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

Ambroise Baudot, Marceau Dida, Louise Pount

January 27, 2020

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

Broken property:
Mutual-Authentication: *A must trust B as indeed being B and B must trust A as indeed being A.*

1. $A \rightarrow S : A,\{< A, B >\}_{K_{AS}}$
2. $A \rightarrow B : A$
3. $B \rightarrow S : B,\{< B, A >\}_{K_{BS}}$
4. $S \rightarrow A : \{< K, B >\}_{K_{AS}}$
5. $S \rightarrow B : \{< K, A >\}_{K_{BS}}$
   ==========
   — NEW SESSION —
   ==========
6. $C(A) \rightarrow S : A,\{< A, B >\}_{K_{AS}}$
7. $C(A) \rightarrow B : A$
8. $B \rightarrow S : B,\{< B, A >\}_{K_{BS}}$
9. $S \rightarrow A : \{< K, B >\}_{K_{AS}}$
10. $S \rightarrow B : \{< K, A >\}_{K_{BS}}$

Role played by C : C start a fresh session using the same first message as A in the previous one. Then the server S thinks it has come from A and continue the protocol as if it was the case. B, who have received both the identity of A (from C) and the message from the server have no doubt that is talking to A. When S will send the 9th message to A, she will ignore it because she has already received it at the end of the preceding session. Then, even if C doesn't

know the secret key K, B will think is talking to A whereas is talking to C. As A is passive during the two last messages of the protocol, messages 9 and 10, event sent to the good host (A and not C), that as no effect. Then, the **mutual-authentication** property is broken.