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 readings (including the papers).

1. Anything from before the midterm
2. Elections and Electronic Voting
3. Identity
   a. Users, groups, roles
   b. Host naming, DNS
   c. Certificates
   d. Anonymity
4. 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. EKE protocol
   g. Biometrics and other validation techniques
5. 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
6. Malware
   a. Types of malware
   b. Countermeasures
7. Information flow
   a. Entropy and its relevance to information flow
   b. Static analysis
   c. Dynamic analysis
   d. Firewalls
8. Confinement problem
   a. Principle of transitive confinement
   b. Sandboxes
   c. Virtual machines