Sketch of Class

• Goals
  – To learn some of the theory underlying computer and information security
  – To understand the limits of security

• What we will cover (roughly)
  – Foundations: computability of security
  – Policy models: various types, composition
  – Information flow (and not flow!)
  – A bit of malicious logic
Basic Components

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

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
Assurance

- Requirements analysis
- Specification
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design
- Deployment, maintenance, operation, retirement
  - Policies and procedures

Human Issues

- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?
- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
  - Social engineering
Basics of Principles

• Simplicity
  – Less to go wrong
  – Fewer possible inconsistencies
  – Easy to understand

• Restriction
  – Minimize access
  – Inhibit communication

Least Privilege

• A subject should be given only those privileges necessary to complete its task
  – Function, not identity, controls
  – Rights added as needed, discarded after use
  – Minimal protection domain
Fail-Safe Defaults

- Default action is to deny access
- If action fails, system as secure as when action began

Economy of Mechanism

- Keep it as simple as possible
  - KISS Principle
- Simpler means less can go wrong
  - And when errors occur, they are easier to understand and fix
- Interfaces and interactions
Complete Mediation

- Check every access
- Usually done once, on first action
  - UNIX: access checked on open, not checked thereafter
- If permissions change after, may get unauthorized access

Open Design

- Security should not depend on secrecy of design or implementation
  - Popularly misunderstood to mean that source code should be public
  - “Security through obscurity”
  - Does not apply to information such as passwords or cryptographic keys
Separation of Privilege

• Require multiple conditions to grant privilege
  – Separation of duty
  – Defense in depth

Least Common Mechanism

• Mechanisms should not be shared
  – Information can flow along shared channels
  – Covert channels
• Isolation
  – Virtual machines
  – Sandboxes
Psychological Acceptability

• Security mechanisms should not add to difficulty of accessing resource
  – Hide complexity introduced by security mechanisms
  – Ease of installation, configuration, use
  – Human factors critical here

Key Points

• Principles of secure design underlie all security-related mechanisms
• Require:
  – Good understanding of goal of mechanism and environment in which it is to be used
  – Careful analysis and design
  – Careful implementation