BACHELOR THESIS

Bachelor of computer science

A Serious Game Helping Android Users to Make Their Devices More Secure

---

Supervisors:

Prof. Dr. Rainer Malaka

Dr. Karsten Sohr

Author:

Jonas Schmutte

[redacted]

Matrikelnummer: [redacted]

March 17, 2019

[This page intentionally is left blank.]

Declaration of Authorship

I hereby declare that I am the sole author of this bachelor thesis and that I have not used any sources other than those listed in the bibliography and identified as references. I further declare that I have not submitted this thesis at any other institution in order to obtain a degree.

Place, Date: _____

Signature: _____

[This page intentionally is left blank.]

Abstract

Granting to much permissions to applications on *Android* devices is a direct threat to it's user's security because it allows access to otherwise protected system features. Neither the *Android* menu nor the installation page for applications is providing sufficient and easy-to-get information about the consequences of granting dangerous permissions to applications. Therefore *Android* users need a way to get this information and to learn how to handle *Android* permissions as a whole. Serious games allow their players to learn while having fun and being engaged. With the goal of teaching the consequences deriving from granting *Android* permissions and to teach the way to change them on *Android* devices to it's players, the serious game *Make my phone secure!* is developed by integrating a rebuild of the original *Android* menu in a playful and explanatory environment. An empiric research is applied to analyze the influences *Make my phone secure!* has on its players. To analyze the significance of the game's influence it is compared to two other more basic variants, one representing the rebuild of the *Android* menu and the other one adding hints and explanations of *Android* permission's consequences to it. The commissioned study with 20 participants resulted in showing that all three variants are increasing the participant's results significantly, while it does not show significant differences between the different variants. Despite having an in average high prior knowledge, the participants found *Make my phone secure!* to be the most fun variant and to be more informative than the rebuild of the *Android* menu.

Contents

List of Figures

List of Tables

[This page intentionally is left blank.]

Chapter 1

Introduction

1.1 Motivation

Statistics in 2017 have shown that 81% of the German population over an age of 14 used smartphones [1], while a study from 2012 suggests that only 17% of the *Android* users pay attention to the permissions that they grant to application during install-time [2]. The users allow unrestricted access to photos, videos and contacts, as well as to location data, camera and microphone of the device, which allows the applications to send the user's sensitive data to its companies servers.

An example of a permission abusing application is the official application of the Spanish soccer league called *La Liga - Spanish Soccer League Official*. With the permissions to access the microphone and the location of its user's phone, specifically called RECORD_AUDIO and ACCESS_COARSE_LOCATION in *Android*, the application is localizing and identifying bars, where soccer games are broadcast without permission [3, 4]. Because their conversations are taped on audio as well, it is a violation of the users privacy.

Another example taking the abuse of its permissions to an even higher level is the application *Flashlight LED Widget*. At launch, the application asks for device administrator rights, the permission to draw over other applications, SYSTEM_ALERT_WINDOW, and the permission to access usage statistics, PACKAGE_USAGE_STATS [4, 5]. With these permissions, it is able to hide it's menu icons to appear like a normal widget [5]. But the application's main goal is not to give the users the functionality of a flashlight, instead it is able to steal their banking credentials [5]. To avoid being targeted by this kind of malware attacks, Stefanko [5] suggests to look at the permissions and rights an application requests precisely [5].

The consequences deriving from giving a permission are never stated directly and are most of the time not obvious to understand. Since the users are asked to make decisions, which consequences they do not understand [6], they need to learn the principal behind dangerous *Android* permissions to make more based decisions.

Therefore users, who have not enough knowledge to make those based decisions, need a tool to learn in a motivating and engaging way. With serious games, general users can learn while having fun doing so [7].

In 2002 the US Army released a recruiting tool in form of a video game called *America's Army*. Even though its main purpose was to raise the attention of possible recruits and test their suitability,

this serious game was studied to see if it is usable for actual army training purposes [8, 9]. A staff sergeant from Fort Benning, told the *America's Army*'s booth staff at the Army's annual AUSA Conference in Washington, DC, that they in Fort Benning love the game and use it for training the soldiers [9]. For example new recruits, who had trouble at the rifle range or obstacle course, had to play *America's Army* [9]. After completing related levels in game, they were allowed back to the range and usually passed it this time [9]. In addition comments from mothers indicate that their children, who played *America's Army* many hours per day, were motivated to learn about the US Army, since they knew everything about it from the game [9].

From these examples it can be suggested that serious games are a suitable tool to help *Android* users learn about consequences of *Android* permissions.

1.2 Google's Presentation of *Android* Permissions

The problem of granting to much permissions to *Android* applications begins with how *Google* is presenting the permissions before the installation of an application in their *Play Store*. Users have to search themselves through multiple pages to find information about the permissions an application requests. They at first see the page, presented in figure 1.1, where they can directly install the application. A prominent feature of this page is the rating information. Interestingly the *La Liga - Spanish Soccer League Official* application has a 4.5 star rating, which suggests general users that they can trust the application and install it. As already mentioned, this application showed that it can be dangerous if users do not pay attention to the permissions' dialog. Pressing the "INSTALL"-button will immediately install the application, without any notification window. When the user presses the "Read more"-button, a lot of information will be presented to them, see figure 1.2. Not until scrolling to the very end of the page, the user can see a "See More"-button under the title "App permissions".

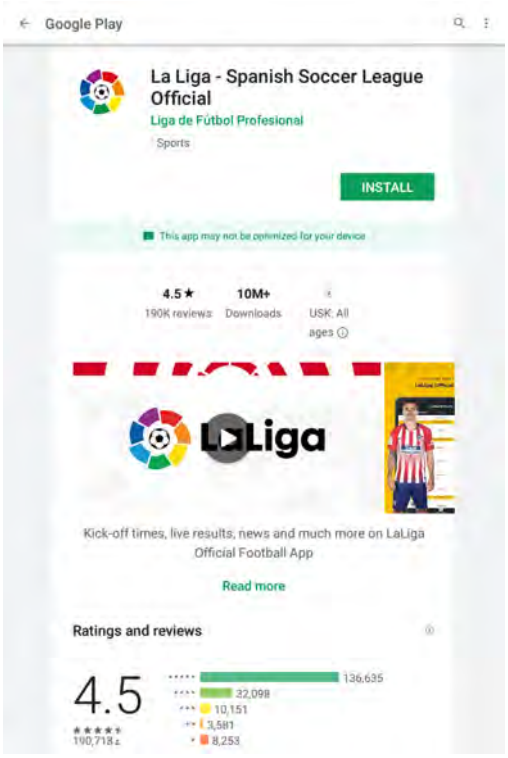

Figure 1.1: The *Play Store*'s installation page of the application *La Liga - Spanish Soccer League Official*.

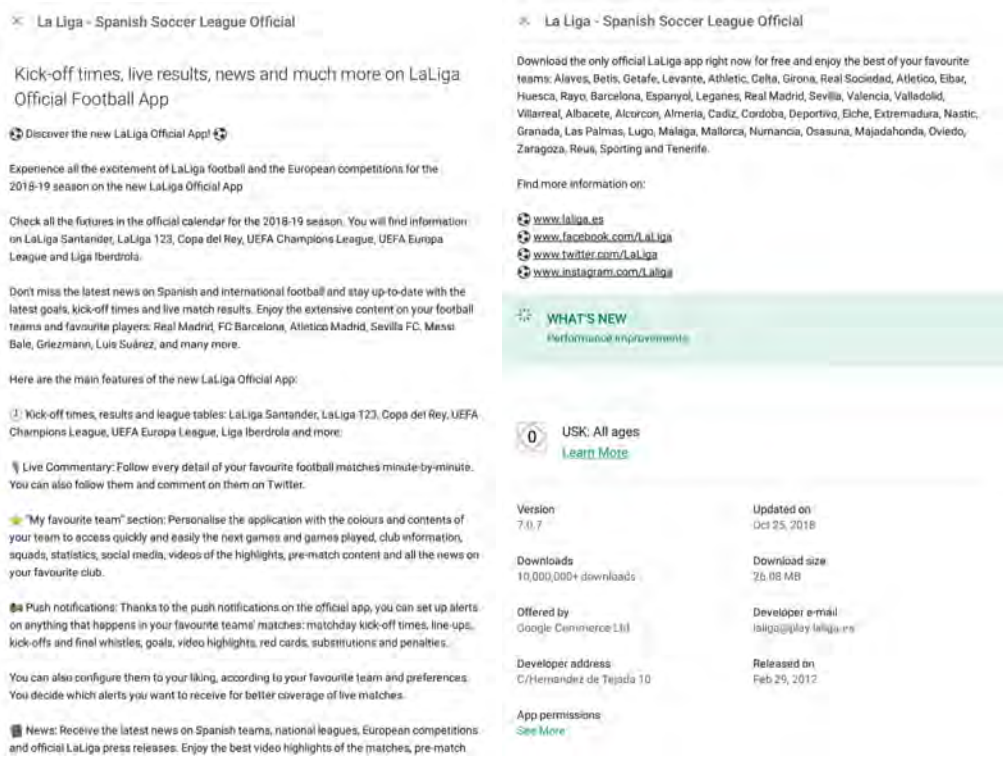

Figure 1.2: The *Play Store*'s information page for the application *La Liga - Spanish Soccer League Official*.

When pressed a list of permissions the application may request will appear as shown in figure 1.3. But it states little information about what the application is allowed to do with this permissions or what kind of information is made accessible to it. Regarding the microphone permission the ability to answer questions like "Can the application use the microphone any time or only when the user presses a button to record a voice message?" or "Is the user informed when the application uses the microphone or can it be used in the background?" is important for general users to evaluate the consequences of granting this permission. In addition, the applications can and will request permissions at runtime, see figure 1.4 for an example. This is opening even more questions like "How long does a user grant an permission?", "What happens if the user denies it?" or "How can the user grant or take the permission away afterwards?" for which general users should have answers for. However, this is not the only problem with runtime requests, such system dialogs are often ignored, because computer systems tend to use them too excessively, and therefore ineffective [10].

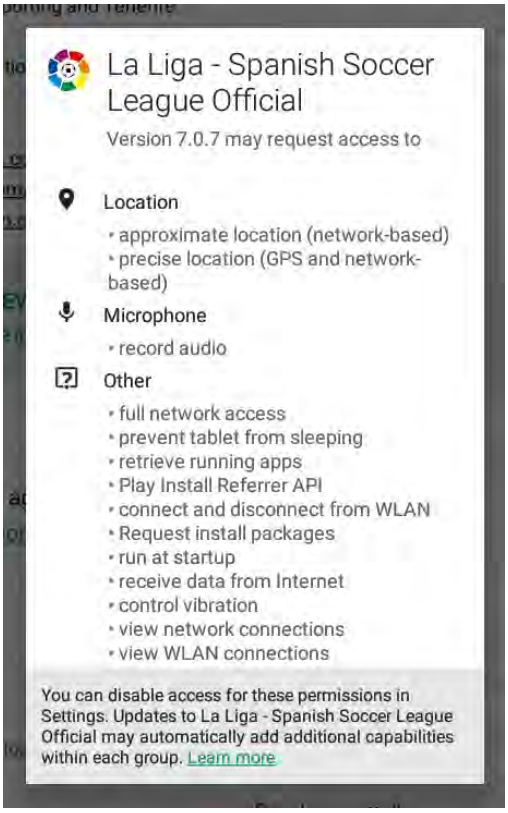

Figure 1.3: The *Play Store*'s permission page of the application *La Liga - Spanish Soccer League Official*.

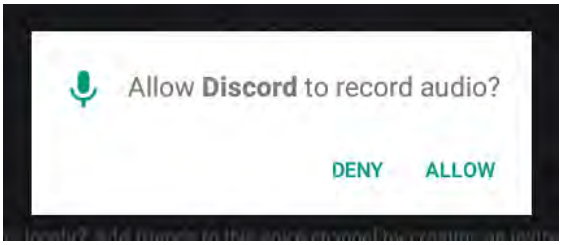

Figure 1.4: A runtime request of an application requesting the RECORD_AUDIO permission.

Another problem is that the navigation to the permission settings is not intuitive. In the menu, which is presented in 1.5, it is not clear where to navigate to. The permission settings would fit under both the "Security" menu and the "Apps" menu. The correct way to navigate begins with selecting the "Apps" menu to select the application and ends with then selecting the now showing "Permission" button. The now opening menu, shown in figure 1.6, does not show information about which information can be affected or accessed by the permissions and neither shows a complete list of all permissions the application has granted. It shows the applications' permissions which are categorized as dangerous by *Android* and editable by the user.

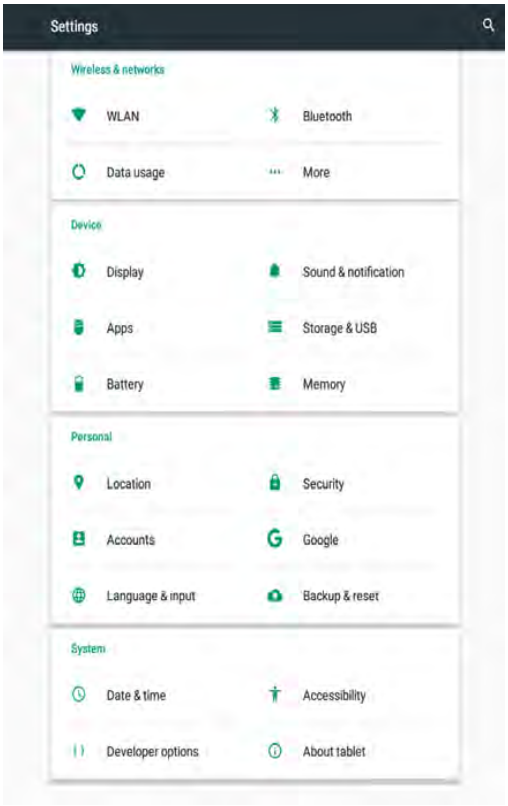

Figure 1.5: The original *Android* menu on a tablet with *Android* version 6.0.1.

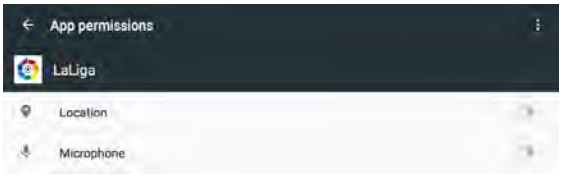

Figure 1.6: The permission settings for the application *La Liga - Spanish Soccer League Official*.

Clicking the button in the top right corner shows the menu entry "All permissions". Just under this hidden menu the user can see all permissions the application might want to have granted, see figure 1.7 for a visualization of this menu. Therefore the user can click on the permission and now sees a sufficient explanation of how it works, an example is presented in figure 1.8.
To sum up, getting information about the permissions an application may require at runtime or installation is hard to get without determination and experience. In addition, the information in runtime requests is not enough and ignored too easily.

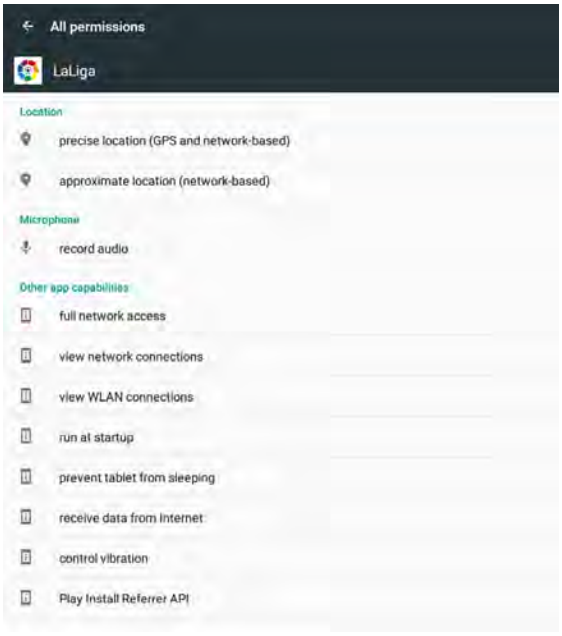

Figure 1.7: All permissions the application *La Liga - Spanish Soccer League Official* wants to have granted. All permissions under "Other app capabilities" are granted automatically on installation, while the permissions above are the permissions from the previous page.

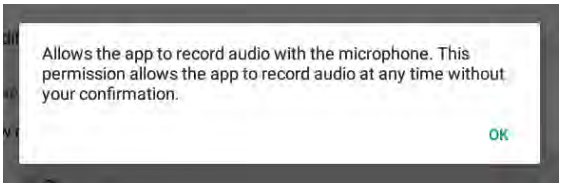

Figure 1.8: The information page of the RECORD_AUDIO permission.

1.3 Objective and Approach

Within the scope of this bachelor thesis it should be analyzed, how good players of a serious game learn the consequences of *Android* permissions and how good they can edit them on their own after playing it.

This brings up the following question:

> *Can we teach smartphone users to understand the consequences of permissions they give to applications and teach them how to change their own permissions by playing a serious game?*

To answer this question a serious game called *Make my phone secure!* will be developed. Its' aim is to let players learn which consequences derive from granting permissions, therefore raising awareness to this topic, and to show them a way to change their current and future *Android* permissions. In *Make my phone secure!* non playable characters (NPCs) come to the player's character in need of help with their smartphones. They ask the player's character to edit their *Android* permissions to fulfill one or more requirements, e.g. the application *La Liga - Spanish Soccer League Official* is not allowed to record audio. Depending on whether the player fulfills the task successfully, good or bad consequences are presented to him. In both cases the player gets explanations of what permissions caused the consequences and how they caused them.

Subsequently, a user study, which analyzes the knowledge enhancement about the consequences of *Android* permissions of a few participants, will be carried. The participants answer questions about what an application can do technically when granted a certain permission and what consequences could arrive from granting a permission, before and after playing the game. The knowledge improvement between the answers is analyzed to measure the learning progress. To analyze of what significance the aspect of playing a serious game is, two other variants are used to compare against. The first variant is a rebuild of the *Android* menu, while the second variant adds hints how to navigate to the permission settings and adds the explanations *Make my phone secure!* gives at the end of a level. This will be the foundation to evaluate the teaching success and therefore to answer the research question.

1.4 Structure of the Work

After introducing the topic and leading question of this work, an overview over the basic concepts follows in Chapter 2. This will represent the knowledge base for further procedures. In addition knowledge from literature and *Android*'s developer website will be summarized clearly and neatly. Chapter 3 is dedicated to the development of the serious game *Make my phone secure!*. The requirements it has to fulfill will be analyzed and it's design is portrayed and explained. In chapter 4, the study will be portrayed and a short description of how it was executed is given, while it's results will be evaluated in chapter 5. Chapter 6 includes a summary and a concluding review of the bachelor thesis. In addition, it will be determined whether all risen questions were answered and whether the defined objectives were achieved. In the end possible improvements will be described.

[This page intentionally is left blank.]

Chapter 2

Background

This chapter will introduce the basic concepts of this work. They will represent the knowledge base for the further procedures. In addition related work is presented.

