

Spring 2010: CS419

Computer Security

Vinod Ganapathy

Lecture 1

Material: Textbook Chapter 1 + Handout

Course Administration

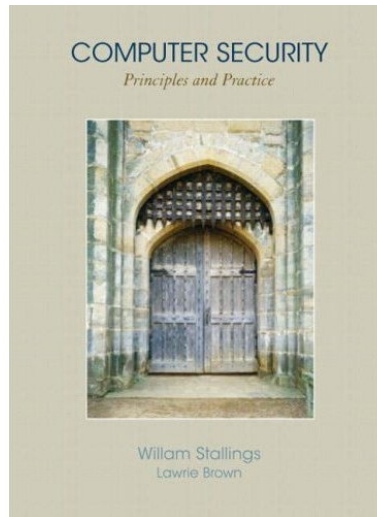
- Class hours: TF 12:00pm-1:20pm.
- Office hours: Thu, 5:00pm-6:00pm.
- TA: Nishat Islam.
- Contacting us outside office hours:
Send email with [cs419] in the subject line

Course Administration

- Class webpage:
www.cs.rutgers.edu/~vinodg/teaching/419/
- Announcements will be posted to webpage:
 - Keeping track of the webpage is **your** responsibility
- We will use Sakai to distribute handouts, manage homeworks, etc.
 - Send me email if you are not on the Sakai page for this course.

Required Textbook

- Computer Security: Stallings and Brown.



Grading

- Homeworks (4) – 30%
 - Requires coding in **C** and **x86** assembly
 - Must be done individually.
- Midterm – 20%
- Project – 20%
 - Groups of size 2 or 3.
 - Implementation of an e-voting protocol.
 - Demos + Report.
- Final exam (cumulative) – 30%

Warnings

- Do NOT ignore these warnings!
- If you do not have good programming skills or cannot work hard consistently on these assignments, don't take this course.
- Cheating will be punished severely.
- We will cover a lot of material: expect to invest a **lot** of work in this course.

Grading

- All homeworks must be submitted via Sakai:
 - For written homeworks, solutions must be neatly typed and submitted in PDF format.
- Assignment hand-ins **MUST be on time**
 - **Late hand-ins will not be accepted**
 - Instructions will be posted on the web
 - We will promptly close the turn-in at the appointed time

Final Note About Grading

- Things that I will **not** do at the end of the course:
 - Give you an incomplete because you think that your grade was bad
 - Give you extra work so that you can try to improve your grade
 - Bump your grade up because you feel you deserve it
 - Give you an F if your grade should actually be a D
 - Review earlier assignments or exams to try to find extra points for you
- Unless there is a grading error, do not come asking for extra points

Special Permissions

Requests must be accompanied by transcript and photo ID. Please write your email address, Rutgers ID, and section you want to join on your transcript

The course is full, so special permission numbers will be granted sparingly.

Cheating, turn-in, and special permission policies will be enforced strictly. There will be no if, but, ... whatever

Topics to be covered

- Cryptography basics:
 - Symmetric and Public key cryptography
- Network security
 - Key exchange protocols, IPSec, SSL.
- System security
 - Memory errors and exploits, authentication, authorization, virtual machines.

Topics to be covered

- Web security
 - Threat landscape: XSS, SQL Injection, XSRF, JavaScript and Browser security.
- Software security
 - Techniques to find vulnerabilities, secure coding practices
- Other topics
 - Anonymity, Information flow.

Introduction

- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Assurance
- Operational Issues
- Human Issues

Basic Components

- Confidentiality
 - Keeping data and resources hidden
- Integrity
 - Data integrity (integrity)
 - Origin integrity (authentication)
- Availability
 - Enabling 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
- Example from operating systems
- Composition of policies
 - If policies conflict, discrepancies may create security vulnerabilities

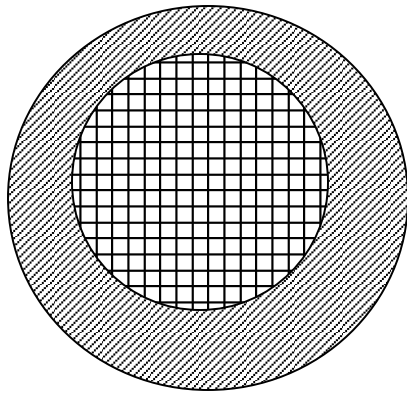
Goals of Security

- 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

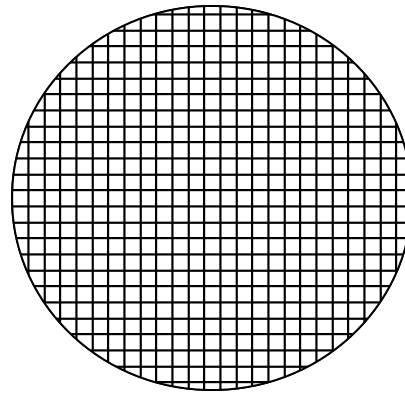
Trust and Assumptions

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

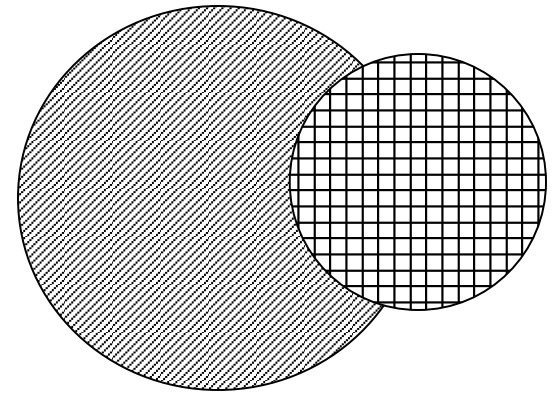
Types of Mechanisms



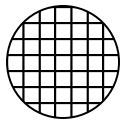
secure



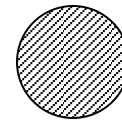
precise



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

Key Points

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

Security Design Principles

- See Lecture 1 Handout.
- Principles
 - Least Privilege
 - Fail-Safe Defaults
 - Economy of Mechanism
 - Complete Mediation
 - Open Design
 - Separation of Privilege
 - Least Common Mechanism
 - Psychological Acceptability

Overview

- **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
- Blacklists versus Whitelists

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

Next class

- Cryptography:
 - Introduction to cryptography
 - Simple symmetric key ciphers