Follow My Recommendations: A Personalized Privacy Assistant for Mobile Apps

Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Zhang, Norman Sadeh, Alessandro Acquisti, Yuvraj Agarwal

Carnegie Mellon University





1

Android Permissions: Better Control, More Burden?





Android Permissions: Better Control, More Burden?

Trip t White Empi build Brool Activity Goma	• • • • • • • • • • • • • • • • • • •	Too many settings to manage!	
Le Go Jou Bee Hhat con	Microphone Google Pinyin Input Google Play services	•	On average:
C(What's ban	8+ Google+		95 apps per u 5 permissions
	Keep Messenger		And
4	Phone Photos		there will be n
\$	Sound Search for Google Play		Health data, Smart home, Internet of Th
	< 0 □		

ge! n average: 5 apps per user permissions per app

ere will be more…

ealth data, mart home, ternet of Things,...

Helping User Configure Their Permission Settings: Recommendations

- Recommendations of permission settings
 - Majority Choice [Agarwal et al. MobiSys 2013]
 - Expert labeling [Rashidi et al. IM 2015]
 - One-size-fits-all solutions

- Users' preferences are **diverse**
 - [Liu et al. WWW 2014]
 - One-size-fits-all recommendations are limited

Personalized Recommendations

- We can learn users' privacy preferences and help users configure many of their settings
 - [Liu et al. WWW 2014, Lin et al. SOUPS 2014]

Personalized Privacy Assistant (PPA) to help real users
In this paper we built such an assistant

Outline: Personalized Privacy Assistant (PPA)

- Capturing Users' Preferences, Building Privacy Profiles
 - 84 participants, 2 weeks
- Generating Profile-based Recommendations for Users
- Field Study: Evaluation of PPA with real Android Users
 - 72 (different) participants, 9 days



Capturing Users' Preferences: Building Privacy Profiles



Collecting Data: Real Android Users

- We want to collect settings from **real** Android users using their phones as part of their regular everyday life.
 - Tradeoffs:
 - Privacy Paradox
 - Self-reported preferences V.S. actual settings
 - The settings should have to have real impact on their apps and their data.
- We built a permission manager of our own, and ran a field study with rooted Android users

Collecting Data: Better Engagement

- By default users are not actively engaging in permission settings
 - [Liu et al. WWW 2014]

- Privacy nudges can help motivate users to review their settings
 - [Almuhimedi et al. CHI 2015]
 - Paying more attention
 - Better awareness

PPA App: Enhanced Permission Manager Awareness + Engagement



PPA App: Enhanced Permission Manager Awareness + Engagement



Dataset Collection

- We got 84 rooted Android users finished the study
 - We recruit from online communities where we can better reach rooted users: Google+, Facebook, Reddit, Android forums.

- Two-week data collection
 - Starting from week 2, the PPA app showed privacy nudges once a day

Dataset Statistics

- 3559 Permission Settings
 - App ran in foreground or got configured by user
 - (Android K & L by default allow the permissions)

- 2888(81.15%) allows and 671(18.85%) denies.
 - Significant factors: (random-effect logistics regression)
 - App Categories
 - Permissions
 - **Purpose** information
 - Importance reported by participants
 - But not frequently available to all the apps

Building Privacy Profiles: Group Like-minded Users

• Quantifying a user's preference:

 Aggregated general preference on each specific triple (app category, permission, purpose)

Based on logistic regression analysis

 Apply weighted tensor factorization to impute the missing values (optimize only on known settings)

Building Privacy Profiles

• Clustering Algorithm

• Hierarchical Clustering

- Performs good on unbalanced data
- Adjustable with non-triangle distance metrics

- K=7, complete linkage, cosine distance
- Silhouette Coefficient=0.2079

Building Privacy Profiles



Generating Profile-based Recommendations for Users



Capturing Users' Preferences: Interactive Dialog to Assign Them to Profiles

For each new user, the PPA app ask up to 5 questions to capture the user's preference. These TRAVEL & LOCAL apps accessed your LOCATION 102 TIMES over the past 2 days: Maps GasBuddy San Francisco Yelp GrubHub (::)Waze In general, are you OK with TRAVEL & LOCAL apps accessing your LOCATION? YES NO

Capturing Users' Preferences: Interactive Dialog to Assign Them to Profiles

For each new user, the PPA app ask up to 5 questions to capture the user's preference.

Types of questions:

- (category, permission)
- (permission, purpose)
- (permission)

These TRAVEL & LOCAL apps accessed your LOCATION 102 TIMES over the past 2 days:				
	Maps GasBuddy San Francisco Yelp GrubHub Waze			
In general, are you OK with TRAVEL & LOCAL apps accessing your LOCATION ?				
	YES			
NO				

Capturing Users' Preferences: Interactive Dialog to Assign Them to Profiles

For each new user, the PPA app ask up to 5 questions to capture the user's preference.

