Metareasoning about Security Protocols using Distributed Temporal Logic

Carlos Caleiro
Dep. Mathematics, IST, TU Lisbon, Portugal

Luca Viganò David Basin
Dep. Computer Science, ETH Zurich, Switzerland

ARSPA WS at IJCAR’04, Cork, Ireland
July 4, 2004
Motivation

- Formal methods for security protocol analysis
- Most problems due to communication and distribution, rather than cryptography
- Many models, many simplifications, many assumptions
Motivation

- Formal methods for security protocol analysis
- Most problems due to communication and distribution, rather than cryptography
- Many models, many simplifications, many assumptions

Goal

- Use a protocol independent distributed temporal logic
- Formalize different models, protocols and security goals
- Prove the correctness of modeling and reasoning simplification techniques
Plan

- Overview of distributed temporal logic
- A simple network model
- Protocol modeling and security goals
- Metareasoning examples
  - Secrecy lemma
  - One intruder is enough
  - The predatory intruder
Distributed temporal logic


H.-D. Ehrich, C. Caleiro, A. Sernadas, and G. Denker.

H.-D. Ehrich and C. Caleiro.
Distributed temporal logic


H.-D. Ehrich, C. Caleiro, A. Sernadas, and G. Denker.

H.-D. Ehrich and C. Caleiro.

\[ \@_i[X \@_j[F \@_u[athome]]] \]

“I will next call Jean and tell her to call you later, when you are at home”
Distributed temporal logic

\[ \Diamond_i [X \Diamond_j [F \Diamond_u [\text{athome}]]] \]

“I will next call Jean and tell her to call you later, when you are at home”
Distributed temporal logic

\[ @_i [ X \ @_j [ F \ @_u [ athome ] ] ] \]

“I will next call Jean and tell her to call you later, when you are at home”
Distributed temporal logic

\[ @_i [ X @_j [ F @_u [ \text{athome} ] ] ] \]

“I will next call Jean and tell her to call you later, when you are at home”
Distributed temporal logic

\[ \text{@}i[X \text{@}j[F \text{@}u[athome]]] \]

“I will next call Jean and tell her to call you later, when you are at home”
Distributed temporal logic

@i[X @j[F @u[athome]]]

“I will next call Jean and tell her to call you later, when you are at home”
Syntax

Distributed signature \( \Sigma = \langle \text{Id}, \{\text{Act}_i\}_{i \in \text{Id}}, \{\text{Prop}_i\}_{i \in \text{Id}} \rangle \)

- \( \text{Id} \) finite set of agent identifiers
- each \( \text{Act}_i \) is a set of local action symbols
- each \( \text{Prop}_i \) is a set of local state propositions

\[
\mathcal{L} ::= @i[\mathcal{L}_i] \mid \bot \mid \mathcal{L} \Rightarrow \mathcal{L}
\]

\[
\mathcal{L}_i ::= \text{Act}_i \mid \text{Prop}_i \mid \bot \mid \mathcal{L}_i \Rightarrow \mathcal{L}_i \mid \mathcal{L}_i \cup \mathcal{L}_i \mid \mathcal{L}_i \cap \mathcal{L}_i \mid @j[\mathcal{L}_j]
\]
Models

\[ \mu = \langle \lambda, \alpha, \pi \rangle \]
Models

\[ \mu = \langle \lambda, \alpha, \pi \rangle \]

\[ \lambda \left\{ \begin{array}{l}
i \quad e_1 \rightarrow e_4 \rightarrow e_5 \rightarrow e_8 \rightarrow \ldots \\
j \quad e_2 \rightarrow e_4 \rightarrow e_7 \rightarrow e_8 \rightarrow \ldots \\
k \quad e_3 \rightarrow e_4 \rightarrow e_6 \rightarrow e_7 \rightarrow e_9 \rightarrow \ldots \\
\end{array} \right. \]

Global configurations \( \Xi \)
Models

\[ \mu = \langle \lambda, \alpha, \pi \rangle \]

Global configurations \( \Xi \)
Models

$$\mu = \langle \lambda, \alpha, \pi \rangle$$

Local configurations $$\Xi_i$$
Models

\( \mu = \langle \lambda, \alpha, \pi \rangle \)

\[
\begin{align*}
\lambda \quad & \left\{ 
\begin{array}{c}
i \quad e_1 \Downarrow e_4 \quad e_5 \quad \cdots \quad e_8 \\
j \quad e_2 \quad e_4 \quad e_7 \quad e_8 \quad \cdots \\
k \quad e_3 \quad e_4 \quad e_6 \quad e_7 \quad e_9 \quad \cdots 
\end{array} \right. \\
\emptyset \quad & \{ e_1 \}
\end{align*}
\]