2.1 Basic Concepts

Serious games

To understand serious games it is needed to first understand what video game are. According to Zyda [9], a video game is a *"mental contest, played with a computer according to certain rules for amusement, recreation, or winning a stake"* [9]. They are composed of story, art and software; the story builds up the game's entertainment, while the game's look and feel is defined by it's art [9]. The addition of pedagogy, to transmit knowledge and skill, is what makes video games serious [9]. The main aspect of serious games stays entertainment, but it is pedagogy which is essential to the games purpose [9]. To allow the success of this interplay, the teams working on the entertainment and pedagogy aspects of a serious game have to work closely together [9]. Since pedagogy is needed in a wide field, serious games have a big target group. This is how Zyda [9] came to his definition of serious games: A serious game is *"a mental contest, played with a computer in accordance with specific rules, that uses entertainment to further government or corporate training, education, health, public, policy, and strategic communication objectives"*[9]. It is to mention that as Susi et al. [7] state and as following from Zyda's [9] definition, every video game can be labeled as a serious game, if it is used for a pedagogic purpose [7, 9]. But serious games are not about teaching the players, they are about giving them a platform to learn [11]. To achieve this goal and to avoid that players learn wrong skills, the focus must be on the most important elements [7].

The usage of serious games has different advantages. Dangerous, cost or time intensive situations cannot always be simulated in the real world, so learners would not be able to experience them without the simulation in serious games [7]. In addition, Susi et al. [7] state that, serious games have the potential to improve *"analytical and spatial skills, strategic skills and insight, learning and recollection capabilities, psychomotor skills, visual selective attention, etc., and [...] provide an outlet to alleviate frustration [in form of violent games]"* [7]. *"Self-monitoring, problem recognition and problem solving, decision making, better short-term and long-term memory, and increased social skills, such as collaboration, negotiation, and shared decision-making"*[7] are even more potential benefits of serious games.

However, Susi et al. [7] also mention possible negative impacts of serious games like *"health issues (headaches, fatigue, mood swings, repetitive strain injuries, etc.), psycho-social issues*

(depression, social isolation, less positive behaviour towards society in general, increased gambling, substitute for social relationships, etc.), and the effects of violent computer games (aggressive behaviour, negative personality development, etc.)" [7].

Information security

Before the security problems of *Android* permissions are to understand, an introduction to information security is needed. Since this field is very broad the focus is set to parts relevant for this work. The task of information security is to protect their protégé from damage caused by confidentiality breaches, manipulations and denial of services [12]. Therefore different security goals need to be accomplished. The most relevant security goals for *Android* permissions are confidentiality, availability and privacy. Confidentiality means that unauthorized information gathering is not able to be accomplished [12]. Availability is the warranty that authorized usage is not disturbable [12]. Privacy describes the right to keep personal matters and relationships secret [13]. In addition, in Germany the right of informational self-determination, which guarantees the determination over the revelation and the utilization of one's data, applies [12].

Android permissions have different ways to injure these goals. In general not granting a permission will likely lead to a violation against the availability of an application's feature, but therefore lead to the realization of another security goal. As introduced allowing *La Liga - Spanish Soccer League Official*to access the microphone will lead to it listening to the users conversations, which is injuring the confidentiality between them and their conversation partners in addition to their privacies. A simple and probably wide known example of a violation to the right of informational self-determination is allowing an application the access to a phone's contacts via the READ_CONTACTS permissions. This allows an application to read the information of all contacts stored on a phone, including name, email and address next to the phone number. On this way applications gain information about persons who did not directly decided over their data's revelation.

Android permissions

To get access to users' sensitive data or particular system features *Android* applications have to request permission [14, Permissions overview]. These permissions are called *Android* permissions. Their purpose is to protect the privacy of Android users [14]. The permissions are split into

two categories, normal and dangerous permissions, depending on their risk to affect the user's privacy or the device's operation [14, Permissions approval]. Normal permissions are granted automatically, if an application lists them as needed, since they do not pose much risk for the user's privacy or the device's operation [14]. See table 2.1 for some examples.

Name	**Meaning**
BLUETOOTH	allows connection to paired bluetooth devices
INTERNET	allows connection to the internet
SET_WALLPAPER	allows to set the wallpaper
VIBRATE	allows usage of the vibrate function
SET_ALARM	allows to set alarms
USE_FINGERPRINT	allows usage of the fingerprint hardware
WAKE_LOCK	allows to keep the processor from sleeping or screen from dimming

Table 2.1: Examples for normal *Android* permissions
Source: AndroidDevelopers [4]

Dangerous permissions pose a higher risk, so the user needs to grant them explicitly [14]. This can either be at runtime, with *Android* 6.0 and higher, or at install-time, with *Android* 5.1.1 and below [14]. Examples are shown in table 2.2 at the end of this chapter.

Runtime requests as shown in 1.4 are prompted in form of a system dialog, when you open an application the first time or at the moment an application is needing the permission [14]. Users are able to block repeating requests, in case they do not want to grant the permission [14]. In addition, users can always enable or disable permissions in their system settings [14].

Install-time requests are prompted before users install an application [14]. They only give the option to grant all requested permissions [14]. Not accepting this will cancel the installation [14].

Normal permissions have rather obvious consequences, e.g. granting the SET_WALLPAPER permission will let the application change the phones wallpaper [4, SET_WALLPAPER]. It could annoy the user by changing it to unwanted pictures, but does not cause much harm.

In contrast, dangerous permissions are able to cause harm to the user or the *Android* system. With the READ_CONTACTS permission, e.g. a malicious application can obtain e-mail addresses from the user's contacts and send them an e-mail with malware, while pretending the e-mail

came from the user themselves [15]. The RECORD_AUDIO, especially in combination with other permissions (ACCESS_COARSE_LOCATION, CAMERA etc.), allows applications to observe the user, like the *La Liga - Spanish Soccer League Official*application, mentioned in the introduction [3].

Since the list of *Android* permissions is very long, it is not possible to cover all permissions in this bachelor thesis. The focus will lay on the permission groups portrayed in table 2.2, as Harbach et al. [16] found out that permissions like contacts, call log and photos are more relevant for users, than technical permissions like access to the list of available Wi-Fi networks [16].

Name	**Allows**
Permission group: CAMERA	
CAMERA	usage of the camera
Permission group: CONTACTS	
READ_CONTACTS	to read the data of all contacts on the phone
WRITE_CONTACTS	to write data to all contacts on the phone
Permission group: LOCATION	
ACCESS_FINE_LOCATION	access to the approximate location
ACCESS_COARSE_LOCATION	access to the precise location
Permission group: MICROPHONE	
RECORD_AUDIO	the recording of audio
Permission group: PHONE	
READ_PHONE_STATE	reading the phone number, current cellular network information and the status of outgoing calls
Permission group: SMS	
READ_SMS	to read SMS messages
WRITE_SMS	to write SMS messages
Permission group: STORAGE	
READ_EXTERNAL_STORAGE	to read the external storage
WRITE_EXTERNAL_STORAGE	to write on external storage

Table 2.2: Examples for dangerous *Android* permissions

Source: AndroidDevelopers [4], AndroidDevelopers [14, Permission groups]

2.2 Related Work

The works of Harbach et al. [16] and Wen et al. [17] build the foundation for the idea of *Make my phone secure!*.

To raise awareness and cautiousness while installing applications, Harbach et al. [16] rebuilt the *Android* app store in an experiment. The app store now showed users personal examples of consequences of permissions, such as which personal photos an application can access and delete, when they tried to install an application [16]. The participants' feedback suggests that the personal examples are engaging to reflect the consequences of those permissions [16]. In addition, their study indicated that the participants were learning what permission sets are reasonable for an application's purpose [16].

Wen et al. [17] developed a serious game named *What.Hack* with the goal of training employees a better handling of phishing mails. In *What.Hack*, the player has to rate business emails as phishing or normal mails, with an increasing amount of rules, restricting what is allowed in a business mail [17]. This way to play seems to be a good example of how to let the player learn an unknown topic.

Both works of Bravo-Lillo et al. [10] and Stoll et al. [6] are engaged in giving users the possibility to make easier and better security decisions.

Therefore Bravo-Lillo et al. [10] added user-interface modifications (attractors) to computer system dialogs with the goal to *"draw users' attention to the most important information"* [10]. In their experiments their participants were asked to install and grant permissions to software, one group with and one without the attractors [10]. The results showed that the attractors did significantly decrease the likelihood of participants installing and granting permissions to software, where clues were indicating that the publisher might not be legitimate [10].

Similar to this, Stoll et al. [6] decided to help users making security decisions with more visual informations. Their tool *Sesame*, a graphical security user interface, connects the known Windows interface with processes, portrayed as little boxes [6]. These are expandable to present extended information understandable for non-expert users. In a study with 20 participants, they analyzed the difference between security decisions of users made either using or not using *Sesame* [6]. The results suggest that *Sesame* succeeds in helping users to make better security decisions [6].

Visualizing what a system dialog means therefore seems to be a good approach to let users make better security decisions.

Hamari et al. [18] analyzed how flow, engagement and immersion affect learning in game-based learning environments [18]. Therefore data gathered from players of two learning games, *Quantum spectre* and *Spumone*, is investigated [18]. In both of these games the player has to apply knowledge from an engineering dynamics course [18]. The results suggest that learning is improved by engagement and the difficulty of the game, while immersion does not seem to have a significant effect [18]. This should be taken into account while designing *Make my phone secure!*.

Felt et al. [19] analyzed the security behind *Android* permissions, they built a tool called *Stowaway* to analyze *Android* applications for over privileges. In this case to have over privileges means that an *Android* application asks for more permissions than it would need for its usage. They applied it to 940 applications and found over privileges in about a third of them [19]. Further analysis showed that this is only caused by an overuse of a few permissions and can be traced back to developer confusion [19]. This shows that not every permission that is asked to much for the normal usage of an application must indicate a malicious intent.

Gechter et al. [20] investigated how big their simulation game's impact on operations management education were [20]. In their simulation game, *HECOpSim*, the player needs to manage a manufacturer involving decisions on the amount of raw materials to purchase, on the number of subassemblies and finished products to assemble and on the hiring and layoff plans [20]. They analyzed the learners' progression in mistakes and a simulated firm's performance, while standard lectures and problem-solving exercises were also taking part [20]. While their results show that the effect on learner's who already mastered the field of operations management through traditional learning methods was small, users for which traditional methods are insufficient had an significant increase of decision-making skills from the simulation game [20]. In case of complex decisions which are hard to understand without experiencing them, *HECOpSim* had a positive impact [20]. This underlines the effect of simulation in game-based learning environments and suggests that the simulation of the *Android* menu will be able to have an effect on the learners.

Chapter 3

The Serious Game:

Make My Phone Secure!

Based on the research question “Can we teach smartphone users to understand the consequences of permissions they give to applications and teach them how to change their own permissions by playing a serious game?” we designed and developed the serious game *Make my phone secure!*. After stating it’s general idea and requirements it has to fulfill, the level and game design of *Make my phone secure!* will be summarized and illustrated. It was developed and build with the Unity Engine of version 2018.3.0f2 (see https://unity3d.com/de) and was tested on a Lenovo Tab2 A10-30 with *Android* version 6.0.1, which was also used to take the screenshots displayed in this work.

3.1 General Idea

The player of *Make my phone secure!* should learn what the consequences of granting *Android* permissions are and how to enable and disable them. Therefore those ideas of Harbach et al. [16] and Wen et al. [17] are combined. The player will take the role of an IT-specialist, who is responsible for making the *Android* devices of his customers secure. The customers come to him with different expectations of what applications should be able to do on their phones. The player then has to edit those permissions to fulfill the customer's expectation. After giving back the customers phone, the player will see either the bad or the good consequences the customer will have to face. In case the player has disabled the corresponding permission, the customer will come back happily, remarking how good the player was. In the other case, the customer will come back sadly and remark how bad the consequences are.

3.2 Requirement Analysis

In order to let the player learn effortless and effectively, the game has to fulfill specific requirements. When the game does not represent the *Android* system accurately, the players cannot learn how to edit the permissions on the original *Android* menu. The applications shown in the game also have to be representative for well-known applications, to allow the players to translate them to applications they have installed or want to install on their own devices. In addition, the stories have to be immersive and engraving, but also realistic, to let the player feel like they could be the stories' protagonist. To yield a simple start, the game must have easy-to-learn and easy-to-understand game mechanics, otherwise players could not want to get into the game. Also the game's playtime cannot be to long, because otherwise the player could lose the interest in playing. Furthermore, the game needs to stay motivating and entertaining over the course of its playtime. To give the game a good usability, its design needs to fulfill the Design Principles of Norman [21] and consider the Designing for Error of Lewis and Norman [22]. The current game status, the available actions and the results of actions should be clear [21]. The results of actions should also have clear and continuous feedback [21]. In addition, the relations between the users' actions and the achieved results needs to be natural and unique [21]. Furthermore, players will make errors while playing, as Lewis and Norman [22] describe that design needs to consider that errors will occur. So the design of the game needs to grant the players a possibility to avoid

and avert errors and a possibility to identify and understand the errors to enable them a way to treat the errors [22]. To reach a huge target group, the game has to be usable on many different *Android* devices. This means it has to be able to run on different *Android* versions and to scale to different aspect ratios, these describe the proportional relationship between the width and hight of the device's display.

3.3 Level Design

For the game three levels "Instagram hears my conversations", "Flashlight could steal my data" and "ShoppingToGo sends spam messages"are designed.

The Level "Instagram Hears My Conversations"

The Level "Instagram hears my conversations" is about the application *Instagram* and the MICROPHONE permission group. In *Android*'s play store, *Instagram* describes itself as *"[...] a simple way to capture and share the world's moments. Follow your friends and family to see what they're up to, and discover accounts from all over the world that are sharing things you love. Join the community of over 1 billion people and express yourself by sharing all the moments of your day — the highlights and everything in between, too"* [23]. In the *Instagram* application users see advertisements while looking at different photographies or videos of other users. This level tells the story of how *Instagram* is presenting personalized advertisements to the customer, while having *Instagram* on their phone with an enabled RECORD_AUDIO permission. For the customer, the presented advertisements seem obviously based on their conversations with other people and therefore they want *Instagram* to stop using their conversations. The good consequence of this level is that *Instagram* stopped basing the presented advertisements on the customers conversations, while the bad consequences are that *Instagram* still does it. The good and bad consequences are portrayed in figure 3.1.

The Level "Flashlight Could Steal My Data"

In the level "Flashlight could steal my data", a flashlight widget called *Flashlight* and the STORAGE permission group are the levels topic. *Flashlight*'s function is to use the camera's flash as a normal flashlight. The story told in this level is about *Flashlight* actually stealing

data from the phone when it is granted the READ_EXTERNAL_STORAGE permission. The customer heard that there actually is a flashlight widget on the market which steals data from its users and wants to avoid that his own data is stolen by his flashlight application. As the good consequence the player gets presented that the customer's data was not stolen. The bad consequence is that the customer's data got leaked on the Internet. These consequence are also presented in figure 3.1.

The Level "ShoppingToGo Sends Spam Messages"

The topic of the level "ShoppingToGo sends spam messages" is the application *ShoppingToGo* and the READ_CONTACTS permission. *ShoppingToGo* is a fictional application where users can buy different products from a wide selection, but it is also using the contact information from their users' phones to send a lot of advertisement messages to contacts of their users when granted the corresponding permission. This is the basis for this level's story. The customer got a lot of those messages themselves and since they also use *ShoppingToGo*, they want to avoid that their contacts will receive these messages as well. The good consequence is that the email accounts of the customer's contacts are not receiving a lot of messages, while the bad consequence is presenting those email accounts filled with messages, see figure 3.1.

Requirement Discussion

The applications used, *Instagram*, *Flashlight* and *ShoppingToGo* are directly found or at least easily comparable to applications found on many *Android* devices, so players should be able to translate these to applications on their own devices or at least to websites they use.
The stories of these levels are kept simple and realistic to allow the players to immerse into them. Therefore the levels fulfill the level specific requirements, established in the section *requirement analysis*.

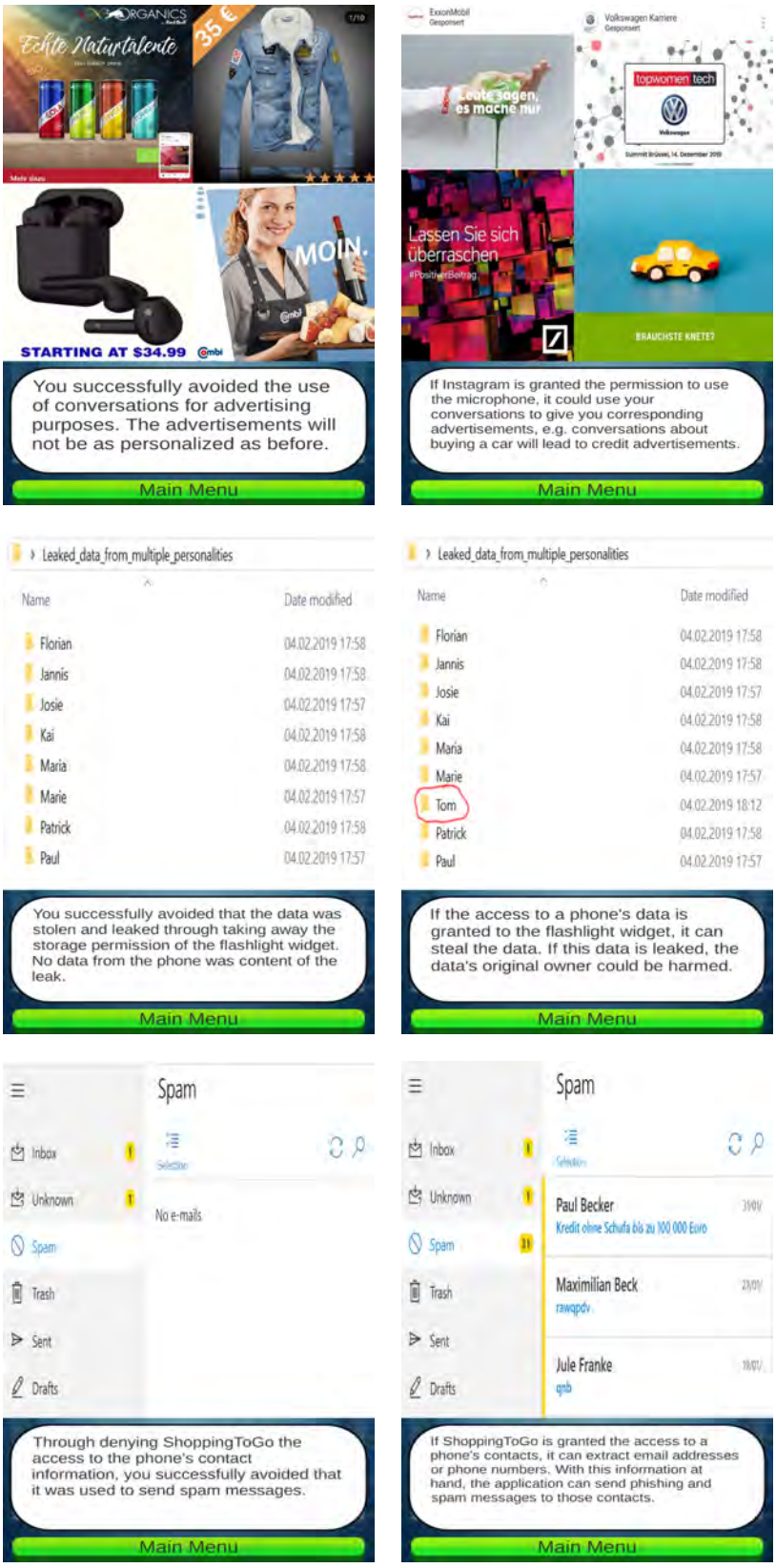

Figure 3.1: The good (left) and bad (right) consequences of Level “Instagram hears my conversations” (top), “Flashlight could steal my data” (middle) and “ShoppingToGo sends spam messages” (bottom) as portrayed in *Make my phone secure!*. The pictures presented within this screenshots are self taken screenshots from the *Windows* explorer and from the applications *Instagram* and *WEB.DE*.

