



Norwegian University of
Science and Technology

Evaluating the Security and Usability of Emoji-Based Authentication

Martin Kjellevand

Markus Rauhut

Master of Science in Communication Technology

Submission date: June 2018

Supervisor: Lillian Røstad, IIK

Co-supervisor: Per Torsheim, Security Manager at Nordic Choice Hotels

Norwegian University of Science and Technology

Department of Information Security and Communication Technology

Title: Evaluating the Security and Usability of
Emoji-Based Authentication

Students: Martin Kjellevand and Markus Rauhut

Problem description:

Passwords and PINs are used on almost every device, platform and service today, and are the dominating choice for authentication. However, these authentication methods have several shortcomings. In quest of replacing passwords and PINs, graphical passwords are getting increased attention and several graphical authentication schemes have been proposed over the years.

Lately, emojis have been introduced to this topic. Although there exists some research on emojis in mobile authentication, little work has been done on the use of emojis in web authentication. We suspect that emoji-based passwords can be more secure and usable than passwords. The fact that a human brain remembers pictures better than words could lead to increased memorability. Also, the huge emoji character set might facilitate passwords that are more secure than text passwords.

Based on insights from a literature review, we will design and develop a prototype of an innovative emoji-based authentication scheme – EmojiStory. This scheme's security and usability will be evaluated with help of two online surveys. The purpose of this project is to study ways of using emojis to improve user authentication.

Supervisor: Lillian Røstad, IIK

Co-supervisor: Per Thorsheim

Abstract

With the increasing digitization of the world, there is a growing need to prove one's identity and to restrict access to both personal and corporate data. Passwords have several drawbacks, but are still the preferred choice for this purpose. Motivated by the fact that the human brain remembers visual information better than text, graphical password schemes – such as the Android Pattern Lock – have been proposed as an alternative to traditional passwords.

Emojis have become an inherent part of almost every digital text message. More than 2700 emojis are currently available, and this number is constantly increasing. The huge amount of characters can provide passwords with higher security than their text-based equivalents. Only limited research on emoji-based authentication exists, making it an interesting subject to study.

In this project, a literature study on the use of emojis as an alternative to PIN entry and text passwords was conducted. By analyzing the current state of emoji-based authentication, a novel password scheme called EmojiStory was proposed. In EmojiStory passwords are created from predefined stories and emojis selected by the user. The security and usability of the system was evaluated through two online surveys, in which more than 1,700 participants took part.

The results from the surveys suggest that EmojiStory offers good usability. The emoji passwords are easy to remember, password creation and login are fast, and a positive user experience is provided. The results also indicate that EmojiStory offers better security than PIN. However, certain emojis were preferred by the participants. Therefore, further research is needed to compare observed bias in the passwords with that of other authentication systems. We also advise that further studies on the memorability provided by EmojiStory should be conducted.

Sammendrag

I takt med den økende digitaliseringen av verden, er det et voksende behov for å bevise sin egen identitet og begrense adgangen til både personlig informasjon og bedriftsdata. Passord har flere ulemper, men er fortsatt det foretrukne valget for dette formålet. Motivert av at den menneskelige hjernen husker visuell informasjon bedre enn tekst, har grafiske passordsystemer – som for eksempel Android Pattern Lock – blitt foreslått som et alternativ til tradisjonelle passord.

Emojis er blitt en essensiell del av nesten alle digitale tekstmeldinger som sendes. Mer enn 2700 emojis er for tiden tilgjengelige, og dette tallet øker stadig. Den enorme mengden tegn kan gi et grunnlag for passord med høyere sikkerhet enn deres tekstbaserte alternativer. På nåværende tidspunkt eksisterer det kun begrenset med forskning på emoji-basert autentisering, noe som gjør det til et interessant emne å studere.

I dette prosjektet ble det gjennomført en litteraturstudie om bruk av emojis som et alternativ til PIN-koder og tekstpassord. Ved å analysere den nåværende tilstanden for emoji-basert autentisering ble det foreslått et nytt passordsystem som heter EmojiStory. I EmojiStory opprettes passord fra forhåndsdefinerte historier og fra emojis valgt av brukeren. Sikkerheten og brukervennligheten til systemet ble evaluert gjennom to nettbaserte undersøkelser, som mer enn 1700 personer deltok i.

Resultatene fra undersøkelsene antyder at EmojiStory har god brukervennlighet. Emoji-passordene er enkle å huske, passorddannelse og innlogging er raskt, og brukeropplevelsen er bra. Resultatene henter også til at EmojiStory gir bedre sikkerhet enn PIN-koder. Imidlertid ble enkelte emoji-er foretrukket av deltakerne. Derfor er det nødvendig med ytterligere forskning for å kunne sammenligne observerte forstyrrelser i passordene med andre autentiseringssystemer. Vi anbefaler også å gjennomføre videre undersøkelser for å fastlå hvor vanskelig eller enkelt det er å huske passord som er laget med EmojiStory.

Preface

This thesis is original and independent work by Martin Kjellevand and Markus Rauhut. It was conducted during the spring semester of 2018 and is the final contribution to the master's degree in Communication Technology at the Norwegian University of Science and Technology (NTNU).

The idea behind this research arose from the desire to develop better methods for user authentication. Associate professor Lillian Røstad at the Department of Information Security and Communication Technology (IIK) was willing to supervise this project. We want to express our sincere gratitude for her support and guidance during the past year. Her knowledge and advice have helped us to keep on track the entire time.

Our thanks also go to Per Thorsheim. His creativity and numerous ideas contributed to the development of our emoji-based password scheme – EmojiStory. Neither would we have received so much response and feedback if he had not actively shared our survey with his enormous network.

Finally, we would like to thank our family, friends and especially girlfriends for all their feedback and emotional support.

Contents

List of Figures	xi
List of Tables	xv
List of Acronyms	xvii
1 Introduction	1
1.1 Background and Motivation	1
1.2 Research Questions	2
1.3 Methodology	2
1.3.1 Literature Study	2
1.3.2 Development of an Emoji-Based Password Scheme	4
1.3.3 Data Collection	4
1.3.4 Data Analysis	4
1.4 Thesis Structure	4
2 Fundamentals of Authentication	5
2.1 Authentication Methods	5
2.2 Text Passwords	6
2.2.1 Password Issues	6
2.2.2 Password Managers	8
2.3 Graphical Authentication	8
2.3.1 Graphical Authentication Schemes	9
2.4 Password Space and Entropy	11
2.4.1 Theoretical and Practical Password Space	12
2.4.2 Password Entropy	12
3 Emoji-Based Authentication	15
3.1 Emojis	15
3.1.1 Statistics	15
3.1.2 Character Growth	16
3.2 Password Schemes Based on Emojis	17
3.2.1 Emoji Passcode	17

3.2.2	EmojiAuth	17
3.2.3	PictoPass	19
3.3	Memorability of Emoji Passwords	20
3.4	Password Selection Strategies	20
3.5	Guessability of Emoji Passwords	22
3.6	Shoulder-Surfing	22
3.7	Emoji Presentation	23
4	EmojiStory: Designing an Emoji-Based Password Scheme	27
4.1	Requirements	27
4.1.1	Secure Mobile and Web Authentication	28
4.1.2	High Memorability of Created Passwords	28
4.1.3	Short Password Creation and Login Time	28
4.1.4	Efficient Use of a Virtual Emoji Keyboard	29
4.1.5	Uniform Presentation of Emojis	29
4.2	Functionality	30
4.2.1	Password Creation Procedure	30
4.2.2	Emoji Design	30
4.2.3	Stories	32
4.2.4	Keyword Categories and Options	32
4.2.5	Emoji Keyboard and Login Process	33
4.2.6	Intended Application	34
4.3	Theoretical Password Space and Entropy	36
4.4	User Experience Testing	38
4.4.1	Emoji Preview	38
4.4.2	Back Button	39
4.4.3	Evolving Stories	40
4.5	Scheme Issues	40
5	Experiment Setup	41
5.1	Survey	41
5.1.1	Planning and Conducting the Survey	42
5.1.2	Survey Design	44
5.1.3	Survey Setup	46
5.1.4	Pre-Testing the Survey	50
5.2	Follow-up Survey	55
5.2.1	Setup and Design	55
5.2.2	Improving the Strategy Question	58
5.2.3	Sampling Technique and Sample Size	59
5.2.4	Changing EmojiStory	59
5.3	Ethics	59

6	Results and Discussion	61
6.1	Preprocessing the Survey Data	61
6.2	Initial Survey	61
6.2.1	Participation	61
6.2.2	Participant Background	62
6.2.3	Password Memorability	64
6.2.4	Scheme Efficiency	66
6.2.5	Memorization Strategy	71
6.2.6	User Satisfaction	72
6.2.7	Practical Password Space	75
6.2.8	Shoulder-Surfing	83
6.3	Follow-Up Survey	83
6.3.1	Participation	83
6.3.2	Participant Background	84
6.3.3	Password Memorability	84
6.3.4	Scheme Efficiency	86
6.3.5	Memorization Strategy	87
6.3.6	Selection Strategy	87
7	Conclusion and Future Work	91
7.1	Future Work	92
7.1.1	Increasing the Keyboard Size and Password Length	92
7.1.2	Testing the Memorability of Multiple Emoji Passwords	92
7.1.3	Creating Stories Using Artificial Intelligence	93
7.1.4	Generating Emoji Passwords Based on Stories	93
7.1.5	Further Exploration of the Practical Password Space	93
7.1.6	Applying Guessing Attacks	93
	References	95

List of Figures

1.1	The methodology used in this project.	3
2.1	Three examples of weak and insecure passwords.	7
2.2	A password that meets various password criteria.	7
2.3	An illustration of Blonder’s patent, the first graphical password scheme. A user creates a password by determining certain <i>tap regions</i> (indicated as squares with numbers inside) in an image.	9
2.4	PicturePIN	10
2.5	Passfaces	10
2.6	The Story scheme (Davis et al.)	11
2.7	Android Pattern Lock	11
3.1	The most used emojis on the Kika Keyboard (1), EmojiXpress (2) and Twitter (3).	16
3.2	The total number of emoji characters between 2010 and 2018.	16
3.3	Emoji Passcode (Intelligent Environments)	17
3.4	EmojiAuth (Kraus et al.)	18
3.5	PictoPass (Golla et al.)	19
3.6	Presentation of the Hugging Face emoji for three different vendors.	23
3.7	Examples of emoji design enhancement and redesign.	23
3.8	Changed emoji meaning. Example (1) shows the Pistol emoji which was changed to a water gun in Apples iOS 10.0 upgrade. Example (2) shows the Cookie emojis presentation on Samsung devices. Prior to Experience version 9.0, the emoji was rendered as a saltine cracker.	24
3.9	The Shocked Face With Exploding Head character in emoji presentation (left) and text presentation (right).	24
3.10	The emojis used in the Seitz et al. study.	25
4.1	Comparison of two virtual keyboard layouts on Apple iOS 11.2.	29
4.2	The different steps to create a password with EmojiiStory.	31
4.3	All the stories that the prototype provides.	32
4.4	The keyword categories in EmojiiStory.	33

4.5	The emoji keyboard and the feedback given to the users after they selected the fourth emoji.	35
4.6	EmojiStory implemented as a browser extension.	36
4.7	The conversion of the emoji password to their text representations.	36
4.8	The situation before an emoji preview was implemented.	39
4.9	The situation after an emoji preview and a back button were added.	39
5.1	The different instructions in the survey.	46
5.2	Memorization	47
5.3	Strategy	47
5.4	Confusion	48
5.5	Enjoyment	48
5.6	Emoji usage	49
5.7	Background	49
5.8	Questions regarding gender, age and nationality.	50
5.9	Closing statement	51
5.10	Making the EmojiStory instructions more understandable.	52
5.11	Making the EmojiStory instructions less overwhelming.	53
5.12	Changes made to the gender question.	54
5.13	Changes made to the strategy question.	55
5.14	A comparison of the text and emoji password creation process in the follow-up survey.	56
5.15	A comparison of text vs. emoji password login.	57
5.16	Opening questions in the follow-up survey.	57
5.17	Changes made to the questionnaire.	58
6.1	A summary of different participant background information.	62
6.2	The age distribution for different groups of ages.	63
6.3	The use of emojis among all participants.	65
6.4	Median and Interquartile Mean (IQM) password creation times.	67
6.5	Median and IQM login times for the first and second authentication processes.	68
6.6	IQM login times categorized by device type.	69
6.7	Average time spent on the EmojiStory instructions depending on the authentication results.	71
6.8	Average time spent on the summary screen depending on the authentication results.	72
6.9	Memorization strategy among all survey participants.	73
6.10	The distribution of enjoyment among all participants.	73
6.11	The percentage of participants who thought EmojiStory was or was not fun to use, based on how often they use emojis.	74

6.12	The percentage of participants who thought EmojiStory was or was not fun to use, based on their background.	75
6.13	The distribution of confusion among all participants.	76
6.14	Three different password positions that were allocated to users exactly three times each. The numbers show the order of the keys in the corresponding password.	77
6.15	The distribution of the first and last password characters at different key positions.	77
6.16	The distribution of story descriptions among all participants.	79
6.17	The distribution of the participants' story descriptions for each story template.	80
6.18	The three most and least popular emojis from the food category.	81
6.19	The three most and least popular object emojis used in story 4.	81
6.20	The distribution of word selections from the person category in story 3.	81
6.21	The distribution of words selected from the country category in story 1. Only a selection of the words are shown.	82
6.22	The results from the third authentication process in follow-up survey, grouped by password type.	84
6.23	The distribution of time spent thinking of password, based on password type.	86
6.24	The distribution of the memorization strategy used by participants with emoji passwords after first login (left) and third login (right).	87
6.25	Frequencies of password selection strategies.	88
6.26	An illustration of how distinct two passwords created with different selection strategies can be.	88

List of Tables

1.1	Examples of keywords used when searching for literature.	3
3.1	Strategy frequencies for the selection of emoji passwords. Some participants said they used more than one strategy.	21
4.1	The number of emojis (keywords) in each category.	34
6.1	Different numbers for the participation of people in the survey.	62
6.2	The distribution of origin among all survey participants.	64
6.3	The use of emojis several times a day for different age groups.	65
6.4	The results from the authentication processes. Both times the participants were given three attempts to successfully authenticate.	66
6.5	Statistical significance for login time based on device type.	69
6.6	Statistical significance for time used on the EmojiStory instructions and authentication result.	71
6.7	Statistical significance for time spent on the summary screen based on the authentication result.	72
6.8	Different numbers for the participation of people in the follow-up survey.	83
6.9	Average time between second and third login depending on participants' password type and authentication result.	85

List of Acronyms

2FA Two-Factor Authentication.

ACM Association for Computing Machinery.

ASCII American Standard Code for Information Interchange.

IEEE Institute of Electrical and Electronics Engineers.

IP Internet Protocol.

IQM Interquartile Mean.

IT Information Technology.

MFA Multi-Factor Authentication.

NIST National Institute of Standards and Technology.

NSD Norwegian Centre for Research Data.

NTNU Norwegian University of Science and Technology.

OS Operating System.

OTP One-Time Password.

PDA Personal Digital Assistant.

PIN Personal Identification Number.

SVG Scalable Vector Graphics.

UTS Unicode Technical Standard.

UX User Experience.

Chapter 1

Introduction

This chapter first describes the background and motivation for this project, defines the primary research questions and illustrates the methodology used, before concluding with an overview of the subsequent chapters.

1.1 Background and Motivation

Despite the many possibilities of authentication and the sheer number of known issues (see Section 2.2.1), text-based passwords are still the first choice [1, 2]. Although digital technology has undergone enormous development, there exists no known method that offers both perfect usability and security.

In quest of replacing text passwords, graphical passwords are getting increased attention. While text passwords involve input of keyboard characters, the idea behind graphical passwords is to relate a memorized secret to visual information such as images. Small pictograms, called emojis, have become very popular in recent years. In fact, an emoji was awarded the *Word of the Year* by Oxford Dictionaries in 2015 [3]. Furthermore, emojis are often used under positive circumstances [4]. The huge amount of existing emojis can be utilized to provide a large theoretical password space. At the same time, the Unicode emoji list [5] is continuously expanding.

Miller [6] claimed that people find it easier to remember sequences of objects, so-called *chunks*, when they are familiar to them. Those chunks can be letters, numbers, words or even emojis. Any new emoji which is nominated for inclusion into the Unicode standard must meet a number of requirements. One of these requirements is to provide evidence that the emoji is frequently used [7]. An approved emoji is therefore likely to represent something familiar to most people. As a result, passwords made of emojis may be easier to remember.

Within the last few years, several graphical authentication methods involving emojis have been proposed. In 2015 *Intelligent Environment* released a banking application

1. INTRODUCTION

which allowed users to log in using emojis [8]. Although there exists some research on emojis as an alternative to traditional Personal Identification Number (PIN) entry [9, 10], little work has been done on the usage of emojis in web authentication. Few emoji-based authentication schemes have been proposed and all of them are targeted at mobile authentication [10, 8]. The purpose of this research is to study ways of using emojis to improve user authentication.

1.2 Research Questions

We have established the following research questions:

- **RQ1:** What is the current state of emoji-based authentication?
- **RQ2:** How can a novel password scheme based on emojis be designed?
- **RQ3:** Can emoji passwords provide satisfactory security and usability?

In this project, the term *usability* embraces *memorability* (to what extent people remember their passwords), *efficiency* (how much time they need for different tasks such as password creation and login) and *satisfaction* (whether they enjoy the authentication process).

1.3 Methodology

Several methods have been identified to answer the research questions. Since RQ1 relates to existing literature in the field of emoji-based authentication, a literature study is necessary. RQ2 requires the design and development of an emoji-based password scheme. This work is only possible by first answering RQ1. RQ3 can be answered by evaluating the security and usability of the developed password scheme. This was achieved by collecting data from two surveys. The research process is visualized in Figure 1.1

1.3.1 Literature Study

We have conducted a literature study on authentication. Special attention has been paid to the use of emojis in the field of authentication. Analyzing the current state of knowledge helped us to develop our research questions, scope our research in the context of what has been done, and to answer RQ1.

It is difficult to find relevant literature on the web due to the enormous amount of material that exists [11]. Fortunately the Internet is full of useful resources that simplify the search for literature. We used online databases such as ACM Digital Library [12], Google Scholar [13] (a search engine which only searches academic publications), and digital libraries like IEEE Xplore [14] and Springer [15].

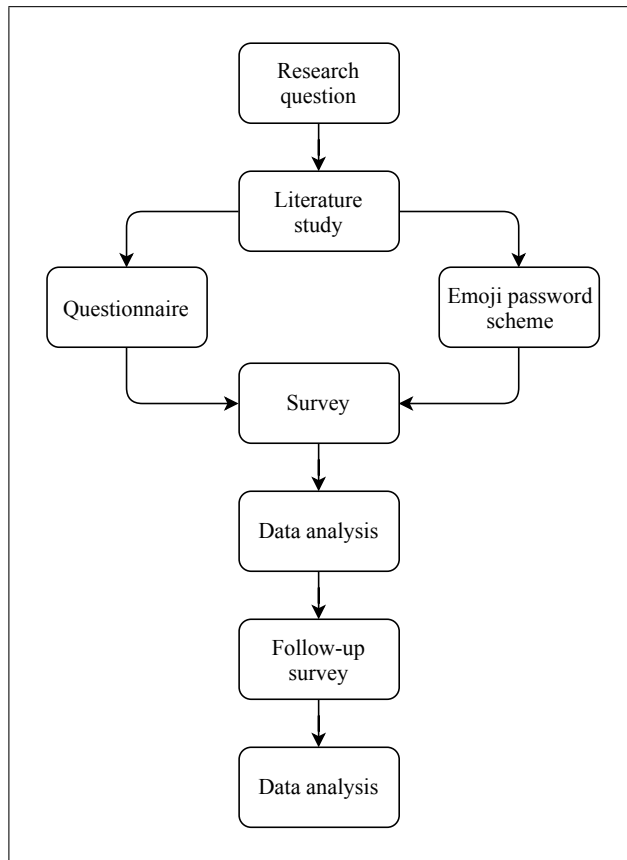


Figure 1.1: The methodology used in this project.

Keywords were used to limit the search for relevant literature. A selection of those are listed in Table 1.1. Multiple keywords were often used simultaneously in combination with the logical operator AND.

Emoji(s)	Authentication	Entropy
Memory	Graphical password	Security
Usability	Issues	Text password

Table 1.1: Examples of keywords used when searching for literature.

The authorship, credibility and authenticity of material on the Web is often unproven and questionable. Consequently, books, journal articles and conference papers were largely used, while content on web pages was avoided. The literature study contains material of high quality that has been reviewed and published.

1. INTRODUCTION

1.3.2 Development of an Emoji-Based Password Scheme

To explore the opportunities of using emojis to improve user authentication, an Information Technology (IT) artifact called EmojiStory was developed. EmojiStory is a password scheme based on emojis. The development of the scheme is not the main focus of our research. The intention is not to develop a full-grown system that can be used without any further research. The role of EmojiStory is to function as a prototype which illustrates the possibilities that emojis can offer. The scheme is described in detail in Chapter 4.

1.3.3 Data Collection

All data was collected via online surveys, as we need a large amount of information to answer the research questions. Since we would like to, among other things, assess usability, the sample should include a broad representation of the entire population. For this purpose, online surveys are a great choice [11]. Furthermore, lack of time makes other data generation methods, such as interviews and observations, difficult to carry out. The surveys are described in detail in Chapter 5.

1.3.4 Data Analysis

The collected data was analyzed in order to evaluate the security and usability of emoji-based authentication. We used tables, charts and graphs to present the data in a visual way and to look for patterns. We have also used statistical methods to find further patterns and determine whether or not the patterns we found in the data were significant.

1.4 Thesis Structure

This thesis is divided into seven chapters. Chapter 2 provides an introduction to user authentication and introduces various graphical authentication schemes. Chapter 3 deals particularly with emojis and their use in the field of information security. The design process of EmojiStory is presented in chapter 4. Chapter 5 explains the setup and execution of the different experiments, while their results are presented and discussed in Chapter 6. The last chapter, Chapter 7, provides a conclusion and suggestions for future work.

Chapter 2

Fundamentals of Authentication

Authentication is the process of verifying someone's identity [16]. This *someone* could be a user, device or any other entity in a system. Consequently, authentication is a security objective for almost every information system and a crucial part of digital communication [17].

This chapter will serve as a brief introduction to authentication. Since the shortcomings of text passwords are the main motivation for this research, they are given special attention. Graphical authentication is also examined in detail, as an understanding of this topic is important for finding out how emojis can be used in authentication.

2.1 Authentication Methods

There exists a vast number of ways to perform authentication, but they can be categorized into three different types of methods:

- Knowledge-based authentication (something you know)
- Token-based authentication (something you have)
- Biometric-based authentication (something you are)

Knowledge-based authentication relies on something the user *knows*. When using this type of authentication, a secret is established between the authenticating entity and the user. The best example of knowledge-based authentication is perhaps what most people associate with authentication; passwords [16].

Token-based authentication is based on something the user *has* which can be used to obtain a token. You are probably exposed to this method almost every day when logging in to your online banking application using a One-Time Password (OTP) generator, a small device or software that generates a sequence of numbers or characters [16].

2. FUNDAMENTALS OF AUTHENTICATION

Biometric-based authentication involves something the user *is*. When applying this method, something about the user's biology is measured. Examples of such schemes are fingerprint, iris and facial recognition [16].

Many modern systems today provide what is known as Multi-Factor Authentication (MFA). MFA combines two or more independent authentication techniques to verify a person's identity [18]. Two-Factor Authentication (2FA), a subgroup of the MFA that uses two independent factors for authentication, is widely used. Typically, 2FA combines something you know with something you have, which could be a password and a mobile phone.

2.2 Text Passwords

As indicated in the previous section, there is a wide range of applications for token- and biometric-based authentication. Yet, most systems implementing these methods still depend on knowledge-based authentication as a fallback. A smartphone with a fingerprint sensor, for instance, will trigger users to input their password if it cannot detect the correct fingerprint after various attempts. For this reason, passwords are still important and widely used. Furthermore, all identified emoji-based authentication schemes which are outlined in Chapter 3 are implementations of the knowledge-based authentication method. Therefore, the focus of this thesis lays on this type of authentication.