Local configurations \( \Xi_i \)
Models

\( \mu = \langle \lambda, \alpha, \pi \rangle \)

\( \lambda \)

\[
\begin{array}{c}
\emptyset \quad \{e_1\} \quad \{e_1, e_4\} \\
\{e_1\} \quad \{e_1, e_4\}\end{array}
\]

Local configurations \( \Xi_i \)
Models

\( \mu = \langle \lambda, \alpha, \pi \rangle \)

\[
\begin{align*}
\lambda & \quad \left\{ 
\begin{array}{l}
i \quad e_1 \rightarrow e_4 \rightarrow e_5 \rightarrow e_8 \rightarrow \cdots \\
j \quad e_2 \rightarrow e_4 \rightarrow e_7 \rightarrow e_8 \rightarrow \cdots \\
k \quad e_3 \rightarrow e_4 \rightarrow e_6 \rightarrow e_7 \rightarrow e_9 \rightarrow \cdots \\
\emptyset \quad \{e_1\} \quad \{e_1, e_4\} \quad \{e_1, e_4, e_5\}
\end{array}
\right. 
\end{align*}
\]

Local configurations \( \Xi_i \)
Models

\( \mu = \langle \lambda, \alpha, \pi \rangle \)

\[
\begin{align*}
\lambda & \quad \\
& \quad \\
& \quad \\
\lambda & \\
\end{align*}
\]

\[
\begin{align*}
i & \quad e_1 \rightarrow e_4 \rightarrow e_5 \rightarrow e_8 \\
j & \quad e_2 \rightarrow e_4 \rightarrow e_7 \rightarrow e_8 \\
k & \quad e_3 \rightarrow e_4 \rightarrow e_6 \rightarrow e_7 \rightarrow e_9 \\
\emptyset & \quad \{e_1\} \quad \{e_1, e_4\} \quad \{e_1, e_4, e_5\} \quad \{e_1, e_4, e_5, e_8\} \quad \cdots
\end{align*}
\]

Local configurations \( \Xi_i \)
Models

\[ \mu = \langle \lambda, \alpha, \pi \rangle \]

\[ \lambda \left\{ \begin{array}{c}
i & e_1 & \rightarrow & e_4 & \rightarrow & e_5 & \rightarrow & \cdots & e_8 & \rightarrow & \cdots \\
j & e_2 & \rightarrow & e_4 & \rightarrow & e_7 & \rightarrow & e_8 & \rightarrow & \cdots \\
k & e_3 & \rightarrow & e_4 & \rightarrow & e_6 & \rightarrow & e_7 & \rightarrow & e_9 & \rightarrow & \cdots \\
\end{array} \right. \]

\[ \alpha = \{ \alpha_i \}_{i \in Id}, \text{ each } \alpha_i : Ev_i \rightarrow Act_i \]

\[ \pi = \{ \pi_i \}_{i \in Id}, \text{ each } \pi_i : \Xi_i \rightarrow 2^\text{Prop}_i \]

\[ \pi_i(0) \xrightarrow{\alpha_i(e_1)} \pi_i(\{e_1\}) \xrightarrow{\alpha_i(e_4)} \pi_i(\{e_1, e_4\}) \xrightarrow{\alpha_i(e_5)} \pi_i(\{e_1, e_4, e_5\}) \rightarrow \cdots \]
Satisfaction

The global satisfaction relation at a given global configuration $\xi$ of $\mu$ is:

- $\mu, \xi \models @_i[\varphi]$ if $\mu, \xi |_i \models \varphi$;
- $\mu, \xi \not\models \perp$; and $\mu, \xi \models \gamma \Rightarrow \delta$ if $\mu, \xi \not\models \gamma$ or $\mu, \xi \models \delta$, where

the local satisfaction relations at given local configurations are:

