An Authorization Framework For App Security Checking

Joseph Hallett
J.Hallett@sms.ed.ac.uk

THE UNIVERSITY *of* EDINBURGH
informatics

What I’m Going To Say

- The problem with app stores
- App Guarden
- Device policies and SecPAL
- Using SecPAL to compare

App Stores

Apple and Google vet apps for sale

…but both their stores sell malware

App Stores

Neither say what they check for

…or how they check for it

…or how thoroughly

We can do better than this!

App Guarden

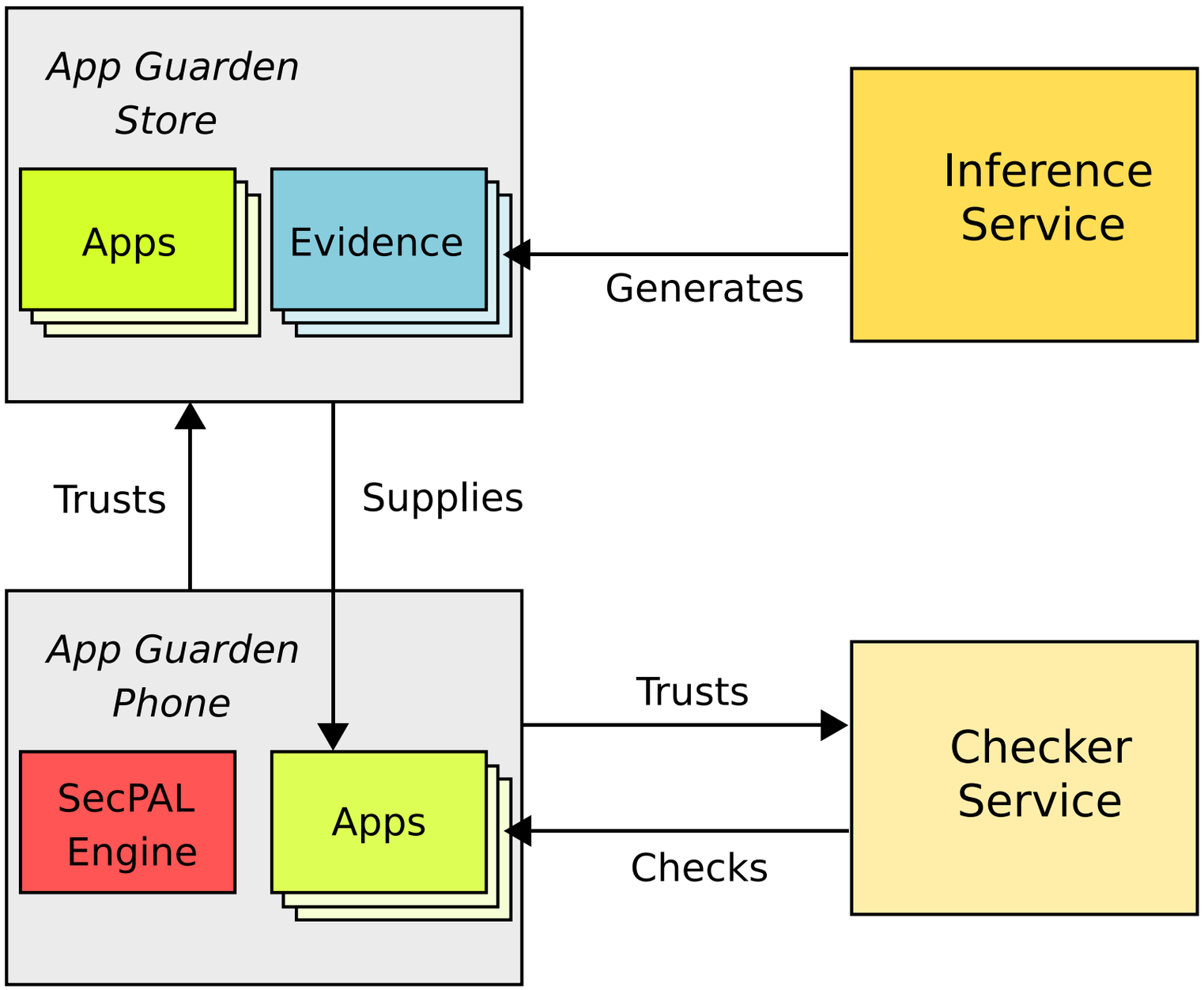
Apps with *digital evidence*

Device policies say what apps should be installed
App policies say how an app should run

Digital evidence is a checkable proof that a program meets an app policy.