3.4 The Game's Design

The Start Screen

The game starts with a welcome screen which is presented in 3.2 together with a level selection which opens by clicking the "Select level" button on the welcome screen and is focused to allow a quick change between the three levels 1, "Instagram hears my conversations", 2, "Flashlight could steal my data"and 3, "ShoppingToGo sends spam messages" and between the three variants A, the rebuild of the *Android* menu, B, the rebuild of the *Android* menu with hints and positive and negative consequences, and C, the actual game *Make my phone secure!*. Variants A and B will be further described in section 4: Research. Clicking the "Sources" button will open a window referencing to the used sound files' origination and clicking the "End game" button will close the game. Selecting a level or a variant via the level selection screen is done by clicking on the corresponding button. Clicking the *Start* button starts the currently selected level and variant combination.

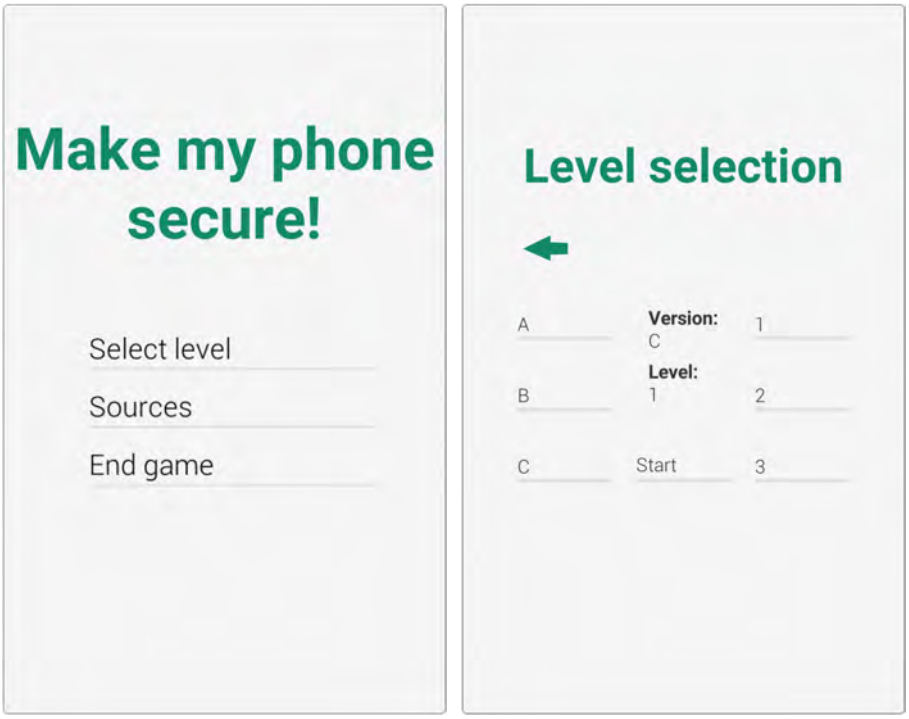

Figure 3.2: The welcome screen (left) and the level selection screen (right) of *Make my phone secure!*.

Start of A Level

The game starts with an introduction of the customer NPC who tells the player about his problem. The player then can start the level by pressing the "Let's Start!" button in the bottom right corner. Screenshots of this screen for the different levels are presented in figure 3.3. The purpose of this screen is that the player gets an overview over the customer's problem and over what kind of permissions might be the correct ones to change.

Figure 3.3: Customer introductions from the levels "Instagram hears my conversations" (left), "Flashlight could steal my data" (middle) and "ShoppingToGo sends spam messages" (right). The characters are build with a character creator from the *Unity Asset Store* called *Fantasy Heroes: Character Editor* [*Basic*] and developed by HIPPO, see https://assetstore.unity.com/packages/2d/characters/fantasy-heroes-character-editor-basic-88537, accessed 2019-05-03, for reference.

Android Menu

After this a rebuild of the *Android* menu will open, see figure 3.4 for a comparison with the original *Android* menu. It simulates the navigation of the original *Android* menu precisely and therefore allows the players to learn navigation routes through the original *Android* menu.

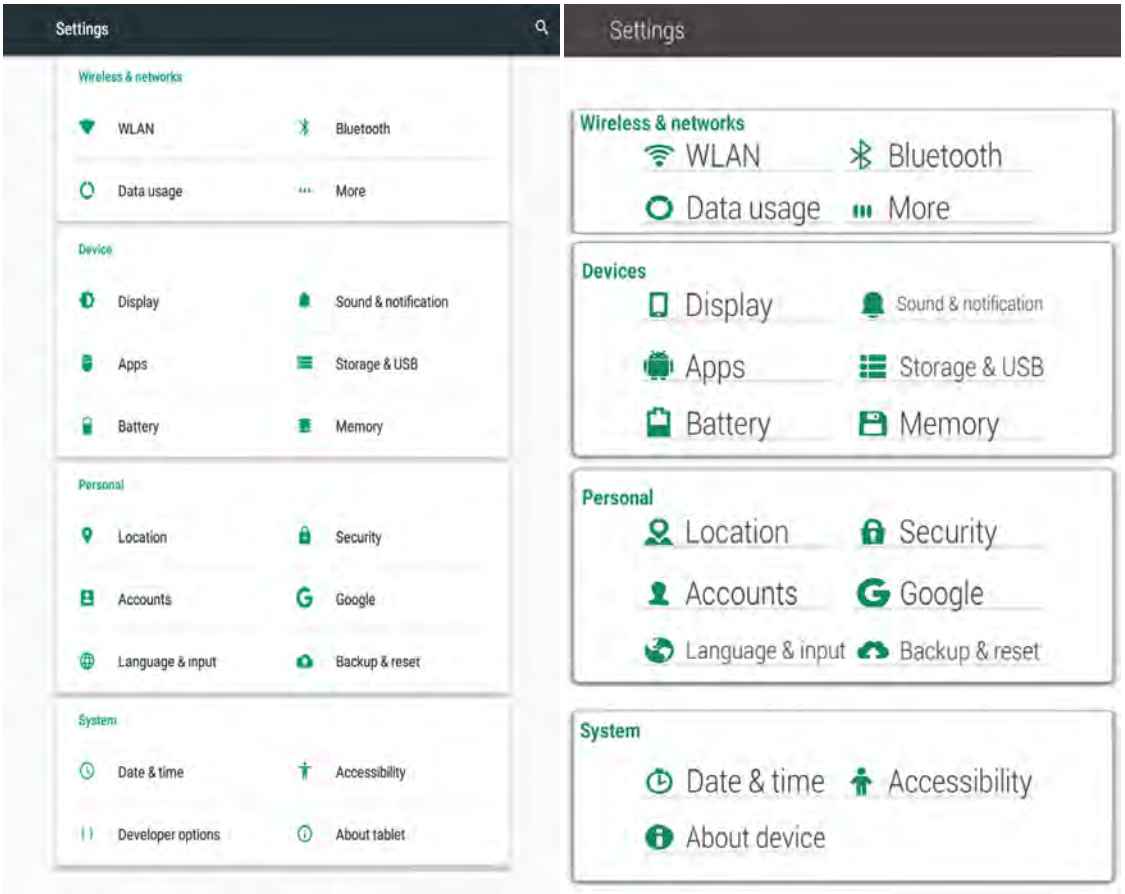

Figure 3.4: Comparison of the original *Android* menu (left) and the rebuild menu in *Make my phone secure!* (right). The original menu originates from *Android* version 6.0.1 on a Lenovo Tab2 A10-30.

Progress bar

In addition the customer NPC shows up in the bottom of the screen, giving a short summary of his problem. Above the NPC a progress bar will tell the player how good they are progressing through the level. The bar fills every time the player does correct actions and is emptying itself every time they takes incorrect actions. It's neutral color is yellow, while its turning green when nearly full and red when nearly empty. In figure 3.5 these status bar is presented like it is appearing in the different levels "Instagram hears my conversations", "Flashlight could steal my data" and "ShoppingToGo sends spam messages".

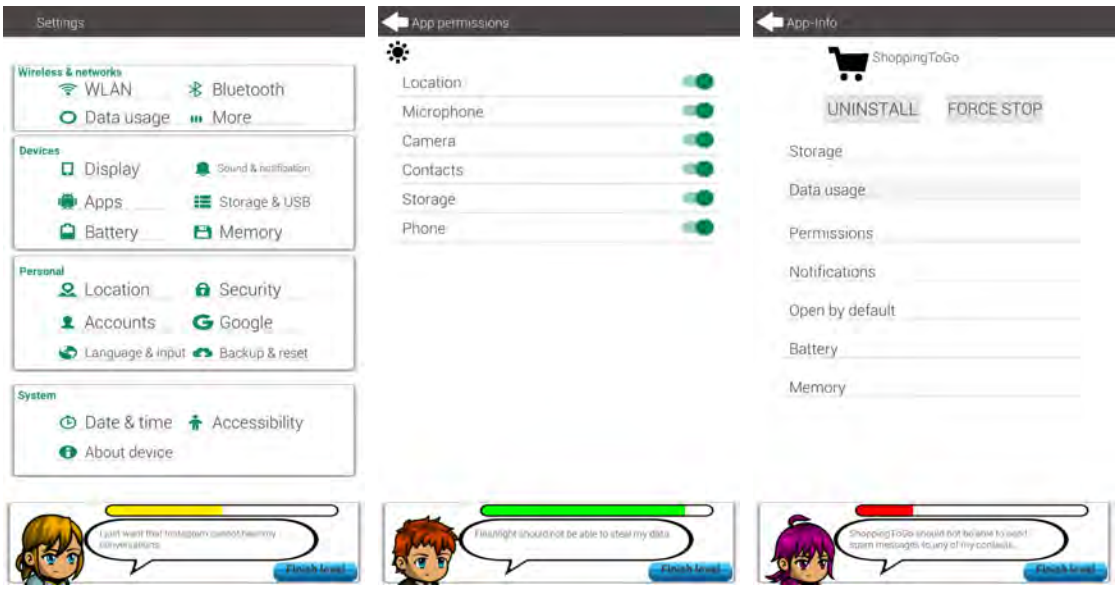

Figure 3.5: Progress bars as they are appearing neutrally filled in level "Instagram hears my conversations" (left), positively filled in level "Flashlight could steal my data" (middle) and negatively filled in "ShoppingToGo sends spam messages" (right).

Feedback

In addition to the progress bar responding to correct or incorrect actions, correct actions will lead to a green flash animation and the customer NPC to respond with positive feedback. In case of an incorrect action a red flash animation will play, the customer NPC will respond with negative feedback and additionally the device will vibrate. The animations are displayed in figure 3.6. The desired effect of this is that the player identifies his errors and is able to eradicate them.

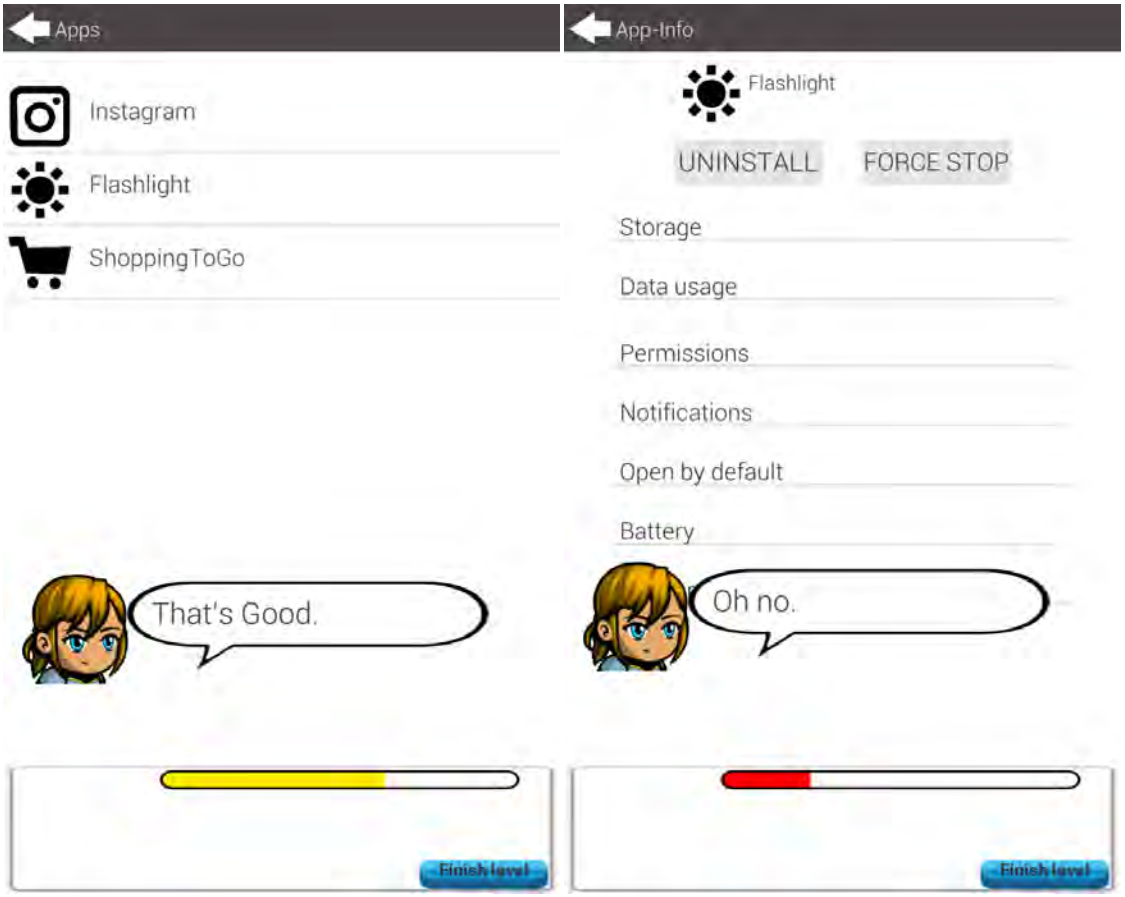

Figure 3.6: The positive feedback animation (left) and the negative feedback animation (right) as appearing in level “Instagram hears my conversations”.

Submenus

Navigating from the “Settings” menu into a different submenu than the “Apps” submenu is not understood as an incorrect action, because the player should be able to explore the different submenus without feeling pressure. Only pressing incorrect buttons in any of the submenus is understood as an incorrect action Opening the “Apps” submenu is considered a correct action and will open a list of the installed applications, as portrayed in figure 3.7. Here the player is able to select the application of which he wants to change the permission settings.

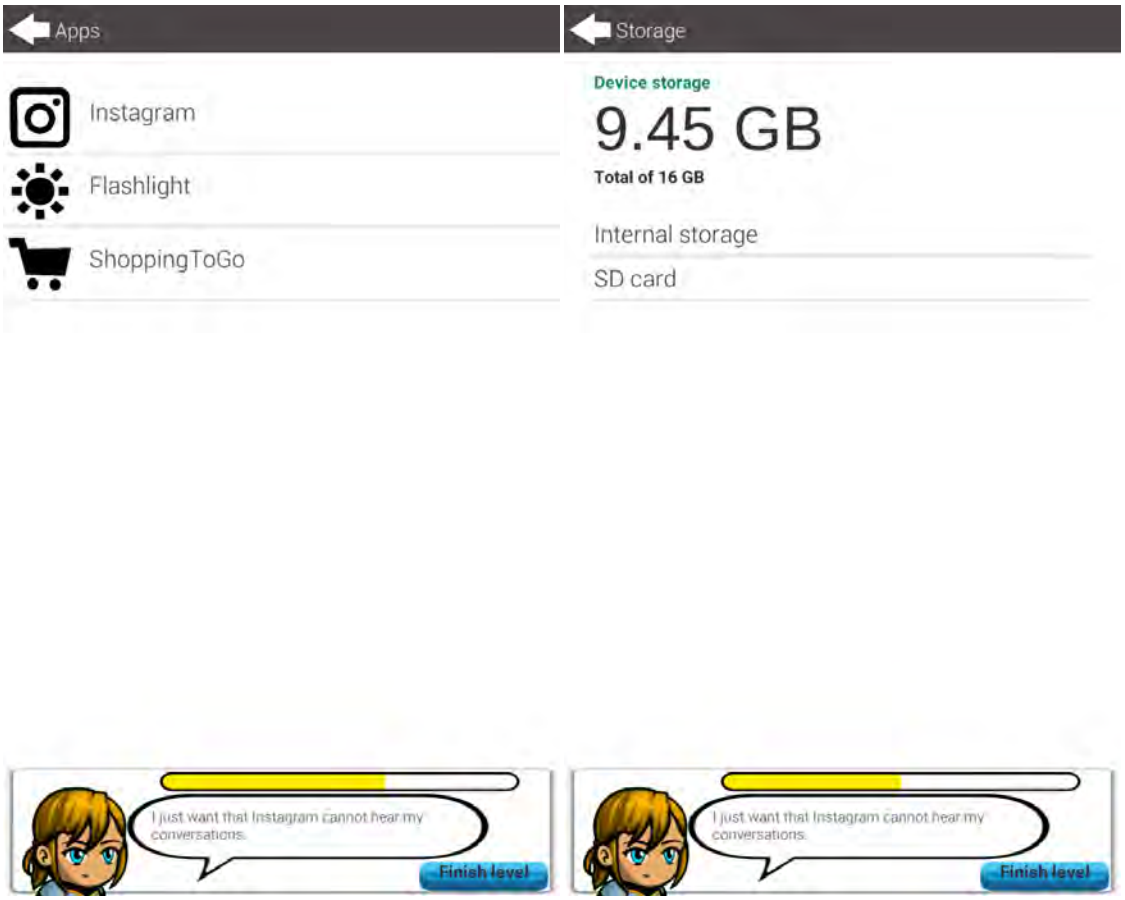

Figure 3.7: The “Apps” submenu (left) showing the installed applications and the “Storage” submenu (right) as examples for different submenus in the rebuild *Android* menu.

Navigation

When the player has selected an application from the list of installed applications, he can now navigate from the “App-Info” submenu to the “App permissions” submenu to turn off the permissions. These submenus are portrayed in figure 3.8.

