Midterm Study Guide

This is simply a guide of topics that I consider important for the midterm. 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 readings (including the papers).

1. Fundamentals
   a. What is security?
   b. Basics of risk analysis
   c. Relationship of security policy to security
   d. Policy vs. mechanism
   e. Assurance and security
2. Saltzer's and Schroeder's principles of secure design
3. Robust programming
4. Access control matrix
   a. Matrix
   b. Primitive operations
   c. Commands
   d. Harrison-Ruzzo-Ullman result (undecidability of safety)
5. Policies
   a. Mandatory access control (MAC)
   b. Discretionary access control (DAC)
   c. Originator-controlled access control (ORCON)
   d. Role-based access control (RBAC)
   e. Policy languages
6. Confidentiality Models
   a. Bell-LaPadula Model
   b. Lattices and the BLP Model
   c. Tranquility
7. Integrity Models
   a. Biba Model
   b. Clark-Wilson model
8. Cryptography
   a. Types of attacks: ciphertext only, known plaintext, chosen plaintext
   b. Classical 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
9. Key Distribution Protocols
   a. Kerberos and Needham-Schroeder
   b. Certificates and public key infrastructure
   c. Key generation
10. Network protocols
    a. Link encryption, end-to-end encryption
    b. PGP, PEM: privacy enhancing e-mail
11. Intrusion detection
    a. Architecture of an IDS
    b. Anomaly-based, signature-based, specification-based IDSes

c. Host-based, network-based, distributed IDSes