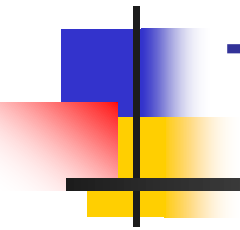
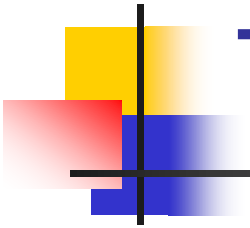


Harden Android Programmers' Toolkit with Symbolic Execution

OWASP Suzhou 2014

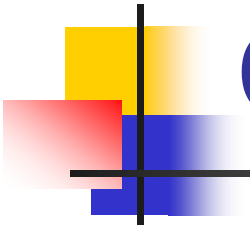
2014.1.21



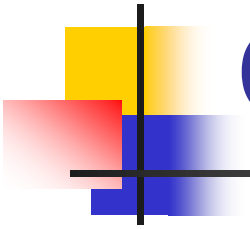
The Problem

- Mobile apps are different from traditional desktop apps
  - Low entry barrier
  - Rapid development
  - Rapid deployment
  - …
- Pressure on industry
  - To guarantee products' correctness and robustness
  - Require better tools (not just a compiler)

Current Research & Tools

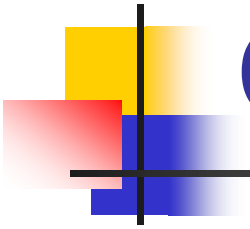


- Develop brand-new tools from scratch
  - Apk-tool, baksmali, ida-pro, debuggers, …
  - “Re-invent the wheels”…
- Leverage existing research…
  - Ded, Dare (DVM-to-JVM), Dexpler (DVM-to-Jimple and Soot), …
  - Partial success



Challenges

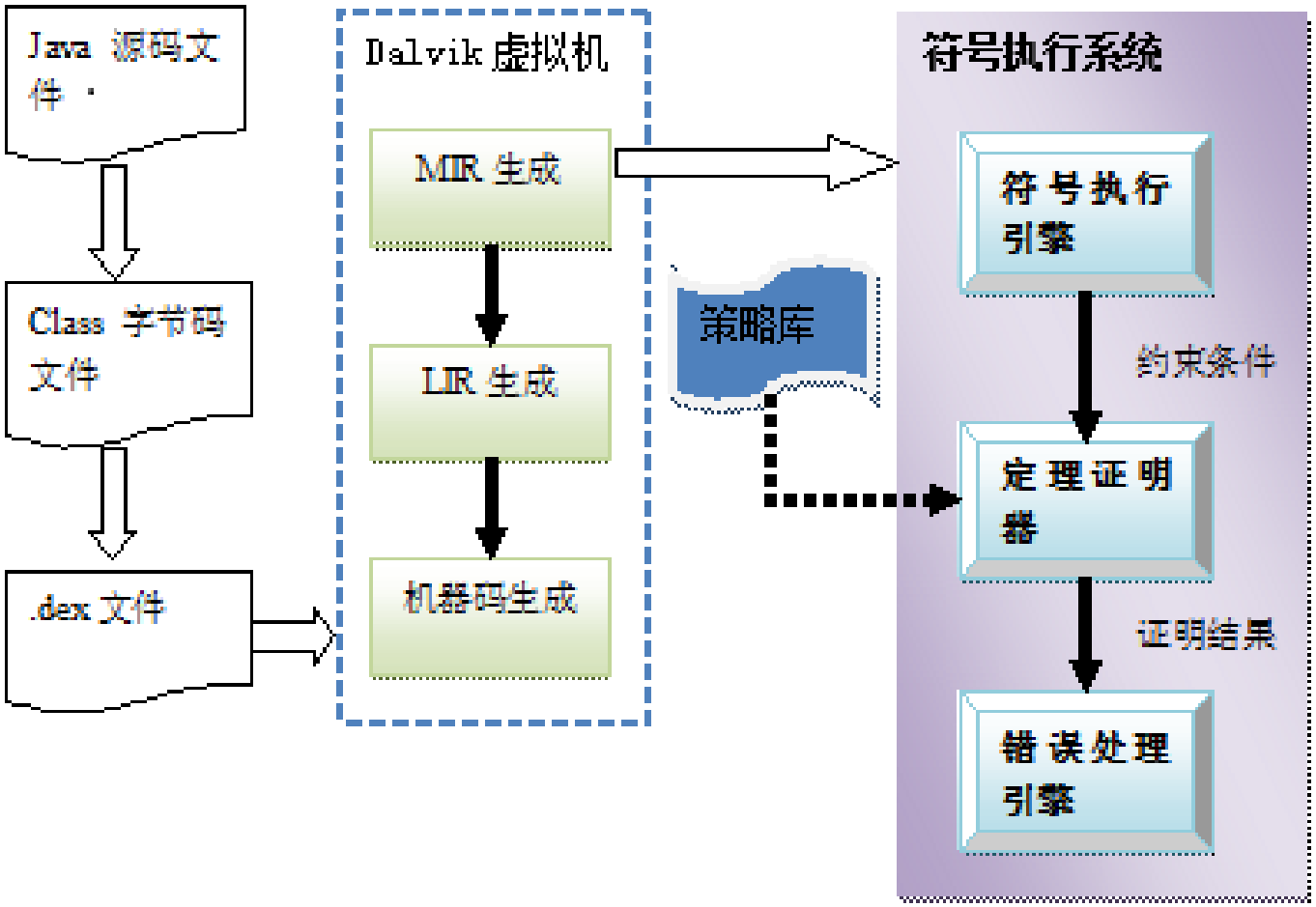
- “New” architectures…
  - Embedded Linux + Dalvik ISA
- New programming models and s.t. stack
  - Android APIs
- Lack common security standard
  - Industry standard?



