Strand spaces:
A framework to prove protocols
and find counterexamples

Joshua D. Guttman
Worcester Polytechnic Institute
The MITRE Corporation

March 2013
Bertinoro International Spring School
Thanks to the US National Science Foundation, under grant 1116557

guttman@wpi.edu

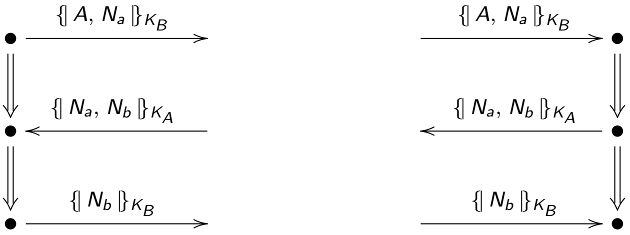
Strands

- Strand: A finite linear sequence $\bullet \Rightarrow \bullet \Rightarrow \bullet \cdots$ of events

  transmission reception neutral

- Strand may represent
  - single local session of a protocol, or
  - an adversary action
- Each event called a node
- Transmission, reception sometimes written $+, -$ resp
- Node n is labeled with a message $\text{msg}(n)$

Example: Needham-Schroeder



Protocol: finite set Π of roles

Strands of Π: all substitution instances

Adversary Strands

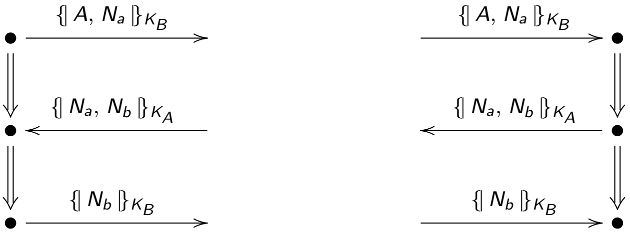
a: basic value $\quad$ t_i: any msg

$$\bullet \xrightarrow{a}$$

$$\begin{tikzcd}
t_1 \arrow[d] & t_2 \arrow[d] & \{\!|\, t_1 \,|\!\}_{t_2} \\
\bullet \arrow[r, Rightarrow] & \bullet \arrow[r, Rightarrow] & \bullet \arrow[u]
\end{tikzcd}
\qquad
\begin{tikzcd}
t_1 \arrow[d] & t_2 \arrow[d] & \mathrm{tag}\ t_1,\ t_2 \\
\bullet \arrow[r, Rightarrow] & \bullet \arrow[r, Rightarrow] & \bullet \arrow[u]
\end{tikzcd}$$

$$\begin{tikzcd}
\bullet \arrow[r, Rightarrow] & \bullet \arrow[r, Rightarrow] & \bullet \arrow[d] \\
\{\!|\, t_1 \,|\!\}_{t_2} \arrow[u] & {t_2}^{-1} \arrow[u] & t_1
\end{tikzcd}
\qquad
\begin{tikzcd}
\bullet \arrow[r, Rightarrow] & \bullet \arrow[r, Rightarrow] \arrow[d] & \bullet \arrow[d] \\
\mathrm{tag}\ t_1,\ t_2 \arrow[u] & t_1 & t_2
\end{tikzcd}$$

