

I don’t know what I’ve all granted. Does it really matter?

Understanding Users’ Awareness of Different Permission Types on Android

Verena Winterhalter, Sarah Prange, Anouk Moreno, Harel Israel Berger, Florian Alt

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026. August 23-26, 2026, Hannover, Germany

On an average phone, there are…

372.8
Apps installed

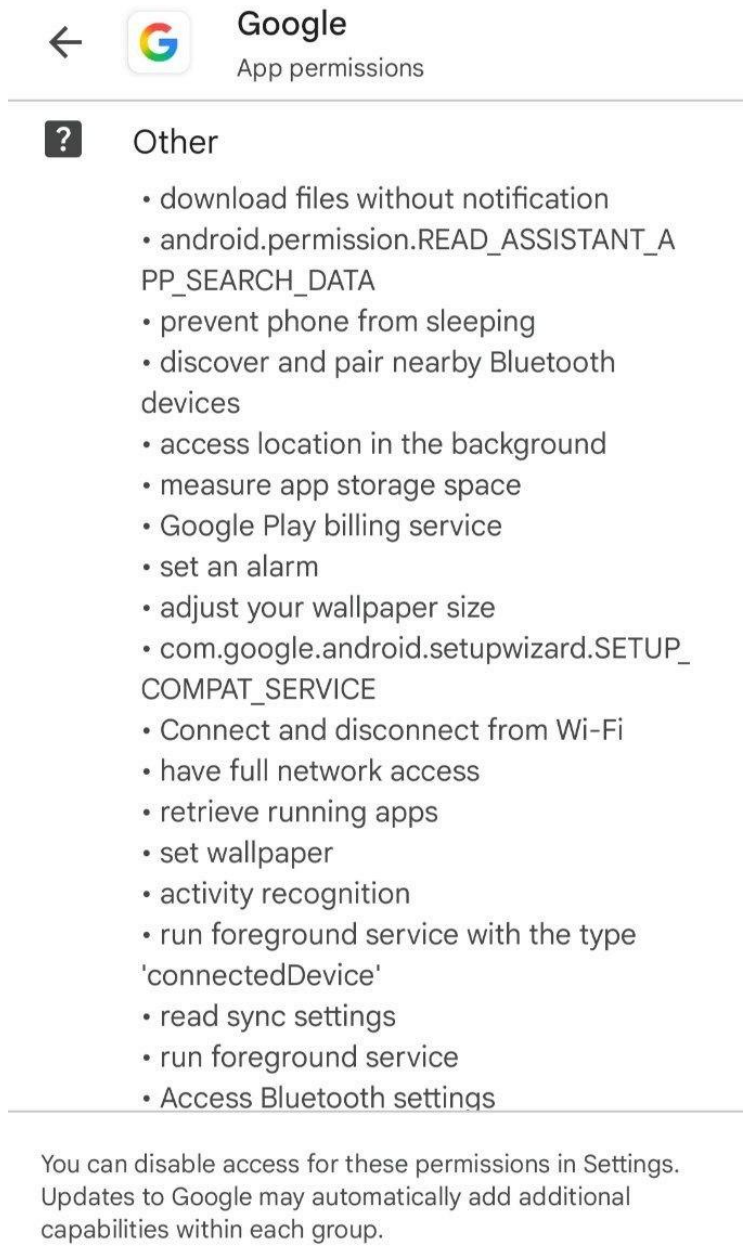
11.8
Permissions Requested
(per App)

(according to our data)

