Cryptographic Protocol Analysis via Strand Spaces: Authentication Tests

Al Maneki, NSA
Protocol Exchange
Naval Postgraduate School

Feb 2004

Slides provided by courtesy of MITRE
Joshua D. Guttman, Jonathan C. Herzoz, F. Javier Thayer

MITRE

Arrows between Nodes

$n_1 \to n_2$	means	n_1, n_2 are nodes with term$(n_1) = +t$, term$(n_2) = -t$	
	i.e.	n_2 receives t from n_1	
$n_1 \Rightarrow n_2$	means	$n_1 = s \downarrow i$, $n_2 = s \downarrow i + 1$	
$n_1 \Rightarrow^* n_2$	means	$n_1 = s \downarrow i$, $n_2 = s \downarrow j$,	where $i \leq j$
$n_1 \Rightarrow^+ n_2$	means	$n_1 = s \downarrow i$, $n_2 = s \downarrow j$,	where $i < j$

- $n_1 \to n_2$ and $n_1 \Rightarrow n_2$ express a *causal* dependence of n_2 on n_1
- Nodes and edges $\to$, $\Rightarrow$ in Σ form a graph G_Σ

MITRE

Bundles

- A subgraph $\mathcal{C}$ of G_Σ is a *bundle* if $\mathcal{C}$ is finite and causally well-grounded, which means:
  1. If $n_2 \in \mathcal{C}$ negative, there is a unique $n_1 \rightarrow n_2$ in $\mathcal{C}$ (everything heard was said)
  2. If $s \downarrow i+1 \in \mathcal{C}$, then $s \downarrow i \Rightarrow s \downarrow i+1$ in $\mathcal{C}$ (everyone starts at the beginning)
  3. $\mathcal{C}$ is acyclic (time never flows backward)
- Causal partial ordering $n_1 \preceq_\mathcal{C} n_2$ means n_2 reachable from n_1 via arrows in $\mathcal{C}$

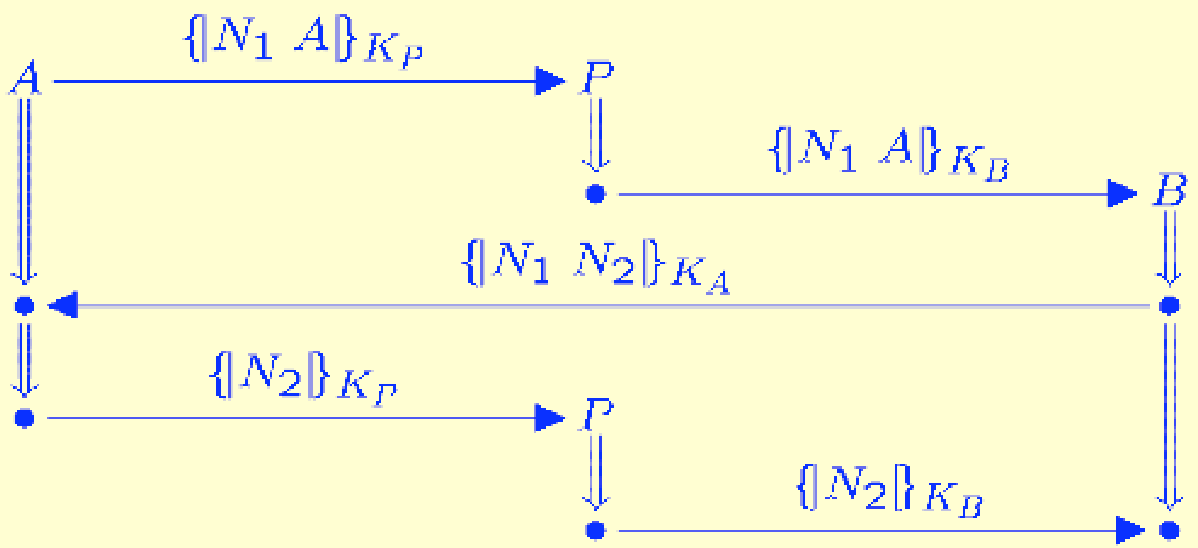
  Induction: Every non-empty set $S \subset \mathcal{C}$ of nodes contains $\preceq_\mathcal{C}$-minimal members

Representing Protocols

- Problem: Given a picture, define some sets of traces
- Associate keys with principals
  - The public key of. . .
  - The long term key shared between server and. . .
  - Ranges disjoint from potential session keys
- Define the behavior
  - Identify roles
  - Note terms that cannot be checked
  - Find parameters for each role
  - List signed terms
- Identify uniquely originating values
  - Nonces
  - Session keys emitted by server

