Using Authorization Logic to Capture User Policies in Mobile Ecosystems

People fall into patterns when thinking about the privacy implications of apps. By capturing these patterns explicitily as policies we can enforce them automatically using the AppPAL authorization logic. Users have opinions about the privacy implications of apps but do they follow them when picking which apps to install?

Using data app installation data from 44,000 users we find that very few users seem to be able to follow these policies consistently when installing apps on their devices. Those that did seem to follow policies seemed to pick better apps generally avoiding PUPs (potentially unwanted programs) and other malware.

AppPAL and Policies for App Installs

AppPAL describes policies specifying when an app is installable. Statements are relative to specific principals, enabling delegation relationships to be expressed. Delegation is natural in the app store setting: it captures trust relationships among the users, the stores, the developers, and security vendors who vet apps.

Alice, a user, can say an app is installable:

```
alice says com.rovio.angrybirds isInstallable.
```

She can introduce conditions and delegation relationships:

```
alice says App isInstallable
  if not-malware-policy isMetBy(App)
  where hasPermission(App, LOCATION) = false.
alice says mcafee can-say
  not-malware-policy isMetBy(App).
```

In a user study of 725 Android users, *Lin et al.* found four patterns that characterise user privacy preferences for apps *(Modelling Users' Mobile App Privacy Preferences: J. Lin, B. Liu, N. Sadeh, & JI. Hong, (2014). SOUPS 2014).*

	C	A	F	U
GET_ACCOUNTS	✘	✘	✘	✘
ACCESS_FINE_LOCATION	✘	✘	✘	
READ_CONTACT	✘	✘	✘	
READ_PHONE_STATE	✘	✘		
SEND_SMS	✘	✘		
ACCESS_COARSE_LOCATION	✘			

We wrote AppPAL policies to describe each of these behaviours as increasing sets of permissions. These simplify the policies; but AppPAL constraints can describe richer policies than permission sets.

Security vendors (like McAfee) classify malware by their behaviour. While some malware tries to steal personal data, or send expensive text messages; others drain the battery, spam notifications or do other *potentially unwanted* actions. This kind of malware is called *PUP.*

We write AppPAL policies to differentiate different kinds of malware, characterising users who have installed trojans from those who install PUPs.

```
user says mcafee can-say malware isKindOf(App).
mcafee says trojan can-act-as malware.
mcafee says pup can-act-as malware.
```

Do Users Follow These Policies?

We found:

- Most users seem to use apps despite how uncomfortable they are with the permissions they request.
- Some users do seem to enforce these policies most of the time.
- But most do not.

Looking at malware and PUP installs:

- 1% of the users had an app McAfee said was a PUP or other malware
- A user is 3 times more likely to have a PUP installed than malware.
- 9 users had both a PUP and malware installed.

To answer whether following a policy reduced malware infection rates:

- Users who had ≥50% compliance with the conservative or advanced policies did not install malware or PUPs.
- Relationship between policies conformance and malware installs is statistically significant (p-value < 0.05).

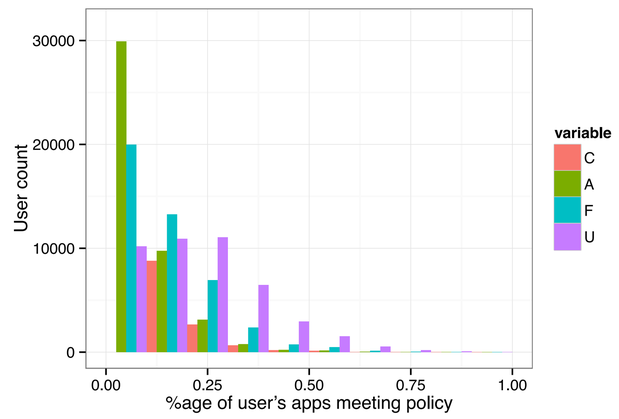
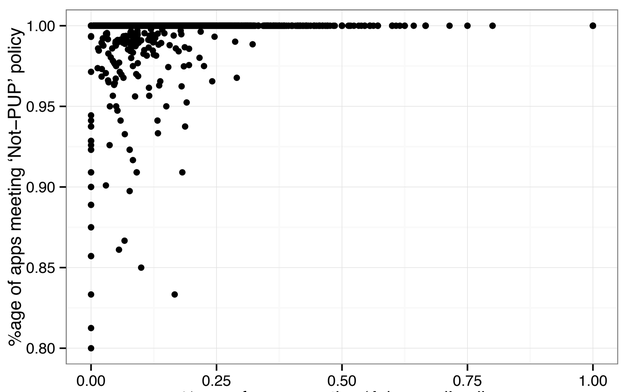
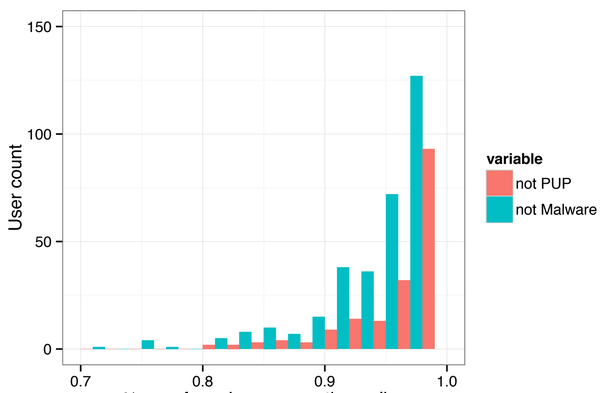