Android Permission System

Install-time permissions

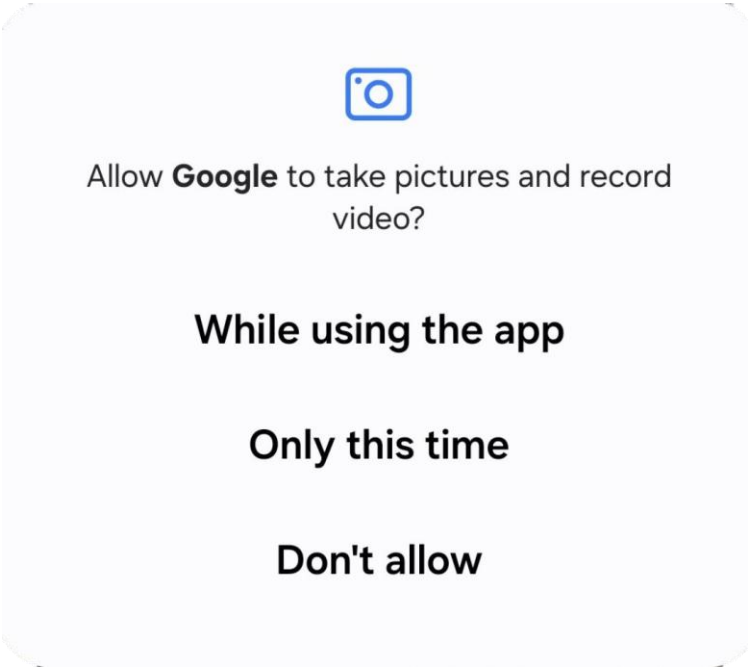
- Install-time permissions
  - Granted upon installation
  - Active as long as app is installed



Android Permission System

Runtime permissions

- Runtime permissions
  - Requested once needed
  - Fine grained options
  - Auto-revoked after 90 days if app is not used

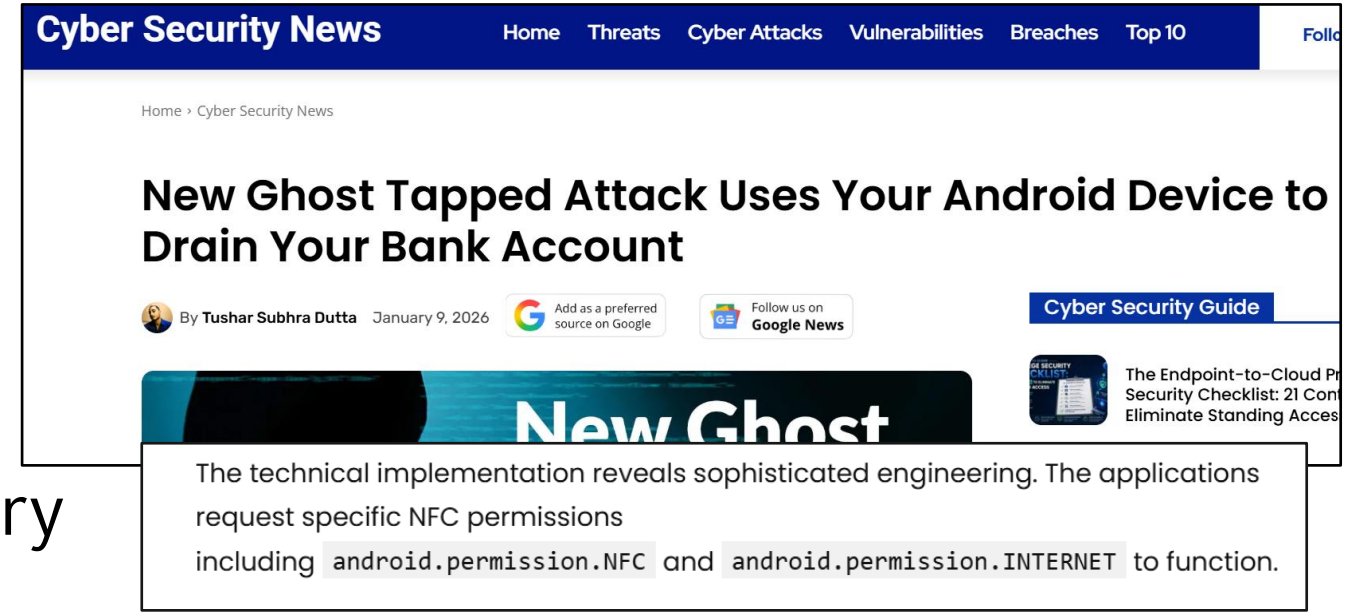


User Awareness of Android Permissions

- User awareness depends on different factors
  - Visibility of permission information
  - Forgetting over time
  - Unnoticed changes due to system updates

Why should we care?