Our Research Plan

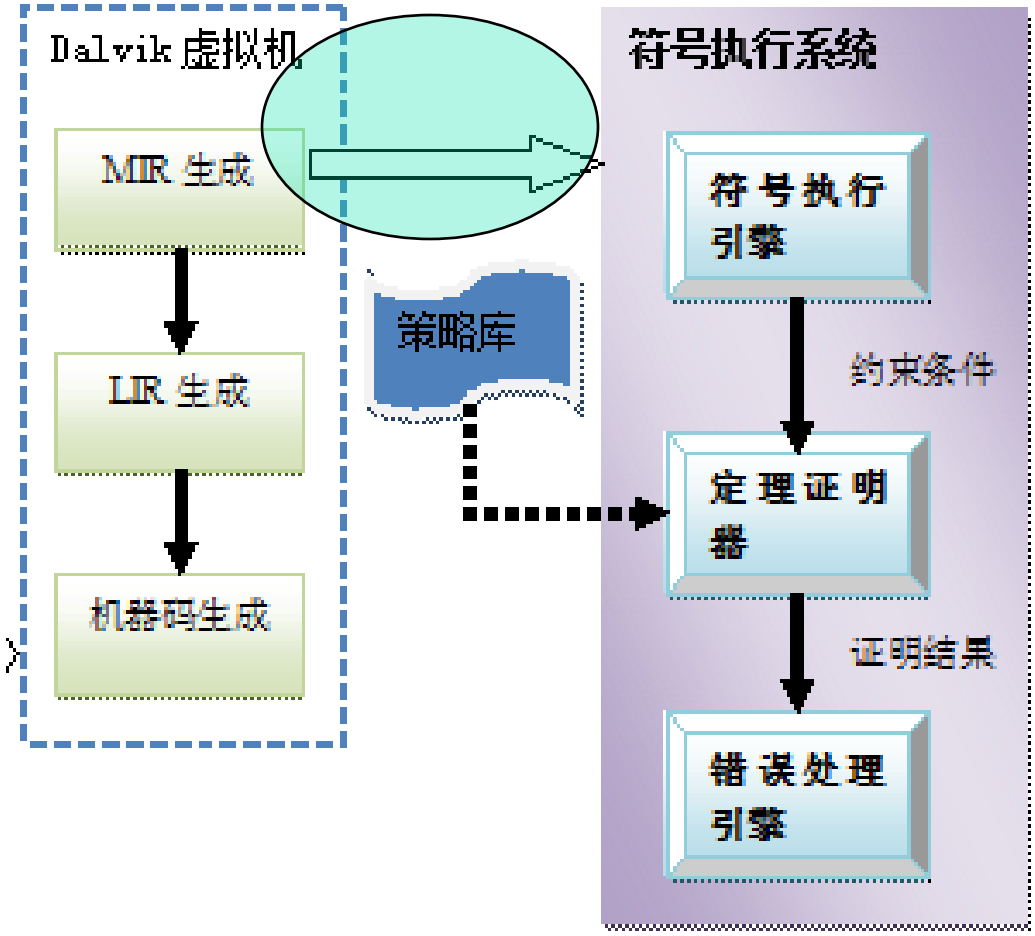
- Build a brand-new security and vulnerability-analysis infrastructure from scratch
  - Both on binary-level (now) and Java (next)
- Techniques: symbolic execution
  - A well-established technique dates back to 70s'
  - Proven to be valuable in many existing systems
    - EXE, KLEE, PLEX, …

