

Final Exam Review

CS461/ECE422 Fall 2007

Exam guidelines

- A single page of supplementary notes is allowed
- Closed book
- A calculator is allowed.
- 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
- Roughly half of the points will be on the last third of the course
- Follows same structure as midterm exams
 - But longer

Exam Logistics

- 8am Wednesday, December 12
 - Last name end in A-K:
 - 32 Psychology
 - <http://webtools.uiuc.edu/ricker/CampusMap?target=search>
 - Last name end in L-Z:
 - 245 Wohler
 - <http://webtools.uiuc.edu/ricker/CampusMap?target=search>
- Conflict exam 8am Thursday, December 13
 - 4124 Siebel
 - Must contact me first to get cleared for the conflict

Security in the News

- 12/6/07 - Dumpster Diving for Bundesbank safe plans
 - <http://uk.reuters.com/article/lifestyleMolt/idUKL061021542007>
- Bot generated Ron Paul Spam
 - <http://arstechnica.com/news.ars/post/20071031-ron-paul-carr>
- 12/5/07 - SAFE Act rushed through congress
 - Increases reporting requirements on operators of open WIFI nets.
 - http://www.news.com/8301-13578_3-9829759-38.html
- 11/7/07 – Peruvian Cyber-guerillas attack Chile
 - <http://ww4report.com/node/4655>
- 11/22/07 – British Government Loses personal info for 20Million
 - <http://www.latimes.com/news/printedition/front/la-fg-privacy22>

Topics First Third

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

Topics Second Third

- Memory protection
- Discretionary access controls
- Authentication
- Trusted OS Policies and Models
- Trusted OS Features and design
- Evaluation
- Malware and commonly exploited program errors
- Secure development techniques

Topics Third Third

- Network Security
 - Overview
 - Threats
 - Architecture and Controls
- Security and Law
- Database
 - Access Control
 - Integrity
 - SQL injection
- Physical Security
- WEP case study

Networks Layers and Vulnerabilities

- L1/2 Physical/data link
 - Sniffing
 - Switches
- L3 Network - IP
 - Routing
 - Arp
- L4 Transport - TCP/UDP
 - Port scanning
 - Syn Flood
 - Session hijack
- L7 Application – HTTP, H.323, FTP, SMTP
 - DNS cache poisoning and open relay

Network Architecture

- Segmentation
- Security Domains or Perimeters
- Virtual Private Networks
- Firewalls
 - Application Proxy, Packet Firewall, Stateful Firewall
 - Address translation
 - Classic Attack prevention
- Intrusion Detection
 - Signature or anomaly/statistical
 - Inline or out-of-band deployments

Security and Law

- Recognize laws and have a basic knowledge of their intent
- Intellectual property laws
 - Patent, Copyright, DMCA, trade secret
- Search laws and crime
 - 4th amendment, US PATRIOT act, ECPA, CALEA, FISA
- Computer Crime
 - CFAA, Economic Espionage Act
- Laws and regulations covering computer configuration
 - FISMA, SOX, GLBA, HIPAA

Database Security

- Inherent integrity
 - Transactions and two phase commit
- Basic Access Control Model
 - Views and Grant
- Advanced policy based access control model
 - Virtual Private Database
- Inferring sensitive data
- SQL injection attacks
 - First order and second order

Physical Security

- Must consider physical world in security planning
- Disaster Business Continuity
 - Recovery time: cold/warm/hot site
 - Test or exercise plan
- Forensics/Spying
 - Chain of custody
 - Finding data on disk
 - Paper disposal
 - Output device
 - Phone

EMSEC

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

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

Thanks for participating!
Good Luck!