- $\mu, \xi_i \models i \text{ act}$ if $\xi_i \neq \emptyset$ and $\alpha_i(\text{last}(\xi_i)) = \text{act}$;
- $\mu, \xi_i \models i \ p$ if $p \in \sigma_i(\xi_i)$;
- $\mu, \xi_i \not\models i \perp$; and $\mu, \xi_i \models i \varphi \Rightarrow \psi$ if $\mu, \xi_i \not\models i \varphi$ or $\mu, \xi_i \models i \psi$;
- $\mu, \xi_i \models i \varphi \cup \psi$ if there exists $\xi''_i \in \Xi_i$ with $\xi_i \subsetneq \xi''_i$ such that $\mu, \xi''_i \models i \psi$, and $\mu, \xi'_i \models i \varphi$ for every $\xi'_i \in \Xi_i$ with $\xi_i \subsetneq \xi'_i \subsetneq \xi''_i$;
- $\mu, \xi_i \models i \varphi \cup \psi$ if there exists $\xi''_i \in \Xi_i$ with $\xi''_i \subsetneq \xi_i$ such that $\mu, \xi''_i \models i \psi$, and $\mu, \xi'_i \models i \varphi$ for every $\xi'_i \in \Xi_i$ with $\xi''_i \subsetneq \xi'_i \subsetneq \xi_i$; and
- $\mu, \xi_i \models @_j[\varphi]$ if $\xi_i \neq \emptyset$, last$(\xi_i) \in Ev_j$ and $\mu, (\text{last}(\xi_i) \downarrow)_j \models j \varphi$.

As usual $\mu \models \gamma$ if $\mu, \xi \models \gamma$ for every global configuration $\xi$. 


A simple network model

*Princ* set of principals

\[ Name = \{ Name_A \}_{A \in Princ} \]

pairwise disjoint sets of names

\[ Id = Princ \uplus \{ Ch \} \]

*Msg* build by composition and encryption, from *Name*, *Nonce* and *Key*

For \( A \in Princ \)

\[ Act_A : \text{send}(M, B'), \text{rec}(M), \text{spy}(M), \text{and nonce}(N) \]

\[ Prop_A : \text{knows}(M) \]

For the channel

\[ Act_{Ch} : \text{in}(M, A'), \text{out}(M, A'), \text{and leak} \]

\[ Prop_{Ch} : \text{none} \]
Network axioms

Knowledge axioms for principals

(K1) $A \text{@}[knows(M_1; M_2) \iff (knows(M_1) \land knows(M_2))];$

(K2) $A \text{@}[(knows(M) \land knows(K)) \Rightarrow knows\{M\}_K];$

(K3) $A \text{@}[(knows\{M\}_K) \land knows(K^{-1})) \Rightarrow knows(M)];$

(K4) $A \text{@}[knows(M) \Rightarrow G_o knows(M)];$

(K5) $A \text{@}[rec(M) \Rightarrow knows(M)];$

(K6) $A \text{@}[spy(M) \Rightarrow knows(M)];$ and

(K7) $A \text{@}[nonce(N) \Rightarrow knows(N)].$

Fresh nonce generation

(N1) $A \text{@}[nonce(N) \Rightarrow Y \neg knows(M_N)];$ and

(N2) $A \text{@}[nonce(N)] \Rightarrow \wedge_{B \in Princ \setminus A} B \text{@} \neg knows(M_N)].$
Network axioms

Behaviour and communication axioms for the channel

\((C1)\) \(\@_{Ch}[in(M, A') \Rightarrow \bigvee_{B \in \text{Princ}} \@_B[send(M, A')]\])

\((C2)\) \(\@_{Ch}[out(M, A') \Rightarrow P\ in(M, A')]\); and

\((C3)\) \(\@_{Ch}[out(M, A') \Rightarrow \@_A[rec(M)]]\).

Behaviour and communication axioms for principals

\((P1)\) \(\@_A[send(M, B') \Rightarrow Y(knows(M) \land knows(B'))]\);

\((P2)\) \(\@_A[send(M, B') \Rightarrow \@_{Ch}[in(M, B')]]\);

\((P3)\) \(\@_A[rec(M) \Rightarrow \@_{Ch}\left[\bigvee_{A' \in \text{Name}_A} out(M, A')\right]]\);

\((P4)\) \(\@_A[spy(M) \Rightarrow \@_{Ch}[leak \land P\ \bigvee_{B' \in \text{Name}} in(M, B')]]\);

\((P5)\) \(\@_A[\bigwedge_{B \in \text{Princ}\ \{A\}} \neg \@_B[\top]]\); and

\((P6)\) \(\@_A[nonce(N) \Rightarrow \neg \@_{Ch}[\top]]\).
Protocol modeling

Protocols described as a series of steps of the form

\[(\text{step}_q) \ x_s \rightarrow x_r : (n_{q_1}, \ldots, n_{q_t}). M\]

- **Hon**: honest principals follow the rules of the protocol and use only one name
- **Intr**: dishonest principals are potential "intruders"

