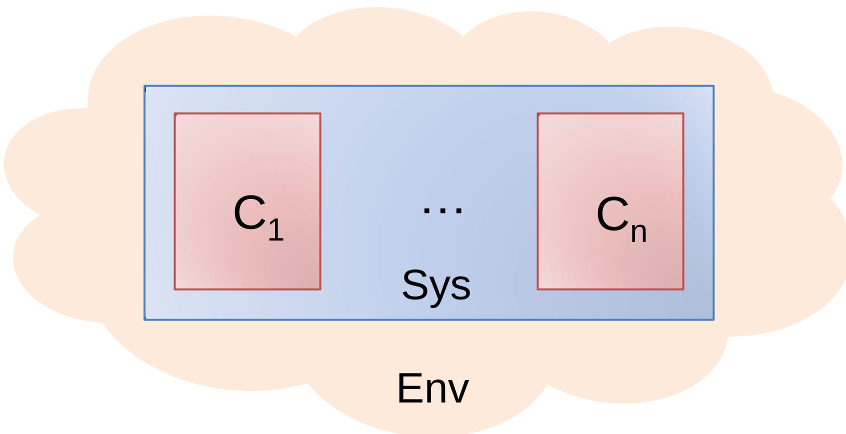
FoMSESS Annual Meeting, September 07, 2017

Taming Message-passing Communication in Compositional Reasoning about Confidentiality

Ximeng Li, Heiko Mantel, Markus Tasch

Modeling and Analysis of Information Systems (MAIS),
TU Darmstadt

Compositional Reasoning about Security



$$\mathrm{LSec}(C_1) \wedge \ \dots \ \wedge \mathrm{LSec}(C_n)$$

$$\Downarrow$$

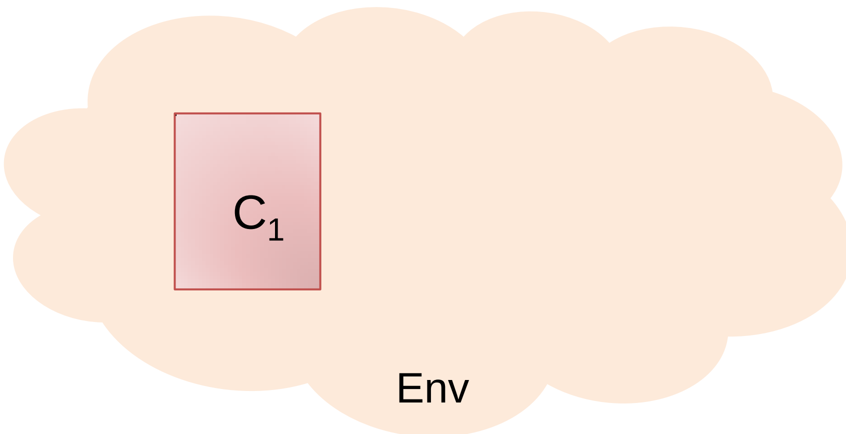
$$\mathrm{GSec}(\mathrm{Sys})$$

In compositional reasoning about information-flow security:

- Global Security of system is inferred from local security of components
- Security at both levels can be expressed by a variant of noninterference

Compositional reasoning reduces the conceptual complexity of verification!

Compositional Reasoning about Security



LSec(C_1, **all-ctx**) ...