- Potential attack vectors
- Permission combinations can introduce additional risk
- User awareness complementary to system-level protection



Screenshots: https://cybersecuritynews.com/new-ghost-tapped-attack-uses-your-android-device/

Research Questions

RQ1	**Self-Reported Awareness** How aware are users of permissions and privacy implications, in particular for dangerous permission combinations?
RQ2	**Misconceptions** How do actual permission states deviate from self-assessment? What are misconceptions?

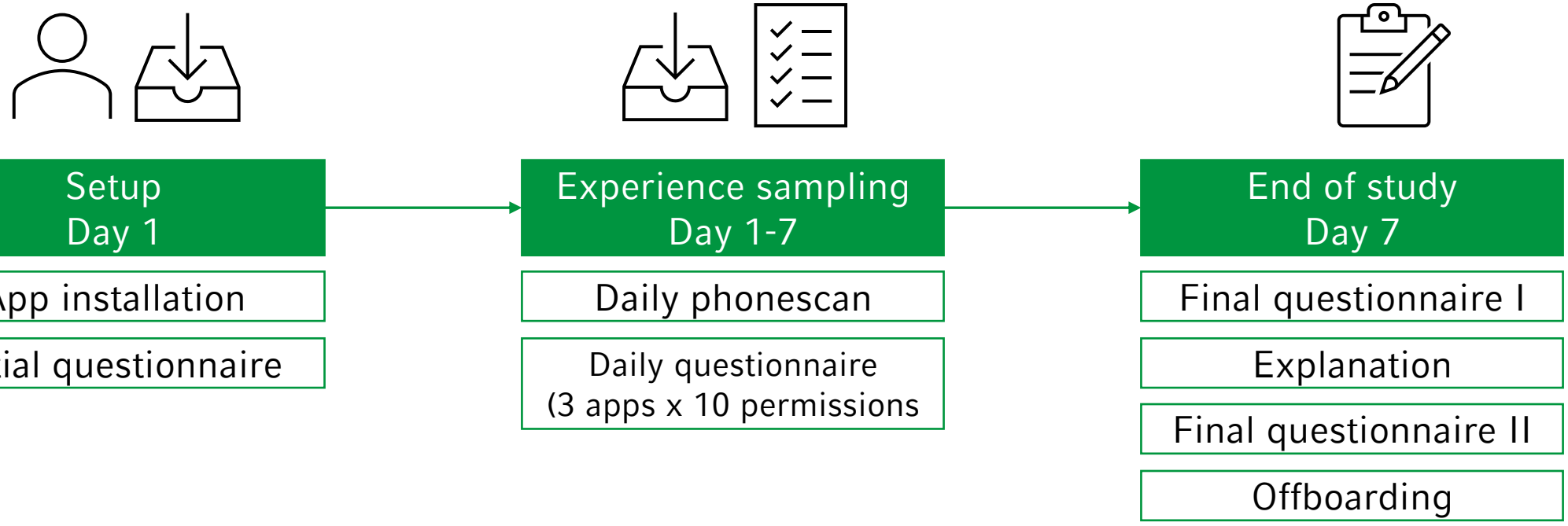
Research Approach

- Field study
- Current android permission system
- User perception
- Actual permission state

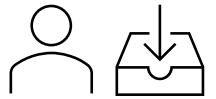
Study Procedure

Field study

- Demographics
- Initial phone scan
- Daily phone scans
- Dailies
- Final questionnaires



Results



Participants & Initial phone scan

- Prolific
- 77 participants for final data set
- Apps installed: 170-668 (M=372.8)
- Runtime permissions: 4.6/app, 51% granted
- Install-time permissions: 7.2/app

