Deconstructing Alice & Bob

Carlos Caleiro

CLC, Dep. Mathematics, IST, TU Lisbon, Portugal

Luca Viganò and David Basin

Dep. Computer Science, ETH Zurich, Switzerland

ARSPA'05 – Lisbon, Portugal – July 16, 2005

The context

- Formal analysis of security protocols
- Strand spaces, multiset rewriting, theorem proving ...

The context

- Formal analysis of security protocols
- Strand spaces, multiset rewriting, theorem proving ...
- Distributed temporal logic

Caleiro, Viganò and Basin. *Relating strand spaces and distributed temporal logic for security protocol analysis*. Logic Journal of the IGPL, in print.

Caleiro, Viganò and Basin. *Metareasoning about security protocols using distributed temporal logic*. ENTCS 125(1):67–89, 2005.

Caleiro, Viganò and Basin. *Towards a metalogic for security protocol analysis*. In Proceedings of the CombLog'04 Workshop, 2004.

The problem

The Needham-Schroeder Public-Key Authentication Protocol

$$
\begin{array}{llcl}
(\textbf{nspk}_1) & a \longrightarrow b & : & (n_1).\,\{n_1; a\}_{K_b} \\
(\textbf{nspk}_2) & b \longrightarrow a & : & (n_2).\,\{n_1; n_2\}_{K_a} \\
(\textbf{nspk}_3) & a \longrightarrow b & : & \{n_2\}_{K_b}
\end{array}
$$

The problem

The Needham-Schroeder Public-Key Authentication Protocol

$$
\begin{array}{llcl}
(\textbf{nspk}_1) & a \longrightarrow b & : & (n_1).\, \{n_1; a\}_{K_b} \\
(\textbf{nspk}_2) & b \longrightarrow a & : & (n_2).\, \{n_1; n_2\}_{K_a} \\
(\textbf{nspk}_3) & a \longrightarrow b & : & \{n_2\}_{K_b}
\end{array}
$$

- How to formalize a protocol specified in Alice&Bob-notation?
- What is the meaning of such protocol descriptions?
- How much is made explicit or left implicit?
- What is the expressive power of Alice&Bob-style protocol specifications?

A little philosophy and literary theory

deconstruction

"(noun) a method of critical analysis of language and text which emphasizes the relational quality of meaning and the assumptions implicit in forms of expression"

taken from the *Compact Oxford English Dictionary*

The plan

- Preliminaries
- The standard semantics
- Good examples and bad examples
- Message forwarding and conditional abortion
- Opaque and transparent messages
- Incremental symbolic runs
- Characterization theorems
- Conclusion and further work

Preliminaries

- Messages are built from atomic messages (identifiers, numbers, and variables) by pairing, encryption and hashing
- Perfect cryptography
- Every message can be used as an encryption key and has an inverse for decryption
- Communication is asynchronous and takes place over a hostile network

Preliminaries

- Messages are built from atomic messages (identifiers, numbers, and variables) by pairing, encryption and hashing
- Perfect cryptography
- Every message can be used as an encryption key and has an inverse for decryption
- Communication is asynchronous and takes place over a hostile network
- Honest actions
  - **s**(M, A) — sending the message M to the principal A
  - **r**(M) — receiving the message M
  - **f**(N) — generating the fresh number N

Preliminaries

In general, a protocol description in Alice&Bob-notation involves a collection of principal variables corresponding to protocol participants (a_i) and of number variables (n_j), and consists of a sequence $\langle \textbf{step}_1 \ldots \textbf{step}_m \rangle$ of message exchange steps, each of the form

$$(\textbf{step}_q) \quad a_s \to a_r \; : \; (n_{q_1}, \ldots, n_{q_t}).\, M$$

Preliminaries

In general, a protocol description in Alice&Bob-notation involves a collection of principal variables corresponding to protocol participants (a_i) and of number variables (n_j), and consists of a sequence $\langle \textbf{step}_1 \ldots \textbf{step}_m \rangle$ of message exchange steps, each of the form

$$(\textbf{step}_q) \quad a_s \rightarrow a_r \ : \ (n_{q_1}, \ldots, n_{q_t}).\ M$$

These steps are meant to prescribe a sequence of actions to be executed by each of the participants in a run of the protocol. But how?

The standard semantics

$$(\textbf{step}_q) \quad a_s \rightarrow a_r \ : \ (n_{q_1}, \ldots, n_{q_t}).\ M$$

The sequence of actions corresponding to the execution of a's role in the protocol is a-run $= \textbf{step}_1^a \centerdot \cdots \centerdot \textbf{step}_m^a$, where $\textbf{step}_q^a$ is defined by

$$\textbf{step}_q^a = \begin{cases} \langle \textbf{f}(n_{q_1}) \ldots \textbf{f}(n_{q_t}) \centerdot \textbf{s}(M, a_r) \rangle & \text{if } a = a_s \\ \langle \textbf{r}(M) \rangle & \text{if } a = a_r \\ \langle \rangle & \text{otherwise} \end{cases}$$

A good example

The Needham-Schroeder Public-Key Authentication Protocol

$$
\begin{array}{llcl}
(\textbf{nspk}_1) & a \longrightarrow b & : & (n_1).\,\{n_1; a\}_{K_b} \\
(\textbf{nspk}_2) & b \longrightarrow a & : & (n_2).\,\{n_1; n_2\}_{K_a} \\
(\textbf{nspk}_3) & a \longrightarrow b & : & \{n_2\}_{K_b}
\end{array}
$$

A good example

The Needham-Schroeder Public-Key Authentication Protocol

$$
\begin{array}{llcl}
(\textbf{nspk}_1) & a \longrightarrow b & : & (n_1).\,\{n_1; a\}_{K_b} \\
(\textbf{nspk}_2) & b \longrightarrow a & : & (n_2).\,\{n_1; n_2\}_{K_a} \\
(\textbf{nspk}_3) & a \longrightarrow b & : & \{n_2\}_{K_b}
\end{array}
$$

a-run : $\langle \mathbf{f}(n_1).\mathbf{s}(\{n_1; a\}_{K_b}, b)\,.\,\mathbf{r}(\{n_1; n_2\}_{K_a})\,.\,\mathbf{s}(\{n_2\}_{K_b}, b)\rangle$