Authentication Tests, I: Outgoing Tests

Needham-Schroeder: Undesirable Run



Due to Gavin Lowe (1995)

Example: NS

- Roles: Initiator, responder; Parameters: A, B, N_a, N_b
  - All terms can be checked
  - Uses K_A to mean "The public key of A"
  - List of terms: (signs depend on role)

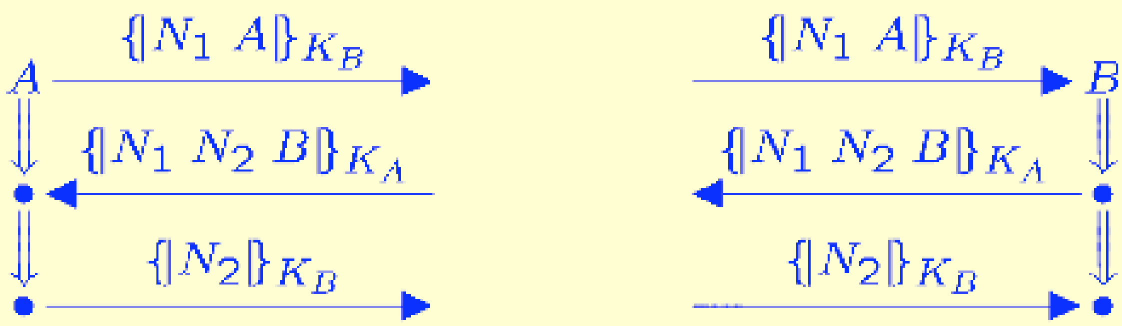
    $\{|N_a\ A|\}_{K_B}, \quad \{|N_a\ N_b|\}_{K_A}, \quad \{|N_b|\}_{K_B}$
  - Values intended to originate uniquely:

    $N_a,\ N_b$
- NSInit$[A, B, N_a, N_b]$: set of strands with trace

  $+\{|N_a\ A|\}_{K_B}, \quad -\{|N_a\ N_b|\}_{K_A}, \quad +\{|N_b|\}_{K_B}$
- NSLResp$[A, B, N_a, N_b]$: set of strands with trace

  $-\{|N_a\ A|\}_{K_B}, \quad +\{|N_a\ N_b|\}_{K_A}, \quad -\{|N_b|\}_{K_B}$

Needham-Schroeder-Lowe Protocol



MITRE

NSL: Responder's Guarantee

- Suppose:

  K_A^{-1} uncompromised

  N_2 uniquely originating
- Responder's edge $\{\!|N_1\ N_2\ B|\!\}_{K_A} \Rightarrow \{\!|N_2|\!\}_{K_B}$ is a test
  - Penetrator can't decrypt $\{\!|N_1\ N_2\ B|\!\}_{K_A}$
  - Super-encrypting does no good
  - Penetrator's only choice: discard it or deliver it?
- If responder receives $\{\!|N_2|\!\}_{K_B}$ then it was delivered
  - But to whom? Which regular strands will receive, change $\{\!|N_1\ N_2\ B|\!\}_{K_A}$?
  - Only regular strand NSInit$[A, B, N_1, N_2]$, at node 2

MITRE

Original NS Responder's Guarantee

- Suppose again:
  K_A^{-1} uncompromised
  N_2 uniquely originating
- Responder's edge $\{\!|N_1\ N_2|\!\}_{K_A} \Rightarrow \{\!|N_2|\!\}_{K_B}$ is a test
  - Penetrator can't decrypt $\{\!|N_1\ N_2|\!\}_{K_A}$
  - Super-encrypting does no good
  - Penetrator's only choice: discard it or deliver it?
- If responder receives $\{\!|N_2|\!\}_{K_B}$ then it was delivered
  - But to whom?
  - Only regular strand NSInit$[A, *, N_1, N_2]$ can receive $\{\!|N_1\ N_2|\!\}_{K_A}$ and change it
- Whoops: What if $* \neq B$?

The Algebra of Terms: Components

- Term t_0 is a component of t, written $\boxed{t_0} \sqsubset t$

  If $t \in T \cup K$, then $\boxed{t} \sqsubset t$

  If $t = \{\!|h|\!\}_K$, then $\boxed{t} \sqsubset t$

  $\boxed{t_0} \sqsubset g$ implies $\boxed{t_0} \sqsubset g\ h$

  $\boxed{t_0} \sqsubset h$ implies $\boxed{t_0} \sqsubset g\ h$

- A component is a "largest non-concatenated part"
  Penetrator fully controls concatenation anyway

