Security and Privacy,
Blatt 1

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

9. 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. $A \rightarrow \langle A, N_A \rangle$
2. $\langle B, x \rangle \rightarrow \{\langle A, \langle B, \langle N_A, x \rangle\rangle\rangle\}^s_{K_{AS}}$
3. $\{\langle B, \langle N_A, \langle x, y \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle N_A, x \rangle\}^s_y \rightarrow \{x\}^s_y$

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

1. $\langle A, x \rangle \rightarrow \langle B, N_B \rangle$
2. $\{\langle A, \langle B, \langle x, N_B \rangle\rangle\rangle\}^s_{K_{AS}} \rightarrow \{\langle B, \langle x, \langle N_B, K_{AB} \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle x, N_B \rangle\}^s_{K_{AB}}$
3. $\{N_B\}^s_{K_{AB}} \rightarrow \{secret\}^s_{K_{AB}}$

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

1. $B \rightarrow \{\langle A, \langle B, \langle x, N_B \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle A, \langle B, \langle x, N_B \rangle\rangle\rangle\}^s_{K_{BS}}$

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

1. $\{\langle A, \langle B, \langle x, y \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle A, \langle B, \langle x, y \rangle\rangle\rangle\}^s_{K_{BS}}$
   $\rightarrow \{\langle B, \langle x, \langle y, K_{AB} \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle A, \langle x, \langle y, K_{AB} \rangle\rangle\rangle\}^s_{K_{BS}}$

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

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

$\Pi_i = \Pi_j$ as described in problem 1 for $i, j \in \{1, 2, 3, 4\} \wedge i = j$ where both, the roles of A and S are performed by the Attacker I, denoted as I_A and I_S.

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

1. $A \to \langle A, N'_A \rangle$
2. $\langle B, x \rangle \to \{\langle A, \langle B, \langle N'_A, x \rangle\rangle\rangle\}^s_{K_{AS}}$
3. $\{\langle B, \langle N'_A, \langle x, y \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle N'_A, x \rangle\}^s_y \to \{x\}^s_y$

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

1. $\langle A, x \rangle \to \langle B, N'_B \rangle$
2. $\{\langle A, \langle B, \langle x, N'_B \rangle\rangle\rangle\}^s_{K_{AS}} \to \{\langle B, \langle x, \langle N'_B, K_{AB} \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle x, N'_B \rangle\}^s_{K_{AB}}$
3. $\{N'_B\}^s_{K_{AB}} \to \{secret\}^s_{K_{AB}}$

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

1. $B \to \{\langle A, \langle B, \langle x, N'_B \rangle\rangle\rangle\}^s_{K_{AS}}, \{\langle A, \langle B, \langle x, N'_B \rangle\rangle\rangle\}^s_{K_{BS}}$

where Π_5 through Π_7 ressemble the second session of the protocol

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

with

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

and

$\sigma =?$

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 will be able to conclude that K is the key to decrypt the secret.
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 that the secret is never revealed to the intruder.

Problem 4: AVISPA Tool: Woo and Lam Attack

Problem 5: AVISPA Tool: Woo and Lam Fix

Problem 6: Reduction from G3C