A good example

The Needham-Schroeder Public-Key Authentication Protocol

$$
\begin{array}{llcl}
(\textbf{nspk}_1) & a \longrightarrow b & : & (n_1).\,\{n_1;a\}_{K_b} \\
(\textbf{nspk}_2) & b \longrightarrow a & : & (n_2).\,\{n_1;n_2\}_{K_a} \\
(\textbf{nspk}_3) & a \longrightarrow b & : & \{n_2\}_{K_b}
\end{array}
$$

$$a\text{-run}: \quad \langle \mathbf{f}(n_1).\mathbf{s}(\{n_1;a\}_{K_b}, b)\,.\,\mathbf{r}(\{n_1;n_2\}_{K_a})\,.\,\mathbf{s}(\{n_2\}_{K_b}, b)\rangle$$

$$b\text{-run}: \quad \langle \mathbf{r}(\{n_1;a\}_{K_b})\,.\,\mathbf{f}(n_2)\,.\,\mathbf{s}(\{n_1;n_2\}_{K_a}, a)\,.\,\mathbf{r}(\{n_2\}_{K_b})\rangle$$

Another example

The Otway-Rees Authentication/Key-Exchange Protocol

$$
\begin{array}{llcl}
(\textbf{or}_1) & a \longrightarrow b & : & (n_1).\, i; a; b; \{n_1; i; a; b\}_{K_{as}} \\
(\textbf{or}_2) & b \longrightarrow s & : & (n_2).\, i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}} \\
(\textbf{or}_3) & s \longrightarrow b & : & (\ k\ ).\, i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}} \\
(\textbf{or}_4) & b \longrightarrow a & : & \qquad i; \{n_1; k\}_{K_{as}}
\end{array}
$$

Another example

The Otway-Rees Authentication/Key-Exchange Protocol

$$
\begin{array}{llcl}
(\textbf{or}_1) & a \rightarrow b & : & (n_1).\, i; a; b; \{n_1; i; a; b\}_{K_{as}} \\
(\textbf{or}_2) & b \rightarrow s & : & (n_2).\, i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}} \\
(\textbf{or}_3) & s \rightarrow b & : & (\ k\ ).\, i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}} \\
(\textbf{or}_4) & b \rightarrow a & : & \qquad i; \{n_1; k\}_{K_{as}}
\end{array}
$$

b-run :

$\langle \mathbf{r}(i; a; b; \{n_1; i; a; b\}_{K_{as}})\,.$

$\mathbf{f}(n_2)\,.$

$\mathbf{s}(i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}}, s)\,.$

$\mathbf{r}(i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}})\,.$

$\mathbf{s}(i; \{n_1; k\}_{K_{as}}, a)\rangle$

A bad example

The Otway-Rees Authentication/Key-Exchange Protocol

$$
\begin{array}{llcl}
(\textbf{or}_1) & a \longrightarrow b & : & (n_1).\, i; a; b; \{n_1; i; a; b\}_{K_{as}} \\
(\textbf{or}_2) & b \longrightarrow s & : & (n_2).\, i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}} \\
(\textbf{or}_3) & s \longrightarrow b & : & (\ k\ ).\, i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}} \\
(\textbf{or}_4) & b \longrightarrow a & : & \qquad i; \{n_1; k\}_{K_{as}}
\end{array}
$$

b-run :

$\langle \mathbf{r}(i; a; b; \{n_1; i; a; b\}_{K_{as}})\ .$

$\mathbf{f}(n_2)\ .$

$\mathbf{s}(i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}}, s)\ .$

$\mathbf{r}(i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}})\ .$

$\mathbf{s}(i; \{n_1; k\}_{K_{as}}, a)\rangle$

Message variables

The Otway-Rees Authentication/Key-Exchange Protocol

$$
\begin{array}{llcl}
(\textbf{or}_1) & a \rightarrow b & : & (n_1).\, i; a; b; \{n_1; i; a; b\}_{K_{as}} \\
(\textbf{or}_2) & b \rightarrow s & : & (n_2).\, i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}} \\
(\textbf{or}_3) & s \rightarrow b & : & (\ k\ ).\, i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}} \\
(\textbf{or}_4) & b \rightarrow a & : & i; \{n_1; k\}_{K_{as}}
\end{array}
$$

b-run :

$\langle \mathbf{r}(i; a; b; \{n_1; i; a; b\}_{K_{as}})\ .$

$\mathbf{f}(n_2)\ .$

$\mathbf{s}(i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}}, s)\ .$

$\mathbf{r}(i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}})\ .$

$\mathbf{s}(i; \{n_1; k\}_{K_{as}}, a)\rangle$

symbolic b-possrun :

$\langle \mathbf{r}(i; a; b; m_1)\ .$

$\mathbf{f}(n_2)\ .$

$\mathbf{s}(i; a; b; m_1; \{n_2; i; a; b\}_{K_{bs}}, s)\ .$

$\mathbf{r}(i; m_2; \{n_2; k\}_{K_{bs}})\ .$

$\mathbf{s}(i; m_2, a)\rangle$

Message variables

The Otway-Rees Authentication/Key-Exchange Protocol

$$
\begin{array}{llcl}
(\textbf{or}_1) & a \longrightarrow b & : & (n_1).\, i; a; b; \{n_1; i; a; b\}_{K_{as}} \\
(\textbf{or}_2) & b \longrightarrow s & : & (n_2).\, i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}} \\
(\textbf{or}_3) & s \longrightarrow b & : & (\ k\ ).\, i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}} \\
(\textbf{or}_4) & b \longrightarrow a & : & \quad i; \{n_1; k\}_{K_{as}}
\end{array}
$$

