Midterm 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).

1. Fundamentals
   (a) What is security?
   (b) Basics of risk analysis
   (c) Relationship of security policy to security
   (d) Policy vs. mechanism
   (e) Assurance and security
2. Saltzer's and Schroeder's principles of secure design
3. Robust programming
4. Penetration studies
   (a) Flaw hypothesis methodology
   (b) Scoping the system
5. Vulnerabilities models
   (a) RISOS model
   (b) PA model
   (c) NRL model
   (d) Aslam's model
   (e) CVE, CWE, MITRE/SANS Top 25, OWASP Top 10
6. Attacks
   (a) Attack trees
   (b) Requires/provides model
   (c) Attack graphs
7. Access control matrix
   (a) Matrix
   (b) Primitive operations
   (c) Commands
   (d) Harrison-Ruzzo-Ullman result (undecidability of safety)
8. Policies
   (a) Mandatory access control (MAC)
   (b) Discretionary access control (DAC)
   (c) Originator-controlled access control (ORCON)
   (d) Policy languages
9. Confidentiality Models
   (a) Bell-LaPadula Model
   (b) Lattices and the BLP Model
   (c) Tranquility