Permissions Included in Dailies

- Permpair combinations by Arora et al.
- Runtime permissions
- Install-time permissions

PermPair Permission 1	PermPair Permission 2
Internet	Access_Network_State
Internet	Wake_Lock
Internet	Read_Phone_State*
Internet	Access_Wifi_State
Write_External_Storage*	Internet
Write_External_Storage*	Access_Network_State
Write_External_Storage*	Read_Phone_State*
Access_Network_State	Wake_Lock
Access_Network_State	Read_Phone_State*
Access_Network_State	Access_Wifi_State

* = Runtime Permission

Anshul Arora, Sateesh K. Peddoju, and Mauro Conti. PermPair: Android Malware Detection Using Permission Pairs. *IEEE Transactions on Information Forensics and Security*, 15:1968–1982, 2020. doi:10.1109/TIFS.2019.2950134.

Apps Included in Dailies

Most common apps, sorted by number of occurrences in dailies

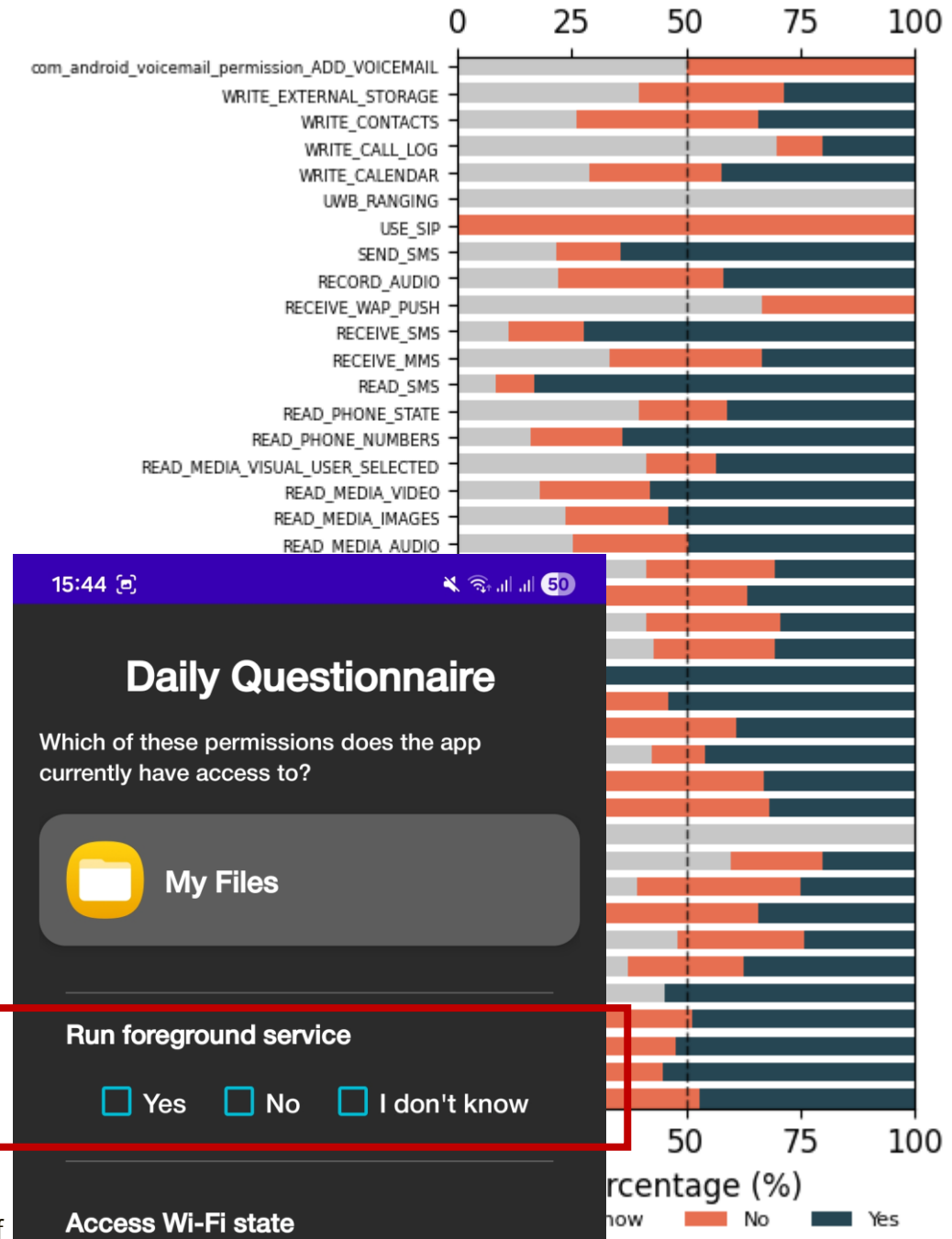
- 3 apps per daily
- Usage categories:
  - Most recently used
  - Occasionally used
  - Least recently used