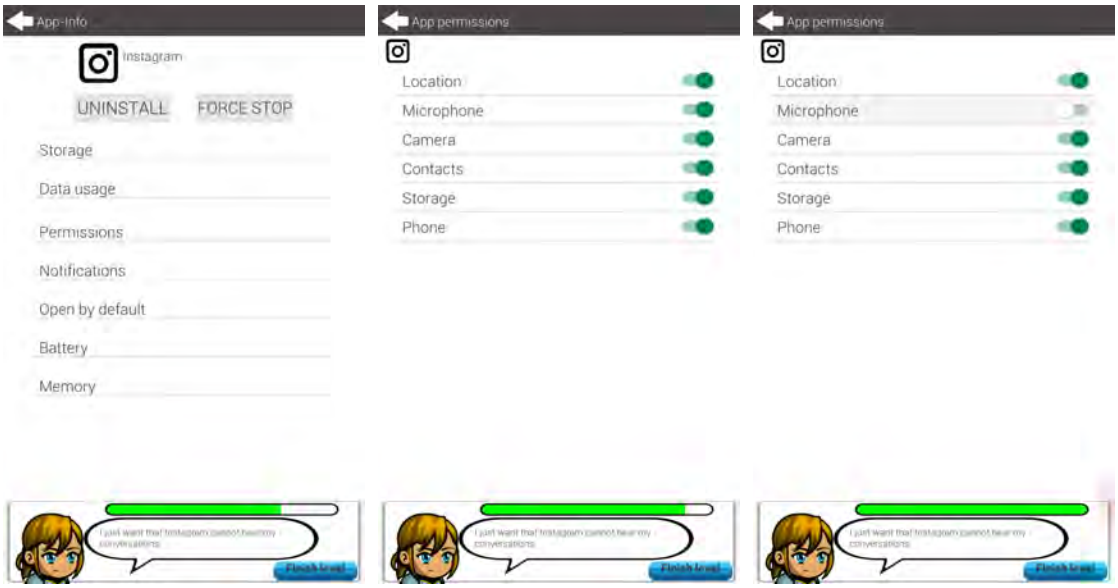

Figure 3.8: The “App-Info” submenu (left), the “App permissions” submenu with all permissions granted (middle) and the “App permissions” submenu after turning off a permission (right).

End Screen

The next step is to press the “Finish level” button on the bottom right corner. This opens a screen with a “Continue” button which leads to the return of the customer NPC in form of an end screen portraying either a success or a loose scenario, these are presented in figure 3.9 and figure 3.10. The player gets a different score, in form of a three star scale, based on the amount the progress bar was filled. The goal is to motivate the player to find and therefore learn the most effective way of editing the permissions and to motivate him to complete the level again for a higher score. In addition, a sound effect, which emphasizes the respective scenario, will play. For license information of the sound files see the “Source References” file on the appended CD.

Figure 3.9: Customer success scenarios as presented in the levels “Instagram hears my conversations” (left), “Flashlight could steal my data” (middle) and “ShoppingToGo sends spam messages” (right)

Figure 3.10: Customer failure scenarios as presented in the levels “Instagram hears my conversations” (left), “Flashlight could steal my data” (middle) and “ShoppingToGo sends spam messages” (right)

Explanation

Pressing the "Explain" button on the bottom right corner of the different scenarios will present the consequences displayed in figure 3.1 corresponding to the current level. The failure scenario will present only the bad consequences, while the success scenario will first present the bad and then following the good consequences.

Requirement discussion

As figure 3.4 shows the rebuild *Android* menu is very similar to the original *Android* menu, therefore players should be able to learn how to change the permissions of an application. However, this effect has to be proven by the study carried out within this work.
The game mechanics of *Make my phone secure!* are very simple, its basically the *Android* menu navigation plus buttons to progress through the game. This allows players a simple start.
The levels and therefore the time a player needs to complete the game are kept short to prevent players from getting bored. This is another requirement the study will have to prove later on.
To fulfill the Design Principles of Norman [21], every action the player takes in the game gives respective and clear feedback like the animations in figure 3.6, the green or red flashes and the vibration of the device. In addition, the actions a player can take in the *Android* menu are as clear as the original menu allows and the other buttons have descriptive labels, which are making their actions' results clear. Features considering the Designing for Error of Lewis and Norman [22] are the explanations in the bad consequences, as presented in figure 3.1. They explain to the player what the error leading to the failure scenario was and how to make it better. In addition, the adding of negative feedback on incorrect actions tells the player what his errors in navigating through the *Android* menu are.

Conclusively, the game's design fulfills the requirements established in section 3.2: Requirement Analysis.

Chapter 4

Research

To analyze how good players of *Make my phone secure!* are learning the consequences of *Android* permissions and how much they improve on their ability to change *Android* permissions on the original *Android* menu an empiric research is applied.

4.1 Methodology

The main aspect to answer by this study is the research question.

> *Can we teach smartphone users to understand the consequences of permissions they give to applications and teach them how to change their own permissions by playing a serious game?*

The research question consists of two main parts in which it will be split into as hypotheses. These then have to be confirmed in course of this study.

> **Hypothesis 1:** Players of *Make my phone secure!* will understand which consequences derive from granting permissions to an application significantly better than before playing.

> **Hypothesis 2:** Players of *Make my phone secure!* will be able to change the permissions given to applications on *Android* devices more comfortable than before playing.

Understanding consequences deriving from granting specific permissions requires knowledge about what an application can do with a granted permission on a technical level, e.g. an application with the microphone permission is able to record audio whenever it wants, and the ability to evaluate what consequences could derive from granting a permission to an application, e.g. using recorded audio to present personalized advertisements. Therefore hypothesis 1 is split into these two parts.

> **Hypothesis 1a:** Players of *Make my phone secure!* will understand what granting a permission allows an application to do technically significantly better than before playing.

> **Hypothesis 1b:** Players of *Make my phone secure!* will be able to evaluate what uses a permission can have for an application significantly better than before playing.

However, only confirming these hypotheses will not provide information about how significant it was to actually play a serious game. Therefore two other variants are introduced. One

variant, from now on named variant A, will only contain the rebuild *Android* menu, a task and feedback showing whether the task was completed successfully, as presented in figure 4.1. The second variant, variant B, equals variant A, but gives hints on incorrect actions and explains the consequences of *Android* permissions referred to in the current level the same way as *Make my phone secure!* does. Screenshots of this variant are presented in figure 4.2. Variant C is the actual game *Make my phone secure!* as described in section 3.4: The Game's Design.

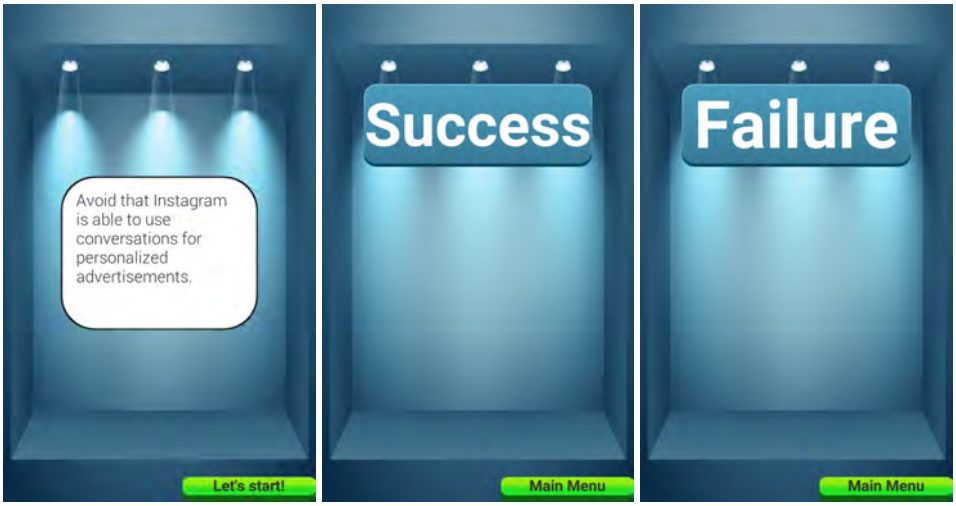

Figure 4.1: Screenshots from variant A showing a given task (left), the success feedback screen (middle) and the failure feedback screen (right).

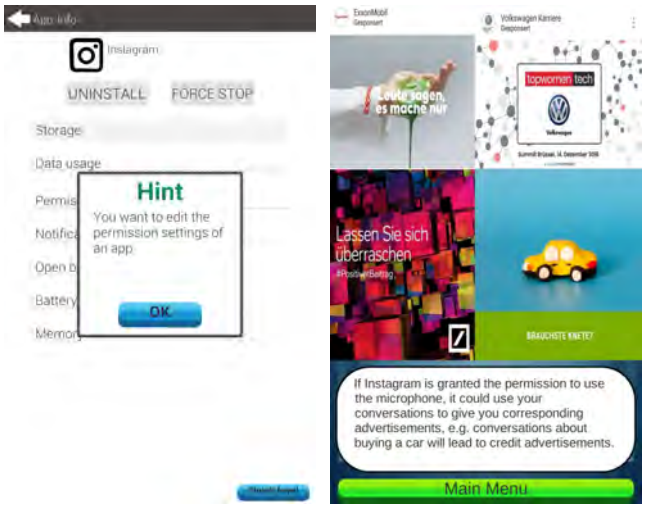

Figure 4.2: Screenshots from variant B showing an added hint (left) and an added consequence (right).

The three variants raise different expectations in teaching the participants, leading to further hypotheses.

> **Hypothesis 3:** *Make my phone secure!* will have the highest affect in improving the participants results.

> **Hypothesis 4:** *Make my phone secure!* will be the most informative and fun variant.

Consequently, the variants have to be compared. Since the amount of participants should be held relatively small, every participant plays every variant, leading to a need of different but equivalent levels, therefore the three introduced levels will be used and labeled with a number, 1 for "Instagram hears my conversations", 2 for "Flashlight could steal my data" and 3 for "ShoppingToGo sends spam messages". To avoid nuisance factors and allow the experiment with a relatively small number of participants the *Latin square design* is used [24]. This is *"a method of placing treatments so that they appear in a balanced fashion within a square block or field. Treatments appear once in each row and column. Replicates are also included in this design"* [24]. From the Latin squares presented in table 4.1 derive nine different combinations. This will be enough for the needs of this study.

A B C	1 2 3
B C A	2 3 1
C A B	3 1 2

Table 4.1: Latin Square for the different variants (left) and for the different levels (right)

To measure the participants' results and to compare the improvement deriving from the different variants, they will answer a questionnaire, Q0, before playing any variant and one after playing a level. The complete questionnaires are included in the appendix.

The questionnaire Q0 begins with the following question which aims to find out how aware the participants are of the permissions their favorite applications are listing in the "App permissions" menu. An example of the "App permission" menu is presented in figure 1.6. The question has two answering fields, one with the name of the application and one where the participants can list the permissions they think of. This question is asked openly to not affect the answers by the way the question or given answers are formulated. To compare the results of the participants, the

percentage of stated dangerous *Android* permissions is calculated. The *Play Store*'s permission page of the selected favorite application is used as reference, see figure 1.3 for an example of a permission page in the *Play Store*.

Question 1: For which permissions does your favorite application ask?

This question is followed by a question in which the participants select a statement which best describes their handling of *Android* permissions. This time multiple answers are given to select from because the participants will be grouped by these answers.

Question 2: How do you handle *Android* permissions?

- I don´t know what *Android* permissions are
- I don´t care about *Android* permissions
- I´m aware of their consequences but always grant them
- I´m not aware of their consequences and always grant them
- I consciously give applications only the permissions I want them to have
- None of these answers is describing me correctly

In addition, the questionnaire Q0 contains the questions of the level specific questionnaires which are introduced in the following. Questions on the level specific questionnaires will be labeled by a number N for the question number and a number L for the level number in the format N\L so e.g. question 3 for level 1 will be labeled as question 3\1. The level specific questionnaires begin with the qualitative question 3 in which the participants select statements that describe activities an application can do technically with the level specific permission. This tests the participants' understanding of what they technically allow the application to do and therefore these questions aim to confirm hypothesis 1a. The answers for these questions are quantified by calculating a score for an easier comparability. This is done by increasing the score, beginning at zero, by one for each correctly selected answer and decreasing the score by one for each incorrectly selected answer. Therefore the score will lay between minus two and three.

Question 3\1: When you grant an application access to your microphone, what could it do? Multiple answers could be correct.

- record audio without your knowledge
- record audio whenever it wants
- use the recorded audio, e.g. for advertisements
- only record audio when you explicitly tell the application to, e.g. recording a voice message
- only record audio when it is notifying you about the usage

Question 3\2: When you grant an application access to your storage, what could it do? Multiple answers could be correct.

- search through and write to your storage without your knowledge
- search through and write to your storage whenever it wants
- harm you or your data, e.g. leak secret files, delete files, download files to your phone
- only search through and write to your storage when you explicitly tell the application to, e.g. save or load a file
- only search through and write to your storage when it notifying you about the usage

Question 3\3: When you grant an application access to your contacts, what can it do? Multiple answers could be correct.

- read the contact information of your contacts without your knowledge
- read the contact information whenever it wants
- abuse the contact information, e.g. to send phishing or spam messages
- only use the contact information when you explicitly tell the application to, e.g. to add a friend
- only use the contact information when it is notifying you about the usage

On the following three questions, 4, 5 and 6 the participant rates the likeliness of consequences of granting the level specific permission on a 7-point Likert scale with 1 being very unlikely, 4 being

neutral and 7 being very likely. Whereby the consequences of those permissions are increasingly dangerous for the participants security. In question 6 the consequence will derive from granting a combination of permissions to an application, with one of them being the level specific permission. The Likert scale is chosen because it is easily understandable by the participant, easily quantifiable and allows agreement in different degrees, which can be easily compared for the evaluation of this study. 7 points are chosen because it allows more differentiable answers than e.g. a 5-point Likert scale. These questions are designed to see how good the participant can evaluate what uses a permission has for an application and with that information to confirm hypothesis 1b.

Question 4\1: Do you think it's likely that social media applications (Instagram, WhatsApp, Facebook etc.) with access to the microphone can record audio without notifying you?

Question 5\1: Do you think it's likely that social media applications with access to your microphone are able to use recorded audio to give you personalized advertisements?

Question 6\1: Do you think it's likely that access to location and microphone allows an application (like the official app of the Spanish football league) to find bars or restaurants which are broadcasting football games illegally?

Question 4\2: Do you think it's likely that widget applications (Flashlights, Clocks etc.) with access to your storage can search through your data?

Question 5\2: Do you think it's likely that widget applications with access to your storage and the internet can steal data from your phone?

Question 6\2: Do you think it's likely that widget applications with access to your storage and the right to install packages can install other malicious software to your phone?

Question 4\3: Do you think it's likely that shopping applications (Amazon Shopping, McDonalds etc.) with access to your contacts can read the information of the contacts stored on your phone without notifying you?

Question 5\3: Do you think it's likely that applications with access to your contacts can use the information from your contacts to send them spam or phishing messages?

Question 6\3: Do you think it's likely that malicious applications with granted permissions for contacts and SMS can spread messages and links from your phone to your contacts?

The next questions ask the participants to select which permissions they find okay to give a level specific type of applications, with the option to select that they are not caring about it anyways.

> **Question 7\1:** Which of the following permissions do you find okay to grant social media applications?
> **Question 7\2:** Which of the following permissions do you find okay to grant widget applications?
> **Question 7\3:** Which of the following permissions do you find okay to grant shopping applications?
> Possible Answers for these questions:
>
> - Location
> - Microphone
> - Camera
> - Contacts
> - Storage
> - Phone
> - None of these
> - I don't care about *Android* permissions I give to applications

The aim of these questions is to collect information about what capabilities the participants are willing to give a certain application type and from that derive how good they are in evaluating uses a permission has for an application. This is to confirm hypothesis 1b in combination with the information gathered from questions 4, 5 and 6. To compare the different variants in how they were perceived, in the last two questions the participants rate how much fun and how informative the variant they played was on a 7-point Likert scale.

> **Question 8:** How much fun did you have with this version?
> **Question 9:** How informative was this version?

Question 8's scale will reach from "very boring" to "very exciting", while question 9's will reach from "I learned nothing" to "I feel enlightened", both with "neutral" in the middle. These two questions aim to answer hypotheses 4.

As already mentioned some questions are designed to answer the hypotheses 1a and 1b. Therefore the improvements the different variants bring to the answers are measured and analyzed. To make sure they are statistically relevant t-tests will be applied. A t-test is used to compare two sets of values from the same measure, it's outcome describes how different the two sets are from each other [25]. The returned p-value is the likelihood of the two sets being similar [25]. As Jankowski et al. [25] suggests, the threshold for the p-value under which the difference between the two sets are treated statistically relevant will be set to 5% [25]. To confirm hypothesis 2 each time the participants answer a questionnaire they are asked to change a permission on the test device, a Lenovo Tab2 A10-30 with *Android* version 6.0.1. The required time will be measured and compared to check how their skills in changing *Android* permissions have increased after playing the different variants. The significance of the improvement is analyzed by a using a t-test.

Confirming these hypotheses with the described method will confirm the serious game *Make my phone secure!* as a reasonable tool for teaching the consequences of *Android* permissions and for teaching the ability to change *Android* permissions on *Android* devices.

4.2 Conducting the Study

The participants were recruited via notices in buildings belonging to the *University Bremen*, via an email distributor to students from the *faculty 3 computer science and mathematics* and via informing acquaintances. They were informed that they will play a serious game and will fill out a questionnaire. The topic and further information were withheld to minimize outer influences on the participants, especially because the participants should not be able to prepare themselves for the experiment. No participation requirements were applied to the study. During and after the participation, participants were allowed to take offered sweets and cookies. Participants were invited into the room 5310 of the MZH building in the University Bremen on the 11., 12., 18., 19. and 27. February 2019. A few participants were invited into another room of the University on the 23. February due to room 5310 being unavailable. In all used rooms the study was conducted isolated from outer influences and disruptive factors. The study's procedure was followed with every participant. They first answered the questionnaire Q0 and were asked to edit the permission of an application via the original *Android* menu, before playing the first variant. After playing a variant, they answered the level specific questionnaire and again were asked to edit the permission of an application over the original *Android* menu, until all variants and levels were played.

[This page intentionally is left blank.]

Chapter 5

Evaluation

In this chapter the procedure of the analysis is explained before the results of the conducted study will be evaluated by using this procedure.

5.1 Procedure

First results from the overall data are analyzed. This is done by giving a short description of the participants followed by analyzing how the participants performed on the task of taking away a permission from an application via the original *Android* menu before and after playing any of the variants. The next steps within this analysis are to analyze the permissions the participants selected as okay to grant to a certain application type before and after playing any of the variants, to analyze the improvements of participants in evaluating the consequences deriving from granting certain permissions to an application and to analyze how the participants rate the different variants. To identify whether *Make my phone secure!* has relevant differences in influencing users with different behaviors in handling *Android* permissions different groups are analyzed with the same procedure. The grouping is done by the participants' self-assessments in question 2, in which the participants were asked to select a statement describing their handling of *Android* permissions. Actually only the groups "I'm aware of their consequences and always grant them" and "I consciously give applications only the permissions I want them to have" are analyzed in this chapter. The remaining groups "I don't know what *Android* permissions are", containing two participants, and "I don't care about *Android* permissions", "None of these answers is describing me correctly" and "I'm not aware of their consequences and always grant them", containing one participant each, are too small and do not deliver meaningful conclusions when analyzed separately, therefore the analyzes for these groups are let out.

In the following M and SD will represent mean and standard deviation of a set of values. In addition the questions with a level number will be referenced all together under the question number. For example questions 3\1, 3\2 and 3\3 will be referenced all together as question 3.

The plots are generated via a *Python* script in form of a *Jupyter Notebook* available on the attached CD. The same script is used to calculate the means, the standard deviations, the t-tests and other used values.

