Veton Abazovic

NetID: va187

Computer Security

2/13/2019

Assignment 2

Question 1

(a) What form of the chmod command would you run to change the file to read-only by only the group members? Run man chmod if you are not familiar with the command or see this page for a clearer overview.

Answer: To change the file to read-only by only the group members you would use the Chmod 040 to achieve this type of privileges.

(b) Can you still access the file contents since you are a member of the group?

Answer: When using the command above, I still can not access the file as I, the user can't do anything.

(c) Can you delete the file without changing permissions (e.g., *rm -f myfile*)?
Answer: You can delete the file without changing permissions.

Question 2

To get access control matrices to scale better, the text states that the two main ways are "to compress the users and to compress the rights".

(a) What is meant by "compressing the users"?

Answer: "Compressing the users" means to use groups or roles to manage the privileges of large sets of users. This is used to manage admins to regular users and others.

(b) What is meant by "compressing the rights"?

Answer: "Compressing the rights" means that we give each user some privilege based on their role. We do this by having an access control matrix by using tickets as either columns or rows.

Question 3

What four deficiencies does the author point out with Unix ACLs? Write your answers briefly: one short sentence per deficiency.

Answer:

1. The first deficiency that the author points out with Unix ACLs is that the sysadmin can do anything, making it harder to be traced.

2. The next deficiency is a way of implementing access to a program because ACLs only consist of names of users.

3. The third deficiency is that it is difficult to change access to a user because we would need to know what files they could assess with the change of privileges.

4. The last deficiency is that ACLs only names one user and only holds one group ID.

Veton Abazovic

NetID: va187

Question 4

(a) What is the simple security property of the Bell-LaPadula model?

Answer: The simple security property of the Bell-LaPadula model is the *No Read Up*. The No Read Up basically means if a process is trying to read some data that is at a higher level, then it won't be able to read the data.

(b) What is the *-property of the Bell-LaPadula model?

Answer: The *-property of the Bell-LaPadula model is the No Write Down. The No Write Down model states that a process can not write data to a lower level than itself.