Protocols safety project
Déclaration d'attaque sur le protocole HKT.2
Attack 1

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 authentication.

Broken property:
Mutual authentication: *Both A and B can assume to be talking to each other, since the correspondent is able to append into the encrypted payload.*

1. $A \rightarrow S : B,\{A\}_{pub(B)}$
2. $S \rightarrow B : \{\{\mathrm{A}\}_{pub(B)}\}_{K_{BS}}$
3. $C \rightarrow S : \{A,\{\mathrm{nonce}_C\}_{pub(A)}\}_{K_{CS}}$
4. $S \rightarrow A : \{\{\mathrm{nonce}_C\}_{pub(A)}\}_{K_{AS}}$

Role played by C : Assuming C knows that A want to talk with B. C wait until S send the message to B. Then C send the third message to S. If C shares a symmetric key with the server, then S sends the final message. A think it comes from B and C so the authentification proporty is broken.
So C **impersonates** B, which is the conclusion and at this step the **authentication property** is violated.