ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Ralf Sasse
January 2016

Verifying Security Protocols in Tamarin

Exercise Sheet 2

Assignment 2.1: Practical Tool Usage: NSPK

Understand the given NSPK specification. Fix it! (Hint: Use Lowe's fix.)

Assignment 2.2: Group Theory – Equational Proof

The theory of groups has an unsorted signature with a constant 1, a unary function $()^{-1}$ and a binary function $\circ$ and has the following equations G:

(1) $x \circ 1 = x$

(2) $x \circ (y \circ z) = (x \circ y) \circ z$

(3) $x \circ (x)^{-1} = 1$

Give G-equality proofs for the following theorems of Group Theory:

(4) $1 \circ x = x$

(5) $(x)^{-1} \circ x = 1$

(6) $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$

(Hint: Note that you can use any theorem you already proved as lemma to help in the remaining proofs.)

Assignment 2.3: Unification

(This exercise is modified from Term Rewriting and All That by F. Baader and T. Nipkow.)

(1) Solve the following syntactic unification problems. If there is no unifier, explain why.

(a) $f(x, y) \stackrel{?}{=} f(h(a), x)$

(b) $f(x, y) \stackrel{?}{=} f(h(x), x)$

(c) $f(x, b) \stackrel{?}{=} f(h(y), z)$

(d) $f(x, x) \stackrel{?}{=} f(h(y), y)$

(2) Now solve each of the above, modulo associativity-commutativity of f.

(3) Solve the matching problems, where $s <^? t$ means that t should match s, i.e., there is a substitution σ and position p so that $t|_p = s\sigma$.

Use the above unification problems, read as matching problems from left to right. You only need to consider the syntactic case, and the top position $p = [\,]$.

Assignment 2.4: Dolev-Yao intruder deductions

Consider the Dolev-Yao deduction rules from the lecture and the adversary knowledge

$$\mathcal{K} = \mathsf{K}(\{\!|k|\!\}_{h(n_1,n_2)}), \mathsf{K}(\{n_1\}_{\mathsf{pk}(ski)}), \mathsf{K}(\{\!|n_2|\!\}_{n_1}), \mathsf{K}(\mathsf{pk}(ska)), \mathsf{K}(\mathsf{pk}(ski)), \mathsf{K}(ski), \mathsf{K}(\{\!|secret|\!\}_k)$$

where $h \in \Sigma_p$ is a public function. Formally prove or disprove:

(a) $\mathsf{K}(secret)$

(b) $\mathsf{K}(\{secret\}_{ska})$

(c) $\mathsf{K}(\{\!|n_1|\!\}_{h(k,secret)})$

Note that you may omit the E annotated intermediate steps.

Assignment 2.5: Algebraic Operators

The *free algebra assumption* that syntactically different terms denote different messages is an assumption that is known to be non attack preserving. This arises because cryptographic functions, for example XOR ($\oplus$), have algebraic properties that the free algebra assumption ignores. $\oplus$, for instance, is associative, commutative, and has the cancellation property that $X \oplus X = 0$.

Consider the following modified version of the Needham-Schroeder-Lowe protocol which uses $\oplus$:

$$\begin{array}{lll} 1. & A \to B: & \{N_A, A\}_{K_B} \\ 2. & B \to A: & \{N_B, N_A \oplus B\}_{K_A} \\ 3. & A \to B: & \{N_B\}_{K_B} \end{array}$$

Show that the free algebra assumption is non attack preserving by finding an attack on this protocol that exploits the algebraic properties of $\oplus$ and would therefore be excluded when assuming a free algebra. (*Hint:* The structure of the attack is similar to the standard attack on NSPK. Assume the goal is to keep N_B secret from the intruder and that there is an instance of A who wants to initiate a session with I.)