FoMSESS Annual Meeting 2016, Duisburg 17th – 18th February

I-MAKS

Formalizing Information Flow Properties in Isabelle/HOL

Markus Tasch

Joint work with:
Heiko Mantel, Henning Sudbrock, Sylvia Grewe, Steffen Lortz & Richard Gay

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

MAIS Modellierung und Analyse von Informationssystemen

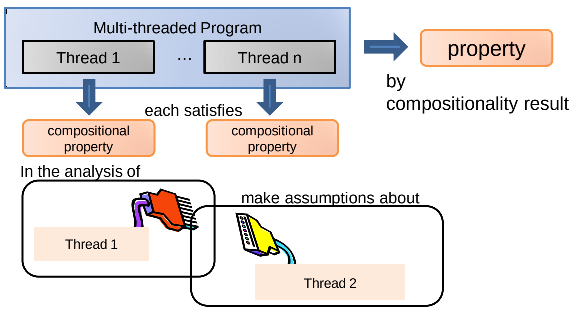
TECHNISCHE UNIVERSITÄT DARMSTADT

Modeling & Analysis of Information Systems

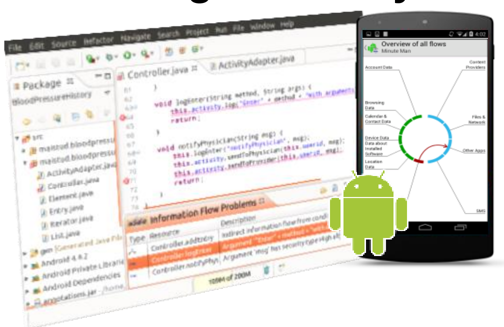
Chair at TU Darmstadt led by **Heiko Mantel**

