   c. File signature generation (integrity checksumming, *etc*.) and checking
   d. Safe practises ("safe hex")
   e. Type checking
8. Computerized Vermin
   a. Trojan horse
   b. Computer virus
   c. Computer worm
   d. Bacteria
   e. Logic bomb
9. Trust
10. Network Security
   a. ISO Model and security services
   b. PGP
   c. Certioficates and certificate management

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. Anything from the *Study Guide for Midterm*
2. Encryption schemes, their strengths and weaknesses
   a. Types of attacks: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext
   b. Types of ciphers: substitution, transposition, product (both substitution and transposition)
   c. Goal of ciphers; what makes a cipher theoretically unbreakable
   d. Caesar cipher, Vigenère cipher, one-time pad
   e. What the DES is, characteristics
   f. Public key cryptosystems
   g. RSA
   h. Confidentiality and authentication with secret key and public key systems
3. 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
4. Privileges
   a. UNIX real, effective, saved, audit UIDs
   b. Setuid, setgid
   c. Roles
   d. Nested program units
5. Memory Management
   a. Tagged architectures
   b. Segmentation
   c. Paging
   d. Paged segmentation
6. Access Control
   a. Multiple levels of privilege
   b. UNIX protection scheme
   c. MULTICS ring protection scheme
   d. ACLs, capabilities, lock-and-key
   e. Mandatory Access Control (MAC), Bell-LaPadula model; lattices
   f. Discretionary Access Control (DAC)
   g. Originator Controlled Access Control (ORCON)
   h. Differences between MAC, DAC, ORCON
7. Integrity Models
   a. Biba's model
   b. Clark-Wilson model