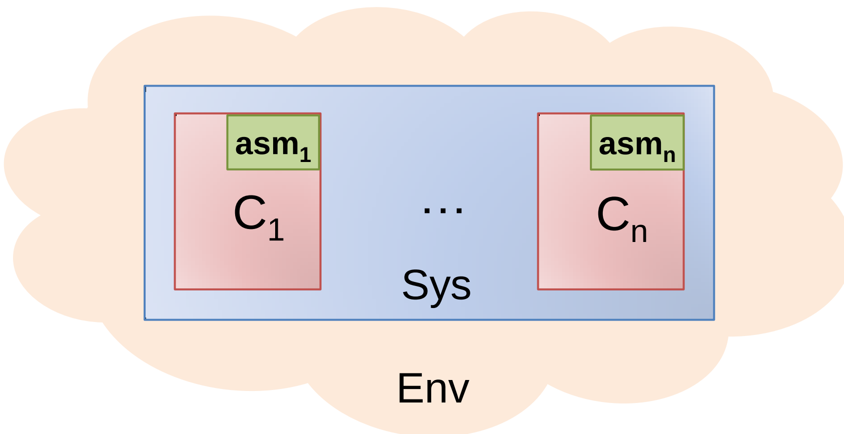
$\Downarrow$

GSec(Sys)

A **problem** with the rudimentary form of compositional reasoning:

- ❑ The context of each component in the system is omitted.
- ❑ Local security needs to be verified for **all (possible & impossible) contexts**.

Rely-Guarantee Reasoning about Security



$\mathrm{LSec}(C_1,\textbf{asm-ctx}_1) \land \ldots \land \mathrm{LSec}(C_n,\textbf{asm-ctx}_n)$

$\mathrm{justified}(\textbf{asm-ctx}_1) \land \ldots \land \mathrm{justified}(\textbf{asm-ctx}_n)$

$\Downarrow$

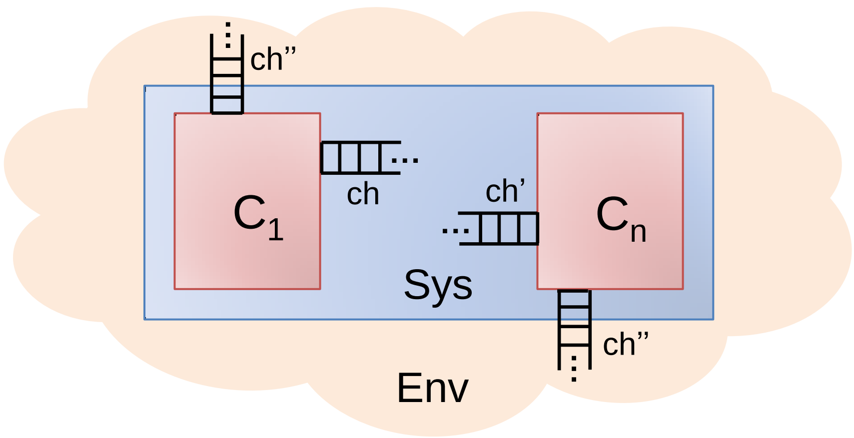
$\mathrm{GSec}(\mathrm{Sys})$

In **rely-guarantee-style reasoning** about information-flow security:

- ❑ Potential contexts of a component in the system are assumed.
- ❑ Local security is verified for **a restricted sub-class of contexts**.

Mantel/Sands/Sudbrock(CSF'11); Askarov/Chong/Mantel(CSF'15); Murray/Sison/Pierzchalski/Rizkallah(CSF'16); …

Message-passing Communication



- Each channel has a message buffer
- send(ch, e)
- recv(ch, x)

Differences of message-passing from memory-sharing:

- The **presence** of messages needs to be protected in addition to their content.
- A receive can **block** if no message is available to be received.
- A receive not only observes, but also **changes**, the state.

Contributions

We propose a rely-guarantee-style solution for security verification in distributed systems using message-passing communication.

Main technical contributions:

- A sound, yet precise solution for compositional reasoning
  - key ingredient: a process-local security condition
- A sound, fine-grained security type system
  - automates the verification of process-local security

Main Focus:

- Achieving **all** of soundness, modularity, precision in the verification of message-passing security

Motivating Examples

Context sends secret

```
recv(enc, x);
send(pub, x)
```

Context provides public message

```
recv(enc, x);
send(pub, x)
```

$^{\{\mathbb{L}^{\bullet}\}}$recv(enc, x);
send(pub, x)

Context only sends a message if secret is positive

```
recv(pri, x);
send(pub,1)
```