App	Count
Chrome	36
Gmail	31
WhatsApp	30
Google, Spotify, Instagram	23
Messages	20
Live Transcribe & Sound Notifications, Youtube	19
Google Play Store	18
Google TV, Android Switch, Meet, Facebook	17
Security, Telegram	15
Reminder	13
Messenger, Photos, Samsung Internet, Outlook, Discord	12

Results

Dailies

- 7 dailies per participant
- 654 unique apps
- 14-21 apps per participant
- Total of 14400 data points



RQ1: Users' Awareness of Permissions & Implications



Examples from final questionnaire

General awareness (install-time)

I am generally aware that I grant permissions by installing an app.

Strongly Agree O O O O O Strongly Disagree

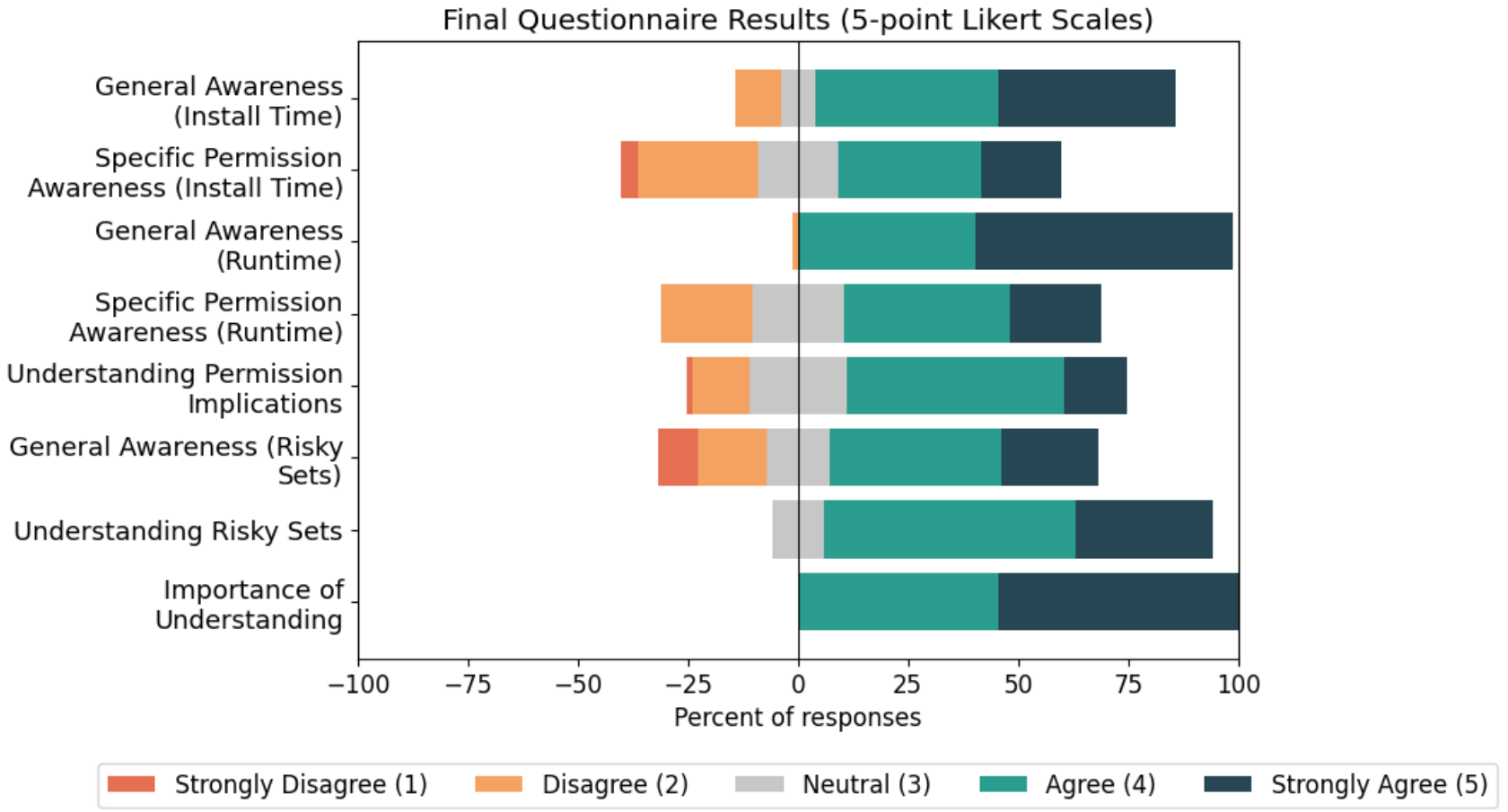
Specific permission awareness (install-time)

