Empowering Users

End User Development for Mobile Applications Privacy Management

Politecnico di Torino

Juan Pablo Sáenz and Luigi De Russis

juan.saenz@polito.it, luigi.derussis@polito.it
Dipartimento di Automatica e Informatica
Politecnico di Torino

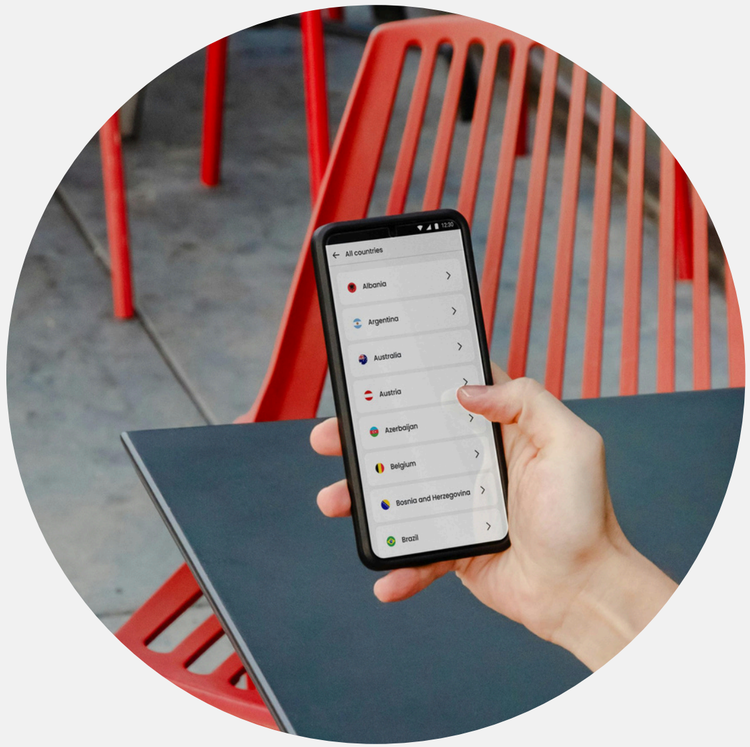
International Workshop on Trusted Computing and Artificial Intelligence applied to Cybersecurity

Background

Users generally **lack trust in app permissions** and **OS-provided privacy measures**

In the current permission mechanisms provided by the OS

If the user understand the tecnhical details, he could judge if whether permissions are correct and be aware of possible privacy concerns while using the app



However, these mechanisms are insufficient to non-expert users...

Due to their **inattention** and **misunderstanding** of the system's prompts. Additionally, privacy settings are not easy to configure

Indeed...

The challenges users encounter in efficiently managing their security settings stem partly from the **lack of user-centered privacy designs** and control features

