The 51 Annual International Carnahan Conference on Security Technology
Madrid, 23-26 October, 2017

Understanding and Granting Android Permissions: a User Survey

Selvakumar Ramachandran[1], Andrea Dimitri[2], Maulahikmah Galinium[3], Muhammed Tahir[4], Indirajith Viji Ananth[5], Christian H. Schunck[6], and Maurizio Talamo[7]

[1]University of Sunderland, Sunderland, UK
[2]Fondazione Universitaria' INUIT "Tor Vergata", Rome, Italy
[3]Swiss German University, Jakarta, Indonesia
[4]Sir Syed University of Engineering and Technology, Karachi, Pakistan
[5]Department of Business Engineering "Mario Lucertini", University of Rome "Tor Vergata", Rome, Italy

INTRODUCTION

Introduction

- August 2017: More than 3 million Android apps are available
- At time of this study (spring 2016) most devices run KitKat or Lollipop operating systems: At installation time apps require access to device features like:
  - Sensors
  - data storage
  - device location
  - device identity
  - user's personal contacts.
- Large Android user base: incentive to distribute grayware or malware is high

The problem

- App permissions: significant potential impact on users' data privacy and security
- User's task: correctly assess whether requested permissions are actually aligned with the app's key functionalities.
- If not the case: important indicator that the app is trying to exploit the user.
- Androids' permission warnings: should support and enhance the user's ability to give "informed consent"

Previous work

- Previous work[1]: Android permission warnings fail to inform the majority of users:

> wherein we interviewed and observed 25 Android users. Study participants displayed low attention and comprehension rates: both the Internet survey and laboratory study found that 17% of participants paid attention to permissions during installation, and only 3% of Internet survey respondents could correctly answer all three permission comprehension questions. This indicates that current Android

- Permission comprehension question example:

Permission	*n*	Options	Responses	
INTERNET Category: Network communication Label: Full Internet access	109	✔ Send information to the application's server	45	41.3%
		✔ Load advertisements	30	27.5%
		✗ None of these	16	14.7%
		✗ Read your text messages	13	11.9%
		✗ Read your list of phone contacts	11	10.1%
		I don't know	36	33.0%

[1]A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner,"Android permissions: User attention, comprehension, and behavior," in Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, 2012, p. 3

This work

1. There is more reason for confusion:
   In Android KitKat and Lollipop App permission information is actually provided at three different instances of the app installation cycle:
   a) Before installation in the Google Play Store
   b) During the installation process
   c) After installation in the Application Manager.

   ➡ How does this impact the users?

2. What about higher degree of contextualization: does this lead to higher attention and comprehension rates?

Contextualization: Mirror App

Mirror

[redacted]

★★★★☆ 3,483

PEGI 3

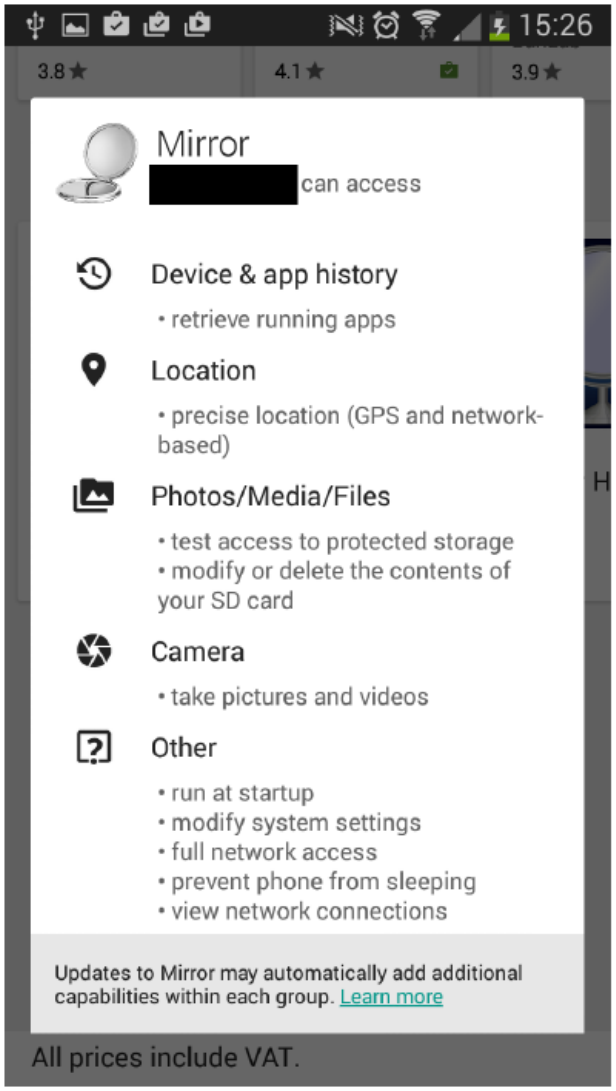
This app is compatible with your device.

