# 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. Cryptography
   a. Public key cryptography
   b. Cryptographic checksums (one-way hashes)
   c. Digital signatures
3. Cryptographic Techniques
   a. Interchange, session keys
   b. Needham-Schroeder
   c. Key generation, random numbers
   d. Certificates and infrastructure; public key infrastructure
   e. Networks and ciphers
   f. PGP, TLS protocols
4. Network Security
   a. Firewalls
   b. DMZs
   c. Denial of service attacks, countermeasures
5. Intrusion detection
6. 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. Biometrics and other validation techniques
7. 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
8. Malware
   a. Types of malware
   b. Countermeasures