The infrastructure



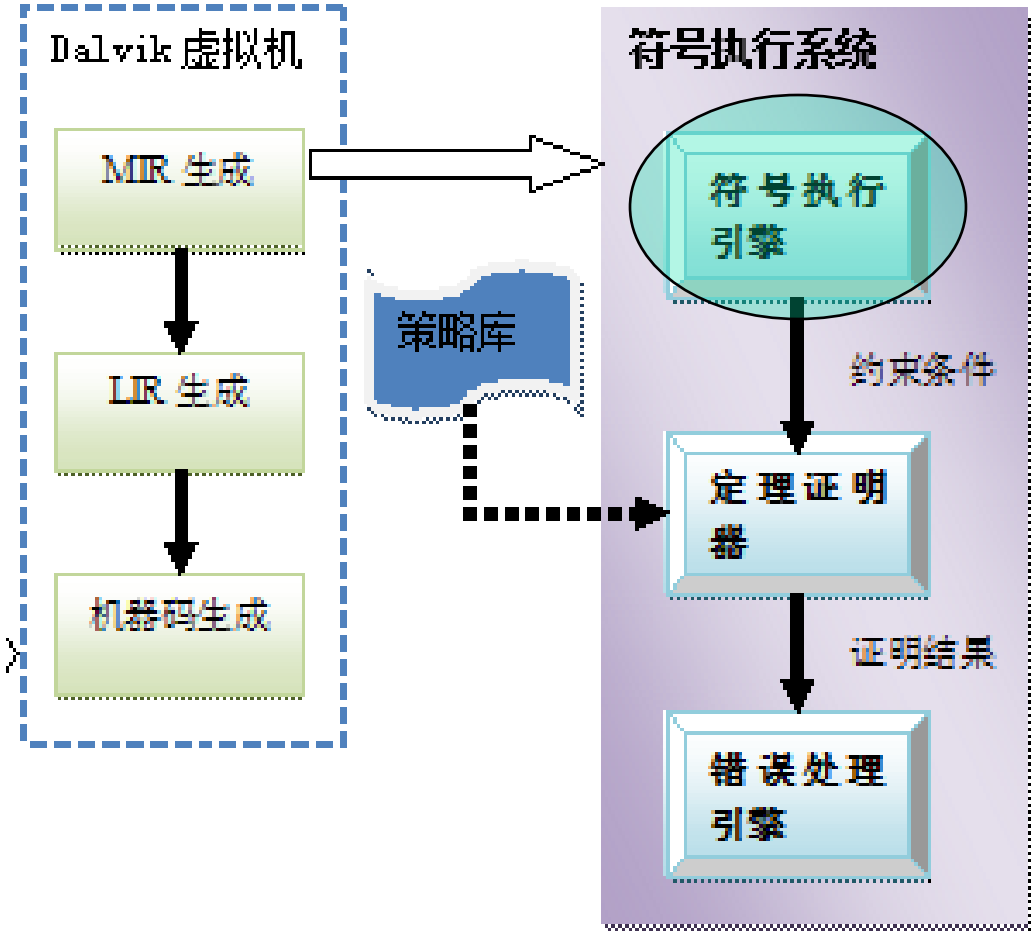
The compiler

- Take as input the raw APKs
- Generate internal IRs
- IRs designed for checking purpose with care



