Advanced Projects at the Quality and Usability Lab
Project: Usable Security
PD Dr. Esther Ruiz Ben

Usable Security in Web-Applications

-

Project Interim Report

16. May 2019

Group A:
Georgi Ivanov
Nizan Goldstein
Yagmur Uckunkaya

Table of Contents

1 Introduction

Since the invention of the internet, the private person allows more and more organisations to enter his/her private sphere. Whether it’s teenagers looking to make some virtual friends through applications or the digital world forcing elderly to use its innovative products. The users stand often at a point where they don’t have a choice anymore. What they can do though, is control what information to whom they give it, when and why.

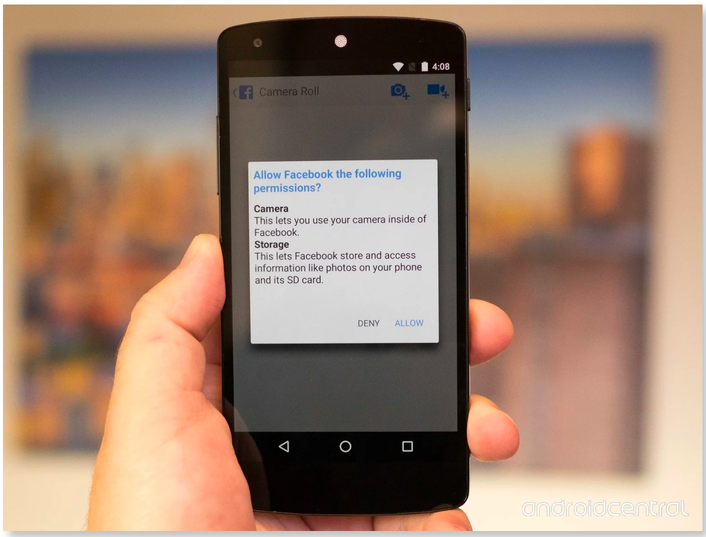
Each application requires the users’ permission to access their personal data and is bound to a set of rules legislate by the European government. On the other hand users are bound to permit the application to read his data, otherwise they won’t be able to use it.

Sixty two percent of the IOS application ask permission to access the ‘Photo Library’, fifty five percent ask access to the camera, fifty one percent want access to your location and twenty three precent want access to your microphone (La Porta, 2019).

According to the Data protection report, written by the European Union only fifth of the users are always informed about the conditions and true uses of their data collections (Díaz, 2016). That leaves eighth percent aware, semi-aware or not aware at all users. It also says in the Report that those eighty precent don’t read or read partly the privacy statements, because it’s too long or not understandable.

The companies want the permissions, for whatever reasons. And the users want to use the services the companies provide. Our goal is to maintain this natural balance, but just to make sure that the users are aware of their actions and rights, provide them some extra information and alert them when an application makes a wrong use of their private data. For example a usage of their camera or microphone while they do not even use the application, or make them ask themselves if a flashlight application really needs accesses to their contacts and microphone.

The following interim report will give an outlook about how we plan to keep this balance with our application, our methods and timeline.



Allow Facebook the following permissions?

Camera
This lets you use your camera inside of Facebook.
Storage
This lets Facebook store and access information like photos on your phone and its SD card.

2. Usable Security App

During our researches we came to the realisation that most common social media applications have practically the same steps for the registration. Which also meant for us that these apps essentially ask for the same allowances. So instead of focusing on one specific app or one security problem, we decided to have a general approach towards the security awareness problem.
Our approach towards solving the security and privacy awareness problems regarding the mobile applications is through an app that reminds the user possible security and privacy threats during the registration and use of the app. We want our app to not only raise awareness but also not get in the way of registration. In a nutshell, we want to focus on two main points: Raise the awareness during and after the registration and make it as usable as possible. Our app should not stop the registration process but remind the user smoothly of potential risks. We aim to achieve these two main goals through pop-ups that our app generates, which will intervene at the necessary moments during the registration and afterwards. In order to determine these necessary steps, we again adapted a practical approach. Going through registration process of various apps we managed to list the most important key points, which we will further explain in the following shortly.

1- Privacy License

Recent statistics show that 30% of the internet users in Germany never read the privacy policies of web applications yet they agree to them. The percentage of people who always read it before agreeing to them is only 7%(Wundere, 2019) . We aim to make user think twice before they agree to conditions that they never read before. Through our app the user will see automatically a pop up when the privacy agreement appears on the screen. This pop-up will suggest the user to read the privacy license. Considering the length of the privacy agreements, it will highlight the importance of reading, at least, some parts of the agreements such as “data collection” and “how that data will be used”.

