Sample Final

These questions are very similar to the types of questions I will ask on the final. The final will be longer, though.

1. In computer security, a *Trojan horse* is:
   (a) A program that has components distributed over many systems, and is used to launch denial of service attacks
   (b) A program that absorbs all available resources of a particular type
   (c) A program with an overt, known purpose and a covert, unknown (and probably undesireable) purpose
   (d) A program that blocks any incoming spam emails

2. How does the Clark-Wilson model require authentication of users to be done?
   (a) A trusted user must vouch for the new user
   (b) Two-factor authentication must be used
   (c) If passwords are used, they must be at least 12 characters long, and use a mixture of letters, digits, and other characters
   (d) None of the above

3. Which of the following does the Needham-Schroeder protocol require?
   (a) A trusted third party
   (b) A public key cryptosystem
   (c) A certificate authority to identify the users
   (d) A connection to the Internet

4. Show how ACLs and C-Lists are derived from an access control matrix.

5. Discuss the revocation problem with respect to access control lists and capabilities. How might one efficiently implement a command to revoke access to an object by one particular user?

6. Consider the problem of managing certificates. One expert said that a hierarchical scheme, such as that employed by PEM, is more likely to be used for business than the Web of Trust employed by PGP. What specific features of the hierarchical system as implemented for PEM (and for other Internet applications) led him to make this assertion? Why might these features lead him to make this statement?

7. Represent an integrity compartment label using the notation

   (*integrity level* ; *set of categories*)

   where the integrity levels are "high", "medium", "low", or "unknown" (in decreasing order of trust) and the integrity categories are "dog", "cat", and "pig". Can a user cleared for (*medium* ;{ *dog* , *cat* }) have read or write access (or both) to documents classified in each of the following ways under the Biba model?
   (a) (*high* ;{ *dog* })
   (b) (*low* ;{ *dog* })
   (c) (*medium* ;{ *dog* , *cat* })
   (d) (*unknown* ;{ *pig* })
   (e) (*high* ;{ *dog* , *pig* , *cat* })

8. Why do some organizations use a DMZ in their network configuration, rather than simply filtering traffic and allowing connections intended for the web and email servers to pass through the firewall?