Secure multiparty sessions with topics

Ugo de'Liguoro

University of Turin

BETTY - London, April 2015

Based on STSM with Dezani to Sophia Antipolis (host Castellani), March 2015.

Non Interference (NI)

> *One group of users, using a certain set of commands, is* non interfering *with another group of users if what the first group does with those commands has no effect on what the second group of users can see.*

(Goguen, Meseguer)

NI and process calculi

(Focardi, Gorrieri, Rossi) Let $\mathcal{L}$ be a complete lattice of levels e.g. $\mathcal{L} = \{\bot < \top\}$, and $\ell : Act \to \mathcal{L}$ then for $\sigma \in Act^*$ and $\ell \in \mathcal{L}$ define

$$\sigma \downarrow \ell = \text{the substring of } \sigma \text{ with symbols of level} \leq \ell$$

A system S is Strongly Non-deterministic NI (SNNI) if

$$\forall \sigma \in \text{trace}(S)\ \exists \tau \in \text{trace}(S).\ \tau = \sigma \downarrow \ell.$$

Intuition: actions of level $\not\leq \ell$ have no observable effects at levels $\leq \ell$

SNNI is implied by monotonicity of levels of actions in a trace.

The multiparty scenario

Communication actions:

$$Act \ni \alpha ::= p \xrightarrow{\mathrm{v}^{\ell}} q, \qquad p \neq q$$

Bridge:

$$\mathsf{Bridges} \ni \theta ::= p_0 \xrightarrow{\mathrm{v}_1^{\ell_1}} p_1; p_1 \xrightarrow{\mathrm{v}_2^{\ell_2}} p_2; \cdots$$

Example:

$$p \longrightarrow q; q \longrightarrow r; q \longrightarrow s$$

The multiparty scenario

Communication actions:

$$Act \ni \alpha ::= p \xrightarrow{\mathrm{v}^{\ell}} q, \qquad p \neq q$$

Bridge:

$$\mathsf{Bridges} \ni \theta ::= p_0 \xrightarrow{\mathrm{v}_1^{\ell_1}} p_1; p_1 \xrightarrow{\mathrm{v}_2^{\ell_2}} p_2; \cdots$$

Example:

$$p \longrightarrow q; q \longrightarrow r; q \longrightarrow s$$

The multiparty scenario

Communication actions:

$$Act \ni \alpha ::= p \xrightarrow{\mathrm{v}^{\ell}} q, \qquad p \neq q$$

Bridge:

$$\mathsf{Bridges} \ni \theta ::= p_0 \xrightarrow{\mathrm{v}_1^{\ell_1}} p_1; p_1 \xrightarrow{\mathrm{v}_2^{\ell_2}} p_2; \cdots$$

Example:

$$p \longrightarrow q; q \longrightarrow r; q \longrightarrow s$$

Secure systems

If $\xi = \alpha_1; \alpha_2; \cdots$ is any (finite or infinite) sequence of communication actions then:

$$\mathsf{Brd}(\xi) = \{\theta \in \mathsf{Bridges} \mid \theta \sqsubseteq \xi \ \ \& \ \ \neg\exists\, \theta' \text{non empty}.\ \theta'\theta \sqsubseteq \xi\}$$

Given an algebra of systems S together with an LTS over Act, we set

$$\mathsf{Brd}(S) = \{\mathsf{Brd}(\xi) \mid \xi \text{ is a trace of } S\}$$

Definition (SNNI on Bridges)

S is ℓ-*secure* if

$$\forall \theta \in \mathsf{Brd}(S)\ \exists\, \theta' \in \mathsf{Brd}(S).\ \theta' = \theta \Downarrow \ell$$

where $\theta \Downarrow \ell$ is the subsequence of all actions $p \xrightarrow{\mathrm{v}^{\ell_0}} q$ in θ such that $\ell_0 \leq \ell$. S is *secure* if it is ℓ-secure for all level $\ell \in \mathcal{L}$.

Examples 1

Let $\mathcal{L} = \{\bot < \top\}$.

$$\text{trace}(S_1) = \{p \xrightarrow{\text{u}^{\bot}} q; q \xrightarrow{\text{v}^{\top}} r\}^{\text{pref}}$$

S_1 is $\bot$-secure since

$$(p \xrightarrow{\text{u}^{\bot}} q; q \xrightarrow{\text{v}^{\top}} r) \Downarrow \bot = p \xrightarrow{\text{u}^{\bot}} q \in \text{Brd}(S_1) \quad \checkmark$$

$$\text{trace}(S_2) = \{p \xrightarrow{\text{u}^{\top}} q; q \xrightarrow{\text{v}^{\bot}} r\}^{\text{pref}}$$

S_2 is not $\bot$-secure because

$$(p \xrightarrow{\text{u}^{\top}} q; q \xrightarrow{\text{v}^{\bot}} r) \Downarrow \bot = q \xrightarrow{\text{v}^{\bot}} r \notin \text{Brd}(S_2) \quad \times$$

