NESSOS ESSoS 14
Engineering Secure Software and Systems

PhD Symposium

# An Authorization Framework For App Security Checking

Photo by Johan Larsson


## SUMMARY

Apps do not come with guarantees they are not malicious—just promises from stores that they have checked them and that they don't think they are malware. The *App Guarden* project will create a new kind of app store where apps come with *digital evidence* to make explicit why an app isn't dangerous. Users can describe with an *authorization language* how apps should behave and the phone can enforce this policy with the evidence from the store.


## PROBLEM

- Users have to trust the app stores
- The trust is misplaced!
  - Malware found on app stores
  - Developers make poor security decisions
- We want to fix this:
  - Apps come with digital evidence
  - Users say how their apps should behave

## DEVICE POLICY

- A User says:
  *"I'll only install apps if they don't leak my personal information and Google says they are not malware"*
- Using the SecPAL language this becomes:

**User** says *app* is-installable if
*app* meets(**NoInfoLeaks**),
*app* meets(**NotMalware**).

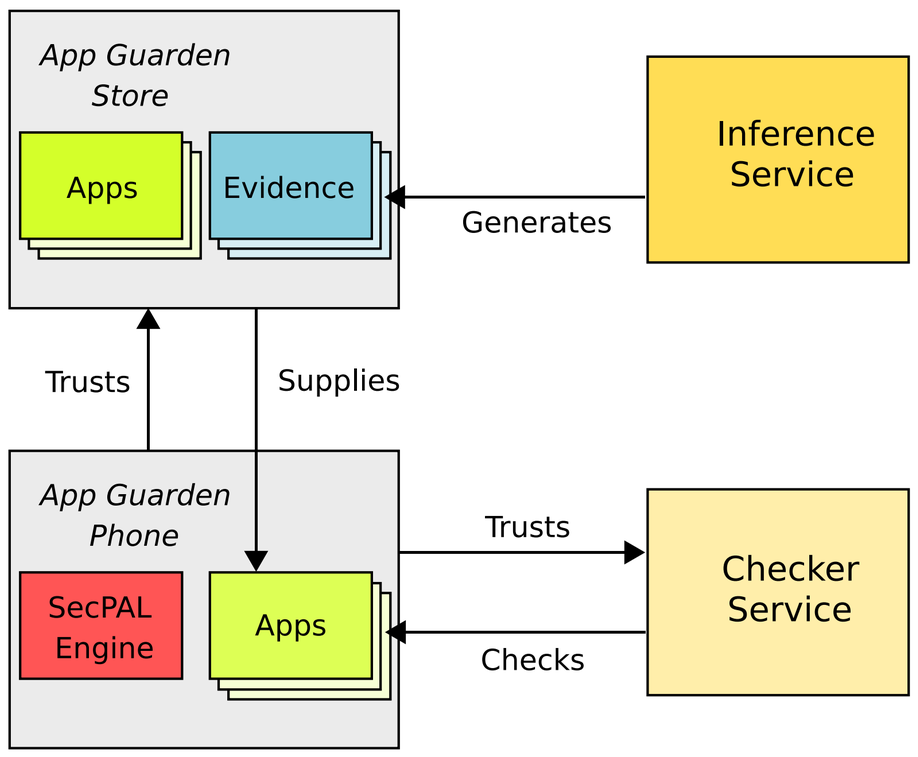
**User** says **Google** can-say$_\infty$ *app* meets(**NotMalware**).

**User** says **NILChecker** can-say$_0$ *app* meets(**NoInfoLeaks**).

## STATUS AND FUTURE WORK

- Early stage project
  - Started porting SecPAL
  - Exploring the device policies users have.
- We want to evaluate these policies:
  - How good are they at stopping malware?
  - Can they replace authorization pop-ups?
- Can we use SecPAL to compare policies?
  - Can we describe the differences between an iPhone, Android and Blackberry?

## THE APP GUARDEN





THE UNIVERSITY of EDINBURGH
informatics

**Joseph Hallett**
**David Aspinall**

http://groups.inf.ed.ac.uk/security/appguarden/Home.html