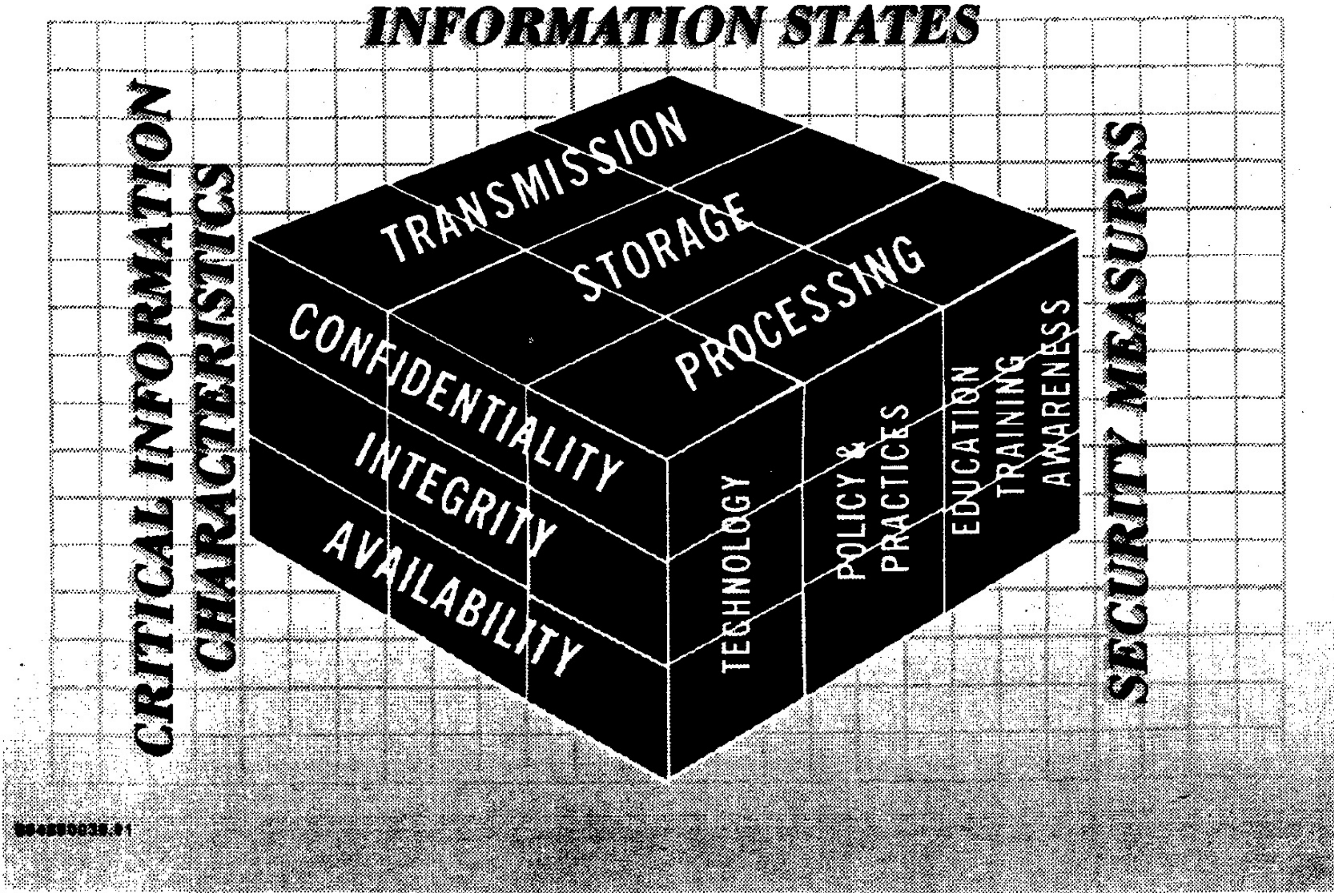
- CIA Triad

Information States

- Stages in handling information

Security Measures

- Controls for information access and handling



Picture from McCumber, John. “Information Systems Security: A Comprehensive Model”, *Proceedings 14th National Computer Security Conference* p. 328–337 (Oct. 1991), on p.334.

Information States

- Storage
  - Where data is kept
  - Examples: disks, USB memory sticks
- Transmission
  - How data moves from one place to another
  - Examples: network connections, pipes
- Processing
  - Computations using the information
  - Examples: computing statistics, drawing pictures

Security Measures

- Technology
  - Something implemented and used to ensure critical information characteristics maintained through information states
  - Example: encryption, access controls
- Policy and Practice
  - Something which says what information can be accessed, by whom, and how; a procedure to enhance security
  - Example: students may not access one another's homework files
- Education, Training, and Awareness
  - Make people understand security at level appropriate for them
  - Example: cybersecurity training UC Davis folks must take

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

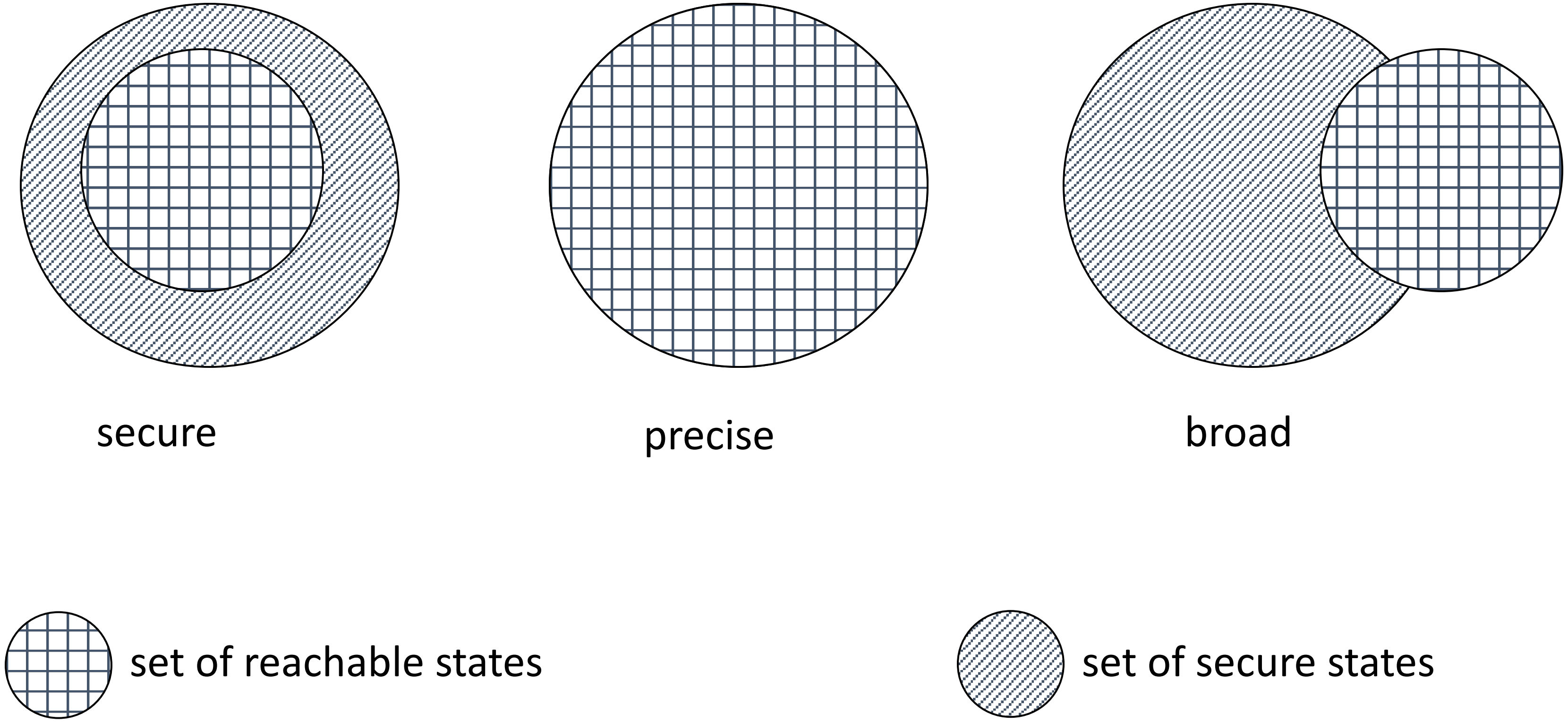
Assumptions and Trust

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

Examples

- Trustworthiness of aspirin purchased from a supermarket
    - In US, Food and Drug Administration (FDA) testing, certification
    - Manufacturing methods to ensure no contamination
    - Safety seal(s) on the bottles
- Correctness of mathematically verified kernel
    - Theorem prover proves design matches specification
    - Implementation matches design
    - Implementation correctly translated into machine code
    - Hardware runs machine code 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

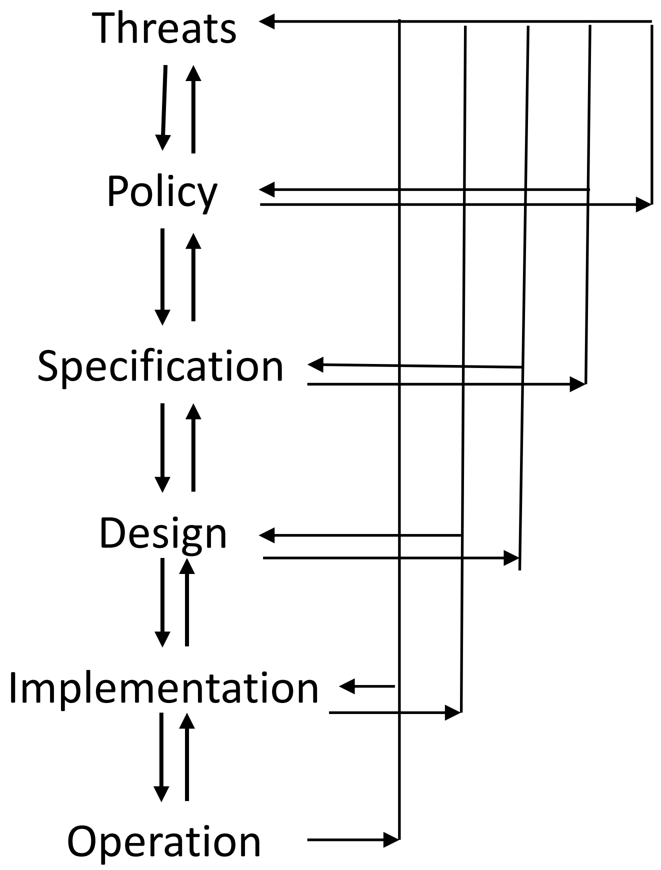
Operational Issues

- 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 It All Together



Key Points

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