In the field of computer security, passwords can be divided into two different types: text passwords and graphical passwords (the latter is introduced in Section 2.3). Text passwords are strings of characters with varying length. These characters may be uppercase and lowercase letters, digits, and special characters such as punctuation marks.

2.2.1 Password Issues

It is no secret that text passwords have several issues. The never-ending search for better authentication methods confirms this assumption. This section gives an outline of identified problems regarding password quality, reuse and entry, before introducing so-called password managers which improve the situation in some way.

Password Quality

People often tend to choose insecure passwords (see Figure 2.1 for some examples) when not restricted by any rules [19]. One reason for this behavior might be the lack of knowledge about how to form strong passwords, but it is more likely that this is a consequence of creating passwords that are easy to remember. Regardless of whether

weak passwords are created knowingly or unknowingly, they are more vulnerable to malicious attacks.

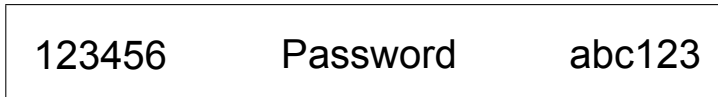


Figure 2.1: Three examples of weak and insecure passwords.

In order to counteract this behavior, many services have developed password-composition policies to enhance password strength. Enforcing a certain password length, the use of numbers, capital letters and punctuation are some of the restrictions that are practiced on many websites today. Unfortunately, passwords satisfying these criteria tend to be more difficult to remember [20, 21]. Figure 2.2 shows an example of a password that takes different criteria into account.

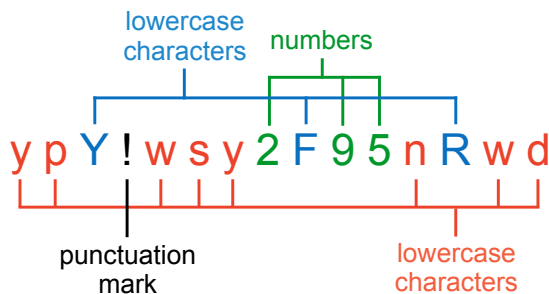


Figure 2.2: A password that meets various password criteria.

Password Reuse

According to a large-scale study of web password habits carried out in 2007, the average user of an online service has 6.5 different passwords which are used on 25¹ distinct password-protected web accounts [19].

Password reuse can have serious consequences. Ives et al. [22] introduced the phrase *domino effect of password reuse*. When a hacker compromises a user's password, it is very likely that the same password is used somewhere else, giving the hacker access to multiple services. Furthermore, users tend to reuse elements from earlier passwords when they create new ones [23]. For instance, adding a number at the start or end of a former password while retaining a base phrase is quite common [1].

¹ Due to the enormous increase in online services in recent years, it is likely that this number is even higher today.

2. FUNDAMENTALS OF AUTHENTICATION

Password Entry

Over the last years, smartphone and tablet usage has increased tremendously. As a result, password entry and creation have become necessary on mobile devices. Such devices use virtual keyboards (see Figure 4.1(a)) that differ from their physical counterparts. For example, small screen sizes limit the number of keys visible at the same time. Research shows that text passwords are less usable on mobile devices than on devices with physical keyboards [24, 25].

2.2.2 Password Managers

In an attempt to make passwords stronger and more unique, and removing the necessity to remember them at all, so called *password managers* have emerged and gained popularity. A password manager can store a user's passwords for different web applications and services in one single place. Some managers keep the encrypted passwords on the same device, while others store them online. Many different password managers exist today. LastPass² and Dashlane³ are popular examples.

Usually, the passwords are accessed via a browser extension⁴. When using a password manager, you only need to remember a master password. This particular password is used to authenticate with the manager, and to decrypt all the other passwords. Browser extensions for password managers can often insert username and password combinations into login forms automatically.

Although password managers solve some of the issues described in Section 2.2.1, they also introduce new ones. For example, forgetting the master password might lead to losing access to all the other passwords. Furthermore, it may take many steps to insert a password from the password manager into a mobile application. It is, however, possible to integrate password managers into applications, but it is up to the developers of these applications to support them or not.

2.3 Graphical Authentication

In the pursuit of solving the issues related to text passwords, graphical authentication is getting increased attention. While text passwords involve input of keyboard characters, the idea behind graphical passwords is to relate the secret to visual information such as images. The motivation for doing this is based on the belief that people find it easier to remember visual information than text. This effect has been

² <https://www.lastpass.com/>

³ <https://www.dashlane.com/>

⁴ Browser extensions are software application generally created by a third party to extend or customize a web browser's functionality [26].

demonstrated in several psychological studies [27, 28, 29], and is referred to as the *picture superiority effect* [30].

The picture superiority effect was demonstrated already in the 1960s [31, 32]. The consequence of this effect is that items we view as pictures are easier to remember than items we study as text. However, the picture superiority is still debated and research has shown that the effect depends on the content of the information that is to be remembered. In research, the effect has often been tested by instructing participants to recognize items that are displayed individually or in pairs [32, 27]. Therefore, it is uncertain how evident the effect is in graphical authentication, since users usually have to identify their secret from a large amount of visual information.

2.3.1 Graphical Authentication Schemes

Although the motivation behind graphical authentication is old, the idea was not described until the middle of the 1990s by Greg Blonder. He presented the first graphical password scheme in a patent published in 1996 [33]. An illustration of it can be seen in Figure 2.3. In the scheme, a user creates a password by determining certain *tap regions* in an image. In Figure 2.3 such tap regions are displayed as small squares with numbers inside. In order to authenticate, the user has to identify the correct tap regions in a specific order. The scheme was only proposed in Blonder’s patent, it was not further analyzed nor was it developed. However, the same concept has been realized in a graphical password scheme called *PassPoints* [34].

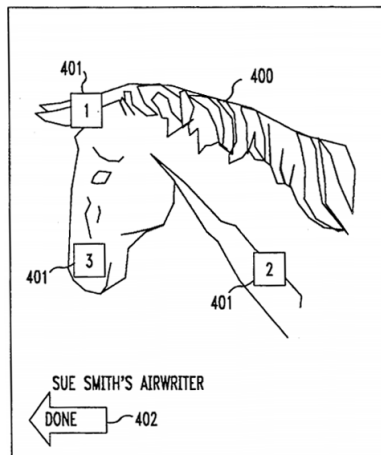


Figure 2.3: An illustration of Blonder’s patent, the first graphical password scheme. A user creates a password by determining certain *tap regions* (indicated as squares with numbers inside) in an image.

2. FUNDAMENTALS OF AUTHENTICATION

In 2002, a graphical authentication scheme called *PicturePIN*⁵ was developed by Pointsec Mobile Technologies [35]. PicturePIN is a graphical PIN system where the numbers are replaced with images. The intention was to make users create stories based on the images. The images are shuffled each time and the length of passwords created with PicturePIN can vary from 4 to 13 images. There is no research on whether this scheme offers greater memorability than traditional PIN entry or not. Figure 2.4 illustrates the PicturePIN scheme used on a Personal Digital Assistant (PDA).



Figure 2.4: PicturePIN

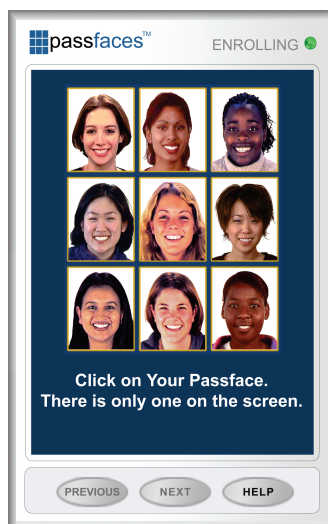


Figure 2.5: Passfaces

*Passfaces*⁶ is a graphical authentication scheme that was developed by *Passfaces Corporation* (originally *Real User Corporation*) [36]. The scheme is similar to *PicturePIN*, but images of common objects are replaced with images of human faces. Also, passwords are not selected by users, but randomly determined by the *Passfaces* scheme [37]. Users are given a password that consists of a random set of faces. The amount of faces can range from three to seven. During the authentication process, the faces are displayed together with eight other faces that serve as decoys. As seen in Figure 2.5, users have to identify the correct faces, one at a time, in order to authenticate themselves.

In earlier releases of *Passfaces*, passwords were not randomly assigned, but user-chosen. Research has shown that this implementation resulted in biased passwords [38]. Faces chosen by users were affected by the users' skin tone, and both men

⁵ http://www.pencomputing.com/newspro_pen_data/arc7-2002.html

⁶ http://www.passfaces.com/enterprise/news/logo_and_graphics.htm

and women chose female faces far more often than male faces. Studies have also shown that this implementation offers good memorability, but login times greater than those of text passwords [39]. The Passfaces scheme has not been scientifically studied after the inclusion of random passwords.

In 2004, Davis et al. [38] developed a graphical password scheme called *Story*. In this scheme, a user selects a password that consists of k unique images from a set of n images. The intention was that the password should represent a story. Therefore, the images the users can chose from illustrates a wide variety of things (see Figure 2.6). Davis et al. found that the Story scheme offered lower memorability then Passfaces, but the passwords were less predictable [38].

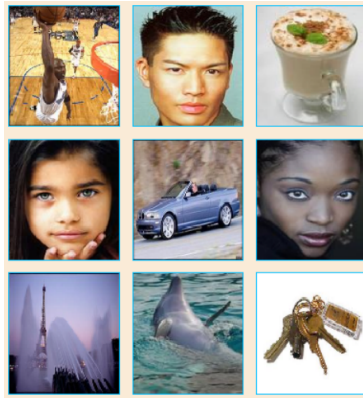


Figure 2.6: The Story scheme (Davis et al.)

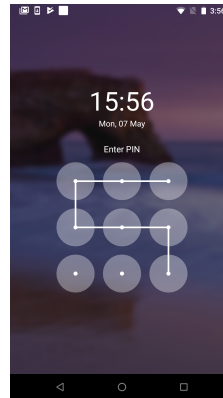


Figure 2.7: Android Pattern Lock

So far, the graphical authentication schemes that have been mentioned, have neither been well known nor extensively used. However, when the Android Operating System (OS) was released by Google in 2008, it came with a gesture-based protection mechanism called *Android Pattern Lock* [40]. Android Pattern Lock is perhaps the best known and most commonly used graphical password scheme today. Users authenticate with a self-defined pattern by connecting circles on a 3x3 grid. Figure 2.7 illustrates the Android Pattern Lock scheme. The security of Android Pattern Lock has been extensively researched and multiple studies show that people tend to create predictable unlock patterns. For instance, in 2013, Uellenbeck et al. [41] found that a common selection strategy is to start at the top left corner.

2.4 Password Space and Entropy

As already mentioned several times during this chapter, people often create predictable passwords. In this section we will go more into depth on this topic and explain how

2. FUNDAMENTALS OF AUTHENTICATION

it affects the security of authentication systems by introducing the terms *password space* and *password entropy*.

2.4.1 Theoretical and Practical Password Space

The size of the *theoretical password space* of an authentication scheme, is a common concept in the field of authentication and is often used when discussing the security of a scheme. Theoretical password space (also referred to as key space or password space [42]) can be defined as the number of all possible passwords offered by a password scheme [43]. For instance, the size of the theoretical password space of text passwords, where the full 95 American Standard Code for Information Interchange (ASCII) character set is allowed and eight characters are required, can be calculated as: $95^8 = 6.63 \times 10^{15}$. This is obviously a very large number, which is needed to make the password scheme resistant to *guessing attacks*.

In a guessing attack, the attacker attempts to determine a password by trying every possible combination in the theoretical password space (i.e. brute-force attack) or by trying passwords that have higher probability (i.e. dictionary attack). Therefore, authentication schemes with small theoretical password spaces or with skewed password distributions are particularly susceptible to guessing attacks. Still, such systems are common and can be useful. Four-digit PINs only offer a theoretical password space of 10,000 (10^4), but is perhaps one of the most widespread authentication schemes today. The reason for this is that its application is not vulnerable to *offline* guessing attacks, which means that it is not possible for an attacker to make endless guesses. PIN codes are either used in combination with a mobile device or credit card, or in combination with another authentication system (often a token-based authentication method).

Although the theoretical password space is an essential part of an authentication scheme, the *practical password space* is a more important concept. People often use a predictable strategy when they select their password [19, 38]. As a result, user-chosen passwords tend to fall into a subset of the theoretical password space which we call the practical password space [43, 44]. As mentioned earlier, the size of the password space is crucial to the security of a scheme since it determines the guessability of the passwords. Therefore, what really matters when evaluating the security of a scheme is the practical password space. Research has shown that graphical authentication is especially vulnerable to guessing attacks since the practical password space of such systems tend to be quite limited [43, 45].

2.4.2 Password Entropy

A concept that is closely related to password space is *password entropy*. Password entropy is commonly used to describe password strength and is defined by National

Institute of Standards and Technology (NIST) as "*the uncertainty in the value of a password*" [46]. In other words, if attackers try to randomly guess a password, entropy is a measurement of how likely they are to succeed.

Password entropy is usually expressed in bits. So, if a randomly selected password is represented by b bits, there are 2^b possible values and you would say that the password has b bits of entropy. In order to give you an example we need the formula for entropy E , which is generally given by:

$$E = \log_2(a^l)$$

Where a denotes the number of possible input characters and l is the password length. In the previous section, we showed that the theoretical password space when the 95 ASCII characters was used to create a password with eight characters, was 6.63×10^{15} . The entropy of such a password would be $\log_2(6.63 \times 10^{15}) = 52.5$ and we say that it has 52.5 bits of entropy.

Notice the extensive use of the words *random* and *randomly* in the discussion of password entropy so far. The reason for this is that it is far more difficult to calculate entropy of passwords that are user-chosen. As already mentioned, users do not select password at random. They tend to choose passwords that they will remember, and as a result the formula described above cannot be used to estimate the entropy of user-chosen passwords. NIST considers past efforts to determine password entropy so imprecise that they have started to use password length to characterize password strength instead [47]. However, they do not specifically express how long a password should be. In this research, both password entropy and length will be used when discussing the security of authentication systems.

Chapter 3

Emoji-Based Authentication

Even though authentication based on emojis is a new concept, there exist some research on the subject. Important insights from this research are presented in this chapter. The chapter also examines necessary background theory on emojis.

3.1 Emojis

An *emoji* is a digital image used in electronic communication (usually inline in text) that can represent things such as weather, vehicles, countries, food, animals etc. or express emotions, feelings, or activities [48, 49]. The word emoji origins from Japanese where *e* means *picture* and *moji* stands for *written character* [50, 49]. In 1999, the first emojis arrived on Japanese mobile phones. However, it was not before in 2009 that the first emojis were added to *Unicode* [51]. The *Unicode Standard* ensures consistent encoding, as well as trouble-free international exchange of characters and text, and is maintained by the *Unicode Consortium* [52, 53].

3.1.1 Statistics

Since emojis became part of Unicode and leading mobile OSs such as Apple's iOS and Google's Android introduced emoji keyboards, the usage of emojis has increased on many social platforms. According to *Instagram* almost half of all text comments and captions on their platform contained emojis in 2015 [54].

The tracking of emojis in different applications indicate that some emojis are used more often than others. Moreover, they suggest which emojis are used the most. In 2016, researchers analyzed a data set from the popular emoji keyboard *Kika Keyboard*. The data set contained 427 million messages which included at least one emoji each. The messages were collected from 3.88 million active users during one month [55]. *Emojitracker* [56] and *Emoji Stats* [57] are examples of services that intercept all emojis used on Twitter and the emoji keyboard *EmojiXpress* respectively. Figure 3.1 shows the most popular emojis on those three platforms.

3. EMOJI-BASED AUTHENTICATION



Figure 3.1: The most used emojis on the Kika Keyboard (1), EmojiXpress (2) and Twitter (3).

3.1.2 Character Growth

Since Unicode adopted emojis in 2010, the number of characters has increased annually (see Figure 3.2). While 1145 emojis were standardized in 2010, more than twice as many (2789 emojis) became part of the standard in 2018. This is an average increase of more than 200 characters per year. The Unicode Consortium estimates that approximately 60 characters will be added annually in the years to come [49].

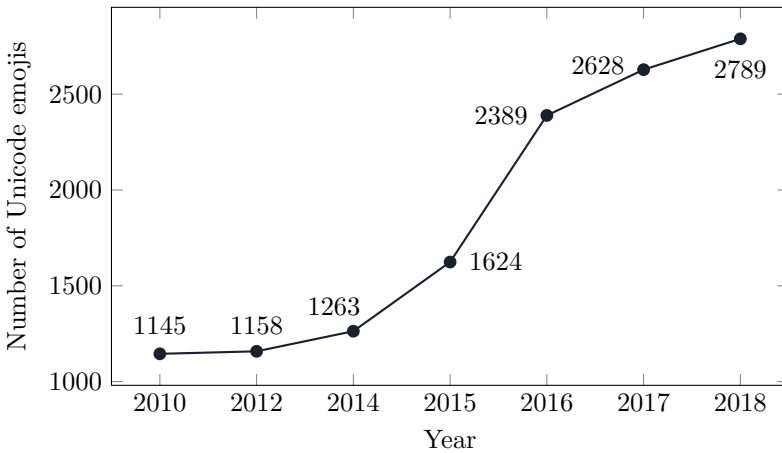


Figure 3.2: The total number of emoji characters between 2010 and 2018.

3.2 Password Schemes Based on Emojis

This section introduces three different emoji-based password schemes called *Emoji Passcode*, *EmojiAuth* and *PictoPass*.

3.2.1 Emoji Passcode

The first authentication scheme using emojis was proposed in 2015 by Intelligent Environments [8], a provider of innovative financial services technology. They designed a concept called *Emoji Passcode*, which replaces the traditional four-digit PIN with a sequence of emojis. As seen in Figure 3.3, users select four emojis from a set of 44. In theory, this scheme is more secure than PIN, since the number of possible combinations is much higher. However, as discussed in Section 2.4.1, the security of a password scheme should be evaluated based on the practical password space. There has not yet been done any formal research to determine the size of the practical password space of *Emoji Passcode*. The main goal of developing the password scheme was to enhance memorability of the user's password, but no research has been done on whether this was achieved.

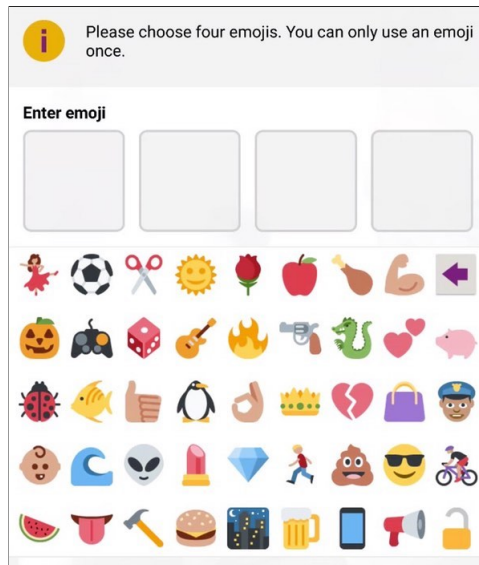


Figure 3.3: Emoji Passcode (Intelligent Environments)

3.2.2 EmojiAuth

In 2016, Kraus et al. developed a study artifact called *EmojiAuth* [58]. As seen in Figure 3.4, *EmojiAuth* is a mobile authentication scheme. *EmojiAuth* provides slightly larger theoretical password space than PIN since the keyboard consist of 12

3. EMOJI-BASED AUTHENTICATION

emojis. With respect to four-digit passwords, the theoretical password space of PIN is 10,000 (10^4), while it is 20,736 (12^4) for EmojiAuth.

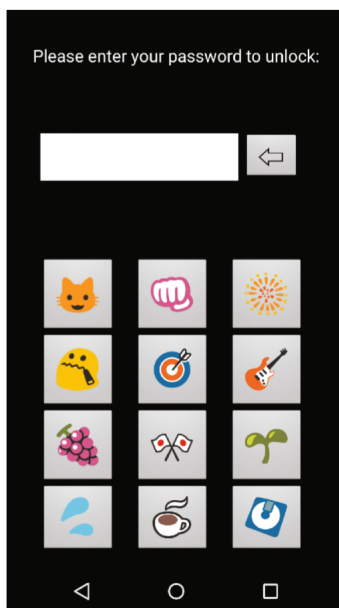


Figure 3.4: EmojiAuth (Kraus et al.)

Kraus et al. identified four requirements for a mobile authentication scheme based on emojis: short login time, system feedback, shoulder surfing resistance and resistance to guessing attacks [58]. They believed that emoji passwords are vulnerable to guessing attacks since research on icon-based authentication has shown that users tend to favor certain icons over others [59]. A recent study on emojis supports this theory [9]. In order to make EmojiAuth resistant to guessing attacks, each user gets an individual keyboard. 761 different emojis are separated into four categories: person and face, object, nature, and activity. When a keyboard is being generated, three emojis are randomly chosen from each category. After the keyboard has been initialized, the position of the emojis are fixed. According to Kraus et al. [58], this method enables a larger practical passwords space, hence the probability that some emojis will be favored, is decreased.

EmojiAuth was used by Kraus et al. to gain insight into how emoji passwords compare to traditional PIN entry and how emojis can be used to improve mobile authentication [10]. More specifically they carried out a lab study where memorability, selection strategies and user experience of emoji passwords were evaluated. They also conducted a field study and a shoulder-surfing experiment. Kraus et al. concluded that emoji-based authentication seems to be a practical alternative to PIN entry.

However, generalizations should be carefully made since the sample size in their research was quite limited. Still, Kraus et al. believe that the consistency between the results from the lab and the field study indicates validity.

3.2.3 PictoPass

Another study on emoji-based authentication was conducted by Golla et al. in 2017 [9]. Similar to Kraus et al., they developed a password scheme based on emojis, which they called *PictoPass*. The scheme was described as a web-based prototype and a variant of EmojiAuth. As seen in Figure 3.5, PictoPass is very much alike EmojiAuth, except that it has a larger keyboard. In their research, Golla et al. conducted a survey where each participant chose an emoji password and answered a questionnaire. Two days later the participants were invited by email to enter their password. They were given three attempts to log in successfully. Since the prototype was optimized for mobile devices, participants were encouraged to take the survey on such devices. The goal of the research was to evaluate the security of the PictoPass scheme.

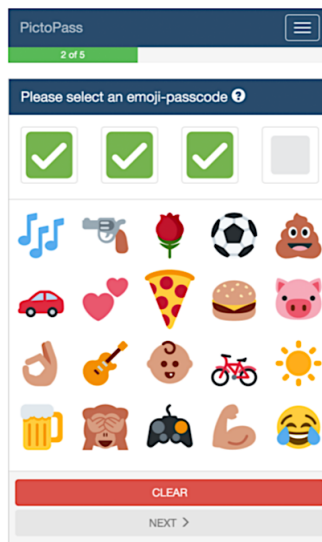


Figure 3.5: PictoPass (Golla et al.)

While the EmojiAuth keyboard has 12 emojis, PictoPass has 20. This keyboard size was chosen since Golla et al. experienced that it was still easy to select from 20 emojis on a small screen, and it ensures that the scheme offers a significantly higher theoretical password space than PINs. A variety of emojis from different categories such as flora and fauna, activities, and food were selected. Since Golla et al. were particularly interested in how the position of emojis on a keyboard affects a user's

3. EMOJI-BASED AUTHENTICATION

selection strategy, the order of the emojis was randomized for each user. Only the positions of the emojis were random, not the actual emojis as in EmojiAuth.

3.3 Memorability of Emoji Passwords

The 53 people who participated in Kraus et al.'s lab study were separated into four subgroups. One group created an emoji password with four emojis, one created an emoji password with six emojis, while the two remaining groups created PIN codes (four digits and six digits). Afterwards, they had to enter their password three times in order to memorize it. A few days later, the participants were invited to a second session to test whether they remembered their password. In average, the time between the first and second session was seven days. Kraus et al. claim that the results of the lab study indicate high memorability of both EmojiAuth passwords and PIN codes. The emoji passwords seem slightly harder to remember than PINs. While 92.3% of the participants in the 6-digit PIN group remembered their password after two weeks, 69.2% of the people in the group with emoji passwords containing six characters remembered their password. However, Kraus et al. did not find any statistically significant differences between the four groups in terms of memorability. They claim that they found that EmojiAuth provided login times comparable to PIN, but no numbers are given.