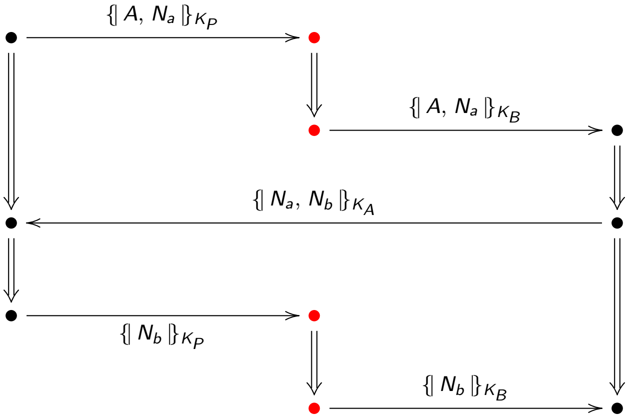
Executions are bundles, 1



Executions are bundles, 1

$$
\begin{tikzcd}[column sep=huge, row sep=large]
\bullet \arrow[r, "\{\!|\, A,\, N_a \,|\!\}_{K_B}"] \arrow[d, Rightarrow] & \bullet \arrow[d, Rightarrow] \\
\bullet \arrow[d, Rightarrow] & \bullet \arrow[l, "\{\!|\, N_a,\, N_b \,|\!\}_{K_A}"'] \arrow[d, Rightarrow] \\
\bullet \arrow[r, "\{\!|\, N_b \,|\!\}_{K_B}"] & \bullet
\end{tikzcd}
$$

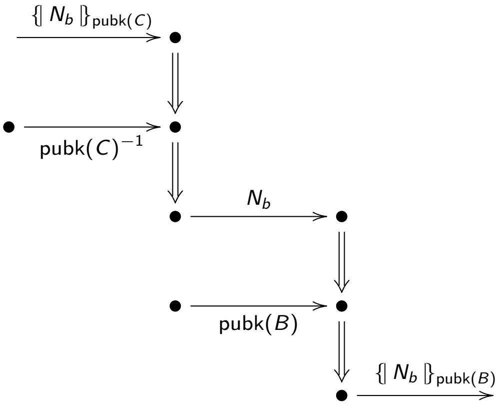
Executions are bundles, 2



Some adversary strands for bundle 2

$$
\begin{tikzcd}
{} \arrow[r, "\{\!|\, A,\ N_a \,|\!\}_{\mathrm{pubk}(C)}"] & \bullet \arrow[d, Rightarrow] & & \\
\bullet \arrow[r, "\mathrm{pubk}(C)^{-1}"'] & \bullet \arrow[d, Rightarrow] & & \\
& \bullet \arrow[r, "A,\ N_a"] & \bullet \arrow[d, Rightarrow] & \\
& \bullet \arrow[r, "\mathrm{pubk}(B)"'] & \bullet \arrow[d, Rightarrow] & \\
& & \bullet \arrow[r, "\{\!|\, A,\ N_a \,|\!\}_{\mathrm{pubk}(B)}"] & {}
\end{tikzcd}
$$

More adversary strands for bundle 2



Bundle: Definition

Let $\mathcal{B}$ be a finite directed acyclic graph V, E where

V consists of nodes

E is $(\Rightarrow_E \cup \rightarrow_E)$ where:

$n_1 \Rightarrow_E n_2$ implies $n_1 \Rightarrow n_2$

$n_1 \rightarrow_E n_2$ implies n_1 transmission,
n_2 reception, and
$\mathrm{msg}(n_1) = \mathrm{msg}(n_2)$

$\mathcal{B}$ is a bundle if

1. $n_2 \in V$ and $n_1 \Rightarrow n_2$ implies $n_1 \in V$ and $n_1 \Rightarrow_E n_2$ — start at beginning
2. $n_2 \in V$ is a reception node implies there is a unique $n_1 \in V$ such that $n_1 \rightarrow_E n_2$ — what's heard was said

Bundle ordering $\preceq_{\mathcal{B}}$

Let $\mathcal{B}$ be a bundle

- Define $\preceq_{\mathcal{B}}$ to be $(\Rightarrow_E \cup \rightarrow_E)^*$
- So $n_1 \preceq_{\mathcal{B}} n_2$ means there is a path in $\mathcal{B}$ from n_1 to n_2

Bundle ordering $\preceq_{\mathcal{B}}$

Let $\mathcal{B}$ be a bundle

- Define $\preceq_{\mathcal{B}}$ to be $(\Rightarrow_E \cup \rightarrow_E)^*$
- So $n_1 \preceq_{\mathcal{B}} n_2$ means there is a path in $\mathcal{B}$ from n_1 to n_2
- $\preceq_{\mathcal{B}}$ is a partial order by acyclicity