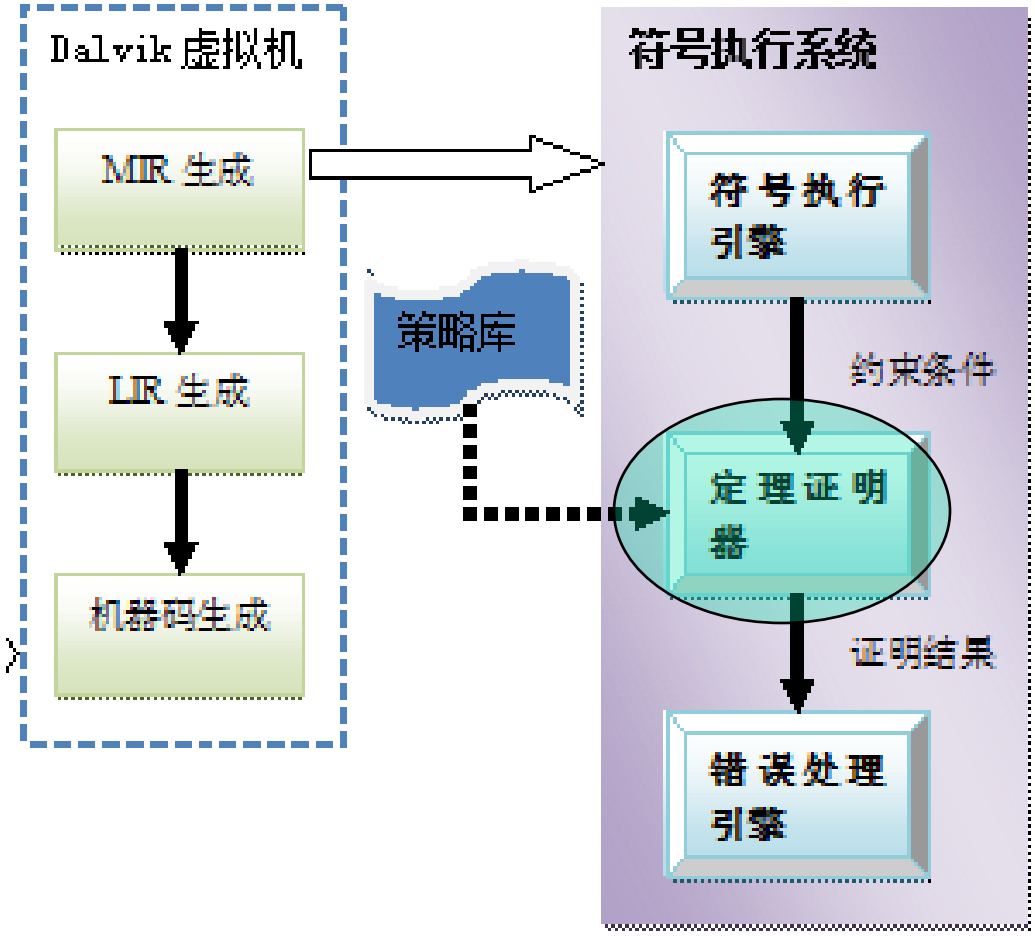
The symbolic executor

- Take as input the IRs
- Generate security constraints (logic theorems)
  - 1st-order logic with special domain theory