Context sends a message irrespective of secrets

```
recv(pri, x);
send(pub,1)
```

$^{\{\mathbb{L}^{o}\}}$recv(pri, x);
send(pub,1)

Context does not send any message

```
if h>0 then
  recv(pri, x)
else
  skip
fi;
send(pub, 1)
```

Context definitely provides a message

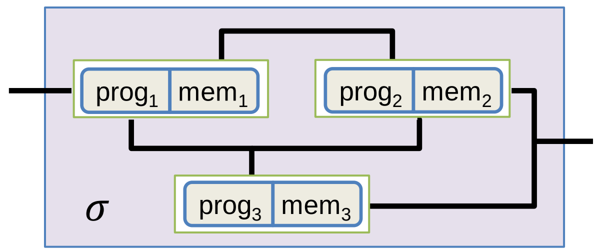
```
if h>0 then
  recv(pri, x)
else
  skip
fi;
send(pub, 1)
```

if h>0 then
$^{\{NE\}}$recv(pri, x)
else
skip
fi;
send(pub, 1)

Computation Model and Baseline Security

Distributed Systems

process

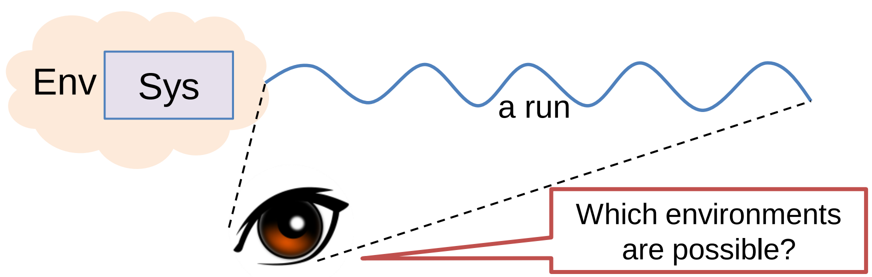


distributed system

$prog_1 \,||\, \ldots \,||\, prog_n$

Distributed program

Global Security



- Sys is secure if all environments with the same publicly observable behavior as Env are deemed possible by the attacker.

Process-local Security (1)

We modularize global security for distributed systems by defining a notion of **local-security**.

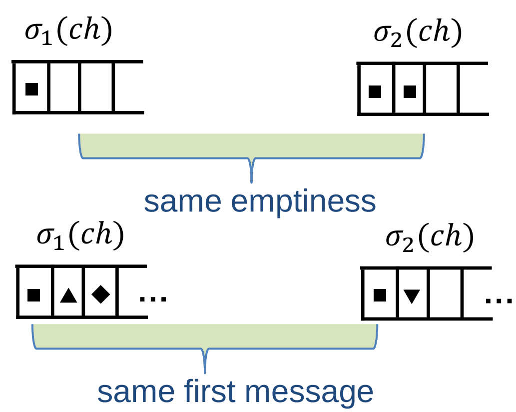
A few similarity relations:

$mem_1 =_{\mathbb{L}} mem_2$	The memories mem_1 and mem_2 are **low-equivalent**.
$\sigma_1 \;=_{att}\; \sigma_2$	The channel states σ_1 and σ_2 are **indistinguishable to the attacker**.
$\sigma_1 \overset{asc}{=\!=} \sigma_2$	The channel states σ_1 and σ_2 are **similar**, **under assumptions**.

