Security Protocols and Verification

Attack of Cryptographic Protocols

Garance Frolla
Ely Marthouret
Ewan Decima

Team: **ASKO OM8464A2**

September / November 2025

Contents

1 Attack on BitSentinel V3

We present an attack where an intruder I exploits the fact that A is an *hash oracle*: for a given encrypted nonce, A give us the nonce digest.

1. $I(A) \rightarrow B : \{N_I\}_{pub(B)}\{K_I\}_{pub(B)}, A$
2. $B \rightarrow I(A) : \{|\{|N_I|\}_{N_I}|\}_{K_I}, N_{B_{pub(A)}}, B$
3. $I \rightarrow A :$ "Send a request to initiate the protocol"
4. $A \rightarrow I : \{N'_A\}_{pub(I)}, \{K'\}_{pub(I)}, I$
5. $I \rightarrow A : \{|\{|N'_A|\}_{N'_A}|\}_{K'}\{N_B\}_{pub(A)}, I$
6. $A \rightarrow H(N_B)$
7. $I(A) \rightarrow B : H(N_B)$

2 Description

- **Message 1:** The intruder I impersonates A and craft a correct message and sends it to A. A thinks that B sends a legitimate message.
- **Message 2:** B sends a legitimate respond to A, but I intercepts this answer and store $N_{B_{pub(A)}}$ for later. At this point, $\mathcal{K}_I = \{K(\{N_B\}_{pub(A)})\}$.
- **Message 3:** I sends a request to A. I demands to A to initiate the key exchange protocol.
- **Message 4:** A start a legitimate key exchange protocol with I.
- **Message 5:** I answers to A, but instead of creating a new fresh nonce he uses the stored $\{N_B\}_{pub(A)}$ from the session between $I(A)$ and B.
- **Message 6:** A still thinks that the communication is legit and sends back to B the digest that I needs to finis the attack. At this point $\mathcal{K}_I = \{K(\{N_B\}_{pub(A)}), K(H(N_B))\}$.
- **Message 7:** Finally I sends to B his hashed nonce.

3 Attack Results

While the messages are correctly encrypted and appear authentic, B incorrectly believes they are establishing a new session with A. In reality, B is speaking with I.