The field study in Kraus et al.'s research, which included 41 participants, also indicated that PIN codes and EmojiAuth passwords have almost equal memorability. During the field study, EmojiAuth and a PIN application were installed on the participants smartphones as an authentication method for their email application. This way the participants used their emoji passwords and PINs codes regularly over a longer period of time (15-17 days). The participants who used EmojiAuth had 1,924 correct and 58 incorrect unlock attempts, while PIN users had 1,590 correct and 25 incorrect unlock attempts. According to Kraus et al., this suggests that EmojiAuth is a practical authentication method.

In the study by Golla et al., 84.6% of the participants remembered their emoji password after two days. 535 participants successfully entered their password, while 97 failed. Golla et al. believed two days were enough time to measure the memorability of emoji passwords created with PictoPass. However, if this result suggests good or bad memorability is not discussed.

3.4 Password Selection Strategies

Password selection strategies are important to understand, as attackers can take advantage of them in order to guess passwords. For instance, a common PIN selection strategy is to use birth dates. Obviously this is not a good idea since it is very easy

3.4. PASSWORD SELECTION STRATEGIES

for an attacker to discover a persons' birth date. In this section we will explore what strategies people use when they select emoji passwords.

Kraus et al. [10] identified five emoji password selection strategies:

- **Emoji preference:** Selection of emojis based on personal preference.
- **Association and story:** Emojis are selected based on an association, by creating a story or a combination of both.
- **Pattern and position:** A pattern on the keyboard is used to create the password.
- **Repetition and similarity:** Emojis are repeated in a certain way or chosen based on their similarity.
- **Color and shape:** Selection of emojis with similar color or shape.

Table 3.1 shows the distribution of the selection strategies. The strategies were recognized in both the lab and the field study. No strategy stands significantly out in degree of popularity, but the importance of the *Emoji Preference* strategy is apparent when analyzing the most popular and unpopular emojis used in passwords. For instance, a Santa Claus emoji occurred 12 times on keyboards, but were only selected two times. Consequently, Kraus et al. found that EmojiAuth offers a skewed password distribution.

Kraus et al. also reported that some emojis appeared more often on the keyboards. This is because the emoji categories vary in size. For instance, the *Person and Face* category contains 226 emojis, while the *Activity* category only contains 44 emojis.

Strategy	Lab (n=27)	Field (n=20)
Emoji preference	10 (37%)	12 (60%)
Association and story	10 (37%)	8 (40%)
Pattern and position	12 (44%)	8 (40%)
Repetition and similarity	9 (33%)	4 (20%)
Color and shape	2 (7%)	9 (33%)

Table 3.1: Strategy frequencies for the selection of emoji passwords. Some participants said they used more than one strategy.

Golla et al. identified 13 different password selection strategies. However, five of them were utilized by less than 0.8% of the participants. Roughly 65% of the users either created a story or included important things in their lives when they selected their passwords. The remaining strategies are summarized in the list below.

- Random selection
- Recreate an event in life

3. EMOJI-BASED AUTHENTICATION

- Frequently used emojis
- Repetition
- Utilization of a spatial pattern on the keyboard
- Emoji preference

3.5 Guessability of Emoji Passwords

Golla et al. [9] estimated the security of PictoPass by measuring the guessability of emoji passwords. Three different attack models were created based on either emoji content, selection patterns on the keyboard, or a combination of those. The results were compared to the security of two well known mobile authentication schemes; Android Pattern Lock and four-digit PINs entry. Golla et al. found that PictoPass offers better resistance against guessing attacks than both the Android scheme and four-digit PINs. Yet, the research has some limitations. To name a few, it is not clear how accurate the attack models are or how the differences in origin and sampling in the compared data sets affect the results. Golla et al. did not determine the entropy of passwords created with PictoPass.

3.6 Shoulder-Surfing

Shoulder-surfing is a technique used by attackers in order to obtain your password. They typically do this by watching over your shoulder as you enter your password. This is a common issue in graphical authentication [60]. Although text passwords are also vulnerable to shoulder-surfing, it is often a greater problem in graphical password schemes. It can be easier for an attacker to observe users' actions on a screen, than to see input from a keyboard.

As mentioned earlier, Kraus et al. [10] performed a shoulder-surfing experiment in their research. They found that when shoulder-surfing emoji passwords, 16 out of 21 attackers used a *pattern* strategy to observe the password. The pattern strategy involves that attackers focus on the spatial position of each emoji on the keyboard and do not try to remember what the emojis in the password look like. Kraus et al. suggest that this result indicates that emoji passwords created using spatial patterns, are especially vulnerable to shoulder-surfing attacks. However, they also claim the results indicate that emojis offer slightly better resistance against shoulder-surfing than PIN.

Golla et al. implemented a common defence mechanism in PictoPass to avoid shoulder-surfing. The selected emoji is replaced with a checkmark after being displayed for only half a second. Golla et al. expected that this protects against shoulder-surfing

almost in the same way as it does for traditional password and PIN codes. Whether this is true was not studied.

3.7 Emoji Presentation

So far in this chapter, emojis have only been regarded as a way to replace PINs. In 2017, Seitz et al. [61] conducted a study on potential usage of emojis inside text passwords. Among other things, they were interested in how memorability is affected by different renderings of the same emojis.

The Unicode Consortium does not design emojis themselves, but leaves this to various software vendors. Consequently, emojis can look quite different (see Figure 3.6). However, the Unicode Technical Standard (UTS) provides design guidelines in order to ensure some form of interoperability. These guidelines include recommendations for attributes such as gender and diversity (e.g. skin tone) [51].

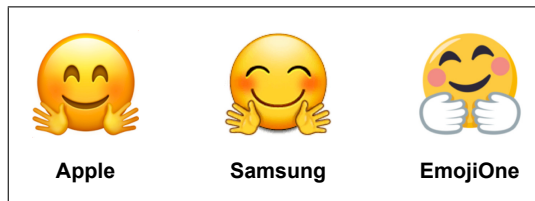
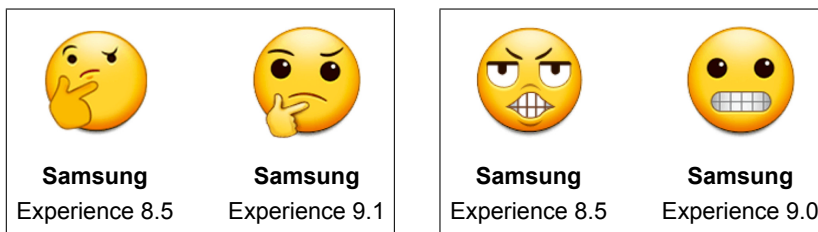


Figure 3.6: Presentation of the Hugging Face emoji for three different vendors.

Emoji presentations may also change over time. This includes everything from minor enhancements (see Figure 3.7(a)) to entire redesigns (see Figure 3.7(b)). In some of these redesign cases, the emoji might even change meaning which is shown in Figure 3.8.



(a) Emoji design enhancements between two different Samsung user interface versions.

(b) Emoji redesign from one Samsung user interface version to another.

Figure 3.7: Examples of emoji design enhancement and redesign.

3. EMOJI-BASED AUTHENTICATION



Figure 3.8: Changed emoji meaning. Example (1) shows the Pistol emoji which was changed to a water gun in Apples iOS 10.0 upgrade. Example (2) shows the Cookie emojis presentation on Samsung devices. Prior to Experience version 9.0, the emoji was rendered as a saltine cracker.

A system’s ability to show an emoji depends on whether there exists a representation for it on this specific system. If there does not exist any emoji presentation, it may fall back to a text presentation which is less detailed and plain-colored [51]. Figure 3.9 shows an example.

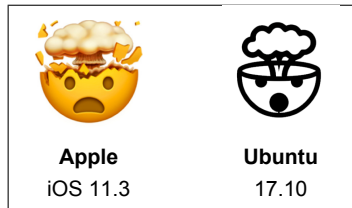
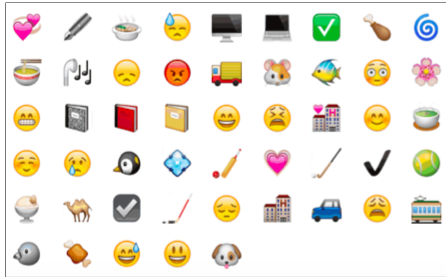


Figure 3.9: The Shocked Face With Exploding Head character in emoji presentation (left) and text presentation (right).

The study by Seitz et al. [61] consisted of two parts. During the first part, participants created a password that included at least one emoji and eight regular characters. As seen in Figure 3.10(a), they could choose between 50 different Apple emojis. One week later the participants were asked to recreate their passwords. At this time, the participants were divided into two groups: a control group and an experimental group. When entering their passwords, the participants in the experimental group were exposed to Android emojis that look quite different. As seen in Figure 3.10(b), some emojis look similar while others do not. The control group, on the other hand, could choose from the same emojis that were used to create the password.

3.7. EMOJI PRESENTATION

In the control group there were 15 successful logins and 5 failures. In the experimental group there were 13 correct and 6 failed logins. The difference was not statistically significant. Seitz et al. conclude that people are able to log in with different visual rendering of emojis. They claim that this is due to picture-word associations that persist even though the emoji rendering changes.



(a) Available emojis



(b) Some examples indicating how Android emojis look different from Apple emojis

Figure 3.10: The emojis used in the Seitz et al. study.

Chapter 4

EmojiStory: Designing an Emoji-Based Password Scheme

We have come up with a design of an innovative emoji-based authentication scheme which we call *EmojiStory*. In this chapter we will explain how the scheme works and the decisions that went into making it.

According to Oates [11], IT artifacts can have one of three roles in research projects. They can be "*the main focus of the research*", "*a vehicle for something else*", or "*a tangible end-product*", with focus on the development process. The development of *EmojiStory* is not the main focus of our research. The intention is not to develop a full-grown system that can be used without any further research. The role of the emoji-based authentication scheme is to be a prototype which illustrates the possibilities that emojis can offer and to be a means to collect data. So, according to Oates [11], *EmojiStory* is "*a vehicle for something else*" in our research.

4.1 Requirements

As mentioned in Section 1.3.1, we conducted a literature study on the use of emojis in authentication. Based on the findings from this work, the following requirements for an emoji-based password scheme were identified.

EmojiStory should facilitate:

- Secure mobile and web authentication
- High memorability of created passwords
- Short password creation and login time
- Efficient use of a virtual emoji keyboard
- Uniform presentation of emojis

The requirements are explained in detail and justified in the next sections.

4. EMOJISTORY: DESIGNING AN EMOJI-BASED PASSWORD SCHEME

4.1.1 Secure Mobile and Web Authentication

Biddle et al. [43] state that graphical password schemes are rarely suitable for all domains. Consequently, it is important to define the intended application for such a scheme. Emojis initially appeared on mobile phones where they still are used the most. Nevertheless, emojis are quite popular on social networking applications such as Facebook and Twitter. The emoji-based authentication scheme developed in this study should accordingly support both mobile and desktop platforms.

While text passwords are the natural choice for authentication on the web, PIN codes are frequently used on smartphones. EmojiStory should be able to substitute both techniques. When used as an alternative to PIN, the scheme should offer equal or higher theoretical and practical password space than four-digit PIN. When used as an alternative to text passwords, the scheme should offer the same security as eight-character text passwords in terms of theoretical and practical password space, and entropy [47].

Resistance to Guessing Attacks

The research of Kraus et al. (see Section 3.4) shows that people tend to use certain strategies, such as forming patterns or repeating the same emoji, when creating passwords with a virtual PIN or emoji keyboard. Additionally, some emojis are more popular than others (see Section 3.1.1).

With this information in mind, it is possible to predict passwords and perform guessing attacks. Circumventing the use of password selection strategies to avoid guessing attacks is therefore important.

4.1.2 High Memorability of Created Passwords

Ideally, it should be possible to create passwords that are both easy to remember and difficult to guess. Unfortunately, this is rarely the case. Passwords that are easy to remember also tend to be easy to guess. Strong passwords, on the other hand, are generally more difficult to remember [62]. Section 1.1 describes why emojis might have an advantage in terms of memorability compared to text. The emoji password scheme should consequently support the creation of passwords with high memorability, while maintaining satisfying password strength.

4.1.3 Short Password Creation and Login Time

People frequently authenticate themselves. Accordingly, authentication should take as little time as possible. This applies to both the creation and the input of passwords. The time used for these processes in EmojiStory should not differ much from PIN and text passwords.

4.1.4 Efficient Use of a Virtual Emoji Keyboard

A keyboard is an essential instrument for inserting characters into software. Since smartphones usually do not have any physical keyboards, these need to be virtual and part of the phone's OS instead. Most smartphones are tiny devices that fit into your pocket. Therefore, the virtual keyboards on smartphones need to be much smaller than their physical counterparts.

While qwerty¹ keyboards have consistent keys, the number of emojis is constantly growing. For this reason, emoji keyboard layouts should be limited in size and designed so that finding and using emojis is as efficient as possible. If this cannot be accomplished, the login time in an emoji-based authentication scheme might be influenced negatively.

A comparison of an ordinary virtual qwerty keyboard layout and a typical emoji keyboard (called *palette* by Unicode [51]) can be seen in Figure 4.1.

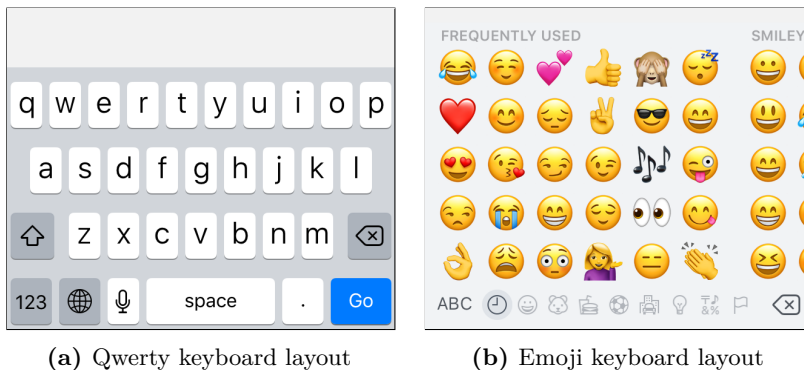


Figure 4.1: Comparison of two virtual keyboard layouts on Apple iOS 11.2.

4.1.5 Uniform Presentation of Emojis

Section 3.7 showed that emojis can look quite different and still have the same meaning. Although Seitz et al. concluded that this does not seem to be a significant challenge in the scheme they developed (this conclusion is based on the results from an experiment involving only 19 participants), we wanted to leave nothing to chance. Therefore, the scheme should employ the same emoji presentation across all platforms and devices. Furthermore, to avoid that some people could have an advantage when testing the scheme, the majority of the participants should not be familiar to the emoji display. Especially emojis designed by leading vendors, such as Apple, Samsung or Google, should be avoided.

¹ The standard order of keys on a keyboard where the letters q, w, e, r, t and y are at the beginning of the top line [63].

4.2 Functionality

This section gives an introduction to EmojiStory and illustrates how it can fulfill the requirements defined in the previous section.

4.2.1 Password Creation Procedure

In EmojiStory, the user creates a story by selecting keywords to substitute for blanks. Each keyword corresponds to an emoji. The sequence of emojis that occurs will form the user's password. This process is shown in Figure 4.2. In Figure 4.2(a) the user has to select a keyword from a specific category (see Section 4.2.4) and in Figure 4.2(b) the corresponding emoji is shown to the user. This step is repeated three times (see Figure 4.2(c) to Figure 4.2(h)). Figure 4.2(i) shows that the password creation procedure is finished, and the whole password is shown to the user.

The fact that EmojiStory guides users through the creation of passwords might contribute to shorten the password creation time. Users do not need to create a story themselves or find other ways of selecting and remembering a sequence of emojis.

4.2.2 Emoji Design

One requirement was to support uniform presentation of the emojis used in the scheme. This cannot be achieved by using OS- or software-specific emojis since they would change presentation when switching to a different platform (as illustrated in Figure 3.6 in Section 3.7). The emojis that were used in EmojiStory must therefore be presented in such a way that they look the same everywhere. This can be accomplished by embedding the emojis as images instead of Unicode characters.

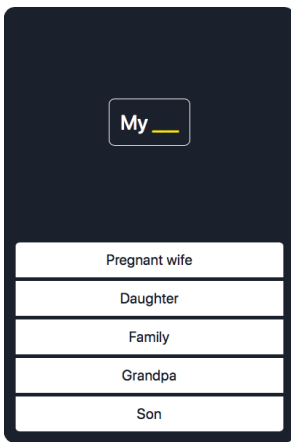
Images on the web should scale so that they fit all different screen sizes. Scalable Vector Graphics (SVG) images [64] do not lose quality when they are zoomed or resized. In addition, we wanted to use a design that is not used as frequently as those of the biggest emoji vendors, but which has an equivalent amount of characters.

EmojiOne ² is an emoji design that satisfies all these requirements. To this day, it is not used as the standard emoji representation on any popular OSs. EmojiStory uses the slightly older EmojiOne 2.3 ³ which was released in June 2016 (the newest version is EmojiOne 3.1 and was released in July 2017). This particular version is licensed as open-source under CC BY 4.0 ⁴ and contains 1833 emojis in different image formats – including SVGs. EmojiOne was therefore the appropriate choice for the emoji-based authentication scheme.

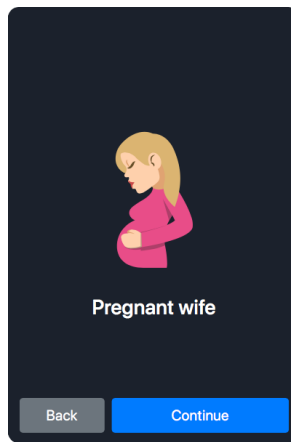
² <https://www.emojione.com/>

³ <https://www.emojione.com/emoji/v2>

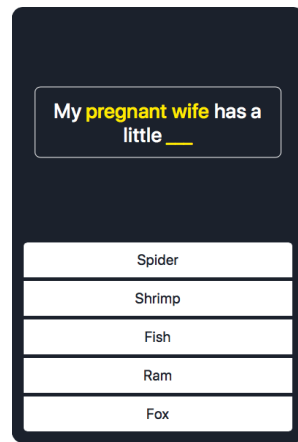
⁴ <https://creativecommons.org/licenses/by/4.0/legalcode>



(a) Step 1a



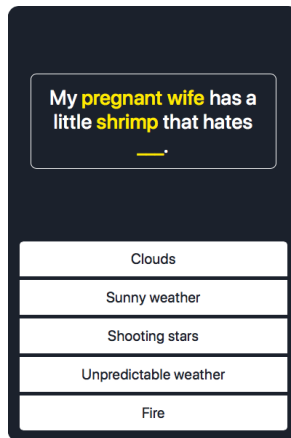
(b) Step 1b



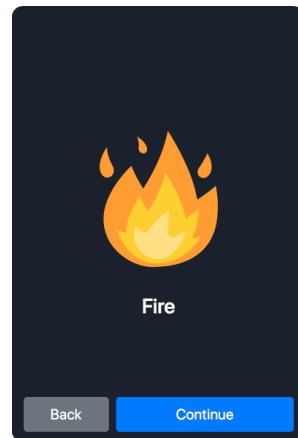
(c) Step 2a



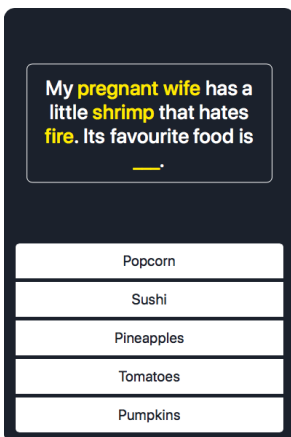
(d) Step 2b



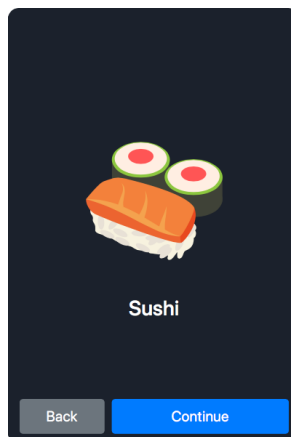
(e) Step 3a



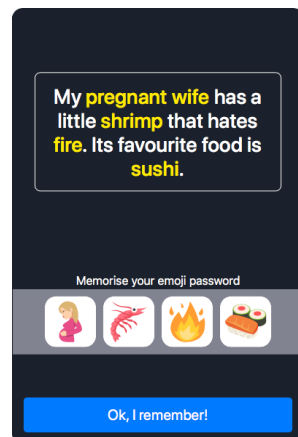
(f) Step 3b



(g) Step 4a



(h) Step 4b



(i) Summary

Figure 4.2: The different steps to create a password with EmojiStory.

4.2.3 Stories

Studies have shown that users often use personal stories as a password selection strategy [9, 10] to increase the password’s memorability. EmojiStory has a pool containing five different stories (see Figure 4.3). A story is randomly chosen when a user is initiating the password creation process. We encourage users to create random stories, maybe even crazy stories which do not make any sense. This story might function as a mnemonic [65], something that assists people in remembering their password. A positive consequence of random stories is that guessing attacks are more difficult to perform.

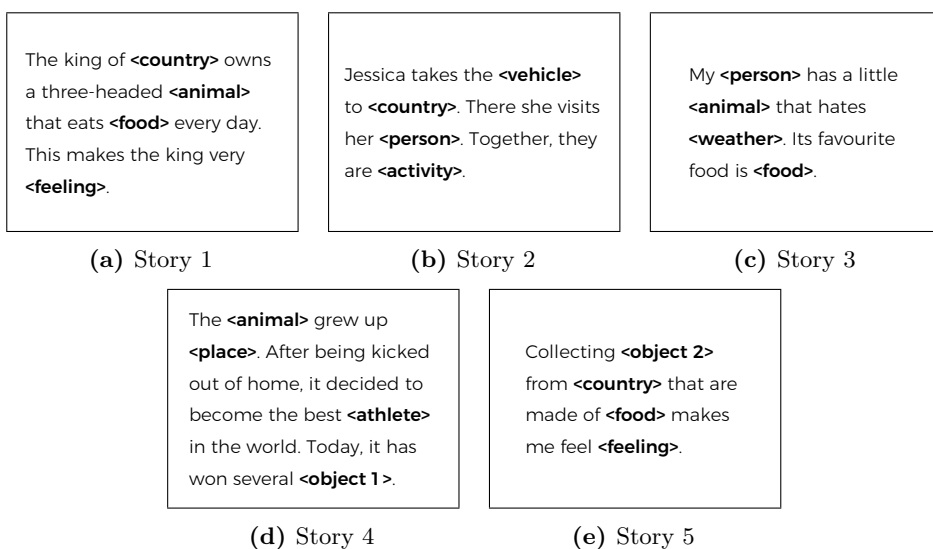


Figure 4.3: All the stories that the prototype provides.

4.2.4 Keyword Categories and Options

After users have been assigned a story template, the process of completing it is initiated. Each blank in the story can be filled with a keyword from a predefined category only. This keyword is selected from a list of five randomly chosen keywords which all derive from the same category, like shown in Figure 4.2(a). As a result, the EmojiStory scheme does not facilitate the creation of personal stories. For example, it is quite unlikely that a user gets to select their own country among the five answer options that are taken from more than 150 emojis.

We defined 12 different categories (Unicode’s own categorization of all emojis served as a starting point) so that each key on the keyboard (see Section 4.2.5) is representing exactly one of them. All categories are shown in Figure 4.4.

The next step was to link every emoji to a keyword and to place them into the different categories. This time-consuming process was done by hand which is why we decided to reduce workload by decreasing the total amount of emojis. The resulting number of elements in each category are summarized in Table 4.1.

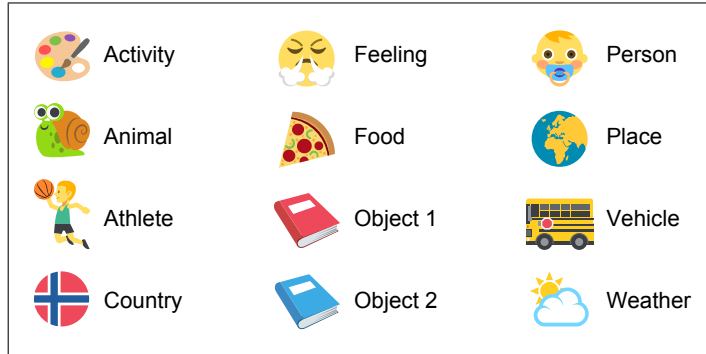


Figure 4.4: The keyword categories in EmojiStory.

