RS3 Practitioner Day, June 7-8, 2016, Darmstadt

Reliably Secure Software Systems (RS^3) - A National Research Priority Program

Prof. Dr.-Ing. Heiko Mantel (Coordinator)

Modeling and Analysis of Information Systems (MAIS),
Technische Universität Darmstadt

work funded by the DFG in Priority Program 1496:
Reliably Secure Software Systems (RS^3)

IT-Security as a Business

Evolution

Worldwide total revenue
with security software in 2008
about 10.5 billion USD

[source: Gartner Inc]

IT-Security as a Business

Evolution

Worldwide total revenue
with security software in ~~2008~~ 2014
about ~~10.5~~ 21.4 billion USD

[source: Gartner Inc]

Relevance of IT-Security

Evolution

IT-security is a fundamental problem of secondary importance.

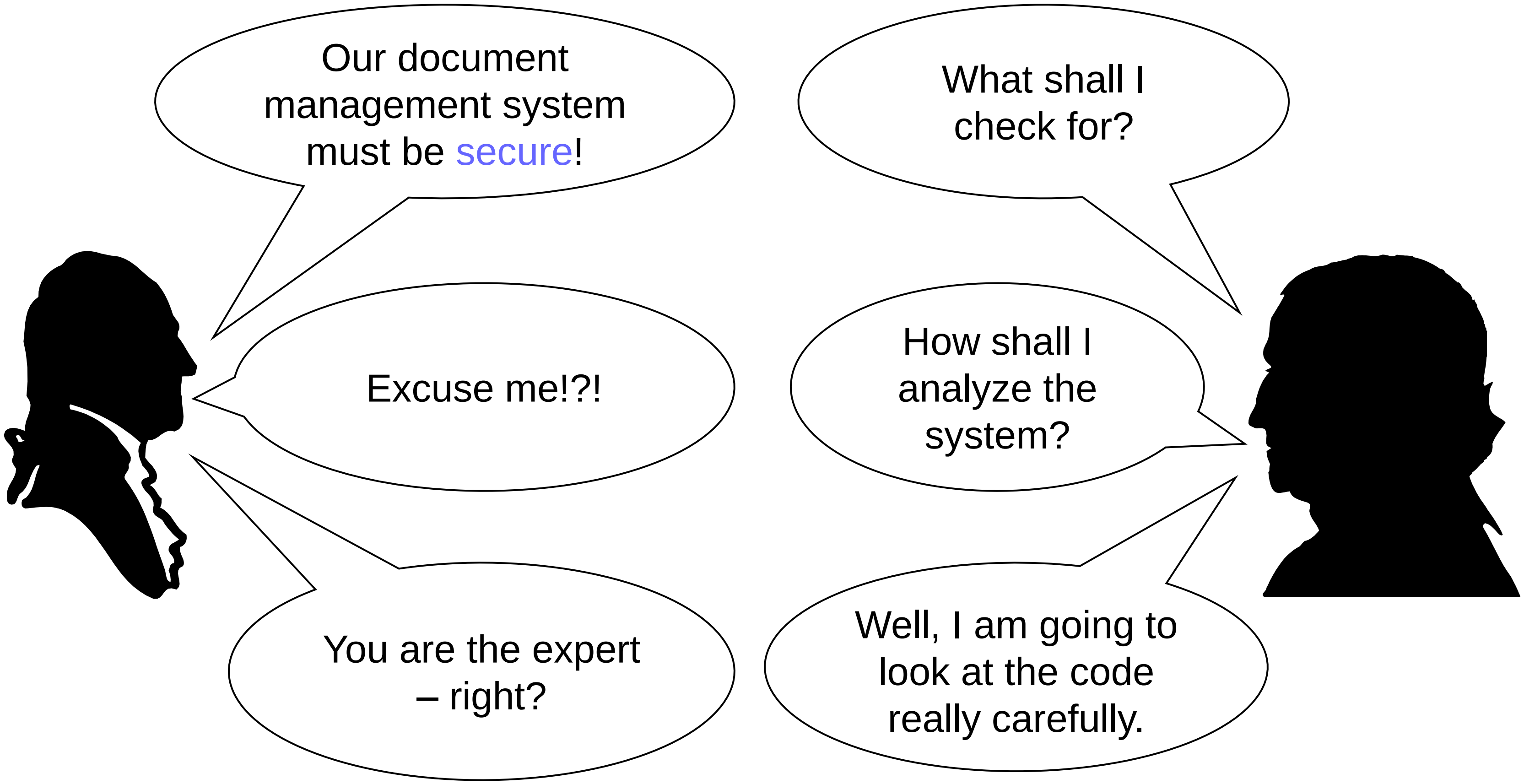
IT-security vulnerabilities is a problem of primary importance for business and government.

