Secure multiparty sessions with topics

Ilaria Castellani, Mariangiola Dezani-Ciancaglini,
Ugo de'Liguoro

INRIA Sophia Antipolis, University of Turin

PLACES - Eindhoven, April 2016

Motivation and goal

Motivation and goal

- control flow based security analysis relies on security levels and level drop detection to discover information leaks

Motivation and goal

- control flow based security analysis relies on security levels and level drop detection to discover information leaks
- in case of multiparty communication this leads to unreasonable restrictions

Motivation and goal

- control flow based security analysis relies on security levels and level drop detection to discover information leaks
- in case of multiparty communication this leads to unreasonable restrictions
- previous work where multiparty sessions have been endowed with security levels and type systems enforcing leak-free communication, suffers from similar restrictions

Motivation and goal

- control flow based security analysis relies on security levels and level drop detection to discover information leaks
- in case of multiparty communication this leads to unreasonable restrictions
- previous work where multiparty sessions have been endowed with security levels and type systems enforcing leak-free communication, suffers from similar restrictions
- here we add a further dimension, called topics, to relax these restrictions, and show that this can be ensured via a type system

Secure information flow

Secure information flow

Let $(\mathcal{L}, \sqsubseteq)$ be the lattice of security *levels*:

$$\ell \sqsubseteq \ell' \Leftrightarrow \ell \text{ is less confidential than } \ell'$$

$\bot =$ public, $\top =$ secret.

Secure information flow

Let $(\mathcal{L}, \sqsubseteq)$ be the lattice of security *levels*:

$$\ell \sqsubseteq \ell' \Leftrightarrow \ell \text{ is less confidential than } \ell'$$

$\bot =$ public, $\top =$ secret.

A *leak* is an information flow

$$\cdots \mathsf{v}^{\ell} \cdots \mathsf{u}^{\ell'} \cdots \quad \text{where} \quad \ell \not\sqsubseteq \ell' \quad \text{and}$$

v^{ℓ} is sent from a participant p to a participant q and q is either the sender or the receiver of $\mathsf{u}^{\ell'}$

Motivating example

Alice as PC member:

Motivating example

Alice as PC member:

- receives the opinion of Bob on paper 1

Motivating example

Alice as PC member:

- receives the opinion of Bob on paper 1
- sends her judgment on paper 2 to Charlie

Motivating example

Alice as PC member:

- receives the opinion of Bob on paper 1
- sends her judgment on paper 2 to Charlie

the level of Bob opinion is not smaller than the level of Alice judgment

Motivating example

Alice as PC member:

- receives the opinion of Bob on paper 1
- sends her judgment on paper 2 to Charlie

the level of Bob opinion is not smaller than the level of Alice judgment

standard information flow security

Motivating example

Alice as PC member:

- receives the opinion of Bob on paper 1
- sends her judgment on paper 2 to Charlie

the level of Bob opinion is not smaller than the level of Alice judgment

standard information flow security ✗

Motivating example

Alice as PC member:

- receives the opinion of Bob on paper 1
- sends her judgment on paper 2 to Charlie

the level of Bob opinion is not smaller than the level of Alice judgment

standard information flow security ✗

information flow security with topics

Motivating example

Alice as PC member:

- receives the opinion of Bob on paper 1
- sends her judgment on paper 2 to Charlie

the level of Bob opinion is not smaller than the level of Alice judgment

standard information flow security ✗

information flow security with topics ✓

Safety with topics

A leak is an information flow

$$\cdots \mathsf{v}^{\ell} \cdots \mathsf{u}^{\ell'} \cdots \quad \text{where} \quad \ell \not\sqsubseteq \ell'$$

Adding *topics* a leak is

$$\cdots \mathsf{v}^{\ell,\varphi} \cdots \mathsf{u}^{\ell',\psi} \cdots \quad \text{where} \quad \ell \not\sqsubseteq \ell' \quad \text{and} \quad \varphi, \psi \text{ are correlated}$$

