Security Protocols and Verification

Attack of Cryptographic Protocols

Garance Frolla
Ely Marthouret
Ewan Decima

Team: **ASKO OM8464A2**

September / November 2025

Contents

1 Attack on Bourget-Saunier-Werck

We present a replay attack where an intruder I exploits the lack of freshness verification in the protocol. The attack uses previously captured session values:

1. $I(A) \rightarrow S : A, \{|B, N_A^*, \{K^*\}_{pub(B)}|\}_{K_{AS}}$
2. $S \rightarrow B : \{|A, N_A^*, \{K^*\}_{pub(B)}|\}_{K_{BS}}$
3. $B \rightarrow I(A) : B, \{|ACK|\}_{K^*}$

Where K^* and N_A^* are old values from a previous legitimate session that the intruder has captured and knows.

2 Attack Description

2.1 Attack Flow

- **Message 1: Message Replay**

  The intruder I replays the exact message previously sent by A to the server S. Since this message is properly encrypted with K_{AS} and contains all required fields, the server S cannot distinguish it from a fresh, legitimate request.

  $$I(A) \rightarrow S : A, \{|B, N_A^*, \{K^*\}_{pub(B)}|\}_{K_{AS}}$$

  The server S decrypts this message and believes it is receiving a new session establishment request from A.

- **Message 2: Server Forwarding**

  The server S, finding the message well-formed and properly authenticated, forwards it to B:

  $$S \rightarrow B : \{|A, N_A^*, \{K^*\}_{pub(B)}|\}_{K_{BS}}$$

  Participant B decrypts the message using K_{BS}, extracts $\{K^*\}_{pub(B)}$, and decrypts it with their private key to obtain K^*.

- **Message 3: Acknowledgment Interception**

  B, believing they are establishing a fresh session with A, sends an acknowledgment encrypted with the session key K^*:

  $$B \to I(A) : B, \{|ACK|\}_{K^*}$$

  Since I knows K^*, they can decrypt this acknowledgment and verify that B has accepted the replayed session.

2.2 Attack Results

This replay attack successfully violates several critical security properties:

- **Freshness:** The protocol fails to ensure that messages are fresh. The server S accepts and processes replayed messages without detecting that they are from an old session.
- **Authentication** While the messages are correctly encrypted and appear authentic, B incorrectly believes they are establishing a new session with A. In reality, A is not participating in this session at all.
- **Key Establishment** B accepts an old, potentially compromised session key K^* as if it were freshly generated, violating the principle of key freshness.
- **Non-repudiation** A can later deny having initiated this session, since they did not actually send the replayed message during this time period.