Add to Wishlist

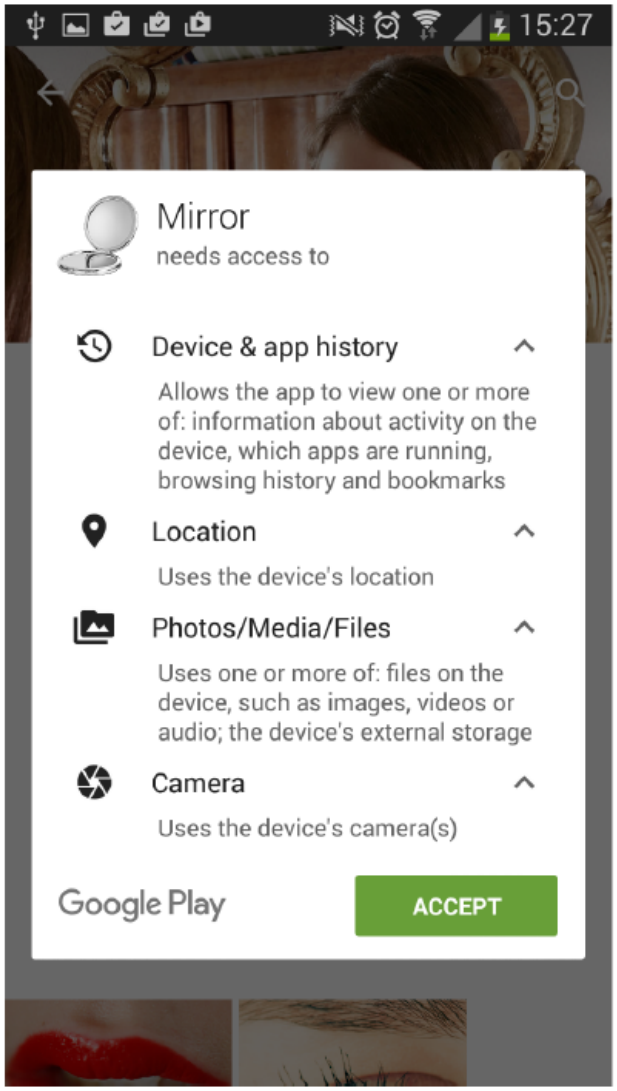
Install

This mirror app (like any other mirror app...) uses your front facing camera to function as a mirror, only that it also offers a selfie camera, freeze frame feature and some other great settings.

