# Final Exam Review

CS461/ECE422 Fall 2009

# 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 Friday, December 18
  - Last name begins with A-O:
    - 1310 DCL
  - Last name begins with P-Z:
    - 138 Henry Administration Building (HAB)
- 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

- Database Access Control
- Trusted OS
  - Policies and Models
  - Features and design
- Assured Systems
  - Design and development
  - Evaluation
- Malware
- Network Security Controls and Architecture
- Security and Law

# Topics Third Portion

- IPSEC and SSL
- Physical Security
  - Forensics
- EMSEC
- Wireless
  - WEP as a case study
  - WPA

# 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

# Physical Security

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

# EMSEC

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

# WEP Case Study

- Good Crypto put together badly
  - RC4 stream cipher
    - Must restart key stream with each packet
    - Not avoiding known bad keys
  - CRC used for message integrity
  - No provision for automatic rekeying
- Corrected in two phases in WPA and WPA2
  - New chopchop attack against TKIP

# Thanks for participating!
# Good Luck!