Selected Research Topics

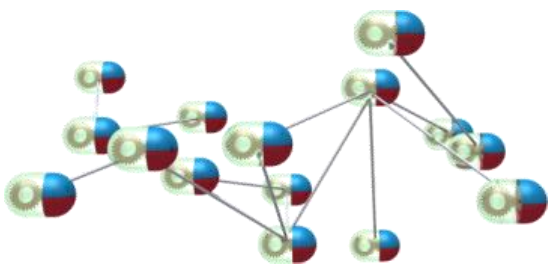
Concurrency & Parallelism



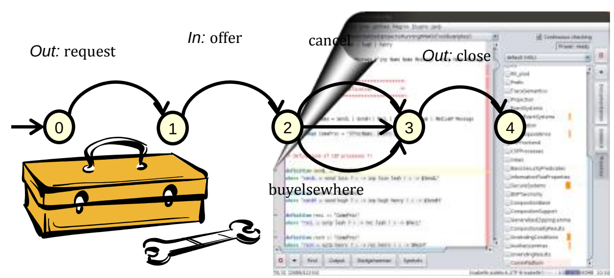
Static Program Analysis



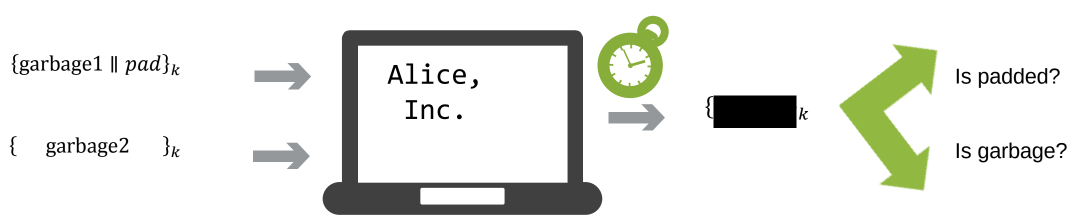
Runtime Monitoring



Security Engineering



Side Channel Analysis & Mitigation



Modeling & Analysis of Information Systems

Chair at TU Darmstadt led by **Heiko Mantel**

Selected Projects

RS³ — **Reliable Secure Software Systems**

CASED — **Center for Advanced Security Research Darmstadt**

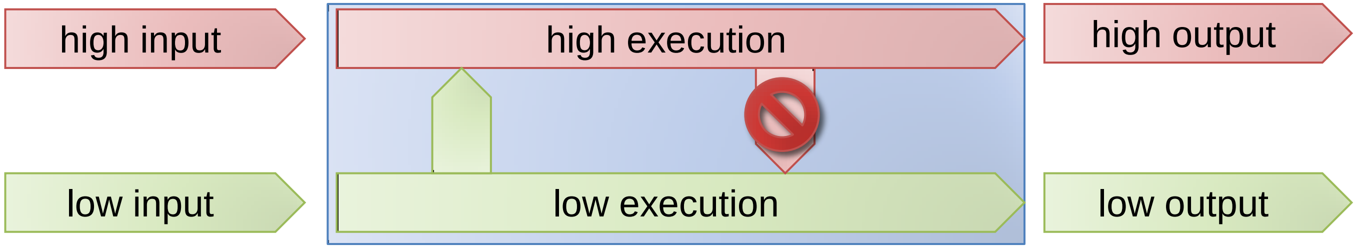
CRISP Center for Research in Security and Privacy — **Center for Research in Security and Privacy**

CROSSING — **Cryptography-Based Security Solutions: Enabling Trust in New and Next Generation Computing Environments**

EC SPRIDE European Center for Security and Privacy by Design — **European Center for Security and Privacy by Design**

Possibilistic Information Flow

[Goguen/Meseguer '82]



System is split in two security domains

- High: Confidential part of the system invisible to the attacker
- Low: Non-confidential part of the system visible to the attacker

When is a system possibilistic secure?

- Each low execution of the system can be explained by multiple high executions such that no confidential information can be deduced

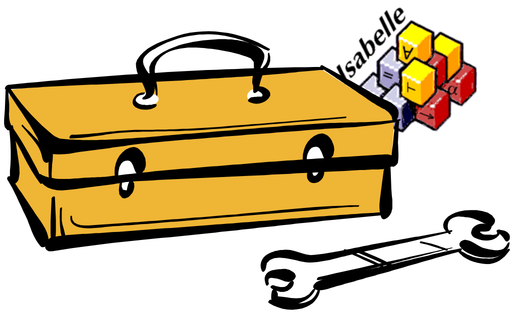
How to define confidential information for a system?

How to guarantee possibilistic information flow security?

I-MAKS

An extendable tool for possibilistic information flow that allows to …

- specify your system as an event structure.
- tailor your security requirement.
- verify security in a unified way.



I-MAKS directly benefits from its …

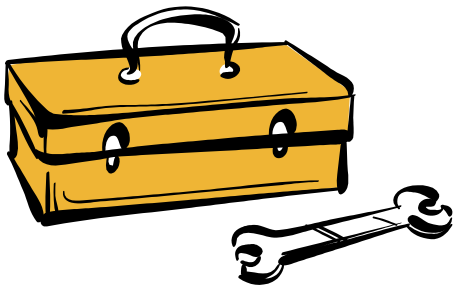
- conceptual basis:
  MAKS in its version from [Man03]
- technical basis:
  the Isabelle/HOL theorem prover [NPW02]

I-MAKS allows machine-aided specification & verification of possibilistic information flow!

MAKS

[Mantel '00, '03]

Modular Assembly Kit for Security Properties



- Uniform framework for the specification & verification of information flow properties
- MAKS provides …
  - support for event-based system models
  - building blocks for the definition of information flow properties
  - compositionality and unwinding results

Tailor your security property, verify the security of your system components and obtain the security of the whole system for free!

MAKS keeps evolving …

- it is used and adapted by scientists around the world Deepak D'Souza [DSHKRS08, DSHRS11], Dieter Hutter [HS04, Hut06, HMSS08], Ketil Stølen [SS06, SS09], …

Isabelle/HOL

[Nipkow/Paulson/Wenzel '02]

