The Exam

The Exam

- 1:10-4:00, Thursday, Dec 21, 535 Mudd
- Same style of questions as the midterm
- I'm not asking you to write programs
- Approximately 12 questions (2.27× the time; 1.7× the number of questions)
- Roughly 1/3 from the first half, 2/3 from the second half (or combined)

Material

- If it's in my slides or I said it in class, you're responsible for it
- There may be some questions based on the readings
- You're responsible for the assigned readings at about the level of class coverage.

Limits

The Exam
The Exam
Material
Limits
Test Conditions
Introduction
Cryptography
Web Security
IPsec
Applications
Firewalls
Scanning and Intrusion Detection
Worms and Denial of Service

- I can't quiz you on everything I've covered during the semester
- I can't review 30+ hours of class time today
- I'm to some extent limited by the kinds of things it's feasible to ask on an exam

Test Conditions

- Open book
- Open notes
- You can bring a calculator but save your energy; you won't need it
- No laptops or phones. . .

Introduction

Terminology

- Confidentiality, integrity, availability
- Privacy
- Threats, attacks, and vulnerabilities

Kinds of Threats

- Joy hackers
- Criminals
- Competitors
- Nation states
- Insiders

Assets

- Protect what?
- Bandwidth, CPU, data, identity
- Attacker powers?

Cryptography

Ciphers

- What is a cryptosystem?
- What is a block cipher? What are generic properties of block ciphers?
- What are the different modes of operation? What are their properties? When would you use each mode?
- What is a stream cipher?

Public Key Cryptography

- What is it? What is it good for? Limitations?
- How are public key systems used?
- Random numbers and where they come from
- Digital signatures

Hash Functions

- What are cryptographic hash functions?
- What are their essential properties?
- Birthday paradox

Message Integrity

- MACs
- CBC MAC
- HMAC

Authentication

- Passwords and their limitations
- Tokens
- Connection hijacking

Certificates

- Trust properties
- CAs
- Authorization versus identity certificates
- Web of trust
- Types of certificates
- Revocation

Key Management

- Purpose
- KDCs; Needham-Schroeder
- Man-in-the-middle attacks
- Other protocols

Kerberos

- Goals
- How it works
- Tickets and ticket-granting tickets
- Authenticators
- Authorization

The Exam

Introduction

Cryptography

Web Security

SSL

Web Certificates

Browser Security

Continuing Authentication

Other Issues

Web Server Security

Email Security

PGP versus S/MIME

Phishing

Defenses

IPsec

Applications

Firewalls

Scanning and Intrusion Detection

Worms and Denial of Service

Web Security

SSL

- What is SSL?
- Client authentication types
- Properties and requirements
- Uses
- Trust model

Web Certificates

- Root certificates
- The browser vendor's role
- Bindings
- Human factors

Browser Security

- Why is it a problem?
- Active content
- Javascript
- ActiveX

Continuing Authentication

- Cookies
- Embedded values
- Cryptographically sealing data

Other Issues

- Cross-site scripting
- Sanitizing input

Web Server Security

- Why?
- Trust model
- Scripts and their dangers
- Injection attacks
- Permissions

Email Security

- Usual evaluation
- How to sign and encrypt?
- Details
- Threats: eavesdropping, password theft, spool file

PGP versus S/MIME

- Hierarchical versus web of trust
- Finding keys

Phishing

- What is it?
- How it’s done
- Tracing

Defenses

- Mutual authentication
- Personalization
- DKIM
- Non-reusable credentials
- (MITM attacks; human factors)

IPsec

IPsec

- What is IPsec, and why?
- ESP and AH
- SPI
- SAs
- Tunnel and transport mode

Packet Processing

- Outbound and inbound
- SPD and SADB
- Rule characteristics

IPsec Key Management

- Static keys or dynamically-negotiated keys
- Replay protection

IKE

- General properties
- SAs, selectors
- Rekeying
- Control messsages
- Denial of service and defenses

Attacking IPsec

- Cut-and-paste attacks
- Probable plaintext
- Interactions with other layers

Applications

Applications

- SSH
- SIP
- Networked storage

SSH

- Features
- Security model
- Client authentication
- Connection-forwarding
- SSH Agent

SIP

- SIP architecture
- What's at risk?
- Protecting voice versus signaling
- What type of crypto is used where
- Complex scenarios

Networked Storage

- Networked file system vs. networked disk
- NFS, RPC, and rpcbind
- Randomness
- CIFS
- Authentication
- iSCSI and FCIP
- Using crypto

Firewalls

Firewalls

- Why?
- Positioning firewalls
- Types of firewalls (packet filter, stateful packet filter, application, circuit)
- Limits of firewalls

Application Firewalls

- Advantages
- Tuning for high-layer threats
- DNS, DNSsec
- Special proxies

Scanning and Intrusion Detection

Scanning

- Tools
- Purpose
- Nmap's many options
- Fingerprinting

What is IDS?

- Purpose
- Host versus network IDS
- Logs and traces

Limits of Network IDS

- Insertion and evasion attack
- Checksum errors
- TTLs
- TCP normalization

IDS Architecture

- Detector
- Database
- Analyzer
- Countermeasure
- Signature versus anomaly

Worms and Denial of Service

Worms

- Worms versus viruses
- Spread: program versus social engineering
- Payloads
- Spam
- Detection

Denial of Service

- Types of DOS attack
- TCP attacks
- DDoS
- Defenses

Routing Attacks

- Why they happen
- Goals
- SBGP, SO-BGP

Wireless Security

- Evil twin
- Battery lifetime
- WEP — why the crypto is bad
- War-driving
- Access control

Privacy

- What is privacy?
- Traffic analysis
- Authentication issues
- Secondary uses
- Mixnets