ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

S. Mödersheim
Ch. Sprenger
AS 2009

# Formal Methods for Information Security

## Exercise Sheet 4

Hand-in date: Oct 26, 2009

## Assignment 4.1: Non-injective Agreement

Consider the two definitions of non-injective agreement from the lecture. The first defines $Agreement_{NI}(A, B, M)$ as the set of traces $tr$ satisfying

$$\begin{array}{l}\forall tid.\ (tid, \mathsf{sig}(commit_A, A, B, M)) \in set(tr) \wedge B \neq \mathsf{i} \\ \Rightarrow \exists tid'.\ (tid', \mathsf{sig}(running_B, B, A, M)) \in set(tr)\end{array}$$

The second one is based on the prefix relation $\sqsubseteq$ and defines $Agreement'_{NI}(A, B, M)$ as the set of traces $tr$ satisfying

$$\begin{array}{l}\forall tid, tr'.\ tr' \cdot (tid, \mathsf{sig}(commit_A, A, B, M)) \sqsubseteq tr \wedge B \neq \mathsf{i} \\ \Rightarrow \exists tid'.\ (tid', \mathsf{sig}(running_B, B, A, M)) \in set(tr')\end{array}$$

The second definition emphasizes the temporal ordering of the signals: the matching running signal must occur before the commit signal in a trace. The first one is a simplification where only the (unordered) set of events occurring on a trace is considered.

Convince yourself that the two definitions are equivalent, i.e.,

$$Tr \subseteq Agreement_{NI}(A, B, M) \text{ if and only if } Tr \subseteq Agreement'_{NI}(A, B, M)$$

where $Tr = traces(P, IK_0, th_0)$ is the set of traces generated by an arbitrary protocol $P$ from the initial state $([], IK_0, th_0)$.

**Hint:** The set if traces $Tr$ is closed under prefixes, i.e., whenever $tr \in Tr$ and $tr' \sqsubseteq tr$ then also $tr' \in Tr$.

## Assignment 4.2: The Lazy Intruder

Consider the constraint set:

$$\begin{array}{l}from(\ \langle i, N_A \rangle\ ;\ IK_0) \\ from(\ \langle b, \{\!|i, N'_A, N_B|\!\}_{\mathsf{sk}(b,s)} \rangle\ ;\ IK_1) \\ from(\ \langle \{\!|i, K_{AB}|\!\}_{\mathsf{sk}(b,s)}, \{\!|nb_1|\!\}_{K_{AB}} \rangle\ ;\ IK_2)\end{array}$$

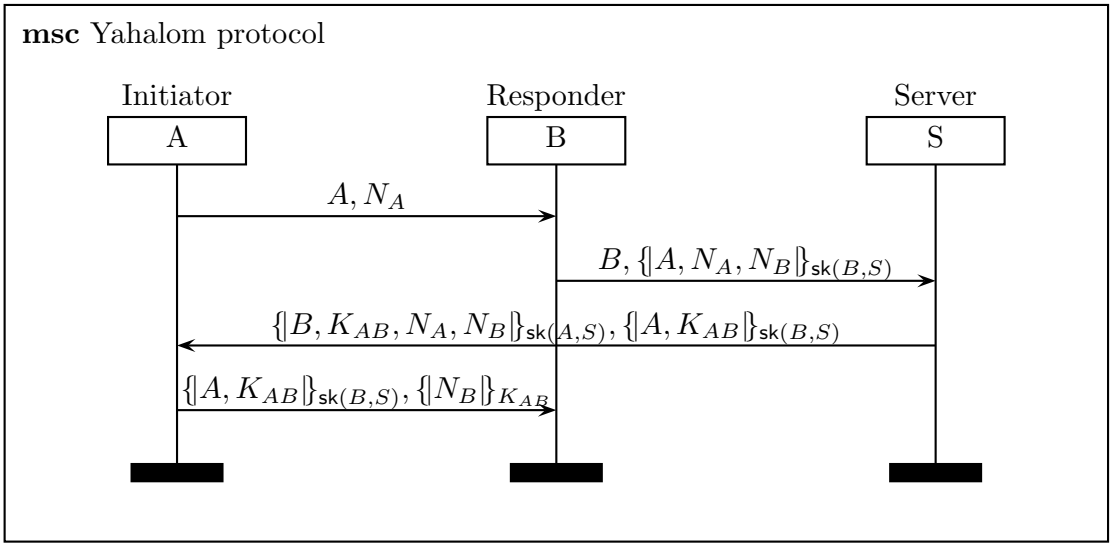
where

$$
\begin{aligned}
IK_0 &= \{a, b, s, i, \mathsf{sk}(i, s)\} \\
IK_1 &= IK_0 \cup \{\ \{|i, N_A, nb_1|\}_{\mathsf{sk}(b,s)}\ \} \\
IK_2 &= IK_1 \cup \{\ \{|b, kab_1, N'_A, N_B|\}_{\mathsf{sk}(i,s)}, \{|i, kab_1|\}_{\mathsf{sk}(b,s)}, kab_1, N'_A, N_B\}
\end{aligned}
$$

(a) Show that this constraint set together with the initial substitution $\sigma = [\,]$ is a satisfiable constraint store.

(b) Find *all* solutions of this constraint store using the composition and unify rules.

(c) Show that the above constraint store is induced by the Yahalom protocol if we instantiate $A$ with the intruder $i$, and $B$ and $S$ with the honest agents $b$ and $s$:[1]




**Hint:** Assume that the initial threads are closed, i.e., instantiated except for the bound variables just as in the ground semantics. Recall that the intruder does not instantiate roles and execute threads himself.

(d) Why is there both $N_A$ and $N'_A$ in the constraint store (i.e. why may these be different values)?

(e) Consider the goal $B$ weakly authenticates $S$ on $K_{AB}$. Show that this goal is violated by the trace resulting from one solution of the constraint store above.

[1] Since we have omitted the analysis rules of the lazy intruder in the lecture, we have already decomposed pairs and added the contents of all messages encrypted with $\mathsf{sk}(i, s)$ that the intruder can read to the respective intruder knowledges $IK_0$, $IK_1$ and $IK_2$.