Message Forwarding

symbolic b-possrun :

$\langle \mathbf{r}(i; a; b; m_1)\ .$

$\mathbf{f}(n_2)\ .$

$\mathbf{s}(i; a; b; m_1; \{n_2; i; a; b\}_{K_{bs}}, s)\ .$

$\mathbf{r}(i; m_2; \{n_2; k\}_{K_{bs}})\ .$

$\mathbf{s}(i; m_2, a)\rangle$

Another bad example

The Asokan-Shoup-Waidner Optimistic Fair-Exchange Subprotocol

(**asw**$_1$)	$a \longrightarrow b$	:	$(n_1).\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}$
(**asw**$_2$)	$b \longrightarrow a$	:	$(n_2).\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}}$
(**asw**$_3$)	$a \longrightarrow b$	:	n_1
(**asw**$_4$)	$b \longrightarrow a$	:	n_2

Another bad example

The Asokan-Shoup-Waidner Optimistic Fair-Exchange Subprotocol

$$
\begin{array}{llll}
(\textbf{asw}_1) & a \longrightarrow b & : & (n_1).\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}} \\
(\textbf{asw}_2) & b \longrightarrow a & : & (n_2).\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}} \\
(\textbf{asw}_3) & a \longrightarrow b & : & \quad n_1 \\
(\textbf{asw}_4) & b \longrightarrow a & : & \quad n_2
\end{array}
$$

b-run :

$\langle \mathbf{r}(\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}) . \quad \mathbf{f}(n_2) . \mathbf{s}(\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; \quad H(n_2)\}_{K_b^{-1}}, a) . \mathbf{r}(n_1) . \quad \mathbf{s}(n_2, a) \rangle$

Another bad example

The Asokan-Shoup-Waidner Optimistic Fair-Exchange Subprotocol

$$
\begin{array}{llcl}
(\textbf{asw}_1) & a \rightarrow b & : & (n_1).\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}} \\
(\textbf{asw}_2) & b \rightarrow a & : & (n_2).\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}} \\
(\textbf{asw}_3) & a \rightarrow b & : & n_1 \\
(\textbf{asw}_4) & b \rightarrow a & : & n_2
\end{array}
$$

b-run :

$$\langle \mathbf{r}(\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}) . \quad \mathbf{f}(n_2) . \mathbf{s}(\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; \quad H(n_2)\}_{K_b^{-1}}, a) . \mathbf{r}(n_1) . \quad \mathbf{s}(n_2, a) \rangle$$

Message Variables Needed

Even so ...

The Asokan-Shoup-Waidner Optimistic Fair-Exchange Subprotocol

$$
\begin{array}{llll}
(\textbf{asw}_1) & a \longrightarrow b & : & (n_1).\,\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}} \\
(\textbf{asw}_2) & b \longrightarrow a & : & (n_2).\,\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}} \\
(\textbf{asw}_3) & a \longrightarrow b & : & \quad n_1 \\
(\textbf{asw}_4) & b \longrightarrow a & : & \quad n_2
\end{array}
$$

b-possrun :

$\langle \mathbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}})\,.\quad \mathbf{f}(n_2)\,.\mathbf{s}(\{\{K_a; K_b; t; m_1\}_{K_a^{-1}}; \quad H(n_2)\}_{K_b^{-1}}, a)\,.\mathbf{r}(n_1)\,.\quad \mathbf{s}(n_2, a)\rangle$

Even so ...

The Asokan-Shoup-Waidner Optimistic Fair-Exchange Subprotocol

$$
\begin{array}{llll}
(\textbf{asw}_1) & a \rightarrow b & : & (n_1).\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}} \\
(\textbf{asw}_2) & b \rightarrow a & : & (n_2).\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}} \\
(\textbf{asw}_3) & a \rightarrow b & : & n_1 \\
(\textbf{asw}_4) & b \rightarrow a & : & n_2
\end{array}
$$

b-possrun :

$\langle \textbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}}) . \quad \textbf{f}(n_2) . \textbf{s}(\{\{K_a; K_b; t; m_1\}_{K_a^{-1}}; \quad H(n_2)\}_{K_b^{-1}}, a) . \textbf{r}(n_1) . \quad \textbf{s}(n_2, a) \rangle$

Eager Check
Needed

With eager checking

The Asokan-Shoup-Waidner Optimistic Fair-Exchange Subprotocol

$$\begin{array}{llcl}
(\textbf{asw}_1) & a \longrightarrow b & : & (n_1).\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}} \\
(\textbf{asw}_2) & b \longrightarrow a & : & (n_2).\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}} \\
(\textbf{asw}_3) & a \longrightarrow b & : & n_1 \\
(\textbf{asw}_4) & b \longrightarrow a & : & n_2
\end{array}$$

b-possrun :

$\langle \mathbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}}) . \ \mathbf{f}(n_2) . \mathbf{s}(\{\{K_a; K_b; t; m_1\}_{K_a^{-1}}; \ H(n_2)\}_{K_b^{-1}}, a) . \mathbf{r}(n_1) . \ \mathbf{s}(n_2, a)\rangle$

b-possruns :

$\langle \mathbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}})\rangle$

$\langle \mathbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}}) . \ \mathbf{f}(n_2)\rangle$

$\langle \mathbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}}) . \ \mathbf{f}(n_2) . \mathbf{s}(\{\{K_a; K_b; t; m_1\}_{K_a^{-1}}; \ H(n_2)\}_{K_b^{-1}}, a)\rangle$

$\langle \mathbf{r}(\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}) . \ \mathbf{f}(n_2) . \mathbf{s}(\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; \ H(n_2)\}_{K_b^{-1}}, a) . \mathbf{r}(n_1)\rangle$

$\langle \mathbf{r}(\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}) . \ \mathbf{f}(n_2) . \mathbf{s}(\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; \ H(n_2)\}_{K_b^{-1}}, a) . \mathbf{r}(n_1) . \ \mathbf{s}(n_2, a)\rangle$

