Completeness of the Authentication Tests

Joshua D. Guttman
F. Javier Thayer
Shaddin F. Doghmi

September 2006

Supported by the National Security Agency
An Example: Yahalom’s Protocol

Slightly modified: $\{A, K\}_{KB}$ not forwarded via $A$
Yahalom Responder’s Guarantee: Idea

Assume $K_A^{-1}, K_b^{-1}$ non-originating

Does $K' = K$? Otherwise, must be another transforming edge, but no regular strand can transform $\{N_b\}_{K'}$ into $\{N_b\}_K$
Yahalom Responder’s Guarantee

\[ S_1 = \{ [B, K', N_a, N_b]_{K_A} : K' \text{ is a key} \} \cup \{ [A, N_a, N_b]_{K_B} \} \]

\[ S_2 = \{ [A, N_a, N_b]_{K_B} \} \]

Either \( K = K' \) or \( K \neq K' \)
Yahalom Initiator Guarantee

An incoming test on $N_a$ returning in safely encrypted form
The Incoming Test

Let $H : A_0 \leftrightarrow A_1$, where $A_1$ is realized. Let $n_1 \in A_0$ be a negative node and $\{ t_0 \}_K \sqsubseteq \text{term}(n_1)$. If $\{ t_0 \}_K$ originates nowhere in $A_0$, then either:

1. $H = H'' \circ H'$, where $H'$ is an incoming augmentation originating $\{ t_0 \}_K$; or
2. $K$ is compromised in $A_1$

There is a listener augmentation $H' : A_0 \leftrightarrow A_0'$ for $K$, and a homomorphism $H'' : A_0' \rightarrow A_1'$ such that:

(a) $A_1'$ is realized,
(b) $A_1' \sim_L A_1$, and
(c) $H'' \circ H' = I \circ H$, where $I$ is an inclusion homomorphism.
Some Definitions

- “Listener strand:” $\text{Lsn}[a]$
  - Regular strand
  - Single negative node $\neg a$

Certifies that $a$ is compromised

- “Listener Augmentation:”
  homomorphism that embeds $\mathbb{A}_0$
  in a skeleton also containing a listener strand
Defns: Skeleton

A four-tuple $A = (\text{nodes}, \preceq, \text{non}, \text{unique})$ is a *preskeleton* if:

1. nodes is a finite set of regular nodes; $n_1 \in \text{nodes}$ and $n_0 \Rightarrow^+ n_1$ implies $n_0 \in \text{nodes}$;
2. $\preceq$ is a partial ordering on nodes such that $n_0 \Rightarrow^+ n_1$ implies $n_0 \preceq n_1$;
3. non is a set of keys, and for all $K \in \text{non}$, either $K$ or $K^{-1}$ is used in nodes;
4. $3'$ for all $K \in \text{non}$, $K$ does not occur in nodes;
3. unique is a set of atoms, and for all $a \in \text{unique}$, $a$ occurs in nodes.

A preskeleton $A$ is a *skeleton* if in addition:

4. $a \in \text{unique}$ implies $a$ originates at no more than one node in nodes.
Defns: Homomorphism

Let $A_0, A_1$ be preskeletons, $\alpha$ a replacement, $\phi : \text{nodes}_{A_0} \rightarrow \text{nodes}_{A_1}$. 
$H = [\phi, \alpha]$ is a homomorphism if

1a. For all $n \in A_0$, $\text{term}(\phi(n)) = \text{term}(n) \cdot \alpha$;
1b. For all $s, i$, if $s \downarrow i \in A$ then there is an $s'$ s.t. for all $j \leq i$, $\phi(s \downarrow j) = (s', j)$;
2. $n \preceq_{A_0} m$ implies $\phi(n) \preceq_{A_1} \phi(m)$;
3. $\text{non}_{A_0} \cdot \alpha \subset \text{non}_{A_1}$;
4. $\text{unique}_{A_0} \cdot \alpha \subset \text{unique}_{A_1}$
Outgoing Augmentation

Let $H : \mathbb{A}_0 \mapsto \mathbb{A}_1$, with $\mathbb{A}_1$ realized.
Let $X$ be a set of keys, and
let $n_0, n_1 \in \mathbb{A}_0$ be an outgoing test pair for $a, S, X,$
for which $\mathbb{A}_0$ contains no transforming edge.
At least one of the following holds:

1. $H = H'' \circ H'$, where $H'$ is some outgoing augmentation for $a, S, X;$
2. $H = H'' \circ \text{hull}_\alpha(\mathbb{A}_0)$ for some contraction $\alpha;$
3. Some $K \in X$ is compromised in $\mathbb{A}_1$
   There is a listener augmentation $H' : \mathbb{A}_0 \mapsto \mathbb{A}'_0$ for some $K \in X,$ and
   a homomorphism $H'' : \mathbb{A}'_0 \mapsto \mathbb{A}'_1$ such that:
   (a) $\mathbb{A}'_1$ is realized,
   (b) $\mathbb{A}'_1 \sim_L \mathbb{A}_1$, and
   (c) $H'' \circ H' = I \circ H$, where $I$ is an inclusion homomorphism.
Defn: Shape (Minimal Realized Skeleton)

\( H : A_0 \mapsto A_1 \) is a shape for \( A_0 \) if \( A_1 \) is “nodewise minimal” among realized skeletons \( A' \) such that \( H = H_1 \circ H_0 \) where

1. \( H_0 : A_0 \mapsto A' \)
2. \( H_0 : A' \mapsto A_1 \)

\( A_0 \) is nodewise less than or equal to \( A_1 \) if for some \([\phi, \alpha] : A_0 \mapsto A_1\), \( \phi \) is injective.
Authentication Tests Completeness

Let $H : A_0 \mapsto A_1$ be a shape. $H = H_k \circ H_{k-1} \circ \ldots \circ H_1 \circ H_0$ for some sequence of homomorphisms $\{H_i\}_{0 \leq i \leq k}$, where:

1. $H_0$ is a node-surjective homomorphism from $A_0$ onto a substructure (possibly the identity); and
2. For each $i$ with $1 \leq i \leq k$, $H_i$ is a contraction or an augmentation as in Incoming and Outgoing Tests.
Main Lemma

Suppose there exists some $H : A \leftrightarrow A'$ where $A'$ is realized. If term($n$) is not penetrator-derivable before $n$ in $A$, then either:

1. $n$ is an incoming transformed node for some $K \in \text{non}_A \cup \text{unique}_A$; or else
2. $(m, n)$ is an outgoing transformed pair with respect to $a, S, X$ for
   (i) some $a \in \text{unique}_A$ originating at a node $m \in A$;
   (ii) some set $S$ of encrypted terms such that
        $a$ occurs only within $S$ in the nodes of $A$ below $n$; and
   (iii) some set of keys $X \subset \text{non}_A \cup \text{unique}_A$
        such that for each $K \in X$, $K^{-1}$ is used for encryption in support($n$).