- Components of $N_b\ \{\!|K\ N_b\ A|\!\}_{K_B}\ \{\!|N_a\ B\ K|\!\}_{K_A}$

  N_b
  $\{\!|K\ N_b\ A|\!\}_{K_B}$
  $\{\!|N_a\ B\ K|\!\}_{K_A}$

MITRE

The Anatomy of the Case, I

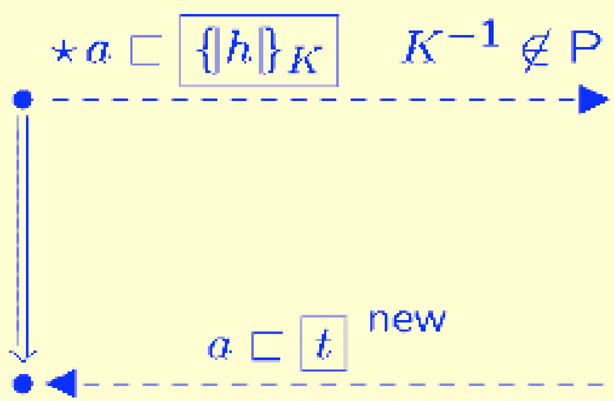
- Find values uniquely originating on $s_r \in \mathsf{NSLResp}[A, B, N_a, N_b]$
  - N_b only, in $\{\!|N_a\ N_b\ B|\!\}_{K_A}$ on node $n_0 = s_r \downarrow 2$
- Find negative (receiving) nodes containing value N_b

$$n_1 = s_r \downarrow 3 \text{ with term } \{\!|N_b|\!\}_{K_B}$$

check: K_A^{-1} is not "penetrable" $(*)$
$\{\!|N_a\ N_b\ B|\!\}_{K_A}$ not a subterm of a regular node
N_b occurs in only one component of n_0

- Therefore, $n_0 \Rightarrow n_1$ is an "outgoing test"

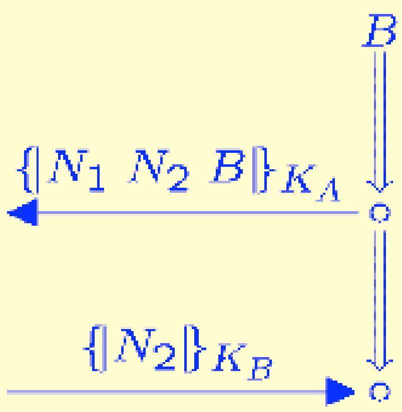
Outgoing Test



a uniquely originates at $\star$

$\boxed{t}$ means a component

NSL Responder Test

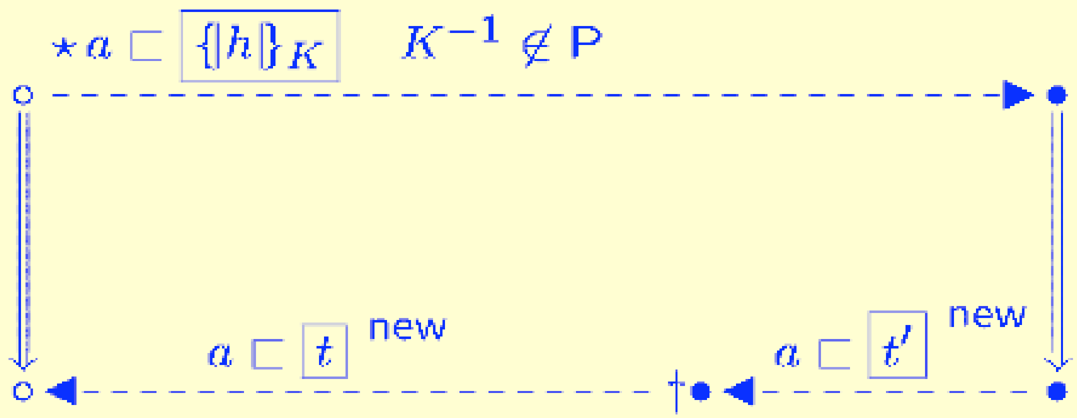


MITRE

The Anatomy of the Case, II

- Since $n_0 \Rightarrow n_1$ is an outgoing test, there's a regular transforming edge $m_0 \Rightarrow m_1$ such that
  - $\boxed{\{|N_a\ N_b\ B|\}_{K_A}} \sqsubset \mathsf{term}(m_0)$
  - m_0 negative (receiving)
  - m_1 contains N_b in a new component
- Inspecting protocol, $m_0 = s_i \downarrow 2$, where $s_i \in \mathsf{NSLInit}[A, B, N_a, N_b]$, so
  - $m_1 = s_i \downarrow 3$
  - s_i has $\mathcal{C}$-height 3
- This is the NSL responder's guarantee

