COMP90043 Cryptography and Security
Semester 2, 2020, Workshop Week 9 Solutions

Symmetric Key Distribution Protocol

1. Consider a variation of the symmetric key distribution protocol discussed in the lecture involving n users and a KDC. Here every user decides to generate random number themselves for the communication they seek to start. All users share a master key with the KDC, all communications can be observed by all users.
   The steps are as follows:

   (a) A generates a random session key K_s and sends to the KDC his identity ID_A, destination ID_B, and $E(K_A, K_s)$.

   (b) KDC responds by sending $E(K_B, K_s)$ to A.

   (c) A sends $E(K_s, M)$ together with $E(K_B, K_s)$ to B.

   (d) B knows K_B, thus decrypts $E(K_B, K_s)$, to get K_s and will subsequently use K_s to decrypt $E(K_s, M)$ to get M.

   Is this secure?

   It's not secure. Consider the following steps:
   An attacker Z could send to the server the source identity ID_A, the destination ID_Z (his own), and $E(K_A, K_s)$, as if A wanted to send Z a message encrypted under the same key K_s as A did with B.
   The server will respond by sending $E(K_Z, K_s)$ to A which could be intercepted by Z.
   Because Z knows his own key K_Z, he can decrypt $E(K_Z, K_s)$, thus getting his hands on K_s that can be used to decrypt $E(K_s, M)$ and obtain M.

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

$$
\begin{aligned}
A \rightarrow B &: ID_A, N_A \\
B \rightarrow A &: E(K_{AB}, [N_A, K_s]) \\
A \rightarrow B &: E(K_s, N_A)
\end{aligned}
$$

   (a) Why would A and B believe after the protocol ran that they share K_s with each other?

   A believes that she shares K_s 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_s with A since N_A was encrypted with K_s, which could only be retrieved from message 2 by someone who knows K_{AB} (and this is known only by A and B).

(b) Why would they believe that this shared key K_s is fresh?

A believes that K_s 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_s is fresh since He chose it himself.

(c) 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 he has only been communicating with C). Thus, in particular, the belief in (a) is false.

Consider the following interleaved runs of the protocol:

$$\begin{aligned} A \to C :& ID_A, N_A \\ & C \to A : ID_B, N_A \\ & A \to C : E(K_{AB}, [N_A, K_s]) \\ C \to A :& E(K_{AB}, [N_A, K_s]) \\ A \to C :& E(K_s, N_A) \end{aligned}$$

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. Note that C cannot decrypt any further message from A, nor sending any message to A, but A will accept the unprimed protocol run and believe that B is present.

(d) Propose a modification of the protocol that prevents this attack.

To prevent the attack, we need to be more explicit in the messages. For example, by changing message 2 to include both the sender and receiver: $E(K_{AB}, [ID_A, ID_B, N_A, K_s])$.

Key Management and Distribution

1. Discuss four methods which are used in distributing public keys.

   Public announcement
   Publicly available directory
   Public-key authority
   Public-key certificates

2. What are the essential ingredients of a public-key directory?

   (a) The authority maintains a directory with a name, public key entry for each participant.

   (b) Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.

(c) A participant may replace the existing key with a new one at any time, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way.

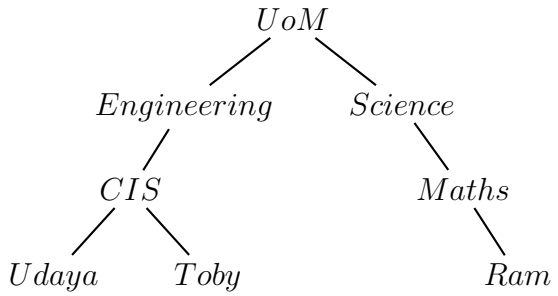
(d) Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widely circulated newspaper.

(e) Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.

3. What is a chain of certificates? What are forward and reverse certificates?

   A chain of certificates consists of a sequence of certificates created by different certification authorities (CAs) in which each successive certificate is a certificate by one CA that certifies the public key of the next CA in the chain.
   Forward Certificates: Certificates of X generated by other CAs.
   Reverse Certificates: Certificates generated by X that are the certificates of other CAs.

4. For the following hierarchy, what is the chain of certificates that user "Udaya" needs to obtain in order to establish a certificate path to "Ram"? You can use X.509 conventions for the certificate chain, for example the certificate for "Udaya" by CA "CIS" is represented as CIS«Udaya».



   CIS«Engineering» Engineering«UoM» UoM«Science» Science«Maths» Maths«Ram»