5.2 Evaluation of the Overall Data

Description of the Participants

Overall 20 participants took part in the study. Among them 13 participants identified themselves as male and 7 participants identified themselves as female. Figure 5.1 shows the age distribution of the participants with an average age of 27. In average only 30% of the permissions the participant's favorite application would list as wished are remembered. The standard deviation of 24% suggests that some participants were significantly better or worse than the average.

Figure 5.1: Age distribution of participants in the overall data

Taking Away a Permission From an Application Via the Original *Android* Menu

While the half of the participants were not able to take away a permission from an application via the original *Android* menu in under 60s on the first try, the average time it took the other half is 31.6s. The standard deviation of this value is 18.22s which indicates that these values are widely distributed over the participants. As figure 5.2 shows variant C seems to be the best to improve users who unsuccessfully took away a permission from an application via the original *Android* menu in under 60s. To mention is that variant B failed twice in improving from unsuccessfully to successfully solving the task. For participants who were successfully solving the task before Variant B and C show averagely similar improvements, while variant C's improvements are less spread than variant B's. Variant A shows a low average with a high standard deviation. The applied t-tests show that the differences between the time improvements of each variant are not

statistically relevant. However, t-tests analyzing the differences between the participants' times before playing any variant and after playing a variant were applied to each variant. For the overall data these differences for each variant are significant. This shows that each variant was able to improve the time needed for taking away a permission from an application via the original *Android* menu significantly.

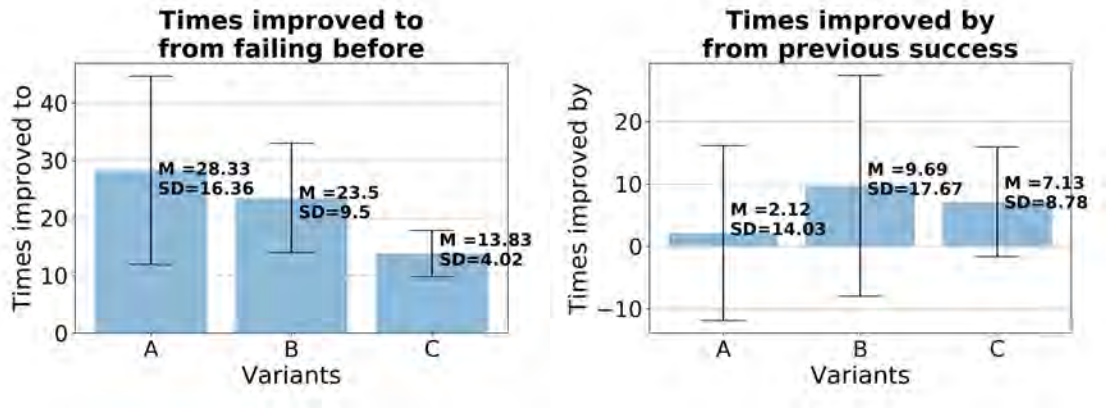

Figure 5.2: Bar plots showing the mean and standard deviation of the time improved to after unsuccessfully taking away a permission from an application via the original *Android* menu in under 60s (left) and the time improvements of successfully solving the task (right) for each of the three variants for the overall data.

Permissions That Are Selected As Okay to Grant to a Certain Application Type

As figure 5.3 shows, on the question which permissions they find okay to grant social media applications several dangerous permissions were selected more than seven times, while only four participants selected that no permission is okay to grant to a social media application. This shows that the participants are overall okay to give social media applications different dangerous permissions. For widget applications a different picture is presented by figure 5.3, the most selected option, with eight selections is that no permission is okay to grant to widget application. The location and storage permissions have seven and five selections, showing that some of the participants find it okay to grant some system features to this type of applications. A similar selection is shown for shopping applications. Overall the answers suggest that the participants make well informed decisions on what *Android* permissions are okay to grant to a specific application.

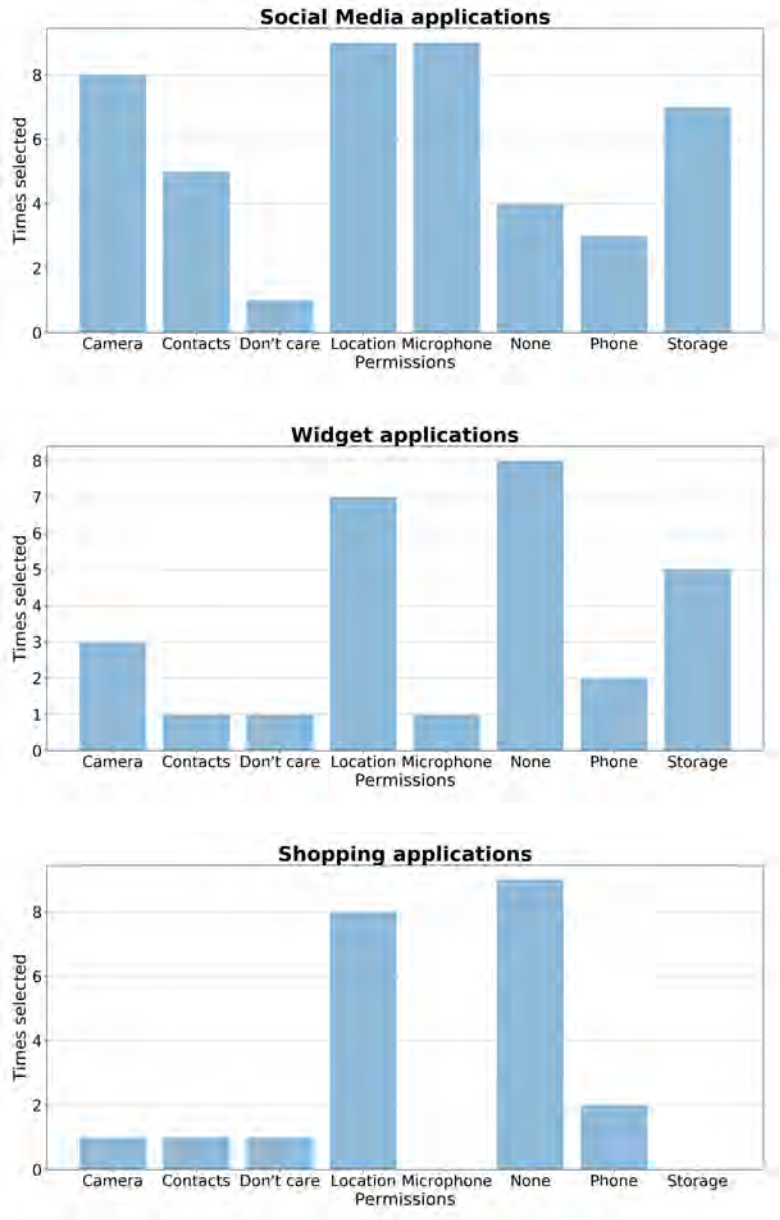

Figure 5.3: Bar plots showing how often a permission was selected as okay to grant for the application types social media (top), widget (middle) and shopping (bottom) for the overall data.

As figure 5.4 shows, after playing variant A some participants removed a few dangerous permissions from their selection as okay to grant to social media and widget applications, for shopping applications no differences were found. A different picture is drawn for playing variant B and C, some participants removed and added a few dangerous permissions for social media and widget applications. Overall playing the different variants does not seem to lead to a significant change in selections of what permissions are okay for a specific application type to have granted. This

could be caused by the already well informed decisions the participants applied on the before questionnaires, which are portrayed in figure 5.3.

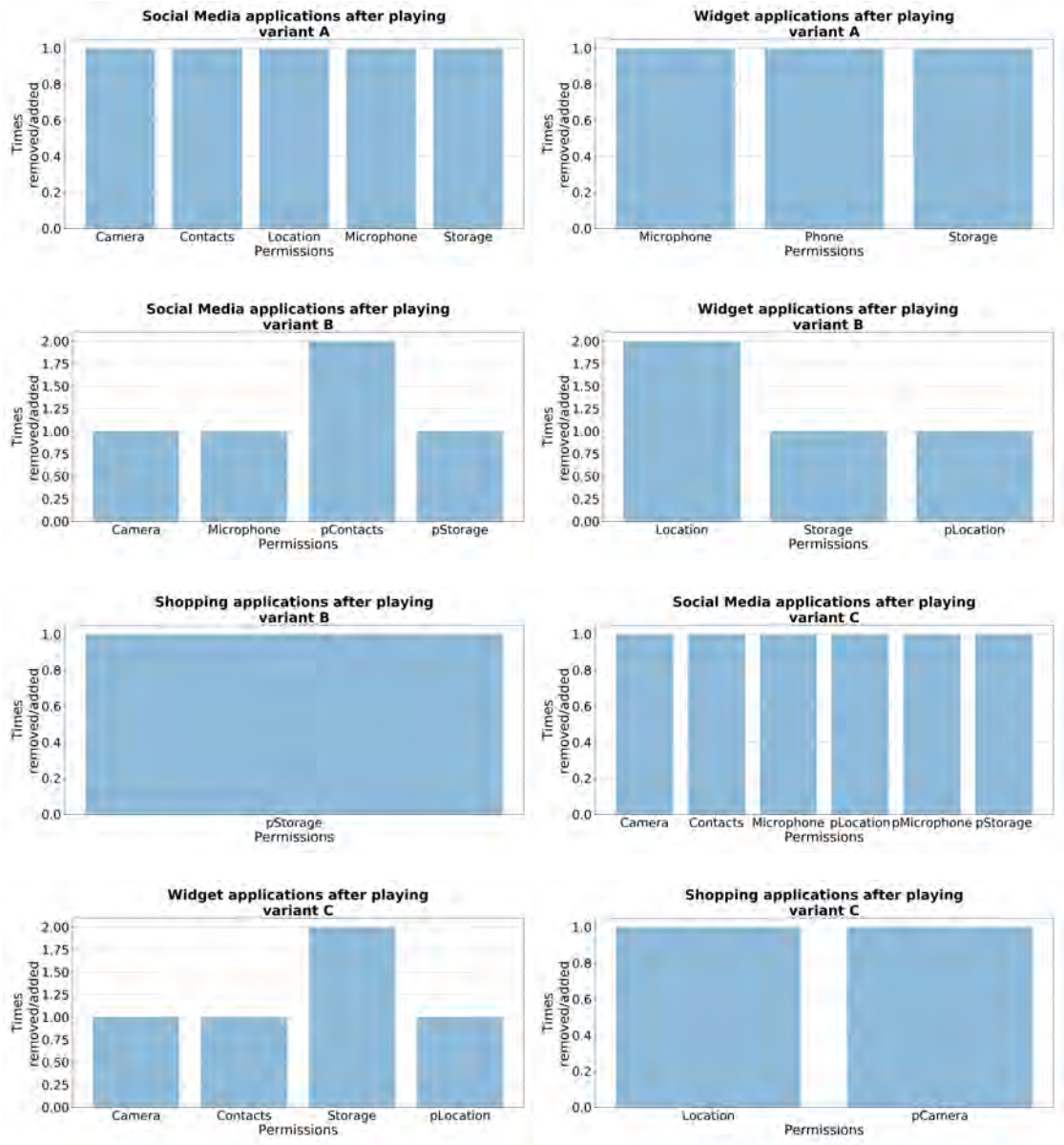

Figure 5.4: Bar plots showing how often a permission was removed or added as selected as okay to grant for a certain permission type for the overall data after playing variant A, B and C. The letter *p* before a permission name indicates that it was added as okay to grant for a certain permission type.

Consequences That Derive From Granting Certain Permissions to an Application

The answers from questions three to six are visualized in figure 5.5. The answers for question 3\1, 3\2 and 3\3 suggest that most of the participants were good in estimating what a permission allows an application to do technically, while some participants slipped back a lot. The questions testing how good the participants can evaluate what uses a permission can have for an application, question four to six for each level, show that the participants overall were already good in this sort of evaluation skills, while some participants were falling slightly behind.

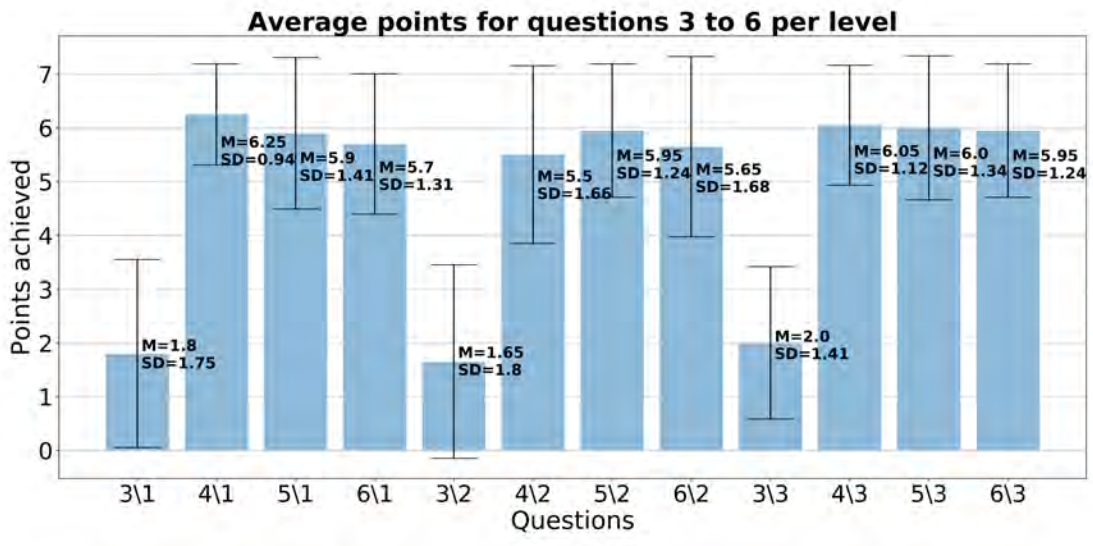

Figure 5.5: Bar plot showing the participants' average points achieved in questions 3 to 6 per level for the overall data. For question 3 minus two to three points are achievable, while zero to seven points are achievable in questions 4 to 6.

As figure 5.6 shows, the average improvements from variant A, B and C are below one point. While the comparatively high standard deviation suggests that the participants who scored lower than the average have improved significantly. From this data a best variant cannot be exposed.

The applied t-tests between each of the three variants show that the differences between them are not statistically relevant for the overall data. T-tests analyzing the differences between points before playing any variant and after playing a variant were applied to each variant once for question 3 and once for question 4, 5 and 6. For the overall data this differences for each variant are significant. This shows that each variant was able to improve the participants answers significantly.

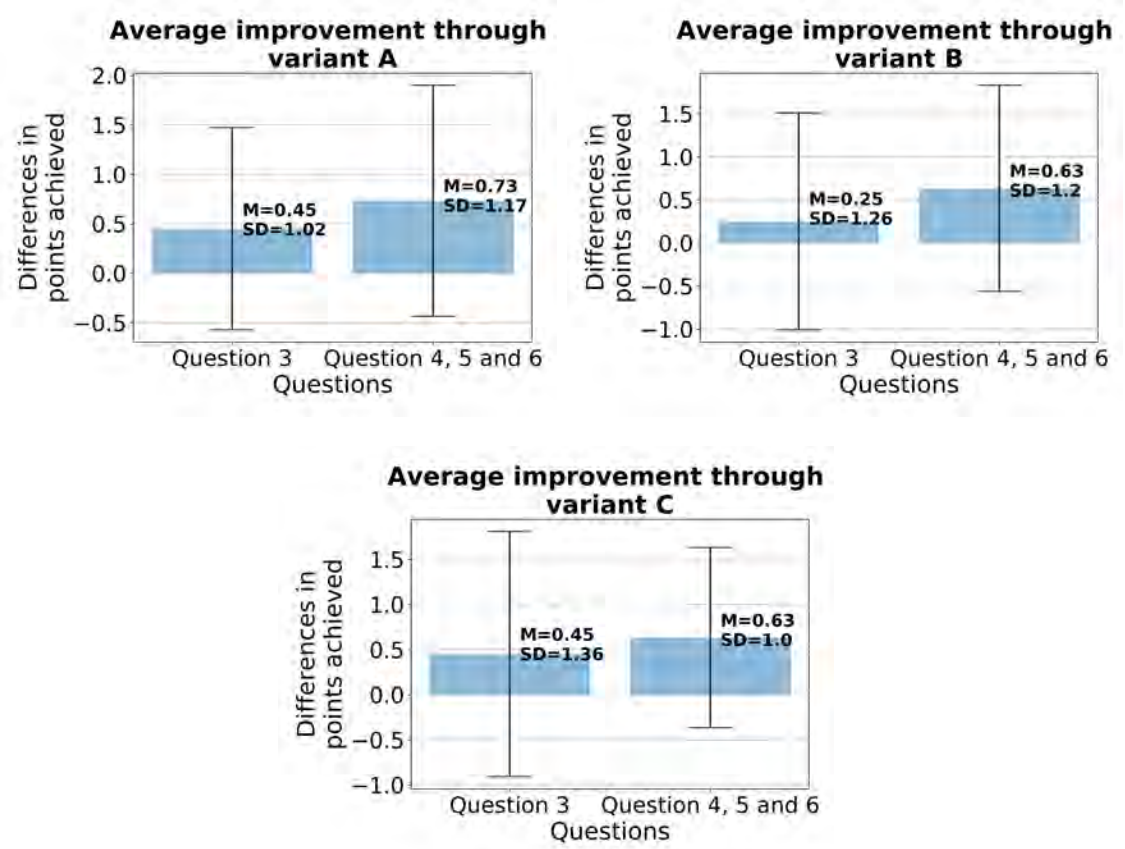

Figure 5.6: Bar plots showing the participants' average improvements in question 3 and in questions 4 to 6 for the variants A (left), B (right) and C (bottom) for the overall data.

Fun and Informative Ratings of The Different Variants

Averagely variant C the actual game *Make my phone secure!* is rated as the most informative and most fun variant, while variant A and B seem similarly rated from the data presented in figure 5.7. The applied t-tests show that the difference in fun ratings from variant C to variant A and B is statistically relevant. For the informative rating the difference between variant A and C is statistically relevant too. This shows that variant C is the most fun variant and more informative than the rebuild *Android* menu.

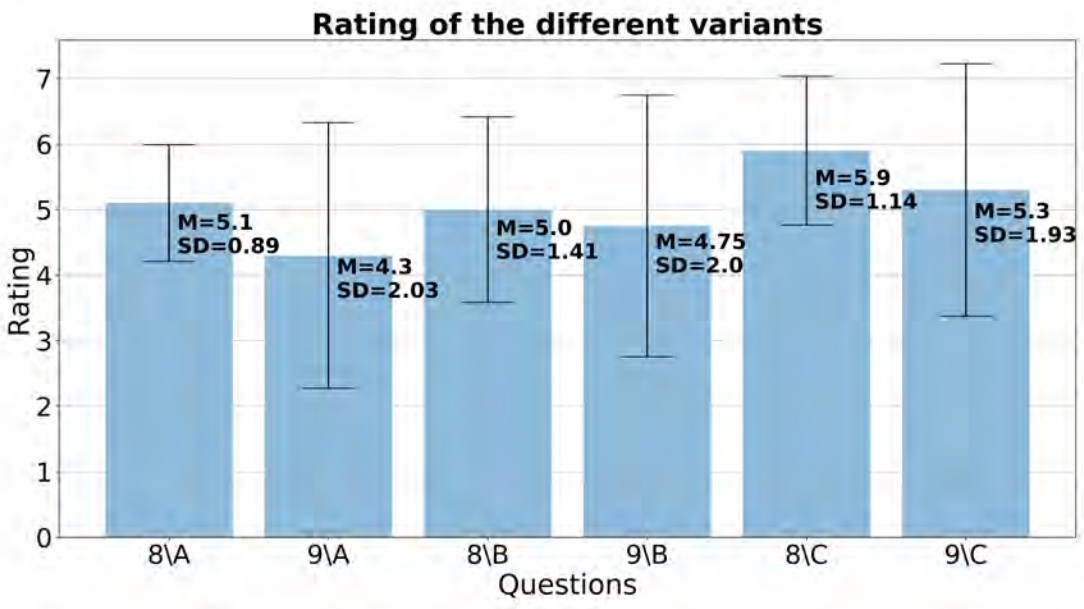

Figure 5.7: Bar plot showing the average ratings for the different variants for the overall data, question 8 was about how much fun the participant found the variant and question 9 about how informative they found the variant.

