Security and Privacy, Blatt 1

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

3. Mai 2018

Problem 1: Specification of Protocols

Formal specification of the Woo and Lam Mutual Authentication Protocol:

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

with

W = {A, B, S}

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

$\Pi_1 = \Pi_B^{r,A,S} = ?$

$\Pi_1 = \Pi_S^{i,A,B} = ?$

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