As seen in Table 4.1, there are almost five times as many *activity* emojis as *weather* emojis. This might not be very surprising considering that activities include everything from taking a selfie to playing basketball. Unfortunately, this leads to some unwanted behavior. While the probability that an arbitrary activity keyword is one of the five options is about 3%, the same probability for a weather keyword is approximately 15%, which is much higher.

In practice this means that emojis from categories containing only a few emojis will be part of passwords more often. We could have circumvented this by making all categories contain the same number of elements, but did not believe that this was required for the prototype we created in this project.

All the categories are represented at least once in the five different stories. Country is used three times, which makes it the most frequently used category. Note that in a final version of EmojiStory, no stories should have the exact same sequence of categories, since this would make some passwords more likely than others.

4.2.5 Emoji Keyboard and Login Process

After finishing the creation of an emoji password, the user will get an individual keyboard for login which contains 12 different emojis. Once a keyboard is generated it does not change its content. Four of the keyboard's emojis are determined by the user's password, while the remaining ones are randomly chosen. Each keyword category is represented on the keyboard, meaning that every key contains an emoji

4. EMOJISTORY: DESIGNING AN EMOJI-BASED PASSWORD SCHEME

Category	Number of emojis (n=1145)
Activity	165
Animal	92
Athlete	130
Country	153
Feeling	120
Food	60
Object 1	61
Object 2	75
Person	87
Place	49
Vehicle	44
Weather	34

Table 4.1: The number of emojis (keywords) in each category.

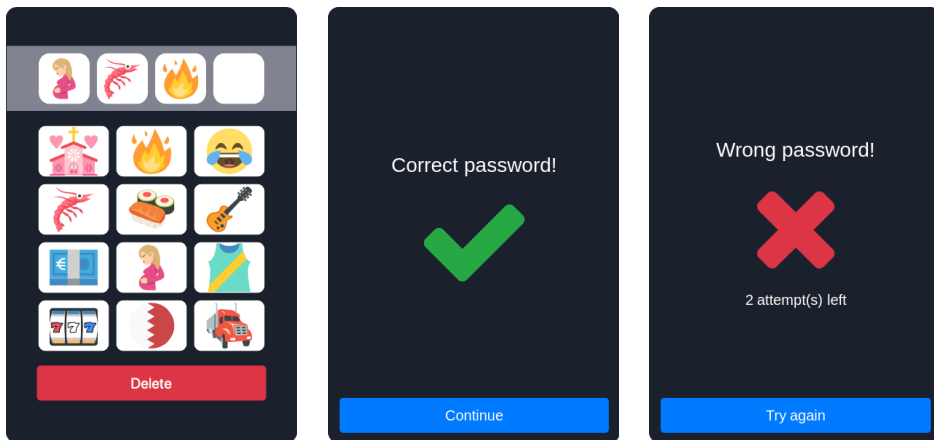
from a different category. This way, an attacker should not be able to identify which story the user’s password is based on by just looking at the keyboard.

Furthermore, it should be impossible for an attacker to predict visual patterns as there is no connection between the password and the positioning of the emojis on the keyboard. An example keyboard and the different outcomes of a login attempt are shown in Figure 4.5.

With only 12 different keys on the keyboard, it can easily fit into a single view on almost every screen size. The fact that users can see all possible emojis without the need to swipe or click anything, makes finding emojis more efficient and could have a positive influence on login time.

4.2.6 Intended Application

EmojiStory can be used in a wide range of authentication scenarios. The most obvious ways are perhaps as a method for unlocking devices and as an alternative to PIN entry. However, EmojiStory might also replace text passwords and be used to authenticate against web services that have a high number of users. Although this distinction is not the main focus of our research, the following sections will briefly explain how EmojiStory could be used in a wider range of applications.



(a) The keyboard after the user has chosen three out of four emojis.

(b) The screen that is displayed when the user has successfully authenticated.

(c) The screen that is shown after an unsuccessful login attempt.

Figure 4.5: The emoji keyboard and the feedback given to the users after they selected the fourth emoji.

Browser Extension

If EmojiStory was to be used in web authentication as an alternative to text passwords, it is important that the scheme offers a large theoretical password space to combat offline brute-force attacks (see Section 2.4). This can be achieved by employing user-specific keyboards that are accessible through a browser extension. Figure 4.6 illustrates how this would work. The browser extension functions similarly to a password manager (see Section 2.2.2), but instead of storing passwords, it stores EmojiStory keyboards.

Since every emoji is represented by a unique word in the scheme, the browser extension could convert emoji passwords into regular text passwords. This is visualized in Figure 4.7(a). However, the extension could also be designed to convert the emojis into a set of random ASCII characters. This method is visualized in Figure 4.7(b). In this case, the extension would assign random ASCII characters to each emoji on the keyboard during the password creation process. As a result, the ASCII outputted from the extension would be unique for each emoji password. Consequently, two identical emoji passwords would be represented differently (and completely random). This would not be the case if the extension converts the emoji passwords based on their textual representation in the scheme. The security and usability aspects of such functionality are explored in the next section.

4. EMOJISTORY: DESIGNING AN EMOJI-BASED PASSWORD SCHEME

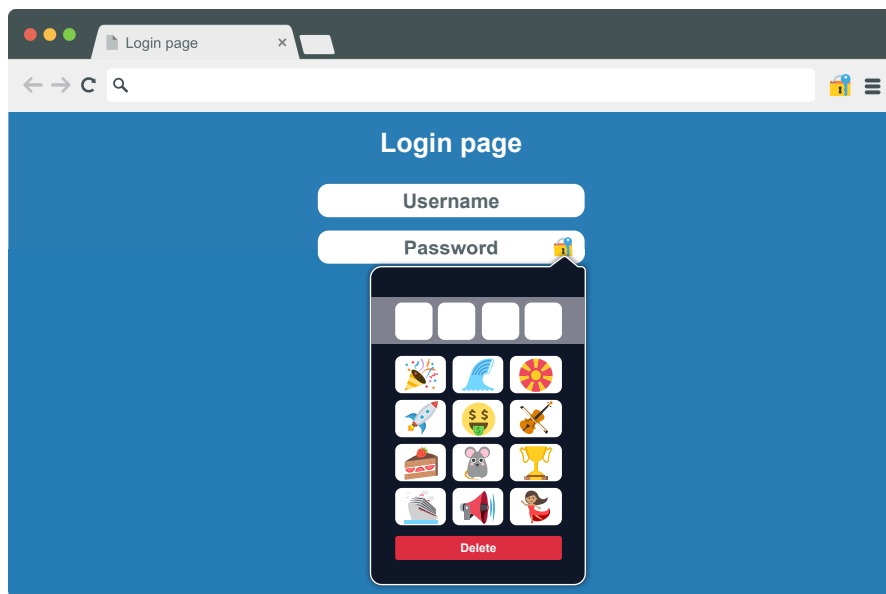
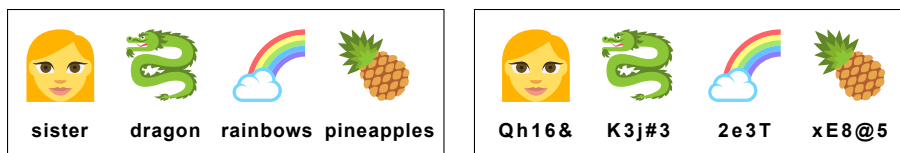


Figure 4.6: EmojiStory implemented as a browser extension.



(a) Emojis are converted to their text representations. The resulting password is "sisterdragonrainbowspineapples".

(b) Emojis are converted to random ASCII characters. The resulting password is "Qh16&K3j#32e3TxE85".

Figure 4.7: The conversion of the emoji password to their text representations.

4.3 Theoretical Password Space and Entropy

In this section we will only focus on the theoretical password space and entropy that EmojiStory can offer. Other security aspects of EmojiStory were evaluated by embedding the scheme into a survey. How this was done is explained in more detail in Chapter 5 and the results are therefore presented and discussed in Chapter 6. The usability of EmojiStory is also analyzed in Chapter 6.

When used in web authentication, a browser extension needs to translate the emojis in EmojiStory into text. As described in the previous section, this can be done by two different techniques: one converts the emojis into their textual meaning,

4.3. THEORETICAL PASSWORD SPACE AND ENTROPY

while the other converts the emojis into random text characters. Regardless, it would be tempting to argue that the entropy of EmojiStory can be calculated as: $\log_2(\text{number of ASCII characters}^{\text{password length}})$. However, this is only true if the emojis are converted into random ASCII characters.

The entropy that EmojiStory offers is significantly lower if the emojis are converted into their text representation, since it is the method that you use to create your password that determines the entropy of the password. If the emojis are converted into their textual meaning, it would result in a passphrase that consist of four words. Attackers can utilize the fact that the password can be broken down to four elements, to enhance the likelihood of guessing the correct password.

If emojis are translated into their corresponding words, the categorization of emojis in the scheme also has a negative impact on the entropy. Imagine attackers who know all the stories and the emoji words in the scheme. They also know the order of the categories in each story. If they were to guess your password created with EmojiStory, they can narrow the amount of possibilities by considering the categories that the words belong to. This can be illustrated by an example based on the EmojiStory prototype. Lets say the attackers try to guess a password that is constructed with a story that contains the following sequence of categories: country (153), feeling (45), food (58), animals (81). Then the number of possible passwords are 32,345,730 (calculated by multiplying the number of *words* in each category and the number of stories) and the entropy would be: $\log_2(32,345,730) = 25$ bits. Clearly, this entropy is significantly lower than when the ASCII representation of the emoji password is random.

In a final version of EmojiStory, the entropy can be increased by adding emojis and stories. If all categories contains 150 words and the scheme has 100 stories, an emoji-password of four emojis would offer the following entropy: $\log_2(150^4 \times 100) = 35,6$ bits. If the password had six emojis the entropy would be 50 bits.

These numbers are acceptable when comparing them to the strength of user-chosen text passwords. Shay et al. [66], conducted a study on text passwords with 8,143 participants. Each participant created a password that had to meet one (out of eight) randomly assigned password policy with a variety of metrics for strength and usability. No passwords were shorter than eight characters, while one of the policies required a password length of 20 characters. Shay et al. found that among all the participants the average password entropy ranged from 34 bits to 56 bits. Accordingly, the strength of user-chosen text passwords is close to the entropy of passwords created with EmojiStory.

An advantage of converting the emojis to their textual meaning is that it might enable users to authenticate on devices other than those on which the browser extension is

4. EMOJISTORY: DESIGNING AN EMOJI-BASED PASSWORD SCHEME

installed. If they remember their emoji passwords without the use of the keyboard, they can manually type the textual representation of their passwords. This, however, is close to impossible when the emoji password is represented by a set of random ASCII characters.

When EmojiStory is used as an alternative to PIN entry, the theoretical password space and entropy are much lower and easier to calculate. The size of this password space is calculated based on the number of emojis in the login keyboard. Since no passwords can contain the same emoji multiple times, the size of the theoretical password space is calculated as: $12 \times 11 \times 10 \times 9 = 11,880$. This is slightly larger than the size of the theoretical password space that PIN offers (9,999).

All previous calculations for the entropy of passwords created with EmojiStory, are based on the assumption that the size of the practical password space is equal to the theoretical password space. In Chapter 6 we will look into if this is true or if users select predictable passwords which causes a low practical password space.

4.4 User Experience Testing

Before any data from survey participants was collected, the User Experience (UX) of EmojiStory in combination with the survey were tested. The test conditions and its execution are described in detail in Section 5.1.4 in the next chapter. However, relevant feedback to EmojiStory and the resulting improvements are presented in this section.

4.4.1 Emoji Preview

According to feedback from several users, they did not understand the connection between the words they chose and the corresponding emojis while creating their emoji password. In the initial version of EmojiStory, users were immediately sent to the next blank in the story after selecting a keyword. They were not exposed to any of the emojis they selected for their passwords during the creation of it.

The emojis are deliberately excluded from the keyword options to prevent users from selecting the emojis they like best. However, the feedback is indicating that it might be counterproductive not to show them at all. This is why we added a new view which is shown right after the user selected a keyword from the different options. The view shows the keyword together with the corresponding emoji. Thereafter, the user continues to fill in for the next blank in the story. Figure 4.8 and Figure 4.9 illustrate the password creation process before and after the preview was implemented.

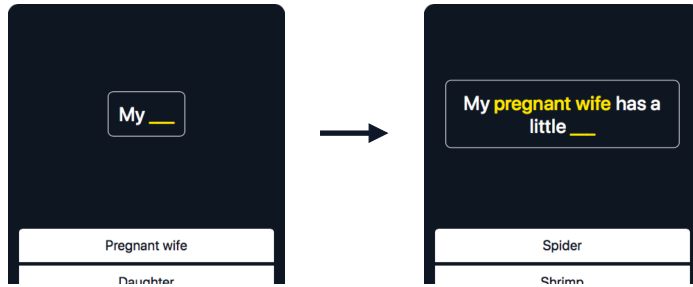


Figure 4.8: The situation before an emoji preview was implemented.

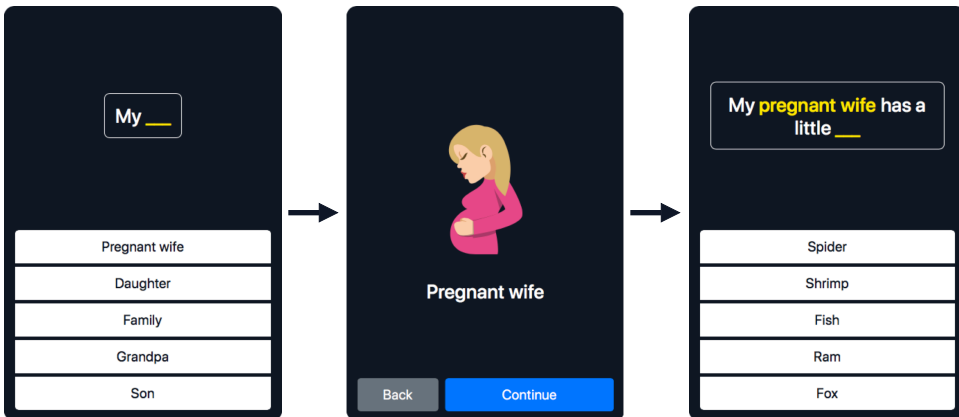


Figure 4.9: The situation after an emoji preview and a back button were added.

4.4.2 Back Button

Further feedback made us aware that it was impossible to change a selected keyword. Users may accidentally click on one of the options and make an unintentional selection or simply change their mind about which keyword they want to use.

This led to adding a back button to the same view introduced in Section 4.4.1 in *EmojiStory*. Its implementation is shown in the middle screen of Figure 4.9. Pressing this button sends users back to the previous screen where they can select a different keyword. Theoretically, users can now choose their favourite emoji by using this button (since the overview also shows the emoji). Although this would be unwanted behavior, we suspect that only a few people actually use this button actively. To confirm or refute this assumption, the online survey counts how often the button is pressed by every user (see Section 6.2.7 for results).

4.4.3 Evolving Stories

Several participants commented that they forgot the story while creating their password. Previously, users had to complete four independent sentences before they were merged into a story. We decided to increase people's exposure to their story to solve this issue. The final history is displayed to the user only once. However, by gradually developing the story, we enable users to become familiar with it. This functionality can be seen in Figure 4.2.

4.5 Scheme Issues

Already during the development of EmojiStory, we identified some issues regarding the usability of the scheme. For instance, sharing your password (e.g. to give access to an online streaming service) with friends or family might be difficult. How would you tell a person your password? This is not an impossible task, but there is no easy way to do so. Moreover, if you want to use EmojiStory on a device other than the one used to create your Emoji password (e.g. your work computer), you have the problem that this device does not know the corresponding keyboard. This is why this version of EmojiStory is not particularly well suited for the use of multiple passwords either, as each of them is linked to a different keyboard. Although it is important to solve these problems, it was not part of this thesis due to the limited lifespan of this project.

Chapter 5

Experiment Setup

In this chapter we will explain how the different experiments in this project were constructed and executed.

5.1 Survey

If collecting data from many people across the world is important to your research, a survey can be a great research strategy. Obtaining data can be convenient and practical by conducting a survey. You could, for instance, send a list of questions to people by email or ask visitors to a website to complete a questionnaire. Also, surveys provide a relatively simple way to study people's mindsets and motives [67]. Therefore, a survey seems like a great choice in order to evaluate the usability and security of EmojiStory.

A survey lets you obtain the same data from a large number of people in an organized and consistent way. Then you can analyze the data and look for patterns that can be generalized to a larger population than the group you collected the data from.

According to Colin Robson [67], surveys can be administered in three different ways: self-completion, face-to-face interview and telephone interview. In a *self-completion* survey, people can fill in answers by themselves. The biggest advantages of using this approach is that large samples can be reached in a short period of time with little effort. Due to limited resources and a need for a large sample, we chose to design an online, self-completion survey.

In the field of computer science, surveys are well-established and widely used. However, it is easy to get it wrong and many surveys are poorly designed and executed [11]. In this section we will describe how we planned and designed the first survey in this project.

5. EXPERIMENT SETUP

5.1.1 Planning and Conducting the Survey

The planning and conducting of a survey involves six important aspects: data generation method, sampling frame, sampling technique, response rate and non-responses, sampling size and data requirements [11]. This section will briefly discuss how each of them are covered.

Data Generation Method

Every research strategy needs a way to produce empirical data or evidence, that is, a data generation method. It is a common belief that surveys always use a questionnaire as data generation method. However, Oates [11] mentions four different data generation methods that can be used in a survey: interviews, observations, questionnaires and documents. We chose to generate data by basing the survey on a questionnaire. Section 5.1.2 describes how the questionnaire was designed.

Sampling Frame

A list of what people you want to include in a survey is called a *sampling frame* [11]. The sampling frame does not consist of the actual people you will send your survey to, it is a list which you will choose your sample from. A sampling frame is specific and could for instance be a list with names of the people in your target population. Since the population of interest in this research is everyone that uses passwords, it is obviously not feasible to summer the sampling frame in such a list.

A disadvantage of online surveys is that they will not reach people that do not have access to a device with Internet access. However, this is not a large issue in our case since those people usually does not use passwords and are therefore not part of the target population. You could argue that people who own a credit card use passwords since they enter a PIN code each time they use it, but we do not think of emojis as a possible replacement to PIN in such an application.

Sampling Technique

A *sampling technique* is a method for selecting actual people from the sampling frame. Sampling techniques can be divided into two different kinds: probabilistic and non-probabilistic. Probability sampling techniques have a high probability of producing a sample that is representative for the population being studied. The sample is gathered based on some sort of randomization that ensures that all individuals in the population have an equal chance of being selected. Since probability sampling requires great knowledge about the population it is not feasible to have a representative sample. Instead, we opted for non-probabilistic sampling.

A sample plan where it is not possible to determine the probability that a specific person will be part of the sample, is called *non-probability sampling* [67]. According to Oates [11] there are four different non-probability sampling techniques: purposive, snowball, self-selection, and convenience sampling. We chose to use *self-selection sampling*. When using this technique, researchers advertise their need for respondents and collect data from people who are willing to participate. A survey is practical to spread online and it is easily accessible on the Internet. Therefore, self-selection sampling may result in a larger sample compared to the other techniques which involves some sort of hand-picking when choosing the sample. We wish to be able to make generalizations to the wider population, so it is important that the sample is large and contains as little bias as possible. As a result, self-selection sampling seems like a good choice.

Response Rate and Non-Responses

Low response rate and non-response are common issues in self-completion questionnaires. It is not unusual to get response rates of only 10% [11]. Since the survey is distributed with a self-selection sampling technique over the Internet, we have no control of who will respond to it. It is more likely to convince people to participate by contacting them directly, but this is not possible with the chosen sampling technique.

If we identify that certain subgroups are inadequately represented during the data collection, we will specifically target people in such groups. For instance, it is likely that people from other countries than Norway will be underrepresented, since we do not have a large international network. To increase the response rate of this subgroup, we can contact exchange students on campus at the NTNU.

Sample Size

It is important that the sample is large enough to generalize findings and make conclusions from the collected data. The sample size can be calculated based on confidence level, margin of error and target population size [68]. In our case, the target population size is difficult to estimate since it includes all people worldwide that uses passwords. However, the population size is not important unless it is quite limited because the sample size does not increase at the same rate as the population size [68]. According to *Creative Research Systems*, you would need 661 individuals in your sample, for a target population of 100,000, a confidence level of 99% and a margin of error of +/-5% [69]. If the target population was 10,000,000, you would need a sample of 666, that is, only five more people. The amount of people using passwords worldwide is of a significantly large amount, hence the population size is not important when calculating the sample size.

5. EXPERIMENT SETUP

According to Oates [11], researchers usually use 95% as confidence level and +/-3% as margin of error. Increasing these factors in order to obtain a greater accuracy in claiming that the sample represents the whole population, causes a drastically increase in the required sample size. Because the target population size is huge, and since we have a limited amount of time, using 95% and 3% seems like a good idea. This results in a sample size of 1067. So, our goal is to achieve a sample size of at least 1067.

However, we should not stop collecting data if we reach the target sample size. The larger the sample, the lower the probability for error in generalizations [67]. Therefore, we should strive toward a sample size that is as large as possible.

Data Requirements

Since you will not get a second chance to collect data with a survey, it is important to decide what data you need from the beginning. You also need to think ahead since new patterns and interpretations might arise when analyzing your data.

We wanted to generate both data that is directly related to the research questions, and demographic data which is only indirectly related. The reason why, is that demographic data might be interesting when researching security since the level of security depend heavily on the user.

5.1.2 Survey Design

There are many decisions that have to be made and things that should be considered when designing a survey. This section covers some common issues of survey development.

Form

Surveys can be created in different ways, for instance, on paper or electronically. Since the expected number of respondents is close to one thousand, a pen-and-paper survey is obviously not an option since it would require a tremendous amount of effort and resources. Therefore, we decided to design a web-based survey. We will set up the survey on a website so that anyone who visits will be able to participate.

An advantage of conducting an online survey is that the responses are returned electronically. This eliminates the need for coding the responses and removes the danger of errors by manually typing data into a software program. However, as already mentioned, an online survey will not reach people without Internet access. This is not a serious issue, since such people are not part of the target population for the survey. Another disadvantage is that a web-based survey introduces several anonymity and privacy concerns. These are discussed in Section 5.1.2.

Length

Research has shown that the length of a web-based survey affects the response rate. The longer the survey length, the fewer people start and complete the survey [70]. Therefore, we should strive towards designing a survey that is simple and short. If leaving out questions to shorten the length is not an option, you can focus on creating questions that are easily answered and reduce the complexity of the survey. This process is discussed below.

Question Wording

The survey questions are perhaps the most essential part of a survey. They should be designed to answer the research questions and are therefore crucial to the research. As a result, their wording is very important.

The following suggestions should be considered in order to ensure good wording of survey questions. Questions should be short and easy to understand. They should mean the same thing for all participants and not contain any ambiguity. Questions that encourage certain answers, create opinions and are open-ended, should be avoided [67].

Anonymity and Confidentiality

The use of a web-based survey introduces more problems regarding anonymity and confidentiality for ethical researchers [11]. We can promise confidentiality in the way we collect and use the data, but it is difficult to guarantee that the digital communication between us and the respondents will be kept confidential. Networks could be compromised and dishonest system administrators could read database records.

It can also be difficult to ensure anonymity of participants of an online survey. Their locations could be unintentionally exposed due to logging of Internet Protocol (IP) addresses, and you need to give them some sort of identifier or pseudonym. This is important in our case, since we collect background information about the participants. However, they will not be asked for any information that is sensitive.

Researches often use survey tools and hosting services when conducting a survey. Ensuring that third parties do not have access to your data, can complicate matters. We do not need the help of survey tools, since we create the entire survey ourselves, but we will need a hosting service in order to deploy the survey. How anonymity and confidentiality were ensured is elaborated on in Section 5.3

5. EXPERIMENT SETUP

5.1.3 Survey Setup

In order to evaluate the security and usability of emoji-based authentication, we included a password creation process and two authentication processes in the survey. This was achieved by utilizing EmojiStory and resulted in a survey consisting of six different parts: an introduction, an emoji-password creation process, authentication, a questionnaire, re-authentication, and a closing statement. In this chapter, each part will be described in detail.

Introduction

The introduction of the survey consists of two parts. First, the participants are met with a description of the research project, before an instruction on how to use EmojiStory is given.

