ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

S. Mödersheim
Ch. Sprenger
AS 2009

Formal Methods for Information Security

Exercise Sheet 3

Hand-in date: Oct 19, 2009

Assignment 3.1: Station-to-station protocol

The Station-to-station (STS) protocol is specified as follows:

$$\begin{array}{ll} A \to B: & \exp(g, X) \\ B \to A: & \exp(g, Y), \{|\{\exp(g, Y), \exp(g, X), A\}_{\mathsf{inv}(\mathsf{pk}(B))}|\}_{K_{AB}} \\ A \to B: & \{|\{\exp(g, X), \exp(g, Y), B\}_{\mathsf{inv}(\mathsf{pk}(A))}|\}_{K_{AB}} \end{array}$$

where $K_{AB} = \exp(\exp(g, X), Y)$ is the derived shared key. We want to verify that the term $\exp(\exp(g, X), Y)$ is a secret shared by A and B. In OFMC (latest verion "2009b"), there are two ways to specify that a message M is secret between A and B:

- In "classical" notation: `M secret between A, B` from both A and B's point of view, and
- In channel notation: `A ->* B : M` (from A's point of view) and `B ->* A : M` (from B's point of view).

However, there is a subtle difference between these two specifications. Whereas in the first case, the secrecy claim (signal) is placed at the latest possible point in the given role, in the second case, it is placed in the earliest possible position in the role.

(a) Formalize the STS protocol as an Alice&Bob specification in OFMC.

(b) Verify the protocol with each of the two secrecy claims and explain the difference.

Assignment 3.2: Semantics of Alice&Bob notation

The following protocol is an excerpt from a contract signing protocol by Asokan, Shoup, and Waidner:[1]

$$\begin{array}{lll} A \to B: & \{A, B, text, h(N_A)\}_{\mathsf{inv}(\mathsf{pk}(A))} & (= m_1) \\ B \to A: & \{\{A, B, text, h(N_A)\}_{\mathsf{inv}(\mathsf{pk}(A))}, h(N_B)\}_{\mathsf{inv}(\mathsf{pk}(B))} & (= m_2) \\ A \to B: & N_A & \\ B \to A: & N_B & \end{array}$$

[1] The full specification and the actual goal of this protocol are beyond the limitations of AnB notation. We consider only this excerpt as an exercise.

where $text$ is the text of the contract that is being signed and h is a public hash function. In the first round, the agents sign and countersign the contractual text and exchange their *public commitments* $h(N_A)$ and $h(N_B)$. In the second round, they exchange the corresponding secret commitments N_A and N_B. The main goal of the protocol is that at the end of the protocol run each participant is in possession of a *valid contract* of the form m_1, m_2, N_A, N_B.

Initially, role A knows A, B, the hash function h, pk and its own signing key, $\mathsf{inv}(\mathsf{pk}(A))$. The situation for B is analogous. For our purposes, we can consider $text$ as a nonce generated by A. Roles A and B also generate their respective secret commitments N_A and N_B.

(a) Translate the role A from Alice&Bob notation to a role script.

(b) Can you reformulate the result using pattern matching? Justify your answer.

(c) What is the initial knowledge of the intruder if we consider $Agent = \{a, b, i\}$?

Assignment 3.3: Intruder models

In the lecture, the receive transition rule was defined as follows:

$$\frac{th(tid) = \mathsf{rcv}(t) \cdot tl \qquad dom(\sigma) = vars(t) \qquad t\sigma \in \mathcal{DY}(IK)}{(tr, IK, th) \rightarrow (tr \cdot (tid, \mathsf{rcv}(t\sigma)), IK, th[tid \mapsto tl\sigma])}$$

(a) Modify this rule to model a passive attacker who only eavesdrops communication, but does not actively participate by modifying messages.

(b) Does your solution still allow replays?

(c) Under which assumptions may you restrict the message derivation rules for a passive intruder to destruction rules only (i.e., remove the Composition rule)?