COMP90043: Cryptography and security

Week 9: Workshop-9

Part1: Symmetric Key Key distribution

Q1 This is a variation of the protocol discussed in the class symmetric key description involving n users and a KDC. Here every user decides to generate random number themselves for the communication they seek to start.

The steps are as follows:

1. A generates a random number R and sends to the KDC his name A, destination B, and E(Ka, R).

2. KDC responds by sending E(Kb, R) to A.

3. A sends E(R, M) together with E(Kb, R) to B.

4. B knows Kb, thus decrypts E(Kb, R), to get R and will subsequently use R to decrypt

E(R, M) to get M.

Is this secure?

PS: Assume all other assumptions made in the protocol. All users share a master key with KDC, all communications can be observed by the users.

Solution:

i) sending to the server the source name A, the destination name Z (his own), and E(*Ka*, *R*), as if A wanted to send him the same message encrypted under the same key R as A did it with B
ii) The server will respond by sending E(*Kz*, *R*) to A and Z will intercept that
iii) because Z knows his key *Kz*, he can decrypt E(*Kz*, *R*), thus getting his hands on R that can be used to decrypt E(*R*, *M*) and obtain *M*.

Q2.

Consider the following protocol, designed to let A and B decide on a fresh, shared session key K=AB. We assume that they already share a long-term key K_{AB}.

1. A → B: A, N_A.

2. B → A:E(K_{AB}, [N_A, K'$_{AB}$])

3. A → B:E(K'$_{AB}$, N_A)

a. We first try to understand the protocol designer's reasoning:

— Why would A and B believe after the protocol ran that they share K'$_{AB}$ with the

other party?

—Why would they believe that this shared key K'_{AB} is fresh?

In both cases, you should explain both the reasons of both A and B, so your answer should complete the sentences

A believes that she shares K'_{AB} with B since…

B believes that he shares K'_{AB} with A since…

A believes that K'_{AB} is fresh since…

B believes that K'_{AB} is fresh since…

b. Assume now that A starts a run of this protocol with B. However, the connection is intercepted by the adversary C. Show how C can start a new run of the protocol using reflection, causing A to believe that she has agreed on a fresh key with B (in spite of the fact that she has only been communicating with C). Thus, in particular, the belief in (a) is false.

c. Propose a modification of the protocol that prevents this attack.

Solution: a. A believes that she shares K'_{AB} with B since her nonce came back in message 2 encrypted with a key known only to B (and A). B believes that he shares K'_{AB} with A since *NA* was encrypted with K'_{AB}, which could only be retrieved from message 2 by someone who knows K'_{AB} (and this is known only by A and B). A believes that K'_{AB} is fresh since it is included in message 2 together with N_A (and hence message 2 must have been constructed after message 1 was sent). B believes (indeed, knows) that K'_{AB} is fresh since he chose it himself.

b. B. We consider the following interleaved runs of the protocol:

1. A →C(B) : A, N_A
1`. C(B) →A : B, N_A
2`. A →C(B) : E(K_{AB}, [N_A, K'_{AB}])
2. C(B) →A : E(K_{AB}, [N_A, K'_{AB})
3. A →C(B) : E(K'_{AB}, N_A)

C cannot encrypt A's nonce, so he needs to get help with message 2. He therefore starts a new run with A, letting A do the encryption and reflecting the reply back. A will accept the unprimed protocol run and believe that B is present.

c. To prevent the attack, we need to be more explicit in the messages, e.g. by changing message 2 to include the sender and receiver (in this order), i.e. to be E(K_{AB}, [A, B, N_A, K'_{AB}]).