Lack of security guarantees is a problem of primary importance for business and government.

Example areas with high security needs

fourth industrial revolution (Industrie 4.0), vehicle control, e-banking, e-commerce, e-government, e-voting, smart on-line services, cloud, wearable devices, digital identity, third-party apps, third-party code, ….

IT-Security as a Requirement



Our document management system must be secure!

What shall I check for?

Excuse me!?!

How shall I analyze the system?

You are the expert – right?

Well, I am going to look at the code really carefully.

Next

a metaphor

Mechanism-Centric Security (1)

How to decide whether security has been achieved?

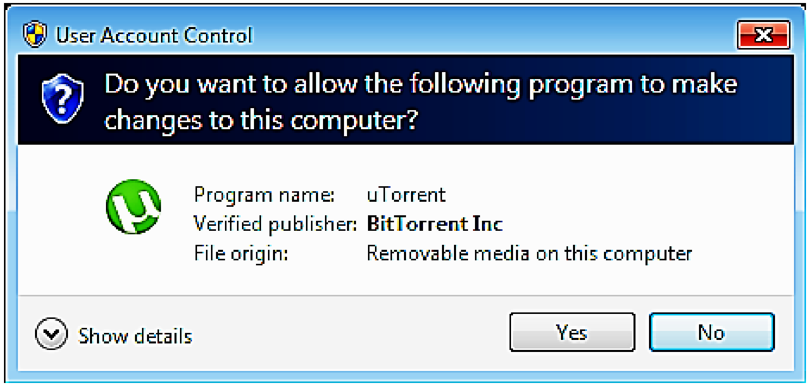
Mechanism-Centric Security (2)

Problems

- How can a system developer ensure that all relevant security aspects have been properly addressed?
- How can a user decide whether a system is sufficiently secure?
- How can a user assess the consequences of his decisions?

Do you want to grant "browser.exe" access to the Internet?

Do you allow "setup.exe" to make changes to your setup?



User Account Control

Do you want to allow the following program to make changes to this computer?

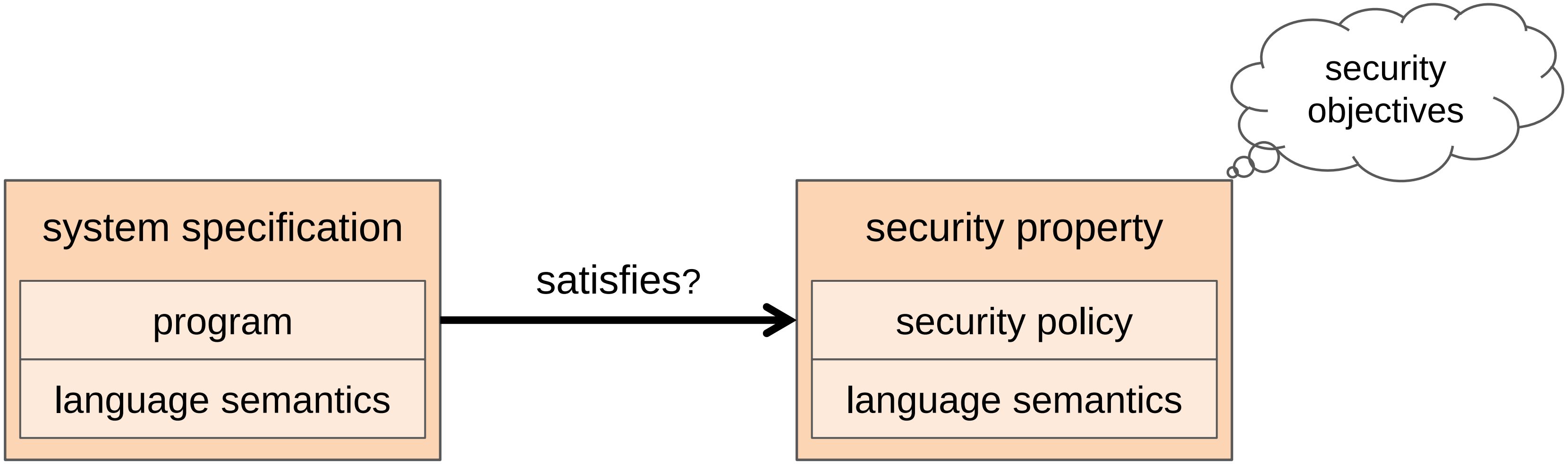
Program name: uTorrent
Verified publisher: BitTorrent Inc
File origin: Removable media on this computer

Next

the vision

Property-Centric Security (1)