When you collect personal data about participants, you are obligated to disclose certain information regarding the research project [71]. Therefore, the landing page of the survey contains such information. As seen in Figure 5.1(a), the landing page describes the background and purpose of the research, how much time it takes to complete the survey, how the data will be handled, and contact information.

After the participants start the survey, they are given some information on how to create an emoji-password using EmojiStory. The instructions can be seen in Figure 5.1(b).

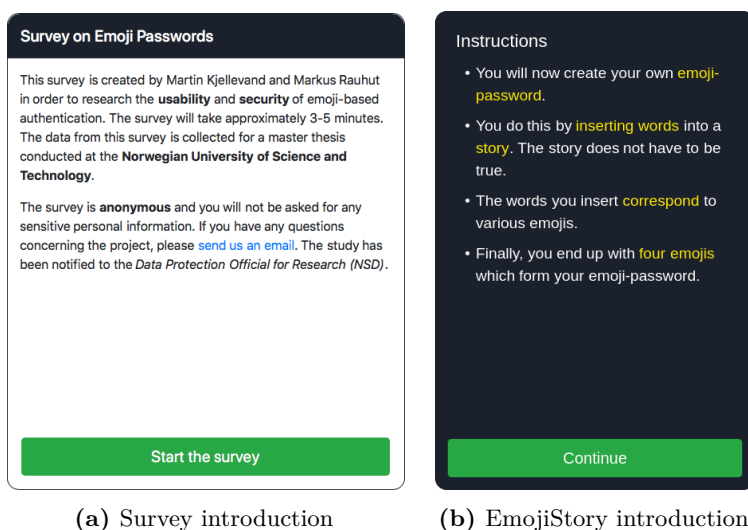


Figure 5.1: The different instructions in the survey.

Emoji-Password Creation Process

The first thing participants are asked to do in the survey, is to create an emoji-password using EmojiStory. This process is demonstrated in Chapter 4. When the process is finished, the password is shown and the participants are encouraged to memorize their passwords.

Authentication

After the password is created, the participants are asked to authenticate themselves by entering their passwords. Participants are given three attempts and are not restricted by time. The authentication process is described and visualized in Chapter 4.

Questionnaire

The questionnaire includes nine questions. All of them, except one, are multiple choice questions with only one possible answer. All questions are mandatory in order to complete the survey and they have to be answered in the same order as they are given.

If the participants enter their passwords correctly, they are first asked a question about how they remembered their passwords. The question can be seen in Figure 5.2. It is asked to find out whether the stories help in remembering the passwords. Naturally, the participants who are not able to remember their passwords, are not asked this question.

The screenshot shows a mobile application interface titled "Survey on Emoji Passwords". The question displayed is "I remembered my emoji-password by memorizing...". Below the question are four dark grey buttons with white text, representing the possible answers: "the emojis", "the story", "the emojis and the story", and "something else".

Figure 5.2: Memorization

The screenshot shows a mobile application interface titled "Survey on Emoji Passwords". The question displayed is "Select the most accurate statement: My story...". Below the question are four dark grey buttons with white text, representing the possible answers: "has a personal touch", "is crazy", "contains random emojis", and "is created in another way".

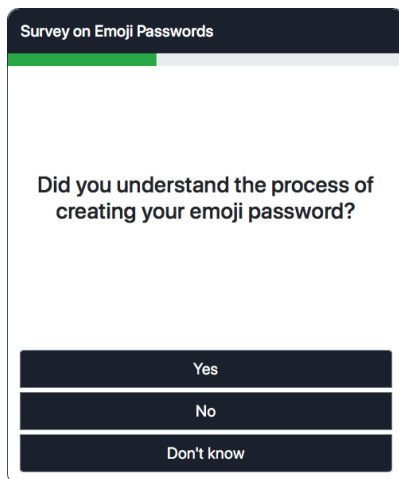
Figure 5.3: Strategy

5. EXPERIMENT SETUP

Next, the participants are asked to select a statement that best describes their stories. This question is asked in order to study what selection strategies participants use when they create their passwords. What the question looks like can be seen in Figure 5.3.

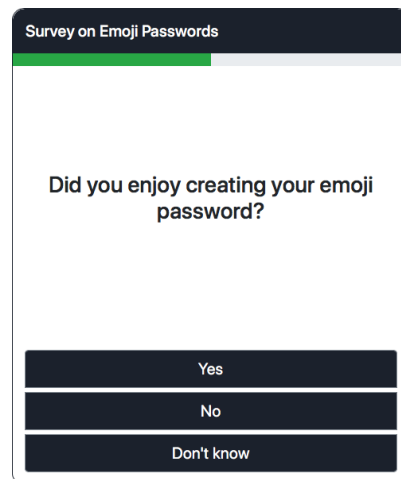
We believe EmojiStory offers a innovative way of creating passwords that is new and unfamiliar to people. Therefore, we suspect that some participants will be confused by the scheme. Since we are afraid that this will affect their behaviour and ability to remember their passwords, a question regarding confusion is asked (see Figure 5.4).

We also suspect that the use of emojis in authentication will lead to a positive user experience. For that reason, we ask participants if they enjoyed creating their emoji passwords. The question can be seen in Figure 5.5.



The screenshot shows a mobile application interface for a survey titled "Survey on Emoji Passwords". The question displayed is "Did you understand the process of creating your emoji password?". Below the question are three dark blue buttons with white text: "Yes", "No", and "Don't know".

Figure 5.4: Confusion



The screenshot shows a mobile application interface for a survey titled "Survey on Emoji Passwords". The question displayed is "Did you enjoy creating your emoji password?". Below the question are three dark blue buttons with white text: "Yes", "No", and "Don't know".

Figure 5.5: Enjoyment

The remaining questions in the questionnaire serve to better understand the background of the participants. First, we ask how often they use emojis in their everyday life, to investigate how this impacts their attitudes towards emoji passwords. Not surprisingly, we suspect that people who often use emojis, will be more positive to the idea of using emoji-passwords. As seen in Figure 5.6, the respondents have to answer the question on a scale from *never* to *several times a day*.

Next, we ask the respondents if they have a background in IT or information security. People with a great level of knowledge in this field, may be better at using the emoji-based password scheme than others. This could cause bias in the data, which is why we ask the question seen in Figure 5.7.

Survey on Emoji Passwords

How often do you use emojis?

Several times a day

Once a day

Several times a week

Once a week

Never

Figure 5.6: Emoji usage

Survey on Emoji Passwords

Do you have a background in IT or information security?

Yes

No

Figure 5.7: Background

In the seventh question, we ask the participants about their gender. As seen in Figure 5.8(a), the gender question is answered by selecting the appropriate gender icon. The idea behind this is that it saves the respondent from reading, making the question quicker to answer. The main reason for asking about gender is due to the gender disparity in the field of IT and information security [72]. People who participate in research, often do so since they have strong feelings on the subject [11]. This may cause a gender bias in the sample. Also, research on *Passfaces* (see Section 2.3.1), showed that there was bias in the password selection process when considering gender.

The final questions in the questionnaire is about the respondents age and nationality. They can be seen in Figure 5.8(b). Respondents state their age by entering a numerical value in a text field and their nationality by selecting the appropriate country from a dropdown menu. Age and nationality are properties that can be useful in order to detect bias in the sample. We suspect that there will be a considerably amount of people in their twenties from Norway in the sample. Also, since we want to research the usability of emoji-based authentication, the age and nationality of participants can affect the results. Likely, young people have a greater experience with passwords and emojis, and language preferences may prevent people from grasping new concepts and functionality.

Re-Authentication

After completing the questionnaire, participants are asked to enter their passwords one last time. The idea behind this is to test how the participants ability to remember their passwords are affected by the short distraction that the questionnaire provides. The re-authentication is identical to the first authentication process.

5. EXPERIMENT SETUP

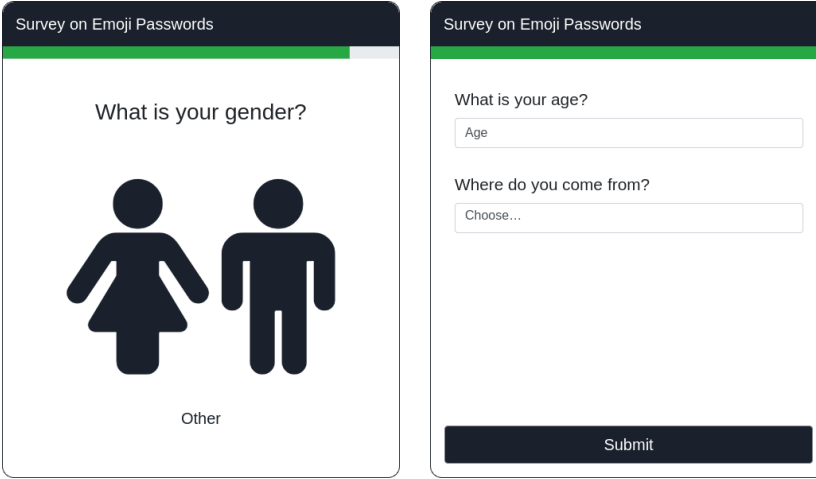


Figure 5.8 consists of two side-by-side screenshots of a mobile survey application. Both screenshots have a dark blue header with the text 'Survey on Emoji Passwords' in white. Screenshot (a) displays the question 'What is your gender?' in black text. Below the question are two black icons: a female figure on the left and a male figure on the right. Underneath these icons is the word 'Other' in black text. Screenshot (b) displays two questions. The first is 'What is your age?' followed by a white input field with the placeholder text 'Age'. The second is 'Where do you come from?' followed by a white input field with the placeholder text 'Choose...'. At the bottom of the screen in screenshot (b) is a dark blue button with the word 'Submit' in white text.

Figure 5.8: Questions regarding gender, age and nationality.

Closing Statement

After completing the survey, participants are shown the closing statement seen in Figure 5.9. Contact information of those responsible for the survey was provided, and participants were encouraged to share the survey in social media. Sharing the survey was facilitated by implementing *share buttons* which are convenient to use. Convincing people to share the survey is important in order to increase the number of respondents.

5.1.4 Pre-Testing the Survey

Prior to the release of the survey, it was pre-tested in a controlled environment. This is an important step in the process of conducting a survey since you can get feedback on how people interpret the questions and how intuitive they think the survey is. The test can also help to improve question wording by getting the participants thoughts on how clear, simple and ambiguous they think the questions are.

The test was carried out in a meeting room on the campus of NTNU with eight students. Five of them were boys and three of them were girls, all studying either Communication Technology or Computer Science. The test was done individually and the participants used their own device to answer the survey. One half used smartphones, while the other used laptops. The participants were asked to speak aloud during the test and give any thoughts that occurred to them. In the following sections we will present some improvements we did to the survey based on feedback we got from the test.

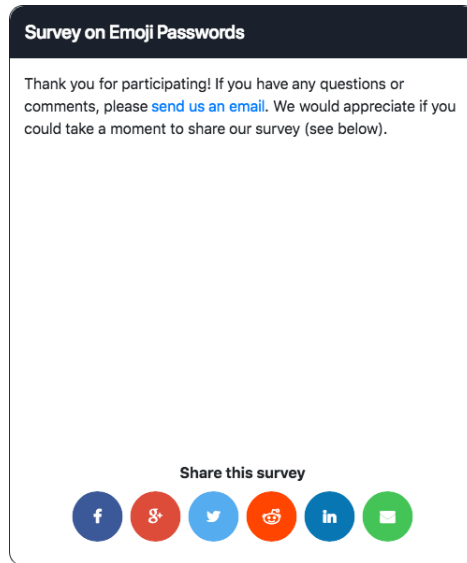


Figure 5.9: Closing statement

Adding a Progress Bar

During the test, one participant felt frustrated because he was unaware of how many questions he had to answer. This is a problem since it might lead to people abandoning the survey. As a solution we implemented a progress bar in the survey as a means to keep participants motivated. This is important in order to avoid that they leave the survey before completing it. A progress bar was only added to the questionnaire, and not to the password scheme. The reason for this is that we observed that participants stayed motivated and were excited during the password creation and login process. We would also had some design issues trying to add a progress bar to EmojiStory.

Removing Question on Interpretation of Emojis

In the test nearly everyone answered «*I do not know*» on the following question: «*Were you able to interpret all the emojis you encountered?*». Some people did not understand this question, while others were intimidated by it since they were not certain they had interpreted the meaning of the emojis the correct way. We tested several different ways of asking this question, but we were not able to make it unambiguous, short and to the point. After some time we concluded that the question was not really relevant to our research and we removed it from the questionnaire.

5. EXPERIMENT SETUP

Rephrasing the EmojiStory Instructions

«What are keywords?», «Does the story has to be true?», and «Do I have to come up with a story?» were some of the questions we got from participants after they had read the EmojiStory instructions. Based on this feedback, we decided to change the phrasing of the instructions on how to use EmojiStory.

First of all, we removed the term "keyword(s)" since several persons spent unnecessary time pondering how "keywords" was going to be different from regular words. Next, we added that the story do not have to be true, because two participants thought they had to create true stories. Finally we made the language more explicit in order to remove ambiguity. For instance, one participant interpreted the instructions in such a way that he believed he had to come up with an entire story himself. Therefore, we changed the second instruction to express "...by inserting words into a story".

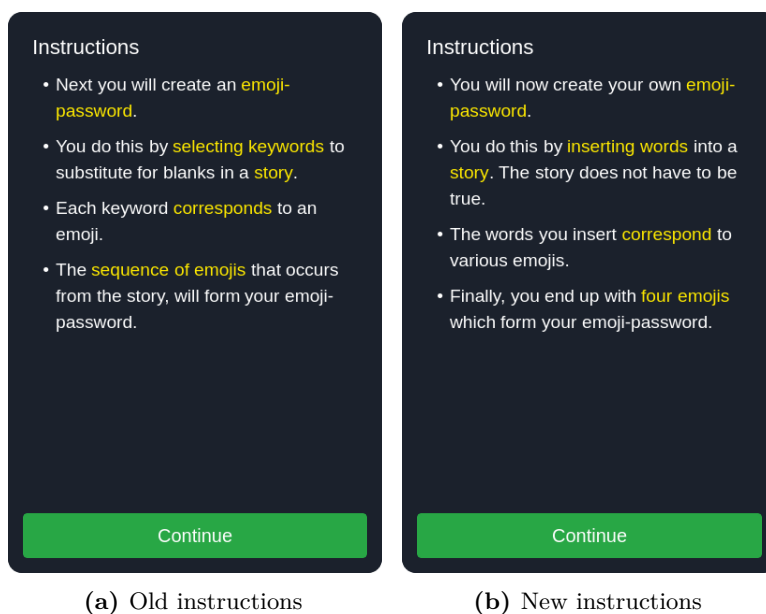


Figure 5.10: Making the EmojiStory instructions more understandable.

Changing the Appearance of the EmojiStory Instructions

Several participants felt the instructions were overwhelming and that they required a lot of effort to understand. In order to prevent this we changed the appearance of the instructions, as seen in Figure 5.11. By transforming the instructions into steps and requiring the user to actively request the next instruction, the text became more readable. Also, by fading text that the user already has read, the instructions feel less intimidating.



Figure 5.11: Making the EmojiStory instructions less overwhelming.

Adding Support for Norwegian and German

Everyone who participated in the usability test were from Norway. Some of them had trouble understanding different aspects of the survey due to language issues. This feedback were mostly given by people of higher age with poor skills in the English language. The introduction and the questionnaire were some of the things they found difficult to understand. In anticipation of the majority of the respondents being from Norway, we therefore implemented Norwegian language support. Since we have a

5. EXPERIMENT SETUP

large network in Germany, we also implemented support for German in the survey. The survey application automatically selects the appropriate language based on the browser language settings, but it also allows the user to manually set their preferred language. Everything in the survey was translated except the EmojiStory password scheme. Translating nearly 1,000 unique words that represents emojis, would have been too time consuming.

Changing the Gender Icons

Some participants expressed the following: «*I do not know which gender icon I should select.*» Based on this feedback, we decided to change the gender icons. Figure 5.12 shows the old and the new icons. People taking part in the test, thought that the icons seen in Figure 5.12(a) were difficult to interpret. Therefore, we changed the icons and used some that were easier to understand, see Figure 5.12(b).

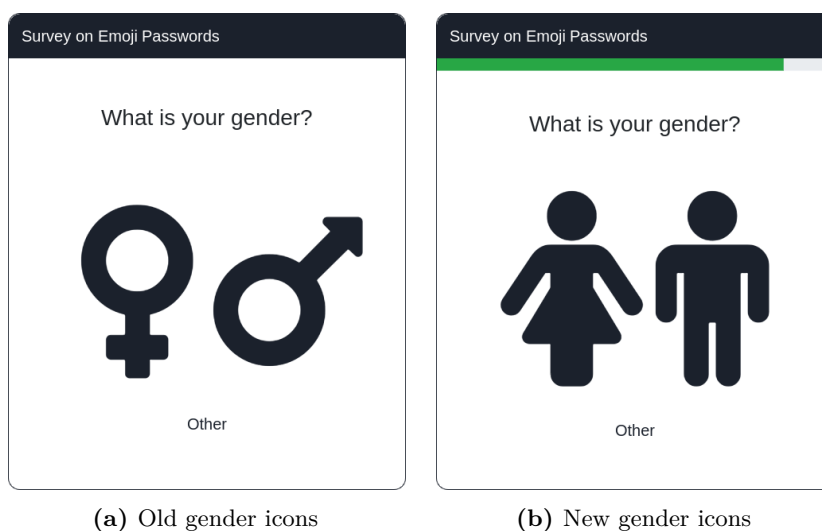


Figure 5.12: Changes made to the gender question.

Rephrasing the Strategy Question

During the usability testing of the survey, several people thought that the strategy question was very demanding to answer. As seen in Figure 5.13(a), both the question and the answer options were quite long. As described in Section 5.1.2, it is important that the question wording is good. For that reason, we rephrased the question. Figure 5.13(b) shows the new formulation. The answer option are a lot shorter, making the question much easier to answer.

In hindsight, the new phrasing of the strategy question was perhaps not the best. We believe it lost the *strategy* aspect. It also lost the answer option: "I chose the words that fitted the story the best", which we believe would have been important. As a result, the data it produced could only partially be used to identify password selection strategies.

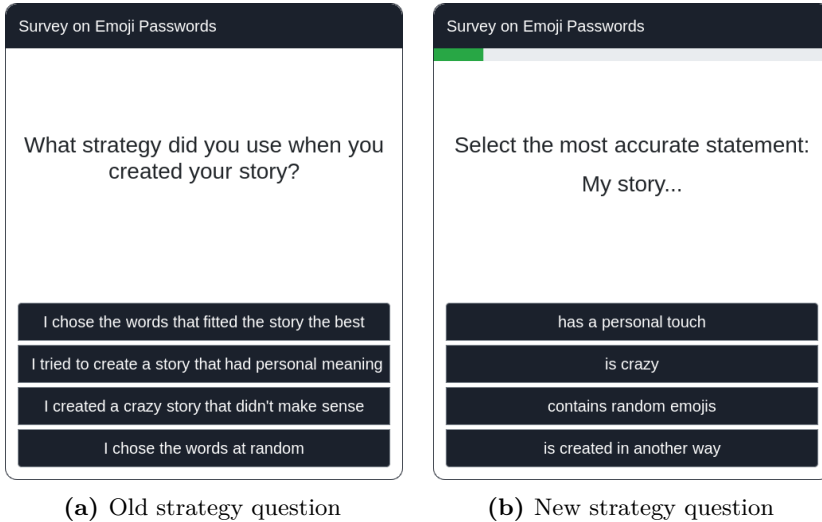


Figure 5.13: Changes made to the strategy question.

5.2 Follow-up Survey

After analyzing the results from the survey, we saw the need for conducting a follow-up survey in order to answer our research questions. The collected data from the initial survey could not be used to evaluate the long-term memorability of EmojiStory. This is discussed in more detail in Section 6.2.3 in the next chapter. Since the follow-up survey is quite similar to the initial one, we will not discuss it in detail. Instead, we will briefly describe how the follow-up survey differs from the first one in terms of setup and how it was conducted.

5.2.1 Setup and Design

The initial survey and the follow-up survey differ most in terms of setup. The main motivation for conducting the follow-up survey was to evaluate the memorability of EmojiStory over a longer period of time. As a result, the survey consist of two parts that are separated by seven days. The first part of the follow-up survey is almost identical to the initial survey, while the second part only include one login and two

5. EXPERIMENT SETUP

questions. This way, we are able to test how difficult emoji passwords created with EmojiStory, are to remember over a longer period of time.

We wish to evaluate the memorability that EmojiStory provides by, among other things, comparing our findings to the memorability of text passwords. Since there exist little research on this topic, some of the respondents actually create text passwords in the follow-up survey. When participants starts the survey, it is randomly determined if they will create a text or emoji password. Either way, the survey and creation process is the same until the password is generated and the summary screen is shown. Then, as seen in Figure 5.14, some users get a text password. The text is determined by what words users choose and is the textual counterpart of the emojis in the scheme.

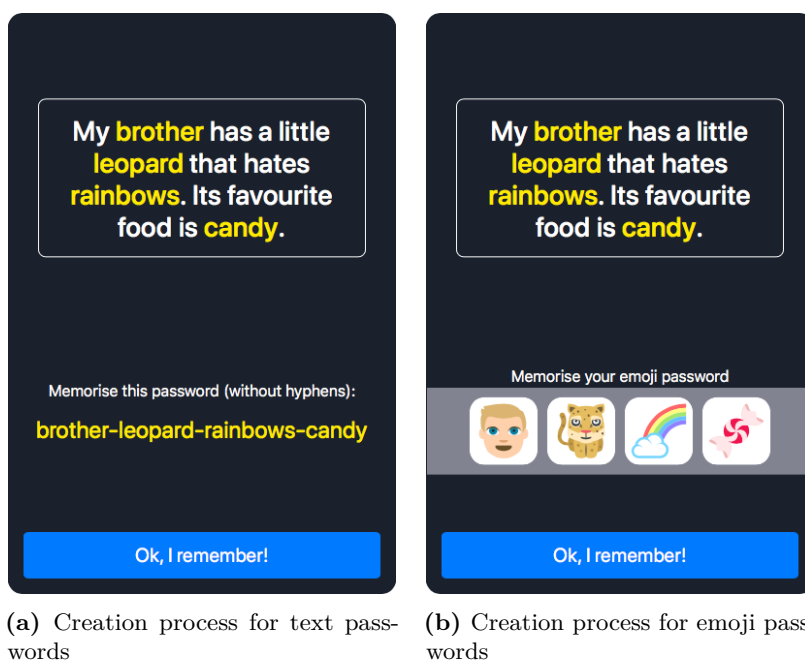


Figure 5.14: A comparison of the text and emoji password creation process in the follow-up survey.

The authentication process differs depending on the password type. As seen in Figure 5.15(a), participants with text passwords authenticate by entering text in a regular input field. Participants with emoji password log in using the emoji keyboard (Figure 5.15(b)) used in the first survey. However, the emoji characters are shuffled during the second login to test how this impacts the usability.

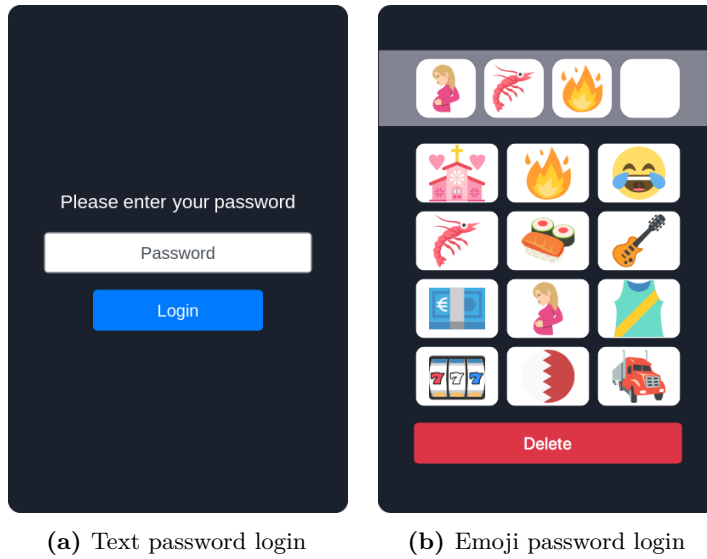


Figure 5.15: A comparison of text vs. emoji password login.