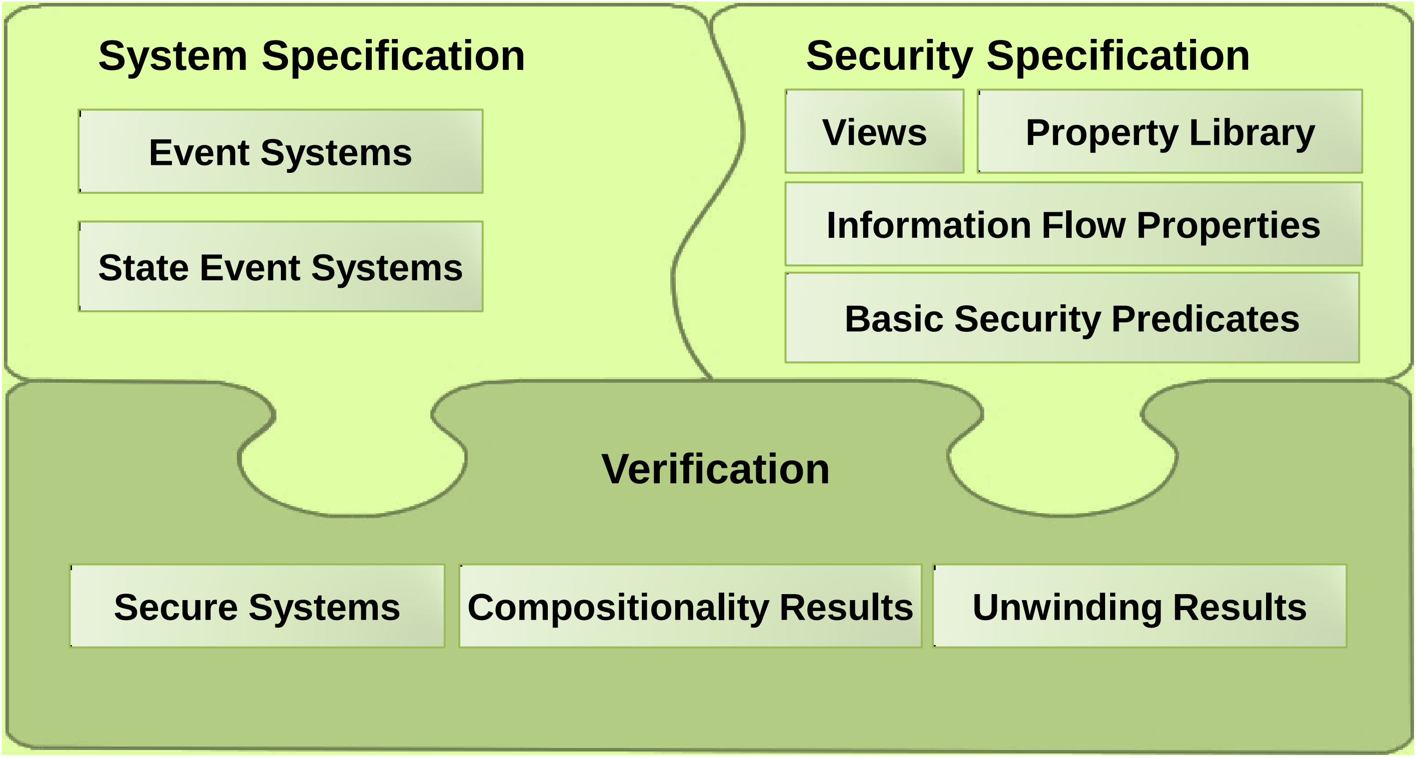
Proof Assistant with support for

- reasoning about meta-theory
- reasoning in higher order logic
- reasoning in first order logic

Relevant for this talk …

- definitions of terms and functions (keyword `definition`)
- record types, i.e, tuples with named fields (keyword `record`)
  - as notational convention `F`$_{S}$ denotes the field `F` of the record `S`
- libraries for lists and sets (parametric types `'e set` and `'e list`)
  - empty list `[]`, cons (`x # xs`), concatenation `[a,b,c]@[d,e]`
  - empty set `{}`, union ∪, intersection ∩, setminus –

Overview of I-MAKS



- **System Specification:** Concepts to define security properties
- **Security Specification:** Supported systems models
- **Verification:** Verification techniques and helpful results

I-MAKS – Preliminaries

Events

- Events are terms that model an atomic action of a system
- In Isabelle/HOL: Formalized by a type `'e`

Traces

- Traces are lists of events that model the behavior of a system
- In Isabelle/HOL: Formalized by instances of the type `'e list`