With eager checking

The Asokan-Shoup-Waidner Optimistic Fair-Exchange Subprotocol

$$
\begin{array}{llll}
(\textbf{asw}_1) & a \longrightarrow b & : & (n_1).\,\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}} \\
(\textbf{asw}_2) & b \longrightarrow a & : & (n_2).\,\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}} \\
(\textbf{asw}_3) & a \longrightarrow b & : & n_1 \\
(\textbf{asw}_4) & b \longrightarrow a & : & n_2
\end{array}
$$

Conditional Abortion

b-possruns :

$\langle \mathbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}})\rangle$

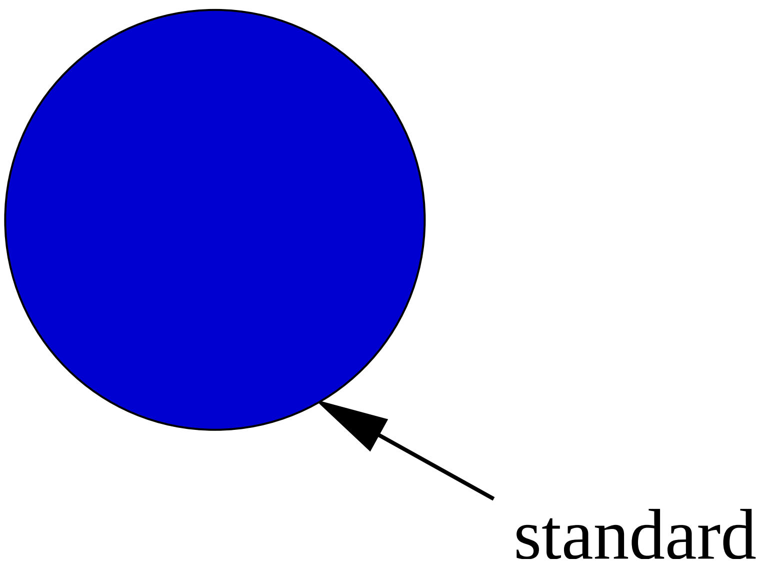
$\langle \mathbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}})\,.\;\mathbf{f}(n_2)\rangle$

$\langle \mathbf{r}(\{K_a; K_b; t; m_1\}_{K_a^{-1}})\,.\;\mathbf{f}(n_2)\,.\mathbf{s}(\{\{K_a; K_b; t; m_1\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}}, a)\rangle$

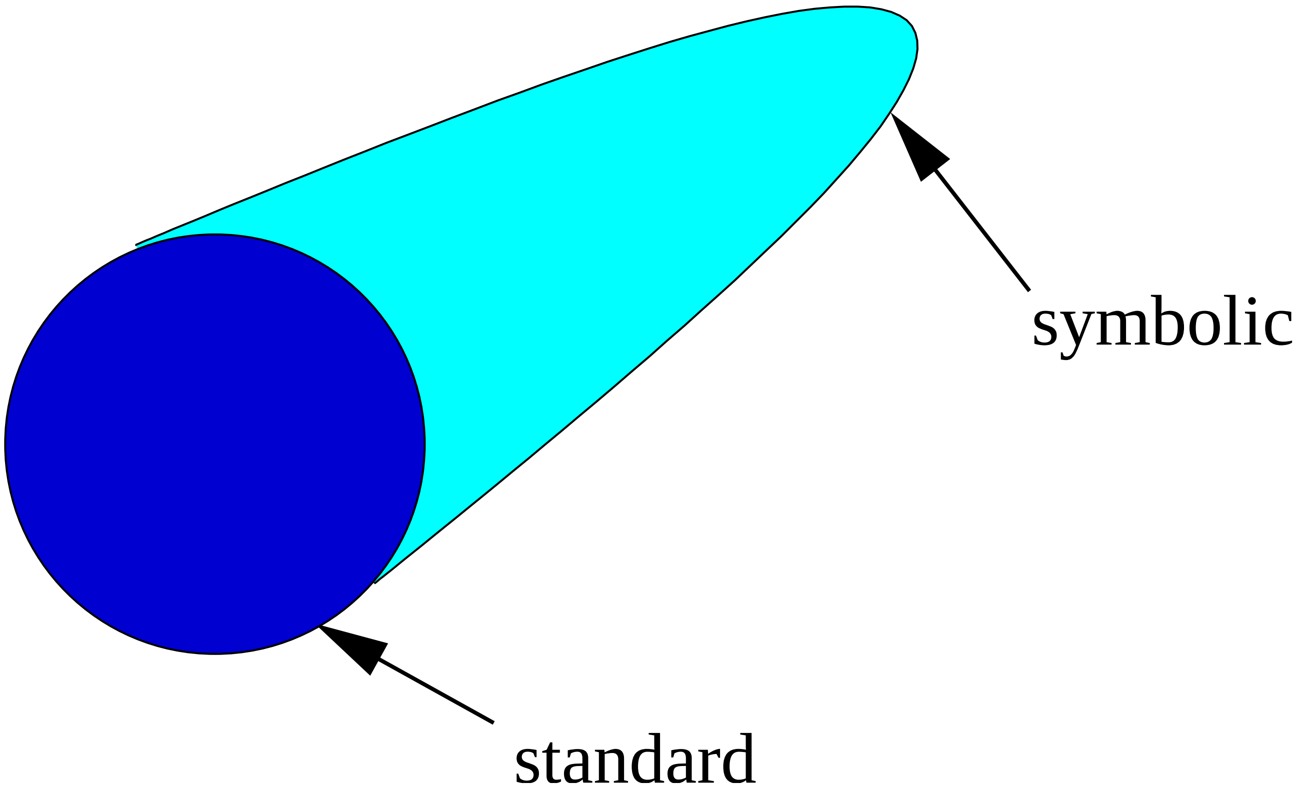
$\langle \mathbf{r}(\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}})\,.\;\mathbf{f}(n_2)\,.\mathbf{s}(\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}}, a)\,.\mathbf{r}(n_1)\rangle$

