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

Ambroise BAUDOT, Marceau DIDA, Louise POUNT

January 31, 2020

Overview The following scenario follows the protocol presented as the ABT v.2 protocol. The broken property is the authentication.

Broken property:
Authentication: *B knows that he's talking to agent A when at the final step he receives the nonce N_B encrypted by K_{AB}. Because S and B were the only one to know N_B and S share it with A so B can trust A.*

1. $C \rightarrow S : C,\ \{B\}_{K_{CS}}$
2. $S \rightarrow ...B : C,\{N_C\}_{pk_B}$ ×[interception by C]
   C(S) $\rightarrow B : A,\{N_C\}_{pk_B}$
3. $B \rightarrow S : \{N_C\}_{K_{BS}}$
4. $S \rightarrow C : \{\langle\langle\{\mathrm{K}\}_{K_{BS}}, \mathrm{K}\ \rangle, N_C\rangle\}_{K_{CS}}$
5. $C(A) \rightarrow B : \{K\}_{K_{BS}},\ \{N_C\}_K$

Role played by C : B has only one way to be sure that he's indeed talking to A, that is the presence of A in the message at the step 2 of your protocol. C can still impersonate A, as described in our attack before the correction (scenario described by e-mail), and for this attack to be valid, it still initiates a session with S to talk to B, and intercepts the message 2 and modifies it before to "forward" the new message to B, where C has been replaced by B. So, the **property of authentication**, is violated.

***Nota Bene*:** From the point of view of C, B is talking to C.