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$^3$)
Worldwide total revenue with security software in 2008 about 10.5 billion USD

[source: Gartner Inc]
Evolution

Worldwide total revenue with security software in 2008 about 10.5 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?
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:

"trusted" system  sound security analysis  trustworthy system

RS³ 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

\[ \forall S, T, S', T' \in \text{states}. \quad S = \text{public } T \land \langle P, S \rangle \rightarrow S' \land \langle P, T \rangle \rightarrow T' \Rightarrow S' = \text{public } T' \]

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]

“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]

“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]
Reliably Secure Software Systems

A nation-wide research program on reliable software security

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

Timeline

- final event: summer 2017

Participants

- 37 funded projects
- various associated projects

Friends of RS³ (FoRS³)

informal club of experts from industry who participated in RS³ events
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 RS³

Themes

Project clusters:
sequential & concurrent noninterference, security engineering, usage control
Progress in $\text{RS}^3$

$\text{RS}^3$ @ top conferences, e.g.,

- CSF ’11,12, 14,15
- Security&Privacy ’11,12, 14
- CAV ’11,14,15
- CAV ’11,14,15
- MPC ’12
- MPC ’12
- RV ’11
- RV ’11
- CODASPY ’13
- CODASPY ’13
- CADE ’13
- CADE ’13
- POPL ’11
- POPL ’11
- POST ’14
- POST ’14
- VMCAI ’11,12
- VMCAI ’11,12
- LOPSTR ’15
- LOPSTR ’15

Reviewed $\text{RS}3$ 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

Software Security for Mobile Devices

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

Security in Web-based Workflow Management Systems

**CoCon**, a conference management system with verified confidentiality properties
Presentations by RS³ Researchers

Reference scenarios

Prof. Dr. Eric Bodden
Faderborn University

Prof. Dr. Dieter Hutter
DFKI GmbH and Bremen University

Prof. Dr. Ralf Küsters
Trier University

Impulse talks

Prof. Dr. Bernhard Beckert
Karlsruhe Institute of Technology

Prof. Dr. Wolfgang Reif
Augsburg University

Posters

© Heiko Mantel, 2016
This work was supported by the DFG in the Priority Program “Reliably Secure Software Systems” (RS³).

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