Context-Aware Privacy Management on Smartphones

Saksham Chitkara, Nishad Gothoskar, Suhas Harish, Jason I. Hong, Yuvraj Agarwal

E-Mail: schitkar@andrew.cmu.edu, yuvraj@cs.cmu.edu

PrivacyCon – Feb 2018
Smartphones: Ensuring User Privacy

Changed landscape: Smartphones and “Apps”
- >1.4M Apps, 100 Billion downloads, >100K developers
Concerns: untrusted, inexperienced developers
- Financial models unclear – Free Apps, Ad support
Result: Mobile Apps access your private data
- May be for valid reasons, or for no clear utility?
Decision overload:

- 80 Apps * ~5 Permissions => 400 Decisions

Purpose of data access is still unclear

- “Why” is the data accessed, “where” does it flow?

Android privacy controls are still at an App level

- Developers routinely use 3rd Party Libraries
- Cannot currently allow access based on functionality
- These libraries have access to the same user data
Decision (further) overload?
- **App x Permissions x Purpose** (multiple libraries?)
- User attention is scarce

- Sounds like we might make things even worse…. 

- Question: What are these 3rd party libraries?
  - Is there something that we can leverage?
Private Data Accesses by 3\textsuperscript{rd} party Libraries

- Collected "stack-trace" data
- Shows context around privacy sensitive data accesses
- Categorized accesses by the App itself or some 3\textsuperscript{rd} party lib

Insight #1: 3rd Party Libraries are responsible for a large fraction of the accesses in popular Apps.
Understanding 3rd Party Library Data Accesses

Insight #2: Use of libraries in apps is heavy tailed
Insight #3: A small set of libraries account for many privacy sensitive data accesses
App+Library Based Controls

{App, permission} + {Library, permission}
- Separate out data flows between app and library

What about the purpose?
- Third-party libraries have specific use cases

Use crowd-sourcing to scale data collection
- Users upload App stack traces, need at least one
- Multiple users can upload different stack traces
PmP v2: App Screenshots

4:53 AM
Tuesday, April 25

PMP needs your Decision
TapJoy - a 3rd party service used by:
- Subway Surf
- Talking Angela

want to access your Phone Unique ID

ALLOW DENY FAKE

5:52 AM
Tuesday, May 9

PMP Advisory
Unity Ads being used by:
- Talking Angela
- Temple Run 2
- 8 Ball Pool

want to access your Phone Unique ID. PMP will continue to use your previous decision: Fake, for all future requests from Unity Ads. This setting can be modified from within PMP.

4:53 AM
Tuesday, April 25

ProtectMyPrivacy

MY APPS SYSTEM APPS LIBRARIES

Third party libraries which collect personally identifiable information. Decisions here do not affect the rest of the application.

AdMob (used by 4 apps)

AppsFlyer (used by 2 apps)

Flurry (used by 2 apps)

TapJoy (used by 2 apps)

Vungle (used by 2 apps)

Fabric (used by 2 apps)

Other Libraries

Millenial Media

The purpose of the data is Targeted Ads.

Millenial Media is being used by the following 1 apps:

Phone Unique ID
Deny

FINE GRAINED LOCATION
Fake

RESET APP PERMISSIONS TO "ASK"
Results: Reduced Number of Decisions

1300+ real world users who discovered our

- 90 Decisions
- About 18 Apps
  - 5 permissions
Results: Effectiveness Against Data Leaks

- Data flowing to 3rd party libraries is reduced
  - On average 25% more users protected
- Users are better protected in all cases
## Results: Changes in User’s Decisions

- Overall users block more decisions
  - Both for “Native” as well as “Library” accesses

<table>
<thead>
<tr>
<th>Features</th>
<th>Percent of accesses blocked</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Features</td>
<td>40, 52, 75</td>
</tr>
<tr>
<td>Phone Unique Id</td>
<td>47, 59, 76</td>
</tr>
<tr>
<td>Location</td>
<td>39, 45, 78</td>
</tr>
</tbody>
</table>

Legend:
- **App-only controls**
- **App+Library controls on native accesses**
- **App+Library controls on third party libraries**
Results: Why do users make these decisions?

Why do users allow **ANY** data to libraries? Gather In-App feedback for libraries, use ESM.
Results from User Feedback

Results for Allowing Library Access

- 25% of all accesses by Libraries were allowed
  - 74.7%
  - 16.9%
  - 3.9%
  - 4.5%

Results for Denying Library Access

- 75% of all accesses by Libraries were blocked
  - 43.6%
  - 31.0%
  - 22.7%
  - 2.7%

Legend:
- I allowed data sharing for functionality
- I'm okay with sharing this private data
- Sharing data supports free apps
- I don't trust this library
- I'm not okay with sharing this specific data
- I don't want to share any data
- No response
Conclusion

ProtectMyPrivacy for Android
- Context driven privacy controls => App, Libraries
- Annotate purposes for private data accesses
- Built an PmP App + crowdsourcing based backend

Evaluate on 1300+ users, 11K Popular Apps
- 25% fewer decisions in App+Library model
- Users are more effectively protected against libraries
- Users more likely to share data for native App access
Thank you!

:: Systems, Security, Privacy
:: Domain: IoT / Mobile / Buildings

Others contributing to this research:
Edison Gao, Vikram Shanker, David Simon, Joseph Chan
Sandeep Agarwal, Kunal Bhuwalka, Dohyun Kim, ....!