Access control and leak freedom w.r.t. topics

Access control and leak freedom w.r.t. topics

Access control (AC): for each participant $\mathtt{p}$ and topic φ:

participant $\mathtt{p}$ is able to receive $\mathtt{v}^{\ell,\varphi}$ if $\ell \sqsubseteq \rho(\mathtt{p}, \varphi)$ (reading level)

Access control and leak freedom w.r.t. topics

Access control (AC): for each participant $\mathtt{p}$ and topic φ:

participant $\mathtt{p}$ is able to receive $\mathsf{v}^{\ell,\varphi}$ if $\ell \sqsubseteq \rho(\mathtt{p}, \varphi)$ (reading level)

Leak freedom (LF): a session is *leak free* if for each participant $\mathtt{p}$ whenever $\mathtt{p}$ receives $\mathsf{v}^{\ell,\varphi}$, she just sends values $\mathsf{u}^{\ell',\psi}$ s.t.

$$\ell \sqsubseteq \ell' \quad \text{or} \quad \varphi \curlyvee \psi$$

where $\varphi \curlyvee \psi$ if φ and ψ are *independent* topics.

A multiparty session calculus

Expressions:

$$e ::= x \mid \mathrm{v}^{\ell,\varphi} \mid \mathrm{op}(e_1, \ldots, e_n)$$

Processes:

$$P ::= \mathrm{q}!\lambda(e).P \mid \mathrm{p}?\lambda(x).Q \mid P \oplus P \mid P + P \mid \mu X.P \mid X \mid \mathbf{0}$$

Multiparty sessions:

$$\mathcal{M} ::= \mathrm{p}_1 \triangleleft P_1 \mid \ldots \mid \mathrm{p}_n \triangleleft P_n$$

Operational semantics:

$$\frac{P \xrightarrow{\mathrm{q}!\lambda(\mathrm{v}^{\ell,\varphi})} P' \quad Q \xrightarrow{\mathrm{p}?\lambda(\mathrm{v}^{\ell,\varphi})} Q'}{\mathrm{p} \triangleleft P \mid \mathrm{q} \triangleleft Q \xrightarrow{\mathrm{p}(\lambda,\mathrm{v}^{\ell,\varphi})\mathrm{q}} \mathrm{p} \triangleleft P' \mid \mathrm{q} \triangleleft Q'}$$

Safe sessions

Definition

A multiparty session $\mathcal{M}$ is *safe* if it satisfies:

- *Access control (AC):*
  whenever $\sigma \cdot \mathtt{p}(\lambda, \mathtt{v}^{\ell,\varphi})\mathtt{q}$ is a trace of $\mathcal{M}$, then $\ell \sqsubseteq \rho(\mathtt{q}, \varphi)$;
- *Leak freedom (LF):*
  whenever $\sigma \cdot \mathtt{p}(\lambda, \mathtt{v}^{\ell,\varphi})\mathtt{q} \cdot \sigma' \cdot \mathtt{q}(\lambda', \mathtt{u}^{\ell',\psi})\mathtt{r}$ is a relay trace of $\mathcal{M}$, then either $\ell \sqsubseteq \ell'$ or $\varphi \curlyvee \psi$.

where $\sigma \cdot \mathtt{p}(\lambda, \mathtt{v}^{\ell,\varphi})\mathtt{q} \cdot \sigma' \cdot \mathtt{q}(\lambda', \mathtt{u}^{\ell',\psi})\mathtt{r}$ is a *relay trace* from $\mathtt{p}$ to $\mathtt{r}$ mediated by $\mathtt{q}$.