Given a protocol with \(j\) distinct roles, and an instantiation with names \(A'_{1}, \ldots, A'_{j}\) of principals \(A_{1}, \ldots, A_{j}\)

\[
\text{step}_q^i = \begin{cases} 
\langle \text{nonce}(N_{q_1}) \ldots \text{nonce}(N_{q_t}). \text{send}(M, A'_r) \rangle & \text{if } i = s \\
\langle \text{rec}(M) \rangle & \text{if } i = r \\
\langle \rangle & \text{otherwise}
\end{cases}
\]

Each run\(i_A = \langle \text{act}_1 \ldots \text{act}_n \rangle\) is characterized by

\[
\text{role}^i_A = \text{act}_n \land P(\text{act}_{n-1} \land \cdots \land P(\text{act}_1) \ldots).
\]
Security goals

\[ \text{secrecy goal for } S \text{ among honest participants } A_1, \ldots, A_j \]

\[ \bigwedge_{i=1}^{j} \mathcal{A}_i[P \circ \text{role}_A^i] \Rightarrow \bigwedge_{B \in \text{Princ} \setminus \{A_1, \ldots, A_j\}} \bigwedge_{M \in S} \mathcal{A}_B[\neg \text{knows}(M)] \]

\[ \text{authentication goal for honest } A \text{ in role } i \text{ wrt some } B \text{ in role } j \]

\[ \mathcal{A}_A[\text{role}_A^i] \Rightarrow \mathcal{A}_B[P \circ \text{send}(M, A)], \text{ if } B \text{ is honest} \]
\[ \mathcal{A}_A[\text{role}_A^i] \Rightarrow \bigvee_{C \in \text{Intr}} \mathcal{A}_C[P \circ \text{send}(M, A)], \text{ if } B \text{ is dishonest} \]

assuming that step \( q \) requires \( x_j \) to send message \( M \) to \( x_i \)
**Metareasoning: secret data lemma**

Given $S \subseteq Msg$, $Msg_S$ are the $S$-secure messages, that is, messages where items from $S$ can only appear under the scope of an encryption with a key whose inverse is also in $S$.

**Protocol independent secret data lemma**

$G \subseteq Princ$, $\mu$ network model such that

\[
\mu \models \bigwedge_{A \in G} \Diamond_A [\neg send(M, C')] \text{ for every } M \notin Msg_S \text{ and every name } C', \text{ and} \]

\[
\mu \models \bigvee_{A \in G} \Diamond_A [\ast \Rightarrow F \text{ nonce}(N)] \text{ for every nonce } N \in S.
\]

If it is the case that

- $\mu, \xi \models \bigwedge_{B \in Princ \setminus G} \Diamond_B [\neg \text{ knows}(M)]$ for every $M \notin Msg_S$,

then also

- $\mu, \xi \models \bigwedge_{B \in Princ \setminus G} \Diamond_B [G \circ \neg \text{ knows}(M)]$ for every $M \notin Msg_S$. 

Metareasoning: secrecy lemma

\[ \text{secre}_F = \bigwedge_{i=1}^{j} \forall A_i \left[ P \circ \text{role}_i \right] \Rightarrow \bigwedge_{B \in \text{Princ} \setminus \{A_1, \ldots, A_j\}} \bigwedge_{M \in F} \forall B \left[ \neg \text{knows}(M) \right]. \]

Secrecy lemma

A protocol guarantees \( \text{secre}_F \) for a protocol instantiation with honest participants \( A_1, \ldots, A_j \), provided that all the messages ever sent by \( A_1, \ldots, A_j \) in any protocol run are \( (\{K_{A_1}^{-1}, \ldots, K_{A_j}^{-1}\} \cup F) \)-secure.
Metareasoning: secrecy lemma

$$\text{secre}_F = \bigwedge_{i=1}^{j} \@_{A_i} [\mathcal{P} \circ \text{role}_{A_i}] \Rightarrow \bigwedge_{B \in \text{Princ}\setminus\{A_1,...,A_j\}} \bigwedge_{M \in F} \@_{B} [\neg \text{knows}(M)].$$

Secrecy lemma

A protocol guarantees $\text{secre}_F$ for a protocol instantiation with honest participants $A_1,...,A_j$, provided that all the messages ever sent by $A_1,...,A_j$ in any protocol run are $(\{K^{-1}_{A_1},...,K^{-1}_{A_j}\} \cup F)$-secure.

