Security Protocols and Verification

Defense of Cryptographic Protocol

Garance Frolla
Ely Marthouret
Ewan Decima

Team: **ASKO OM8464A2**

September / November 2025

Contents

1 Defense against PROTOxyde d'alCOl

1.1 Notation

- Let $\mathcal{K}_I$ denote the set of all facts known to the intruder I.
- Let $\big(K_I\big)_{I\in\mathcal{I}}$ the set of key use by I during the *bruteforce* step.
- Let $\mathcal{M}$ denote the set of all messages sent during a communication between to agents.
- Let $M_{1,A} \in \mathcal{M}$ denote the first message sends by Alice, i.e., $M_{1,A} = \{|\langle A, N_A\rangle|\}_{K_{AB}}$
- Let $s(\cdot,\cdot)$ denote the sender function, i.e., $s(m,x)$ means message M is sent by agent C.
- Let $[\cdot]_{(\cdot)}$ denote the extract function of a tuple message, i.e., for $M = \langle m_1, m2, ..., m_n\rangle \in \mathcal{M}$, $[M]_i = m_i \quad \forall i \in [|1,n|]$.
- Let $\langle X', Y', Z', \Sigma'\rangle$ denote four random value.

1.2 The attack

- First this our understanding of your attack : the intruder I steal the first alice's message : $M_{1,A}$. At this step $K(N_A) \notin \mathcal{K}_I$ and $K\big(K_{AB}\big) \notin \mathcal{K}_I$.
- After that, I impersonates S by crafting the ticket $\{|\langle A, \tau, \lambda, K_{AB}\rangle|\}_{K_{BS}}$, replacing K_{BS} with keys K_I to form $T_I := \{|\langle X', Y', Z', \Sigma'\rangle|\}_{K_I}$ and sending $M_{1,A}$ and T_I to B.
- B gets $M_{1,A}$. At this point $K\big(S(M_{1,A}, A)\big) \notin \mathcal{K}_B$. But it's normal according to the ASKO OM8464A2 protocol. Then B gets the crafted ticket T_I. B will decipher it with K_{BS} and send back to $[dec(T_I, K_{BS})]_1$

$$\Big\{\Big|dec\big(\{|N_A+1|\}_{KAB}, [dec(T_I,K_{BS})]_4\big)\Big|\Big\}_{[dec(T_I,K_{BS})]_4}$$

For better understanding, let us denote $[dec(T_I, K_{BS})]_1$, $[dec(T_I, K_{BS})]_2$, $[dec(T_I, K_{BS})]_3$, $[dec(T_I, K_{BS})]_4$ as X, Y, Z, Σ respectively.

- The attack lies on the fact that identities are short bitstring, B will always decipher the ticket T_I with his symmetric key K_{BS}, and hoping that:

$$\exists\, J \in \mathcal{I}\,|J \neq BS \wedge\ dec(T_J, K_{BS}) = \langle A, Y, Z, \Sigma\rangle.$$

  With such a key K_J, B will think that Σ is K_{AB}. At this point $K\big(\Sigma\big) \notin \mathcal{K}_I$ and $K\big(K_J\big) \notin \mathcal{K}_I$.

1.3 Refutation

2 Conclusion