$\langle \mathbf{r}(\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}})\,.\;\mathbf{f}(n_2)\,.\mathbf{s}(\{\{K_a; K_b; t; H(n_1)\}_{K_a^{-1}}; H(n_2)\}_{K_b^{-1}}, a)\,.\mathbf{r}(n_1)\,.\;\mathbf{s}(n_2, a)\rangle$

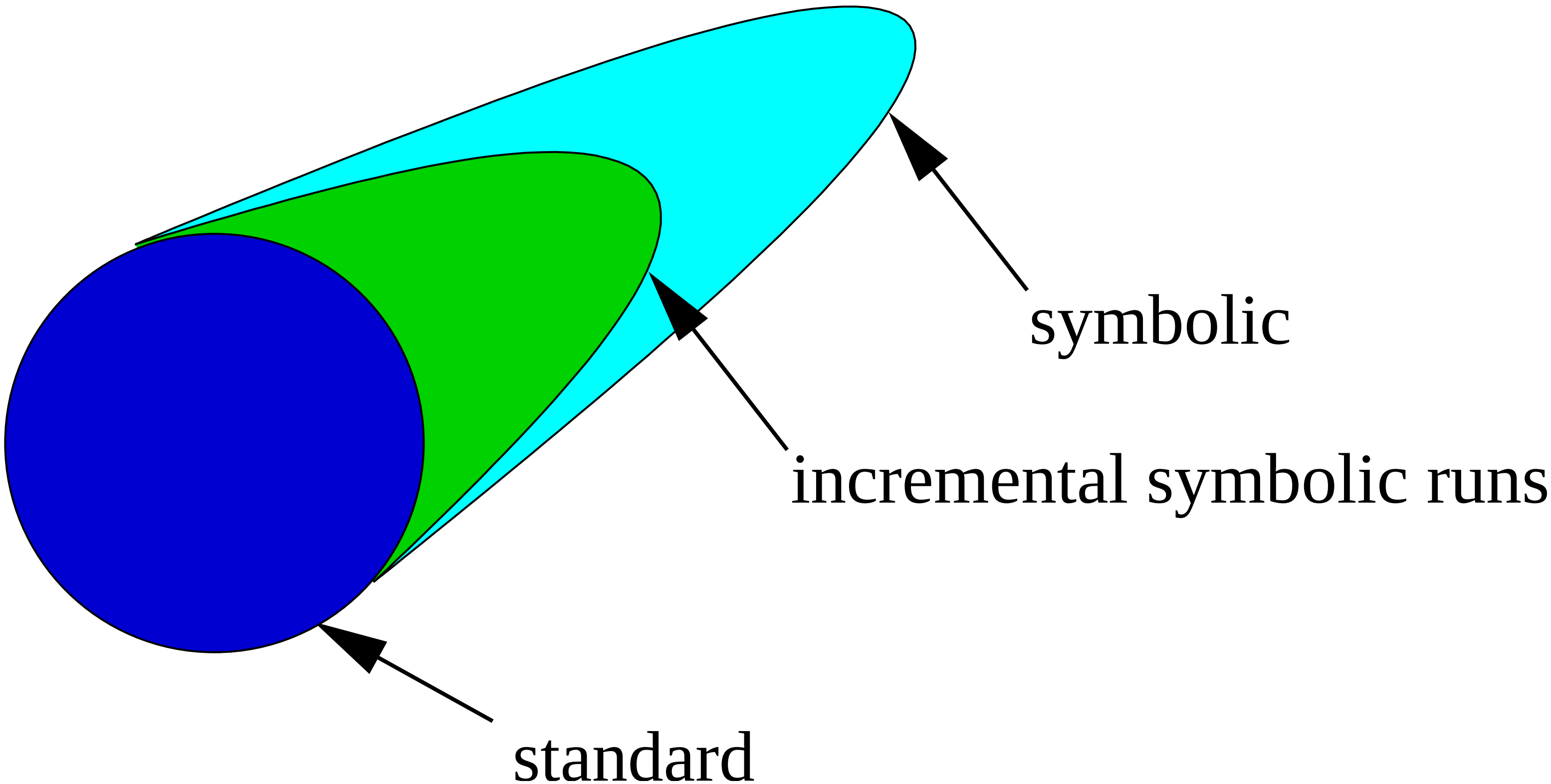
Forwarding and conditional abortion



Forwarding and conditional abortion



Forwarding and conditional abortion



Opaque and transparent messages

analysis

$$\frac{M_1; M_2}{M_1} \qquad \frac{M_1; M_2}{M_2} \qquad \frac{\{M\}_K \quad K^{-1}}{M}$$

synthesis

$$\underbrace{\frac{M_1 \quad M_2}{M_1; M_2} \qquad \frac{M \quad K}{\{M\}_K} \qquad \frac{M}{H(M)}}_{\textit{close}(S)}$$

Opaque and transparent messages

a-run $= \langle \textbf{act}_1, \ldots, \textbf{act}_s \rangle$ initial data D_a^0

$$D_a^0 \xrightarrow{\textbf{act}_1} D_a^1 \xrightarrow{\textbf{act}_2} D_a^2 \xrightarrow{\textbf{act}_3} \cdots \xrightarrow{\textbf{act}_{s-1}} D_a^{s-1} \xrightarrow{\textbf{act}_s} D_a^s$$

$$D_a^{i+1} = \begin{cases} D_a^i & \text{if } \textbf{act}_{i+1} = \textbf{s}(M, y) \\ \textit{close}(D_a^i \cup \{M\}) & \text{if } \textbf{act}_{i+1} = \textbf{r}(M) \\ \textit{close}(D_a^i \cup \{n\}) & \text{if } \textbf{act}_{i+1} = \textbf{f}(n) \end{cases}$$