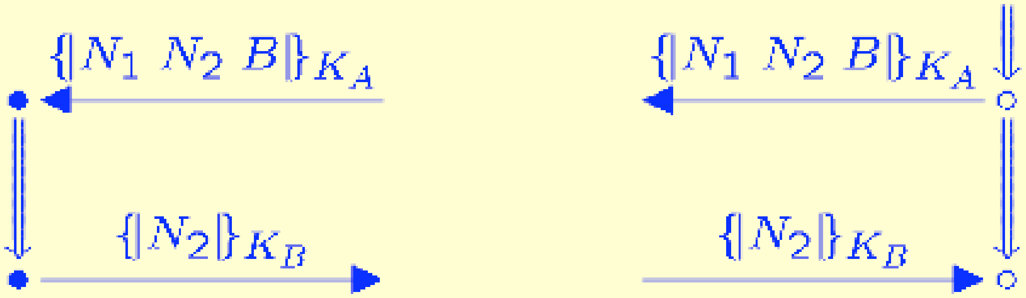
Outgoing test Authentication



"•" means the test shows this regular node exists

† this node depends on extra conditions

NSL Responder Authentication



Outgoing test establishes

- nodes present and non-penetrator

Anatomy of Original NS

- Part I identifies outgoing test, as in NSL
- Since $n_0 \Rightarrow n_1$ is an outgoing test, there's a regular $m_0 \Rightarrow m_1$ such that
  - $\boxed{\{\!|N_a\ N_b|\!\}_{K_A}} \sqsubset \mathsf{term}(m_0)$
  - m_0 negative (receiving)
- Inspecting protocol, $m_0 = s_i \downarrow 2$, where $s_i \in \mathsf{NSInit}[A, *, N_a, N_b]$, so
  - $m_1 = s_i \downarrow 3$
  - s_i has $\mathcal{C}$-height 3
- This is the NS responder's guarantee; B unconstrained

NSL Initiator's Guarantee, I

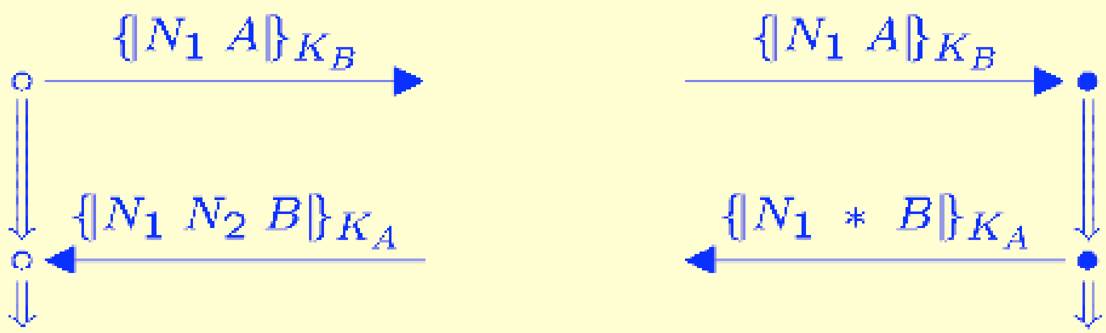
- Suppose:

  K_B^{-1} uncompromised

  N_1 uniquely originating
- Initiator's edge $\{\!|N_1\ A|\!\}_{K_B} \Rightarrow \{\!|N_1\ N_2\ B|\!\}_{K_A}$ is a test
  - Penetrator can't decrypt $\{\!|N_1\ A|\!\}_{K_B}$
  - Super-encrypting does no good
  - Penetrator's only choice: discard it or deliver it?
- If initiator receives $\{\!|N_1\ N_2\ B|\!\}_{K_A}$ then it was delivered
  - But to whom? Which regular strands will receive, change $\{\!|N_1\ A|\!\}_{K_B}$?
  - Only regular strand $s_r \in \text{NSResp}[A, B, N_1, *]$, at node 1

