Security and Privacy, Blatt 1

Franziska Hutter (3295896)
Felix Truger (3331705)
Felix Bühler (2973410)

15. Mai 2018

Problem 1: Specification of Protocols

Formal specification of the Woo and Lam Mutual Authentication Protocol:

P = ($\{\Pi_1, \Pi_2, \Pi_3\}$, $\mathcal{W}$)

with

$\mathcal{W}$ = {A, B, S}

$\Pi_1 = \Pi_A^{i,B} =$

1. $B \rightarrow \langle A, N_A \rangle$
2. $\langle B, x_1 \rangle \rightarrow \{\langle A, \langle B, \langle N_A, x_1 \rangle\rangle\rangle\}_{K_{AS}}^s$
3. $\{\langle B, \langle N_A, \langle x_1, x_2 \rangle\rangle\rangle\}_{K_{AS}}^s, \{\langle N_A, x_1 \rangle\}_{x_2}^s \rightarrow \{x_1\}_{x_2}^s$

$\Pi_2 = \Pi_B^{r,A} =$

1. $\langle A, x_3 \rangle \rightarrow \langle B, N_B \rangle$
2. $x_{11} \rightarrow x_{12}, \{\langle x_3, N_B \rangle\}_{K_{AB}}^s$
3. $\{N_B\}_{K_{AB}}^s \rightarrow \{secret\}_{K_{AB}}^s$

$\Pi_3 = \Pi_B^{i,S} =$

1. $S \rightarrow x_{11}, \{\langle A, \langle B, \langle x_4, N_B \rangle\rangle\rangle\}_{K_{BS}}^s$

$\Pi_4 = \Pi_S^{r,B} =$

1. $\{\langle A, \langle B, \langle x_5, x_6 \rangle\rangle\rangle\}_{K_{AS}}^s, \{\langle A, \langle B, \langle x_5, x_6 \rangle\rangle\rangle\}_{K_{BS}}^s$
   $\rightarrow \{\langle B, \langle x_5, \langle x_6, K_{AB} \rangle\rangle\rangle\}_{K_{AS}}^s, \{\langle A, \langle x_5, \langle x_6, K_{AB} \rangle\rangle\rangle\}_{K_{BS}}^s$

with x_i, $i \in \mathbb{N}$ being variables.

Problem 2: Attacks on Protocols

Formal description of an attack on the Woo and Lam Mutual Authentication Protocol:

Protocol P = $(\{\Pi_1, ..., \Pi_n\}, \mathcal{W}), n \in \{1, ..., 7\}$

with

$\mathcal{W} = \{\text{I, A, B, S, } K_{IS}\}$

$\Pi_i = \Pi_j$ as described in problem 1 for $i, j \in \{1, 2, 3, 4\} \wedge i = j$

$\Pi_5 = \Pi_A^{i,B} =$

1. $B \rightarrow \langle A, N'_A \rangle$
2. $\langle B, x_7 \rangle \rightarrow \{\langle A, \langle B, \langle N'_A, x_7 \rangle\rangle\rangle\}^s_{K_{AS}}$
3. $\{\langle B, \langle N'_A, \langle x_7, x_8 \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle N'_A, x_7 \rangle\}^s_{x_8} \rightarrow \{x_7\}^s_y$

$\Pi_6 = \Pi_B^{r,A} =$

1. $\langle A, x_9 \rangle \rightarrow \langle B, N'_B \rangle$
2. $x_{14} \rightarrow x_{15}, \{\langle x_9, N'_B \rangle\}^s_{K_{AB}}$
3. $\{N'_B\}^s_{K_{AB}} \rightarrow \{secret\}^s_{K_{AB}}$

$\Pi_7 = \Pi_B^{i,S} =$

1. $S \rightarrow x_{14}, \{\langle A, \langle B, \langle x_{10}, N'_B \rangle\rangle\rangle\}^s_{K_{BS}}$

where Π_5 through Π_7 ressemble the second session of the protocol

Attack $\mathcal{A}_{WLMAP} = (\pi, \sigma)$

with

π = the execution ordering for P = (1, 2, 1, 3, 5, 6, 5, 7, 4, 2, 1, 2)

and

$\sigma = \{x_1 \mapsto N_B, x_2 \mapsto K_{AB}, x_3 \mapsto N_A, x_4 \mapsto N_A, x_5 \mapsto N_A, x_6 \mapsto N_B, x_7 \mapsto N'_B, x_8 \mapsto K'_{AB}, x_9 \mapsto N'_A, x_{10} \mapsto N'_A, x_{11} \mapsto \{\langle A, \langle B, \langle N_A, N_B\rangle\rangle\rangle\}^s_{K_{AS}}, x_{12} \mapsto \{\langle B, \langle N_A, \langle N_B, K_{AB}\rangle\rangle\rangle\}^s_{K_{AS}}, x_{14} \mapsto \{\langle A, \langle B, \langle N'_A, N'_B\rangle\rangle\rangle\}^s_{K_{AS}}\}$

Note: There is no substitution for x_{15}, because step 2 of Π_6 is never executed according to the execution ordering π.

The actual attack, as already described in Homework 0, is possible due to the intruder being able to impersonate A and S, and selecting N_A and N'_A arbitrarily. Furthermore, the key K_{AS} may be selected arbitrarily by the intruder, since he impersonates both users of the key and others can not verify the use of K_{AS}.

Problem 3: Security Proof by Hand

$\mathcal{W} = \{I, A, B\}$ (initial intruder knowledge). Let $\mathcal{L}$ be the set of messages, that the intruder could ever accumulate throughout the execution of P. $\mathcal{L} = \{\{K, A\}^s_{K_{AS}}, \{secret\}^s_K\}$.
Note: Since the intruder knows the rules of the protocol, he would be able to conclude that K is the key to decrypt the secret. The corresponding substitution is $\sigma = \{x \mapsto K\}$.
The *secret* would be revealed to the intruder if the following holds: $secret \in d(\mathcal{W} \cup \mathcal{L})$. Since $K_{AS} \notin (\mathcal{W} \cup \mathcal{L})$ and $K \notin (\mathcal{W} \cup \mathcal{L})$, not futher knowledge can be derived from $\mathcal{W} \cup \mathcal{L}$. Thus the given protocol is secure in terms of confidentiality – *secret* is never revealed to an intruder.
As for authentication, there is obviously no way for the intruder to impersonate any of the participants without knowledge of the symmetric key K_{AB}, which is necessary for both instances Π_1 and Π_2 to be properly executed.

Problem 4: AVISPA Tool: Woo and Lam Attack

See Ilias

Problem 5: AVISPA Tool: Woo and Lam Fix

See Ilias

Problem 6: Reduction from G3C

—