

Projet de sécurité des protocoles

Déclaration d'attaque sur le protocole KWZ.2

Attaque 1

Ambroise BAUDOT, Marceau DIDA, Louise POUNT

February 4, 2020

Overview The following scenario follows the protocol presented in the KWZ v.2 protocol. The broken property is the mutual-authentication.

1. $A \rightarrow C : \{\langle A, \{N_A\}_{K_{AS}} \rangle\}_{pk_C}$
2. $C(A) \rightarrow B : \{\langle A, \{N_A\}_{K_{AS}} \rangle\}_{pk_B}$
3. $B \rightarrow S : B, \{\langle A, \{\{N_A\}_{K_{AS}}, N_B \rangle\}\}_{K_{BS}}$
4. $S \rightarrow B - C : \{\langle K, A \rangle\}_{K_{BS}}$
5. $S \rightarrow A - C : \{\langle K, \langle N_B, N_A \rangle \rangle\}_{K_{BS}}$
6. $C(S) \rightarrow A : \{\langle K, \langle N_B, N_A \rangle \rangle\}_{K_{BS}}$
7. $A \rightarrow C - A : \{N_B\}_K$
8. $C(S) \rightarrow B : \{\langle K, A \rangle\}_{K_{BS}}$
9. $C(A) \rightarrow B : \{N_B\}_K$

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

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

Nota Bene: These messages are presented in the chronological order.

Conclusion: Having a global view of the scenario, following your protocol, it is seen that A initiates the protocol in order to talk to C , and B (here, "responder") to talk to A . However, at the final step, the "connection" is established between these two hosts, and A talks to B . That is why we claim that the property of **mutual-authentication** is violated. Indeed, to help your understanding of the reason of this attack, you can see that A , once he has sent its first message, has no way to ensure that it is really talking to B .