Final Exam Review

CS461/ECE422 Fall 2010

Exam guidelines

- A single page of supplementary notes is allowed
- Closed book
- No calculator
- Students should show work on the exam. They can use supplementary sheets of paper if they run out of room.
- Students can use scratch paper if desired.

Topic Distribution

- The final is cumulative
  - Material from the first two exams
  - Plus material from after Thanksgiving
- Follows same structure as midterm exams
  - But longer
  - Aiming for 1.5-2 hours

Exam Logistics

- 8am Thursday, December 16
  - 1320 DCL
- Conflict exam as needed

Course Goals

- Introduction to computer security information
  - Basis for deeper study
  - Ability to interpret security articles/information more critically
  - Improve your security awareness as a computer professional
  - Some fun party tricks

Topics First Half

- Introductory definitions
- Security Policies
- Risk Analysis
- Historical Cryptography
- Symmetric Cryptography
- Public or Asymmetric Cryptography
- Authentication
- Key Management

Topics Second Half

Access Control

  - Access Control Matrix
  - Discretionary OS models
  - Database Access Control
  - Mandatory Models

- Assured Systems
  - Design and development
  - Evaluation
- Malware
- Network Security Controls and Architecture

Topics Third Portion

- Security and Law
- Physical Security
  - Forensics
- EMSEC
- SSL and IPSec

Law and Security

- Different laws apply for service providers, law enforcement, intelligence, war fighter
- Privacy
  - 4th amendment
  - Wiretapping and ECPA
  - CALEA
  - FISA

Law and Security

- Crime
  - CFAA
  - Economic Espionage Act
  - International laws
    - Cryptography and the law
- Computer Use and Configuration
  - FISMA
  - SOX
  - GLB
  - HIPAA

Physical Security

- Must consider physical world in security planning
- Forensics/Spying
  - Chain of custody
  - Finding data on disk
  - Paper disposal

EMSEC

- Emanations Scanning
  - TEMPEST
- Use AM radio to detect screen radiation
- Hide information in dither
- Tempest fonts
- Protections
  - Shielding
  - Physical separation. red/back
- RFID

SSL and IPSec

- Examples of crypto techniques and protocols used in the real world
- SSL – transport layer
  - Session vs connections
  - Handshake protocol
    - Authenticate and agree upon common data
    - Compression, encryption, and integrity
- IPSec – network layer
  - Tunnel and transport mode
  - AH/ESP
  - Nested tunnels
  - Encryption and integrity

Thanks for participating!
Good Luck!