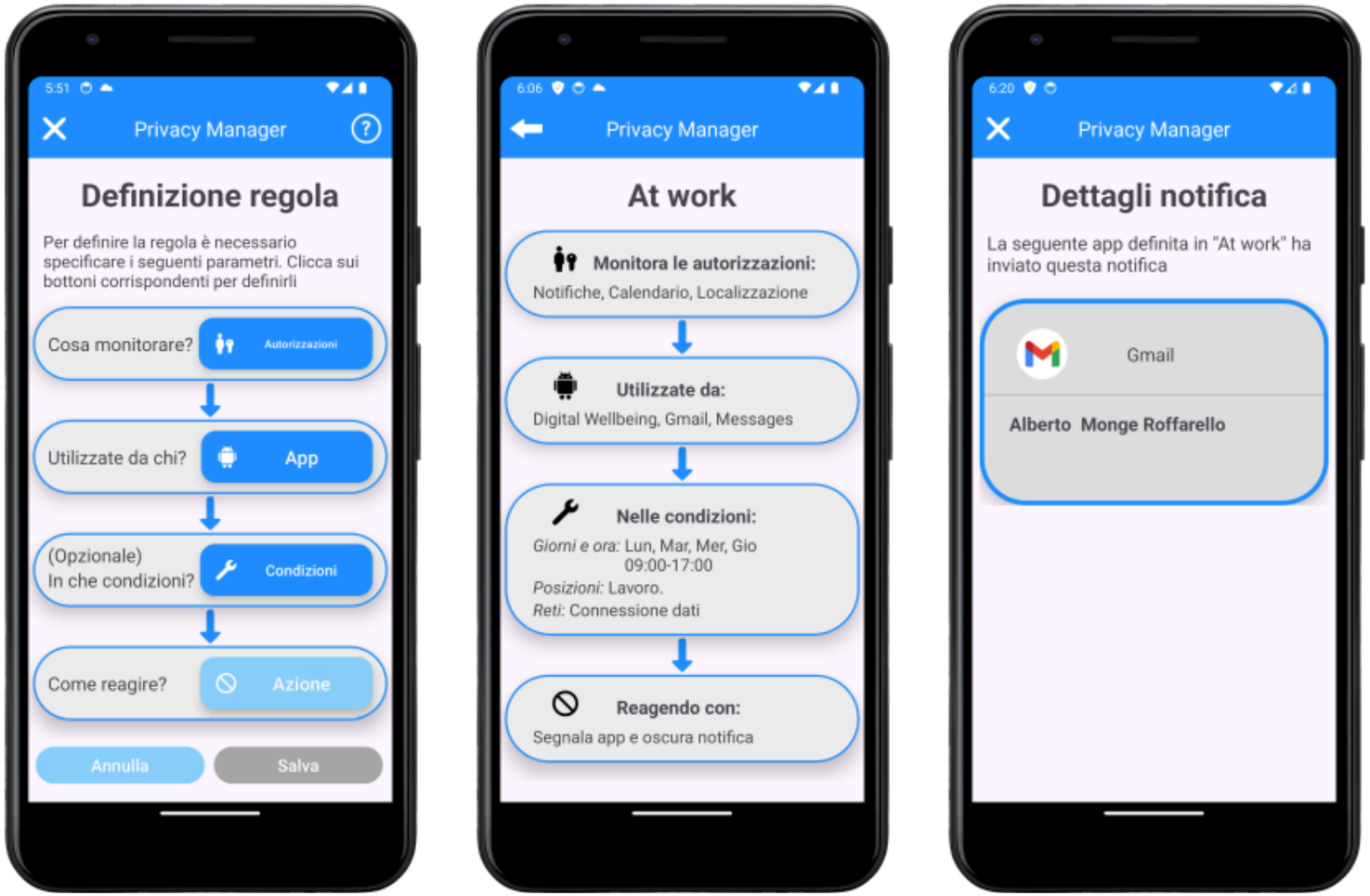
MOTIVATION

Explore to what extent an End-User Development approach can empower the users to protect their privacy and gain insight into the permissions granted to the applications

Privacy Manager

An **Android application** aimed at:

- Providing **non-expert users** with a **friendly** mechanism to effectively manage the privacy and security of their personal data.
- **Enabling customization** of data management based on parameters most relevant to each user.