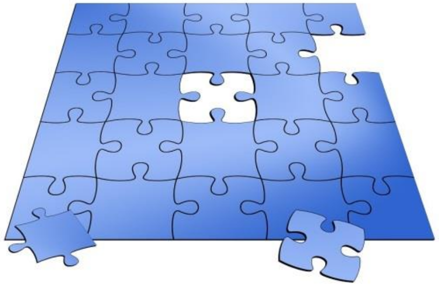
Projection

- Removes all events from a given trace that are not in a given set of events
- In Isabelle/HOL defined as filter on a given list (abbreviated by ↾)
  - Example: `[] ↾ {a,c} = []` and `[a,b,c]↾{a,c} = [a,c]`

Views

Attacker Model (Observer)

- Partial view on the system's execution
  - i.e, can only observe a subset of events
- Goal: Fill gaps with confidential system behavior



Formalization in I-MAKS

record 'e V_rec = V :: "'e set" N :: "'e set" C :: "'e set"

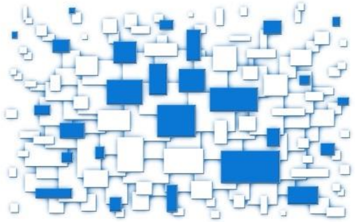
definition V_valid :: "'e set ⇒ 'e V_rec ⇒ bool" **where**
"V_valid E $\mathcal{V} \equiv V_{\mathcal{V}} \cap N_{\mathcal{V}} = \{\} \wedge V_{\mathcal{V}} \cap C_{\mathcal{V}} = \{\} \wedge N_{\mathcal{V}} \cap C_{\mathcal{V}} = \{\}$"

definition isViewOn :: "'e V_rec ⇒ 'e set ⇒ bool" **where**
"isViewOn $\mathcal{V}$ E ≡ V_valid E $\mathcal{V} \wedge V_{\mathcal{V}} \cup N_{\mathcal{V}} \cup C_{\mathcal{V}} = E$"

Definition: Let E be a set of events of a type 'e. A VIEW ON E is an instance $\mathcal{V}$ of the record type 'e V_rec such that isViewOn $\mathcal{V}$ E.

Basic Security Predicates (BSPs)

Building Blocks of Information Flow Properties



- Parametric in the perspective of the attacker
- Closure properties on a system’s behavior
  - i.e., executions potentially allowing deductions by the attacker can be explained by executions falsifying this deductions.

Formalization in I-MAKS

```
type_synonym 'e BSP = "'e V_rec ⟹ ('e list) set ⟹ bool"

definition BSP_valid :: "'e BSP ⟹ bool" where
"BSP_valid BSP ≡ ∀𝒱 Tr E. (isViewOn 𝒱 E ∧ ∀τ ∈ Tr. set τ ⊆ E)
                                    → (∃ Tr'. Tr' ⊇ Tr ∧ BSP 𝒱 Tr')"
```

Definition: A BASIC SECURITY PREDICATE for a type of events 'e is an instance BSP of the type 'e BSP such that BSP_valid BSP.

Backwards-Strict Deletion (BSD)

Example

definition BSD :: "'e BSP" **where**

BSD $\mathcal{V}$ Tr $\equiv$ $\forall\, \alpha\, \beta.\ \forall\, c \in C_{\mathcal{V}}.$

$$((\alpha\, @\, [c]\, @\, \beta \in Tr \wedge \beta \upharpoonright C_{\mathcal{V}} = [\,])$$
$$\longrightarrow (\exists \beta'.\ \alpha\, @\, \beta' \in Tr \wedge \beta' \upharpoonright V_{\mathcal{V}} = \beta \upharpoonright V_{\mathcal{V}} \wedge \beta' \upharpoonright C_{\mathcal{V}} = [\,]))$$

Explanation

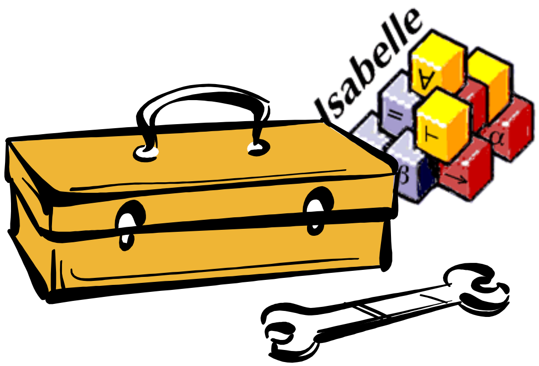
- Considers the last event in of a trace
- Requires that there exists an alternative trace such that …
  - the last event in $C_{\mathcal{V}}$ is deleted
  - the alternative trace is equal to the initial trace w.r.t. $V_{\mathcal{V}}$
  - the trace only differs in events in $N_{\mathcal{V}}$ after the deleted event in $C_{\mathcal{V}}$

BSD ensures that the attacker cannot deduce whether an event in $C_{\mathcal{V}}$ did actually occur in the trace the attacker is observing.

