

Replay Attacks On Monday, Alice uses trusted third party Cathy to establish a se-cure 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.

**1A)** Using the message exchange shown in Slide 1, can Eve launch a successful replay attack? 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 ks” → Alice **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. **2A**) If Alice instead uses the key exchange shown in Slide 2, can Eve launch a successful replay attack? No because there is a random number that is being generated when we do (r2-1) 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 **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? Yes because in difference to the previous question, now she know what Ks is so now she can decrypt the (r2-1) **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? No she won’t be able to do the attack because even if she figured Ks, 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. 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 discre- tionary 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 clear- ances. 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.