University of Newcastle
School of Electrical Engineering and Computing

COMP2240 - Operating Systems
Workshop 10
Topics: *Security and Protection*

1. Assume that passwords are selected from four-character combinations of 26 alphabetic characters. Assume that an adversary is able to attempt passwords at a rate of one per second.

a) Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?

b) Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

c) Assuming that the username is a one to eight-character alphabetic string, unknown to the adversary, and that no feedback is given until both username and password are entered, what is the expected time to discover a correct combination?

d) What inference do you draw from these calculations?

2. The question arises as to whether it is possible to develop a program that can analyse any piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run D(P), the result returned is TRU (P is a virus) or FALSE (P is not a virus). Now consider the following program:

```
Program CV: =
{ …
      main-program :=
          { if  D (CV) then goto next:
               else infect-executable;
          }
next:
}
```

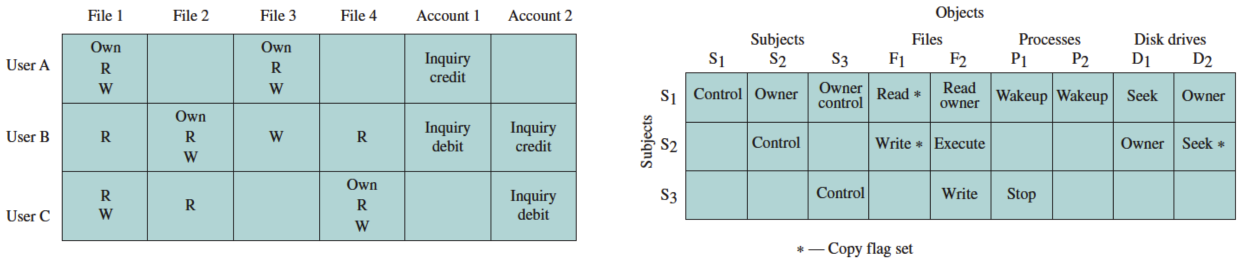
In the preceding program, infect-executable is a module that scans memory for executable programs and replicates itself in those program. Determine if D can correctly decide whether CV is a virus.

3. For the DAC model discussed in the Lecture, an alternative representation of the protection state is a directed graph. Each subject and each object in the protection state is represented by a node (a single node is used for an entity that is both subject and object). A directed line from a subject to an object indicates an access right, and the label on the link defines the access right.

a) Draw a directed graph that corresponds to the access matrix of Figure (a).

b) Draw a directed graph that corresponds to the access matrix of Figure (b).

c) Is there a one-to-one correspondence between the directed graph representation and the access matrix representation? Explain.



	File 1	File 2	File 3	File 4	Account 1	Account 2
User A	Own R W		Own R W		Inquiry credit	
User B	R	Own R W	W	R	Inquiry debit	Inquiry credit
User C	R W	R		Own R W		Inquiry debit

	Objects								
	Subjects			Files		Processes		Disk drives	
Subjects	S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
S_1	Control	Owner	Owner control	Read *	Read owner	Wakeup	Wakeup	Seek	Owner
S_2		Control		Write *	Execute			Owner	Seek *
S_3			Control		Write	Stop			

* — Copy flag set

a) Access control Matrix

b) Extended Access Control Matrix

Figure 1: An example of access matrices

4. The following code fragments show a sequence of virus instructions and a metamorphic version of the virus. Describe the effect produced by the metamorphic code.

Original Code	**Metamorphic Code**

`mov eax, 5`
`add eax, ebx`
`call [eax]`
	`mov eax, 5`
	`push ecx`
	`pop ecx`
	`add eax, ebx`
	`swap eax, ebx`
	`swap ebx, eax`
	`call [eax]`
	`nop`

5. Assume a system with *N* job positions. For job position *i*, the number of individual users in that position is U_i and the number of permissions required for the job position is P_i.

a. For a traditional DAC scheme, how many relationships between users and permission must be defined?

b. For a RBAC scheme, how many relationships between users and permission must be defined?

6. UNIX treats file directories in the same fashion as files; that is, both are defined by the same type of data structure, called an inode. As with files, directories include a 9-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection node 644(octal) contained in a directory with protection mode 730. How might the file be compromised in this case?

Supplementary problems:

S1. Assume that passwords are limited to the use of 95 printable ASCII characters and that all passwords are 10 characters in length. Assume a password cracker with an encryhption rate of 6.4 million encryptions per second. How long will it take to test exhaustively all possible passwords on that system?

S2. Consider the following code fragment:

```
legitimate code
if data is Friday the 13th;
     crash_computer();
legitimate code
```

What type of malicious software is this?

S3. Consider the following code fragment:

```
username = read-username();
password = read_password();
if username is “113t h4ck0r”
     return ALLOW_LOGIN;
if username and password are valid
     return ALLOW_LOGIN;
else return DENY_LOGIN;
```

What type of malicious software is this?