Summary

I-MAKS provides tool support for …

- specifying systems & security properties
- verifying the security of a system



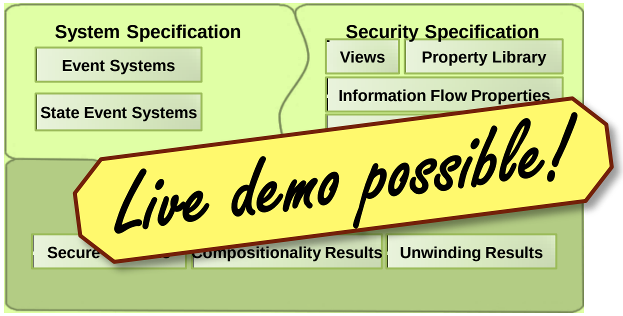
I-MAKS is …

versatile

- no prescribed system model
- tailored security requirements

reliable

- machine-checked meta-theory
- machine-aided verification



evolving

- inherited extendibility of MAKS

References

[DSHKRS08] Deepak D'Souza, Raveendra Holla, Janardhan Kulkarni, Raghavendra K. Ramesh and Barbara Sprick.
On the Decidability of Model-Checking Information Flow Properties.
In Proceedings of the 4th International Conference on Information Systems Security (ICISS), pages 26-40, 2008

[DSHRS11] Deepak D'Souza, Raveendra Holla, K. R. Raghavendra and Barbara Sprick.
Model-Checking Trace-Based Information Flow Properties.
In Journal of Computer Security 19(1): 101-138 (2011)

[HS04] Dieter Hutter and Axel Schairer.
Possibilistic Information Flow Control in the Presence of Encrypted Communication.
In Proceedings of the European Symposium on Research in Computer Security (ESORICS), pages 209–224, 2004.

[Hut06] Dieter Hutter.
Possibilistic Information Flow Control in MAKS and Action Refinement.
In Proceedings of the 2006 International Conference on Emerging Trends in Information and Communication Security (ETRICS), pages 268-281, 2006.

[HMSS08] Dieter Hutter, Heiko Mantel, Ina Schaefer and Axel Schairer.
Security of Multi-Agent Systems: A Case Study on Comparison Shopping.
In Journal of Applied Logic (JAL), 5(2), pages 303-332, 2007.

MAIS Modeling and Analysis of Information Systems
TECHNISCHE UNIVERSITÄT DARMSTADT

References

[GM82] Joseph A. Goguen and Jose Meseguer.
Security Policies and Security Models.
In Proceedings of the 3rd IEEE Symposium on Security and Privacy (S&P), pages 11–20, 1982.

[Man00] Heiko Mantel.
Possibilistic Definitions of Security – An Assembly Kit.
In Proceedings of the 13th IEEE Computer Security Foundations Workshop (CSFW), pages 185–199, 2000.

[Man03] Heiko Mantel.
A Uniform Framework for the Formal Specification and Verification of Information Flow Security.
PhD thesis, Saarland University, Saarbrücken, Germany, 2003.

[NPW02] Tobias Nipkow, Lawrence C. Paulson, and Markarius Wenzel.
Isabelle/HOL — A Proof Assistant for Higher-Order Logic.
LNCS 2283. Springer, 2002.

[SS06] Fredrik Seehusen, Ketil Stølen:
Maintaining Information Flow Security Under Refinement and Transformation.
In Proceedings of the 4th International Workshop on Formal Aspects in Security and Trust (FAST), pages 143-157, 2006

[SS09] Fredrik Seehusen and Ketil Stølen.
Information Flow Security, Abstraction and Composition.
In IET Information Security 3(1): 9-33 (2009)