Conclusions for the Overall Data

The determined statistical relevant differences show that variant C is perceived as the most fun variant and is perceived more informative than variant A. However, this effect is not presented in the improvements of the different variants. In addition, it was shown that all variants are able to improve the time taken to take away a permission from an application via the original *Android* menu and that they are able to improve the ability to evaluate consequences deriving from granting a permission to an application.

5.3 Evaluation of Group: “I’m Aware of Their Consequences and Always Grant Them”

Description of the Participants

Four participants self-assessed themselves as “I’m aware of their consequences and always grant them”. Three of these participants are identifying themselves as male and one as female. Their average age is 24 with three participants of an age between 20 to 29 and one participant without a specified age. This group’s participants remembered averagely 14% of permissions their favorite applications would list as wished, with a standard deviation of 14% indicating mixed results on this question.

Taking Away a Permission From an Application Via the Original *Android* Menu

75% of this groups participants successfully took away a permission from an application via the original *Android* menu in under 60s in their first try within in an average of 38.67s which is a better value than the value from the overall data. The standard deviation of 17.02s suggests that these values are varying.

As figure 5.8 shows variant B seems to be the best in improving users who successfully took away a permission from an application via the original *Android* menu in under 60s. Its to mention that these values for variant B and C are spread widely around their mean. The applied t-tests between each of the two variants show that the differences between variant A, B and C are not statistically relevant. Therefore no conclusions about which version was best in improving times needed to take away a permission from an application via the original *Android* menu can be drawn. However, t-tests analyzing the differences between the time it took the participants to take away a permission from an application before playing any variant and after playing a variant were applied to each variant. For this group only the difference for variant A is significantly different, but the improvement by variant A is so small, that it could likely be due to solving a similar task over and over again.

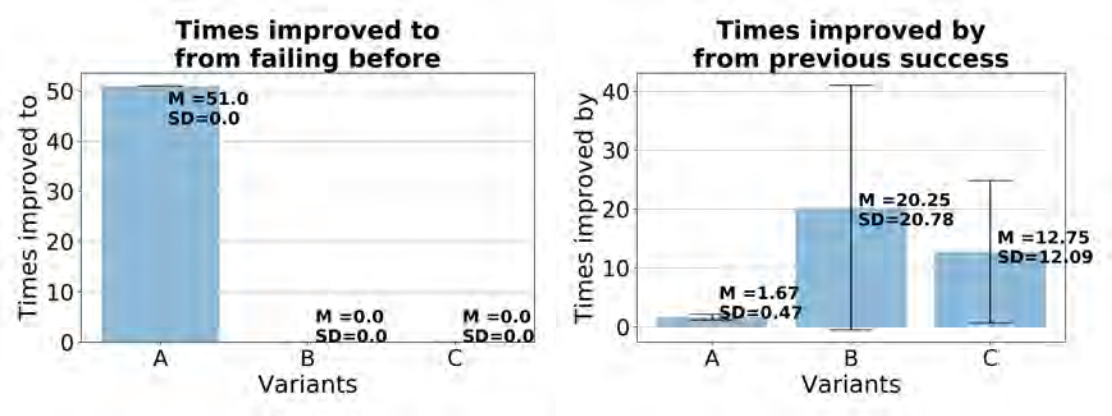

Figure 5.8: Bar plots showing the mean and standard deviation of the time improved to after unsuccessfully taking away a permission from an application via the original *Android* menu in under 60s (left) and the time improvements of successfully solving the task (right) for each of the three variants for the "I'm aware of their consequences and always grant them" group.

Permissions That Are Selected As Okay to Grant to a Certain Application Type

As figure 5.9 shows this group mirrors the information on the question which permissions they find okay to grant social media applications gathered from the overall data. This group selects location more often than none as okay for widget applications and none more often than location for shopping application, which is slightly different from the behavior in the overall data. Almost no changes in these selections are shown after playing any of the variants. The contacts and storage permissions were removed once each as okay to grant social media applications after playing variant A and after playing variant B location was added once as okay to grant widget applications. As in the overall data, the influences of playing each variant are to small to come to conclusions.

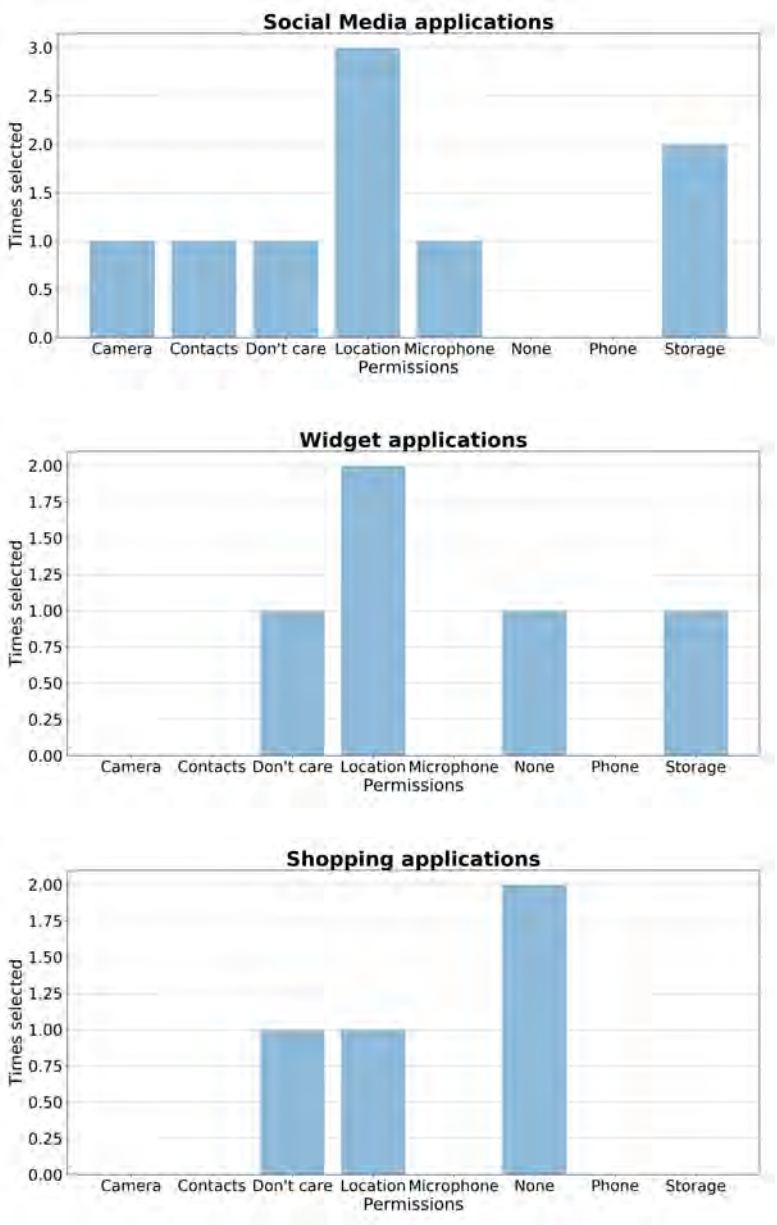

Figure 5.9: Bar plots showing how often a permission was selected as okay to grant for the application types social media (top), widget (middle) and shopping (bottom) for the "I'm aware of their consequences and always grant them" group.

Consequences That Derive From Granting Certain Permissions to an Application

This group's answers for questions three to six are visualized in figure 5.10. The answers for questions 3\2 and 3\3 suggest that most of the participants were very good in estimating what a permission allows an application to do technically. The answers for questions 4 to 6 for each

level, show that the participants were rating what uses a permission can have for an application precisely good. Only in question 6\1 some outliers influence the result. Therefore this group is averagely better than all participants in average, which is suggesting that participants belonging to this group were selecting an applicable answer when asked how they handle *Android* permissions.

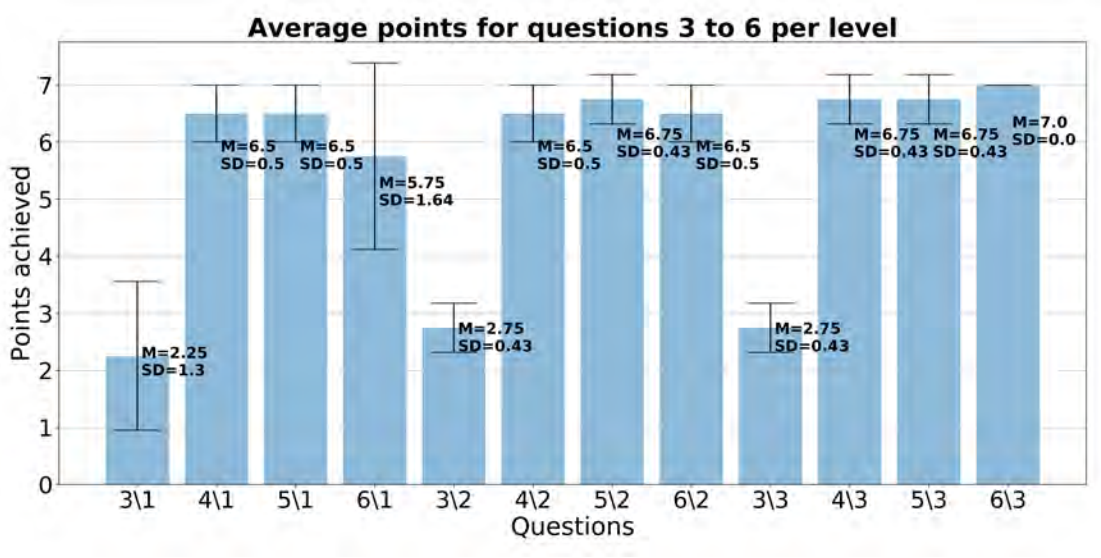

Figure 5.10: Bar plot showing the participants' average points achieved in questions 3 to 6 per level for the "I'm aware of their consequences and always grant them" group. For question 3 minus two to three points are achievable, while zero to seven points are achievable in questions 4 to 6.

As figure 5.11 show the average improvements from variant A, B and C in this group picture a different result as the overall data. While the standard deviation is very high for each variable, variant 1 seems to be best in improving the answers as variant B and C are able to even lower the scores for question 3. The applied t-tests between each of the two variants show that the differences between variant A and B and variant A and C are statistically relevant. The same is not true for the differences between variant B and C. Therefore for this group variant A is better in improving the participants answers than variants B and C. A look in the attached table *After.xlsx* shows that this groups participants got the combination variant A and level 1 at a rate of 75%. Since the questions 3 to 6 for level 1 scored averagely lower than the other levels, this result is not of a significant value. However, t-tests analyzing the differences between points before playing any variant and after playing a variant were applied to each variant once for question 3 and once

for question 4, 5 and 6. For this group this differences for each variant in questions 4, 5 and 6 are significant. Therefore each variant was able to improve the participants answers significantly in those questions. For question 3 no variant showed statistically relevant differences, this could be due to the already very good answers on the before questionnaire.

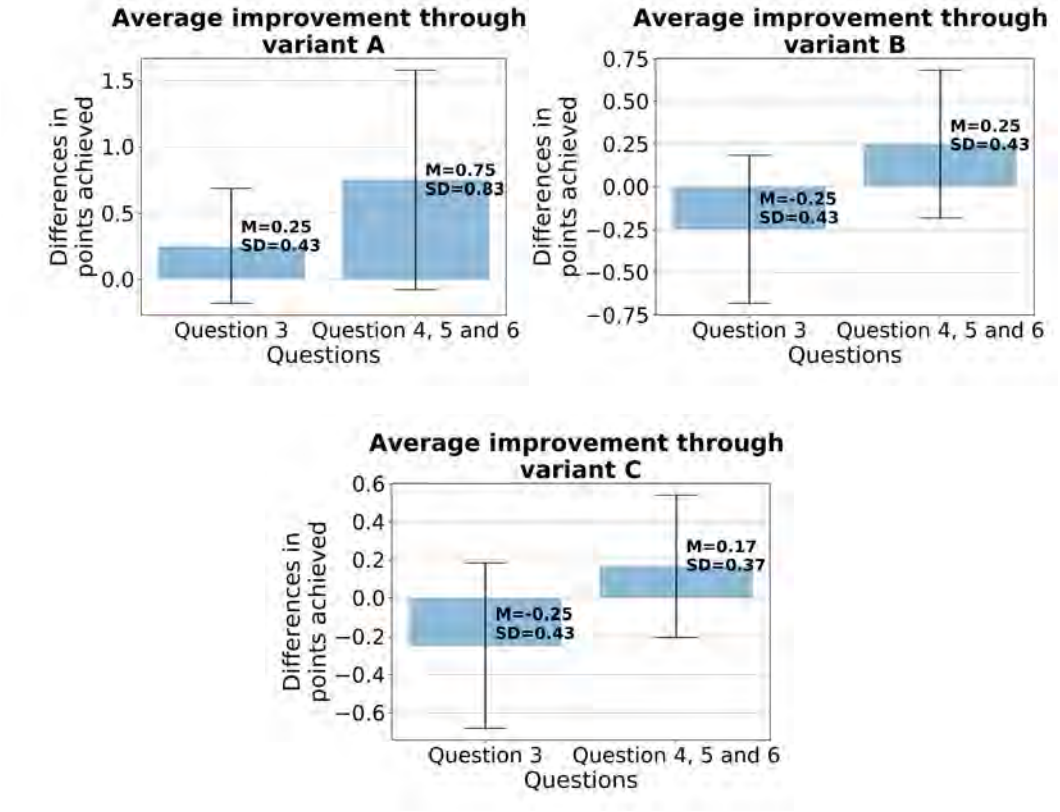

Figure 5.11: Bar plots showing the participants' average improvements in question 3 and in questions 4 to 6 for the variants A (left),B (middle) and C (right) for the "I'm aware of their consequences and always grant them" group

Fun and Informative Ratings of the Different Variants

Figure 5.12 suggests that variant C is in average rated as the most informative and fun variant. Variant B is the second most informative and fun variant, but the standard deviations of all variants are very high. The applied t-tests between each of the three variants show that the differences between variant A, B and C are not statistically relevant. Therefore no conclusion about which version was most fun or most informative can be drawn for this group.

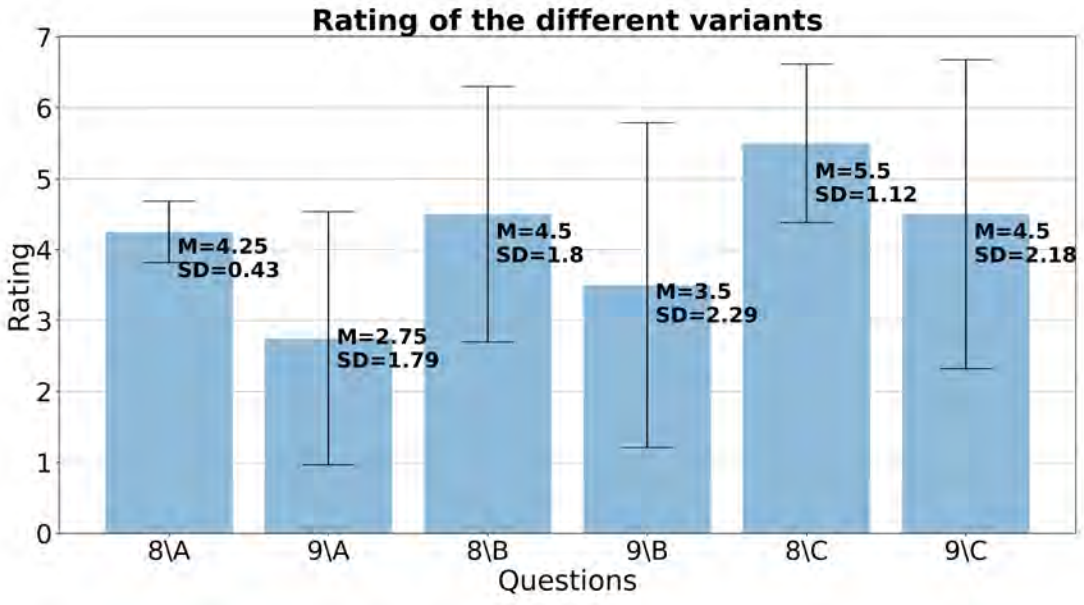

Figure 5.12: Bar plot showing the average ratings for the different variants for the "I'm aware of their consequences and always grant them" group, question 8 was about how much fun the participant found the variant and question 9 about how informative they found the variant

Conclusions for the Group "I'm Aware of Their Consequences and Always Grant Them"

Since no statistically relevant differences between the variants and between before and after playing any of the variants were found no general applying conclusions can be drawn from the "I'm aware of their consequences and always grant them" group besides that all variants were able to improve the participants results in questions 4 to 6 significantly. This shows that users, which self-assess themselves as being aware of the consequences deriving from granting permissions to *Android* applications, are able to be improved in evaluating what uses a permission can have for an application by the three variants and especially by variant C, the serious game *Make my phone secure!*.

5.4 Evaluation of Group: “I Consciously Give Applications Only the Permissions I Want Them to Have”

Description of the Participants

Eleven participants self-assessed their handling of *Android* permissions as “I consciously give applications only the permissions I want them to have”. Seven of these participants are identifying themselves as male and four as female. The age distribution of this group’s participants presented in figure 5.13 has an average age of 28.

Figure 5.13: Age distribution of participants in the “I consciously give applications only the permissions I want them to have” group

The participants remembered 35% of the permissions their favorite applications would list as wished, with a standard deviation of 20% suggesting spread percentages between the participants.

Taking Away a Permission From an Application Via the Original *Android* Menu

45% of this groups participants successfully took away a permission from an application via the original *Android* menu in under 60s in their first try within in an average of 21s which is faster than the value in the overall data. The standard deviation of 14.52s suggests that these values are varying between the participants.

As figure 5.14 shows variant C seems to be the best to improve users who both successfully and

unsuccessfully took away a permission from an application via the original *Android* menu in under 60s. Mentionable is that variant B failed one time in improving from unsuccessfully to successfully solving the task. The applied t-tests between each of the two variants show that the differences between variant A, B and C are not statistically relevant. Therefore no conclusions about which version was best in improving the times needed to take away a permission from an application via the original *Android* menu can be drawn. However, t-tests analyzing the differences between the time it took the participants to take away a permission from an application before playing any variant and after playing a variant were applied to each variant. For this group these differences for each variant are significant. Therefore each variant was able to improve the time needed for the task significantly.