- Types of questions:
 - (category, permission) -> allow/deny
 - (permission) -> allow/deny
 - (permission, purpose) -> allow/deny

Context-specific:

 the questions are chosen by optimizing a decision tree dynamically according to what apps are installed on users' device. These TRAVEL & LOCAL apps accessed your LOCATION 102 TIMES over the past 2 days: Maps GasBuddy San Francisco Yelp GrubHub (::) Waze In general, are you OK with TRAVEL & LOCAL apps accessing your LOCATION? YES NO

Generate Recommendations

• The recommendation task can be formalized as a classification problem

• F: (user, app, permission) -> {allow / deny}

- We train a SVM classifier that takes the following features into consideration:
 - Profile membership, App category, Permission
 - Purpose(s) of the permission request
- Only the recommended "denies" are shown to the user (Android K & L)
- Model optimized on the collected dataset using 10-fold cross validation

Showing Recommendations

Thank you! Based on your answers, we recommend restricting the following 11 app(s):

Click category to view/change recommendations



Do you want to make these changes?

YES, DENY THE 8 APP(S) SELECTED

NO, DO NOT MAKE ANY CHANGES

Revise

 User can revise the recommendations and adjust them to match their preferences.



Showing Recommendations

Thank you! Based on your answers, we recommend restricting the following 11 app(s):

Click category to view/change recommendations



Do you want to make these changes?

YES, DENY THE 8 APP(S) SELECTED

NO, DO NOT MAKE ANY CHANGES

Explanations

 User can click "?" to check the explanations of each recommendation.

Snapchat (84 times)

?	Denv
	Deny

Why deny? This Social app accesses your Location for App Functionality and Consumer Tracking & Profiling.

Field Study: Evaluation of PPA



Field Study: Evaluation of PPA

In this study, we would like know:

- Do users **accept** our recommendations?
- Do there find the recommendations **useful**?
- In addition, do they keep our recommendations and feel comfortable with them?
- Do our privacy profiles model their preference **accurately**?

Field Study: Evaluation of PPA



• We used Experience Sampling Method and Exit Survey to capture their satisfaction and feedback

- 27 participants of 43 in treatment group are shown recommendations
- Majority of the **recommendations were accepted**
 - 196 of 249 recommended items (78.7%)



- Majority of the **recommendations were accepted**
 - 196 of 249 recommended items (78.7%)



- Participants kept most of the accepted recommendations
 - During the remaining 6 days after they are shown recommendations, we continue to show daily privacy nudges. Only 10 of the previously accepted recommendation (5.10%) were changed back to allow.

- Recommendations helped users **converge** more quickly
 - Permission Denies: the earlier, the better!
 - The treatment group finished 82.51% of their settings in the day when they are shown recommendation, significantly more than 68.42% of control group.



 Most of the participants remained in the same profile they were assigned to. (35/49)

- Participants are **comfortable** with the recommendations.
- Recommendations are helpful

"It made what would have **taken 10-20 clicks** through menus looking to change these settings **done in one click**."

"It provides you with recommendations **using your preferences** so you can quickly change the settings without having to do much yourself."

Limitations

- Sample **population**
 - In this study: Young, male, tech-savvy
 - Our methodology and results would extend to a more general population.
- Relatively short **time length** of the study
 - Daily privacy nudges are effective
 - Longer studies might be interesting to see how users' preferences change over time

Existing Permissions Are Not Expressive Enough

- App behavior affects users' choices
 - Some apps need some permissions to function.
 - Some permissions are used for multiple purposes.

"I want to use a feature of the app that requires this permission"

- Resource-centric control => Purpose-centric control
 - "I want to allow location only for navigation"
 - "I want to deny contact access to third-parties"

Other Considerations

- Degree of **automation** to permission settings configuration
 - Many different possible modes of interaction with the user - varying degrees of automation

• Better **awareness**

- Frequency and purpose information are useful
- Possible Improvement: Tell users how privacy and app functionality would be affected by permission change
- PPA could be applied to support privacy decision making in other domains as well
 - Web browser, Internet of Things, etc.

Summary

Personalized Privacy Assistant

- Privacy Profiles
- Interactive Profile-Assigning Dialog
- Recommendations

Field study shows the effectiveness and the usability of our PPA app

http://www.privacyassistant.org

Enhanced version to be released this summer! Email us to get notified bliu1@cs.cmu.edu sadeh@cs.cmu.edu

