An Architecture Style for Android Security.

Bradley Schmerl, Jeffrey Gennari, David Garlan
schmerl@cs.cmu.edu jsg@sei.cmu.edu garlan@cs.cmu.edu
institute for SOFTWARE RESEARCH
Carnegie Mellon University

Problem and Approach

Frameworks need to balance flexibility and security

- Flexibility supports diverse ecosystems
- Security supports safe ecosystems

How can we provide better framework support for enhancing both of these qualities?

- Mix of static and dynamic checks
- Base analysis on architecture models

Domain – Android as framework

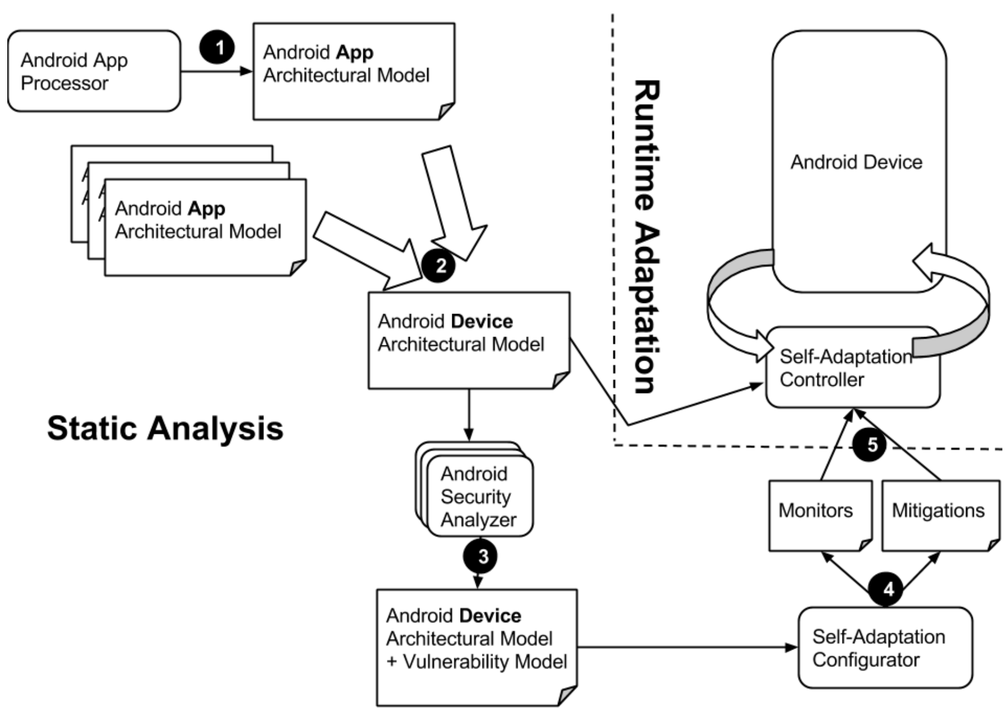
- Intents allow flexible app communication
- Permissions protect resources

However, intents are a source of many vulnerabilities in Android

- Apps can be added/removed at run time so complete static check impossible
- Framework relies on plugins (apps) to check permissions for intents

Many vulnerabilities can be detected statically, but dealing with them all reduces flexibility

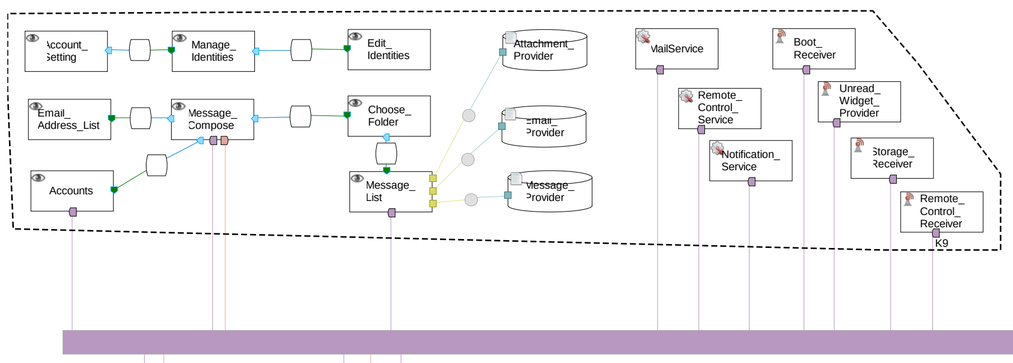
Statically Check Apps, Dynamically Check Android



Approach Detail

❶ Analyze app to produce architecture model. Check correctness.
❷ Combine with models of other apps.
❸ Statically analyze to detect potential vulnerabilities
❹ Use results to focus run-time monitoring
❺ Use self-adaptation techniques to detect run time exploits and mitigate as they are detected

Android Architecture Style



Used for static analysis and dynamic adaptation

- Static analysis can produce model
- Style constraints can check construction-time security, e.g.:
  - Verify permission usage in apps
  - Detect unintended implicit intent targets
- Data-flow and ownership analysis can pinpoint vulnerabilities, annotate model
- Self-adaptation uses architecture model to monitoring intent usage, adapt as necessary

Style Characteristics:

- Separate implicit and explicit intents to separate connectors
- Use groups to represent apps
- Single implicit event bus to make obvious global communication
- Permissions, intent filters, etc. represented as properties in the model

http://hot-sos.org/

The Science of Security initiative is funded by the National Security Agency.