MITRE

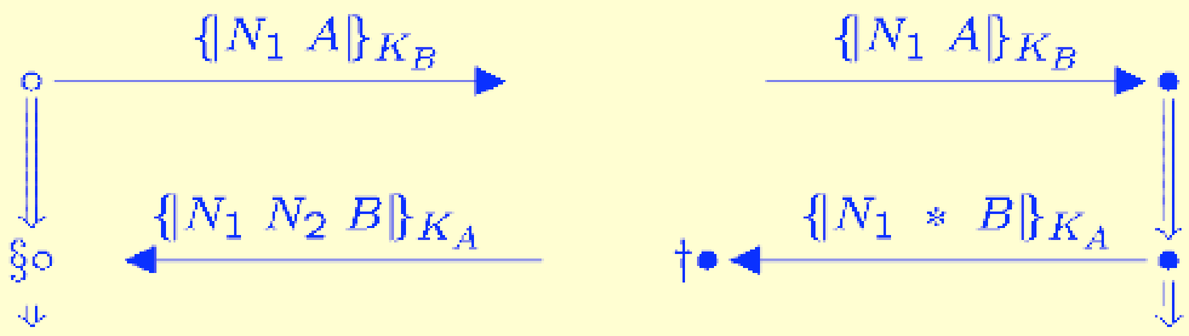
NSL Initiator Authentication, I



NSL Initiator's Guarantee, II

- Suppose also K_A^{-1} uncompromised
- Penetrator choice: discard or deliver $\{\!|N_1 * B|\!\}_{K_A}$
  - Must have delivered it to some regular strand, an initiator strand NSInit$[A, B, N_1, *]$
  - But N_1 originates uniquely
- So $* = N_2$ and $s_r \in$ NSResp$[A, B, N_1, N_2]$
- Uses additional node in Outgoing Test Authentication

NSL Initiator Authentication, II

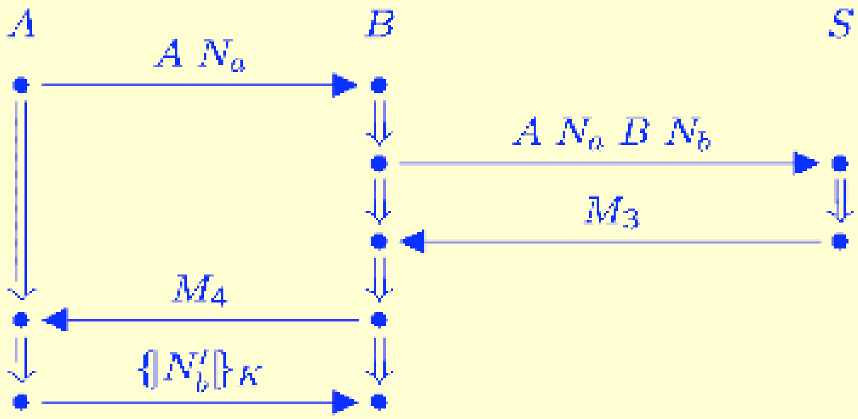


$\S\circ = \dagger\bullet$

because of unique origination of N_a

Authentication Tests, II: Incoming Tests

Carlsen



$$M_3 = \{\!|K\ N_b\ A|\!\}_{K_B}\ \{\!|N_a\ B\ K|\!\}_{K_A}$$
$$M_4 = \{\!|N_a\ B\ K|\!\}_{K_A}\ \{\!|N_a|\!\}_K\ N_b'$$

Example: Carlsen, I

- Roles: Initiator, responder, server;
  Parameters: A, B, N_a, N_b, K, N_b'
  - B cannot check $\{|N_a\ B\ K|\}_{K_A}$, part of M_3
  - Uses K_A to mean "Long term shared key of A"
- Values intended to originate uniquely:
  - Nonces N_a, N_b, N_b'
  - Session key K
- Obligations of key server:
  - Never re-use session key K
  - Never use long-term key K_A as session key
  - Never chooses value known initially to penetrator

Example: Carlsen, II

- CInit$[A, B, N_a, K, N_b']$: set of strands with trace

  $+A\ N_a, \quad -\{\!|N_a\ B\ K|\!\}_{K_A}\ \{\!|N_a|\!\}_K\ N_b', \quad +\{\!|N_b'|\!\}_K$

- CResp$[A, B, N_a, N_b, K, N_b', H]$: set of strands with trace

  $-A\ N_a, \quad +A\ N_a\ B\ N_b, \quad -\{\!|K\ N_b\ A|\!\}_{K_B}\ H,$

  $+H\ \{\!|N_a|\!\}_K\ N_b', \quad -\{\!|N_b'|\!\}_K$

- CServ$[A, B, N_a, N_b, K]$: set of strands with trace

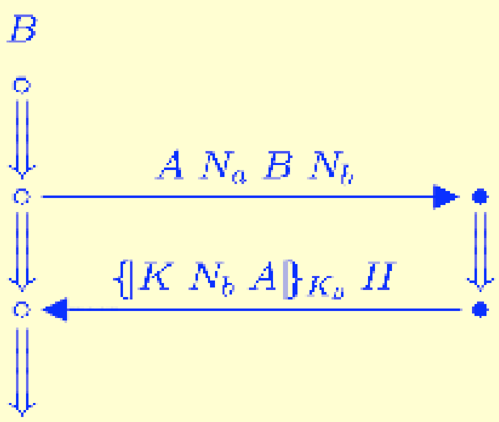
  $-A\ N_a\ B\ N_b, \quad +\{\!|K\ N_b\ A|\!\}_{K_B}\ \{\!|N_a\ B\ K|\!\}_{K_A}$