Opaque and transparent messages

a-run $= \langle \textbf{act}_1, \ldots, \textbf{act}_s \rangle$ initial data D_a^0

$$D_a^0 \xrightarrow{\textbf{act}_1} D_a^1 \xrightarrow{\textbf{act}_2} D_a^2 \xrightarrow{\textbf{act}_3} \cdots \xrightarrow{\textbf{act}_{s-1}} D_a^{s-1} \xrightarrow{\textbf{act}_s} D_a^s$$

$$D_a^{i+1} = \begin{cases} D_a^i & \text{if } \textbf{act}_{i+1} = \textbf{s}(M, y) \\ \textit{close}(D_a^i \cup \{M\}) & \text{if } \textbf{act}_{i+1} = \textbf{r}(M) \\ \textit{close}(D_a^i \cup \{n\}) & \text{if } \textbf{act}_{i+1} = \textbf{f}(n) \end{cases}$$

Executability

for each participant a and $1 \leq i \leq t$, if $\textbf{act}_i = \textbf{s}(M, b)$ then $M \in D_a^{i-1}$

Opaque and transparent messages

Given the closed dataset D

$$v_D(M) = \begin{cases} M & \text{if } M \text{ is atomic} \\ v_D(M_1); v_D(M_2) & \text{if } M = M_1; M_2 \\ \{v_D(M_1)\}_{v_D(K)} & \text{if } M = \{M_1\}_K \text{ and } K^{-1} \in D \text{ or } M_1, K \in D \\ H(v_D(M_1)) & \text{if } M = H(M_1) \text{ and } M_1 \in D \\ m_M & \text{otherwise} \end{cases}$$

Opaque and transparent messages

Given the closed dataset D

$$v_D(M) = \begin{cases} M & \text{if } M \text{ is atomic} \\ v_D(M_1); v_D(M_2) & \text{if } M = M_1; M_2 \\ \{v_D(M_1)\}_{v_D(K)} & \text{if } M = \{M_1\}_K \text{ and } K^{-1} \in D \text{ or } M_1, K \in D \\ H(v_D(M_1)) & \text{if } M = H(M_1) \text{ and } M_1 \in D \\ m_M & \text{otherwise} \end{cases}$$

Abadi and Rogaway. *Reconciling two views of cryptography*. Journal of Cryptology 15(2):103–127, 2002.

Opaque and transparent messages

Given the closed dataset D

$$v_D(M) = \begin{cases} M & \text{if } M \text{ is atomic} \\ v_D(M_1); v_D(M_2) & \text{if } M = M_1; M_2 \\ \{v_D(M_1)\}_{v_D(K)} & \text{if } M = \{M_1\}_K \text{ and } K^{-1} \in D \text{ or } M_1, K \in D \\ H(v_D(M_1)) & \text{if } M = H(M_1) \text{ and } M_1 \in D \\ m_M & \text{otherwise} \end{cases}$$

A message M is

- D-transparent if $v_D(M) = M$
- D-opaque if $v_D(M) = m_M$, i.e.
  - $M = \{M_1\}_K$, $K^{-1} \notin D$ and $\{M_1, K\} \not\subseteq D$, or else
  - $M = H(M_1)$ and $M_1 \notin D$

Opaque and transparent messages

Given the closed dataset D

$$v_D(M) = \begin{cases} M & \text{if } M \text{ is atomic} \\ v_D(M_1); v_D(M_2) & \text{if } M = M_1; M_2 \\ \{v_D(M_1)\}_{v_D(K)} & \text{if } M = \{M_1\}_K \text{ and } K^{-1} \in D \text{ or } M_1, K \in D \\ H(v_D(M_1)) & \text{if } M = H(M_1) \text{ and } M_1 \in D \\ m_M & \text{otherwise} \end{cases}$$

A message M is

- D-transparent if $v_D(M) = M$
- D-opaque if $v_D(M) = m_M$, i.e.
  - $M = \{M_1\}_K$, $K^{-1} \notin D$ and $\{M_1, K\} \not\subseteq D$, or else
  - $M = H(M_1)$ and $M_1 \notin D$

Eagerness

Incremental symbolic runs

a-run $= \langle \textbf{act}_1, \ldots, \textbf{act}_s \rangle$ initial data D_a^0

$$D_a^0 \xrightarrow{\textbf{act}_1} D_a^1 \xrightarrow{\textbf{act}_2} D_a^2 \xrightarrow{\textbf{act}_3} \cdots \xrightarrow{\textbf{act}_{s-1}} D_a^{s-1} \xrightarrow{\textbf{act}_s} D_a^s$$

Incremental symbolic runs

a-run $= \langle \textbf{act}_1, \ldots, \textbf{act}_s \rangle$ initial data D_a^0

$$D_a^0 \xrightarrow{\textbf{act}_1} D_a^1 \xrightarrow{\textbf{act}_2} D_a^2 \xrightarrow{\textbf{act}_3} \cdots \xrightarrow{\textbf{act}_{s-1}} D_a^{s-1} \xrightarrow{\textbf{act}_s} D_a^s$$

a-possrun$_1$: $\langle \textbf{act}_1^1 \rangle$
a-possrun$_2$: $\langle \textbf{act}_1^2 \,.\, \textbf{act}_2^2 \rangle$
a-possrun$_3$: $\langle \textbf{act}_1^3 \,.\, \textbf{act}_2^3 \,.\, \textbf{act}_3^3 \rangle$
$\ldots$
a-possrun$_s$: $\langle \textbf{act}_1^s \,.\, \textbf{act}_2^s \,.\, \textbf{act}_3^s \,.\, \ldots \,.\, \textbf{act}_s^s \rangle$

where each a-possrun$_i = v_{D_a^i}(a\text{-run}|_i)$, i.e. $\textbf{act}_j^i = v_{D_a^i}(\textbf{act}_j)$