Can be more efficient to check the proof than to generate it

App Guarden


App Guarden
Store
Apps
Evidence
Inference
Service
Generates
Trusts
Supplies
App Guarden
Phone
SecPAL
Engine
Apps
Trusts
Checker
Service
Checks

Device Policies

“I’ll only install an app if it doesn’t leak my personal data and Google says it isn’t malware.”

SecPAL

Security **P**olicy **A**uthorization **L**anguage

Designed to be readable

Decentralized authorization policies

$$\frac{AC,\infty \vdash A \text{ says } B \text{ can-say}_D \text{ fact} \qquad AC,D \vdash B \text{ says fact}}{AC,\infty \vdash A \text{ says fact}} \text{(can say)}$$

$$\frac{(A \text{ says fact if } fact_1,\ldots,fact_k,c) \in AC \qquad AC,D \vdash A \text{ says } fact_i\theta\ (\forall\, i \in \{1\ldots k\}) \qquad \vdash c\theta \qquad vars(fact\theta) = \varnothing}{AC,\infty \vdash A \text{ says } fact\theta} \text{(cond)}$$

Device Policies

“I’ll only install an app if it doesn’t leak my personal data and Google says it isn’t malware.”

User says *app* is-installable if
app meets **NoDataLeaks**,
app meets **NotMalware**.

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

Device Policies

*"**I'll only install an app if** it doesn't leak my personal data and Google says it isn't malware."*

User says *app* is-installable if
app meets **NoDataLeaks**,
app meets **NotMalware**.

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

Device Policies

"I'll only install an app ***if it doesn't leak my personal data and*** *Google says* ***it isn't malware.****"*

User says *app* is-installable if
app meets **NoDataLeaks**,
app meets **NotMalware**.

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

Device Policies

"I'll only install an app if it doesn't leak my personal data and ***Google says it isn't malware.****"*

User says *app* is-installable if
app meets **NoDataLeaks**,
app meets **NotMalware**.

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

Can Construct Proof

User says *app* is-installable if
app meets **NoDataLeaks**,
app meets **NotMalware**.

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

User says **NDLInferer** can-say$_0$
app meets **NoDataLeaks**.

anyone says *app* meets *policy*
if *e* shows *app* meets, *policy*.

Google says **McAffee** can-say$_0$
app meets **NotMalware**.

McAffee says
AngryBirds meets **NotMalware**.

NDLInferer says
E shows **AngryBirds**
meets **NoDataLeaks** if
NDLChecker(**E**, **Game**) = True.

Digital Evidence

User says *app* is-installable if
app meets **NoDataLeaks**,
app meets **NotMalware**.

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

User says **NDLInferer** can-say$_0$
app meets **NoDataLeaks**.

anyone says *app* meets *policy*
if *e* shows *app* meets, *policy*.

Google says **McAffee** can-say$_0$
app meets **NotMalware**.

McAffee says
AngryBirds meets **NotMalware**.

NDLInferer says
E shows **AngryBirds**
meets **NoDataLeaks** if
NDLChecker(**E**, **Game**) = True.

Delegation

User says *app* is-installable if
app meets **NoDataLeaks**,
app meets **NotMalware**.

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

User says **NDLInferer** can-say$_0$
app meets **NoDataLeaks**.

anyone says *app* meets *policy*
if *e* shows *app* meets, *policy*.

Google says **McAffee** can-say$_0$
app meets **NotMalware**.

McAffee says
AngryBirds meets **NotMalware**.

NDLInferer says
E shows **AngryBirds**
meets **NoDataLeaks** if
NDLChecker(**E**, **Game**) = True.

Make Comparisons

iPhone says **Apple** can-say$_\infty$
app is-installable.

Android says **User** can-say$_\infty$
app is-installable.

User says **Google** can-say$_0$
app is-installable.

iPhone says **User** can-say$_0$
app can-access *resource*.

Android says
app can-access *resource* if
app is-installable,
app requires *resource*.

Related Work

- G.C. Necula and P. Lee. *Proof-Carrying Code*
- N. Whitehead, M. Abadi, and G. Necula. *By reason and authority: a system for authorization of proof-carrying code*
- G. Barthe, L. Beringer, P. Crégut, B. Grégoire, M. Hofmann, P. Müller, E. Poll, G. Puebla, I. Stark, and Eric Vétillard. *MOBIUS: Mobility, Ubiquity, Security*
- M.Y. Becker, C. Fournet, and A.D. Gordon. *SecPAL: Design and semantics of a decentralized authorization language*
- M. Abadi. *Logic in access control*
- W. Enck and P. McDaniel. *Not So Great Expectations.*
- J. Oberheide and C. Miller. *Dissecting the android bouncer*

Conclusion

- App stores are rubbish
- App Guarden is an improvement
- Device policies let users say how they want their devices to behave
- SecPAL can be used to write and compare policies