Examples

A trace of a safe session (that was not such in past systems)

Examples

A trace of a safe session (that was not such in past systems)

Bob (evaluation,"reject"$^{\ell_1,\ \text{paper } 1}$) Alice

Examples

A trace of a safe session (that was not such in past systems)

$$\text{Bob} \xrightarrow{(\text{evaluation}, \text{"reject"}, \ell_1, \text{paper } 1)} \text{Alice}$$

$$\text{Alice} \xrightarrow{(\text{evaluation}, \text{"accept"}, \ell_2, \text{paper } 2)} \text{Charlie}$$

Examples

A trace of a safe session (that was not such in past systems)

$$\text{Bob} \ (\text{evaluation}, \text{"reject"}^{\ell_1}, \ \text{paper } 1) \ \text{Alice}$$

$$\text{Alice} \ (\text{evaluation}, \text{"accept"}^{\ell_2}, \ \text{paper } 2) \ \text{Charlie}$$

ℓ_1 is not smaller than ℓ_2

Examples

A trace of a safe session (that was not such in past systems)

$$\text{Bob} \xrightarrow{(\text{evaluation}, \text{"reject"}, \ell_1, \text{paper } 1)} \text{Alice}$$

$$\text{Alice} \xrightarrow{(\text{evaluation}, \text{"accept"}, \ell_2, \text{paper } 2)} \text{Charlie}$$

ℓ_1 is not smaller than ℓ_2

paper 1 and paper 2 are independent

Types

Sorts:

$$S \quad ::= \quad \texttt{nat} \parallel \texttt{int} \parallel \texttt{bool} \parallel \texttt{string}$$

Global types:

$$G ::= \mathtt{p} \to \mathtt{q} : \{\lambda_i(S_i^{\ell_i,\varphi_i}).G_i\}_{i\in I} \parallel \mu\mathbf{t}.G \parallel \mathbf{t} \parallel \texttt{end}$$

Session types:

$$T ::= \bigvee_{i\in I} \mathtt{q}!\lambda_i(S_i^{\ell_i,\varphi_i}).T_i \parallel \bigwedge_{i\in I} \mathtt{p}?\lambda_i(S_i^{\ell_i,\varphi_i}).T_i \parallel \mu\mathbf{t}.T \parallel \mathbf{t} \parallel \texttt{end}$$

Level, topic agreement with a type

$\langle \ell, \varphi \rangle$ agrees with T, $\langle \ell, \varphi \rangle \prec T$, if according to T only values of level $\ell' \sqsupseteq \ell$ are sent on topics related with φ

Level, topic agreement with a type

$\langle \ell, \varphi \rangle$ agrees with T, $\langle \ell, \varphi \rangle \prec T$, if according to T only values of level $\ell' \sqsupseteq \ell$ are sent on topics related with φ

$\langle \ell, \varphi \rangle \prec T$ is co-inductively defined by

- $\langle \ell, \varphi \rangle \prec \mathtt{end}$
- if $\langle \ell, \varphi \rangle \prec T_i$ for all $i \in I$ then

$$\langle \ell, \varphi \rangle \prec \bigwedge_{i \in I} \mathtt{p}?\lambda_i(S_i^{\ell_i, \varphi_i}).T_i$$

- if $\langle \ell, \varphi \rangle \prec T_i$ and either $\ell \sqsubseteq \ell_i'$ or $\varphi \curlyvee \psi_i$ for all $i \in I$ then

$$\langle \ell, \varphi \rangle \prec \bigvee_{i \in I} \mathtt{q}!\lambda_i(S^{\ell_i', \psi_i}).T_i$$

Safe session types

Type T is safe if

1. all input continuations are safe and agreed by the respective participant, topic pairs,
2. all output continuations are safe and outputs are sent to participants with the proper reading level

Safe session types

Type T is safe if

1. all input continuations are safe and agreed by the respective participant, topic pairs,
2. all output continuations are safe and outputs are sent to participants with the proper reading level

Coinductively

- $\mathtt{end}$ is safe
- if $\langle \ell_i, \varphi_i \rangle \prec T_i$ and T_i is safe for all $i \in I$ then

$$\bigwedge_{i \in I} \mathrm{p}?\lambda_i(S_i^{\ell_i, \varphi_i}).\, T_i \quad \text{is safe}$$

