Sample Midterm

These are sample questions that are very similar to the ones I will ask on the midterm. The midterm will be about an hour long (but you can take the full class period if you like).

1. Why is a precise statement of security requirements critical to the determination of whether a given system is secure?

2. 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++;
        *t = '\0';
}
```

3. Which of the following demonstrate violations of the principle of least privilege? Please justify your answer.

   (a) The Linux *root* account?

   (b) A user whose function is to maintain and install system software. This user has access to the source files and directories, access to only those programs needed to build and maintain software, and can copy executables into system directories for other users. This user has no other special privileges.

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. 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