J.Millen, H.Ruess - Protocol independent secrecy, 2000

Discreetness

Avoiding artificial notions like spells
Metareasoning: one intruder is enough

\[ \begin{array}{c}
\text{send} & \text{spy} & \text{nonce} & \text{rec} & \text{spy} \\
\text{in} & \text{leak} & \text{out} & \text{leak} & \xi \\
\end{array} \]

can be reduced to

\[ \begin{array}{c}
\text{send} & \text{spy} & \text{nonce} & \text{rec} & \text{spy} \\
\text{in} & \text{leak} & \text{out} & \text{leak} & \xi \\
\end{array} \]
Metareasoning: one intruder is enough

\[
\begin{array}{ccccccc}
Z_1 & \cdots & \text{send} & \cdots & \text{spy}_1 & \cdots & \text{nonce}_1 & \cdots \\
Z_2 & \cdots & \text{nonce}_2 & \cdots & \text{rec} & \cdots & \text{spy}_2 & \cdots \\
\text{Ch} & \cdots & \text{in} & \cdots & \text{leak}_1 & \cdots & \text{out} & \cdots & \text{leak}_2 & \cdots & \xi
\end{array}
\]

can be reduced to

\[
\begin{array}{ccccccc}
Z & \cdots & \text{send} & \text{spy}_1 & \text{nonce}_1 & \text{nonce}_2 & \text{rec} & \text{spy}_2 & \cdots \\
\text{Ch} & \cdots & \text{in} & \text{leak}_1 & \cdots & \text{out} & \cdots & \text{leak}_2 & \cdots & \xi
\end{array}
\]

\[
\mu, \xi \models @_A[\varphi] \iff \mu', \xi \models @_A[\varphi] \text{ for } A \in \text{Hon}, \varphi \in \mathcal{L}_A \text{ without } @
\]

\[
\mu, \xi \models \bigvee_{A \in \text{Intr}} @_A[P \circ \text{act}] \iff \mu', \xi \models @_Z[P \circ \text{act}]
\]

if \( \mu, \xi \models \bigvee_{A \in \text{Intr}} @_A[\text{knows}(M)] \) then \( \mu', \xi \models @_Z[\text{knows}(M)] \)
Metareasoning: one intruder is enough

H. Comon-Lundh, V.Cortier - Security properties: two agents are sufficient, 2003
Intruders part of the model
Metareasoning: the predatory intruder

- $Z$ spies every message sent by an honest principal immediately after it arrives to the channel, and that is all the spying he does

\[ \forall_{Ch} [\forall_Z [spy(M)] \iff Y \bigvee_{A \in Hon} \forall_A [\bigvee_{B' \in Name} send(M, B')]] \]

- $Z$ never bothers receiving messages (he has already spied them)

\[ \forall_Z [\neg rec(M)] \]

- $Z$ only sends messages to honest principals, and just immediately before the honest principal gets them

\[ \forall_Z [\neg send(M, Z')] \text{ and } \forall_Z [send(M, A) \implies \forall_{Ch} [X \forall_A [rec(M)]]] \]
Metareasoning: the predatory intruder

\[ Z \quad \ldots \quad \nonceN \quad \sendN \quad \sendM \quad \spyM \quad \recM \quad \spyA \quad \recZ \quad \spyA \quad \ldots \]

\[ Ch \quad \ldots \quad \inA \quad \inN \quad \inM \quad \text{leak} \quad \inZ \quad \outM \quad \outA \quad \text{leak} \quad \outZ \quad \text{leak} \quad \outN \quad \ldots \]

\[ \xi \]

Can be reduced to

\[ Z \quad \ldots \quad \spyA \quad \spyZ \quad \nonceN \quad \sendN \quad \ldots \]

\[ Ch \quad \ldots \quad \inA \quad \text{leak} \quad \inZ \quad \text{leak} \quad \outA \quad \inN \quad \outN \quad \ldots \]

\[ \xi' \]
Metareasoning: the predatory intruder

Can be reduced to

Towards justifying the linearization of distributed communication in trace models

Corollary: the intruder only needs to send messages according to the protocol
Conclusion and further work

- Distributed temporal logic as a tool for security protocol model analysis
- A few of its potentialities

**Further work**

- Other widely used reductions: bounds on the number of honest principals, step compression
- Nicer conditions for secrecy, and its relationship to authentication
- New meaningful partial order reductions
- Protocol compositionality

Thank you!
Conclusion and further work

• Distributed temporal logic as a tool for security protocol model analysis
• A few of its potentialities
• Further work
  – Other widely used reductions: bounds on the number of honest principals, step compression
  – Nicer conditions for secrecy, and its relationship to authentication
  – New meaningful partial order reductions
  – Protocol compositionality

Thank you!