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

Ambroise Baudot, Marceau Dida, Louise Pount

January 27, 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 atthe finalstep 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. $A \rightarrow S : A, \{B\}_{K_{AS}}$
2. $C(S) \rightarrow B : \{N_C\}_{pk_B}$
3. $B \rightarrow S : \{N_C\}_{K_{BS}}$
4. $S \rightarrow A :$ *id.* as the 4^{th} message of the original protocol.
5. $A \rightarrow B :$ *id.* as the 5^{th} message of the original protocol.

Role played by C : There is no proof that the 2^{nd} message is really from S. Here, C impersonates S. This formulation of the scenario is indeed a shortcut for all the process. In practice, the message from S to B ($N_{B_{pk_B}}$) will be ignored by B, as B has already received the following of the process, C having taken the initiative with its message. However, you have specified in your query: "S and B were the only one to know N_B". So, the **property of confidentiality is broken**, N_B being known to C.