

Dave Latham
CS162 Fall 203
Midterm Review III Topics

Note: The midterm exam will be cumulative, but the review is not. Be prepared for questions on any material from the course.

1. I/O Devices

- a. Know general performance characteristics where (ballpark figures)
 - i. Data transfer rate
 - ii. Storage capacity
 - iii. Storage density
 - iv. Response Time
 - v. Reliability (Error rate / MTBF)
 - vi. Physical Size
- b. Have some idea of how the I/O is physically done
- c. When/why was it used?
- d. What is a...
 - i. Terminal
 - ii. Line Printer
 - iii. Raster Printer
 - iv. CRT Display
 - v. Liquid Crystal Display
 - vi. Reel to Reel Tape
 - vii. DAT Tape
 - viii. Other possible tape formats
 - ix. Floppy Disk
 - x. Hard Disk
 - xi. CD
 - xii. DVD

2. Networks and Communication

- a. What's a LAN? What's a WAN?
- b. What is latency?
 - i. Transmission versus Set-up
- c. What is bandwidth?
- d. Protocols
 - i. What are the seven ISO layers?
 - ii. What are actual examples of them?
- e. Topology
 - i. Broadcast versus ring
 - ii. Examples?
 1. Ethernet
 2. Token Ring
- f. What's the difference between circuit switching, packet switching, and "message" switching?
- g. Understand possible problems

- i. Dropped packets
 - ii. Network congestion
 - h. What are the following protocols?
 - i. IP
 - ii. TCP
 - iii. UDP
 - iv. SMTP
 - v. DNS
 - vi. FTP
 - i. What is a distributed file system?
- 3. Protection and Security
 - a. What is the goal of protection?
 - i. Why not just lock your computer in a room, unplugged?
 - b. Know and understand the motivation for these design principles of a good protection system
 - i. Economy of mechanism (KISS)
 - ii. Fail safe defaults
 - iii. Complete mediation
 - iv. Open design
 - v. Separation of privilege
 - vi. Least privilege
 - vii. Least common mechanism
 - viii. Psychological acceptability
 - c. What are the three aspects to a protection mechanism?
 - i. Authentication
 - 1. Passwords
 - a. Paradox – should they be long or short?
 - b. Salt
 - ii. Authorization determination
 - 1. Access lists versus capabilities
 - iii. Access enforcement
 - d. What are some common weaknesses?
 - i. Abuse of valid privileges
 - ii. Imposter or Trojan Horse
 - iii. Listener / Eavesdropping
 - iv. Spoiler
 - v. Trap doors
 - e. What are some countermeasures?
 - i. Logging
 - ii. Minimum privilege
 - iii. Correctness proofs
 - iv. Callbacks
 - v. Consistency / Plausibility Checks
 - 4. Encryption
 - a. What is the goal of encryption?
 - b. What is the sequence of steps involved?

- c. How do the following work?
 - i. Substitution
 - ii. Transposition
 - iii. Polyalphabetic Cipher
 - iv. Running Key Cipher
 - 1. One-time Pads / Perfect Encryption
 - v. Codes
 - vi. Public Key Cryptography
 - 1. Digital signatures
 - d. What are challenges of implementation in practice?
 - i. Key distribution
 - ii. True randomness
 - e. What are examples of crypto systems in use?
 - i. DES
 - ii. RSA
 - iii. PGP
 - iv. AES
 - v. Clipper Chip
5. Virtual Machines
- a. What is a virtual machine?
 - b. How is it different from an emulator?
 - c. How is it different from an OS?
 - d. What are they used for?
 - e. How does a virtual machine manage virtual memory?
 - f. How can a virtual machine manage other resources? (Disk? Network?)
 - g. How good is the performance?
6. Performance Evaluation
- a. Important to consider in initial design
 - b. Measurement
 - i. How can we do measurement?
 - ii. Hardware versus software
 - 1. Pros vs. Cons
 - c. What is workload characterization and why is it important?
 - d. What is analytic modeling?
 - i. Examples?
 - 1. Queuing networks
 - 2. Stochastic processes
 - e. Pros/cons of Simulation