Bundle ordering $\preceq_{\mathcal{B}}$

Let $\mathcal{B}$ be a bundle

- Define $\preceq_{\mathcal{B}}$ to be $(\Rightarrow_E \cup \rightarrow_E)^*$
- So $n_1 \preceq_{\mathcal{B}} n_2$ means there is a path in $\mathcal{B}$ from n_1 to n_2
- $\preceq_{\mathcal{B}}$ is a partial order — by acyclicity
- $\preceq_{\mathcal{B}}$ is well-founded — by finiteness

Bundle ordering $\preceq_{\mathcal{B}}$

Let $\mathcal{B}$ be a bundle

- Define $\preceq_{\mathcal{B}}$ to be $(\Rightarrow_E \cup \rightarrow_E)^*$
- So $n_1 \preceq_{\mathcal{B}} n_2$ means there is a path in $\mathcal{B}$ from n_1 to n_2
- $\preceq_{\mathcal{B}}$ is a partial order — by acyclicity
- $\preceq_{\mathcal{B}}$ is well-founded — by finiteness

Well-founded means:

Every non-empty $S \subseteq \text{nodes}(\mathcal{B})$ has $\preceq_{\mathcal{B}}$-minimal members

Bundle ordering $\preceq_{\mathcal{B}}$

Let $\mathcal{B}$ be a bundle

- Define $\preceq_{\mathcal{B}}$ to be $(\Rightarrow_E \cup \rightarrow_E)^*$
- So $n_1 \preceq_{\mathcal{B}} n_2$ means there is a path in $\mathcal{B}$ from n_1 to n_2
- $\preceq_{\mathcal{B}}$ is a partial order — by acyclicity
- $\preceq_{\mathcal{B}}$ is well-founded — by finiteness

Well-founded means:

Every non-empty $S \subseteq \text{nodes}(\mathcal{B})$ has $\preceq_{\mathcal{B}}$-minimal members

Serves as an induction principle — Bundle induction

If S has no $\preceq_{\mathcal{B}}$-minimal members, $S = \emptyset$

Messages

Basic messages:

Names for principals

Keys basic keys are either symmetric or asymmetric

Data maybe used as nonces etc

Built up using

Encryption of t using K is $\{\!|\, t \,|\!\}_K$

Tagged pair of t_1, t_2, tagged with *tag* is $\mathit{tag}\ \ t_1,\ t_2$

Messages

Basic messages:

- **Names** for principals
- **Keys** basic keys are either symmetric or asymmetric
- **Data** maybe used as nonces etc

Built up using

- **Encryption** of t using K is $\{\!| \, t \, |\!\}_K$
- **Tagged pair** of t_1, t_2, tagged with *tag* is $\mathit{tag} \;\; t_1, \; t_2$

Special tag *nil* : Write $\mathit{nil} \;\; t_1, \; t_2$ as $t_1, \; t_2$

Messages

Basic messages:

- **Names** for principals
- **Keys** basic keys are either symmetric or asymmetric
- **Data** maybe used as nonces etc

Built up using

- **Encryption** of t using K is $\{\!|\, t \,|\!\}_K$
- **Tagged pair** of t_1, t_2, tagged with tag is $tag\ \ t_1,\ t_2$

Special tag nil : Write $nil\ \ t_1,\ t_2$ as $t_1,\ t_2$

Messages are an inductively defined structure

Two notions of subterm: $\sqsubseteq$ and $\ll$

Both are reflexive, transitive relations

$\sqsubseteq$ generated by: "ingredient"

$$t_1 \sqsubseteq tag\ \ t_1,\ t_2 \qquad\qquad t_2 \sqsubseteq tag\ \ t_1,\ t_2$$

$$t_1 \sqsubseteq \{\!| \ t_1 \ |\!\}_K$$

Two notions of subterm: $\sqsubseteq$ and $\ll$

Both are reflexive, transitive relations

$\sqsubseteq$ generated by: "ingredient"

