Midterm Study Guide

This is simply a guide of topics that we consider important for the midterm. We don't promise to ask you about them all, or about any of these in particular; but we may very well ask you about any of these, as well as anything we discussed in class, in the discussion section.

1. What is security?
   a. Confidentiality
   b. Integrity
   c. Availability
   d. What does it do?
2. Security policy and security mechanisms
3. Assurance
   a. What it is
   b. Trust, assumptions, assurance
   c. Assurance in policy, design, implementation, operation
4. Threats and Defenses
   a. On the Internet
   b. Consequences
   c. Defenses
   d. Costs
5. Malware and defenses
   a. Trojan horses
   b. Computer viruses
   c. Computer worms
   d. Rabbits, bacteria, logic bombs
6. Vulnerabilities
   a. Role of assumptions
   b. Types of vulnerabilities
7. "Secure" systems and programs
   a. Basic requirements
   b. What does the program depend on?
   c. Does the program do what you expect?
   d. What happens if you give it strange input?
   e. Does it interact with other programs?
   f. What does it do if something "impossible" happens?
   g. Tools for analysis
8. Detecting and blocking atacks
   a. Access controls
   b. Intrusion detection
9. Privacy and anonymity
   a. What to anonymize
   b. Remailers (cypherpunk, mixmaster)
   c. Proxies
   d. Repudiation, non-repudiation