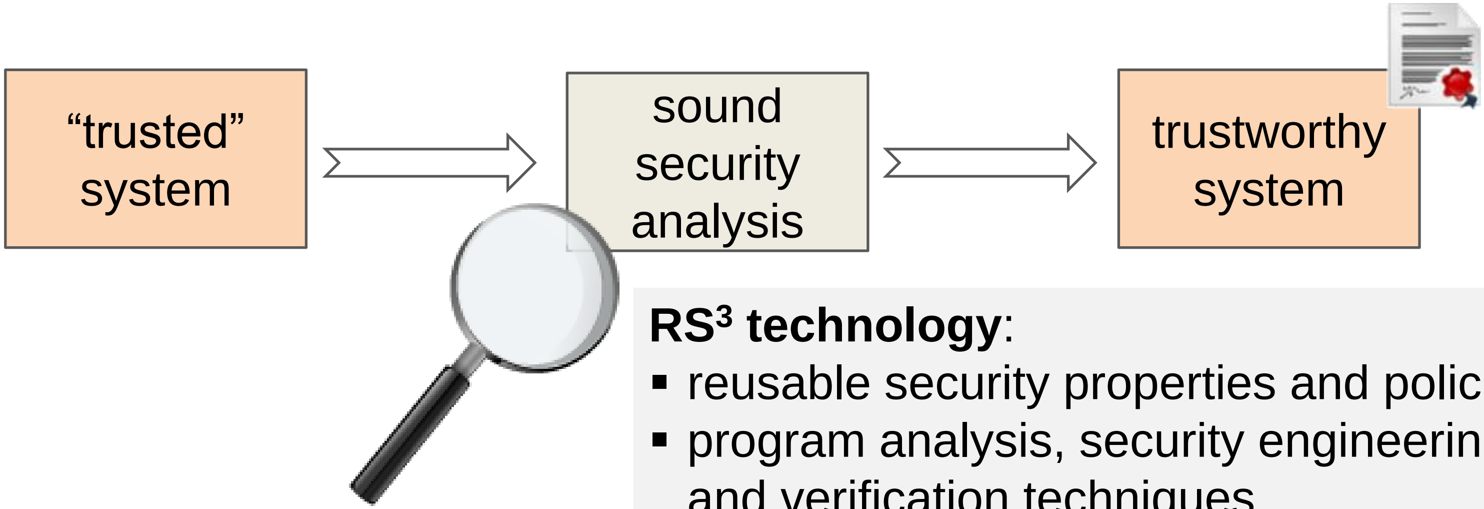
Formal definition of security requirements based on well-defined semantics of programs and security aspects:



Declarative security properties specify what is achieved rather than how it is achieved!

Property-Centric Security (2)

Formal verification of selected, formally specified security requirements using program analysis and verification tools:



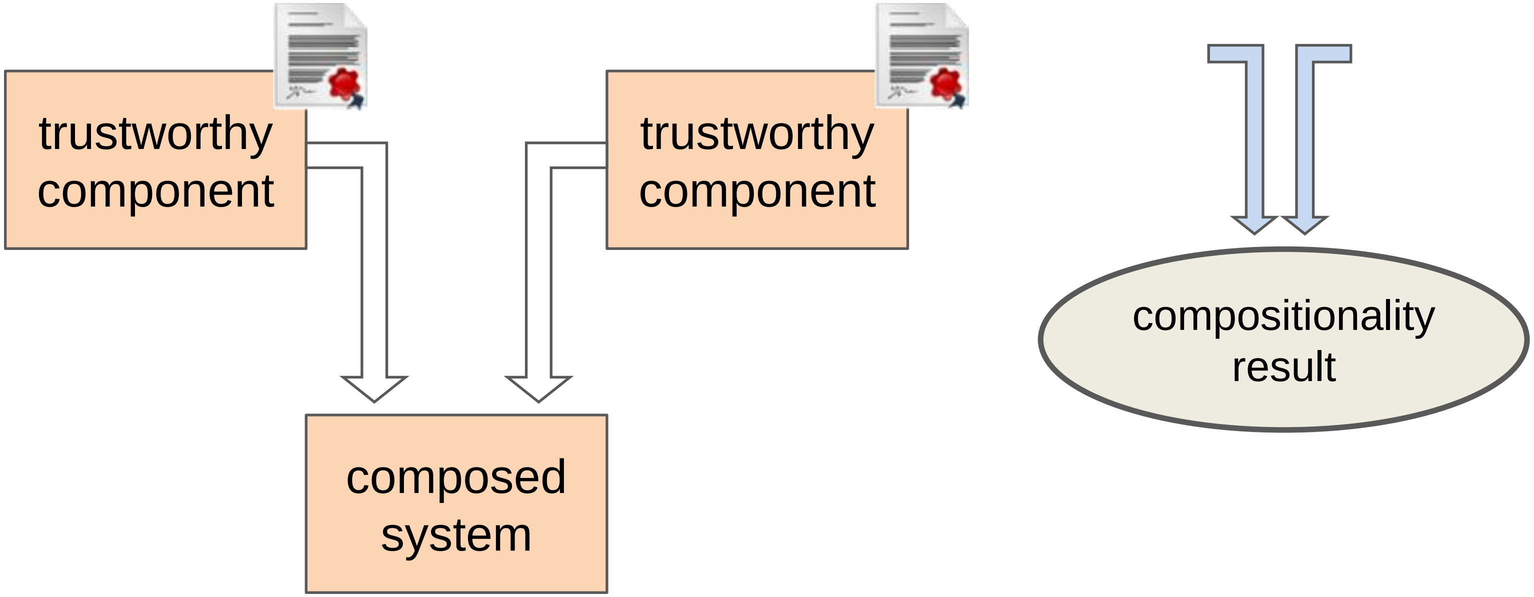
RS^3 technology:

- reusable security properties and policies
- program analysis, security engineering, and verification techniques
- tool support
- case studies

Semantic gap between declarative security property and operational system specification makes verification meaningful!

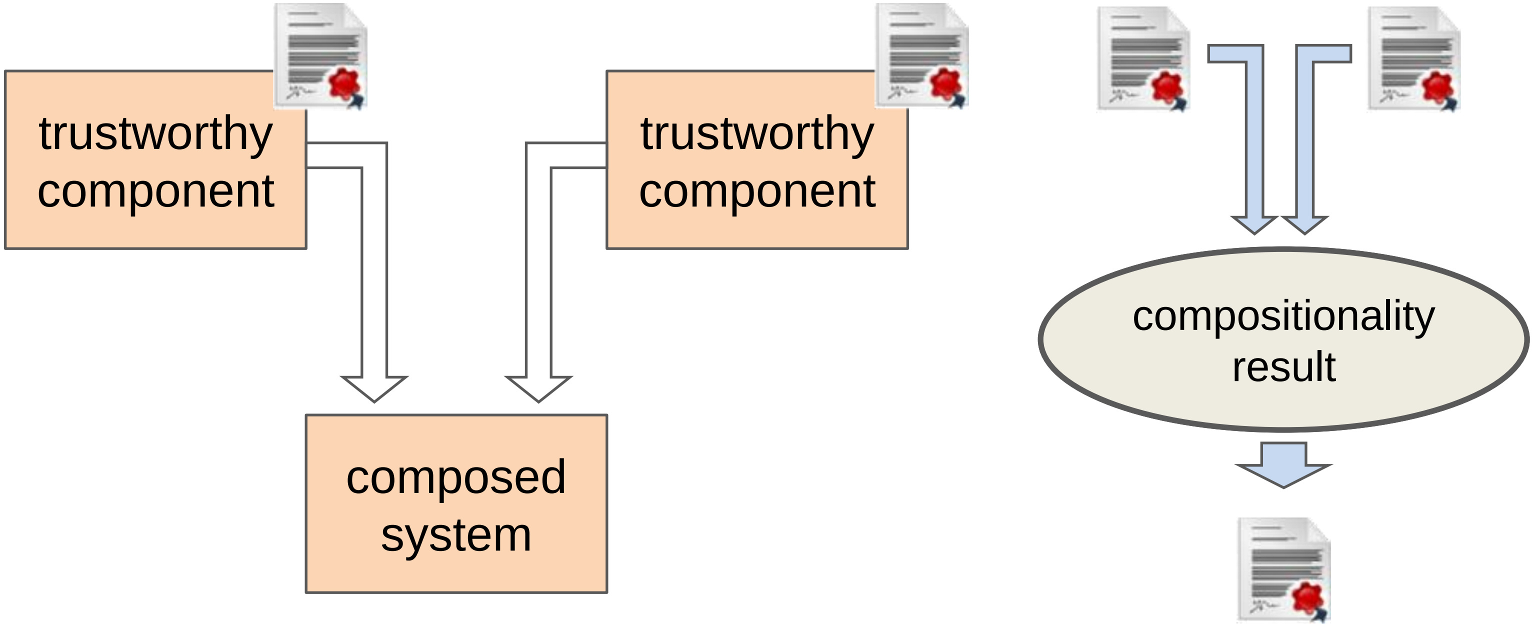
Property-Centric Security (3)

Reduction of conceptual complexity based on declarative security guarantees and modular reasoning:



Property-Centric Security (3)

Reduction of conceptual complexity based on declarative security guarantees and modular reasoning:

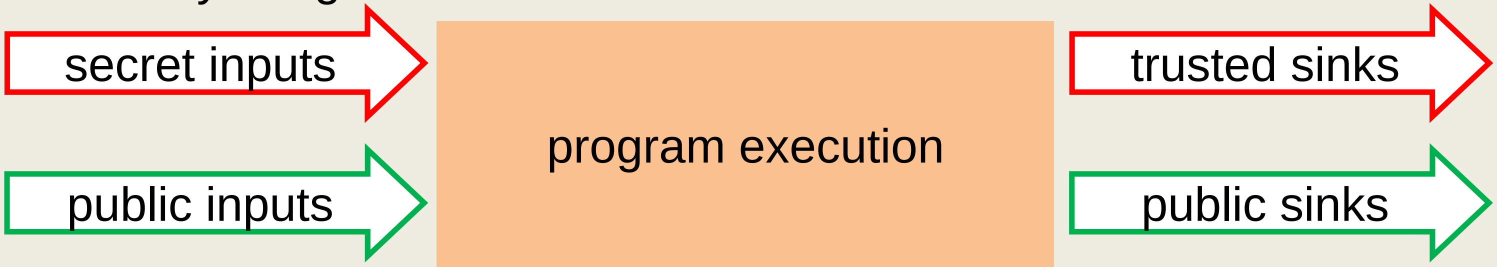


Compositionality results for declarative security properties provide a basis for making security scale in a sound way!

Information-Flow Security

A role model for declarative security properties

Is there any danger that secrets are leaked?



secret inputs

public inputs

program execution

trusted sinks

public sinks

Formalization

$$\forall S, T, S', T' \in states.$$

$$S =_{public} T \;\wedge\; \langle P, S \rangle \rightarrow S' \;\wedge\; \langle P, T \rangle \rightarrow T' \;\Rightarrow\; S' =_{public} T'$$

Intuition: If publicly visible output does not depend on secrets then there is no danger that secrets are leaked.

Next

the priority program

DFG Priority Programs

Aims of DFG priority programs

“To advance knowledge in an emerging field of research through collaborative networked support over several locations”

[www.dfg.de]

“[…] nationwide cooperation between its participating researchers”

[www.dfg.de]

“Priority programmes are characterized by their

- enhanced quality of research through the use of new methods and forms of collaboration in emerging fields
- added value through interdisciplinary cooperation
- networking”

[www.dfg.de]

“The priority programme has the potential for increasing international importance, or is likely to have a lasting impact on the scientific landscape.”

[DFG guideline 50.05]

Reliably Secure Software Systems

A nation-wide research program on reliable software security

- coordinator: Prof. Dr. Heiko Mantel
- funded by the DFG

Timeline

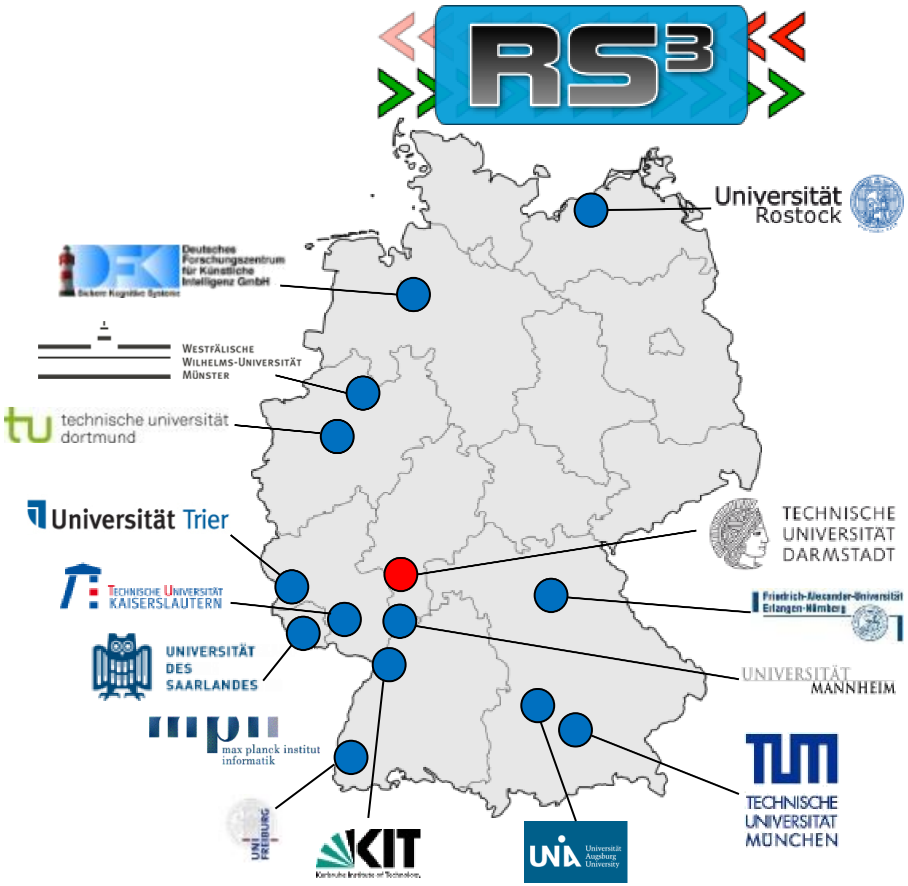
- preparation phase: 2008–2010
- funding phases:
  2010–2012–2014–2016
- final event: summer 2017

