Final 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).

Please note that the final is *cumulative*.

1. Everything contained in the midterm study guide
2. Electronic voting
3. Cryptography
   a. Types of attacks: ciphertext only, known plaintext, chosen plaintext
   b. Classical ciphers, Cæsar cipher, Vigenère cipher, one-time pad, DES
   c. Public key cryptosystems; RSA
   d. Confidentiality and authentication with secret key and public key systems
   e. Cryptographic hash functions
   f. Digital signatures
4. Key Distribution Protocols
   a. Kerberos and Needham-Schroeder
   b. Certificates and public key infrastructure
5. Network protocol
   a. Link encryption, end-to-end encryption
   b. PGP, PEM: privacy enhancing e-mail
6. Passwords (selection, storage, attacks, aging)
   a. One-way hash functions (cryptographic hash functions)
   b. UNIX password scheme, what the salt is and its role
   c. Password selection, aging
   d. Challenge-response schemes
   e. Attacking authentication systems: guessing passwords, spoofing system, countermeasures
   f. Biometrics and other validation techniques
7. Anonymity
8. Access Control
   a. ACLs, C-Lists, lock-and-key
   b. UNIX protection scheme
   c. Lock and key
   d. MULTICS ring protection scheme
9. Confinement problem
   a. Principle of transitive confinement
   b. Sandboxes
   c. Virtual machines
10. Malware
    a. Types of malicious logic
    b. Countermeasures