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. Access Control Mechanisms
   a. Access control matrix
   b. Access control lists
   c. Capabilities and capability lists
   d. Multics ring-based mechanisms
2. Firewalls
   a. What they are
   b. Proxy (application layer) vs. filtering (network layer)
   c. Filtering and redirection
   d. How they are used
3. Applications
   a. Electronic voting
   b. Electronic recordation of real estate
4. Malicious logic
   a. Trojan horses, computer viruses, computer worms, bacteria (rabbits), logic bombs
   b. Different types of viruses: boot sector infectors, executable infectors, multipartite, TSR, stealth, encrypted, polymorphic, and macro
   c. Theory: can't write a program to detect all computer viruses without error
   d. Practice: type checking, sandboxing, limiting sharing, integrity checking, etc.
5. Safety on the web
   a. WWW: applets, images, filtering content, CGI and server-side problems, redirection, naming
   b. Email: attachments, spam, anti-spam technologies, phishing
6. Assurance
   a. Trust, assurance, requirements, and the software life cycle
   b. Evaluation of assurance: Orange Book, Common Criteria, and best practices
7. Intrusion Detection
   a. Anomaly detection
   b. Misuse detection
   c. Specification detection
   d. Host-based vs. network-based IDS
8. Any of the handouts
9. Anything on the *Study Guide for Midterm*