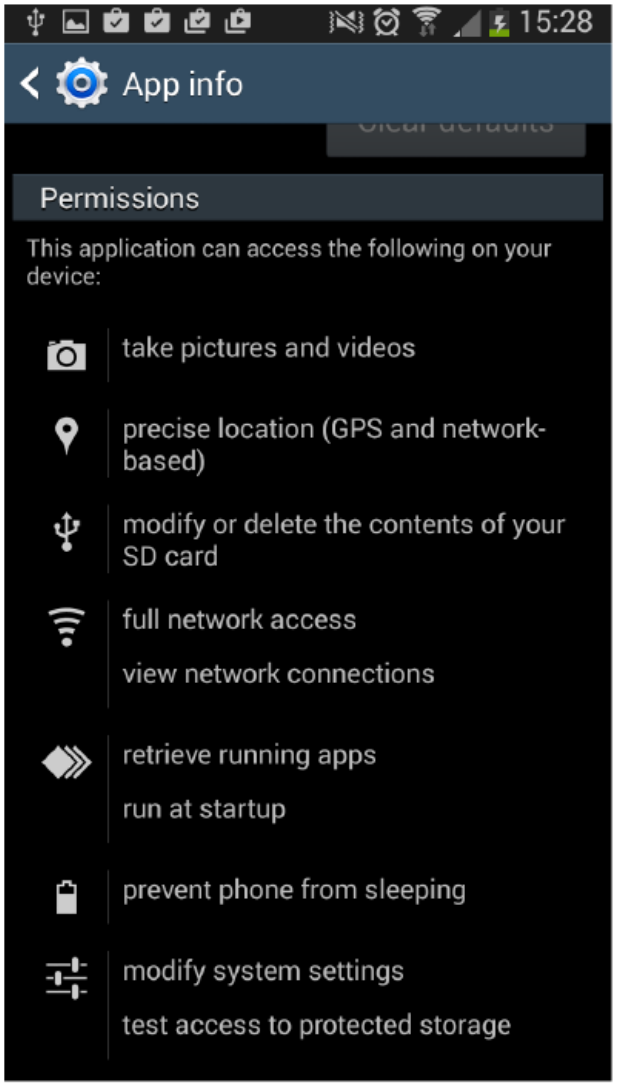
3 types of Permission warnings



In Google Play Store



At Installation Time

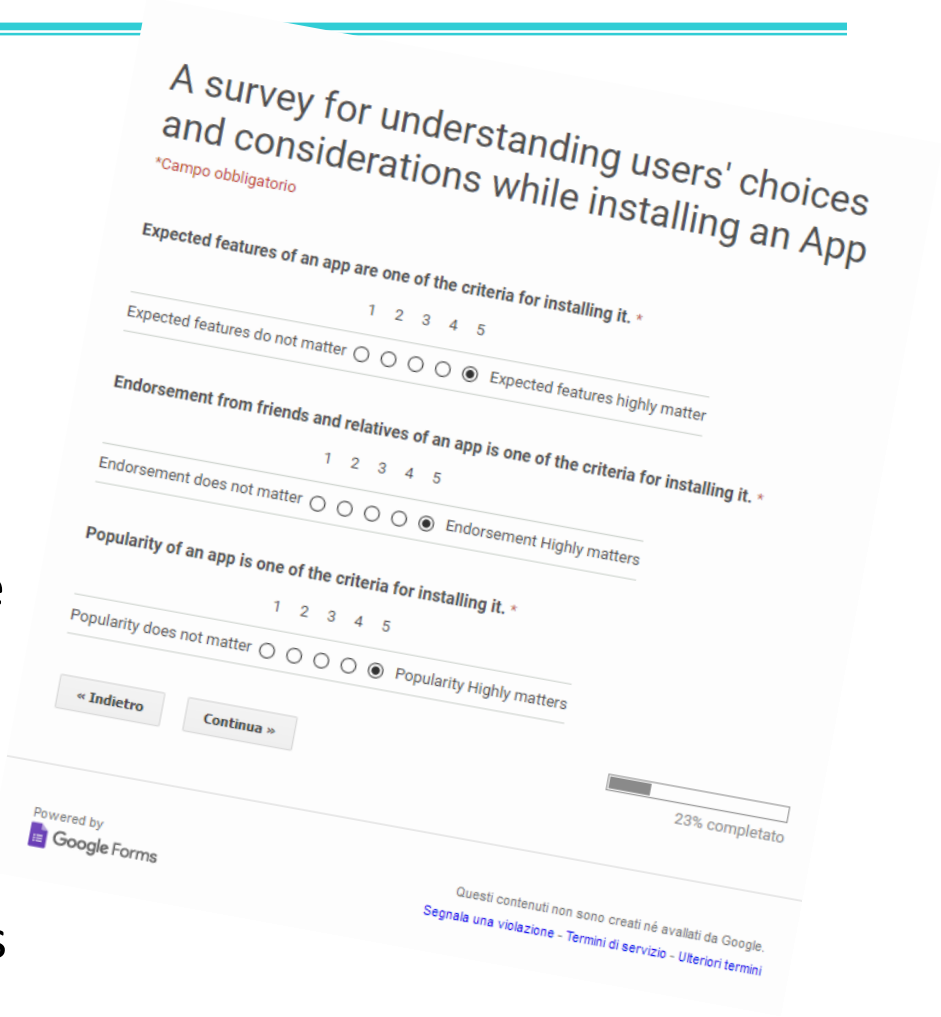


In the Application Manager

The Survey

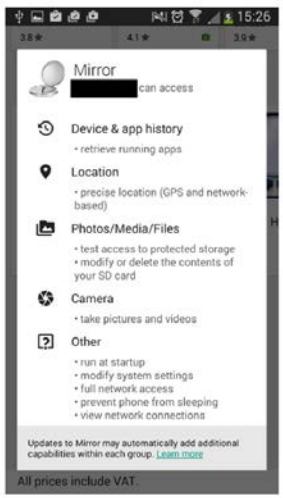
The Survey

- Internet based survey during the period of March 18, 2016 to May 2, 2016.
- Survey was promoted via social media.
- A total of 510 fully completed Android users surveys were obtained.
- Respondents were required to be Android users: 31 responses were excluded since respondents stated that they never installed an App on an Android device.
- One response included inappropriate comments and was thus excluded.
- The total number of analyzed questionnaires is 478.

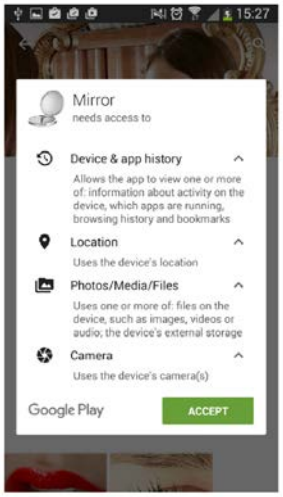


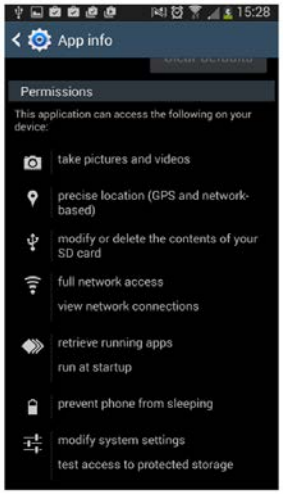
Survey Questions

- 2 survey types:
  Users were asked to evaluate either Google Play Store permission OR installation-time permissions warnings WITH Application Manager Permission overview.
- 13 technical questions
- 6 demographical questions



OR





Play Store Perspective

Installation Perspective

Application Manager Perspective

Survey Questions (contd.)

- Technical questions:
  - Understanding users' choice of an app (Q2, Q3, Q4)
  - Carefulness while reading a Permission List? (Q5)
  - Insight that Camera permission is required for the Mirror app to function (Q5)
  - Level of Comfort with Permission warnings Play Store/Installation time – (Q8)
  - Knowledge about possibility to check permissions after installation (Q10)
  - How are discrepancies between the Application manager perspective and the Play Store/Installation perspective perceived – (Q11)

