Projet de sécurité des protocoles
Déclaration d'attaque sur le protocole FP.2
Attaque 1

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.

(i) 1^{st} `SESSION`

(a) $C(A) \rightarrow B : \{\langle A, N_0 \rangle\}_{pk_B}$

(b) $B \rightarrow A - C : B, \{\langle A, N_0 \rangle\}_B$

(ii) 2^{nd} `SESSION`

(a) $C(B) \rightarrow S : B, \{\langle A, N_0 \rangle\}_{K_{BS}}$

(b) $S \rightarrow B - C : \{\langle B, N_0 \rangle\}_{K_{AS}}$
At this step, the process B is not useful anymore.

(iii) 3^{rd} `SESSION`

(a) $A \rightarrow B - C : \{\langle A, N_A \rangle\}_{pk_B}$

(b) $C(S) \rightarrow A : \{\langle B, N_0 \rangle\}_{K_{AS}}$

Notation: In order to help your understanding of this attack, we use the following notations

- $X(Y) \rightarrow$ means "from X, which impersonates Y"
- $\rightarrow X - Y$ means "to X but intercepted by Y in the case of this attack

Important *Nota Bene*: Theses messages are **not necessarily presented in the chronological order**, but are grouped by session, to highlight the Independence of each process. Another way to understand this scenario is, for instance, to see the scenario like that:

- First, A wants to communicate with B and initiates a session (iii.a).
- Then, C intercepts the message, and plays the role of A with B, thats are the messages i.a (C impersonates A) and i.b (reply of B).
- Then, C intercepted this last message (i.b) etc.

Conclusion: At the final step, B has impersonated A, and what's more, has chosen N_B. Otherwise, we have called N_0 the nonce, which could have been called N_C in the message $i.a$, or N_B in the message $iii.b$... At the message $iii.c$ (not explicitly written, but obviously the end of the process of A, when A puts on the channel N_{0pk_B}), C has effectively impersonated B. So the property of mutual-authentication is violated.