Table: *Numbers of users enforcing a policy.*

	C	A	F	U
≥ 50%	179 *(0.41%)*	206 *(0.47%)*	696 *(1.58%)*	2390 *(5.43%)*
≥ 60%	45 *(0.10%)*	49 *(0.11%)*	209 *(0.48%)*	867 *(2.0%)*
≥ 70%	18 *(0.04%)*	19 *(0.04%)*	79 *(0.18%)*	331 *(0.75%)*
≥ 80%	15 *(0.03%)*	16 *(0.04%)*	49 *(0.11%)*	151 *(0.34%)*
≥ 90%	13 *(0.03%)*	14 *(0.03%)*	37 *(0.08%)*	69 *(0.16%)*
= 100%	13 *(0.03%)*	14 *(0.03%)*	37 *(0.08%)*	67 *(0.15%)*





Experiments

We want to understand:

- How well do these policies capture actual user behaviour?
- To what extent malware is present on Android compared to PUPs?
- Do users who follow policies install less malware?

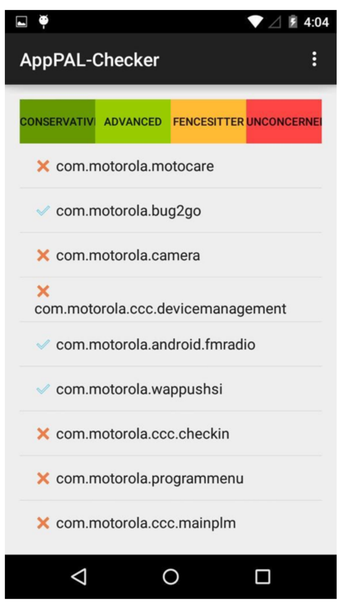
The *Carat* dataset (*Carat: Collaborative energy diagnosis for mobile devices. AJ. Oliner, AP. Iyer, I. Stoica, & E. Lagerspetz. ENSS 2013*) has anonymised records of what users installed. We were able to identify around 4,300 apps of the 90,000 present in the dataset. We selected 44,000 users for whom we knew at least 20 installed apps.

We checked:

- Which apps met which policies.
- What percentage of each user's apps met each of the policies.
- The percentage of a user's apps meeting the policy measured the users conformance to a policy.

User	com.rovio. angrybirds	?	com.facebook. katana	…
1	✘	✔	✔	
2	✔	✘	✔	
⋮				⋱

Future Work



There appears to be a disconnect between how users feel about permissions and how they act. Next steps include:

- Mining categories and policies describing how users pick apps from app installation data.
- Using AppPAL to model the policies and enforcing them automatically through nudging and tailored app stores.
- Extending AppPAL to support richer policies and constraints, as well as new methods of enforcement.

Exploring the disconnect between user's policies and behaviour is another research area. We would also like to:

- Work with users to find policies that describe how they think and want apps to behave.
- Actively query users when they make decisions that go against their policies.

THE UNIVERSITY of EDINBURGH

Joseph Hallett
David Aspinall (supervisor)