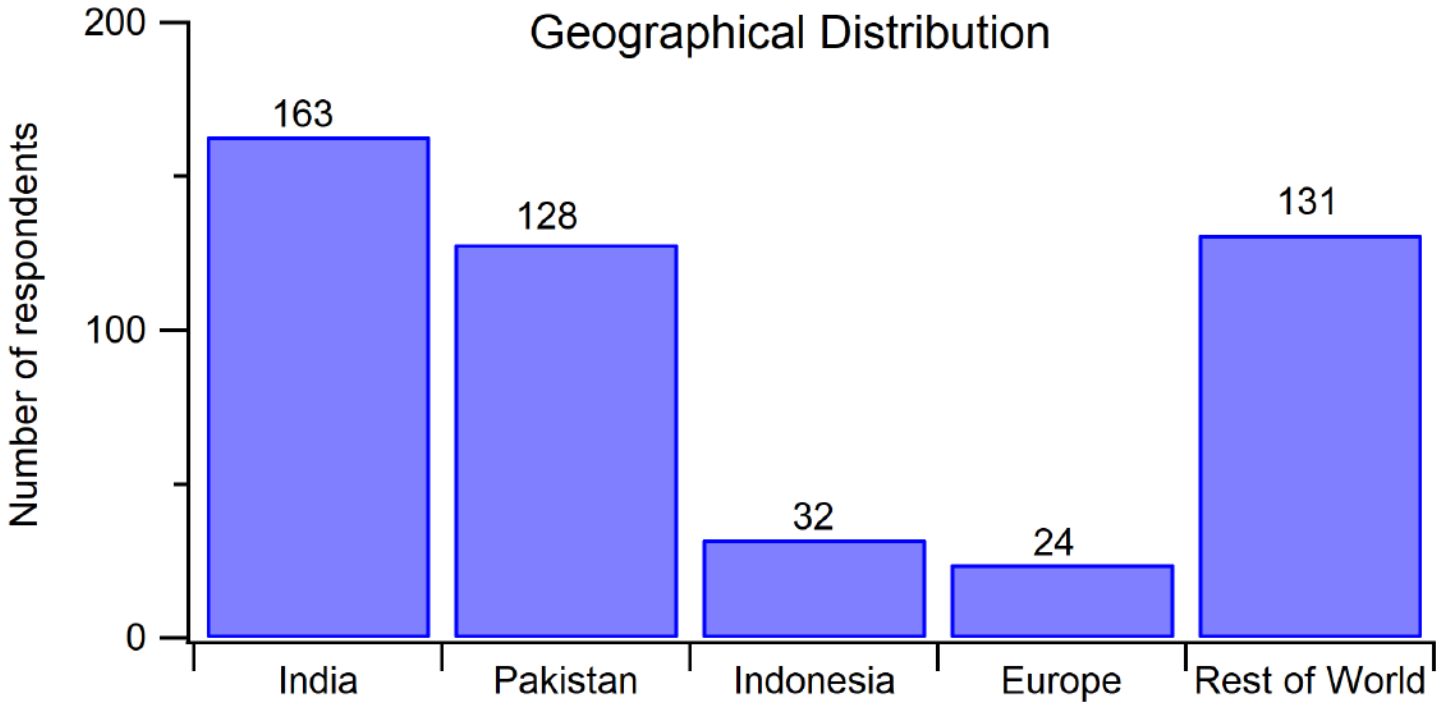
Analysis

- Measure the influence of an expertise level X on a single answer Y to a question
- Logistic regression model where every level of expertise X is a candidate predictor and the dichotomic dependent variable is the answer Y: for every couple (X,Y) the beta (correlation) parameter is calculated and its significance is verified using the Wald test.
- We give the beta correlation parameter and Wald test values: the significance threshold for a p value of 0.05 corresponds to a Wald test value of 3.84.

RESULTS

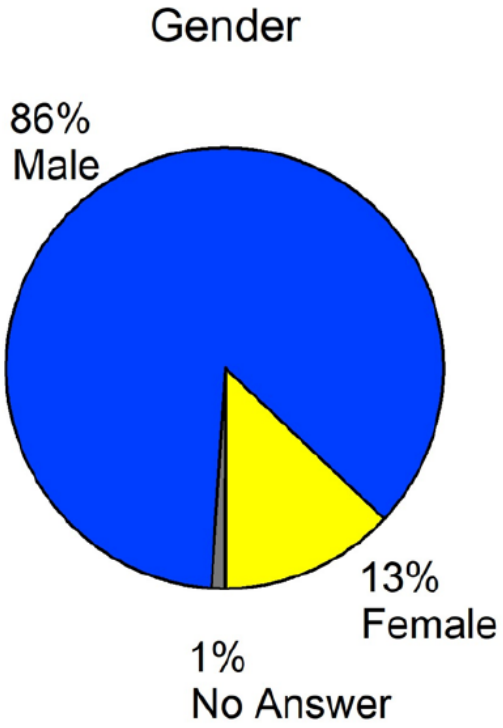
Demographics 1

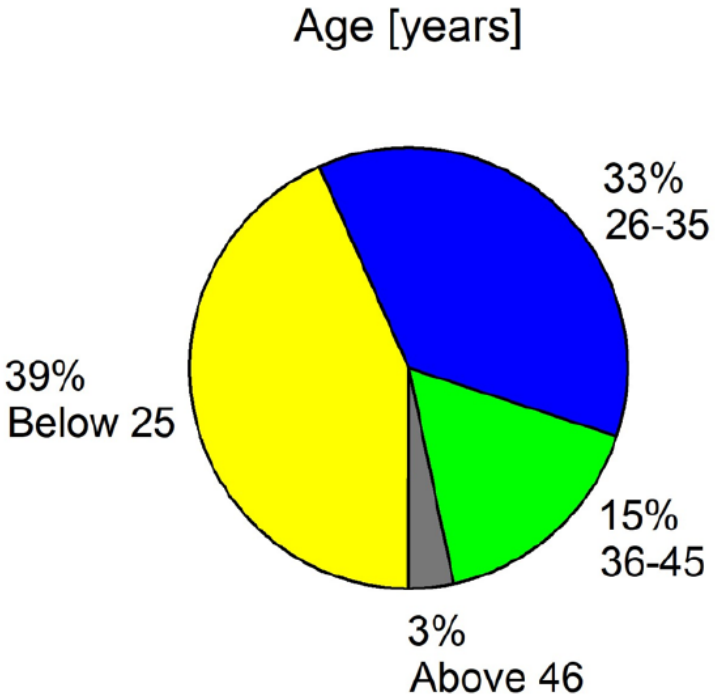
- The surveys received responses predominantly from India, Pakistan, Indonesia, Europe and North America



Demographics 2

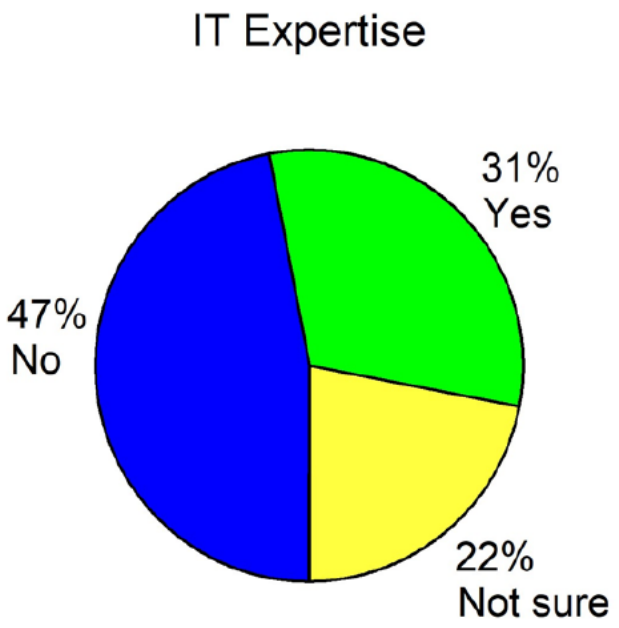
- 13% of the respondents were female and 80% male.
- 97% of respondents were below the age of 45 years.