Example for $\sigma_1 \overset{asc}{=\!=} \sigma_2$

$$\sigma_1 \overset{\{(\mathbb{L}^{\circ}, ch)\}}{=\!=} \sigma_2$$

$$\sigma_1 \overset{\{(\mathbb{L}^{\bullet}, ch)\}}{=\!=} \sigma_2$$



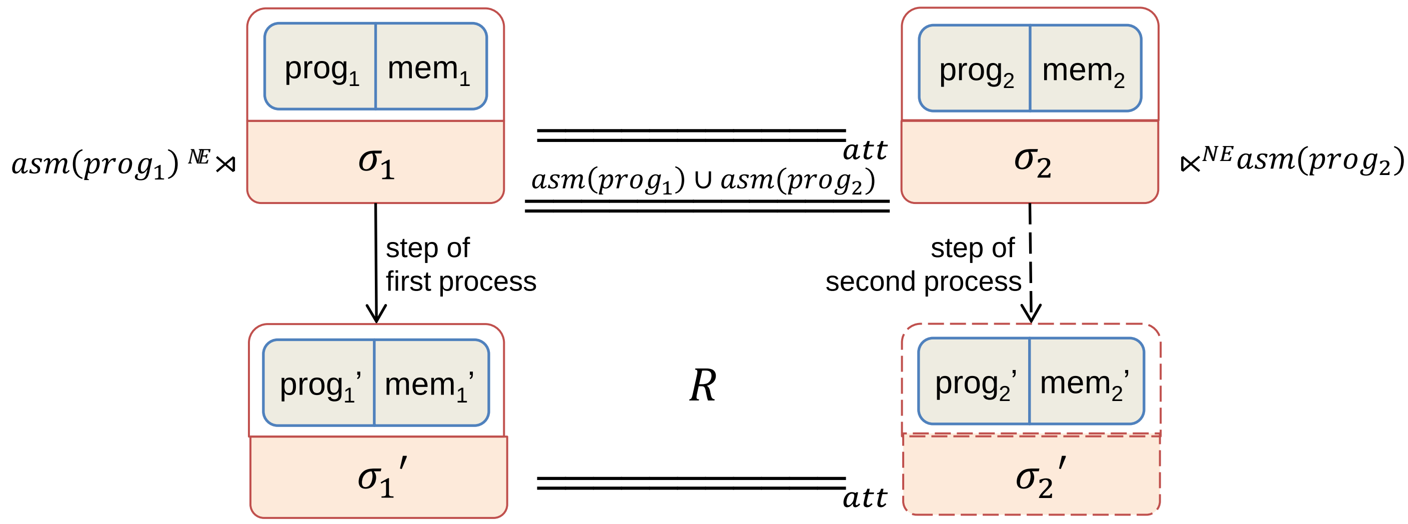
Process-local Security (2)

Definition

A symmetric relation R is an assumption-aware bisimulation if

$\langle prog_1 \mid mem_1 \rangle \; R \; \langle prog_2 \mid mem_2 \rangle$ implies

$$mem_1 =_{\mathbb{L}} mem_2 \wedge (prog_1 = stop \Leftrightarrow prog_2 = stop)$$ and



Process-local Security (3)

Definition (Local Security)

A program *prog* is locally secure, if

$$\forall mem_1, mem_2 \colon mem_1 =_{\mathbb{L}} mem_2 \Rightarrow \boxed{\mathit{prog} \mid mem_1} \approx \boxed{\mathit{prog} \mid mem_2}$$

assumption-aware bisimilarity

Compositional Reasoning about Security

Theorem 1 (Soundness of Compositional Reasoning)**.**
For distributed program $dprog = prog_1 || \ldots || prog_n$, if each $prog_i$ is **locally secure**, and $dprog$ ensures a **sound use of assumptions**, then $dprog$ is **knowledge-based secure**.

defined using an instrumented semantics

modularity

precision

LSec(prog$_1$,**asm-ctx$_1$**) /\ … /\ LSec(prog$_n$,**asm-ctx$_n$**)

justified(**asm-ctx$_1$**) /\ … /\ justified(**asm-ctx$_n$**)

$\Downarrow$

soundness

GSec(prog$_1$||…||prog$_n$)

RS³

CRISP Center for Research in Security and Privacy

MAIS Modeling and Analysis of Information Systems

TECHNISCHE UNIVERSITÄT DARMSTADT

Typing Local Security (1)

Security levels under assumptions:

$lev^{\bullet}(ch, as)$	The confidentiality level of the content of messages over ch, under the assumptions in as ($as \subseteq \{\mathbb{L}^{\bullet}, \mathbb{L}^{\circ}, NE\}$).
$lev^{\circ}(ch, as)$	The confidentiality level of the presence of messages over ch, under the assumptions in as ($as \subseteq \{\mathbb{L}^{\bullet}, \mathbb{L}^{\circ}, NE\}$).