Participants

- 37 funded projects
- various associated projects

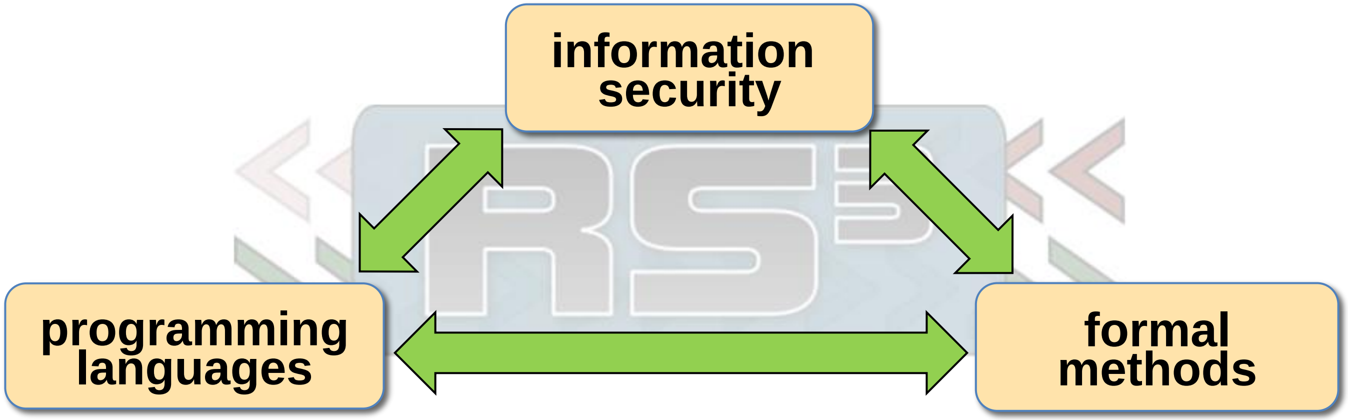
Friends of RS^3 (FoRS^3)

informal club of experts from industry who participated in RS^3 events


RS³
Universität Rostock
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH
Sichere Kognitive Systeme
Westfälische Wilhelms-Universität Münster
technische universität dortmund
Universität Trier
Technische Universität Kaiserslautern
Universität des Saarlandes
max planck institut informatik
Uni Freiburg
KIT
Karlsruhe Institute of Technology
UNIA
Universität Augsburg University
TUM
Technische Universität München
Universität Mannheim
Friedrich-Alexander-Universität Erlangen-Nürnberg
Technische Universität Darmstadt

Intra-Disciplinary Research

Enable synergy-potential across different sub-disciplines of CS



to push forward

1. property-centric approaches to IT-security,
2. reliable verification of declarative security guarantees, and
3. scaling reliable security guarantees to larger IT-systems

Scope: Reliable security guarantees for software-based systems based on formal semantics of programs and of security aspects.

Research Topics in RS^3

Themes

Information
Flow
Analysis
Noninterference
Security
Systems
Programs
Control
Dynamic
Usage
Verification
Java
Model
Quantitative
Business
Data
workflow
Properties
Coercion-Resistance
Checking
Memory
Storage
Model-Driven
Linear
Flow-Secure
Networks
Processes
models
Multi-level
approach
Monitoring
Approach
Verifiability
Cryptographic
Type
Process
Side
Privacy
IFlow
Tracking
flow
XML
Typing
Study
via
Web
JavaScript
Towards
Graphs
Efficient
systems
model-driven
Automatic
Proving
Gradual
Pushdown
Concurrent
Models
information
Framework
Distributed
Formal
Machine-Checked
Formalizing
Possibilistic
Guarantees
Temporal
Applications
Using
Quantification
Enforcement
Development
control
confidential
Network
Social
Malware
Compatibility
Confidentiality
PKCS
POG-based
Empirical
Behaviour
Transformations
Synchronized
User
E-Voting
References
Runtime
Compositionality
Unified
Compliance-Preserving
IF
new
Lock-sensitive
Dependence
Mix
v1.5
Weakest
Firewalls
Scantegrity
Antecedent
eHealth
Application
Geographic
Smart
general-purpose
Strikes
Data-Driven
Joana
Hard
Applying
Implementation
tale-charts
Organizational
Closures
Nets
Safety
enforcement
Wireless
Simplification
Procedure
Proxies
Representation-Independent
Cloud
Stubborn
Locking
System
Static
Dependency
Sound
Randomized
analyzes
processes
Type-based
regions
Conference
Superposition
Permissive-Upgrade
Encoding
Sets
Networked
Insights
Workflow-Modellen
Game-Based
Federation
Blame
Encryption
Condition
Enterprise
Secrecy
Mitigation
Example
Generalizing
Experiences
business
multi-layer
Mind
Rules
SAT
Tree
New
domain-specific
Compositional
Modeling
Bleichenbacher's
Anwenden
Interference
Partial
service-oriented
zur
Strong
Precise
Path
Ceiling
Proof
Weak
Attack
Criteria
Clash
Matters
Indistinguishable
Filter
Channels
Isabelle
wizard
Aware
Java-like
Automata
WebKI's
UML
Creation
Non-interference
Non-Malicious
Environmental
Manipulating
Self-Composition
Probabilistic
Contextual
Annotated

