

COS214 Tutorial 11

Roberto Togneri, 2000

1. (a) A computer science department has a large collection of UNIX machines on its local network. Users on any machine can issue a command of the form:
machine4 who
and have the *who* command executed on *machine4*, without having the user log in on the remote machine. This feature is implemented by having the user's kernel send both the command and the *uid* to the remote machine. Currently the department's workstations are on the local network. It is proposed to allow students to also connect their PC to the network. Why is this a dangerous move?
(b) One of the computer support people proposes to solve the security problem by restricting such commands to a group of trusted hosts. Is this solution fool-proof?

2. (a) After getting your degree, you apply for a job as director of a large university computer center that has just put its ancient operating system out to pasture and switched over to UNIX. You get the job. Fifteen minutes after starting work, your assistant bursts into your office screaming: "Some students have discovered the algorithm we use for encrypting passwords and posted it on the bulletin board." What should you do?
(b) When a file is removed, its blocks are generally put back on the free list, but they are not erased. Do you think it would be a good idea to have the operating system erase each block before releasing it?

3. The Unix file system has *rwX* permissions for the user (i.e. owner), the group, and others. Write, in pseudo code, a function, *check()*, that is given the user id (*uid*) and group id (*gid*) of the calling process, an operation (*op* = r, w, or x), the owner and group id of the file (*fuid*, *fgid*) and the set of 9 bits for the permissions (*perm*). It returns a boolean to indicate whether the operation is legal.

4.
 - (a) Explain what the UNIX *rxw* bits mean for:
 - (i) a regular file
 - (ii) a directory
 - (b) Derive the UNIX file type and permissions, uid and gid:
 - (i) to allow only the owner read/write access to a file?
 - (ii) to allow only a selected group of users to create/delete/list/modify files in a directory?
 - (iii) to allow only a selected group of users to list/modify files in a directory, but a single maintainer to create/delete files?
 - (c) What can you say about the following UNIX file permissions:
 - (i) `drwx-wx--x` john student
 - (ii) `-rw-rw-rw` root sys
 - (iii) `-rwxr-x--x` root wheel

5. Consider a system that supports 5000 users. Suppose that you want to allow 4990 of these users to be able to access one file. How would you specify this protection scheme in UNIX?

6. For each of the following protection problems, indicate which mechanisms (ACL, C-lists or UNIX *rxw*) can be used most effectively:
 - (a) Ken wants his files readable by everyone except his office mate
 - (b) Mitch and Steve want to share some secret files
 - (c) Linda wants some of her files to be public.
 - (d) George wants his files read/writable by a close group of friends, readable by another group of friends, and inaccessible by everybody else.