Characterization theorems

The Needham-Schroeder Public-Key Authentication Protocol

$$
\begin{array}{llcl}
(\textbf{nspk}_1) & a \longrightarrow b & : & (n_1).\,\{n_1;a\}_{K_b} \\
(\textbf{nspk}_2) & b \longrightarrow a & : & (n_2).\,\{n_1;n_2\}_{K_a} \\
(\textbf{nspk}_3) & a \longrightarrow b & : & \{n_2\}_{K_b}
\end{array}
$$

a-run : $\langle \textbf{f}(n_1).\textbf{s}(\{n_1;a\}_{K_b},b)\,.\,\textbf{r}(\{n_1;n_2\}_{K_a})\,.\,\textbf{s}(\{n_2\}_{K_b},b)\rangle$

Characterization theorems

The Needham-Schroeder Public-Key Authentication Protocol

$$
\begin{array}{llcl}
(\textbf{nspk}_1) & a \longrightarrow b & : & (n_1).\ \{n_1; a\}_{K_b} \\
(\textbf{nspk}_2) & b \longrightarrow a & : & (n_2).\ \{n_1; n_2\}_{K_a} \\
(\textbf{nspk}_3) & a \longrightarrow b & : & \{n_2\}_{K_b}
\end{array}
$$

a-run : $\langle \mathbf{f}(n_1).\mathbf{s}(\{n_1; a\}_{K_b}, b)\,.\,\mathbf{r}(\{n_1; n_2\}_{K_a})\,.\,\mathbf{s}(\{n_2\}_{K_b}, b)\rangle$

a-possrun$_1$: $\langle \mathbf{f}(n_1)\rangle$

a-possrun$_2$: $\langle \mathbf{f}(n_1)\,.\,\mathbf{s}(\{n_1; a\}_{K_b}, b)\rangle$

a-possrun$_3$: $\langle \mathbf{f}(n_1)\,.\,\mathbf{s}(\{n_1; a\}_{K_b}, b)\,.\,\mathbf{r}(\{n_1; n_2\}_{K_a})\rangle$

a-possrun$_4$: $\langle \mathbf{f}(n_1)\,.\,\mathbf{s}(\{n_1; a\}_{K_b}, b)\,.\,\mathbf{r}(\{n_1; n_2\}_{K_a})\,.\,\mathbf{s}(\{n_2\}_{K_b}, b)\rangle$

Characterization theorems

Theorem
The standard sequence a-run is representative if and only if every received message is transparent when it is received, i.e. if $\mathbf{act}_i = \mathbf{r}(M)$, then M is D_a^i-transparent.

Characterization theorems

Theorem
The standard sequence a-run is representative if and only if every received message is transparent when it is received, i.e. if $\mathbf{act}_i = \mathbf{r}(M)$, then M is D_a^i-transparent.

For instance, NSPK fulfils this condition
Otway-Rees and Asokan-Shoup-Waidner do not

Characterization theorems

The Otway-Rees Authentication/Key-Exchange Protocol

$$\begin{array}{llcl}
(\textbf{or}_1) & a \rightarrow b & : & (n_1).\, i; a; b; \{n_1; i; a; b\}_{K_{as}} \\
(\textbf{or}_2) & b \rightarrow s & : & (n_2).\, i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}} \\
(\textbf{or}_3) & s \rightarrow b & : & (\ k\ ).\, i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}} \\
(\textbf{or}_4) & b \rightarrow a & : & \qquad i; \{n_1; k\}_{K_{as}}
\end{array}$$

b-possrun :

$\langle \mathbf{r}(i; a; b; m_1) \,.\, \mathbf{f}(n_2) \,.\, \mathbf{s}(i; a; b; m_1; \{n_2; i; a; b\}_{K_{bs}}, s) \,.\, \mathbf{r}(i; m_2; \{n_2; k\}_{K_{bs}}) \,.\, \mathbf{s}(i; m_2, a) \rangle$

Characterization theorems

The Otway-Rees Authentication/Key-Exchange Protocol

$$
\begin{array}{llcl}
(\textbf{or}_1) & a \rightarrow b & : & (n_1).\, i; a; b; \{n_1; i; a; b\}_{K_{as}} \\
(\textbf{or}_2) & b \rightarrow s & : & (n_2).\, i; a; b; \{n_1; i; a; b\}_{K_{as}}; \{n_2; i; a; b\}_{K_{bs}} \\
(\textbf{or}_3) & s \rightarrow b & : & (\ k\ ).\, i; \{n_1; k\}_{K_{as}}; \{n_2; k\}_{K_{bs}} \\
(\textbf{or}_4) & b \rightarrow a & : & \qquad i; \{n_1; k\}_{K_{as}}
\end{array}
$$

b-possrun :

$\langle \textbf{r}(i; a; b; m_1) \,.\, \textbf{f}(n_2) \,.\, \textbf{s}(i; a; b; m_1; \{n_2; i; a; b\}_{K_{bs}}, s) \,.\, \textbf{r}(i; m_2; \{n_2; k\}_{K_{bs}}) \,.\, \textbf{s}(i; m_2, a)\rangle$

b-possruns :

$\langle \textbf{r}(i; a; b; m_1)\rangle$

$\langle \textbf{r}(i; a; b; m_1) \,.\, \textbf{f}(n_2)\rangle$

$\langle \textbf{r}(i; a; b; m_1) \,.\, \textbf{f}(n_2) \,.\, \textbf{s}(i; a; b; m_1; \{n_2; i; a; b\}_{K_{bs}}, s)\rangle$

$\langle \textbf{r}(i; a; b; m_1) \,.\, \textbf{f}(n_2) \,.\, \textbf{s}(i; a; b; m_1; \{n_2; i; a; b\}_{K_{bs}}, s) \,.\, \textbf{r}(i; m_2; \{n_2; k\}_{K_{bs}})\rangle$

$\langle \textbf{r}(i; a; b; m_1) \,.\, \textbf{f}(n_2) \,.\, \textbf{s}(i; a; b; m_1; \{n_2; i; a; b\}_{K_{bs}}, s) \,.\, \textbf{r}(i; m_2; \{n_2; k\}_{K_{bs}}) \,.\, \textbf{s}(i; m_2, a)\rangle$

Characterization theorems

Theorem

The symbolic sequence a-possrun is representative if and only if every received message preserves the message variables that occur in the views of previously received messages, i.e.
if $j < i$, $\textbf{act}_j$ and $\textbf{act}_i$ are receiving actions, and m_M occurs in $v_{D_x^{i-1}}(\textbf{act}_j)$, then m_M also occurs in $v_{D_x^i}(\textbf{act}_j)$.

