

Security and Privacy, Blatt 1

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

8. Mai 2018

Problem 1: Specification of Protocols

Formal specification of the Woo and Lam Mutual Authentication Protocol:

$$P = (\{\Pi_1, \Pi_2, \Pi_3, \Pi_4\}, \mathcal{W})$$

with

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

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

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

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

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

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

1. $B \rightarrow \{\langle A, \langle B, \langle x, N_B \rangle \rangle \rangle\}_{K_{AS}}^s, \{\langle A, \langle B, \langle x, N_B \rangle \rangle \rangle\}_{K_{BS}}^s$
2. $\{\langle B, \langle x, \langle N_B, y \rangle \rangle \rangle\}_{K_{AS}}^s, \{\langle A, \langle x, \langle N_B, y \rangle \rangle \rangle\}_{K_{BS}}^s$

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

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

Problem 2: Attacks on Protocols

Protocol $P = (\{\Pi_1, \dots, \Pi_n\}, \mathcal{W})$

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

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

with

π = the execution ordering for P =?

and

σ =?

Problem 3: Security Proof by Hand

Problem 4: AVISPA Tool: Woo and Lam Attack

Problem 5: AVISPA Tool: Woo and Lam Fix

Problem 6: Reduction from G3C