Sample Final

This is an example of the sort of questions I will ask. The actual final will be longer, of course, and may well have questions about the readings as well as the lectures.

1. Please define the following terms in one or two sentences.

   (a) public key cryptosystem

   (b) privacy

   (c) overvote

   (d) originator-controlled access control

2. Please circle the best answer, and *justify it*.

   (a) In computer security, a Trojan horse is:

      i. A program that has components distributed over many systems, and is used to launch denial of service attacks

      ii. A program that absorbs all available resources of a particular type

      iii. A program with an overt, known purpose and a covert, unknown (and probably undesirable) purpose

      iv. A program that blocks any incoming spam emails

   (b) Which of the following access control models would be most useful to a company selling DVDs containing music and movies, if the goal is to prevent the purchaser from making copies of the DVD's content and distributing it further?

      i. discretionary access control

      ii. mandatory access control

      iii. originator-controlled access control

      iv. role-based access control

   (c) Which of the following is not an approach to intrusion detection?

      i. Signature-based

      ii. Cookie-based

      iii. Anomaly-based

      iv. Specification-based

   (d) Which of these is the best definition of the principle of least privilege?

      i. Processes should share as few privileges as possible

      ii. A process should have no more than the minimum privileges needed to perform its tasks

      iii. A process should have as few privileges as possible

      iv. Users should not be able to change their level of privilege to that of a system administrator

3. A company has offices in San Francisco and London. It needs to send sensitive information between those two offices. It plans to use encryption to protect the information while in transit. Should it use link encryption or end-to-end encryption? Justify your answer.

4. What is the difference between the anti-malware (anti-virus) detection methods of signature scanning and behavioral analysis?

5. What is a sandbox? Why does the Android run apps in it?