Sample Midterm

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

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++;
        *s = '\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. Identify which of the following are mandatory access control policies, which are discretionary access control policies, and which are originator-controlled access control security policies.

   (a) The file access control mechanisms of the UNIX operating system

   (b) A system in which no memorandum can be distributed without the creator's consent

   (c) A military facility in which only generals can enter a particular room

   (d) A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.

5. Please describe how the vulnerabilities models are used during the Flaw Hypothesis Methodology. Be explicit: which phase of the methodology uses them, and how?

6. Represent a security compartment label using the notation

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

   where the security levels are "high", "medium", "low", or "unknown" (in decreasing order of trust) and the security categories are "dog", "cat", and "pig". Can a user cleared for (*medium* ;{ *dog* , *cat* }) have read or write access (or both or neither) to documents classified in each of the following ways under the Bell-LaPadula model?

   (a) (*high* ;{ *dog* })

   (b) (*low* ;{ *dog* })

   (c) (*medium* ;{ *dog* , *cat* })

   (d) (*unknown* ;{ *pig* })

   (e) (*high* ;{ *dog* , *pig* , *cat* })