2- Password

Previous studies have shown that majority of the internet users still use passwords which already leaked in other data breaches and are available to attackers in plain text such as “123456” or “password”. Another most common mistake that users do is that using the same password for multiple accounts and creating personal predictable passwords. Having a good password alone isn't secure enough, uniqueness still matters enormously (Hunt, 2018). Considering the fact that having a strong password is one of the most important precautions when it comes to data privacy we aim to remind the user the importance of this step during the registration. The pop-ups will guide user to choose:

i) A unique password that they never chose before.
ii) Which is not predictable.
iii) Has not been leaked in other data branches.

3- Connecting other apps

Through our personal experiences and some research we realised that we as the users tend to choose the easy way and register for many other accounts through our existing social media accounts such as Facebook. Even though this decision helps the user to save some time it creates many other risks. It creates chain of accounts, whose security depends other accounts. Also, with registering through another social media app users give permissions to the app to have access to read their personal information such as their profile and friends. So, our pop-ups at this point of the registration will kindly suggest the user to register with e-mail and password to avoid extra potential risks and to keep their information as private as possible.

4-Location

One of the most common allowances that applications ask for is the location. Even though some applications can not function without location the user should be aware of what it means to allow an app to use their location. Through a pop-up with google maps pictures we aim to make the user understand the seriousness of the issue.

5- Camera/ Microphone/ Contacts/ Pictures

Our aim is to make users realise that this is their private sphere and they should be careful before simply allowing apps to reach their picture, contacts, camera etc.

6- Any information that the app continues to use

We believe that registration process of an app is crucial but also what happens afterwards is also important. User should be aware if the app continues to use their location even though they're not using the it. A pop-up will again make the user remind e.g. "X App is still using your location".

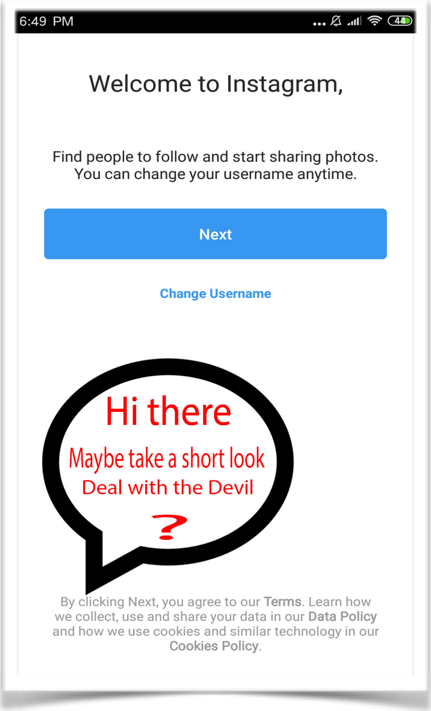
3 Method

Our plan is to create a mock-up application. Since we are going to be a background application, we will build our mock-up on the Instagram registration pages. We chose Instagram because it's one of the most popular social networks, and because the application asks for permission to accesses each part of the users private device.

The participants will Register to Instagram twice. Once with a normal registration and a second time with our mock-up application.

We will check and compare if our tips changed the way the user behaved and if he gave different permissions or different passwords to the registration.

While designing the mock-up application, we will test if it's better to go with more informative pop-ups, which would be less usable, or just small comments, which would be less informative.



6:49 PM

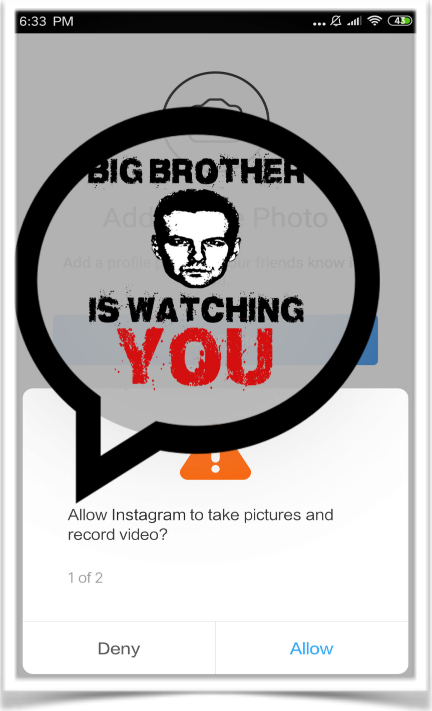
Welcome to Instagram,

Find people to follow and start sharing photos.
You can change your username anytime.

