Protocols safety project
Déclaration d'attaque sur le protocole HKT.2
Attack 2

Ambroise Baudot, Marceau Dida, Louise Pount

January 27, 2020

Overview The following scenario follows the protocol presented as the HKT v.2 protocol. The broken property is the confidentiality (secret of the key).

Broken property:
Confidentiality: *Only A and B know the generated session key* nonce. *Additionally, even if some-one registers to the server with either A's or B's public key, such correspondentwill fail to append into the handshake message "hello".*

0. We can assume that C has initiated a session with A *via* S and has exchanged messages `1.` and `2.` of the protocol.

1. $A \rightarrow S : B,\{A\}_{pub(B)}$
2. $S \rightarrow B : \{\{\mathrm{A}\}_{pub(B)}\}_{K_{BS}}$
3. $C \rightarrow S : \{\mathrm{A},\{\mathrm{N}_C\}_{pub(A)}\}_{K_{CS}}$
4. $S \rightarrow A : \{\{\mathrm{N}_C\}_{pub(A)}\}_{K_{AS}}$
5. $A \rightarrow B : \{"hello"\}_{N_C}$
6. C: $dec(\{"hello"\}_{N_C})$

7. B tries to conclude the session (initiated by S at message `2.`) of the scenario above, without any effect (because C introduced itself into the protocol and has taken the initiative of the following messages).

Role played by C : Assuming C knows that A want to talk with B. The session is initiated by A. C wait until S send the message to B. Then C send the third message to S and take the initiative for the following of the protocol. If C shares a symmetric key with the server, then S sends the final message. The nonce is choosen by C, and A "understand" this message as the key choosen by B. Indeed, in your protocol and your confidentiality query, that seems correspond to the key required by the subject which must be exchanged between A and B. The following of B's protocol is aborted but neither S nor A know that.

Then, C spy the next message, which is from A to B, and can decrypt it. So the **confidentialty** property is broken and that is the conclusion of the attack.