$$t_1 \sqsubseteq tag \;\; t_1,\; t_2 \qquad\qquad t_2 \sqsubseteq tag \;\; t_1,\; t_2$$

$$t_1 \sqsubseteq \{\!|\, t_1 \,|\!\}_K$$

$\ll$ generated by: "occurs in"

$$t_1 \ll tag \;\; t_1,\; t_2 \qquad\qquad t_2 \ll tag \;\; t_1,\; t_2$$

$$t_1 \ll \{\!|\, t_1 \,|\!\}_K \qquad\qquad K \ll \{\!|\, t_1 \,|\!\}_K$$

Origination

a originates at $n \in \text{nodes}(\mathcal{B})$ iff

- $a \sqsubseteq \text{msg}(n)$
- n is a transmission node
- $a \not\sqsubseteq \text{msg}(m)$ whenever $m \Rightarrow^{+} n$

I.e. a is transmitted as an ingredient of $\text{msg}(n)$, and n is its first use as an ingredient

Ingredient $\sqsubseteq$ just uses plaintext, not key

Fresh choice

a is freshly chosen in $\mathcal{B}$ means a originates uniquely in nodes($\mathcal{B}$):

a originates at a node n but at no other node m

Fresh choice

a is freshly chosen in $\mathcal{B}$ means a originates uniquely in nodes($\mathcal{B}$):

a originates at a node n but at no other node m

i.e. a originates at a unique node n

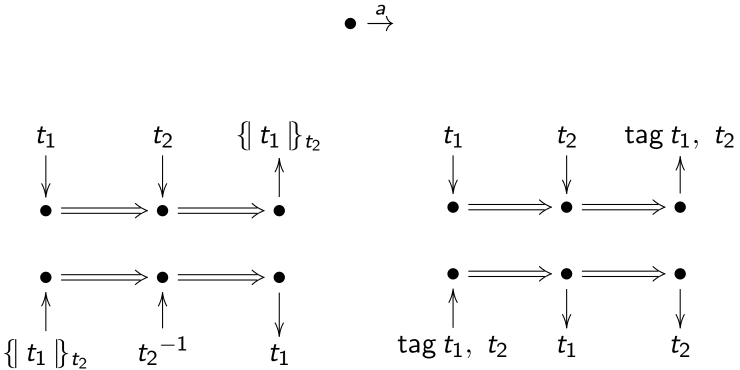
Uncompromised keys

A key K is uncompromised if it originates nowhere:

$$\text{for every } n \in \text{nodes}(\mathcal{B}),\ K \not\sqsubseteq \text{msg}(n)$$

Adversary never uses non-originating keys

If adversary uses K, it must have originated



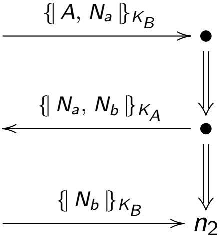
Prove all things. Hold fast
to what is good.

St. Paul, 1 Thessalonians 5:21
with thanks to Imre Lakatos

Proving Authentication: Needham-Schroeder

for the responder

Suppose that N_b is uniquely originating, and K_A^{-1} is non-originating

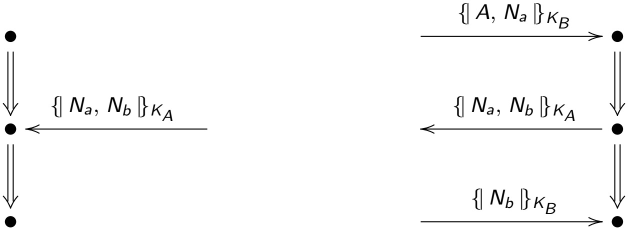


N_b is found outside $\{\!| N_a, N_b |\!\}_{K_A}$ in $\text{msg}(n_2)$.
Thus, there is a $\preceq_{\mathcal{B}}$-minimal node m such that N_b is found outside $\{\!| N_a, N_b |\!\}_{K_A}$ in $\text{msg}(m)$