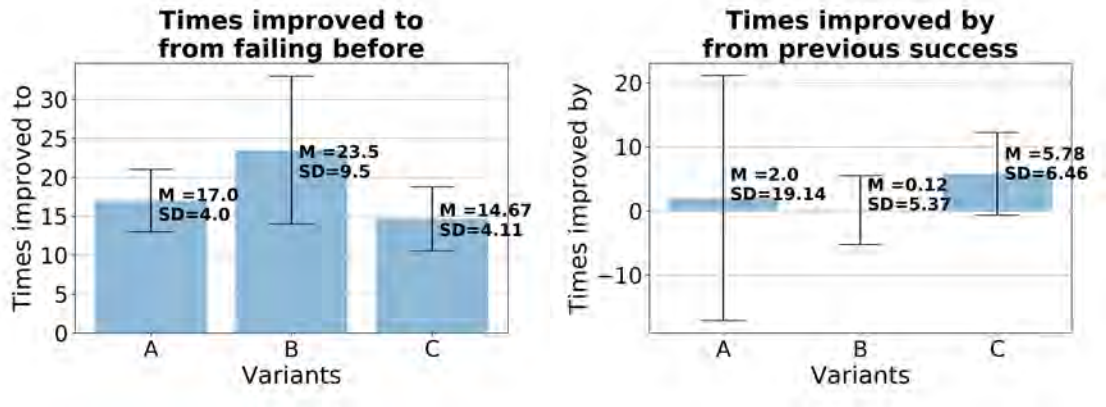

Figure 5.14: Bar plots showing the mean and standard deviation of the time improved to after unsuccessfully taking away a permission from an application via the original *Android* menu in under 60s (left) and and the time improvements of successfully solving the task (right) for each of the three variants for the "I consciously give applications only the permissions I want them to have" group.

Permissions That Are Selected As Okay to Grant to a Certain Application Type

As figure 5.15 shows this groups behavior differs from behavior observed in the overall data. Four participants select that no permission is okay to grant social media applications. The same time microphone, contacts and storage were selected as okay to grant to social media applications. This shows that this group is rather divided in the question of granting dangerous permissions to social media applications. All participants who selected that no permissions are okay to grant to

this type of applications are belonging to this group. However, the average behavior in selecting answers for widget and shopping applications is similar to the average behavior of the overall data. This effect is no coincidence because participants belonging to this group self-assessed themselves as giving applications only the permissions they want them to have.

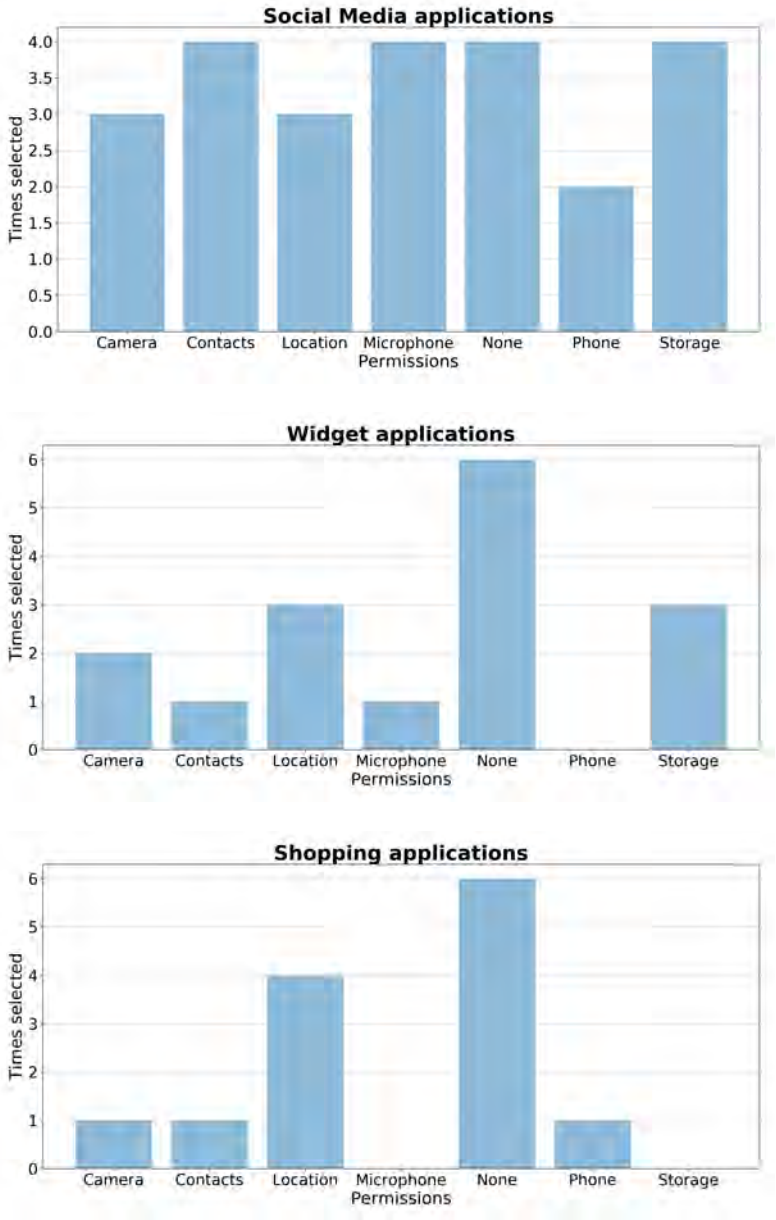

Figure 5.15: Bar plots showing how often a permission was selected as okay to grant for the application types social media (top), widget (middle) and shopping (bottom) for the "I consciously give applications only the permissions I want them to have" group

Figure 5.16 shows that no big changes were made to the selection of what permissions are okay to grant to a certain application type after playing any of the variants.

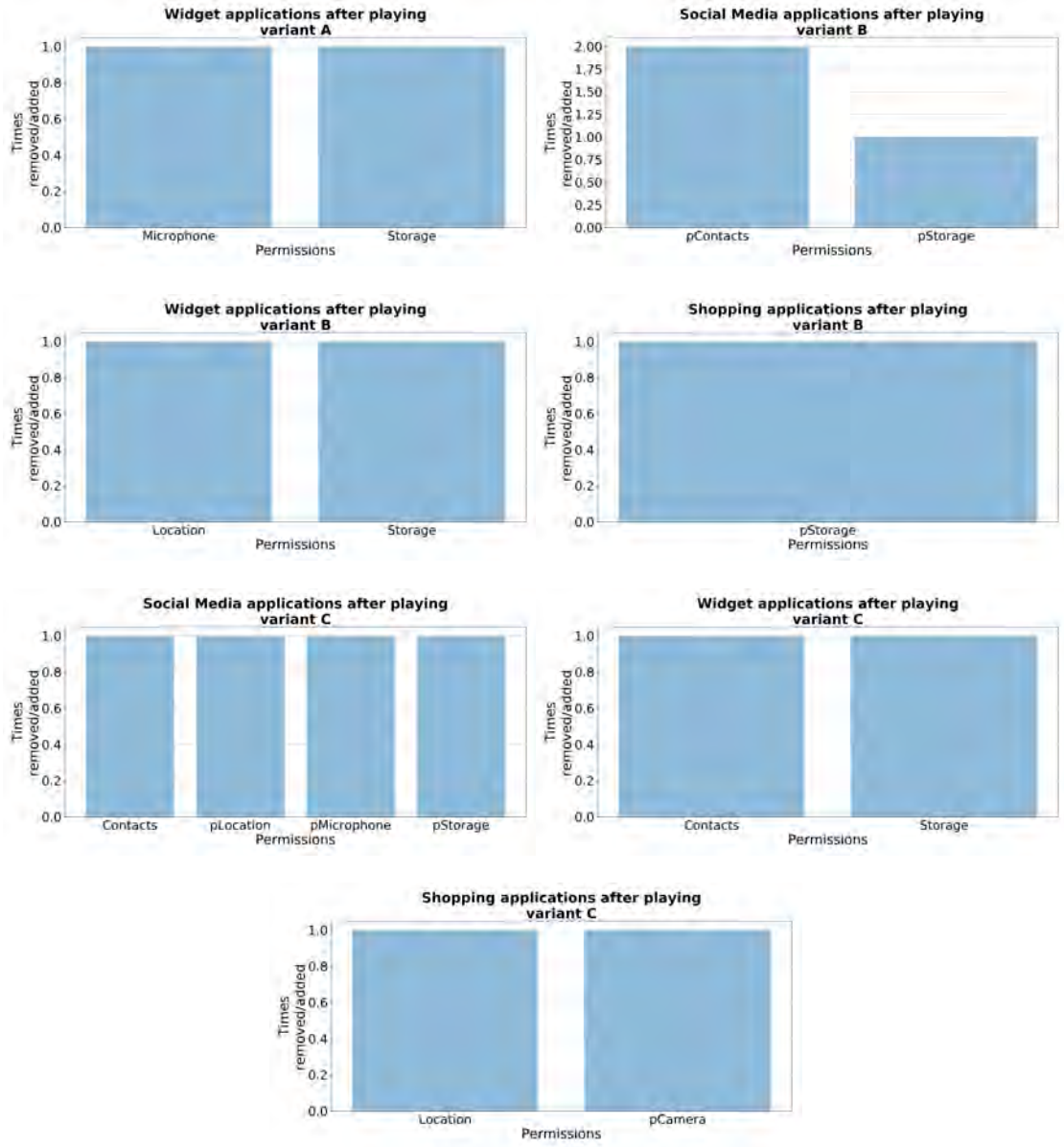

Figure 5.16: Bar plots showing how often a permission was removed or added from the selection as okay to grant for a certain permission type for the "I consciously give applications only the permissions I want them to have" group after playing each variant. The letter *p* before a permission name indicates it was added as okay to grant for a certain permission type

Consequences That Derive From Granting Certain Permissions to an Application

Figure 5.17 visualizes the results from questions three to six of this group. The answers for questions 3\1, 3\2 and 3\3 suggest that most of the participants were slightly worse in estimating what a permission allows an application to do technically than the average in group "I'm aware of their consequences and always grant them". The standard deviation indicates varying skills in this group's members. The questions testing how good the participants can evaluate what uses a permission can have for an application, question four to six for each level, show a similar effect.

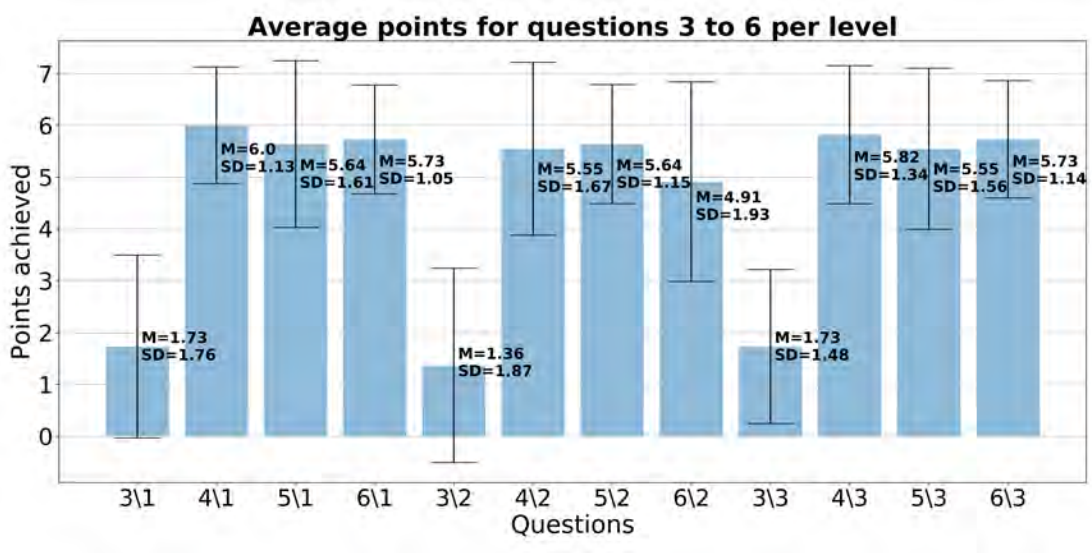

Figure 5.17: Bar plot showing the participants' average points achieved in questions 3 to 6 per level for the "I consciously give applications only the permissions I want them to have" group. For question 3 minus two to three points are achievable, while zero to seven points are achievable in questions 4 to 6.

As 5.18 show the average improvements from variant A, B and C in this group picture a different result as the overall data. While the standard deviation is very high for each variable, variant C seems to be best in improving the answers, followed by variant B. However, the applied t-tests between each of the two variants show that the differences between variant A, B and C are not statistically relevant. So no conclusions about which variant is best in improving answers of questions 3 to 6 can be drawn. T-tests analyzing the differences between points before playing any variant and after playing a variant were applied to each variant once for question 3 and once for questions 4, 5 and 6. For this group these differences for each variant are significant. Therefore each variant was able to improve the participants answers significantly.

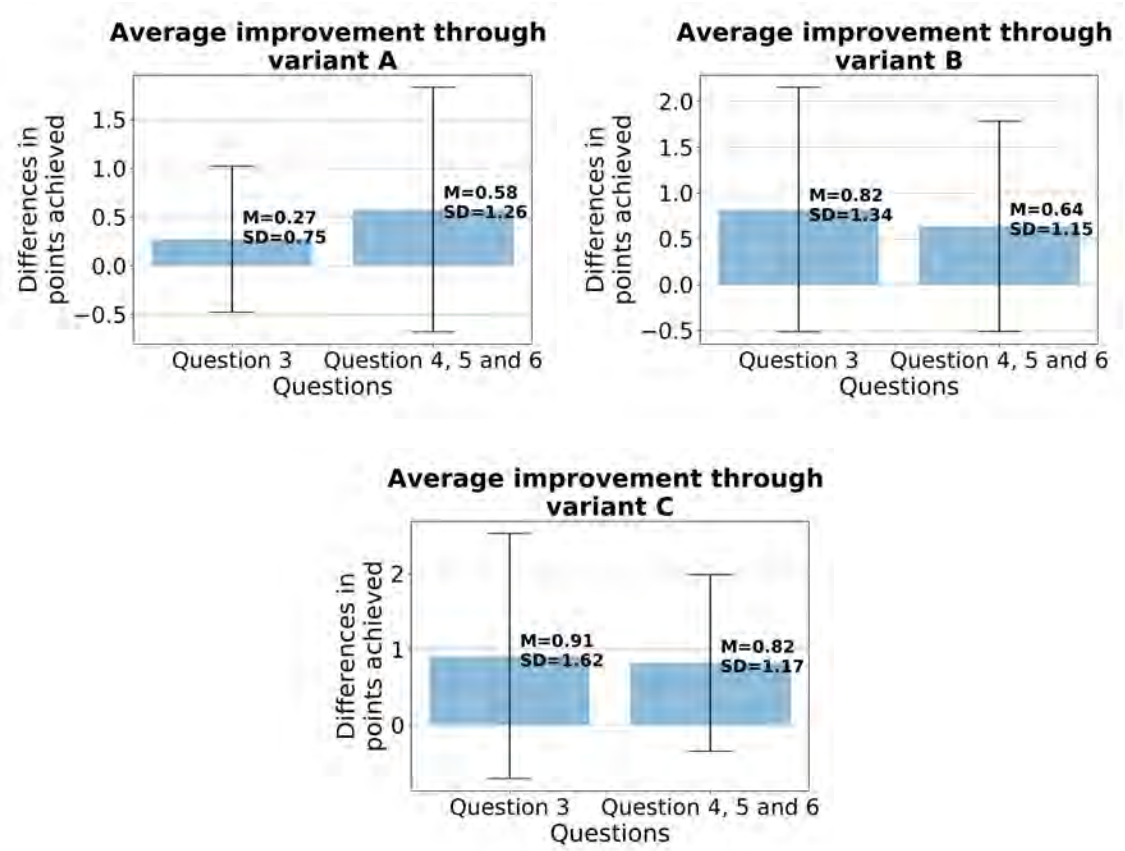

Figure 5.18: Bar plots showing the participants' average improvements in question 3 and in questions 4 to 6 for the variants A (left),B (middle) and C (right) for the "I consciously give applications only the permissions I want them to have" group

Fun and Informative Ratings of The Different Variants

As figure 5.19 suggests, variant C is rated as the most informative and most fun variant. Variant A seems a bit more informative than B, while B seems a bit more fun than A. The applied t-tests between each of the two variants show that the differences between the fun ratings of variant A and C and variant B and C are statistically relevant, as well as the difference between the informative ratings of variant A and C. Therefore within this group variant C is the most fun variant and is also rated as more informative than variant A.

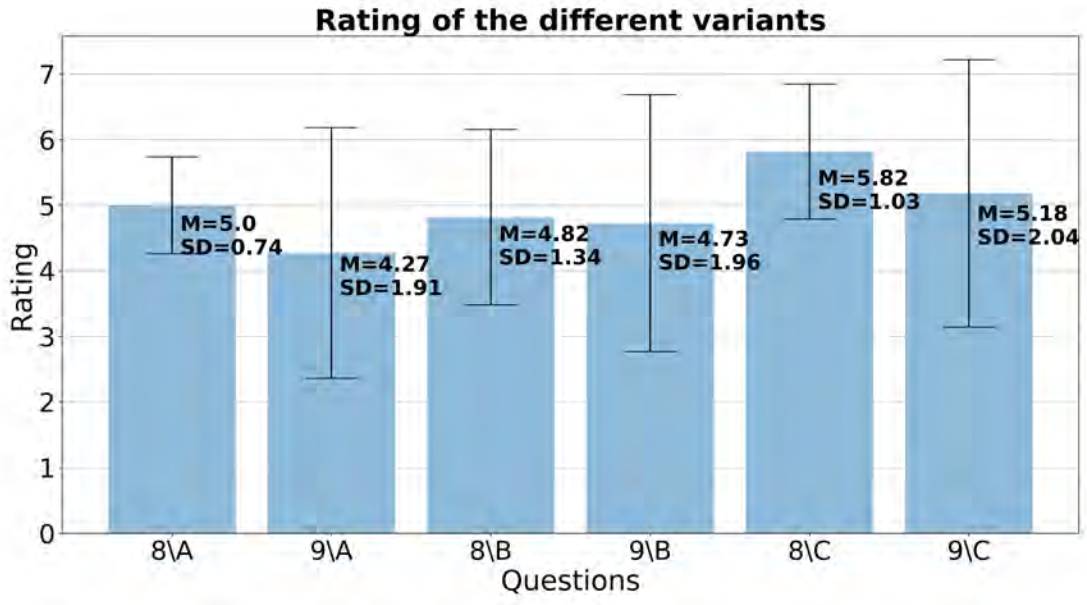

Figure 5.19: Ratings for the different variants in average for the "I consciously give applications only the permissions I want them to have" group, question 8 was about how much fun the participant found the variant and question 9 about how informative they found the variant

Conclusions for the Group "I Consciously Give Applications Only the Permissions I Want Them to Have"

The statistically relevant differences found in the "I consciously give applications only the permissions I want them to have" group show that within this group variant C is perceived as the most fun variant and is perceived more informative than variant A. In addition, all variants are able to improve the times needed for taking away a permission from an application via the original *Android* menu and to improve the ability of evaluating consequences that derive from granting a certain permission to an application. This shows that users', which self-assess themselves as consciously giving applications only the permissions they want them to have, abilities of changing permissions via the original *Android* menu and their abilities to evaluate consequences deriving from granting certain permissions to *Android* applications can be improved py playing any of the variants, especially by playing *Make my phone secure!*, which is perceived as the most fun variant.