Characterization theorems

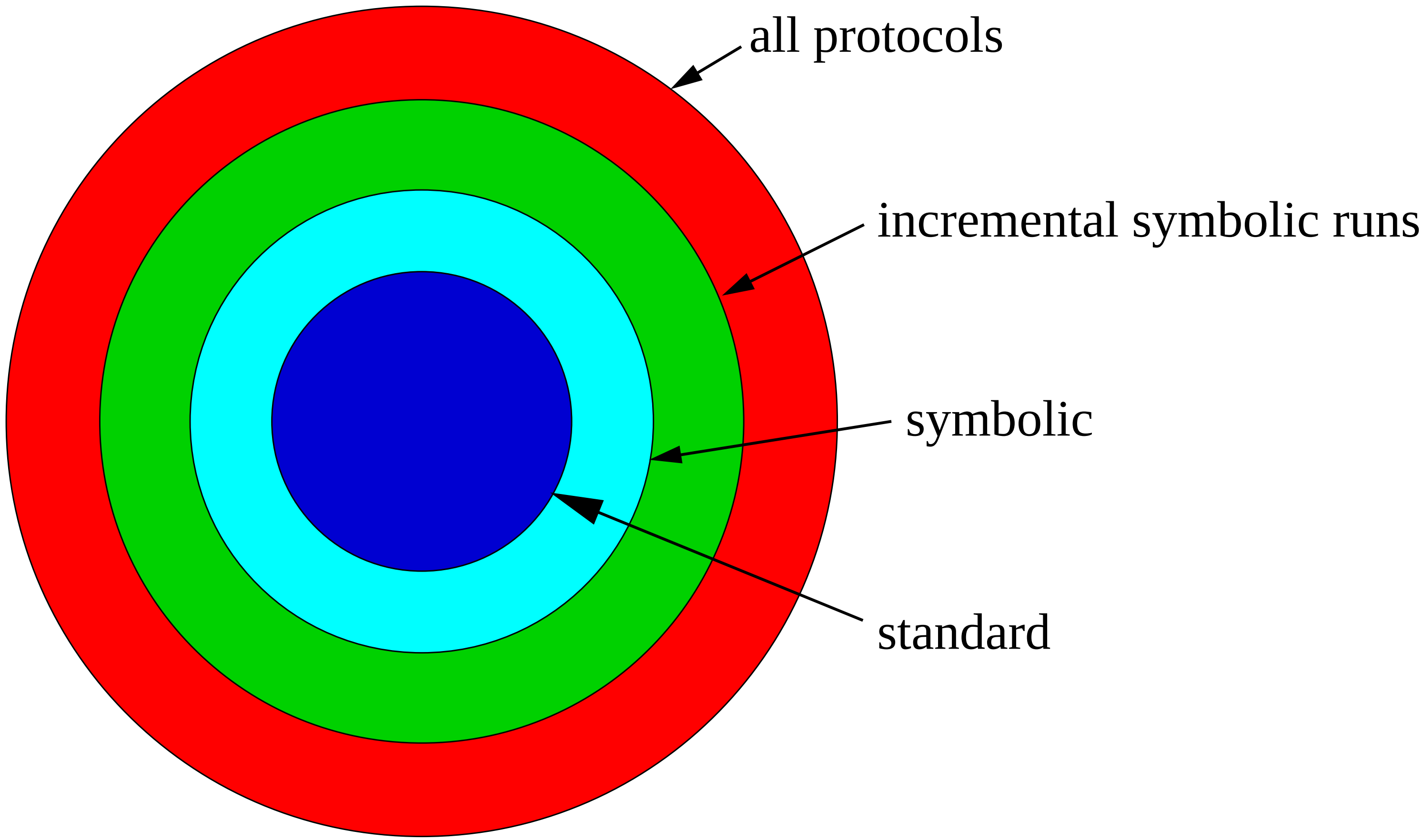
Theorem

The symbolic sequence a-possrun is representative if and only if every received message preserves the message variables that occur in the views of previously received messages, i.e. if $j < i$, $\mathbf{act}_j$ and $\mathbf{act}_i$ are receiving actions, and m_M occurs in $v_{D_x^{i-1}}(\mathbf{act}_j)$, then m_M also occurs in $v_{D_x^i}(\mathbf{act}_j)$.

For instance, NSPK and Otway-Rees fulfill this condition

Still, Asokan-Shoup-Waidner does not

Characterization theorems



Conclusion and further work

- Denotational semantics of Alice&Bob-style protocol specifications
  - Incremental symbolic runs
  - Message forwarding
  - Conditional abortion
- Operational semantics
  - Basis for automated protocol analysis tools
  - Step towards implementation
- Fill in the gap between Alice&Bob-notation and HLPSL
- Distributed temporal logic
  - Object level and metalevel reasoning
  - Reduction results
  - Calculus

Conclusion and further work

- Denotational semantics of Alice&Bob-style protocol specifications
  - Incremental symbolic runs
  - Message forwarding
  - Conditional abortion
- Operational semantics
  - Basis for automated protocol analysis tools
  - Step towards implementation
- Fill in the gap between Alice&Bob-notation and HLPSL
- Distributed temporal logic
  - Object level and metalevel reasoning
  - Reduction results
  - Calculus

Thank you!