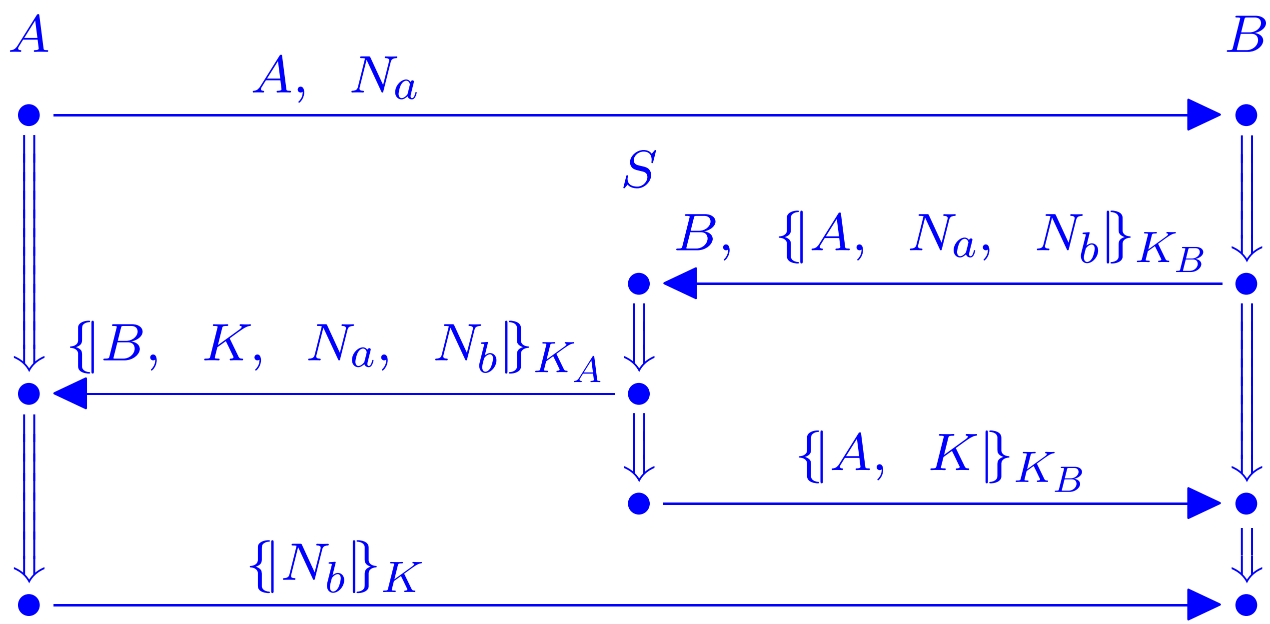
Completeness of the Authentication Tests