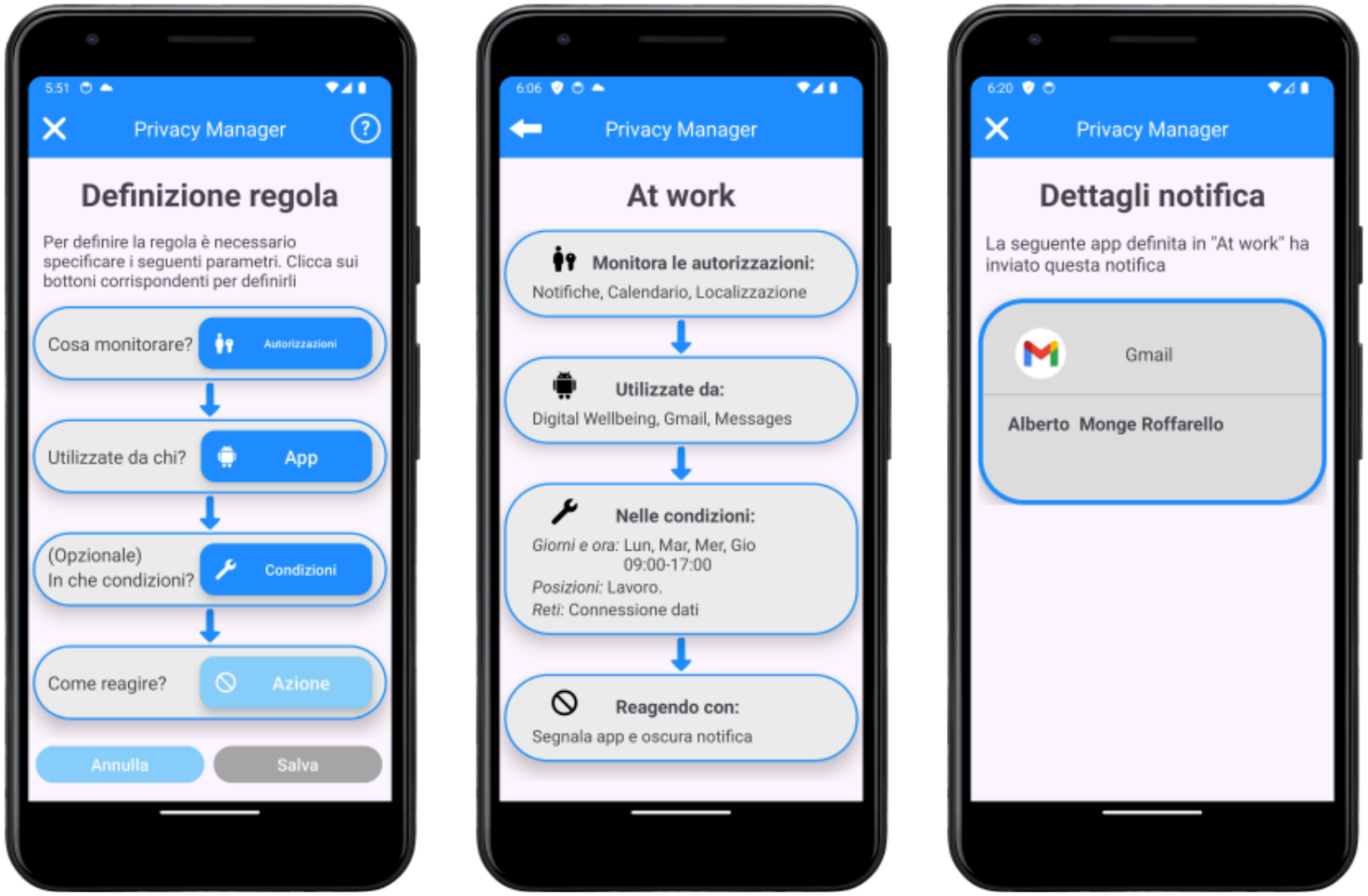


Privacy Manager

Create **security rules** based on a set of **parameters:**

- **Permissions:** location, calendar, camera, and notifications
- **Applications**
- **Conditions:** day and time, locations, network, bluetooth, battery
- **Behaviors:** reporting, stopping, or hiding

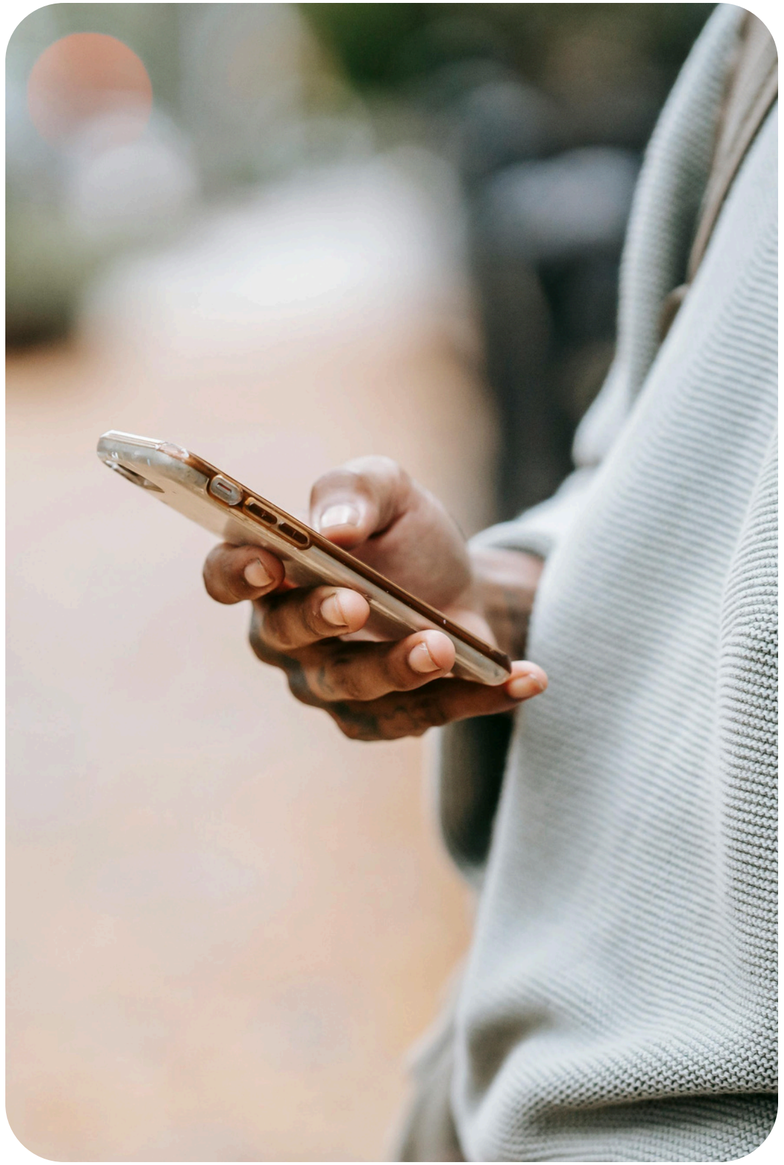
IFTTT



Validation

We conducted an **in-the-wild validation** in which the users utilized Privacy Manager under real-world conditions, reflecting daily routines and habits