Incoming Tests Example: Carlsen

- Carlsen protocol uses different pattern
  - Nonce transmitted as plaintext
  - Received back in encrypted form
  - Demonstrates possession of key
- "Incoming test" because transforming edge act creates the encrypted unit received by strand

Responder Authenticates Server

Assume $K_B \notin K_\mathcal{P}$

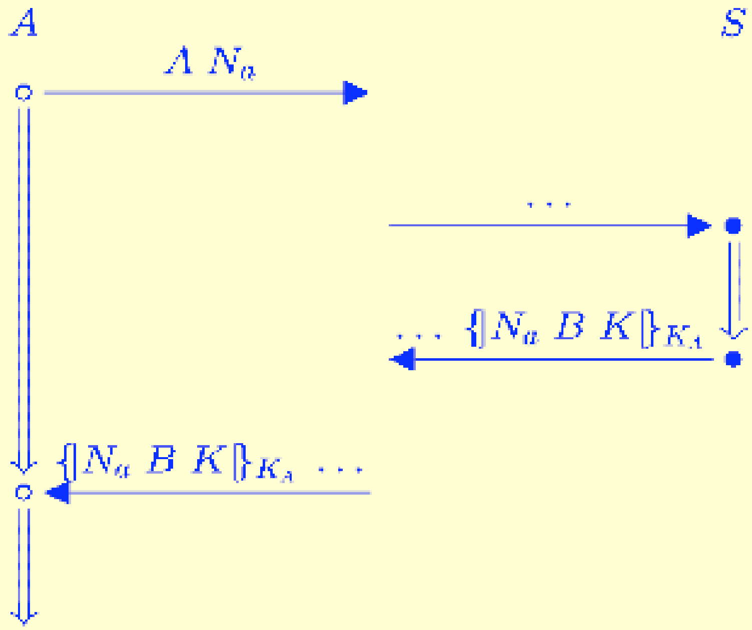


$\bullet^s$ can only lie on CServ$[A, B, *, N_b, K]$

MITRE

Initiator Authenticates Server

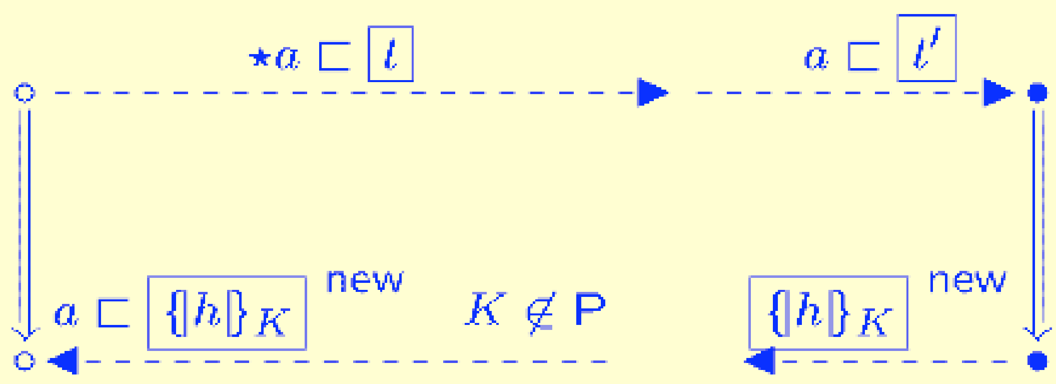
Assume $K_A \notin K_{\mathcal{P}}$



$\bullet^s$ can only lie on CServ$[A, B, N_a, *, K]$

MITRE

Incoming Test Authentication



Authentication Tests, III: Secrecy

MITRE

Penetrable Keys P

- Penetrable keys: the idea
  - If $K \in K_{\mathcal{P}}$, then it's penetrable
  - If K is uttered in $\{\!|\cdots K \cdots|\!\}_{K_0}$ and K_0^{-1} is already penetrable, then K is penetrable
- More rigorously:
  1. $K \in P_0$ if $K \in K_{\mathcal{P}}$
  2. $K \in P_{i+1}$ if exists n regular, positive, with $K \sqsubset_{\mathfrak{K}} \boxed{t}^{new} \sqsubset \text{term}(n)$, and $K_0 \in \mathfrak{K}$ implies $K_0^{-1} \in P_i$
  3. $P = \bigcup_i P_i$
- Carlsen example: $\{\!|K\ N_b\ A|\!\}_{K_B}\ \{\!|N_a\ B\ K|\!\}_{K_A}$