Proving Authentication: Needham-Schroeder

for the responder

Suppose that N_b is uniquely originating, and K_A^{-1} is non-originating

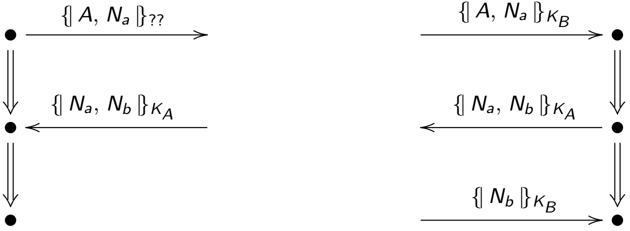


N_b is found outside $\{\!|\, N_a,\ N_b \,|\!\}_{K_A}$ in $\mathrm{msg}(n_2)$.
Thus, there is a $\preceq_{\mathcal{B}}$-minimal node m such that N_b is found outside $\{\!|\, N_a,\ N_b \,|\!\}_{K_A}$ in $\mathrm{msg}(m)$

Proving Authentication: Needham-Schroeder

for the responder

Suppose that N_b is uniquely originating, and
K_A^{-1} is non-originating

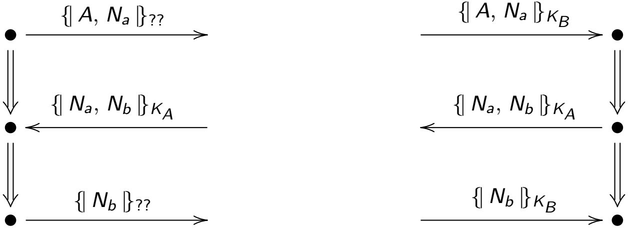


N_b is found outside $\{\!|\, N_a,\ N_b \,|\!\}_{K_A}$ in msg(n_2).
Thus, there is a $\preceq_{\mathcal{B}}$-minimal node m such that N_b is found outside $\{\!|\, N_a,\ N_b \,|\!\}_{K_A}$ in msg(m)

Proving Authentication: Needham-Schroeder

for the responder

Suppose that N_b is uniquely originating, and K_A^{-1} is non-originating



N_b is found outside $\{\!|\, N_a,\ N_b \,|\!\}_{K_A}$ in $\mathrm{msg}(n_2)$.
Thus, there is a $\preceq_{\mathcal{B}}$-minimal node m such that N_b is found outside $\{\!|\, N_a,\ N_b \,|\!\}_{K_A}$ in $\mathrm{msg}(m)$

What did we prove about NS?

If $\mathcal{B}$ is a bundle where

1. $K_A^{-1} \in \text{non}_{\mathcal{B}}$ and $N_b \in \text{unique}_{\mathcal{B}}$
2. $\mathcal{B}$ has a full responder strand with parameters A, B, N_a, N_b

then $\mathcal{B}$ has a full initiator strand with parameters A, C, N_a, N_b

What did we prove about NS?

If $\mathcal{B}$ is a bundle where

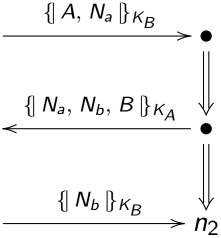
1. $K_A^{-1} \in \text{non}_{\mathcal{B}}$ and $N_b \in \text{unique}_{\mathcal{B}}$
2. $\mathcal{B}$ has a full responder strand with parameters A, B, N_a, N_b

then $\mathcal{B}$ has a full initiator strand
with parameters A, C, N_a, N_b
for some C

