Test Conditions

- Closed book, closed notes, no calculator, no laptop — just brains
- 75 minutes

Form

- 8 questions
- I'm not asking you to write programs or even pseudo-code
- Three types of questions
  - Explanations of certain concepts, somewhat above the pure memorization level
  - Carrying out tasks based on things discussed in class
  - Design questions (i.e., ones intended to make you think)

Material

- If it's in my slides or I said it in class, you're responsible for it
- There will be some material based more on the readings, but that's not the focus
- You're responsible for the assigned readings at about the level of class coverage. Thus, since I've talked about very few equations, you don't really need to know any equations or proofs from the reading

Example

What's important about RSA is (a) it's based on the difficulty of factoring large numbers; (b) primality testing of large numbers is relatively easy; (c) the public and private keys are, in a mathematical sense, interchangeable. I'm not asking you to know that

$$ed \equiv 1 \pmod{()p-1)(q-1)}$$

or how to calculate e given d, p, and q — but that the calculation is feasible is important, because it means that RSA is usable.

It's probably not worth your while to ask me if such-and-such is on the exam

So What's Important?

- Everything. . .

More Seriously

- I can’t quiz you on everything I’ve covered in a dozen lectures
- I can’t review 15 hours of class time today
- I’m to some extent limited by the kinds of things it’s feasible to ask on an exam

Introduction

- What is security?
- What are the different attributes?
- How do they interact?
- Who is the enemy?

Access Control

- The role of hardware
- Historical mechanisms
- Multics; multi-ring protection
- Principle of Least Privilege
- The need for assurance

Operating Systems

- The role of the OS
- Authentication
- Identity versus attribute access control
- File permissions
- *Especially* Unix file permissions
- Forms of access control
- Database access control

Complex Access Control

- Complex access control mechanisms
- Role-based access control
- Mandatory access control — levels and categories
- Determining access rights in a lattice
- Using MAC for read and write permission
- Object security versus information flow security

Privileges

- Kinds of privileges
- Mapping privilege to operating system primitives
- Acquiring privileges
- SetUID, and its strengths and weaknesses
- Combining access controls and SetUID
- Message-passing, and its strengths and weaknesses

Authentication

- What is identification, authentication, authorization?
- Types of authentication
- Passwords and their weaknesses
- How to store passwords
- Tokens, and their strengths and weaknesses
- Two-factor authentication
- Cryptography and authentication

Biometrics

- Types of biometrics, and their properties
- Advantages and disadvantages of biometrics
- Systems issues with biometrics
- Biometrics and cryptography

Certificates

- What is a certificate?
- What is a certificate authority?
- Identity versus authorization certificate
- Revocation
- Systems issues
- Usage scenarios for different authentication schemes

Cryptography and Cryptographic Engineering

- Properties of good cryptosystems
- Kerckhoff's Law
- Keys
- Types of ciphers and their properties
- Brute force attacks
- Cryptographic modes of operation and their properties
- File system encryption

Public Key Cryptography; Hash Functions

- What is public key crypto? What is it good for?
- Key-handling
- Hybrid public/symmetric crypto
- Digital signatures
- Digital versus physical signatures
- Cryptographic hash functions
- Properties of such functions

Key Management; Random Numbers

- What is a cryptographic protocol?
- What are the risks and benefits of symmetric versus public key cryptographic protocols?
- Protecting keys
- Cryptographic hardware
- Random numbers
- Hardware versus software random number generators
- Properties and risks of each
- Seeds for software random number generators

Secure Programming

- Bugs as a security issue
- Buffer overflows and (roughly) how they work
- Defending against buffer overflow attacks
- The role of specifications
- Format string attacks
- Input validation
- Filtering

More Secure Programming

- Macro injection attacks
- Program environment
- Inherited attributes
- Filename parsing
- Unicode
- File access by setUID programs
- Race conditions

Protecting the Client

- Risks to clients
- Email and the web
- Smart cards
- Attacking smart cards
- Understanding the enemy's goal
- Stored value versus database pointer

DRM

- Approaches to DRM
- Policies
- Implementing DRM in the OS
- Attacking DRM
- Trusted hardware and tamper-resistance
- Watermarking