Examples for $lev^{\bullet}(ch, as)$:

- Suppose ch is not one of the channels the attacker directly observes.

$$lev^{\bullet}(ch, \{\mathbb{L}^{\bullet}\}) = \mathbb{L}$$

$$lev^{\bullet}(ch, \{\quad\}) = \mathbb{H}$$

- If ch is one of the channels that the attacker directly observes, then $lev^{\bullet}(ch, as)$ is decided by the security class of the channel.

Typing Local Security (2)

Message presence is leaked through blockage/non-blockage

$$\frac{lev^{\circ}(ch) = \mathbb{L} \quad lev^{\bullet}(ch) \sqsubseteq lev(x)}{lev \vdash recv(ch, x)}$$

Sabelfeld/Mantel, SAS'02

Always non-blockage ⇒ impossible to leak message presence through blockage/non-blockage

$$\frac{\boldsymbol{NE} \notin \boldsymbol{as} \;\Rightarrow\; lev^{\circ}(ch, \boldsymbol{as}) = \mathbb{L} \quad lev^{\circ}(ch, \boldsymbol{as}) \sqcup lev^{\bullet}(ch, \boldsymbol{as}) \sqsubseteq lev(x)}{lev \vdash {}^{\boldsymbol{as}}recv(ch, x)}$$

Use assumptions rather than fixed security classes for the channels not directly observed by attacker

this work

Typing Local Security (3)

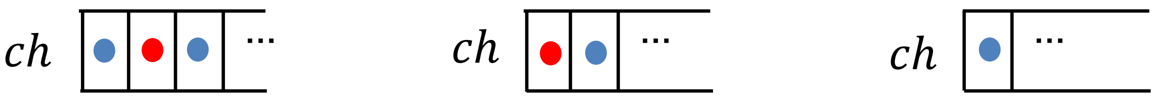
Theorem 2 (Soundness of Security Type System)**.**
If $lev \vdash prog$, then $prog$ is locally secure.

The verification of local security (under assumptions) boils down to **automatic type checking**.

Content-sensitivity, Availability-sensitivity

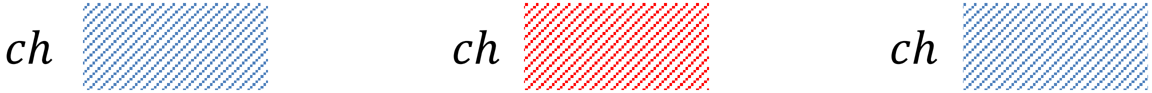
By exploiting assumptions, our security type system supports **content-sensitivity** and **availability-sensitivity**:

- ❑ content-sensitivity: varying confidentiality of message content over one single channel



at 1^{st} recv　at 2^{nd} recv　at 3^{rd} recv

- ❑ availability-sensitivity: varying confidentiality of message presence over one single channel



at 1^{st} recv　at 2^{nd} recv　at 3^{rd} recv

Conclusion

We proposed a solution for reasoning about confidentiality in **message-passing systems** that achieves all of:

- ✓ **soundness**
- ✓ **modularity**
- ✓ **precision**
  - ❑ non-blockage of communication
  - ❑ content-sensitivity
  - ❑ availability-sensitivity

at the **semantic level** as well as the **syntactic level**.

The full paper will appear in **APLAS 2017**
(an online version is already available on our website)

Thank you for your attention!

Any questions?

We thank our sponsors:

DFG

Bundesministerium für Bildung und Forschung

HESSEN
Hessisches Ministerium für Wissenschaft und Kunst

RS³

CRISP
Center for Research in Security and Privacy

MAIS
Modeling and Analysis of Information Systems

TECHNISCHE UNIVERSITÄT DARMSTADT