In order to remind participants of the second part of the survey, we ask them for their email address. The e-mail address entered cannot be registered before. The question can be seen in Figure 5.16.

Survey on Emoji Passwords

What is your age?

Age

Enter your email address:

Email

Submit

Figure 5.16: Opening questions in the follow-up survey.

Seven days after the first part is completed, we send out an invitation that contains a link (unique for each participant) to the second part of the survey. Participants

5. EXPERIMENT SETUP

start the survey by entering their email and are first asked to authenticate with their password. This process is identical to the ones in the first part, people with text passwords submit their password in an input field, while people with emoji passwords use their respective keyboards to login. Note that also this time the position of the emojis on the keyboard are shuffled.

Next, the participants are asked how often they thought about their passwords since they finished part one of the survey. This question can be seen in Figure 5.17(a). In addition, the participants who entered their passwords correctly are asked what they used to memorize their password. This question was also asked in part one of the survey and in the initial survey, and can be seen in Figure 5.2.

The questions regarding confusion and enjoyment were removed since we were satisfied with the data they produced in the initial survey.

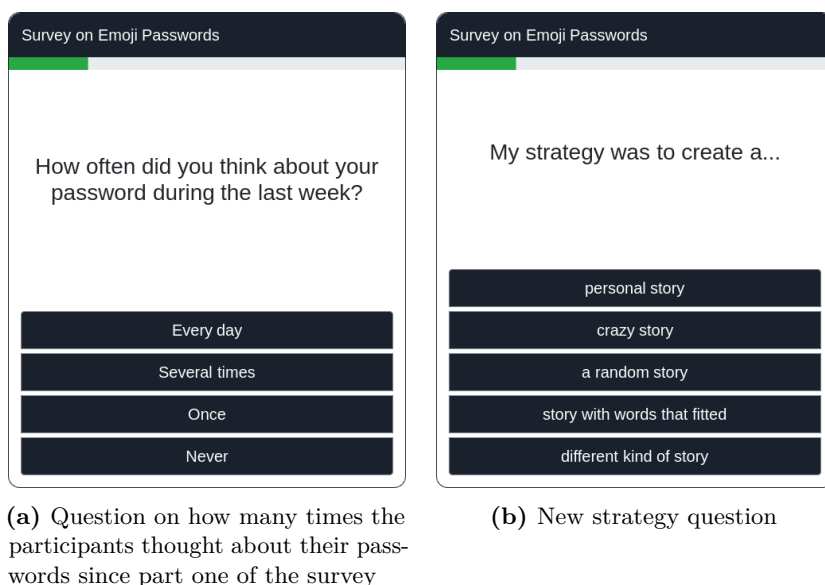


Figure 5.17: Changes made to the questionnaire.

5.2.2 Improving the Strategy Question

As mentioned in Section 5.1.4, we believe the wording of the strategy question in the initial survey was poor. Therefore the question was improved. As seen in Figure 5.17(b), we now specifically ask what strategy the respondents use and another answer option has been included. During and after the initial survey was conducted, we received feedback from several people requesting an alternative that match their selection strategy. Therefore, we added an answer option for people who create their

password by selecting the words they think are best suited for the story, and that make most sense to use.

5.2.3 Sampling Technique and Sample Size

The target population for the follow-up survey is the same as in the initial survey. However, we decided to slightly change the sampling method. We still intend to use a self-selection sampling technique, but we will only advertise the survey in some of our smaller networks in Norway. The reason for this is that we did not have time to test the technical aspects of the survey to a great extent. Therefore, in case something goes wrong, we do not want to deal with too many respondents.

Due to the limited time available, we are not able to carry out another lengthy data collection process. As a result, we do not expect a large sample size.

5.2.4 Changing EmojiStory

People creating text passwords in foreign languages are probably a rarity. It is probably easier for people to remember and use text passwords that are created in their native language. Since we expect the majority of the respondents to be Norwegian, we need to add support for the creation of Norwegian text passwords in the survey. In order to achieve this, we changed the functionality of EmojiStory and translated the meaning of some emojis to Norwegian.

In the follow-up survey, EmojiStory only has one possible story. Doing this reduces the workload significantly since we only have to translate the textual representation of emojis from the four categories used in the story. The story seen in Figure 4.3(c) in the previous chapter, was chosen because the results from the initial survey revealed that it caused the shortest password creation time. Also, the categories it contained were quite limited in size, which reduced the amount of translation work required.

5.3 Ethics

Over the course of this thesis, ethics have been given great consideration. Since this research included collection of personal data, our project was subject to *The Personal Data Act No. 31*. The Act is intended to protect people from violation of their right to privacy when their personal data is processed. Consequently, it was necessary to report the project to NTNUs Data Protection Official for Research, Norwegian Centre for Research Data (NSD) [73]. The personal data we collected included age, gender, nationality, professional background and email address. None of this information is regarded as sensitive.

5. EXPERIMENT SETUP

As discussed in Section 5.1.2, ensuring anonymity and confidentiality when conducting an online survey can be challenging. Since the surveys were made entirely by us, there are no third parties involved that have access to the data. Also, there are no servers that log IP addresses or timestamps. Finally, all data was transferred over encrypted communication channels.

Chapter 6

Results and Discussion

In this chapter the results of all experiments conducted in this project (i.e. initial survey and follow-up survey) are presented and discussed in chronological order.

6.1 Preprocessing the Survey Data

Before we started analyzing the data from the surveys, we had to make sure it was correct. First, corrupt records were removed. Some participants had passwords containing more than four emojis, which is impossible in EmojiStory. In addition, incomplete records (i.e. records that did not contain answers to the survey questions or results from any of the logins) were discarded. Finally, outliers¹ were removed manually in most cases.

6.2 Initial Survey

This section focuses on the first survey of this project. The main objective of the experiment was to collect quantitative data that can be used to evaluate the usability and security of EmojiStory.

6.2.1 Participation

As described in Section 5.1.1, a self-selection sampling technique was used to get people to take our survey. Although we suspected that it could be difficult to achieve a sample size of at least 1067 participants, it turned out that this was not the case (see Table 6.1). 1935 people started the survey and 1691 of them also completed it. In addition, 1787 people created their own emoji password, but did not answer all the questions in the survey.

¹ Data points that are much larger or smaller than all the other.

6. RESULTS AND DISCUSSION

Such a large sample size should allow us to generalize our findings and draw conclusions from the collected data. The next section, however, indicates that there are other factors that need to be taken into account before this may be concluded.

Description	Value
People who started the survey	1935
People who finished the survey	1691
Total number of created emoji passwords	1787

Table 6.1: Different numbers for the participation of people in the survey.

6.2.2 Participant Background

To determine whether the collected data is biased, several questions were asked to collect background information about the participants.

Among the participants there were 1044 males, 626 females and 21 people who identified themselves with a different gender. With 62%, the males made up the clear majority, while females and other genders stood for 37% and 1% respectively. Furthermore, 1062 people (63%) stated that they have a background in IT and information security, while the remaining 629 (37%) answered that they have not. The logging of the device type shows that 56% of all participants answered the survey on their mobile device and 44% on a desktop computer.

This asymmetric distribution of the various attributes obviously affects whether a generalized conclusion can be drawn. All the numbers on gender, IT and security background and different types of devices are summarized in Figure 6.1.

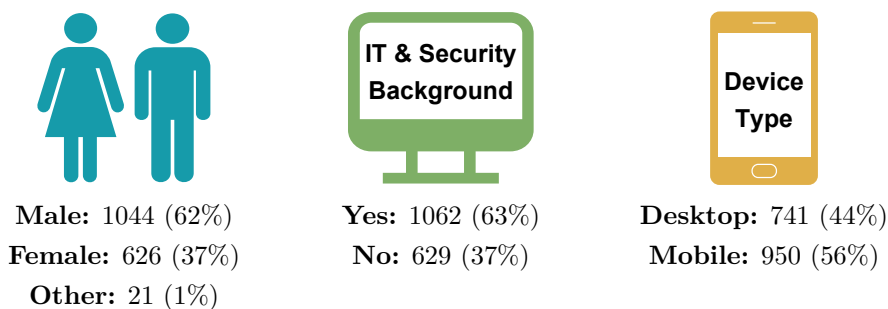


Figure 6.1: A summary of different participant background information.

Age Distribution

To enable visualization of the participants' ages, we divided them into six groups – below 21, 21-32, 33-42, 43-52, 53-64, and over 65 years old. Figure 6.2 shows this distribution.

Almost 49% of all participants were between 21 and 32 years old. This unbalanced distribution is likely to be influenced by how we shared the survey. The resulting sample consequently contains many people of about the same age as us. Still, 45% of the participants were between 33 and 64 years old. The groups with an age below 21 and above 65 years are the ones with the fewest attendees.

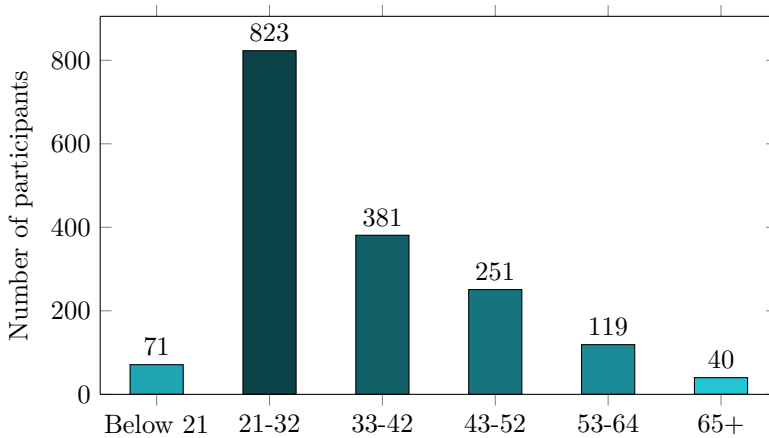


Figure 6.2: The age distribution for different groups of ages.

Participant Origin

The survey asked all participants where they come from. As Table 6.2 is showing, 1101 people came from Norway, which is the vast majority. Furthermore 175 people were from Germany, 98 from the USA and 39 from both Sweden and Great Britain. In total, people from 67 countries took part in the survey.

The fact that the overwhelming majority of all respondents came from Norway has a good reason. The online survey was distributed through our own social network, which mainly consists of Norwegians. Translating the survey into German and English was done to allow a more homogeneous distribution. The numbers prove that this has not been achieved, but it has definitely helped to make Germany and the USA the second and third largest countries of origin.

6. RESULTS AND DISCUSSION

Country	Number of survey respondents (n=1683)
Norway	1101
Germany	175
United States of America	98
Sweden, United Kingdom	39
Belgium	27
France	18
Netherlands	15
India	11
Denmark, Finland, Italy, Spain	9
New Zealand, Poland	8
Australia, Canada, Ireland	7
Croatia, Russian Federation	5
Greece, Slovakia + 2 more	4
Algeria, Argentina, Belarus + 3 more	3
Albania, Austria, Hungary, Serbia + 2 more	2
Czech Republic, Iceland, Portugal + 28 more	1

Table 6.2: The distribution of origin among all survey participants.

Emoji Usage

Figure 6.3 shows how frequently the participants use emojis. 65% use emojis *several times a day*. Looking at the figure, it is clear that people who use emojis often are over-represented in the sample. This can be explained by considering how age relates to emoji usage. As seen in Table 6.3, younger people use emojis more often. The table shows that 76% of the participants in the 21-32 age group use emojis several times a day, while this is only true for 24% of people over 65. Since young people are dominating the sample, the collected data regarding emoji usage is biased. Nevertheless, we believe that people who use emojis less frequently are represented well in the sample. Since emojis are extremely widespread and popular, it is quite impressive that the sample contains 7% that never use any emojis.

6.2.3 Password Memorability

As mentioned in Section 5.1.3 there are two authentication processes in the survey, one immediately after the emoji password is created, and another after the questionnaire. When analyzing the memorability, we chose *not* to exclude participants who did not

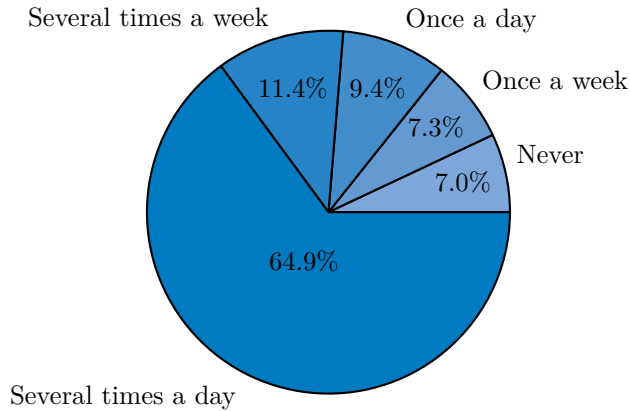


Figure 6.3: The use of emojis among all participants.

Group of age	Using emojis several times a day
Under 21	66%
21-32	76%
43-52	55%
52-64	35%
65+	24%

Table 6.3: The use of emojis several times a day for different age groups.

finish the survey, since some people left the survey after they failed to authenticate the first time. Leaving out this group would be a mistake because they impact the password memorability that EmojiStory provides.

The results from the two authentication processes can be seen in Table 6.4. 98.75% of the respondents were able to successfully authenticate the first time, while 99% entered their correct passwords the second time. The respondents had three attempts each time. The results seem very impressive. However, the first authentication results may be expected in a real scenario. The participants task is to enter four emojis from a keyboard of twelve immediately after the password creation process. We even ensure that each emoji on the keyboard comes from different categories, resulting in twelve quite distinctive emojis. This does not appear to be very challenging and close to everyone entering their emoji passwords correctly within three attempts is to be expected.

On the other hand, the results from the second authentication process are surprisingly good. Participants are asked to re-authenticate in order to see how answering the

6. RESULTS AND DISCUSSION

questionnaire affects their ability to remember the password. According to psychology studies, visual information is only held in short-term memory up to 30 seconds [74]. As the questionnaire takes roughly a minute to complete, it acts as a distraction, removing the participants' emoji passwords from their short-term memory. However, evaluating the memorability of a password scheme based on short-term memorability only is not sufficient. The long-term memorability of EmojiStory is examined in the follow-up survey. Therefore, memorability is further discussed in Section 6.3.3.

Also surprising is the fact that the authentication results are slightly better the second time than the first time. However, this can be explained by the fact that some people fail on the first login and leave the survey before the second login. In addition, two people who failed the first time were able to successfully authenticate the second time.

Authentication result	First login (n=1766)	Second login (n=1699)
Correct password	98.75% (1744)	99% (1682)
Incorrect password	1.25% (22)	1% (17)

Table 6.4: The results from the authentication processes. Both times the participants were given three attempts to successfully authenticate.

6.2.4 Scheme Efficiency

While the participants were answering the survey, different timestamps were recorded in the background. These were used to calculate the time it took to complete various tasks (e.g. creating the emoji password). This section presents the resulting timespans and compares them with those of other password schemes. Note that only the calculated times were stored, not the timestamps themselves.

Most of the collected data regarding time usage was not normally distributed. Therefore, we have generally stated the median times as they are perhaps a better measurement than the average. However, we have also included the Interquartile Mean (IQM) times. If you remove the lowest 25% and the highest 25% of your data and then calculate the mean of the remaining data, you get the IQM. This measurement is also suited for data that has a skewed distribution since outliers are disregarded.

Statistical Significance

To evaluate the validity of the results regarding scheme efficiency, two-tailed t-tests have been performed. The t-test was used to see if there were significant difference in the efficiency of different types of participants. Since a t-test assumes normally

distributed samples, skewed data has been transformed using the IQM. A significance level of 0.05 was used in all tests. Since the tests are two-tailed, statistical significant difference between two samples is assumed if we get a p-value under 0.025.

Password Creation Time

Figure 6.4 shows the average password creation time in EmojiStory. The median time is 33 seconds, while the IQM time is 33.5 seconds.

Although there exist little research on password and PIN creation time, we have identified some evidence that can be used to evaluate the password creation time of EmojiStory. According to Biddle et al. [43], Passfaces Corporation who developed the Passfaces scheme (see Section 2.3.1) reported a password creation time of three to five minutes. Wiedenbeck et al. [42, 34, 60] designed and evaluated a graphical password scheme called PassPoints (see Section 2.3.1) through three user studies. They found that it took 64 seconds on average to create a password. Another study reported that average password creation was 40 seconds in a scheme with close to identical functionality as PassPoints [75]. Finally, in the study by Seitz et al. (see Section 3.7), an average password creation time of 53 seconds was stated. The passwords contained both text characters and emojis.

We suspected that creating passwords in EmojiStory would be a very time consuming task. Even though it probably takes less or similar time to create PINs and text passwords, we believe the results show that the time required to create an emoji password with EmojiStory is definitely acceptable. However, when evaluating the efficiency of a password scheme, we believe login time is more important than creation time. Login is the most frequent task performed in an authentication system.

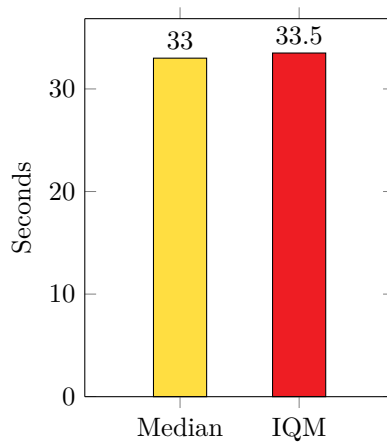


Figure 6.4: Median and IQM password creation times.

6. RESULTS AND DISCUSSION

Login time

As seen in Figure 6.5, the median time for the first login was six seconds, while the IQM was 6.5 seconds. The times ranged from two to 62 seconds. Figure 6.5 also shows that the input times for the second authentication were lower. The second median login time was four seconds, while the second IQM login time was 4.7 seconds. The times ranged from two to 34 seconds. The login times are calculated based on all three login attempts.

We found it surprising that the input times were better the second time. We suspected the questionnaire would distract the users to such an extent that it required more effort to enter the password the second time. However, the position of the emojis on the keyboard is the same both times. As a result, it is likely that the participants perform better the second time as they know the positioning of their emojis.

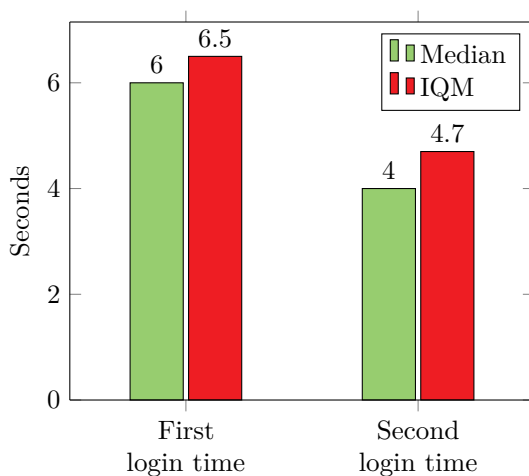


Figure 6.5: Median and IQM login times for the first and second authentication processes.

Figure 6.6 compares the IQM times for logins performed on desktop and mobile devices. During both logins the time used by the participants with desktop devices, was nearly identical to the participants with mobile devices. On the first login, the desktop users spent 6.6 seconds and mobile users 6.5 seconds. On the second login the participants with mobile devices used 4.7 seconds, while participants with desktop devices used 4.8 seconds. Table 6.5 shows that the differences between mobile and desktop login times are not statistical significant.

These results are slightly surprising as we suspected participants with mobile devices to be faster. Graphical password schemes are often more efficient to use on mobile devices and use of emojis is more widespread on mobile devices. However, considering

that the login process only requires straightforward input in form of clicking or physical tapping, the results are perhaps to be expected.

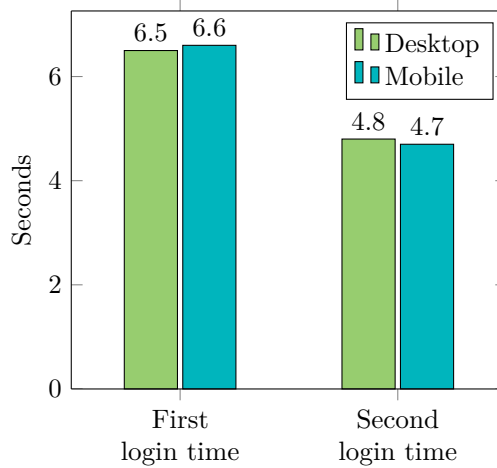


Figure 6.6: IQM login times categorized by device type.

Login	Device	Mean	SD	n	P-value	Result
Login 1	Desktop	6.59	2.76	730	0.6624	Insignificant
	Mobile	6.53	2.77	910		
Login 2	Desktop	4.78	1.95	721	0.4279	Insignificant
	Mobile	4.71	2.06	886		

Table 6.5: Statistical significance for login time based on device type.

Wiedenbeck et al. [42, 34, 60] reported login times between nine and 19 seconds on average for PassPoints. The login times in graphical password schemes are generally significantly longer, some even in terms of minutes [76]. However, we believe it is more important to compare the efficiency of EmojiStory to PIN codes and text passwords.

Unfortunately, very limited research on how long time it takes to enter PINs a passwords exists. Still, it is reasonable to believe that they can be entered within a few seconds on a standard keyboard. A study that included 8,143 participants showed that this was not the case. Login times of text passwords varied from 11.6 to 16.2 seconds [66]. Also, a study by Schaub et al. [77], describes significantly longer entry times of text passwords on mobile devices. The median entry time on iPhone 4s and Nexus One is approximately 20 seconds.

6. RESULTS AND DISCUSSION

Our results seem to suggest that login in EmojiStory is efficient compared to PIN and password entry. In the follow-up survey we also measure login time seven days after not using the emoji password. Therefore, the efficiency of EmojiStory is further discussed in Section 6.3.4.

We cannot trust the calculated times blindly, because time continues even if the participants leave the survey open and do something else on the side. One participant used four seconds on the first login, while the second login took 36 seconds. Both times, the correct password was entered on the first attempt. This seems rather unlikely as our results show that the median login time of the second login was 2.5 seconds lower than the first.

Training Time

Most graphical password schemes require training in order to compensate for the novelty of the schemes [43]. In the case of EmojiStory, it is likely that it needs additional training time to make up for the amount of randomness in the password creation process. In the survey we define training time as the time spent on the EmojiStory instruction screen (see Figure 5.1(b)) and the summary screen (see Figure 4.2(i)). Average time spent on instructions was 13.4 seconds, while it was 9.1 seconds on the summary screen.

The survey results indicate that there is some correlation between training time and the participants' ability to remember their passwords. On average, participants who failed to login used less training time. Figure 6.7 shows that the difference is quite small when looking at the time spent on the EmojiStory instructions, while the difference is large regarding the time used on the summary screen (see Figure 6.8). For instance, participants who failed to log in during the first authentication process, spent 3.4 seconds less on the summary screen.

The results from a two-tailed t-test, which tests the difference in time spent reading the instructions depending on login result, is summarized in Table 6.6. The test revealed that the difference is not statistical significant. Table 6.7 also summarizes the results from another two-tailed t-test. In this test, the difference in time spent on the summary screen based on login result, is analyzed. The test revealed that the difference is significant.

Determining how much training time EmojiStory requires is difficult. Note that we are not talking about the training time needed to use the scheme, but rather to be able to remember the created passwords. Our results suggest that spending under nine seconds on the summary screen is not enough. However, 207 participants (11.7%) used four seconds or less on the summary screen and still entered correct passwords on both logins.

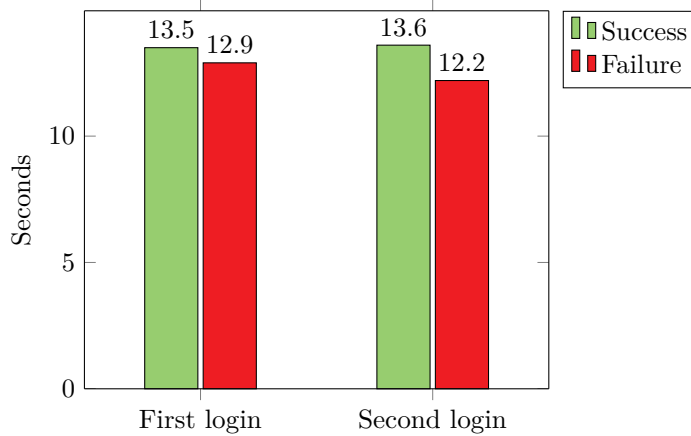


Figure 6.7: Average time spent on the EmojiStory instructions depending on the authentication results.

