ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

S. Mödersheim
Ch. Sprenger
AS 2009

Formal Methods for Information Security

Exercise Sheet 5

Hand-in date: Nov 2, 2009

Assignment 5.1: Intruder knowledge in abstracted NSL

Consider NSL, the Needham-Schroeder public-key protocol with Lowe's fix (i.e. with second message $\{NA, NB, B\}_{\mathsf{pk}(A)}$). Let us work with the abstraction where Alice creates NA as $na(A, B)$ and Bob creates NB as $nb(B, A)$. The set of nonces in this model is

$$\{ni\} \cup \{na(A, B) \mid A, B \in \texttt{Agent}\} \cup \{nb(B, A) \mid A, B \in \texttt{Agent}\}$$

where ni is a nonce that the intruder initially knows.

We consider to a typed model where variables of type agent and nonce can only be instantiated with values from the set of agents and nonces, respectively. Let the set of agents be $\texttt{Agent} = \{a, b, i\}$.

(a) Give the set of rules that describes all messages that the intruder can derive (in the style of module 6, slide 36). Note that only the nonces that an agent creates should be abstracted, while the nonces that the agent receives are not abstracted.

(b) List the entire intruder knowledge that the intruder can ever obtain—resticted to messages that some honest agent can obtain and submessages thereof. (In other words, ignore any uninteresting terms like $\langle i, \langle i, i\rangle\rangle$ that the intruder can construct.)

(c) Can we infer from this list that the nonces are secrets between the respective A and B?

Assignment 5.2: Authentication in abstracted NSL

Consider again the abstracted NSL protocol of the previous assignment and the following "attack" trace:

$$\begin{array}{ll}
a \to b: & \{na(a, b), a\}_{\mathsf{pk}(b)} \\
b \to a: & \{na(a, b), nb(b, a), b\}_{\mathsf{pk}(a)} \\
a \to b: & \{nb(b, a)\}_{\mathsf{pk}(a)} \\
i(a) \to b: & \{ni, a\}_{\mathsf{pk}(b)} \\
b \to i(a): & \{ni, nb(b, a), b\}_{\mathsf{pk}(a)} \\
i(a) \to b: & \{nb(b, a)\}_{\mathsf{pk}(a)}
\end{array}$$

(a) Which authentication/agreement goal that is violated by this trace? (Insert the corresponding signals into the role descriptions.)

(b) Does this attack trace have a counter-part in the concrete protocol model (without the abstraction)? Explain.

(c) (**For experts:)** What can we do about it?