

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 undesirable) 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. Consider a system that used the Bell-LaPadula model to enforce confidentiality and the Biba model to enforce integrity.
 - (a) If the security classes were the same as integrity classes, what objects could a given process (with some security class that also served as its integrity class) access?
 - (b) Why is this scheme not used in practice?
5. What is a certificate? What is it used for?
6. The following routine reads a file name from the standard input and returns its protection mode. It treats the argument as a file name, and returns the protection mode of the file as a short integer. Identify three non-robust features of this routine, and state how to fix them.

```
/* return protection mode of the named file */
short int protmode(void)
{
    struct stat stbuf;
    char inbuf[100];

    gets(&inbuf);
    stat(inbuf, &stbuf);
    return(stbuf.st_mode&0777);
}
```

7. Show how ACLs and C-Lists are derived from an access control matrix.
8. 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?
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?