16-124-836
Marcel Matti ZAUDER

5.2 Question 2

5.2.A In scenario 1, should nonce 1 always differ between different requests for a logical connection? Why?

Yes, it should always differ between the different requests, so A can ensure that the response of the KDC is connected with the request A sent and not any replay of a previous request.

5.2.B In scenario 1, is Responder B confident that the session key was produced by the KDC? Why?

As the message that is sent to B ($E(K_b, [K_s \| ID_A])$ is encrypted with the key K_b, B knows that it is protected from eavesdropping and also that the information was produced by the Key Distribution Center.

5.2.C In scenario 1, assume that steps 4 and 5 are not performed. Is this dangerous? Why?

Yes, it would be dangerous not to perform them as steps 4 and 5 assure that the message which B received in step 3 was not a replay.

5.2.D Which scenario is the Decentralized one? What are the main advantages/disadvantages of each?

Scenario 2 is the decentralized one. As no Key Distribution Center is required, the requirements for it being trusted and secure can be disregarded. However, a full decentralization is not practical for large networks using symmetric encryption only. Nevertheless in a local network this approach is much more useful. Another disadvantage is that for a network with n end systems as many as $\frac{n(n-1)}{2}$ master keys are required.

5.2.E What is the difference between Session keys and Master keys? What problem is being addressed in end-to-end key distribution with their use?

A session key is used for a specific number of messages or a certain amount of time, whereas a master key is used to encrypt those session keys in order to be able to transfer them securely. Session keys are used in order to make it harder for malicious adversaries and eavesdropper to learn the message transferred between two parties using i.e. cryptanalysis to determine the encryption key as they are only valid for a certain amount of time. A master key is established the very first time the user/end system is communicating with the KDC and is only shared between these two parties in order to provide a secure transfer of the later used session keys.