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

September 2006

Supported by the National Security Agency

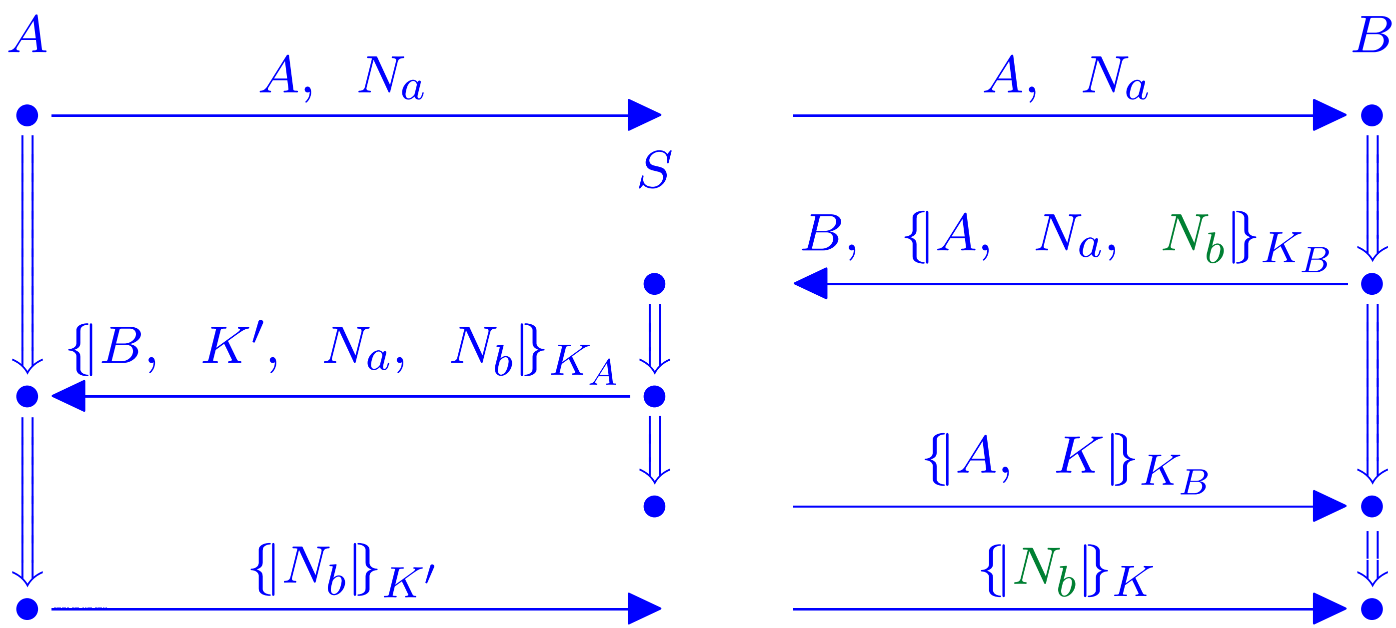
An Example: Yahalom's Protocol



Slightly modified: $\{\!|A, \ K|\!\}_{K_B}$ not forwarded via A

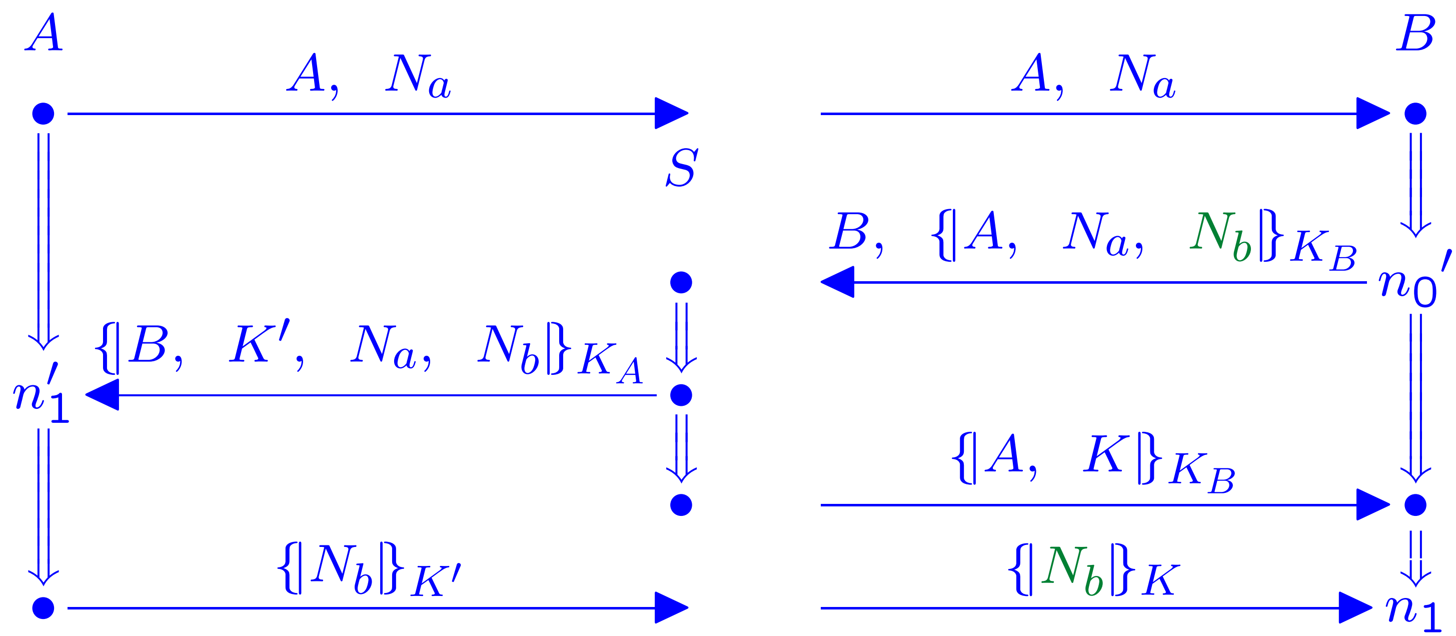
Yahalom Responder's Guarantee: Idea

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 Respondor's Guarantee

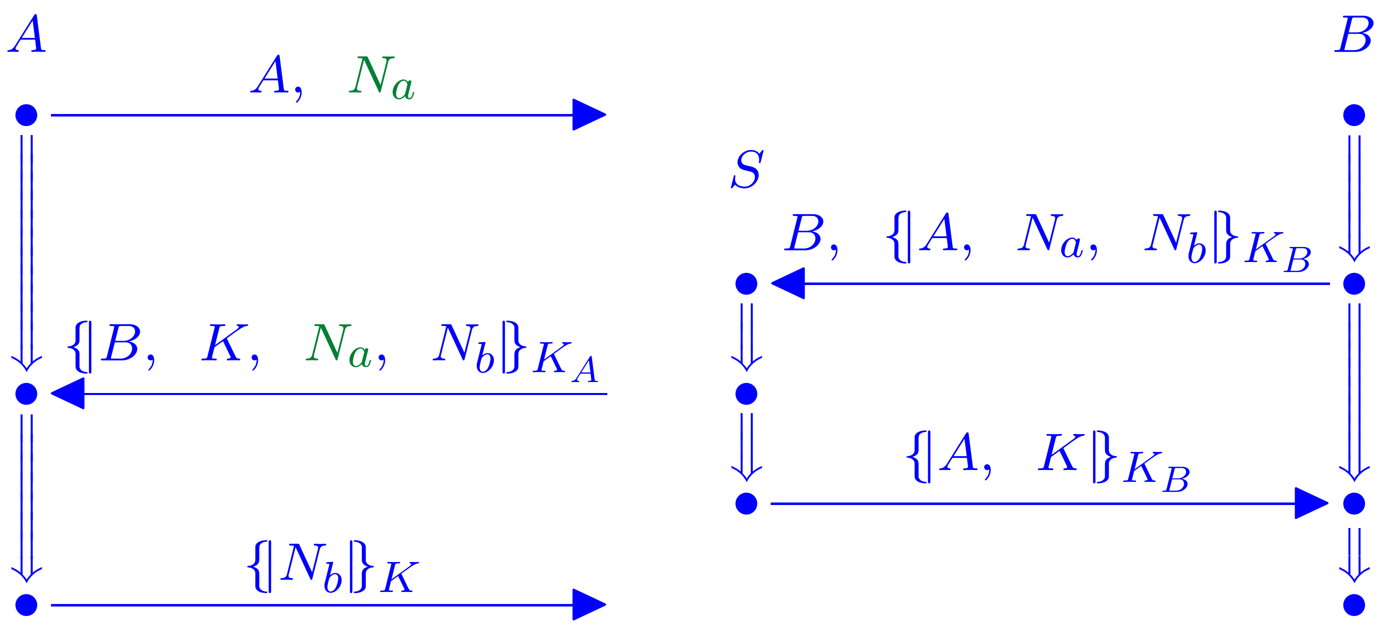


$$S_1 = \{\{\!|B, \ K', \ N_a, \ N_b|\!\}_{K_A} : K' \text{ is a key}\} \cup \{\{\!|A, \ N_a, \ N_b|\!\}_{K_B}\}$$

$$S_2 = \{\{\!|A, \ N_a, \ N_b|\!\}_{K_B}\}$$

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 $H : \mathbb{A}_0 \mapsto \mathbb{A}_1$, where $\mathbb{A}_1$ is realized. Let $n_1 \in \mathbb{A}_0$ be a negative node and $\{|t_0|\}_K \sqsubset \mathsf{term}(n_1)$. If $\{|t_0|\}_K$ originates nowhere in $\mathbb{A}_0$, then either:

1. $H = H'' \circ H'$,
   where H' is an incoming augmentation originating $\{|t_0|\}_K$; or
2. K is compromised in $\mathbb{A}_1$

   There is a listener augmentation $H' : \mathbb{A}_0 \mapsto \mathbb{A}'_0$ for K, and a homomorphism $H'' : \mathbb{A}'_0 \mapsto \mathbb{A}'_1$ such that:
   (a) $\mathbb{A}'_1$ is realized,
   (b) $\mathbb{A}'_1 \sim_{\mathsf{L}} \mathbb{A}_1$, and
   (c) $H'' \circ H' = I \circ H$, where I is an inclusion homomorphism.