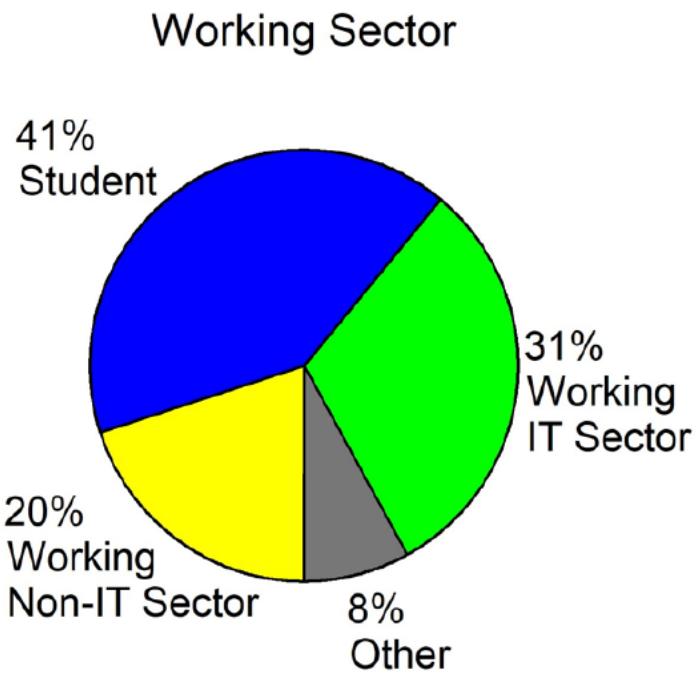




Demographics 3

- Self declared IT Expertise
- Working sector



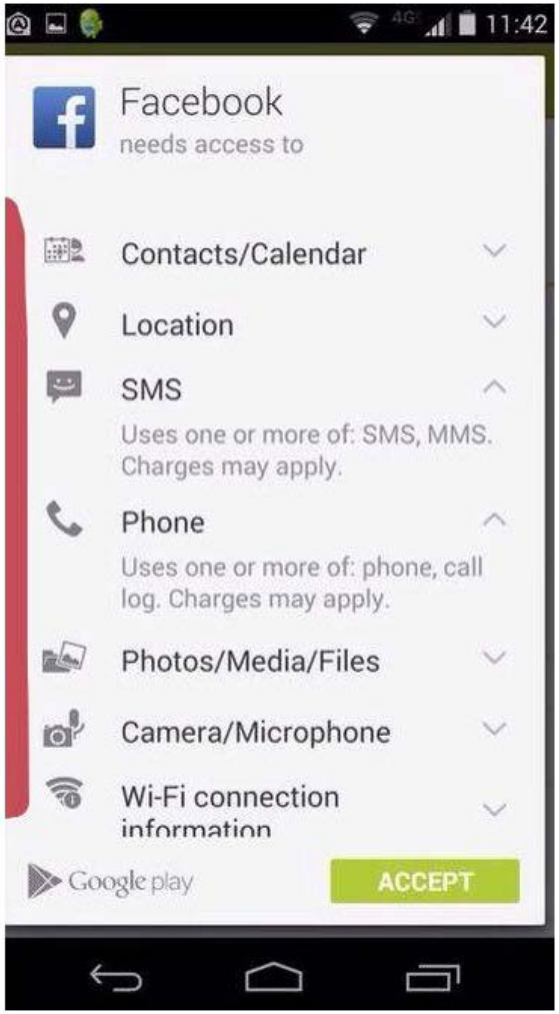


Self declared attention to permissions

How carefully do you usually read the list of permissions when you are about to install an Android App from Google Play Store? *

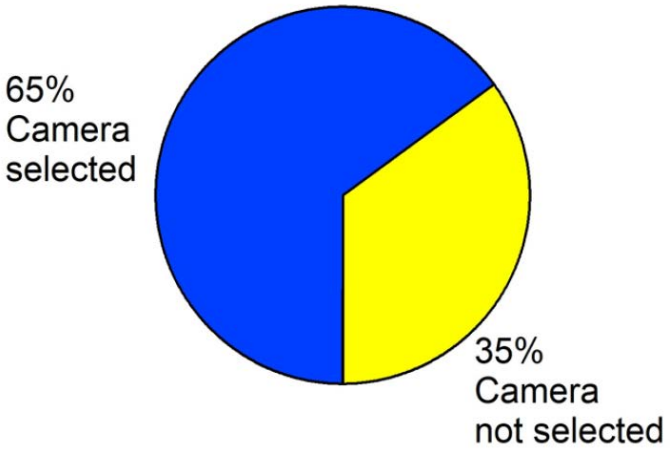
	1	2	3	4	5	
Not At All	○	○	○	○	○	Very Careful

- 23% of respondents answered 5
- 63% of respondents chose an answer between 1 and 3 (about equally distributed).
- Strong correlation between users claiming to be an IT expert and their claim to read app permissions “very carefully”
  (beta 0.896, test 15.8).



Camera Permission

- Task to select Mirror App permissions that “should in your opinion be requested by the app for providing the promised functionalities”.
- 35% of respondents did NOT correctly identify the camera permission as a required one - even in this simple and highly contextualized example.