Login	Outcome	Mean	SD	n	P-value	Result
Login 1	Success	13.45	5.34	1643	0.633	Insignificant
	Failure	12.90	6.77	22		
Login 2	Success	13.61	5.35	1585	0.283	Insignificant
	Failure	12.19	6.42	17		

Table 6.6: Statistical significance for time used on the EmojiStory instructions and authentication result.

Since the initial survey only evaluated the participants' ability to remember the passwords over a short period of time, we cannot use the results to conclude how much training time is required to remember the passwords for a longer duration.. The results are, however, promising when compared to other graphical password schemes. For instance, Wiedenbeck et al. [60] estimated that the average required training time of PassPoints (see Section 2.3.1) was 171 seconds.

6.2.5 Memorization Strategy

In the survey, we asked all participants who successfully entered their passwords what memorization strategy they used to remember them. The results are shown in Figure 6.9. As you can see, most people memorized what the emojis looked like in combination with the story. Surprisingly, 1203 participants (72%) said they used the story in some way when they entered their emoji passwords. Therefore, the results suggest that the story is helpful in order to memorize the passwords.

6. RESULTS AND DISCUSSION

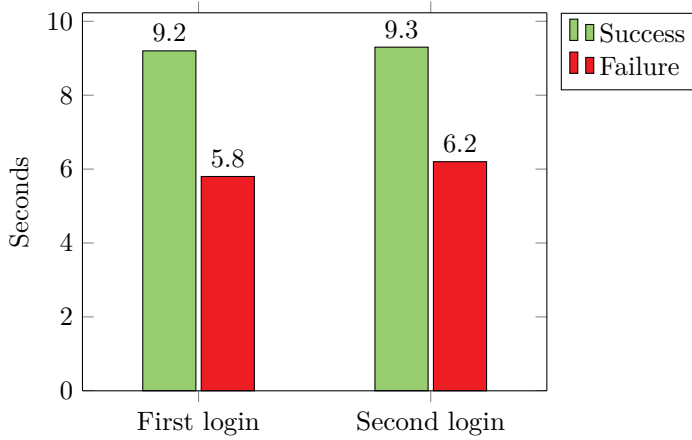


Figure 6.8: Average time spent on the summary screen depending on the authentication results.

Login	Outcome	Mean	SD	n	P-value	Result
Login 1	Success	9.19	4.81	1652	0.0011	Significant
	Failure	5.82	5.11	22		
Login 2	Success	9.25	4.82	1593	0.0102	Significant
	Failure	6.23	4.45	17		

Table 6.7: Statistical significance for time spent on the summary screen based on the authentication result.

Note that the question regarding memorization strategy is only asked after the first authentication process. It would be interesting to see if the results had changed after the second authentication. The memorization strategy is further discussed in Section 6.3.5.

6.2.6 User Satisfaction

As seen in Figure 6.10, 76% of the survey participants enjoyed creating their emoji passwords. 13% did not think it was fun, while 11% were uncertain about what they thought of the enjoyment of EmojiStory. Considering password creation is *not* a process that is usually regarded as fun nor associated with enjoyment, these results were unexpectedly high.

One aspect of usability is satisfaction [78]. Although satisfaction consists of several metrics, one of them is how much fun it is to use the system [79]. A system that

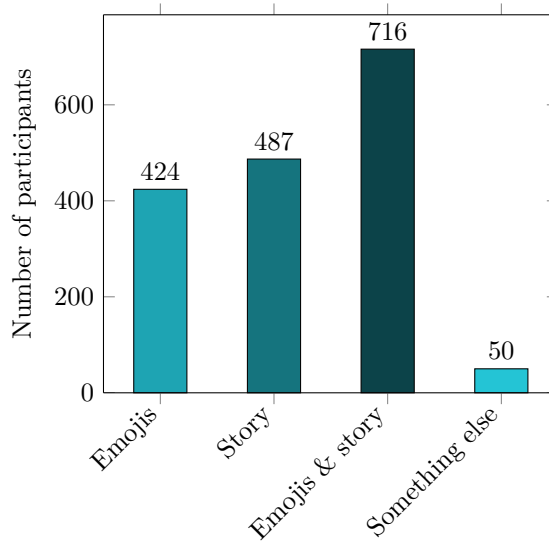


Figure 6.9: Memorization strategy among all survey participants.

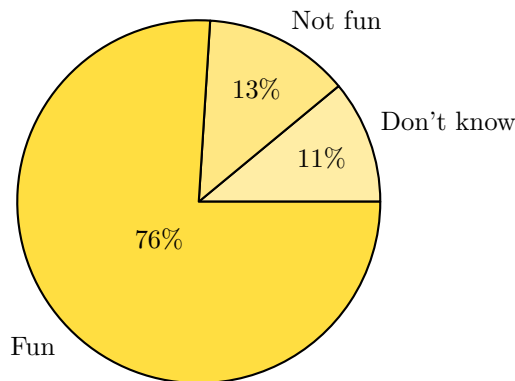


Figure 6.10: The distribution of enjoyment among all participants.

offers a high level of satisfaction can result in more people using it. Also, engaging systems may outweigh low efficiency. If a system is perceived as slow by users, it can still be accepted if it is appealing and offers a positive user experience [42].

The results suggest that EmojiStory provides a positive user experience. However, this single metric is not enough to evaluate the satisfaction of a password scheme. We also believe that the results in terms of enjoyment are artificially high because of bias in the sample. Figure 6.11 shows that the participants attitudes towards EmojiStory are influenced by how often they use emojis. For instance, people who

6. RESULTS AND DISCUSSION

use emojis more frequently enjoyed the scheme more. As seen in the figure, 70% of the people who enjoyed creating passwords use emoji several times a day, while this group only represents 39% of the people who did not enjoy it. Clearly, the results regarding enjoyment should not be generalized to the target population.

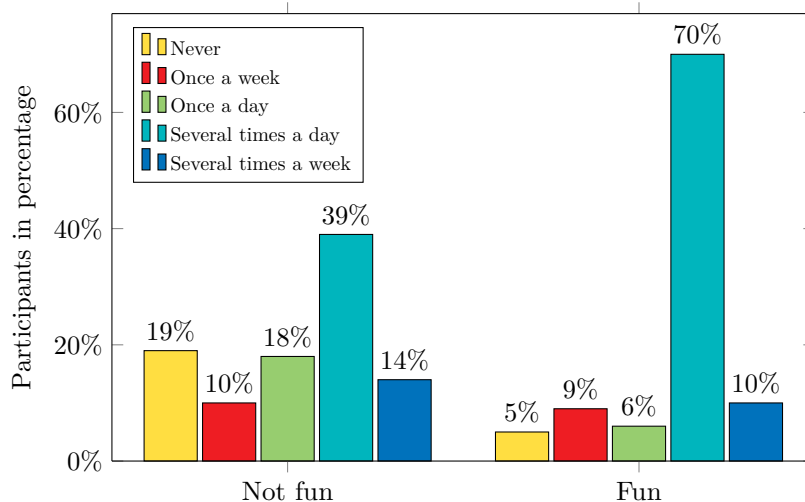


Figure 6.11: The percentage of participants who thought EmojiStory was or was not fun to use, based on how often they use emojis.

Since people with a background in IT or security also are over-represented in the sample, we anticipated that the same phenomenon would be observable in this group. We suspected that people with an IT or security background would enjoy creating passwords with EmojiStory the most since it may be more likely that this group gets excited about digital innovation. However, Figure 6.12 shows that this is not the case. In the figure we see that 90% of the people without an IT and security background enjoyed it, while 83% of the people with this background, said the same. This shows that, in percent, actually more people *without* a background in IT or security thought it was fun to create an emoji password.

As mentioned earlier, 11% said that they did not know if they thought the password creation was fun or not. Since this is a relatively high percentage, we believe that many people in this group were neutral to the enjoyment of EmojiStory. Consequently, we believe the quality of the question about enjoyment was poor. We should have included *neutral* as an answer option or asked the participants to rate the enjoyment on a scale.

Finally, the results regarding enjoyment could be affected by technical difficulties. Based on the collected data and feedback, it is evident that some of the partici-

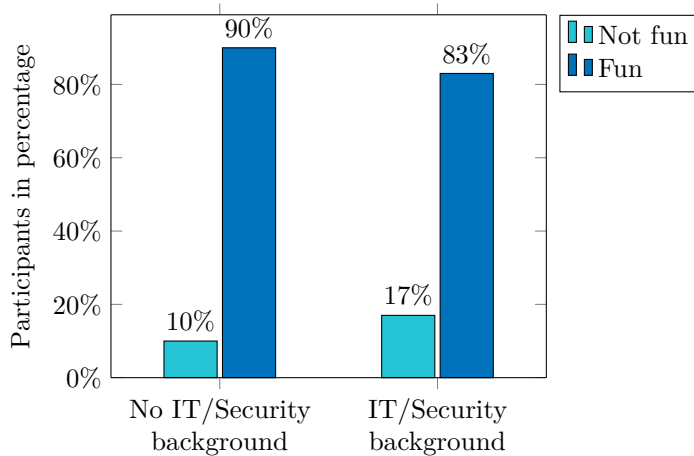


Figure 6.12: The percentage of participants who thought EmojiStory was or was not fun to use, based on their background.

pants experienced minor errors during the survey, which probably influenced their satisfaction with EmojiStory.

Ease of Use

The participants were asked if they felt confused during the password creation process in the survey. Figure 6.13 shows that 3% of the participants were uncertain whether they got confused or not, while 2% said they felt confused during the password creation process. The majority of the participants (95%) did not experience any confusion. This is a surprisingly high percentage, given that the password creation process in EmojiStory is novel and unfamiliar. In addition, the participants were given little training (see Section 6.2.4). Taking this into account, the results regarding confusion suggest that EmojiStory is straightforward and easy to use.

6.2.7 Practical Password Space

The security of a password scheme is affected by the size of the practical password space since it determines the guessability of the passwords. It is very difficult, if not impossible, to calculate the size of the practical password space without looking at actual user data. This section deals with various aspects that influence this security measure and discusses the findings.

Spatial Password Patterns

One useful property to investigate is the placement of the users' passwords on their virtual emoji keyboards. When many passwords share the same positions, attackers

6. RESULTS AND DISCUSSION

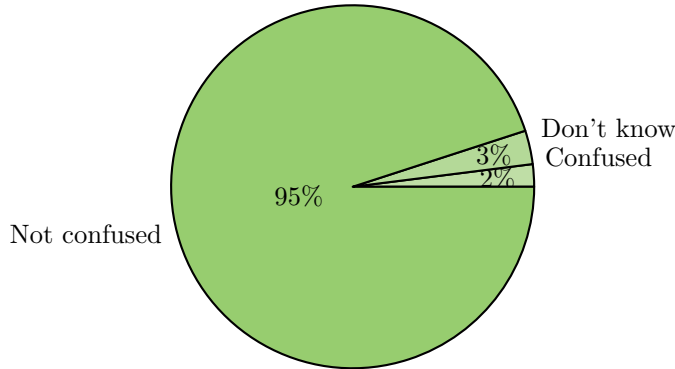


Figure 6.13: The distribution of confusion among all participants.

can take advantage of this fact to guess passwords. Research on graphical password schemes that lets users select their password using the same keyboard or interface they use for login, suggests that people tend to use spatial patterns. This applies to the PIN scheme [80], the emoji schemes EmojiAuth [10] and PictoPass [9], and of course the Android Pattern Lock [41]. For instance, the lab and field studies conducted by Kraus et al. [10] showed that around 42% of all participants used a spatial pattern when selecting their password on the keyboard.

As described in Section 4.2.5, we tried to avoid the use of patterns by placing all keyboard emojis at random positions. The results from our survey show that only a few passwords had the exact same positions on the keyboard. In total, six unique position sequences were each allocated to three participants, while 105 positions were used twice. The remaining 1462 key positions were completely unique, which means they have not been assigned to more than one user each. Figure 6.14 illustrates three examples of the positions that were used most often.

The placement of the entire password on the user's keyboard is not the only factor that can influence the practical password space. One must also consider the individual positions of every password character. Uellenbeck et al. [41] showed that there was bias on entry points for the Android Pattern Lock. 43% of the survey participants started their password in the top left position. The same phenomenon was identified by Golla et al. [9].

Figure 6.15(a) shows the distributions of the first password character positions among all the participants in our survey, while Figure 6.15(b) illustrates the same for the last password character positions. There is no clear keyboard position that dominates, as it is the case for the other graphical password schemes, but some bias still does

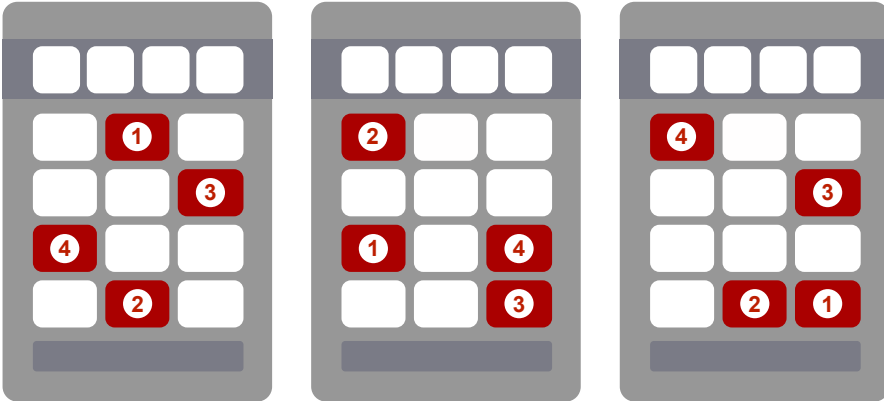
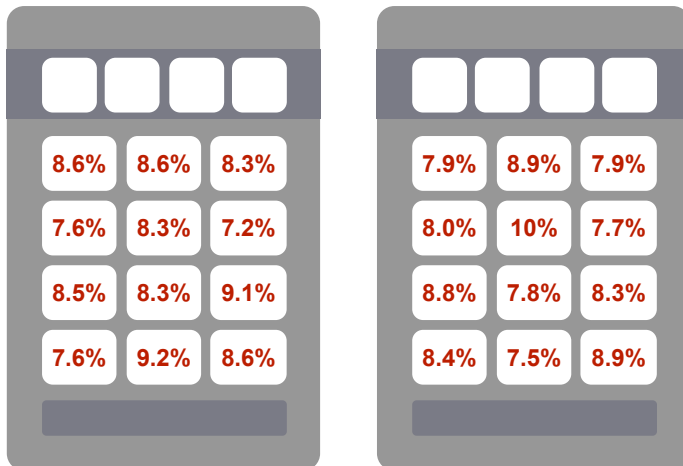


Figure 6.14: Three different password positions that were allocated to users exactly three times each. The numbers show the order of the keys in the corresponding password.

exist. The maximum difference between two first password character positions is 2% (34 positions), while the difference for the last password characters is 2.5% (42 positions). This can be traced back to the lack of proper randomization of the keyboard positions. We used the Fisher–Yates Shuffle algorithm [81] to generate random key orders. However, other algorithms might give better results.



(a) First password character positions (b) Last password character positions

Figure 6.15: The distribution of the first and last password characters at different key positions.

6. RESULTS AND DISCUSSION

Password Duplicates

If all users of an authentication scheme used the same password, it would be trivial for an attacker to gain access to the data of an arbitrary user. Fortunately, this is not the case in the real world. Yet it is not uncommon for some passwords to occur more often than others. Huge publicly disclosed password lists from hacking attacks, such as the *RockYou* list containing over 32 million passwords, show that some passwords are used more than one time [82]. The same applies to the study carried out by Golla et al. [9], in which two passwords occurred more than twice, while 13 occurred more than once.

The separation of password creation and login procedure in EmojiStory seemed to have influenced the formation of password duplicates. All the 1690 passwords that were created with EmojiStory are unique. In other words, there are no duplicate passwords.

Selection Strategy

As mentioned in Section 3.4, analyzing password selection strategies is important. Understanding how people choose their emoji passwords can help to evaluate the practical password space of EmojiStory.

In EmojiStory the user do not actually select emojis, but words that represent them. The words are grouped into specific categories and each word has to be selected from a set of five random options. The password creation process in EmojiStory is described in detail in Section 4.2.4.

In the survey we asked the participants to select the most accurate statement about how their final stories were created. The results can be seen in Figure 6.16. 20% said their stories are made up by random emojis, 19% said their stories have a personal touch, 54% said their stories sound crazy, and 7% said their stories were created in another way. These results can be used to say something about how the participants selected their passwords. However, they cannot be used to determine what selection strategies exist in EmojiStory, only provide an indication. For instance, we cannot claim that the participants who said their story is crazy, used a strategy where they chose the strangest words in order to create a crazy story. People can say that their stories sound crazy even though they selected the words that they thought were best fitted for the stories.

Still, the results from the survey suggest that there could be some correlation between selection strategy and story description. In Story 5 (see Figure 4.3(e)), the users are supposed to select a keyword from the animal category which represents a pet ("...has a little [animal]"). In this case, 14% (13 people) of the participants who

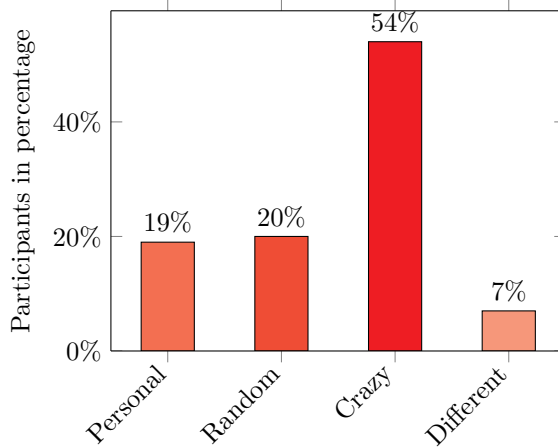


Figure 6.16: The distribution of story descriptions among all participants.

described their stories as personal, selected *cat* or *dog*. In contrast, there were only 3% (6 people) of the participants who described their stories as crazy, that selected *cat* or *dog*. Since cats and dogs are common pets, it is likely that they were selected by people who intend to create a story with personal meaning.

Another example can be found in a different story. In Story 4 (see Figure 4.3(d)), the users are supposed to select a keyword from the place category which represents the home of an animal ("The [animal] grew up [place]."). Only 3.7% (2 people) of the participants who described their stories as personal, selected *on the moon*. On the other hand, 7.2% (14 people) of the participants that described their story as crazy, selected the same. Since it is pretty absurd for an animal to grow up on the moon, it is likely that it was the participants strategy to create a crazy story.

The results also suggest that the way people describe their stories depends on what story template they got. For instance, 59% of the participants who got Story 5 described it as crazy, while only 43% of the participants who got Story 2 said the same. Also, 26% of the participants who got Story 3 described it as personal, while only 15% of the participants who got Story 5 said the same. These results are visualized in Figure 6.17. If there is a correlation between selection strategy and the participants description of their stories, it is likely that the selection strategy is affected by the story template. Consequently, bias in the passwords could be affected by how a story template is designed.

Based on results from the follow-up survey, some password selection strategies commonly used in EmoJiStory are identified in Section 6.3.6.

6. RESULTS AND DISCUSSION

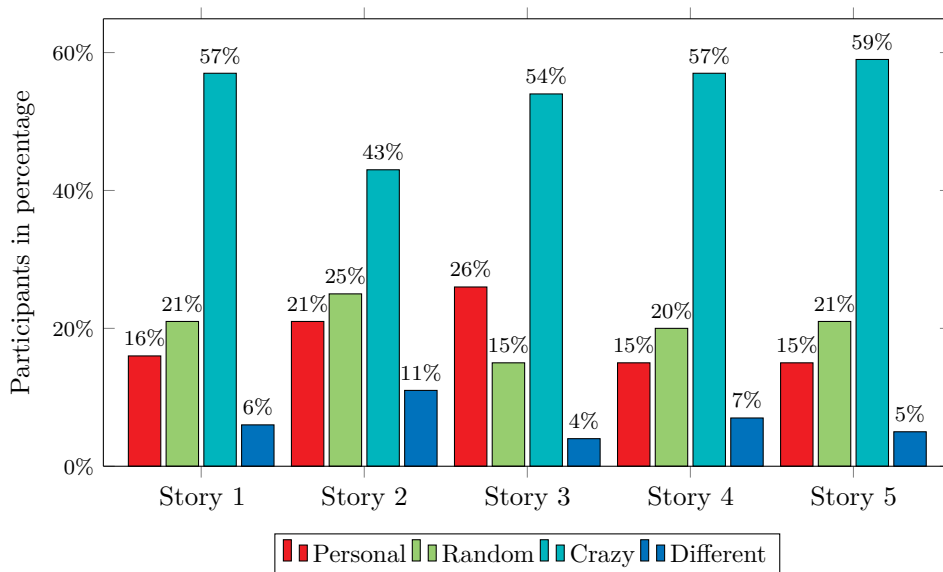


Figure 6.17: The distribution of the participants' story descriptions for each story template.

Emoji Selection

As well as analyzing selection strategies, it may be useful to look at the least and most frequently used emojis. The way a password is chosen can be broken into four individual emoji selections. When looking at those, we find bias in the words selected from every category in every story. Interestingly, chocolate (3.6%), candy (3.2%) and spaghetti (3.1%) are the most popular emojis in the food category (see Figure 6.18(a)), while the least popular emojis are bread (0.6%), eggplants (0.6%) and tomatoes (0.7%). It is not unlikely that this may reflect many people's favorite foods. Bread, eggplants and tomatoes, on the other hand, may be perceived as rather boring food.

The food category was not the only one that was distorted. In Story 4, the user is supposed to select a keyword from one of the object categories which represents something that can be won ("...has won several [object keyword]"). This time, the most frequently used emojis actually represent objects that fit best. Figure 6.19 shows that trophies, medals and crowns are the most popular emojis (6.2%). Prizes with low value, such as rulers (0.6%), paper (0.6%) and thumbtacks (0.9%), are used very rarely.

Another example of this phenomenon can be seen in Figure 6.20, which shows the distribution of words selected from the *person* category in Story 3. In this case,

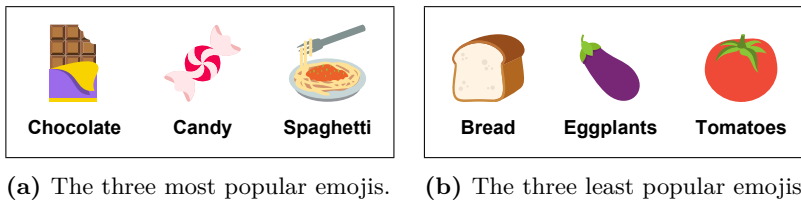


Figure 6.18: The three most and least popular emojis from the food category.

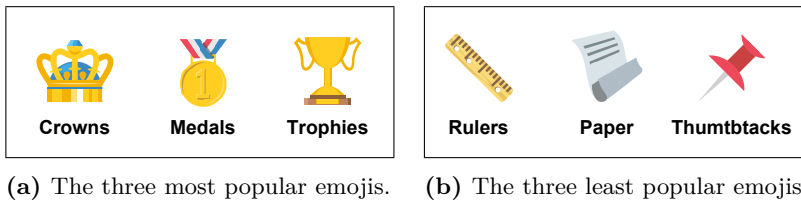


Figure 6.19: The three most and least popular object emojis used in story 4.

family is chosen by 14% of the participants, while *pregnant wife* is only selected by 4.5%. The person category only contains eleven different words.

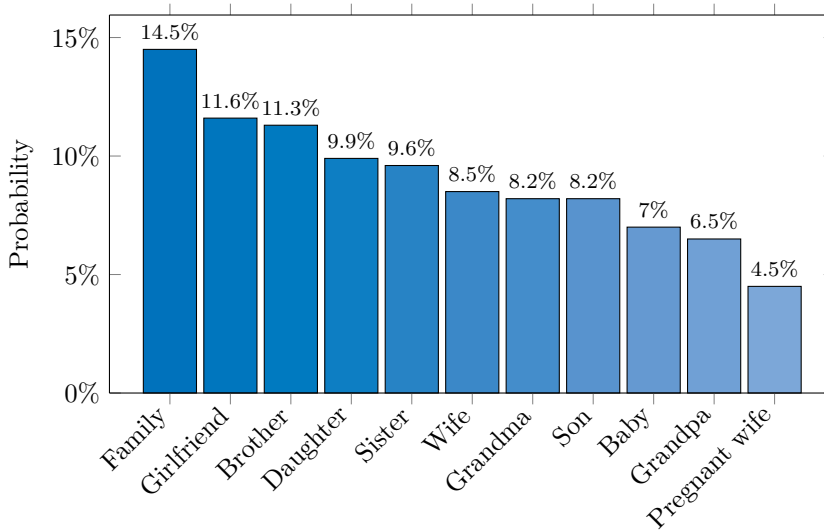


Figure 6.20: The distribution of word selections from the person category in story 3.