Proving Authentication: Needham-Schroeder-Lowe

for the responder

Suppose that N_b is uniquely originating, and K_A^{-1} is non-originating

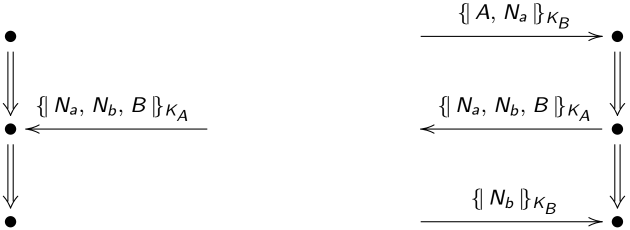


N_b is found outside $\{\!| N_a, N_b, B |\!\}_{K_A}$ in $\mathrm{msg}(n_2)$.
Thus, there is a $\preceq_{\mathcal{B}}$-minimal node m such that N_b is found outside $\{\!| N_a, N_b, B |\!\}_{K_A}$ in $\mathrm{msg}(m)$

Proving Authentication: Needham-Schroeder-Lowe

for the responder

Suppose that N_b is uniquely originating, and K_A^{-1} is non-originating

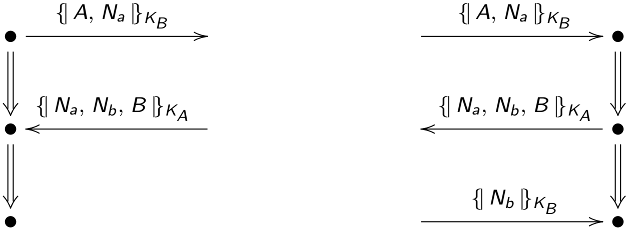


N_b is found outside $\{\!|\, N_a,\ N_b,\ B \,|\!\}_{K_A}$ in $\mathrm{msg}(n_2)$.
Thus, there is a $\preceq_{\mathcal{B}}$-minimal node m such that N_b is found outside $\{\!|\, N_a,\ N_b,\ B \,|\!\}_{K_A}$ in $\mathrm{msg}(m)$

Proving Authentication: Needham-Schroeder-Lowe

for the responder

Suppose that N_b is uniquely originating, and
K_A^{-1} is non-originating

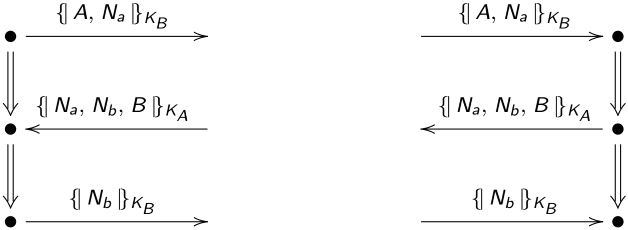


N_b is found outside $\{\!|\, N_a,\ N_b,\ B \,|\!\}_{K_A}$ in $\mathrm{msg}(n_2)$.
Thus, there is a $\preceq_{\mathcal{B}}$-minimal node m such that N_b is found outside $\{\!|\, N_a,\ N_b,\ B \,|\!\}_{K_A}$ in $\mathrm{msg}(m)$

Proving Authentication: Needham-Schroeder-Lowe

for the responder

Suppose that N_b is uniquely originating, and K_A^{-1} is non-originating



N_b is found outside $\{\!|\, N_a,\ N_b,\ B \,|\!\}_{K_A}$ in $\mathrm{msg}(n_2)$.
Thus, there is a $\preceq_{\mathcal{B}}$-minimal node m such that N_b is found outside $\{\!|\, N_a,\ N_b,\ B \,|\!\}_{K_A}$ in $\mathrm{msg}(m)$

What did we prove about NSL?

If $\mathcal{B}$ is a bundle where

1. $K_A^{-1} \in \text{non}_{\mathcal{B}}$ and $N_b \in \text{unique}_{\mathcal{B}}$
2. $\mathcal{B}$ has a full responder strand with parameters A, B, N_a, N_b

then $\mathcal{B}$ has a full initiator strand with parameters A, B, N_a, N_b

Quick Summary

- Breaking and proving protocols: A tight duality
- Strand theory focuses on causal relations
- Questions: What about
  - mechanized support?
  - big, real protocols? For instance, TLS

Subjects for tomorrow