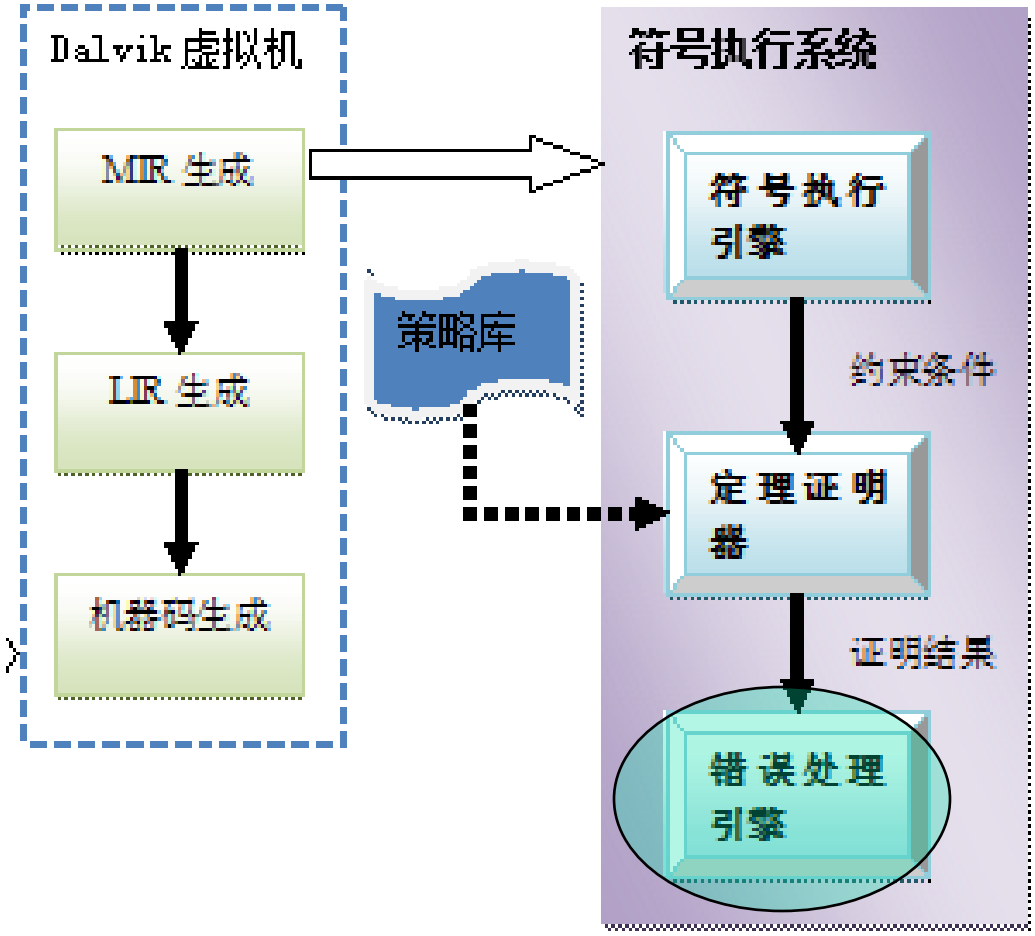
The theorem prover

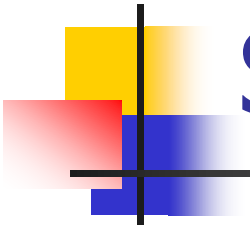
- Take as input the theorems
- Validate it, or generate counter-examples
  - Should be fully automatic



The diagnostic engine

- Feedback to programmers
  - Why are my programs wrong?
- Generate test cases (automatically)
  - Where are bugs?