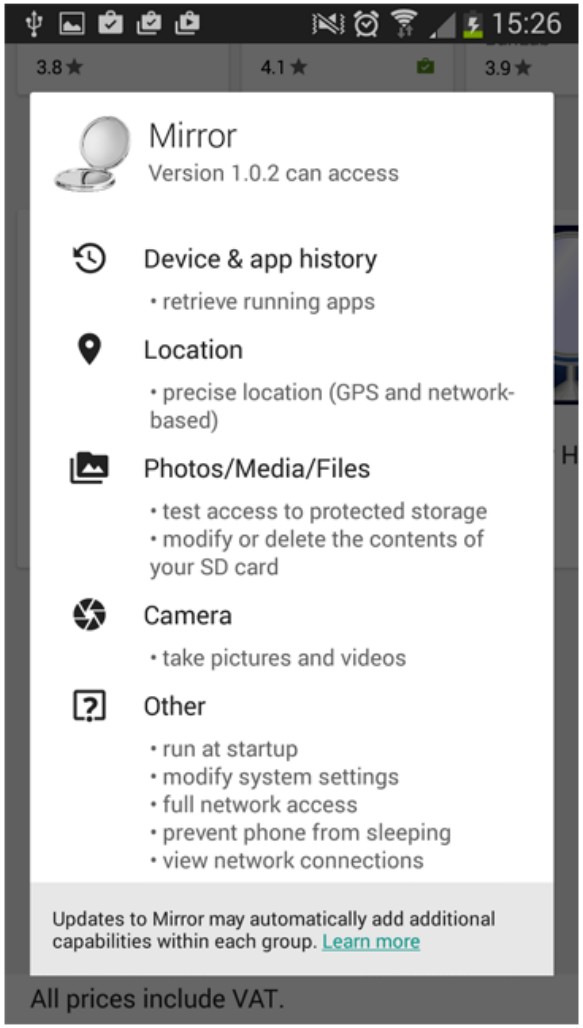


This mirror app (like any other mirror app...) uses your front facing camera to function as a mirror, only that it also offers a selfie camera, freeze frame feature and some other great settings.

Permissions at/before installation

Assuming that you would like to have to such a Mirror App on your device, how comfortable are you with the requested permissions shown above? *

- ◯ Very Comfortable - will install this Mirror App
- ◯ Comfortable - will install this Mirror App
- ◯ Not Comfortable - but will install this Mirror App nevertheless
- ◯ Not Comfortable - will not install this Mirror App



Permissions at/before installation

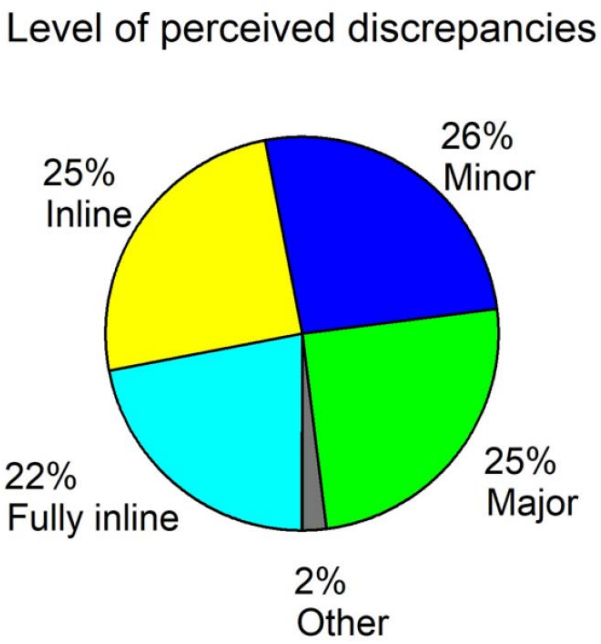
- Strong correlation between correctly identifying the camera permission and “not comfortable - will not install this mirror app” (beta 0.807, test 11.5).

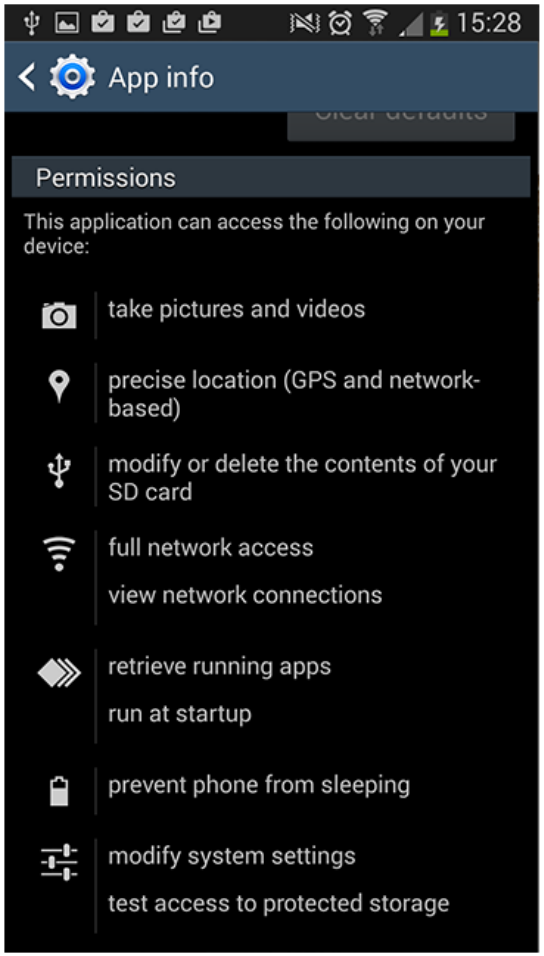
- Respondents who did not identify the camera as required state to be “very comfortable - will install the mirror app” (beta 0.764, test 10.7).

