Software Security for Mobile Devices

S. Arzt, A. Bartel, R. Gay, S. Lortz, E. Lovat, H. Mantel, M. Mohr, B. Nordhoff, M. Perner, S. Rasthofer, D. Schneider, G. Snelting, A. Starostin, A. Weber

Coordinator: Prof. Dr. Heiko Mantel, TU Darmstadt

The RS³ Certifying App Store

- **vision:** user-centric, semantically justified security for Android devices
- **approach:** integrate security technology into an app store for Android
  - a single solution for multiple security concerns
  - accessible to the end user of a mobile device
  - providing explicit security guarantees
  - supporting user-defined security policies

static information-flow analysis

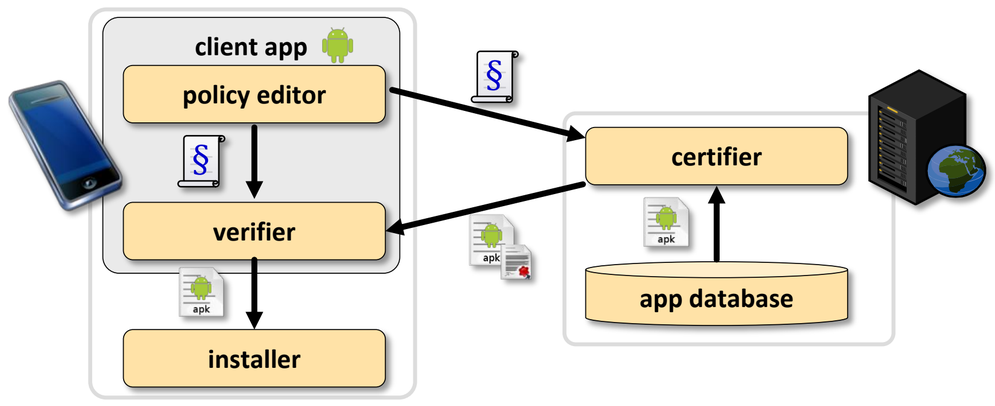
- before installation
- ensures **confidentiality** of sensitive user data

dynamic enforcement

- at run-time
- prevents **unwanted behavior** of applications

Static Analysis

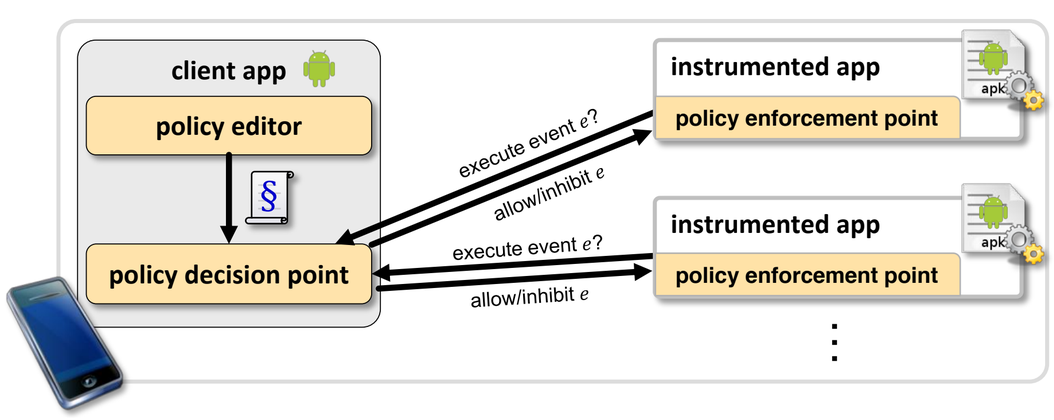
- **certification** of information flow security before installation of apps
  - notion of security formalized by a noninterference property
- two approaches to **static analysis of bytecode**
  - type-based and PDG-based
- **soundness** of the type-based analysis proven
  - w.r.t. formal operational semantics and the notion of security



- **proof-carrying code** principle used by the type-based analysis
  - allows to shift main workload to server
  - without including it in the trusted computing base

Dynamic Enforcement

- **enforcement** of usage control policies
- **instrumentation** of applications before installation
  - by inlining of policy enforcement points (PEPs)
  - intercept critical events and enforce decisions at run-time



- **central decision-making** by a single policy decision point (PDP)
  - enables enforcement of system-wide policies
  - enables exchange of policies without changing controlled apps

RS³

"Software Security for Mobile Devices" is one of the three reference scenarios of the nation-wide research program **"Reliably Secure Software Systems" (RS³)** funded by the German Research Foundation (DFG).

