Lecture 1

January 4, 2015

ECS 235A
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
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