MITRE

Safe Keys $\mathcal{S}$, Disjoint from $\mathcal{P}$

Idea: S_0 immediately safe: no one says it new
$K \in S_{i+1}$ if whenever said newly, protected by some K_0 where $K_0^{-1} \in S_i$

1. $K \in S_0$ if $K \notin K_{\mathcal{P}}$ and $K \not\sqsubset \boxed{t}^{new} \sqsubset \mathrm{term}(n)$ for all n positive regular
2. $K \in S_{i+1}$ if $K \notin K_{\mathcal{P}}$ and $t = \cdots \{\!|\cdots K \cdots|\!\}_{K_0} \cdots$ with $K_0^{-1} \in S_i$, whenever $K \sqsubset \boxed{t}^{new} \sqsubset \mathrm{term}(n)$, for all n positive regular
3. $S = \bigcup_i S_i$

$\{\!|K\ N_b\ A|\!\}_{K_B}\ \{\!|N_a\ B\ K|\!\}_{K_A}$

MITRE

Safe Keys: Examples

- Needham-Schroeder

  $K_A^{-1} \not\sqsubset \text{term}(n)$ for all n positive regular,

  so $K_A^{-1} \notin K_{\mathcal{P}}$ implies $K_A^{-1} \in S_0$
- Carlsen initiator
  1. $K_A, K_B \notin K_{\mathcal{P}}$ implies $K_A, K_B \in S_0$
  2. $s_s \in \text{CServ}[A, B, N_a, *, K]$ implies K originates

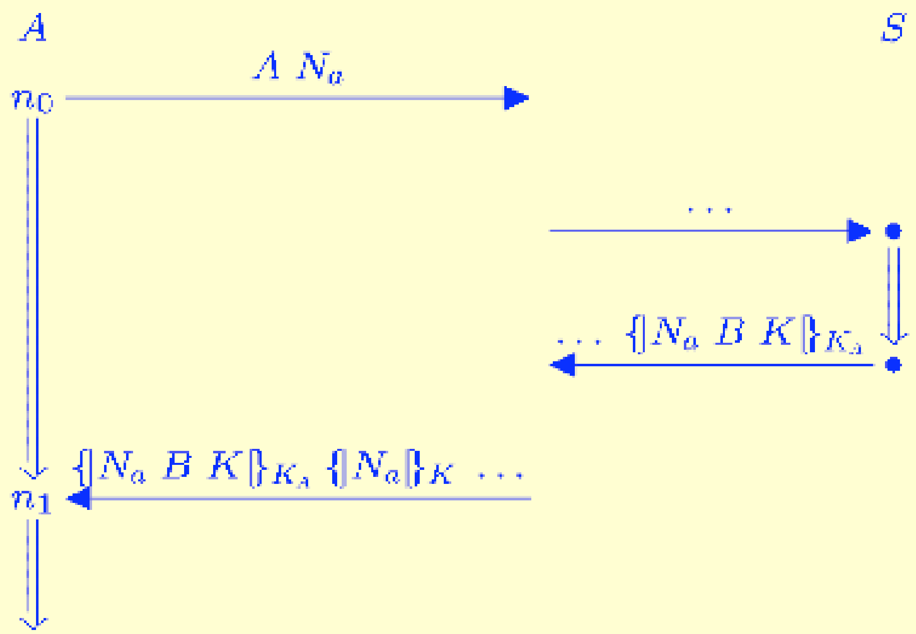
     only on s_s, in $\{\!|K \; * \; A|\!\}_{K_B} \; \{\!|N_a \; B \; K|\!\}_{K_A}$
  3. Hence, $K \in S_1$
- Similar for Carlsen responder with $s_s \in \text{CServ}[A, B, *, N_b, K]$

MITRE

Authentication Tests, IV: Using Safe Keys

Carlsen: Initiator Authenticates Responder

Assume $K_A, K_B \notin K_{\mathcal{P}}$



Since $K \in \mathsf{S}_1$, $n_0 \Rightarrow n_1$ incoming test for N_a in $\{\!|N_a|\!\}_K$

MITRE

Carlsen: Initiator Authenticates Responder, I

- Suppose $s_i \in$ CInit$[A, B, N_a, K, *]$ with $\mathcal{C}$-height $\geq$2
  - So there is $s_{s,1} \in$ CServ$[A, B, N_a, *, K]$
  - $K \in S_1$
  - Exists transforming edge $m_0 \Rightarrow^+ m_1$ with $\boxed{\{\!|N_a|\!\}_K}^{new} \sqsubset$ term(m_1)
- Where is m_1? Two cases:
  1. $m_1 = s \downarrow 4$ for $s \in$ CResp$[X, Y, N_a, *, K, *, *]$
  2. $m_1 = s \downarrow 3$ for $s \in$ CInit$[X, Y, *, K, N_a]$

