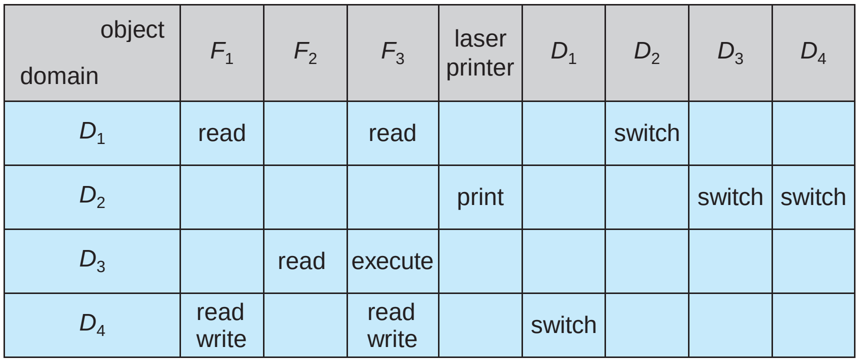
CS471: Operating System Concepts
Module 10: Homework #10
Solution
Points: 20

Question 1 [Points 4] Consider a computer system in which computer games can be played by students only between 10 P.M. and 6 A.M., by faculty members between 5 P.M. and 8 A.M., and by the computer center staff at all times. Suggest a scheme for implementing this policy efficiently.

Sol: This may be achieved in several ways. Here is one way.

Define roles---students, faculty, system staff.
Define computer games as a special resource
Define authorization rules the roles can access and execute the special resource during the specified time.

Question 2 [Points 4] Suppose a process starts executing in domain D4, state two possible sequences of domains it can go through prior to termination.



object domain	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch
D_3		read	execute					
D_4	read write		read write		switch			

Sol: Several scenarios are possible. Here are two examples.
D4 → D1 → D2 → D3;
D4 → D1 → D2 → D4 → D1 → D2

Question 3 [Points 9] Discuss how the asymmetric encryption algorithm can be used to achieve the following goals.
a. Authentication: the receiver knows that only the sender could have generated the message.
b. Secrecy: only the receiver can decrypt the message.
c. Authentication and secrecy: only the receiver can decrypt the message, and the receiver knows that only the sender could have generated the message.

Sol:

a. Sender generates a hash of the message, encrypts the hash using its public key resulting in a digital signatures, and sends the message and the signature to the recipient. The recipient decrypts the signature using sender's public key, generates a hash of the message, and checks if both hashes are identical. This is how the receiver may know that the message was sent by the sender.
b. Sender encrypts the message using receiver's public key. This way only the intended receiver can decrypt the message with its private key.
c. Sender encrypts the message with receiver's public key and attaches a digital signature using its own private key as discussed in (a) above. This way only the intended receiver can decrypt the message and it can verify that it is indeed sent by the claimed sender.
d.

Question 4 [Points 3] Make a list of six security concerns for a bank's computer system. For each item on your list, state whether this concern relates to physical, human, or operating-system security.

Sol: List any six concerns. For example,

Concern 1. Bank's server in a physically unsecure location: (Physical)

Concern 2: The network cables through which the bank's data goes through is physically exposed and hence vulnerable for tapping. (Physical)

Concern 3: Employees share their passwords (advertently or inadvertently) with others (e.g., friends, family, etc.) resulting in a security threat. (Human)

Concern 4: Employees use their personal devices (e.g., USB) on bank's computers or install unverified software on their work computers. This could result installing viruses and stealth software that could damage the system. (Human)

Concern 5: Operating system stores user information (e.g., user login, password, etc.) in an unsecure location that could be attacked. (OS)

Concern 6: Operating system does not provide memory protection so that one user process is able to access/modify the memory content of another process. (OS)