

Study Guide for Final

This is simply a guide of topics that I consider fair game for the final. I don't promise to ask you about them all, or about any of these in particular; but I may very well ask you about any of these.

1. Anything from the *Study Guide for Midterm*
2. Integrity models
 - a. Biba
 - b. Clark-Wilson
3. Cryptography
 - a. Types of attacks: ciphertext only, known plaintext, chosen plaintext
 - b. Caesar cipher, Vigenère cipher, one-time pad, DES
 - c. Public key cryptosystems; RSA
 - d. Confidentiality and authentication with secret key and public key systems
4. Key Distribution Protocols
 - a. Kerberos and Needham-Schroeder
 - b. Certificates and public key infrastructure
5. Passwords (selection, storage, attacks, aging)
 - a. One-way hash functions (cryptographic hash functions)
 - b. UNIX password scheme, what the salt is and its role
 - c. Password selection, aging
 - d. Challenge-response schemes
 - e. Attacking authentication systems: guessing passwords, spoofing system, countermeasures
6. Identity
 - a. UNIX real, effective, saved, audit UIDs
 - b. Host names and addresses
 - c. Cookies and state
 - d. Anonymous remailers
7. Access Control
 - a. Multiple levels of privilege
 - b. UNIX protection scheme
 - c. MULTICS ring protection scheme
 - d. ACLs, capabilities, lock-and-key
8. Computerized Vermin
 - a. Trojan horse, computer virus
 - b. Computer worm
 - c. Bacteria, logic bomb