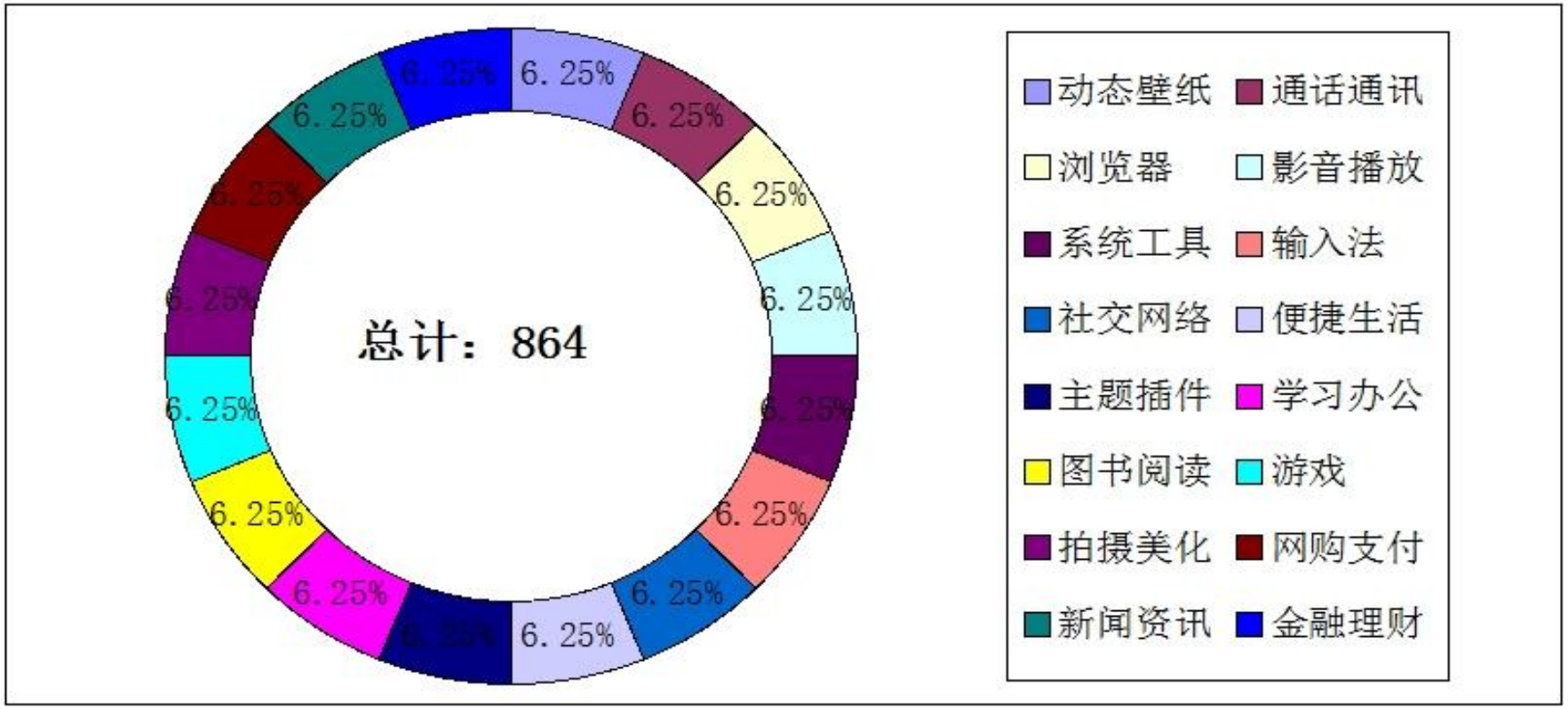


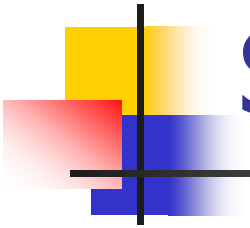
Status

- The project “Carbon”
  - Written in Java
- Compiler finished, other parts are under heavy construction
  - Now ~10K LOC

Initial experiments and experience

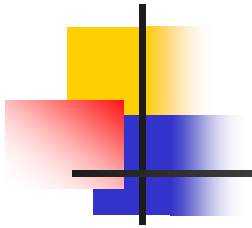
- Benchmarking





Summary

- Build a Android-native security-checking and program testing tools with symbolic execution
- It's profitable to build into the 21st century software security the 19st math. logic



Thanks!

Questions?