Next

Change Username

By clicking Next, you agree to our Terms. Learn how we collect, use and share your data in our Data Policy and how we use cookies and similar technology in our Cookies Policy.



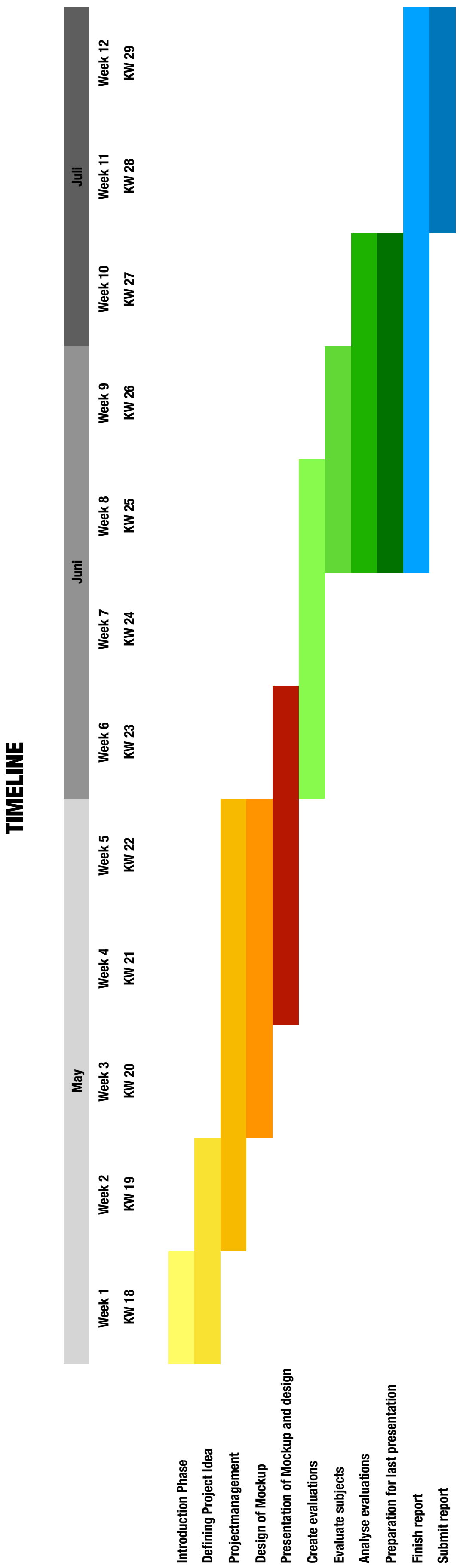
6:33 PM

Allow Instagram to take pictures and record video?

1 of 2

Deny Allow

4 Timeline


TIMELINE
May
Juni
Juli
Week 1
KW 18
Week 2
KW 19
Week 3
KW 20
Week 4
KW 21
Week 5
KW 22
Week 6
KW 23
Week 7
KW 24
Week 8
KW 25
Week 9
KW 26
Week 10
KW 27
Week 11
KW 28
Week 12
KW 29
Introduction Phase
Defining Project Idea
Projectmanagement
Design of Mockup
Presentation of Mockup and design
Create evaluations
Evaluate subjects
Analyse evaluations
Preparation for last presentation
Finish report
Submit report

5 Sources

Díaz, E (2016) The new European Union General Regulation on Data Protection and the legal consequences for institutions, Church, Communication and Culture, 1:1, 206-239, DOI: 10.1080/23753234.2016.1240912

La Porta, L. (2019, 22. April). How do iOS app permissions work?. Wandera. Retrieved from https://www.wandera.com/mobile-security/ios-app-permissions/

Dr. Wundere, F. (2019).Lesen Sie Datenschutzbestimmungen im Internet?. Statista. Retrieved from https://de.statista.com/statistik/daten/studie/189794/umfrage/lesen-der-datenschutzbestimmungen-im-internet/

Hunt, T. (2018 2 .MAY). 86% of Passwords are Terrible (and Other Statistics). Retrived from https://www.troyhunt.com/86-of-passwords-are-terrible-and-other-statistics/