Examples 2

$$\mathrm{trace}(S_3) = \{p \xrightarrow{\mathrm{u}^{\perp}} q, \quad p \xrightarrow{\mathrm{v}^{\top}} q\}^{\mathrm{pref}}$$

S_3 is $\perp$-secure because

$$(p \xrightarrow{\mathrm{v}^{\top}} q) \Downarrow \perp = \varepsilon \in \mathrm{Brd}(S_3) \quad \checkmark$$

$$\mathrm{trace}(S_4) = \{p \xrightarrow{\mathrm{u}^{\top}} q; q \xrightarrow{\mathrm{v}^{\perp}} r, \quad q \xrightarrow{\mathrm{v}^{\perp}} r\}^{\mathrm{pref}}$$

S_4 is $\perp$-secure because

$$(p \xrightarrow{\mathrm{u}^{\top}} q; q \xrightarrow{\mathrm{v}^{\perp}} r) \Downarrow \perp = q \xrightarrow{\mathrm{v}^{\perp}} r \in \mathrm{Brd}(S_4) \quad \checkmark$$

Examples 3

$$\mathrm{trace}(S_5) = \{p \xrightarrow{\mathrm{u}^{\top}} q; q \xrightarrow{\mathrm{v}^{\bot}} p\}^{\mathsf{pref}}$$

S_5 is not $\bot$-secure because:

$$(p \xrightarrow{\mathrm{u}^{\top}} q; q \xrightarrow{\mathrm{v}^{\bot}} p) \Downarrow \bot = q \xrightarrow{\mathrm{v}^{\bot}} p \notin \mathrm{Brd}(S_5) \quad \text{✗}$$

But simply the the “dangerous” information comes back to its source!

Adding topics

We add to the model a set of *topics* $\mathsf{T} = \{\varphi, \psi, \ldots\}$ and a map

$$\mathit{Owner}() : \mathsf{T} \to \wp(\mathsf{P})$$

Participant p sends to participant q a value v of level ℓ on topic φ:

$$p \xrightarrow[\varphi]{\mathrm{v}^{\ell}} q$$

Topic ownership laws

Idea: the SNNI on bridges is too restrictive; adding topics we require the monotonicity condition only when the receiver is unauthorized to observe the effects of a higher action w.r.t. a topic of which its is not owner,

- Owners only may reveal secrets:

$$p \xrightarrow[\varphi]{\mathrm{u}^{\top}} q; q \xrightarrow[\psi]{\mathrm{v}^{\bot}} r, \quad p \notin \mathit{Owner}(\varphi) \vee q \notin \mathit{Owner}(\psi)$$

- Owners have clearance on their own topics:

$$p \xrightarrow[\varphi]{\mathrm{u}^{\top}} q; q \xrightarrow[\psi]{\mathrm{v}^{\bot}} r, \quad r \in \mathit{Owner}(\varphi) \cap \mathit{Owner}(\psi)$$

Examples 4

If $p \in \mathit{Owner}(\varphi)$, $q \in \mathit{Owner}(\psi)$ but $r \notin \mathit{Owner}(\varphi) \cap \mathit{Owner}(\psi)$ then

$$p \xrightarrow[\varphi]{\mathrm{u}^{\top}} q; q \xrightarrow[\psi]{\mathrm{v}^{\bot}} r \quad \text{✗}$$

Always:

$$p \xrightarrow[\varphi]{\mathrm{u}^{\top}} q; q \xrightarrow[\varphi]{\mathrm{v}^{\bot}} p \quad \text{✓}$$

But if $p \in \mathit{Owner}(\varphi), q \in \mathit{Owner}(\psi)$ and $p \notin \mathit{Owner}(\psi)$ then

$$p \xrightarrow[\varphi]{\mathrm{u}^{\top}} q; q \xrightarrow[\psi]{\mathrm{v}^{\bot}} p \quad \text{✗}$$

(p might leak information about ψ)

Secure systems w.r.t. topics

S is *secure w.r.t. topics* if there are not two bridges of the shape:

$$\cdots\ p \xrightarrow[\varphi]{\mathrm{u}_1^{\top}} q \cdots q \xrightarrow[\psi]{\mathrm{v}_1^{\bot}} r\ \cdots$$
$$\cdots\ p \xrightarrow[\varphi]{\mathrm{u}_2^{\top}} q \cdots q \xrightarrow[\psi]{\mathrm{v}_2^{\bot}} r\ \cdots$$

s.t. $p \in \mathit{Owner}(\varphi), q \in \mathit{Owner}(\psi)$ and $r \notin \mathit{Owner}(\varphi) \cap \mathit{Owner}(\psi)$.

S is *safe w.r.t. topics* if, under the same conditions, there is no single bridge of the shape above.

Problems

- What kind of model do topics induce?
- Which are the proper notions of safe and secure system?
- What should be the axioms about transitions with topics?
- Can we encode different policies by changing axioms?
- In a typed setting, what kind of nondeterminism is allowed?
- At which level, global/local, should we attempt to approximate safety by typing?

Thank you!