Permissions after installation

In your opinion, are the permissions given in the list above (as shown in the application manager after installation) consistent with the permissions you have granted at the time of installation *

- ◯ Fully in line with the Permissions shown
- ◯ In line with the Permissions shown
- ◯ Minor Discrepancies
- ◯ Major Discrepancies
- ◯ Altro:





Permissions after installation

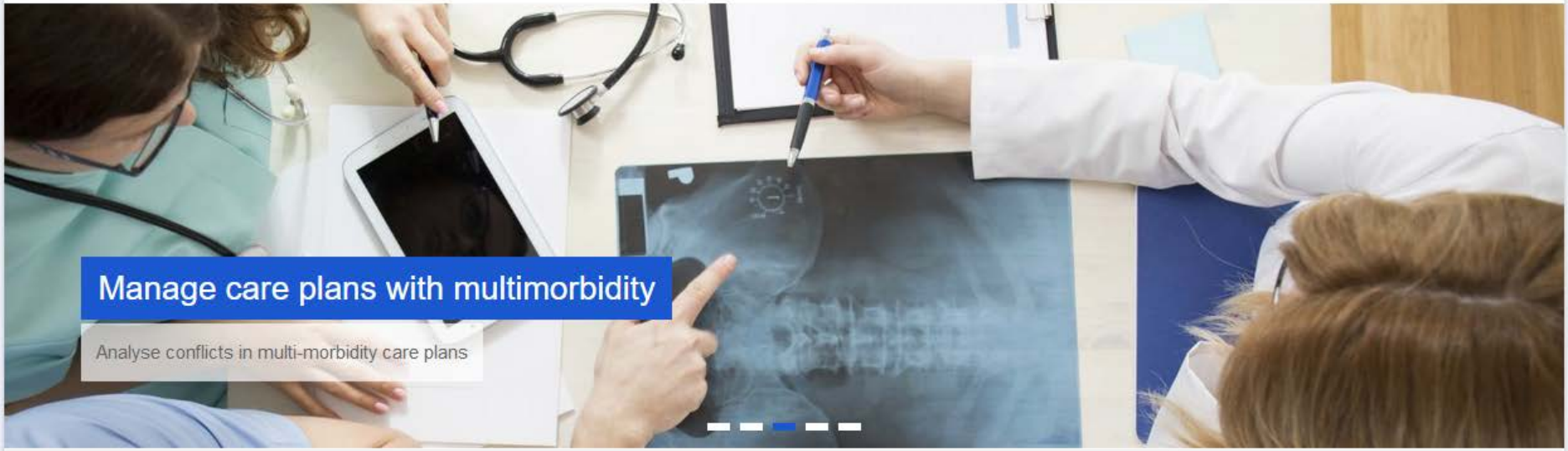
- Very strong correlation between correctly identifying the camera permission and the perception of discrepancies
  (beta 1.36, test 25)
- Respondents who did not identify the camera as required were significantly less likely to perceive discrepancies
  (beta 0.727, test 11.3).

- Sensitivity to differences in app permissions critically depends on a basic level of comprehension and attention which a significant number of respondents do not demonstrate even in this straightforward scenario.

Future Work - PICASO Project

PICASO: integrated care

- Horizon 2020 project
- The PICASO project stands for: A Personalised Integrated Care Approach for Service Organisations and Care Models for Patients with Multi-Morbidity and Chronic Conditions.
- Funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 689209. The project started in February 2016 and will last until July 2019.



Latest Posts

Meet PICASO at ICCST 2017

PICASO Project 10th October 2017

PICASO partner INUIT will be presenting the paper "Understanding and granting Android permissions: A user survey" at the 51st International Carnahan Conference on Security Technology (ICCST 2017) on 25th October 2017, in Madrid, Spain. The ICCST paper is titled: "Understanding...

Read more

Presentation of the UDUS Trial at the DGRh 45th Congress in Stuttgart, Germany

PICASO Project 10th October 2017

The UDUS trial was presented at the German Society for Rheumatology (GDRh) 45th Congress in September 2017. PD Dr. Jutta Richter presented the UDUS trial in the Investigator Initiated Trial (IIT) poster session at the DGRh Congress. The poster presentation,...

