Coursework 1 - Exercise 10

November 9, 2023

Consider the following key distribution protocol in which two users Alice and Bob wish to establish a shared key $\mathsf{K_{AB}}$ with the help of a trusted server S. Assume Alice and Bob share secret keys $\mathsf{K_{AS}}$ and $\mathsf{K_{BS}}$ with S and that nonces are 64 bits long and keys are 128 bits long.

1. $A \to B : Alice, N_A$
2. $B \to S : Bob, N_B, \mathsf{Enc}(\mathsf{K_{BS}}, \langle A, N_A, N_B \rangle)$
3. $S \to A : \mathsf{Enc}(\mathsf{K_{AS}}, \langle \mathsf{K_{AB}}, B, N_A, N_B \rangle), \mathsf{Enc}(\mathsf{K_{BS}}, \langle A, \mathsf{K_{AB}} \rangle)$
4. $A \to B : \mathsf{Enc}(\mathsf{K_{BS}}, \langle A, \mathsf{K_{AB}} \rangle), \mathsf{Enc}(\mathsf{K_{AB}}, N_B)$

a) Describe at least two attacks that can be applied to this protocol (If your attack reduces to simple forwarding, it will not count…).

b) For each attack, give a countermeasure that renders the attack useless.

---

a)

- Attack 1: Server Compromise Given that it is the server the one that creates the key for Alice and Bob, were the server to be comprimised, all the communications established throught the server would be comprimsied too, including the K_{AB}
- Attack 2: Brute Forcing keys

  Eventhough the key sice is significantly big, current computers could crack keys of this size. Taking into account that A, N_A, N_B are sent in plaintext an attackere *Eve* knows the content of $\mathsf{Enc}(\mathsf{K_{BS}}, \langle A, N_A, N_B \rangle)$, so this only helps finding the K_{BS} key.

  Once K_{BS} is found, Eve can access any connection that is tried to establish with Bob by intercepting the last message: $\mathsf{Enc}(\mathsf{K_{BS}}, \langle A, \mathsf{K_{AB}} \rangle)$ and decyphring the key

b)

- Countermeasure for Attack 1:

  To avoid the server having access to the key, a scheme with public-secret keys communication that allows the users to share their parameters with **authenticated** messages would be more secure as well as avoiding the server from saving the keys.
- Countermeasure for Attack 2:

  To avoid this attack having a larger-sized key would suffice. Currently, the considered secure schemes use keys of at least 1024 bits.

  Also, nonces should not be sent plainly and should be sent encrypted with the pk.