1. Then $s_{s,2} \in$ CServ$[X, Y, *, *, K]$ has $\mathcal{C}$-height 2
   so $s_{s,1} = s_{s,2}$, and $X = A$, $Y = B$
   hence $s \in$ CResp$[A, B, N_a, *, K, *, *]$

MITRE

Carlsen: Initiator/Responder, Case 2

- Assuming: $m_1 = s \downarrow 3$ for $s \in$ CInit$[X, Y, *, K, N_a]$
- There's $s_{s,2} \in$ CServ$[X, Y, N, *, K]$,
  so $s_{s,1} = s_{s,2}$, and $X = A$, $Y = B$, $N = N_a$
- Since N_a originates on both s_i and s,
  and N_a originates uniquely,
  $s_i = s$
- Hence $s_i \downarrow 3 \prec_C s_i \downarrow 2$

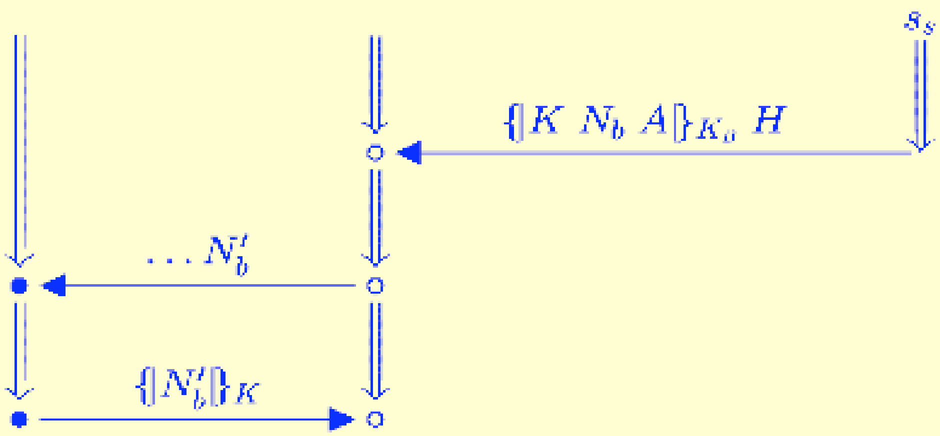
  contradicting acyclicity clause
  in definition of bundle

  (i.e. Case 2 is impossible)

MITRE

Carlsen: Responder Authenticates Initiator

Assuming $N_a \neq N_b'$, and
$K_A, K_B \notin K_\mathcal{P}$, so $K \in S_1$



Since $K \in S_1$, $n_0 \Rightarrow n_1$ incoming test for N_b' in $\{\!|N_b'|\!\}_K$

Carlsen: Responder Authenticates Initiator, I

- Suppose $s_r \in$ CResp$[A, B, N_a, N_b, K, N_b', *]$ with $\mathcal{C}$-height 5
  - There is $s_{s,1} \in$ CServ$[A, B, *, N_b, K]$ and $K \in S_1$
  - Exists transforming edge $m_0 \Rightarrow^+ m_1$ with

    $\boxed{\{\!|N_b'|\!\}_K}^{new} \sqsubset$ term(m_1)
- Where is m_1? Two cases:
  1. $m_1 = s \downarrow 4$ for $s \in$ CResp$[X, Y, N_b', N, K, *, *]$
  2. $m_1 = s \downarrow 3$ for $s \in$ CInit$[X, Y, *, K, N_b']$

1. Then $s_{s,2} \in$ CServ$[X, Y, *, N, K]$ has $\mathcal{C}$-height 2
   so $s_{s,1} = s_{s,2}$, and $X = A$, $Y = B$, and $N = N_b$
   hence $s \in$ CResp$[A, B, N_b', N_b, K, *, *]$
   Since N_b originates uniquely, $s = s_r$, so $N_a = N_b'$ $\rightarrow\leftarrow$

MITRE

Carlsen: Responder/Initiator, Case 2

- Assuming: $m_1 = s \downarrow 3$ for $s \in$ CInit$[X, Y, N, K, N'_b]$
- There's $s_{s,2} \in$ CServ$[X, Y, *, *, K]$,
  so $s_{s,1} = s_{s,2}$, and $X = A$, $Y = B$,
  hence $s \in$ CInit$[A, B, N, K, N'_b]$
- Moreover, $N = N_a$:
  - By Initiator's guarantee,
    $\exists s' \in$ CResp$[A, B, N, *, K, N'_b, *]$
    but N'_b originates uniquely, so $s_r = s'$
- This completes analysis of Carlsen's protocol
- By the way:
  The server gets no guarantees

MITRE