Project clusters:

sequential&concurrent noninterference, security engineering, usage control

Progress in RS^3

RS^3 @ top conferences, e.g.,

CSF ’11,12, 14,15

Security&Privacy ’11,12, 14

CAV ’11,14,15

CCS ’13

ICSE ’12,15

MPC ’12

RV ’11

CODASPY ’13

CADE ’13

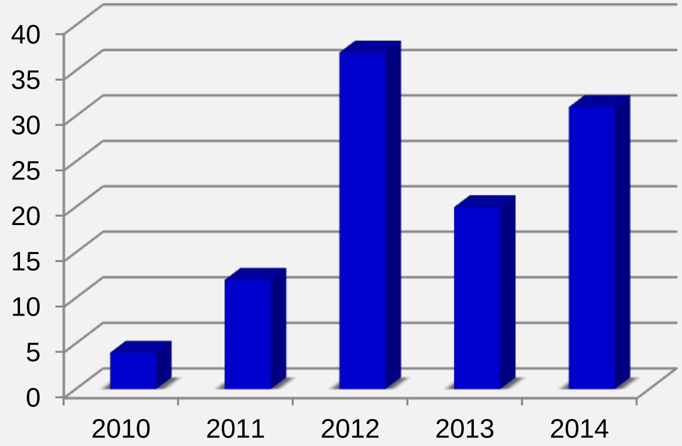
POPL ’11

POST ’14

VMCAI ’11,12

LOPSTR ’15

Reviewed RS3 publications



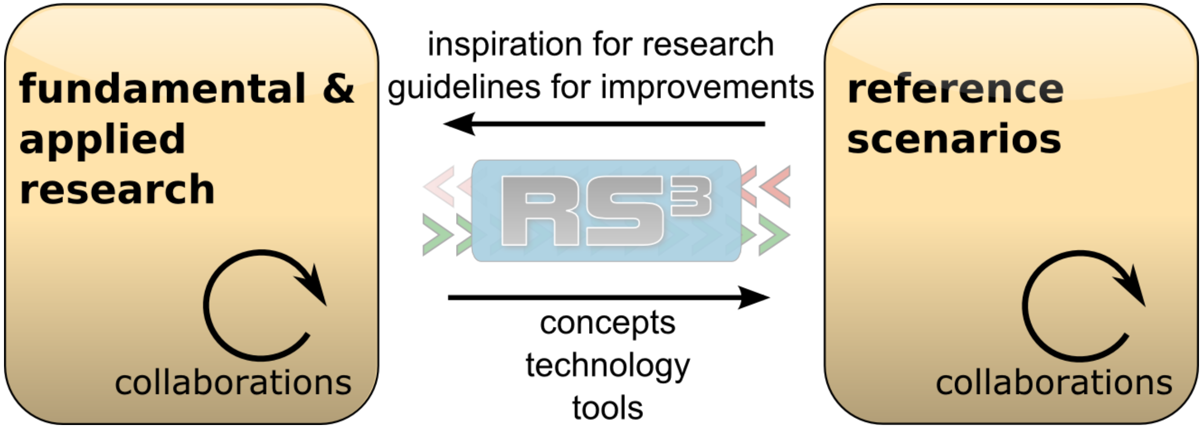
Education (by end of 2014)

- >25 BSc theses
- >45 MSc/Diploma theses
- >8 PhD theses
- 2 professors (or equivalent)

Role of our Reference Scenarios

Reference scenarios are RS^3-wide collaborations on case studies

- grouping of projects by common application scenario



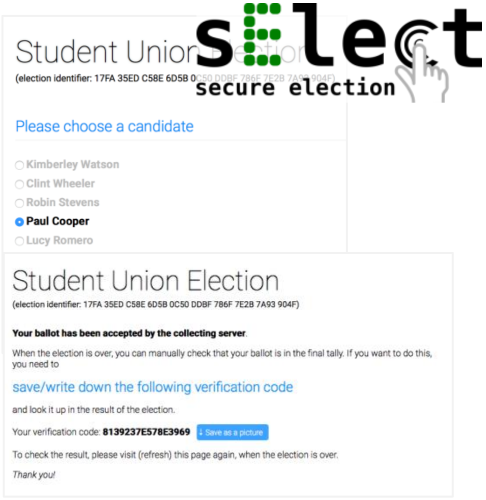
Goals:

- apply technology to solve practical problems
- exchange insights across different areas of expertise
- inspire research questions

From Foundations to Engineering

Security in E-Voting

sElect, an E-Voting system with proven confidentiality of votes and verifiability



Student Union Election
(election identifier: 17FA 35ED C58E 6D5B 0C50 DDBF 786F 7E2B 7A93 904F)

Please choose a candidate

○ Kimberley Watson
○ Clint Wheeler
○ Robin Stevens
● Paul Cooper
○ Lucy Romero

Student Union Election
(election identifier: 17FA 35ED C58E 6D5B 0C50 DDBF 786F 7E2B 7A93 904F)

Your ballot has been accepted by the collecting server.

When the election is over, you can manually check that your ballot is in the final tally. If you want to do this, you need to

save/write down the following verification code

and look it up in the result of the election.

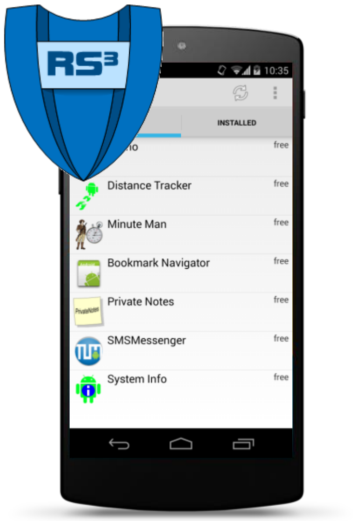
Your verification code: **8139237E578E3969** ↓ Save as a picture

To check the result, please visit (refresh) this page again, when the election is over.

Thank you!

Software Security for Mobile Devices

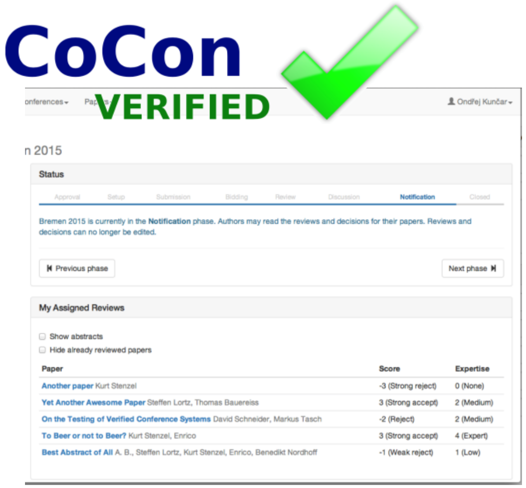
RS³ Certifying App Store, provides user-defined security guarantees about Android apps



...no	free
Distance Tracker	free
Minute Man	free
Bookmark Navigator	free
Private Notes	free
SMSMessenger	free
System Info	free

Security in Web-based Workflow Management Systems

CoCon, a conference management system with verified confidentiality properties



n 2015

Status

Approval Setup Submission Bidding Review Discussion **Notification** Closed

Bremen 2015 is currently in the **Notification** phase. Authors may read the reviews and decisions for their papers. Reviews and decisions can no longer be edited.

Previous phase — Next phase

My Assigned Reviews

□ Show abstracts
□ Hide already reviewed papers

Paper	Score	Expertise
Another paper Kurt Stenzel	-3 (Strong reject)	0 (None)
Yet Another Awesome Paper Steffen Lortz, Thomas Bauereiss	3 (Strong accept)	2 (Medium)
On the Testing of Verified Conference Systems David Schneider, Markus Tasch	-2 (Reject)	2 (Medium)
To Beer or not to Beer? Kurt Stenzel, Enrico	3 (Strong accept)	4 (Expert)
Best Abstract of All A. B., Steffen Lortz, Kurt Stenzel, Enrico, Benedikt Nordhoff	-1 (Weak reject)	1 (Low)

Presentations by RS^3 Researchers

Reference scenarios

Prof. Dr. Eric Bodden
Paderborn University

Prof. Dr. Dieter Hutter
DFKI GmbH and Bremen University

Prof. Dr. Ralf Küsters
Trier Univesity

Impulse talks

Prof. Dr. Bernhard Beckert
Karlsruhe Institute of Technology

Prof. Dr. Wolfgang Reif
Augsburg University

Posters

This work was supported by the DFG in the Priority Program
“Reliably Secure Software Systems” (RS^{3}).

http://www.reliably-secure-software-systems.de