I am aware of the specific permissions I grant during installation.

Strongly Agree O O O O O Strongly Disagree

RQ1: Users' Awareness of Permissions & Implications

Final questionnaire



RQ2: Misconceptions

Correct vs. Incorrect answers

- What is considered a „correct“ answer?

	Granted	Denied
Yes	**Correct**	Incorrect
No	Incorrect	**Correct**
Don‘t know	Don‘t know	Don‘t know

RQ2: Misconceptions

Response correctness across permission types and app categories

Permission Type	Correct	Incorrect	Don‘t know
Permpair	52.33%	20.25%	21.41%
Runtime	39.30%	29.22%	31.48%
Install-time	48.81%	21.63%	29.56%

App Usage Category	Correct	Incorrect	Don‘t know
Most recently	47.06%	24.70%	28.24%
Occasionally	44.52%	25.32%	30.16%
Least recently	37.22%	25.69%	37.08%

RQ2: Misconceptions

False Negatives vs. False Positives

Permission Type	False Positive	False Negative
Permpair	4.40%	15.58%
Runtime	23.95%	5.27%
Install-time	n/a	21.63%

Factors Related to Response Correctness

- Generalized linear mixed-effects model
- Higher likeliness of correct responses for*:

	Odds Ratio	Baseline
Permission Type: Runtime	≈ 3.36	Permission Type: Install-time
Permission State: Granted	≈ 3.05	Permission State: Denied
Permpair Permissions	≈ 2.36	Non-Permpair Permissions
App Category: Most Recently Used	≈ 1.45	App Category: Least Recently Used
App Category: Occasionally Used	≈ 1.45	App Category: Least Recently Used

*assuming all other factors stay constant

Recommendations

How to design for user control & agency

- Focus on permissions where user has **agency**
- Improve **visibility & reviewability** of installtime permissions
- App usage recency as **indicator** for suggesting **app deletion**
- Different intervention approach per **type of misconception**

Understanding Users' Awareness of Different Permission Types on Android

Empirical data from field study with android users

Identified **factors related to response correctness**, i.e. permission state, permission type, and app usage category.

Design recommendations take into account users' agency, visibility of permission information, app usage recency and different types of misconceptions.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Media Informatics Group

Paper

Connect

Verena Winterhalter
LMU Munich
Media Informatics Group
verena.winterhalter@ifi.lmu.de