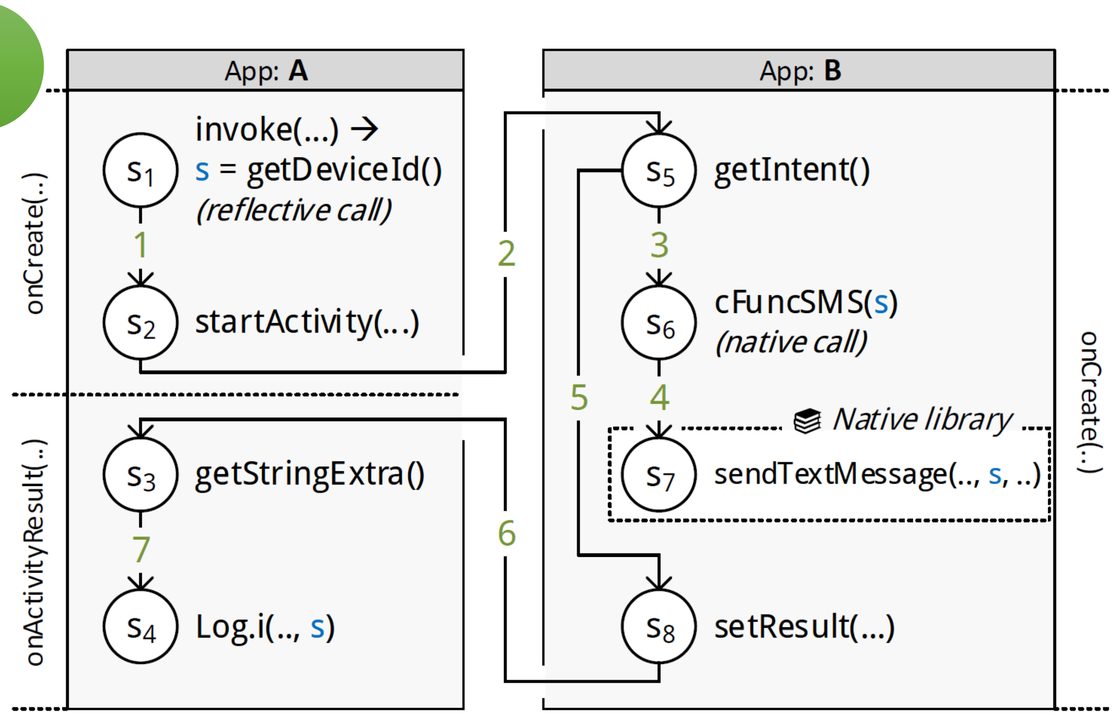
PADERBORN UNIVERSITY

SFB901 ON - THE - FLY COMPUTING

» Android App Analysis Query Language «

Cooperative Android App Analysis finally simple

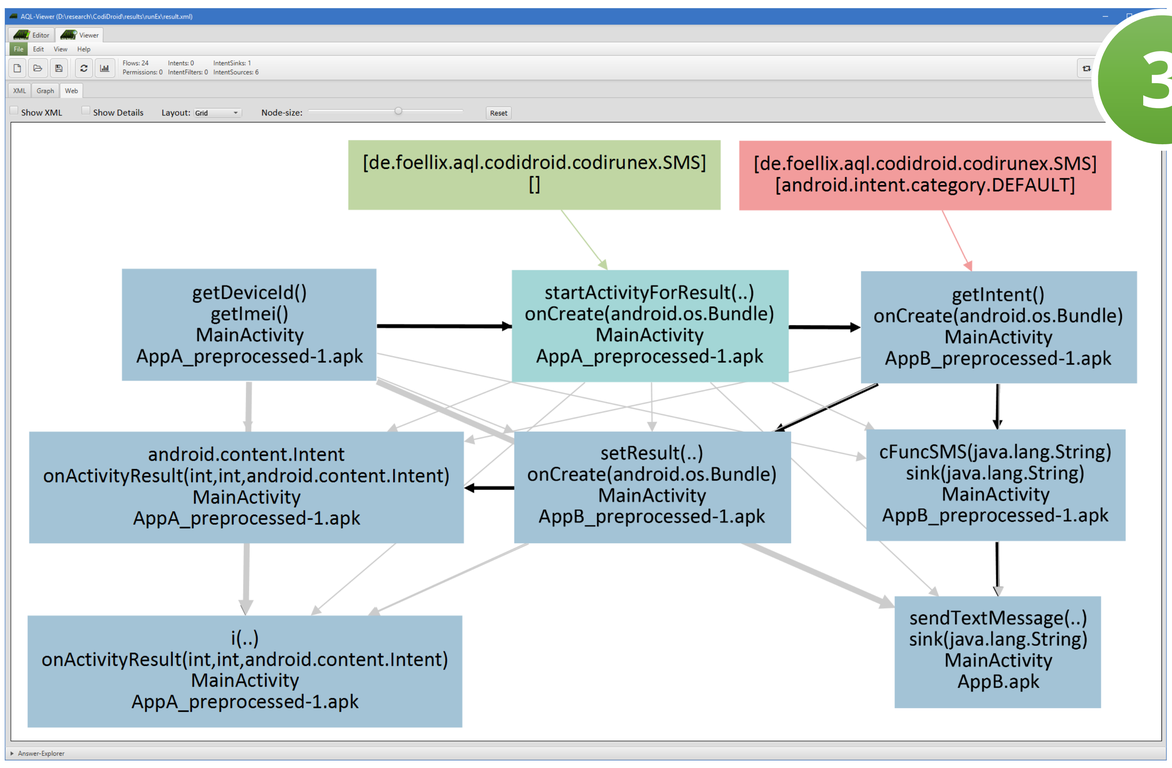
1



2

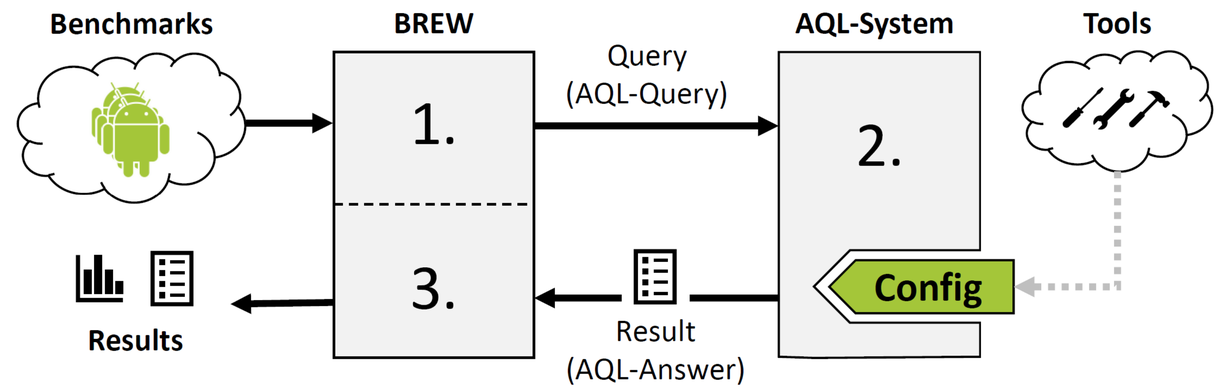
```
Flows FROM App('A.apk') TO App('B.apk') ?

MATCH [
      Flows IN App('A.apk' | 'DEOBFUSCATE') ?,
      CONNECT [
            Flows IN App('B.apk' | 'UNCOVER') ?,
            Flows IN App('B.apk' | 'UNCOVER')
                  FEATURING 'NATIVE' ?
      ],
      IntentSources IN App('A.apk' | 'DEOBFUSCATE') ?,
      IntentSinks IN App('A.apk' | 'DEOBFUSCATE') ?,
      IntentSources IN App('B.apk' | 'UNCOVER') ?,
      IntentSinks IN App('B.apk' | 'UNCOVER') ?
]
```

