1. **Replay Attacks** On Monday, Alice uses trusted third party Cathy to establish a secure communication session with Bob. The attached file homework5.pdf Preview the document contains three slides that show three different ways to establish a shared key. Slide 1 is the simplest key exchange and shows all messages exchanged. Slide 2 and Slide 3 each show a variation of how Alice and Bob establish a shared secret key. For brevity, Slide 2 and Slide 3 focus on the key exchange and do not show the messages exchanged after Alice requests the iPhoneX. You may assume the messages exchanged after Alice requests the iPhoneX are identical regardless of whether the key exchange follows Slide1,2, or 3.

   Eve observes and records all the messages exchanged. Eve also observes that a package arrived at Alice's house the next day and suspects the message exchange caused the package to be delivered. Eve knows Alice going on vacation Friday and Eve could easily pick up any package left at Alice's door. On Saturday, Eve attempts a replay attack.

   Question 1A) Using the message exchange shown in Slide 1, can Eve launch a successful replay attack? If yes, draw a picture similar to Slide that shows all the messages exchanged. If no, explain why.

   Yes she can
   Alice →"Charge an iPhone to my credit card 123456789 and have it delivered to my house" → Bob
   Bob → "I placed the order and it will arrive tomorrow" → Alice
   Alice → "Thanks this session is now completed" → Bob
   Bob → "Acknowledged I am discarding key k_s" → Alice

   Question 1B) As part of the replay attack, does Eve learn Alice's credit number?

   No because she doesn't have the key that Bob has, so she won't be able to decrypt it.

   Question 2A) If Alice instead uses the key exchange shown in Slide 2, can Eve launch a successful replay attack? If yes, draw a picture similar to Slide that shows all the messages exchanged. If no, explain why.

   No because there is a random number that is being generated when we do (r2-1)

so she won't be able to know what that is because without the key and now some random number being subtracted from it then it is not possible

Question 2B) If Alice uses the key exchange shown in Slide 2 and Eve has obtained session key Ks, can Eve launch a successful replay attack? If yes, draw a picture similar to Slide that shows all the messages exchanged. If no, explain why.

Yes because in difference to the previous question, now she know what K_s is so now she can decrypt the (r2-1)

Question 3) If Alice uses the key exchange shown in Slide 3 and Eve has obtained session key Ks, can Eve launch a successful replay attack? If yes, draw a picture similar to Slide that shows all the messages exchanged. If no, explain why.

No she won't be able to do the attack because even if she figured K_s, the message is using r2 and r3 so whenever she tries to decrypt it she won't have matching keys because r2 and r3 are different so she won't return the right message.

2. **Review 4.1** Briefly define the differences between DAC and MAC.

   Access control policies dictate what types pf access are permitted. DAC, or **Discretionary Access Control**, controls this access based on the identity of the requestor and on access rules stating what requestors are allowed to do. This policy is *discretionary* because an entity with access to a source, can permit another entity to access that source. This is, imagine I have access to enter the cafeteria and certain areas of the cafeteria that aren't allowed to everybody. Now let's assume you want to grab a packet of ribs that is saved in those restricted areas that I have access to. But I am super busy cooking eggs, I can grant you access to the restricted area of the cafeteria because I trust you and I can be sure you're only gonna grab the ribs, so under my discretion, I granted you permission to access the area. Now, MAC or **Mandatory Access Control**, controls the access by comparing security labels with security clearances. This policy is *mandatory* because an entity that has clearance to access a source, cannot give access to another entity to access that source. This is, if I have clearance to enter CU's room where the safe box is located, the I can access it but I cannot send someone else to the room to grab something I need or anything. I cannot grant anyone

permission to enter that room only because I have clearance to enter that room. The clearance needs to be approved before I can send some random to that room.

3. **Review 4.8** Briefly define the four RBAC models of Figure 4.8.a.

   [SAND96] defines a family of reference models. This family consists of four models that are related to each other. **$\mathbf{RBAC_0}$** is the base model, this one contains the minimum functionality and minimum requirements for an RBAC system. Having the base settled, we can add **$\mathbf{RBAC_1}$**, this model includes $RBAC_0$ in addition with role hierarchies, which enables one roles to the inherit permissions from another role. **$\mathbf{RBAC_2}$** also includes $RBAC_0$ but this model adds constrains, which restrict the way in which the components of an RBAC system may be configured. Lastly, **$\mathbf{RBAC_3}$** is the combination of ALL other 3 models so it contains the base model $RBAC_0$ and the role hierarchies of $RBAC_1$ and the constrains of $RBAC_2$.

4. **Problem 4.5** UNIX treats files 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 nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644(octal) contained in a directory with protection mode 730. How might the file be compromised in this case?

   We need to first see who has access to what and we do that by converting the number to binary so we obtain :

   $$730 = 1001\ 0011\ 0000$$

   $$644 = 0110\ 0100\ 0100$$

   From this we know that the owner of the directory can execute and the group can write and execute. Now for the file contained in the directory we know that the owner can read and write, the group can read, and every other class can read. Therefore EVERY class of the file can read the file. This is enough for them to know the name of the file and the contain information on it. The file WILL BE compromised because the directory group has write and execute so according to the book in page 118 *"write bits grant the right to list and to create/rename/delete files in the directory"*, this means, the file can be deleted, or renamed or they can create another file and name it as the file in risk.

5. **Problem 4.8** Assume a system with N job positions. For position i, the number of individual users in that position is U_j 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 permissions must be defined?

   (b) for a RBAC scheme, how many relationships between users and permissions must be defined?

   a) For DAC we would **only need one** relationship between user and permissions since DAC defines the access rights of individual users (page 120).

   b) For RBAC we would need the all the individual users in the position times the number of permissions required for the job positions, which is the **U*P**.

6. **Problem 4.12** In the example of the online entertainment store in Section 4.6, with the finer-grained policy that includes premium and regular users, list all of the roles and all of the privileges that need to be defined for the RBAC model

   For RBAC model we would need the following:
   5 roles: Adult , Juvenile, Child, Premier User, Regular User
   5 privileges: Can view → R, PG-13, G, New Release, Old Release

	Adult	Juvenile	Child	Premium	Regular
User 1	X				X
User 2	X			X	
User 3		X		X	
.		X			X
.			X		X
.		X			X
User m	X			X	

	R	PG-13	G	New Release	Old Release
Adult	X	X	X		
Juvenile		X	X		
Child			X		
Premium				X	
Regular					X