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 = ({Π_1, Π_2, Π_3, Π_4}, W)

with

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

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

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

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