- 8 participants
- Comprised an **initial questionnaire**, **one week of application usage**, and a **final questionnaire**



Results

Initial questionnaire

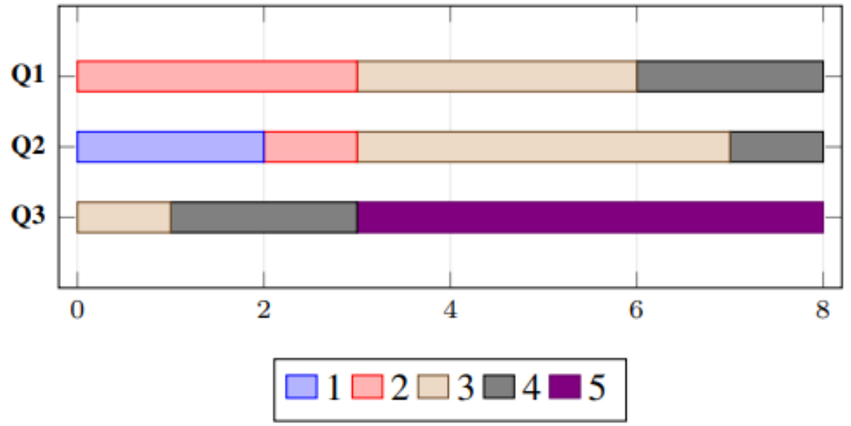


Fig. 2. Participants' perceptions regarding the use of their device and the protection of their privacy using a Likert scale ranging from '*Not at all*' (1) to '*Very much so*' (5).

- **Q1**: How satisfied are you with the privacy and security protections provided by the applications you use?
- **Q2**: How easy do you find the way your smartphone allows you to manage your privacy and security?
- **Q3**: How interested would you be in having greater control over how your smartphone and the applications you use manage your privacy and security?

Results

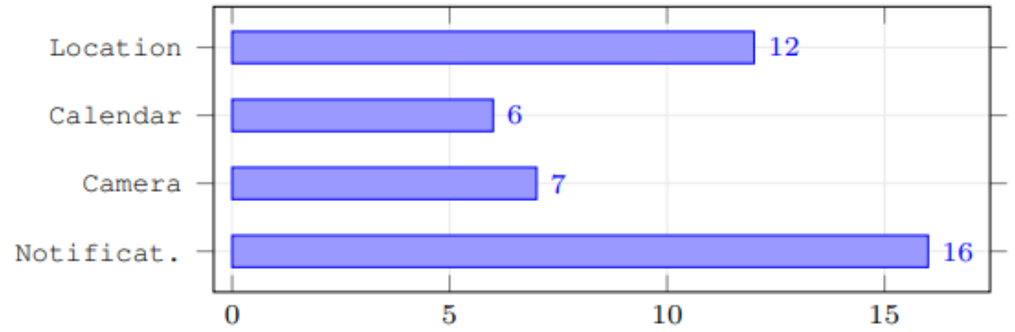


Fig. 3. Permissions chosen by the participants when creating a security rule

The week of application usage (1)

- Participants created **25 security rules**. The number of rules per user ranged from 1 to 12.
- The security rules were quite heterogeneous in terms of monitored permissions. Users preferred to **monitor a single permission per rule** in 72% of cases
- The most monitored permissions were **notifications** (36%) and **location** (24%)

Results

The week of application usage (2)

