Final Study Guide

This is simply a guide of topics that I consider important 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, as well as anything we discussed in class, in the discussion section, or that is in the textbook or readings.

1. Anything from before the midterm
2. Integrity models
   (a) Biba's model
   (b) Clark-Wilson model
   (c) Trust models
3. Hybrid models
   (a) Chinese wall (Brewer-Nash) model
   (b) Originator-controlled access control (ORCON)
   (c) Rile-based access control (RBAC)
4. Cryptography
   (a) Types of attacks: ciphertext only, known plaintext, chosen plaintext
   (b) Symmetric ciphers, Cæsar cipher, Vigenère cipher, one-time pad, AES
   (c) Public key cryptosystems; RSA
   (d) Confidentiality and authentication with secret key and public key systems
   (e) Cryptographic hash functions
   (f) Digital signatures
5. Key Distribution Protocols
   (a) Kerberos and Needham-Schroeder
   (b) Certificates and public key infrastructure
   (c) Key generation
6. Network Security
   (a) Link encryption, end-to-end encryption
   (b) Firewalls
   (c) DMZs
   (d) TLS, SSL
7. Authentication
   (a) Passwords (selection, storage, attacks, aging)
   (b) One-way hash functions (cryptographic hash functions)
   (c) UNIX password scheme, what the salt is and its role
   (d) Password selection, aging
   (e) Challenge-response schemes
   (f) Biometrics and other validation techniques
8. Access Control
   (a) ACLs, C-Lists, lock-and-key
   (b) UNIX protection scheme

(c) Multiple levels of privilege

(d) Lock and key

(e) MULTICS ring protection scheme

9. Malware

(a) Trojan horse, replicating Trojan horse

(b) Computer virus

(c) Computer worm

(d) Bacteria, logic bomb

(e) Keystroke logger

(f) Ransomware

(g) Botnets

(h) Countermeasures

10. Intrusion detection