5.5 Summarizing the Results

The results from the overall data show that every variant was able to increase the time it took participants to take away a permission via the original *Android* menu significantly, therefore hypothesis 2, "Players of *Make my phone secure!* will be able to change the permissions given to applications on *Android* devices more comfortable than before playing", is confirmed. The same applies to the points participants reached for questions 3 to 6. Therefore hypothesis 1, "Players of *Make my phone secure!* will understand which consequences derive from granting permissions to an application significantly better than before playing", is confirmed. Since the differences in improvements between the different variants A, B and C are not statistically relevant, hypothesis 3, "*Make my phone secure!* will have the highest affect in improving the participants results" cannot be confirmed. No relevant changes in finding it okay to grant dangerous permissions to a certain application are found after playing any of the variants. The ratings on how fun and informative the participants perceive the different variants present variant C, the actual serious game *Make my phone secure!*, as the most fun variant. In addition, it is perceived more informative than variant A, the rebuild *Android* menu. Therefore hypothesis 4, "*Make my phone secure!* will be the most informative and fun variant", is confirmed with the restriction of not being significantly better than variant B.

Analyzing the group "I'm aware of their consequences and always grant them" showed that even the ability to evaluate what uses a permission can have for an application of users, which are self-assessing themselves as being aware of the consequences deriving from granting *Android* permission to applications is able to being improved by playing *Make my phone secure!* and the other variants. The analysis of group "I consciously give applications only the permissions I want them to have"showed that users, which self-assess themselves as consciously granting applications only the permissions they want them to have, improve their ability of changing *Android* permissions via the original *Android* menu and their ability to evaluate consequences that derive from granting certain permissions to *Android* applications by playing *Make my phone secure!* and the other variants.

Concluding variant C, the serious game *Make my phone secure!*, is fulfilling it's purposes to teach it's players the consequences deriving from granting dangerous permissions to *Android* applications and the ability to change the permissions they have granted *Android* applications on their own devices. Therefore the research question is answered with a confirmation. Even

though the learning benefits of *Make my phone secure!* are not bigger then the ones of variant A and B players had more fun with *Make my phone secure!* than with the other variants, therefore they would likely be happier to learn with *Make my phone secure!* instead of the others. Further observations are that the average points participants achieved for questions 3 to 6 were already very good before playing any of the variants as figure 5.5 shows. This could be due to 75% of the participants belonging to group "I'm aware of their consequences and always grant them" or group "I consciously give applications only the permissions I want them to have". The other groups are containing not more than two participants each, which is a big factor for the study. Despite this, the participants in average are only able to remember 30% of the dangerous permissions their favorite applications would ask for. Showing that the *Android* users are not aware of which dangerous permissions their favorite application wants to have granted.

Chapter 6

Conclusions

The problem of granting to much permissions to *Android* application leads to applications like *La Liga - Spanish Soccer League Official* abusing their access rights and harming the user's privacy as well as raising the possibility to also harm further security aspects.
In addition, the original *Android* menu and Google Play Store's application installation page are neither informing about what consequences derive from granting permissions nor what permissions an application asks for in an appropriate manner.
Therefore *Android* users need a way to inform themselves, to learn to evaluate consequences of granting a permission to an application and to learn how to edit permissions that are granted to a specific application.
Serious games, which are video games with pedagogy added as a central aspect to them, as *America's Army*, which was used in training for US Army soldiers, show that they are able to teach players relevant skills in a fun way.
This raised this works research question: Can we teach smartphone users to understand the consequences of permissions they give to applications and teach them how to change their own permissions by playing a serious game?
To answer this question the serious game *Make my phone secure!* was developed. In *Make my phone secure!* the player helps non playable characters (NPCs) to solve their problems by changing *Android* permissions on their *Android* phones. This is realized by rebuilding the original *Android* menu. After completing a level of *Make my phone secure!* the player gets an detailed explanation of which permissions are causing the NPC's problem and how the problem can be avoided.
In an empiric research the influences of playing *Make my phone secure!* on the participants' abilities to evaluate what a permission technically allows an application to do and to evaluate what uses a permission has for an application were analyzed. These two abilities together enable to understand what consequences derive from granting certain permissions to an application. In addition, the influences on the participants' time taken to take away a permission via the original *Android* applications were measured. Those influences of two other variants, one rebuilding the original *Android* menu and one with hints and *Make my phone secure!*'s explanations, were analyzed to compare against the results from playing the actual game. The participants were asked to rate the fun they had with each variant and how informative they found it. In the end the significance between each of the variants' results between each other and between themselves and the participant's prior knowledge were analyzed.

20 participants with an age average of 27 participated in the study. They were asked to select a statement describing their handling of *Android* permissions to allow groupings based on this self-assessment. 75% of the participants assessed themselves as aware of the consequences but always granting the requested *Android* permissions or as consciously giving only the *Android* permissions they want applications to have Therefore the prior knowledge of the participants was higher than expected. However, each of the variants were able to significantly increase the participants results. A significant difference in increasing the participant's results between the three variants was not found. However, *Make my phone secure!* was rated as the most fun variant and was rated more informative than the rebuild of the original *Android* menu. The research question is therefore answered successfully.

As already mentioned, the prior knowledge of the participants was higher than expected and more important higher than anticipated. To further analyze the significance in differences between the three variants, the study could be repeated with participants, which are carefully picked by rating their prior knowledge. Additionally *Make my phone secure!* could be expanded by different levels and other versions of the *Android* menu, to allow players to learn the consequences of a broader range of dangerous *Android* permissions and to learn how to change the permission settings of an application on their own devices even better.

Bibliography

[1] Statista, "Anteil der smartphone-nutzer in deutschland in den jahren 2012 bis 2017," https://de.statista.com/statistik/daten/studie/585883/umfrage/anteil-der-smartphone-nutzer-in-deutschland/, 2018, accessed: 2018-07-23.

[2] 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*, ser. SOUPS '12. New York, NY, USA: ACM, 2012, pp. 3:1–3:14. [Online]. Available: http://doi.acm.org/10.1145/2335356.2335360

[3] ZEIT, "Offizielle liga-app aktiviert handy-mikrofone," https://www.zeit.de/digital/datenschutz/2018-06/la-liga-app-spanien-fussball-dsgvo-pay-tv-lizenz-betrug/, 2018, accessed: 2018-08-26.

[4] AndroidDevelopers, "Manifest.permission," https://developer.android.com/reference/android/Manifest.permission, 2018, accessed: 2018-09-25.

[5] L. Stefanko, "Turn the light on and give me your passwords!" https://www.welivesecurity.com/2017/04/19/turn-light-give-passwords//, 2017, accessed: 2018-08-26.

[6] J. Stoll, C. S. Tashman, W. K. Edwards, and K. Spafford, "Sesame: Informing user security decisions with system visualization," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '08. New York, NY, USA: ACM, 2008, pp. 1045–1054. [Online]. Available: http://doi.acm.org/10.1145/1357054.1357217

[7] T. Susi, M. Johannesson, and P. Backlund, "Serious games : An overview," University of Skövde, School of Humanities and Informatics, Tech. Rep. HS-IKI-TR-07-001, 2007.

[8] D. R. Michael and S. L. Chen, *Serious Games: Games That Educate, Train, and Inform*, 2006.

[9] M. Zyda, “From visual simulation to virtual reality to games,” *Computer*, vol. 38, no. 9, pp. 25–32, Sep. 2005. [Online]. Available: http://dx.doi.org/10.1109/MC.2005.297

[10] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, “Your attention please: Designing security-decision uis to make genuine risks harder to ignore,” in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS ’13. New York, NY, USA: ACM, 2013, pp. 6:1–6:12. [Online]. Available: http://doi.acm.org/10.1145/2501604.2501610

[11] A. Stapleton, “Serious games: Serious opportunities,” *Australian Game Developers Conference*, 01 2004.

[12] C. Eckert, *IT-Sicherheit : Konzepte - Verfahren - Protokolle*, 7th ed., ser. Informatik 10-2012. Munich: Oldenbourg, 2012, online-Ressource (XV, 1004 S.). [Online]. Available: http://dx.doi.org/10.1524/9783486719758

[13] CambridgeDictionairy, “privacy,” https://dictionary.cambridge.org/de/worterbuch/englisch/privacy, n.d., accessed: 2019-23-02.

[14] AndroidDevelopers, “Permissions overview,” https://developer.android.com/guide/topics/permissions/overview, 2018, accessed: 2018-09-25.

[15] K. Yamada, “The seven deadly android permissions: How to avoid the sin of slothful preparedness,” https://www.makeuseof.com/tag/the-seven-deadly-android-permissions-how-to-avoid-the-sin-of-slothful-preparedness/, 2013, accessed: 2018-11-26.

[16] M. Harbach, M. Hettig, S. Weber, and M. Smith, “Using personal examples to improve risk communication for security and privacy decisions,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI ’14. New York, NY, USA: ACM, 2014, pp. 2647–2656. [Online]. Available: http://doi.acm.org/10.1145/2556288.2556978

[17] Z. A. Wen, Y. Li, R. Wade, J. Huang, and A. Wang, “What.hack: Learn phishing email defence the fun way,” in *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA ’17. New York, NY, USA: ACM, 2017, pp. 234–237. [Online]. Available: http://doi.acm.org/10.1145/3027063.3048412

[18] J. Hamari, D. J. Shernoff, E. Rowe, B. Coller, J. Asbell-Clarke, and T. Edwards, "Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning," *Computers in Human Behavior*, vol. 54, pp. 170 – 179, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S074756321530056X

[19] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ser. CCS '11. New York, NY, USA: ACM, 2011, pp. 627–638. [Online]. Available: http://doi.acm.org/10.1145/2046707.2046779

[20] F. Gechter, J.-M. Contet, S. Galland, O. Lamotte, and A. Koukam, "Virtual intelligent vehicle urban simulator: Application to vehicle platoon evaluation," *Simulation Modelling Practice and Theory*, vol. 24, pp. 103 – 114, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1569190X12000172

[21] D. A. Norman, *The design of everyday things*, 1st ed. New York [u.a.]: Doubleday/Currency, 1990, xV, 257 S. ; 21 cm : Ill. [Online]. Available: https://suche.suub.uni-bremen.de/peid=B11753891

[22] C. Lewis and D. A. Norman, "Designing for error," in *Human-computer Interaction*, R. M. Baecker, J. Grudin, W. A. S. Buxton, and S. Greenberg, Eds. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1995, pp. 686–697. [Online]. Available: http://dl.acm.org/citation.cfm?id=212925.212990

[23] Instagram, "Instagram's play store page," https://play.google.com/store/apps/details?id=com.instagram.android&hl=en, n.d., accessed: 2019-02-18.

[24] L. Gao, "Latin squares in experimental design," http://compneurosci.com/wiki/images/9/98/Latin_square_Method.pdf, 12 2005, accessed: 2019-02-08.

[25] K. R. B. Jankowski, K. J. Flannelly, and L. T. Flannelly, "The t-test: An influential inferential tool in chaplaincy and other healthcare research," *Journal of Health Care Chaplaincy*, vol. 24, no. 1, pp. 30–39, 2018, pMID: 28622103. [Online]. Available: https://doi.org/10.1080/08854726.2017.1335050

Appendix

In the appendix the different questionnaires used for the study are presented. The first questionnaire is the questionnaire Q0, which was presented before the participant played any levels. The other questionnaires were filled out after playing their corresponding level. They are presented in the following order of levels, “Instagram hears my conversations”, “Flashlight could steal my data” and “ShoppingToGo sends spam messages”. The headline under the title is used to identify the questionnaire. The *identifier* field is used to identify the participant. The *version* field is representing the variant that was played, while the *example* field represents the played level. The *nr* field is used as a sequence indicator starting at 0 in which the participant has to answer the questionnaires.

Furthermore, the code of *Make my phone secure!* as well as the unfilled and filled questionnaires are available on the delivered CD. Additionally, the python script used for data evaluation with all used *Excel* files will be saved on the CD as well.

Questionnaire

Identifier: Version: Example: Before Nr:

The data will be evaluated anonymously. Please answer spontaneously.

About you

Age:

Gender:

- o *Male*
- o *Female*
- o *Non-binary*
- o *No answer*

For which permissions does your favorite application ask?

Your favorite application:_____

Answer:

_____
_____
_____
_____

How do you handle Android permissions?

- o I don't know what Android permissions are
- o I don't care about Android permissions
- o I'm aware of their consequences but always grant them
- o I'm not aware of their consequences and always grant them
- o I consciously give applications only the permissions I want them to have
- o None of these answers is describing me correctly

When you grant an application access to your microphone, what could it do? Multiple answers could be correct.

- o record audio without your knowledge
- o record audio whenever it wants
- o use the recorded audio, e.g. for advertisements
- o **only** record audio when you explicitly tell the application to, e.g. recording a voice message
- o **only** record audio when it is notifying you about the usage

Do you think it's likely that social media applications (Instagram, WhatsApp, Facebook etc.) with access to the microphone can record audio without notifying you?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that social media applications with access to your microphone are able to use recorded audio to give you personalized advertisements?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that access to location and microphone allows an application (like the official app of the Spanish football league) to find bars or restaurants which are broadcasting football games illegally?

very unlikely neutral very likely

o o o o o o o

Which of the following permissions do you find okay to grant social media applications?

- o Location
- o Microphone
- o Camera
- o Contacts
- o Storage
- o Phone
- o None of these
- o I don't care about android permissions I give to applications

When you grant an application access to your storage, what could it do? Multiple answers could be correct.

- o search through and write to your storage without your knowledge
- o search through and write to your storage whenever it wants
- o harm you or your data, e.g. leak secret files, delete files, download files to your phone
- o **only** search through and write to your storage when you explicitly tell the application to, e.g. save or load a file
- o **only** search through and write to your storage when it notifying you about the usage

Do you think it's likely that widget applications (Flashlights, Clocks etc.) with access to your storage can search through your data?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that widget applications with access to your storage and the internet can steal data from your phone?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that widget applications with access to your storage and the right to install packages can install other malicious software to your phone?

very unlikely neutral very likely

o o o o o o o

Which of the following permissions do you find okay to grant widget applications?

- o Location
- o Microphone
- o Camera
- o Contacts
- o Storage
- o Phone
- o None of these
- o I don't care about android permissions I give to applications

When you grant an application access to your contacts, what can it do? Multiple answers could be correct.

- o read the contact information of your contacts without your knowledge
- o read the contact information whenever it wants
- o abuse the contact information, e.g. to send phishing or spam messages
- o **only** use the contact information when you explicitly tell the application to, e.g. to add a friend
- o **only** use the contact information when it is notifying you about the usage

Do you think it's likely that shopping applications (Amazon Shopping, McDonalds etc.) with access to your contacts can read the information of the contacts stored on your phone without notifying you?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that applications with access to your contacts can use the information from your contacts to send them spam or phishing messages?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that malicious applications with granted permissions for contacts and SMS can spread messages and links from your phone to your contacts?

very unlikely neutral very likely

o o o o o o o

Which of the following permissions do you find okay to grant shopping applications?

- o Location
- o Microphone
- o Camera
- o Contacts
- o Storage
- o Phone
- o None of these
- o I don't care about android permissions I give to applications

Questionnaire

Identifier: Version: Example: Instagram Nr:

The data will be evaluated anonymously. Please answer spontaneously.

When you grant an application access to your microphone, what could it do? Multiple answers could be correct.

- o record audio without your knowledge
- o record audio whenever it wants
- o use the recorded audio, e.g. for advertisements
- o **only** record audio when you explicitly tell the application to, e.g. recording a voice message
- o **only** record audio when it is notifying you about the usage

Do you think it's likely that social media applications (Instagram, WhatsApp, Facebook etc.) with access to the microphone can record audio without notifying you?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that social media applications with access to your microphone are able to use recorded audio to give you personalized advertisements?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that access to location and microphone allows an application (like the official app of the Spanish football league) to find bars or restaurants which are broadcasting football games illegally?

very unlikely neutral very likely

o o o o o o o

Which of the following permissions do you find okay to grant social media applications?

- o Location
- o Microphone
- o Camera
- o Contacts
- o Storage
- o Phone
- o None of these
- o I don’t care about android permissions I give to applications

How much fun did you have with this version?

very boring			neutral			very exciting
O	O	O	O	O	O	O

How informative was this version?

I learned nothing			neutral			I feel enlightened
O	O	O	O	O	O	O

If you have some feedback feel free to use this space:

Questionnaire

Identifier: Version: Example: Flashlight Nr:

The data will be evaluated anonymously. Please answer spontaneously.

When you grant an application access to your storage, what could it do? Multiple answers could be correct.

- o search through and write to your storage without your knowledge
- o search through and write to your storage whenever it wants
- o harm you or your data, e.g. leak secret files, delete files, download files to your phone
- o **only** search through and write to your storage when you explicitly tell the application to, e.g. save or load a file
- o **only** search through and write to your storage when it notifying you about the usage

Do you think it's likely that widget applications (Flashlights, Clocks etc.) with access to your storage can search through your data?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that widget applications with access to your storage and the internet can steal data from your phone?

very unlikely neutral very likely

o o o o o o o

Do you think it's likely that widget applications with access to your storage and the right to install packages can install other malicious software to your phone?

very unlikely neutral very likely

o o o o o o o

Which of the following permissions do you find okay to grant widget applications?

- o Location
- o Microphone
- o Camera
- o Contacts
- o Storage
- o Phone
- o None of these
- o I don’t care about android permissions I give to applications

How much fun did you have with this version?

very boring			neutral			very exciting
O	O	O	O	O	O	O

How informative was this version?

I learned nothing			neutral			I feel enlightened
O	O	O	O	O	O	O

If you have some feedback feel free to use this space:

Questionnaire

Identifier: Version: Example: ShoppingToGo Nr:

The data will be evaluated anonymously. Please answer spontaneously.

When you grant an application access to your contacts, what can it do? Multiple answers could be correct.

- o read the contact information of your contacts without your knowledge
- o read the contact information whenever it wants
- o abuse the contact information, e.g. to send phishing or spam messages
- o **only** use the contact information when you explicitly tell the application to, e.g. to add a friend
- o **only** use the contact information when it is notifying you about the usage

Do you think it's likely that shopping applications (Amazon Shopping, McDonalds etc.) with access to your contacts can read the information of the contacts stored on your phone without notifying you?

very unlikely			neutral			very likely
o	o	o	o	o	o	o

Do you think it's likely that applications with access to your contacts can use the information from your contacts to send them spam or phishing messages?

very unlikely			neutral			very likely
o	o	o	o	o	o	o

Do you think it's likely that malicious applications with granted permissions for contacts and SMS can spread messages and links from your phone to your contacts?

very unlikely			neutral			very likely
o	o	o	o	o	o	o

Which of the following permissions do you find okay to grant shopping applications?

- o Location
- o Microphone
- o Camera
- o Contacts
- o Storage
- o Phone
- o None of these
- o I don’t care about android permissions I give to applications

How much fun did you have with this version?

very boring			neutral			very exciting
O	O	O	O	O	O	O

How informative was this version?

I learned nothing			neutral			I feel enlightened
O	O	O	O	O	O	O

If you have some feedback feel free to use this space: