# Sample Final

These are sample questions that are very similar to the ones I will ask on the final.

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. Which of the following describes how a botnet is controlled?
   (a) Centrally; one system controls all associated bots.
   (b) Hierarchically; the botnet forms a tree, with the leaves being the bots.
   (c) Peer-to-peer; the bots communicate with one another directly.
   (d) All of the above.

3. This function's purpose is to copy a string from one buffer to another. It is not robust. Find the problems and say how to fix them. Note that the passing of pointers here is defined in the specification of the interface, and so cannot be changed.

```
void mystrcpy(char *s, char *t)
{
        while(*t != '\0')
                *s++ = *t++;
        *s = '\0';
}
```

4. Define each of the following terms in one short sentence:
   (a) ransomware
   (b) passphrase
   (c) capability
   (d) end-to-end encryption

5. In a Multics ring mechanism, a process is running on ring 5. It needs to call a segment with bracket (2, 4, 6). Which of the following is true?
   (a) The process can access the segment, and a ring-crossing fault occurs.
   (b) The process can access the segment, and no ring-crossing fault occurs.
   (c) The process can access the segment, provided a valid gate is used as an entry point.
   (d) The process cannot access the segment.

6. How are ACLs and C-Lists derived from an access control matrix?

7. 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?

8. Name the 5 steps in the flaw hypothesis methodology. Which step in that methodology is often omitted? Why?

9. 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?