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.

1. What is security?
   a. Confidentiality
   b. Integrity
   c. Availability
2. Security policy and security mechanisms
3. Laws and customs
4. Assurance
   a. What it is
   b. Trust, assumptions, assurance
5. Principles of secure design
6. Malware
   a. Trojan horses
   b. Computer viruses
   c. Computer worms
   d. Rabbits, bacteria, logic bombs
7. Attacks
   a. E-mail security
   b. Tracking people over the web
   c. Cookies and how they work
   d. Social engineering
8. Cryptography
   a. Classical cryptosystems
   b. Public-key cryptosystems
   c. Cryptographic checksums
   d. Digital signatures
   e. Types of attacks on ciphers
9. Authentication
   a. Attributes that identify you
   b. Passwords
   c. Challenge-response
   d. Biometrics
   e. Multi-factor authentication
10. Identity
    a. User identity
    b. Host identity
    c. Web identity
    d. Certificates and cryptographic key infrastructure
11. Email and privacy
    a. How to do secrecy, integrity, authentication
    b. Remailers (cypherpunk type 1, mixmaster)
12. Firewalls