3



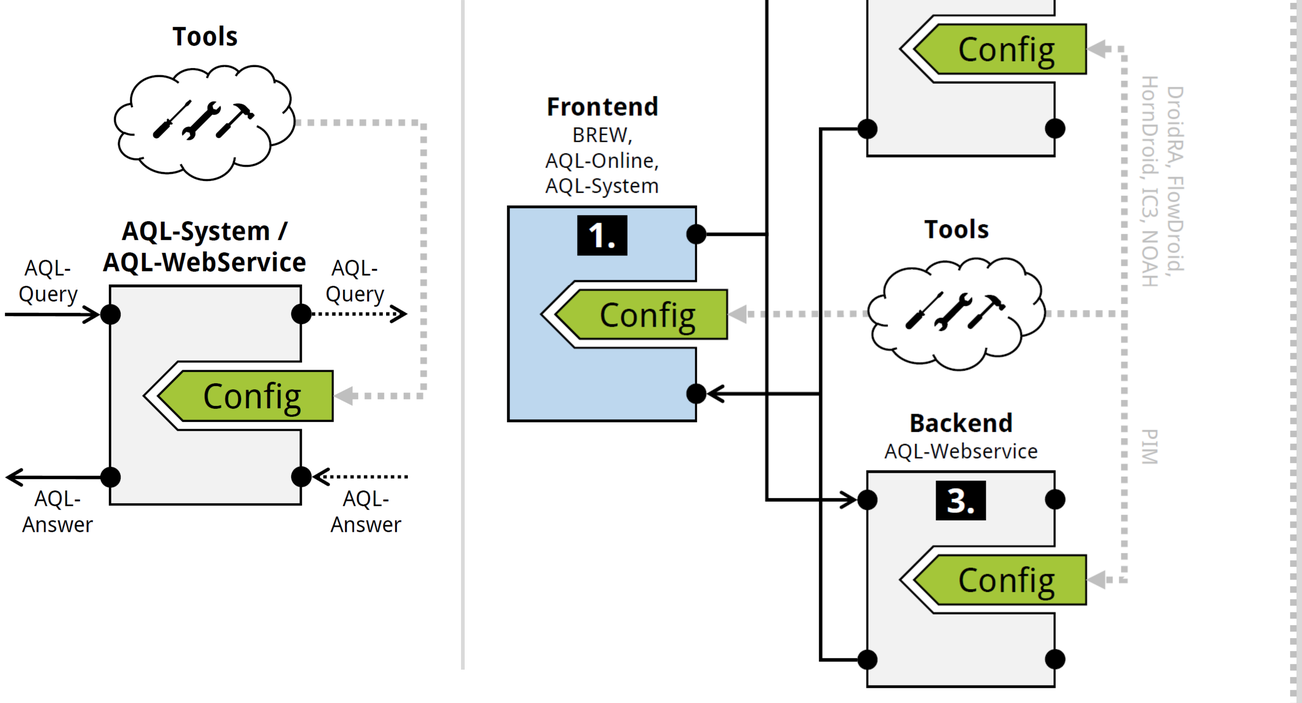
4

reproDroid
Android Benchmark Reproduction Framework



5

CoDiDroid
together strong!



1 Example Overview

Sources: s_1 Taint-Flows: $s_1 \rightarrow s_4$, $s_1 \rightarrow s_7$

Sinks: s_4, s_7

To find both taint-flows (i) sources and sinks in Java and native code must be uncovered, (ii) reflection must be resolved and (iii) inter-app communication has to be analyzed.

2 Example AQL-Query

The simple query gets transformed into a more detailed one considering the challenges of the example.

3 Example AQL-Answer

The web representation shows that both expected taint-flows were identified by the cooperation of DroidRA, FlowDroid, IC3, NOAH and PIM

4 - 5 Usecases:

- ReproDroid: The Android Benchmark Reproduction Framework
- CoDiDroid: Cooperative (and Distributed) App Analysis Tool Framework
- AMT: Android Merge Tool → Benchmark Speed-Up & Analysis Lift-Up
  PHASAR : Philipp's Awesome Static Analysis fRamework

AQL-Publications:

2017: Master's Thesis
ESEC/FSE'18: Do Android Taint Analysis tools keep their promises? *
ESEC/FSE'19: Together Strong: Cooperative Android App Analysis *
???'19: App Merging for Benchmark Speed-Up and Analysis Lift-Up

* Artifacts evaluated / under review

Artifacts Available · Artifacts Evaluated Reusable · Artifacts Evaluated Functional

- Src-Code
- Executables
- Tutorials
- Benchmark Extensions
- Evaluation Results
- …

Felix Pauck fpauck@mail.uni-Paderborn.de http://FelixPauck.de https://FoelliX.github.io