Read more

Poster Presentation at EULAR 2017

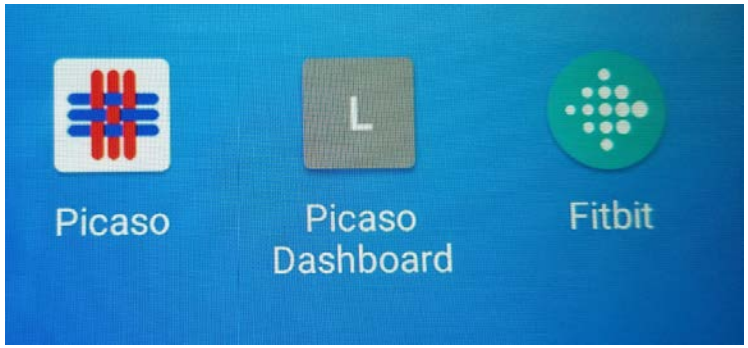
PICASO Project 10th October 2017

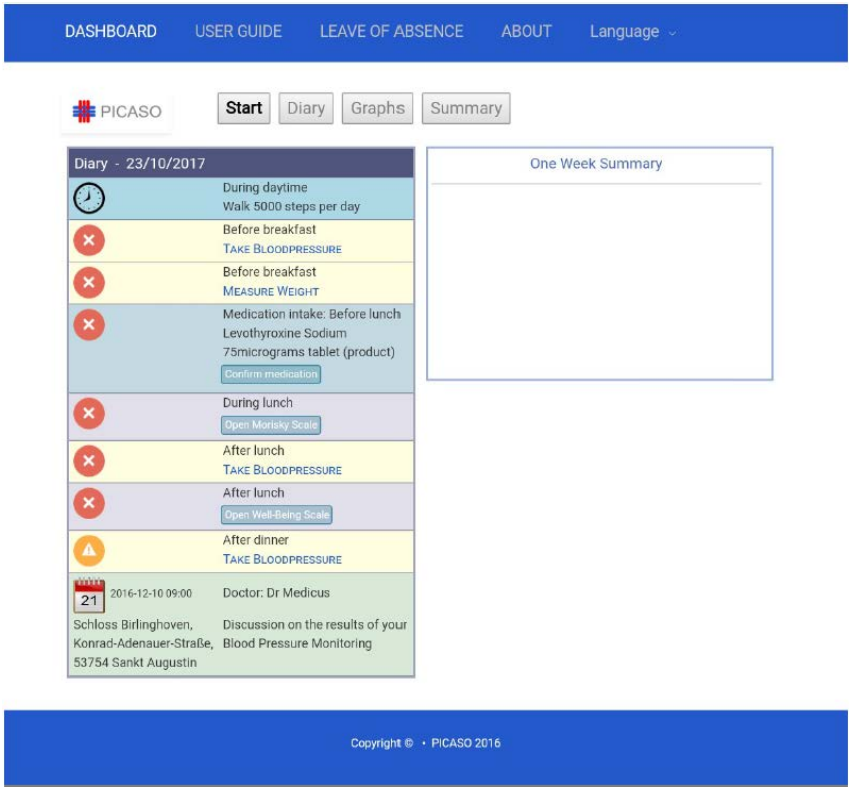
The PICASO trial run by project partner UDUS was presented at the Annual European Congress of Rheumatology (EULAR) in Madrid, Spain, in June 2017. The poster presentation focused on the experiences and knowledge gained so far in developing the PICASO...

Read more

PICASO

- Findings are particularly important if applied to sensitive health-care apps and will be taken into account.
- Providing detailed info about the Apps used in the project and how patient data is collected and processed is critical.





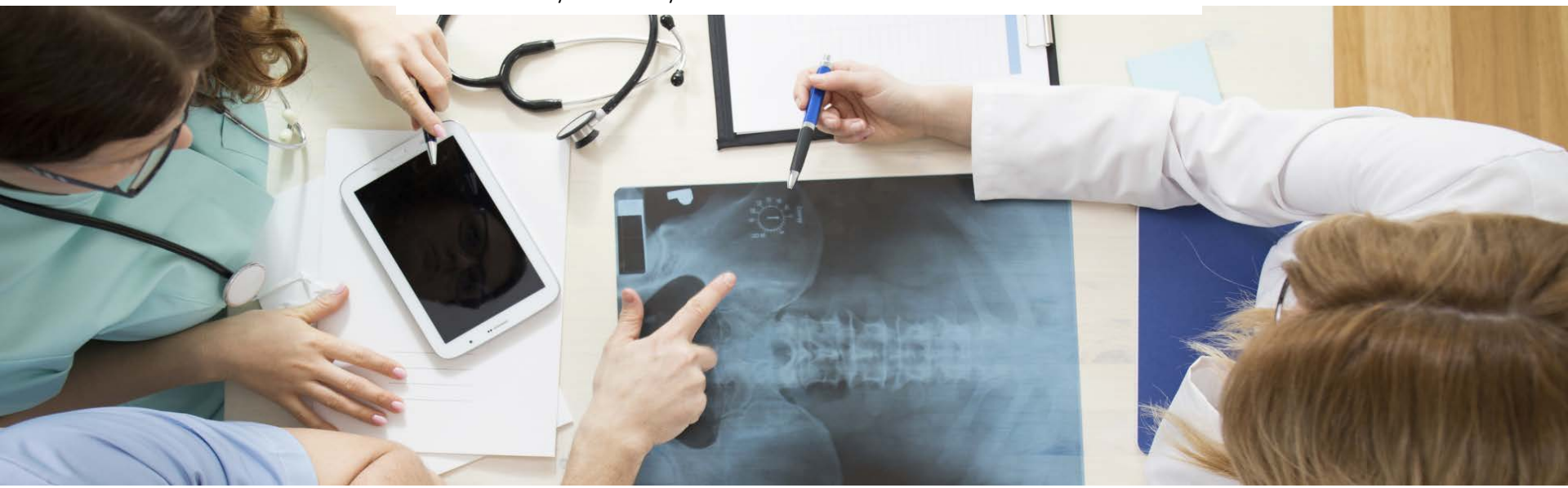
PICASO Partners

- Fraunhofer Institute for Applied Information Technology (DE) – Project coordinator
- CNet Svenska AB (SE)
- In-JeT ApS (DK)
- Research Institute Fondazione Inuit Tor Vergata (IT)
- Technical Universtiy of Kosice (SK)
- Vrije Universiteit Brussel (BE)
- University of Rome “Tor Vergata” (IT)
- Heinrich-Heine-University Düsseldorf, Universitätsklinik Düsseldorf (DE)

PICASO

Please see us here: www.picasso-project.eu

PICASO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 689209.



Conclusion

- Respondents who demonstrate a low degree of attention and comprehension appear to feel comfortable with the requested app permissions even if these cannot be justified by the primary app functionalities.
- A relatively large fraction of users (65%) actually correctly identified a critically required app permission. We believe that this is related to the provided example which supports contextualization.
- Requested app permissions should be contextualized to the largest degree possible. Newer versions of Android have made progress in that regard.
- In current Android versions an editable overview of app permissions is provided in the application manager. However, this has been achieved at the expense of significantly reducing the granularity of permission information.

Thank You!

Christian H. Schunck

Department of Business Engineering “Mario Lucertini”
University of Rome Tor Vergata, Italy
christian.schunck@uniroma2.it