- if $\ell_i \sqsubseteq \rho(\mathrm{q}, \varphi_i)$ and T_i is safe for all $i \in I$ then

$$\bigvee_{i \in I} \mathrm{q}!\lambda_i(S_i^{\ell_i, \varphi_i}).\, T_i$$

Session type system

Type rules:

$$\frac{\Gamma \vdash e : S^{\ell,\varphi} \quad \Gamma \vdash P \blacktriangleright T}{\Gamma \vdash \mathrm{q}!\lambda(e).P \blacktriangleright \mathrm{q}!\lambda(S^{\ell,\varphi}).T} \qquad \frac{\Gamma, x : S^{\ell,\varphi} \vdash Q \blacktriangleright T}{\Gamma \vdash \mathrm{p}?\lambda(x).Q \blacktriangleright \mathrm{p}?\lambda(S^{\ell,\varphi}).T}$$

$$\frac{\Gamma \vdash P_1 \blacktriangleright T_1 \quad \Gamma \vdash P_2 \blacktriangleright T_2}{\Gamma \vdash P_1 \oplus P_2 \blacktriangleright T_1 \vee T_2} \qquad \frac{\Gamma \vdash P_1 \blacktriangleright T_1 \quad \Gamma \vdash P_2 \blacktriangleright T_2}{\Gamma \vdash P_1 + P_2 \blacktriangleright T_1 \wedge T_2}$$

$\Gamma \vdash P \blacktriangleright T$ is a safe typing if all types in the derivation are safe.

Session type system

Type rules:

$$\frac{\Gamma \vdash e : S^{\ell,\varphi} \quad \Gamma \vdash P \blacktriangleright T}{\Gamma \vdash \mathtt{q}!\lambda(e).P \blacktriangleright \mathtt{q}!\lambda(S^{\ell,\varphi}).T} \qquad \frac{\Gamma, x : S^{\ell,\varphi} \vdash Q \blacktriangleright T}{\Gamma \vdash \mathtt{p}?\lambda(x).Q \blacktriangleright \mathtt{p}?\lambda(S^{\ell,\varphi}).T}$$

$$\frac{\Gamma \vdash P_1 \blacktriangleright T_1 \quad \Gamma \vdash P_2 \blacktriangleright T_2}{\Gamma \vdash P_1 \oplus P_2 \blacktriangleright T_1 \vee T_2} \qquad \frac{\Gamma \vdash P_1 \blacktriangleright T_1 \quad \Gamma \vdash P_2 \blacktriangleright T_2}{\Gamma \vdash P_1 + P_2 \blacktriangleright T_1 \wedge T_2}$$

$\Gamma \vdash P \blacktriangleright T$ is a safe typing if all types in the derivation are safe.

Example: if $\rho(\mathtt{p}, \varphi) = \top$ and $\varphi \curlyvee \psi$ we can derive

$$\vdash \mathtt{p}?\lambda(x).\mathtt{r}!\lambda'(\mathsf{false}^{\bot,\psi}).\mathbf{0} \blacktriangleright \mathtt{p}?\lambda(\mathtt{bool}^{\top,\varphi}).\mathtt{r}!\lambda'(\mathtt{bool}^{\bot,\psi}).\mathtt{end}$$

Subtyping

Subtyping of safe types, $T \leq T'$, is co-inductively defined by

- $\mathtt{end} \leq \mathtt{end}$
- if $T_i \leq T_i'$ for all $i \in I \supseteq J$ then

$$\bigwedge_{i \in I} \mathtt{p}?\lambda_i(S_i^{\ell_i, \varphi_i}).T_i \leqslant \bigwedge_{j \in J} \mathtt{p}?\lambda_j(S_j^{\ell_j, \varphi_j}).T_j'$$

- if $T_i \leq T_i'$ for all $i \in I \subseteq J$ then

$$\bigvee_{i \in I} \mathtt{p}!\lambda_i(S_i^{\ell_i, \varphi_i}).T_i \leqslant \bigvee_{j \in J} \mathtt{p}!\lambda_j(S_j^{\ell_j, \varphi_j}).T_j'$$

Global type system

Let's take from [Honda-Yoshida-Carbone 2008]:

- $\mathtt{pt}\{G\}$ is the set of participants of G
- $G \upharpoonright \mathtt{p}$ is the projection into the session type for $\mathtt{p}$

$$\frac{\vdash P_i \blacktriangleright T_i \quad T_i \leq G \upharpoonright \mathtt{p}_i \quad \mathtt{pt}\{G\} \subseteq \{\mathtt{p}_1, \ldots, \mathtt{p}_n\} \qquad \forall i \in \{1, \ldots, n\}}{\mathtt{p}_1 \triangleleft P_1 \mid \ldots \mid \mathtt{p}_n \triangleleft P_n \blacktriangleright G}$$

Typing example

$$\text{Alice} \triangleleft \text{Bob?evaluation}(x).\ \text{Charlie!evaluation}(\text{"accept"}^{\ell_1,\text{paper } 2}).\mathbf{0}$$

$$\text{Bob?evaluation}(\text{String}^{\ell_1,\text{paper } 1}).\text{Charlie!evaluation}(\text{String}^{\ell_2,\text{paper } 2}).\texttt{end}$$

Session and global type reduction

Reduction of session types:

$$T \vee T' \Longrightarrow T \quad \mathtt{p}!\lambda(S^{\ell,\varphi}).T \Longrightarrow T \quad \bigwedge_{i\in I} \mathtt{p}?\lambda_i(S_i^{\ell_i,\varphi_i}).T_i \Longrightarrow T_i$$

Reduction of global types:

$$G \Longrightarrow G \setminus \mathtt{p} \xrightarrow{\lambda} \mathtt{q}$$

where $G \setminus \mathtt{p} \xrightarrow{\lambda} \mathtt{q}$ is the global type obtained from G by executing the communication $\mathtt{p} \xrightarrow{\lambda} \mathtt{q}$

Subject reduction

Theorem

If $\mathtt{p} \triangleleft P \mid \mathcal{M} \xrightarrow{\kappa} \mathtt{p} \triangleleft P' \mid \mathcal{M}'$, *and* $\mathtt{p} \triangleleft P \mid \mathcal{M} \blacktriangleright G$ *and* $\vdash P \blacktriangleright T$, *then:*

1. $\mathtt{p} \triangleleft P' \mid \mathcal{M}' \blacktriangleright G'$ *for some* G' *such that* $G \Longrightarrow^* G'$;
2. $\vdash P' \blacktriangleright T'$ *for some* T' *such that* $T \Longrightarrow^* T'$.

Proved by establishing that:

- if $\mathtt{q}!\lambda(S^{\ell,\varphi}).T \leq G \upharpoonright \mathtt{p}$, then $T \leq (G \setminus \mathtt{p} \xrightarrow{\lambda} \mathtt{q}) \upharpoonright \mathtt{p}$;
- if $\mathtt{p}?\lambda(S^{\ell,\varphi}).T \wedge T' \leq G \upharpoonright \mathtt{q}$, then $T \leq (G \setminus \mathtt{p} \xrightarrow{\lambda} \mathtt{q}) \upharpoonright \mathtt{q}$;
- $G \upharpoonright \mathtt{r} = (G \setminus \mathtt{p} \xrightarrow{\lambda} \mathtt{q}) \upharpoonright \mathtt{r}$ for $\mathtt{r} \neq \mathtt{p}$, $\mathtt{r} \neq \mathtt{q}$.

Soundness theorem

Theorem

If $\mathcal{M}$ is typeable by a derivation containing only safe types then $\mathcal{M}$ is safe.

Proof essentially based on subject reduction theorem.

Conclusion and further work

Conclusion and further work

Advantages of the proposed approach:

- A sequence of messages directed to the same participant is always allowed
- Thanks to the introduction of topics, the standard leak-freedom requirement can be relaxed also on relay sequences, by forbidding only downward flows between messages on related topics.

Conclusion and further work

Advantages of the proposed approach:

- A sequence of messages directed to the same participant is always allowed
- Thanks to the introduction of topics, the standard leak-freedom requirement can be relaxed also on relay sequences, by forbidding only downward flows between messages on related topics.

Further directions:

- consider multiple sessions
- enrich the present calculus by allowing levels and topics to depend on exchanged values, following [Lourenço-Caires 2015]