What I have been doing

Recap

- Apps with ~~proof carrying code~~ digital evidence

- Device policies
  — What must an app show to be runnable?
  “No app should leak my address book”

- App policies
  — How should the app run?
  “Cannot access address book APIs”

What I have been doing

Device Policies

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

SecPAL

Authorization language

Designed to be readable

Evaluation rules

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

$$\frac{\begin{array}{l}(A \text{ says fact if fact}_1,\ldots,\text{fact}_k,c) \in AC \\ AC,D \Vdash A \text{ says fact}_i\theta \ (\forall\ i\in\{1\ldots k\}) \qquad \Vdash c\theta \qquad \text{vars}(\text{fact}\theta) = \varnothing\end{array}}{AC,\infty \Vdash A \text{ says fact}\theta} \text{(cond)}$$

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*.