1. On Monday, Alice uses trusted third party Cathy to establish a secure communication session with Bob. The attached file homework5.pdfPreview 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.

   (a) 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.

   (b) As part of the replay attack, does Eve learn Alice's credit number?

   (c) 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.

   (d) 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.

   (e) 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.

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

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

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 p;roblems. 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?

5. **Problem 4.8** 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 permissions must be defined?

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

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.