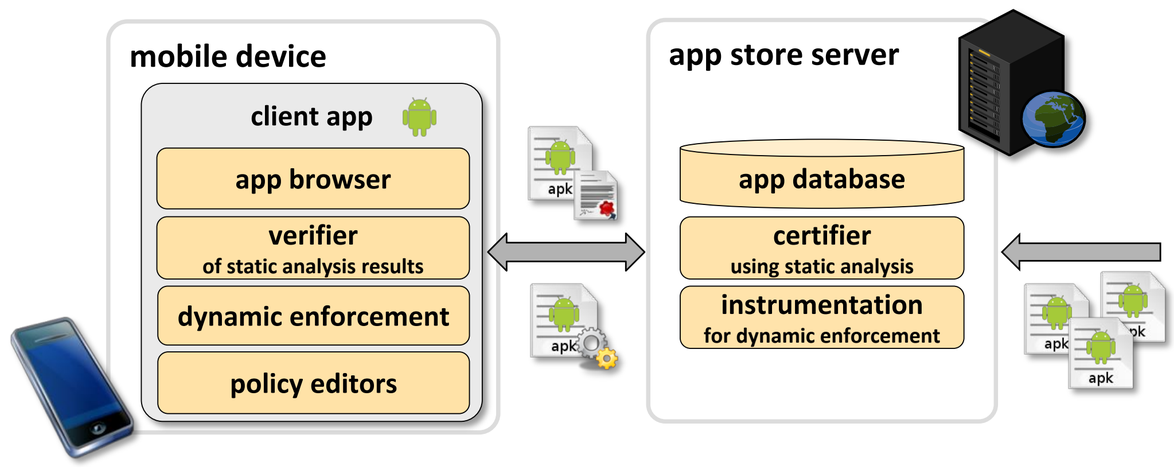
The vision of RS³ is to initiate a shift to a property-centric view on software security based on semantically well-founded approaches.

For more information, visit:

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

Architecture

- **client-server architecture**
  - security technology integrated on both sides



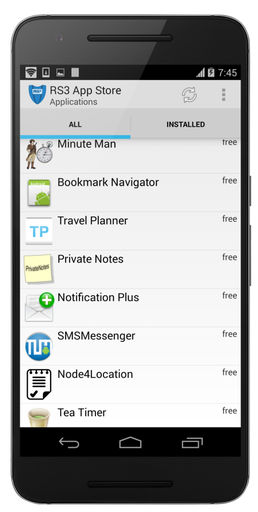
Prototype

- **policy editors** aid the user in specifying his security requirements
  - selection of categories of sensitive data to keep confidential
  - instantiation of generic policy templates restricting the behavior of apps
- **visualization** makes information flow in apps transparent to the user

- **simple** to set up and use
  - client app runs on off-the-shelf devices
  - server-side part runs on conventional web servers

Evaluation

- initial evaluation on self-developed **case studies**
  - core functionality of existing third-party apps
  - check whether problems are found/prevented
- recently: evaluation on **third-party apps**
  - from the F-Droid open-source app store
  - investigate how technologies scale
- **example:** "Tea Timer"
  - provides countdown timers
  - is allowed to read identity and write to SD card
  - concern: identity may be leaked to SD card
  - IF analyses guarantee absence of potential leak



next goal: provide useful guarantees for more third-party apps to user

Selected Publications

- S. Lortz, H. Mantel, A. Starostin, T. Bähr, D. Schneider, and A. Weber. Cassandra: Towards a Certifying App Store for Android. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 93–104, 2014.
- M. Mohr, J. Graf, and M. Hecker. JoDroid: Adding Android Support to a Static Information Flow Control Tool. In *Proceedings of the 8th Working Conference on Programming Languages*, pages 140–145, 2015.
- S. Rasthofer, S. Arzt, E. Lovat, and E. Bodden. DroidForce: Enforcing Complex, Data-Centric, System-Wide Policies in Android. In *Proceedings of the 9th International Conference on Availability, Reliability and Security*, pages 40–49, 2014.

TECHNISCHE UNIVERSITÄT DARMSTADT · TECHNISCHE UNIVERSITÄT MÜNCHEN · Karlsruher Institut für Technologie · Westfälische Wilhelms-Universität Münster · DFG