Some Definitions

- "Listener strand:" Lsn[a]
  - Regular strand
  - Single negative node $-a$

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

1. nodes is a finite set of regular nodes; $n_1 \in$ nodes and $n_0 \Rightarrow^+ n_1$ implies $n_0 \in$ 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 $K \in$ non, either K or K^{-1} is used in nodes;

3′. for all $K \in$ non, K does not occur in nodes;

4. unique is a set of atoms, and for all $a \in$ unique, a occurs in nodes.

A preskeleton $\mathbb{A}$ is a *skeleton* if in addition:

4′. $a \in$ unique implies a originates at no more than one node in nodes.

Defns: Homomorphism

Let $\mathbb{A}_0, \mathbb{A}_1$ be preskeletons, α a replacement, $\phi\colon \text{nodes}_{\mathbb{A}_0} \longrightarrow \text{nodes}_{\mathbb{A}_1}$.
$H = [\phi, \alpha]$ is a *homomorphism* if

1a. For all $n \in \mathbb{A}_0$, $\text{term}(\phi(n)) = \text{term}(n) \cdot \alpha$;

1b. For all s, i, if $s \downarrow i \in \mathbb{A}$
then there is an s' s.t. for all $j \leq i$, $\phi(s \downarrow j) = (s', j)$;

2. $n \preceq_{\mathbb{A}_0} m$ implies $\phi(n) \preceq_{\mathbb{A}_1} \phi(m)$;
3. $\text{non}_{\mathbb{A}_0} \cdot \alpha \subset \text{non}_{\mathbb{A}_1}$;
4. $\text{unique}_{\mathbb{A}_0} \cdot \alpha \subset \text{unique}_{\mathbb{A}_1}$

Outgoing Augmentation

Let $H \colon \mathbb{A}_0 \mapsto \mathbb{A}_1$, 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. $H = H'' \circ \mathrm{hull}_\alpha(\mathbb{A}_0)$ for some contraction α;
3. Some $K \in X$ is compromised in $\mathbb{A}_1$

   There is a listener augmentation $H' \colon \mathbb{A}_0 \mapsto \mathbb{A}'_0$ for some $K \in X$, and a homomorphism $H'' \colon \mathbb{A}'_0 \mapsto \mathbb{A}'_1$ such that:
   (a) $\mathbb{A}'_1$ is realized,
   (b) $\mathbb{A}'_1 \sim_{\mathsf{L}} \mathbb{A}_1$, and
   (c) $H'' \circ H' = I \circ H$, where I is an inclusion homomorphism.

Defn: Shape (Minimal Realized Skeleton)

$H : \mathbb{A}_0 \mapsto \mathbb{A}_1$ is a *shape for* $\mathbb{A}_0$ if $\mathbb{A}_1$ is "nodewise minimal" among realized skeletons $\mathbb{A}'$ such that $H = H_1 \circ H_0$ where

1. $H_0 : \mathbb{A}_0 \mapsto \mathbb{A}'$
2. $H_0 : \mathbb{A}' \mapsto \mathbb{A}_1$

$\mathbb{A}_0$ is *nodewise less than or equal to* $\mathbb{A}_1$ if
for some $[\phi, \alpha] : \mathbb{A}_0 \mapsto \mathbb{A}_1$, ϕ is injective.

Authentication Tests Completeness

Let $H : \mathbb{A}_0 \mapsto \mathbb{A}_1$ 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 $\mathbb{A}_0$ 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 $H : \mathbb{A} \mapsto \mathbb{A}'$ where $\mathbb{A}'$ is realized.
If term(n) is not penetrator-derivable before n in $\mathbb{A}$, then either:

1. n is an incoming transformed node for some $K \in \text{non}_{\mathbb{A}} \cup \text{unique}_{\mathbb{A}}$; or else
2. (m, n) is an outgoing transformed pair with respect to a, S, X

   for

   (i) some $a \in \text{unique}_{\mathbb{A}}$ originating at a node $m \in \mathbb{A}$;

   (ii) some set S of encrypted terms such that
   a occurs only within S in the nodes of $\mathbb{A}$ below n; and

   (iii) some set of keys $X \subset \text{non}_{\mathbb{A}} \cup \text{unique}_{\mathbb{A}}$

   such that for each $K \in X$, K^{-1} is used for encryption in support(n).