Hassan Khousheish

CMPS 297Q

Dr. Haidar Safa

Assignment 1

1-

|  |  |  |  |
| --- | --- | --- | --- |
| FILE NAME  USER | ALEXRC | BRIANRC | CATYRC |
| ALEX | R/W/O/E | R |  |
| BRIAN | R | R/W/O/E |  |
| CATY | R | R/W | R/W/O/E |

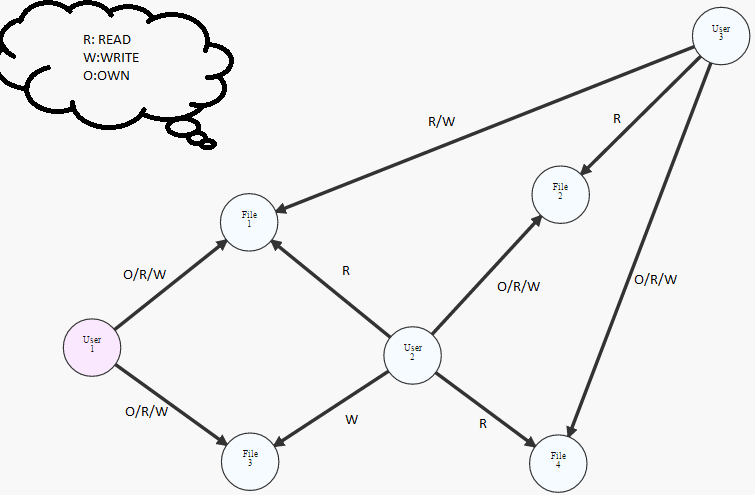
R:READ

W:WRITE

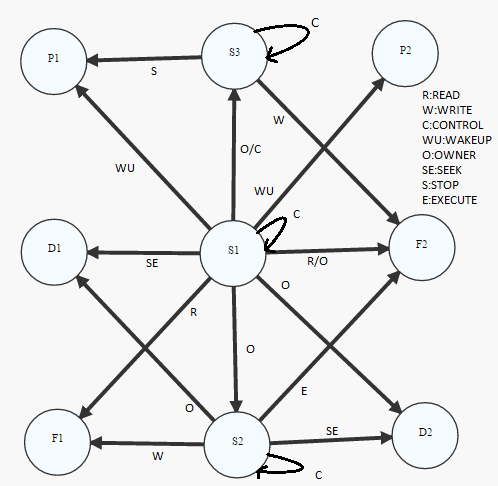
O:OWN

E:EXECUTE

2-

a-

b-



c- The given access matrix generates only one directed graph, and the directed graph generates only one access matrix, so there is a one to one correspondence.

3-

Suppose that a directory D and a file F have the same owner and group and that F contains some text. Disregarding the superuser, no one besides the owner of F can change its contents, because only the owner has write permission. However, anyone in the owner’s group has write permission for D, so that any such person can remove F from D and install a different version, which is the equivalent of being able to modify F.

4-

For DAC:# of relationships between users and permissions = N\*P\*U

For RBAC:# of relationships between users and permissions = N\*P\*R

Where R represents distinct systems that manage their own roles

5-

a-SELECT accounts FROM users WHERE login = ‘doe’ AND pass = ‘secret’ AND pin = 123

b-This could bypass login and compromise the security. The effect of typing in ’ or 1 = 1 - -would be that the condition of the query would be true for each of the rows and therefore return all of the information. This would mean that the malicious user now is authenticated as the user. Therefore, by this the malicious user would have bypassed the login security.

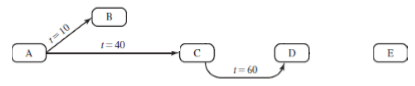
6-

The original first query returns a null set assuming there is nothing equal to “” in the database, but the second query returns information from the table. In this example, it returns the column “CardNo” for the account “10032” which is the card number for account number 10032.

7-

The DELETE privilege giving by X at the time t = 25 must be revoked. This is because of X earliest remaining DELETE privilege was received at time t = 30. The grants of READ and INSERT with X are still permitted because they where granted already a time t = 15 by A.

8-i h



9-

|  |  |
| --- | --- |
| Apple IDrive | Box |
| True archiving: keeps all of your backed up files, including those which are no longer present on your computer, available in your IDrive account | Easily manage access and sharing policies inside and outside your organization while minimizing the risk of data loss through full visibility and central management of files, security, policy and provisioning. |
| The Continuous Data Protection (CDP) feature automatically recognizes the changes made to the files | Ensure the confidentiality and integrity of files with encryption for content in transit and at rest, with the option for customer managed encryption keys. Box also uses multiple data centers with reliable power sources and backup systems to offer 99.9% SLAs and redundancy. |
| Multiple device backup capability | Box makes governance and compliance a seamless part of the way you work. Easily manage the lifecycle of documents, comply with regulatory mandates as well as support defensible e-discovery and data retention policies. |
| File syncing across all devices | User activity tracking |
| Activity and status reporting | Project-management capabilities |
| Hybrid cloud and local storage |  |

10-11-

D is supposed to examine a program P and return TRUE if P is a computer virus and FALSE if it is not.

But when CV calls D.

If D says that CV is a virus, then CV will not infect an executable.

But if D says that CV is not a virus, it infects an executable.

D always returns the wrong answer.

12-

same effect as 1st code fragment

1st line - same eax=5

2nd sample , push then pop ecx, do nothing with that next line same: eax=eax+ebx

2nd sample swap eax <=> ebx, then back again (no net change)

next line same call [eax]

2nd sample nop ( do nothing / wait)

13-

Logic bomb

14-

RootKit

15-

Morris Worm:

Written in november 2 1988 it was one of the first worms get distributed via the internet. It was written by Cornell University graduate Robert Morris and was launched from MIT. It exploited vulnerabilities in unix sendmail, finger and rsh/rexec. It caused damages ranging from 100 thousand to 10 million dollars.

Stuxnet :

A malicious worm which was introduced in 2010. It was believed to be USA-Israel developed to attack the Iran nuclear plan. It was programmed to erase itself in 24 june 2012 thus limiting its damages. It does little to no damage on computers that don't meet the specifications. It was made to act as a man in the middle thus making it not seem harmful or force the system to shut down due to detected abnormal behavior.

CryptoLocker:

A ransomware Trojan that targets computers running Microsoft Windows. It encrypts specific files via a rsa public key cryptography and stores the key on the attacker’s server and sends a message to the user offering to decrypt the files in return for money, and threats to delete the key from the server if the deadline passes.

ILOVEYOU:

Also referred to as Love Letter infected millions of computers on and after may 5th 2000. Its sent via email with title I LOVE YOU containing a text file names LOVE-LETTER-FOR-YOU.txt.vbs, so people who received the email thought that it was a normal text file. Upon opening the file, the visual basic code was ran which overwrites random files and send a similar email to everyone on the person’s mailing list.