

CLOUD COMPUTING

CLOUD SECURITY I

PROF. SOUMYA K. GHOSH

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

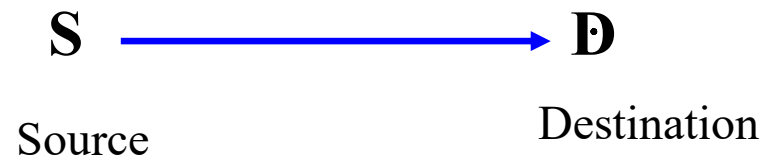
Security - Basic Components

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

Security Attacks

- ▣ Any action that compromises the security of information.
- ▣ Four types of attack:
 1. Interruption
 2. Interception
 3. Modification
 4. Fabrication

- ▣ Basic model:



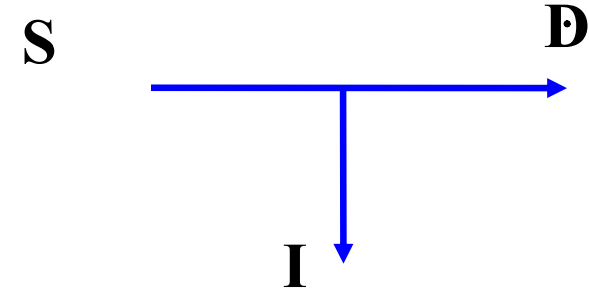
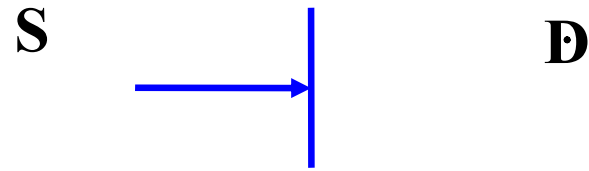
Security Attacks (contd.)

- Interruption:

- Attack on availability

- Interception:

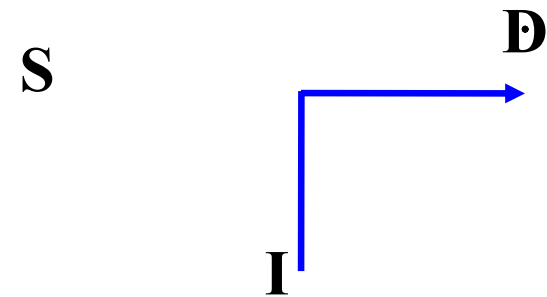
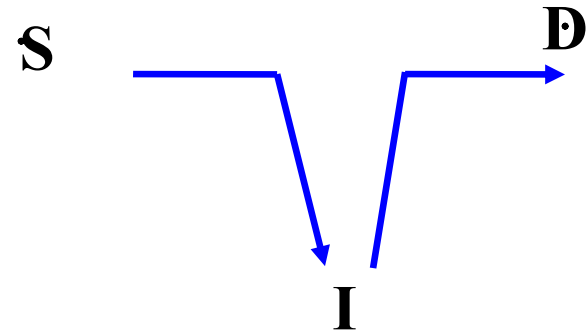
- Attack on confidentiality



Security Attacks

- Modification:
 - Attack on integrity

- Fabrication:
 - Attack on authenticity



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

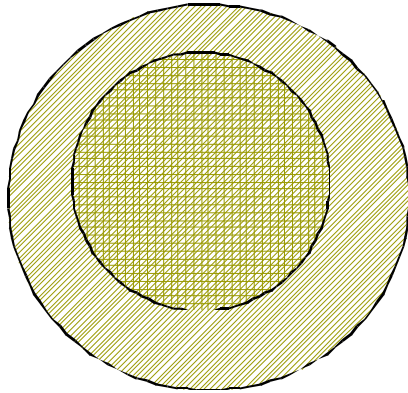
Goals of Security

- 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

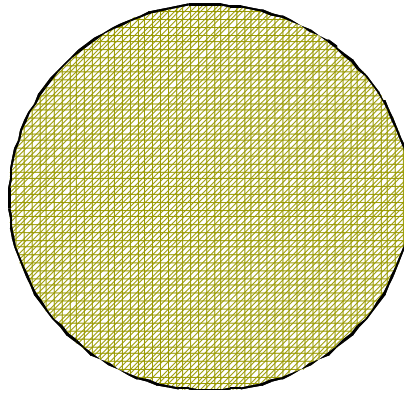
Trust and Assumptions

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

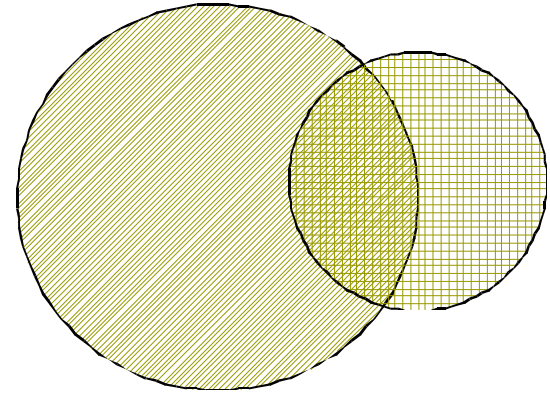
Types of Mechanisms



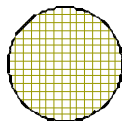
secure



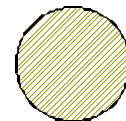
precise



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

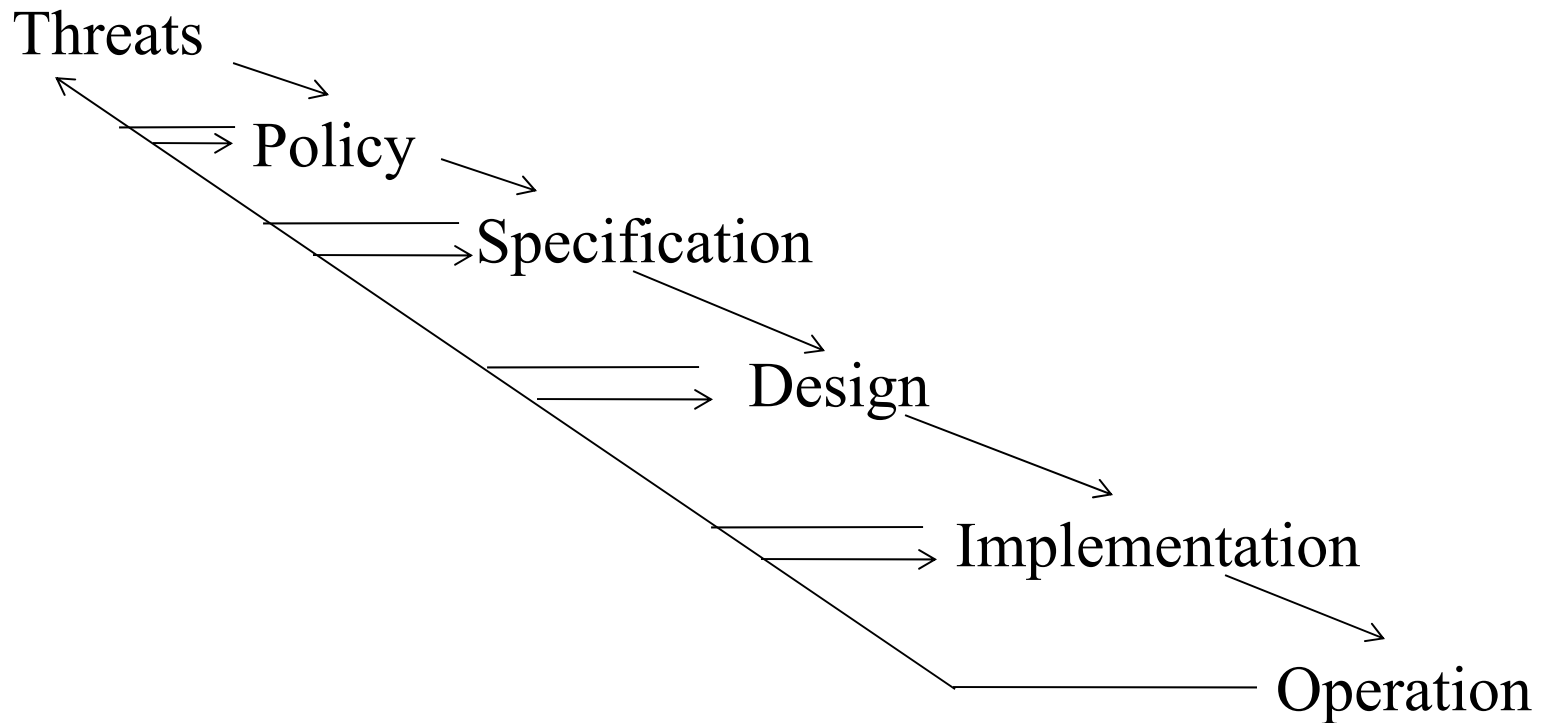
Operational Issues

- 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



Thank You!