9.{2,5,6,7,8,11,12}

**2.** One of the techniques to build a secure operating system is to minimize the size of

TCB. Which of the following functions needs to be implemented inside the TCB and

which can be implemented outside TCB: (a) Process context switch; inside (b) Read a file

from disk; outside(c) Add more swapping space; outside(d) Listen to music;inside (e) Get the GPS coordinates

of a smartphone.outside

1. Inside
2. Inside
3. Inside
4. Outside
5. Outside

**5.** Suppose that a system has 5000 objects and 100 domains at some time. 1% of the objects

are accessible (some combination of *r*, *w* and *x*) in all domains, 10% are accessible

in two domains, and the remaining 89% are accessible in only one domain.

Suppose one unit of space is required to store an access right (some combination of *r*,

*w*, *x*), object ID, or a domain ID. How much space is needed to store the full protection

matrix, protection matrix as ACL, and protection matrix as capability list?

5000\*100= 500,000 full protection, 10\*100\*2 + 100\*2\*2 + 890\*1\*2 = 4180 capabilities

**6.** Explain which implementation of the protection matrix is more suitable for the following

operations:

(a) Granting read access to a file for all users. access

(b) Revoking write access to a file from all users. Access lists for objects

(c) Granting write access to a file to John, Lisa, Christie, and Jeff. Capability list for domains

(d) Revoking execute access to a file from Jana, Mike, Molly, and Shane. capabilities

**7.** Tw o different protection mechanisms that we have discussed are capabilities and access-

control lists. For each of the following protection problems, tell which of these

mechanisms can be used.

(a) Ken wants his files readable by everyone except his office mate. capabilities

(b) Mitch and Steve want to share some secret files. Access and capabilites

(c) Linda wants some of her files to be public. Access and capabilites

**8.** Represent the ownerships and permissions shown in this UNIX directory listing as a

protection matrix. (*Note*: *asw* is a member of two groups: *users* and *devel*; *gmw* is a

member only of *users*.) Treat each of the two users and two groups as a domain, so

that the matrix has four rows (one per domain) and four columns (one per file).

– rw– r– – r– – 2 gmw users 908 May 26 16:45 PPP– Notes

– rwx r– x r– x 1 asw dev el 432 May 13 12:35 prog1

– rw– rw– – – – 1 asw users 50094 May 30 17:51 project.t

– rw– r– – – – – 1 asw dev el 13124 May 31 14:30 splash.gif

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Domain/obj | PPP | Prog1 | Project.t | Splash.gif |
| Asw | Read | Read | Read  Write | Write  Read |
| Gmw | Read  Write | execute | Read  Write |  |
| users |  | Read | Read  write |  |
| Devel | Read  write | execute | None | execute |

**11.** Suppose there are four security levels, 1, 2 and 3. Objects *A* and *B* are at level 1, *C*

and *D* are at level 2, and *E* and *F* are at level 3. Processes 1 and 2 are at level 1, 3 and

4 are at level 2, and 5 and 6 are at level 3. For each of the following operations, specify

whether they are permissible under Bell-LaPadula model, Biba model, or both.

(a) Process 1 writes object *D level 1 w level 2 bell*

(b) Process 4 reads object *A level 2 reads level 1 bell*

(c) Process 3 reads object *C level 2 reads level 2, both*

(d) Process 3 writes object *C level 2 reads level 2, both*

(e) Process 2 reads object *D level 1 reads level 2, biba*

(f) Process 5 writes object *F level 3 writes level 3, both*

(g) Process 6 reads object *E level 3 reads level 3, both*

(h) Process 4 write object *E level 2 writes level 3, bell*

(i) Process 3 reads object *F level 2 reads level 3, biba*

**12.** In the Amoeba scheme for protecting capabilities, a user can ask the server to produce

a new capability with fewer rights, which can then be given to a friend. What happens

if the friend asks the server to remove even more rights so that the friend can give it to

someone else?

A check field change is needed for revocation in Amoeba scheme which invalidates all capabilities. No selective revocation. A kernel managing capabilities as a hydra would solve the problem of letting a friend share a copy.