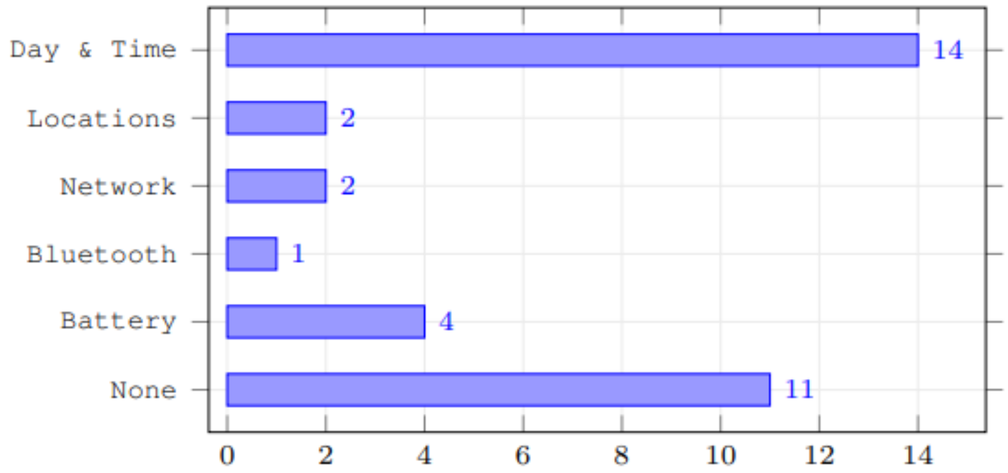
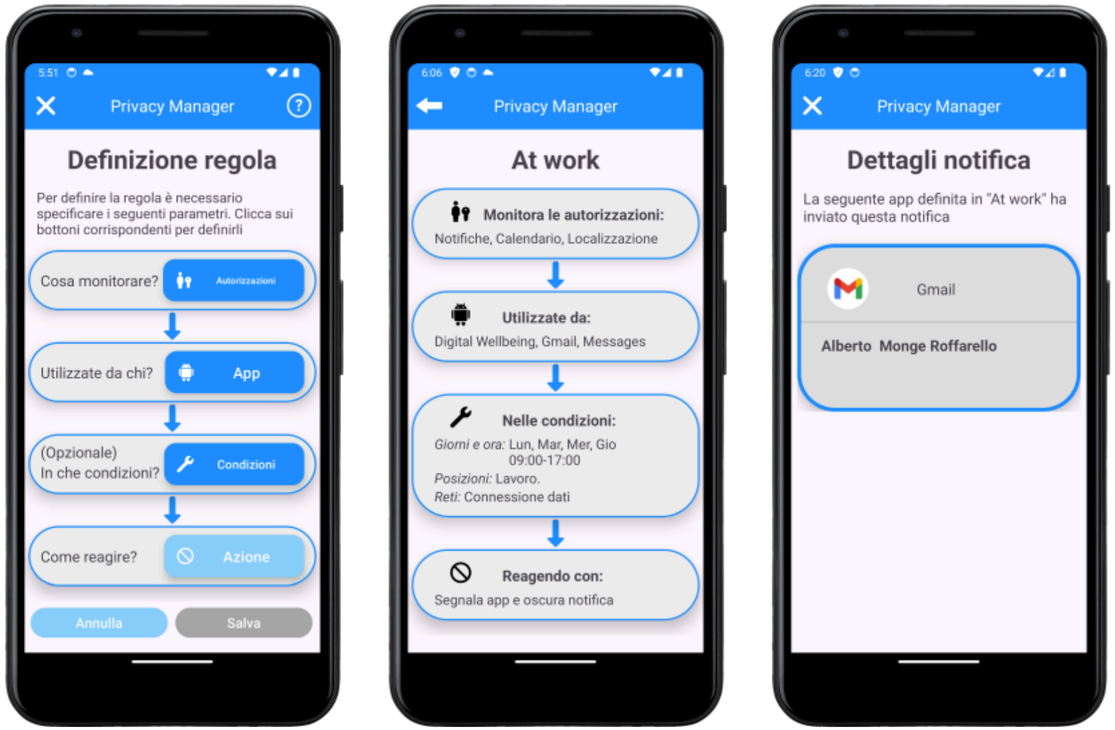


Fig. 4. Conditions defined by the participants when creating a security rule

- A significant majority of security rules included a condition related to the **time slot**.
- During the week of usage, the Privacy Manager application **intercepted 24 actions**, with **notifications** causing **75% of these interceptions**.
- The least reported permissions were **calendar** and **camera**, each reported only once. This emphasizes the prevalence of notification reporting, which was the most monitored permission by users

Conclusion



Private Manager, a mobile application leveraging End-User Development (EUD), empowers users to protect their privacy and understand permissions on their smartphones

In a **one-week study** with eight participants, the application was found to be useful, achieving the goal of adaptable, user-specific privacy protection through customized security rules

Future validation will involve more participants and a **longer testing period**, evaluating parameters like application **opening frequency** and **usage duration** to enhance effectiveness and privacy protection