Projet de sécurité des protocoles
Déclaration d'attaque sur le protocole FP.2
Attaque 1.2

Ambroise Baudot, Marceau Dida, Louise Pount

February 4, 2020

Overview The following scenario follows the protocol presented in the FP2 protocol. The broken property is the mutual-authentication.

1. $C(A) \rightarrow B : \{\langle A, N_C \rangle\}_{pk_B}$
2. $B \rightarrow C \times ...A : B$, $\{\langle A, N_B \rangle\}_{K_{BS}}$ (interception by C)
   Abortion of the protocol responder (for instance with a reply of C, $\{N\}_{pk_B}$ which is *a priori* a false value, that implies the halting of the process)
3. $C(B) \rightarrow S : B$, $\{\langle A, N_B \rangle\}_{K_{BS}}$
4. $S \rightarrow C \times ...A : \{\langle B, N_B \rangle\}_{K_{AS}}$ (interception by C)

   `"real" session`.
5. $A \rightarrow C \times ...B : \{\langle A, N_A \rangle\}_{pk_B}$ (interception by C)
6. $C(S) \rightarrow A : \{\langle B, N_B \rangle\}_{K_{AS}}$
7. $A \rightarrow C \times ...B : \{N_B\}_{pk_B}$ (interception by C)

Notation: In order to help your understanding of this attack, we have changed our notations and then we use the following ones:

- $X(Y) \rightarrow$ means "X which impersonates Y"
- $\rightarrow X \times ...Y$ means "following your protocol, the message should be sent to Y, but X intercepts it.

Remarks

- The messages are written in the **chronological order**.
- The recipients (resp. authors) of messages $\{2, 4, 5, 7\}$ (resp. $\{1, 3, 6\}$) is an **interpretation**. You can consider that for each message the recipient is actually the channel (*i.e.* the attacker, which could be a good hypothesis).
- The above remark justifies the notations defined and used in these specific messages.

Conclusion: At the final step, the property of mutual-authentication is violated.