We thought that such bias would be less pronounced the larger the category. Yet, this does not seem to be the case. Figure 6.21, shows the distribution of words selected

6. RESULTS AND DISCUSSION

from the *country* category in Story 1. Although this category contains 153 words, the bias is even more significant than in the previous example. Yemen is only chosen by 0.3% (one person), while France is chosen approximately eight times more often (2.5%). Nevertheless, a large category leads to much lower chance of guessing the correct word.

Although the stories in the EmojiStory prototype varies in terms of content and style, the results regarding emoji selection show that patterns can be found in all of them. Some words are always favoured when the participants create their passwords. As a result, the practical password space of EmojiStory is lower than the theoretical.

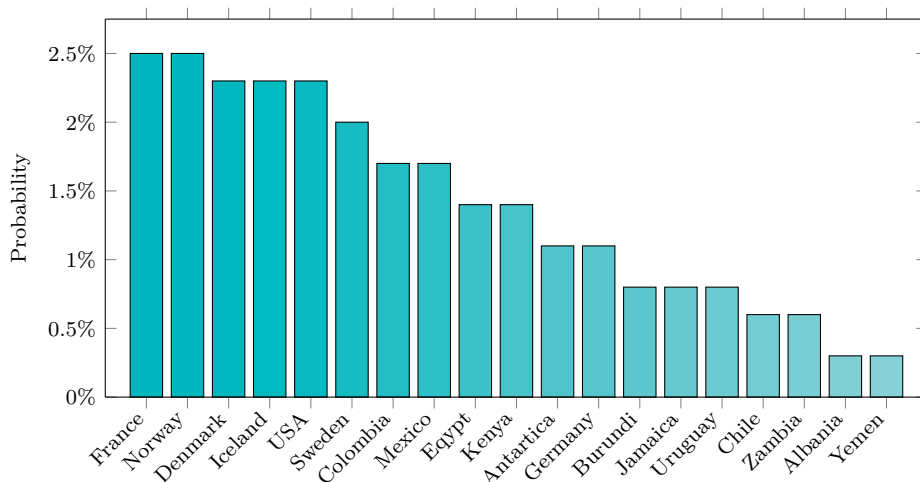


Figure 6.21: The distribution of words selected from the country category in story 1. Only a selection of the words are shown.

Due to insufficient data, our analysis of the practical password space of EmojiStory is limited. As mentioned earlier, only one person selected Yemen. For Yemen to be selected, it must be one of the five random answer options. If only one person had the opportunity to select Yemen, we cannot argue that other countries were favoured over it. Unfortunately, we did not record the answer options, only the answer itself. Therefore, we cannot be sure if the observed bias exist due to people favouring certain words over others or due to chance.

We suspected that we would find patterns suggesting that participants choose emojis which correspond to their origin. Yet, this does not seem to be the case. For instance, only 11 (3%) Norwegians chose the Norwegian flag emoji. Whether this is due to the fact that the keyword options they are presented contain their country emoji only rarely, or the participants deliberately ignore them is not clear.

There was also the possibility that some emojis would be selected more often than others because participants used the back button (introduced in Section 4.4.2) to find the emojis they like best. The great majority of all participants (93.9%) never used the button, while only a few participants used the button once (3.5%), or more than once (2.7%). Therefore, we can assume that most people chose their keywords independently of the corresponding emojis.

6.2.8 Shoulder-Surfing

Shoulder-surfing is a common issue in graphical authentication [60]. As mentioned in Section 3.6, people that use spatial patterns as their password selection strategies are especially vulnerable to shoulder-surfing attacks. Since the keyboards are generated randomly and no password positions are significantly more likely than others (discussed in Section 6.2.7, EmojiStory seems to be less susceptible to shoulder-surfing. In its final form, EmojiStory could mask entered emojis to further protect against shoulder surfing.

6.3 Follow-Up Survey

The second survey was very similar to the initial, with some minor changes and a different goal (as described in Section 5.2). This section presents the most valuable insights that were found regarding the security and usability of EmojiStory.

6.3.1 Participation

For the follow-up survey we again chose to distribute the survey in our own social network, but this time we had no clear idea of how many answers we wanted to achieve. Different numbers on participation are summarized in Table 6.8. Altogether, 65 people started the first part of the survey. Since the sample size is quite limited, we are not in a position to generalize the findings. Still, they can provide a deeper and more comprehensive picture of the security and usability of EmojiStory.

Description	Value
People who started the first part of the survey	65
People who finished the first part of the survey	56
People who finished the second part of the survey	45
Total number of created emoji passwords	35
Total number of created text passwords	28

Table 6.8: Different numbers for the participation of people in the follow-up survey.

6. RESULTS AND DISCUSSION

6.3.2 Participant Background

All survey respondents came from Norway and were between 19 and 54 years old, most of them (82%) were 19 to 54 years old. Furthermore, 54% were male and 46% female. Surprisingly, there were just as many participants with an IT and information security background as there were without.

6.3.3 Password Memorability

The first part of the follow-up survey revealed similar findings to the initial survey in terms of memorability. All participants with emoji passwords authenticated successfully on both logins. Nearly all participants that had text password were also successful. Two participants failed on the first login, while one failed to authenticate the second time.

The authentication results from the third login process are seen in Figure 6.22. Seven participants (41%) remembered their text passwords, while 25 participants (89%) remembered their emoji passwords. Although the sample is very limited, the results suggest that EmojiStory provides better memorability than text passwords. However, the results regarding text passwords are perhaps unfair. We can estimate the similarity between login attempts and the correct password by calculating the Sørensen-Dice coefficient [83]. When looking at the people who failed on their first attempt, their input was 56.5% similar to the correct password on average. You could argue that some of the participants remembered their password, but failed to authenticate due to syntactic errors in their input.

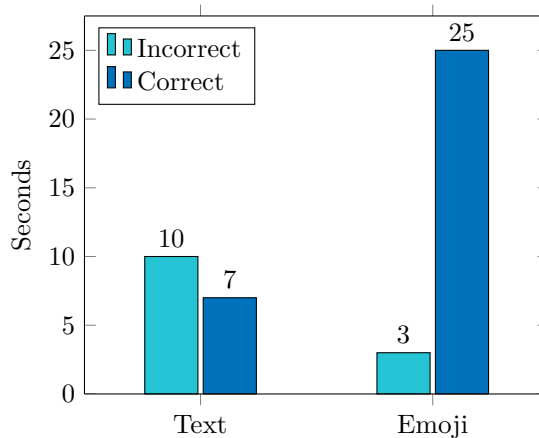


Figure 6.22: The results from the third authentication process in follow-up survey, grouped by password type.

As described in Section 5.2.1, the participants were required to wait seven days before they could start the third authentication process. Since some participants responded faster than others, the average waiting time ranged from seven to 17 days. The average time between part one and part two of the follow-up survey, differs slightly depending on the authentication result. These differences can be seen in Table 6.9. Generally, participants with text passwords waited longer between part one and two. It is likely that this affected the results regarding memorability.

Password type	Successful login	Unsuccessful login
Emoji	7.6 days	8.3 days
Text	7.7 days	9.3 days

Table 6.9: Average time between second and third login depending on participants' password type and authentication result.

It is unclear how well the experiment simulates practical password use. Seven days between two logins are perhaps not so common. Typically you have some passwords that are used more frequently (daily) and other passwords that you use less frequently (monthly). PIN codes used to unlock smartphones are even used several times a day. Consequently, it is difficult to determine whether the collected data reflects the actual memorability of emoji passwords created with EmojiStory.

In the study by Golla et al. [9], 84.6% successfully authenticated within three attempts after two days. Compared to this, the results from the follow-up survey seem impressive. Yet it is not straightforward to compare these results. In the study by Golla et al. [9], participants could select their passwords as they wished from a set of 20 emojis. In our study, on the other hand, participants are rather restricted when they create a password and the login keyboard only contains 12 emojis. Still, we believe the results suggest that EmojiStory offer high memorability.

One aspect that might influence the memorability results, is how often the participants thought about their passwords during the time between the first and second part of the survey. Therefore, participants were asked how much time they spent thinking about their passwords in this period. The results can be seen in Figure 6.23. Most people (79%) with emoji passwords, never thought about them, few (18%) said they thought about them once or more than once, while only one participant (3%) thought about it every day. For respondents with text passwords, these numbers were quite different. 59% thought about their passwords once, 23% never thought of them, and the remaining 18% thought of them several times or every day.

According to these results, participants with text passwords thought about their password more frequently than the participants with emoji passwords. Consequently,

6. RESULTS AND DISCUSSION

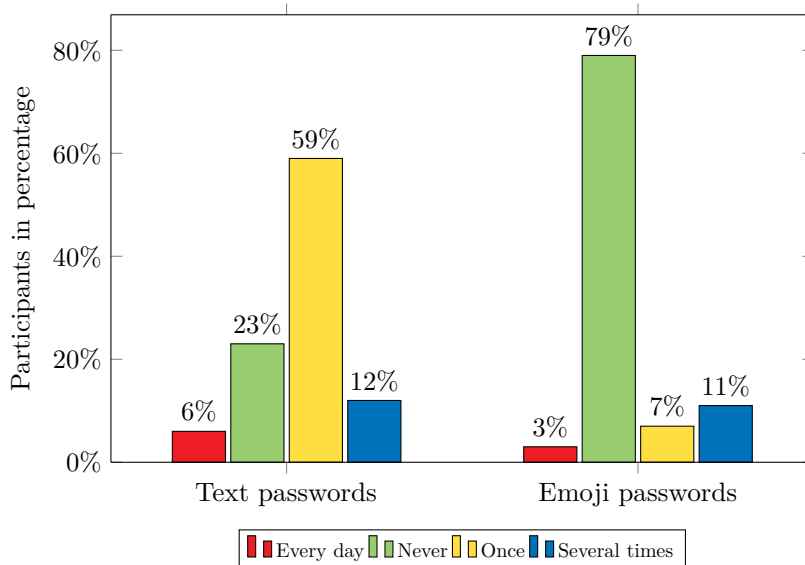


Figure 6.23: The distribution of time spent thinking of password, based on password type.

you would perhaps expect the participants with text passwords to perform better. However, 91% (20/22) of the participants who never thought about their emoji passwords remembered them, while only 40% (4/10) of the participants who thought about their text passwords once did so. These results support the view that emoji passwords created with EmojiStory are easy to remember.

6.3.4 Scheme Efficiency

Due to technical errors in the follow-up survey, we could neither use the measured times for the login nor the password creation process. The consequence of the errors was that the timestamps were captured too late, making the measured times too high.

We expected the average time needed to authenticate after a week without using the password, to be significantly higher than the login times from the initial survey (presented in Section 6.2.4). Of course we are not able to confirm this because of the incorrect data. Still, we would like to mention that the results indicate that the participants spent more time on authentication after about seven days. Most participants seem to have needed 10-25 seconds to log in.

6.3.5 Memorization Strategy

Once again, we asked the participants how they remembered their password, but this time we asked them twice. One time was right after they logged in the first time. The other time was about a week later, after they tried to log in one last time.

Figure 6.24 shows the results for those who were using emoji passwords. For both logins, around half of the participants remembered their passwords by using a combination of story and emojis. This again indicates that the story contributes positively to the memorization of the emoji password. Yet, it could seem like it might be challenging to remember the story over a longer period of time. Figure 6.24 show that some of the participants seem to have forgot their stories while waiting for an invitation to the second part of the survey, and only remembered what the emojis looked like.

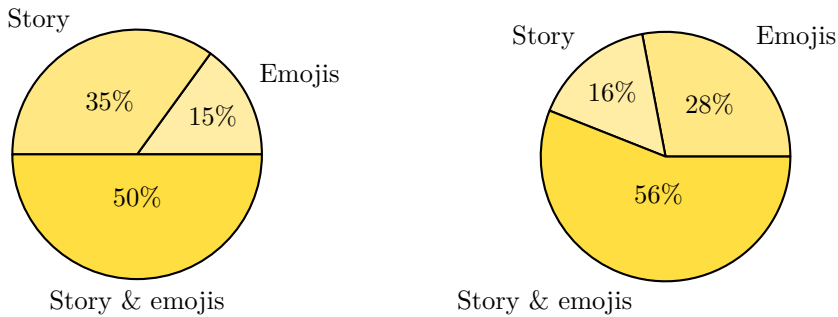


Figure 6.24: The distribution of the memorization strategy used by participants with emoji passwords after first login (left) and third login (right).

6.3.6 Selection Strategy

Based on the results from the follow-up survey, the participants said they used four different password selection strategies when using EmojiStory. They are briefly explained in the list below.

- **Personal:** Selection of words that have personal meaning.
- **Best fitting:** Words are selected based on how well they fit into the story.
- **Crazy:** A strategy involving selection of unsuitable words in order to create a crazy story.
- **Random:** Words are selected randomly.

The distribution of the different strategies can be seen in Figure 6.25. The figure also includes the amount of participants who said that they used a different selection strategy. We find it surprising that most participants (17) said they used the *random*

6. RESULTS AND DISCUSSION

strategy. When looking at password distributions of people who said they selected the emojis at random, there is still considerable bias. Consequently, we believe it is very unlikely that this group selected their passwords truly at random.

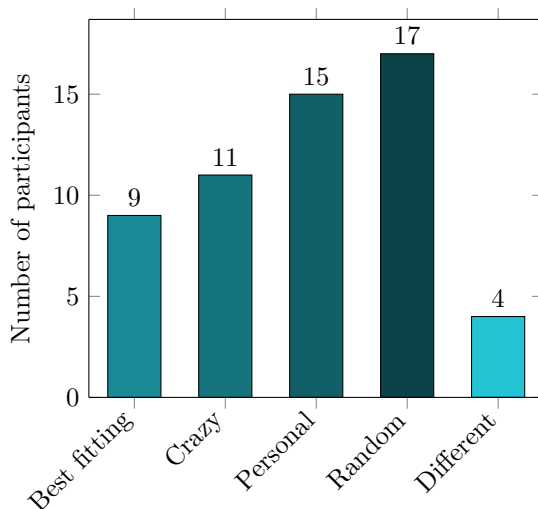


Figure 6.25: Frequencies of password selection strategies.

Although the participants used different selection strategies this is not shown in their passwords. Surely there are some examples of passwords that could reflect the use of selection strategies (see Figure 6.26), but we were not able to identify any patterns based on them. It is likely that there is less opportunity for using a selection strategy due to the random and restrictive nature of EmojiStory.

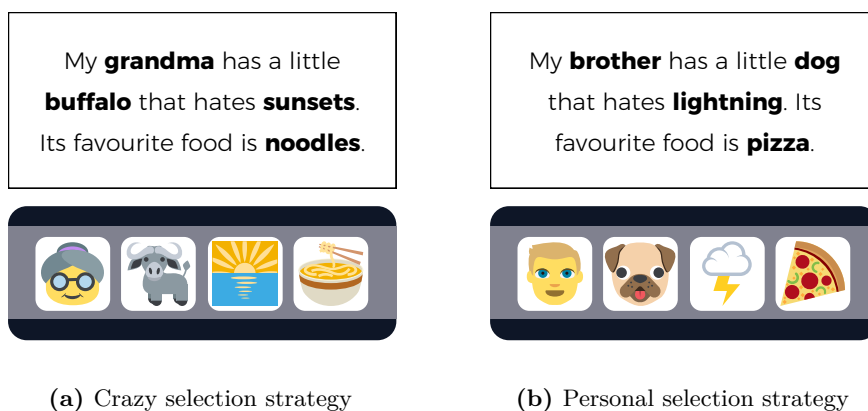


Figure 6.26: An illustration of how distinct two passwords created with different selection strategies can be.

Yet it is possible that the lack of identifiable patterns is due to the limited sample. Especially considering that we were able to find some selection patterns based on how participants described their stories in the initial survey (see Section 6.2.7). However, the results indicate that the practical password space of EmojiStory is not negatively affected by selection strategies. This is a good thing because it leads to better security, but it probably also leads to lower memorability.

As mentioned in Section 6.2.7, the choice of selection strategy is likely to be affected by the type of story that is used. Since only one story was used in the follow-up survey, it is possible that the distribution of selection strategies would be different if another story had been used.

Chapter 7

Conclusion and Future Work

This project explored ways of using emojis to improve user authentication by comparing emojis passwords to PIN entry and text passwords. The first research question asked what the current state of emoji-based authentication looks like. We found that little research has been done in the field of emoji-based authentication so far. Among the few studies that exist, some schemes facilitating the use of emojis passwords have been proposed and evaluated. However, they focus primarily on replacing PIN entry and do not compare emoji passwords to text passwords. Furthermore, none of these solutions are used in any software product to date.

The second research question in this project asked how a novel password scheme based on emojis can be designed. We have demonstrated this by developing a prototype called EmojiStory. Based on existing research, we identified several shortcomings of emoji-based authentication. From this knowledge, we have systematically defined the requirements and the intended application of the scheme. In an attempt to meet these requirements, we have come up with a novel way of creating passwords using stories and emojis.

The conducted experiments revealed that usability and security are interdependent. Increasing the security of a password scheme has a negative impact on usability. The random generation of emojis on the keyboard, for example, reduces the formation of spatial patterns, but may also complicate memorization of the password. All security-related decisions consequently affect usability as well. This must be taken into account when creating a novel password scheme.

Our third research question asked if emoji passwords can provide satisfactory security and usability. Findings from two surveys indicate that EmojiStory can offer good usability. The password creation and login time are short, and a positive user experience is provided. Our research also shows that emoji passwords are easier to remember than text passwords. Yet we were not able to conclude that EmojiStory offers high memorability since this is a difficult attribute to measure, particularly

7. CONCLUSION AND FUTURE WORK

with respect to long-term memory. Therefore, we advise further research on the memorability of emoji passwords.

In order to use emojis for web authentication, it must be possible to enter them efficiently. In this project we have demonstrated that this cannot be achieved without sacrificing some security or usability. Still, in its ultimate form, the EmojiStory scheme could be used as an alternative to text passwords and offer passwords that are more secure, but probably less usable.

The results from this study also suggest that emoji passwords can provide higher security than PIN codes. EmojiStory offers a larger theoretical password space which can be expanded by adding more emoji characters to the keyboard. Also, EmojiStory's practical password space is positively influenced by preventing the use of spatial patterns. However, we found significant bias in the emoji passwords. Although preventive measures were taken to address this problem, users still preferred certain emojis. Further research is needed to compare the observed bias with that of other authentication systems.

7.1 Future Work

This section proposes several modifications to the scheme and new ideas that can be subject to further research.

7.1.1 Increasing the Keyboard Size and Password Length

All keyboards generated in EmojiStory contain a total of 12 characters (i.e. emojis). This can be traced back to the number of keyword categories and the desire to fit them into all types of screen sizes. Nevertheless, it would be interesting to conduct experiments to examine the impact of an increased number of characters on the keyboard. This modification could lead to a reduction in usability, but would possibly contribute to hinder guessing attacks and thus improve the security of the scheme as well.

The same applies to the emoji passwords. A password containing five or six instead of four characters undoubtedly expands the theoretical password space. On the other hand, this probably has a negative effect on memorability, as it should be more difficult to remember longer passwords.

7.1.2 Testing the Memorability of Multiple Emoji Passwords

In this project, only the memorability of a single emoji password was analyzed. In the real world, people own multiple passwords (at least they should) which are used

in various applications. Therefore, it might be of interest to study how many emoji passwords a person can remember over a longer period of time.

7.1.3 Creating Stories Using Artificial Intelligence

The five stories used in our prototype of EmojiStory are definitely not enough to provide adequate security. Unfortunately, creating these stories by hand was very time-consuming. In recent years, artificial intelligence has gained a lot of attention and is now more accessible. It might be possible to use this kind of technology to automatically generate dozens of different stories.

7.1.4 Generating Emoji Passwords Based on Stories

In EmojiStory, users have no control over what story they are given. Yet they choose the different keywords that form their passwords. This method could be turned upside down. Instead of letting the user decide on the result (i.e. the password characters) of this process, the password could be created automatically from a sentence entered by the user. With help from natural language processing and sentiment analysis, this story could be translated into an emoji representation.

7.1.5 Further Exploration of the Practical Password Space

As mentioned in Section 6.2.7, the data collected in the survey is insufficient to assess the practical password space of EmojiStory. For instance, the fact that the keyword categories contained different amount of emojis distorted our results. For this reason, more work should be devoted to the research of the practical password space and how it can be increased.

7.1.6 Applying Guessing Attacks

This thesis only statistically evaluated the security of EmojiStory, but does not test whether the findings also apply in practice. Consequently, it might be interesting to investigate how resistant EmojiStory is to automated guessing attacks such as brute-force or dictionary attacks.

References

- [1] Anupam Das et al. «The Tangled Web of Password Reuse.» In: *NDSS*. Vol. 14. 2014, pp. 23–26.
- [2] Joseph Bonneau et al. *The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes*. Tech. rep. UCAM-CL-TR-817. University of Cambridge, Computer Laboratory, Mar. 2012. URL: <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf>.
- [3] Oxford Dictionaries. *Word of the Year 2015*. <https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2015>. Last accessed: 05.11.2017.
- [4] Petra Kralj Novak et al. «Sentiment of emojis». In: *PLOS One* 10.12 (2015), e0144296.
- [5] Unicode. *Full Emoji List, v5.0*. <https://unicode.org/emoji/charts/full-emoji-list.html>. Last accessed: 03.11.2017.
- [6] George A Miller. «The magical number seven, plus or minus two: Some limits on our capacity for processing information.» In: *Psychological Review* 63.2 (1956), pp. 81–97.
- [7] The Unicode Consortium. *Submitting Emoji Proposals: Evidence of Frequency*. <http://unicode.org/emoji/selection.html#frequency-evidence>. Last accessed: 27.05.2018.
- [8] Intelligent Environments. *Now you can log into your bank using emoji*. <https://www.intelligentenvironments.com/now-you-can-log-into-your-bank-using-emoji/>. Last accessed: 25.10.2017.
- [9] Maximilian Golla, Dennis Detering, and Markus Dürmuth. «EmojiAuth: quantifying the security of emoji-based authentication». In: *Proceedings of the Usable Security Mini Conference (USEC)*. 2017.
- [10] Lydia Kraus et al. «On the Use of Emojis in Mobile Authentication». In: *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer. 2017, pp. 265–280.
- [11] Briony J. Oates. *Researching information systems and computing*. London: Sage Publications, 2006. ISBN: 9781412902236.

REFERENCES

- [12] ACM. *ACM Digital Library*. <https://dl.acm.org/>. Last accessed: 02.11.2017.
- [13] LLC. Google. *Google Scholar*. <https://scholar.google.com/>. Last accessed: 02.11.2017.
- [14] IEEE. *IEEE Xplore Digital Library*. <http://ieeexplore.ieee.org/Xplore/home.jsp>. Last accessed: 02.11.2017.
- [15] Springer. *Springer Digital Library*. <http://www.springer.com/>. Last accessed: 02.11.2017.
- [16] Christoph Kern, Anita Kesavan, and Neil Daswani. *Foundations of Security: What Every Programmer Needs to Know*. Berkeley, CA: Apress, 2007. ISBN: 9781430203773. DOI: 10.1007/978-1-4302-0377-3.
- [17] William Stallings. *Cryptography and Network Security : Principle and Practice*. Boston, MA: Pearson Education, 2013. ISBN: 9780133354690.
- [18] Dipankar Dasgupta, Arunava Roy, and Abhijit Nag. «Multi-Factor Authentication». In: *Advances in User Authentication*. Springer, 2017, pp. 185–233. ISBN: 9783319588087. DOI: 10.1007/978-3-319-58808-7_5.
- [19] Dinei Florencio and Cormac Herley. «A Large-scale Study of Web Password Habits». In: *Proceedings of the 16th International Conference on World Wide Web*. WWW '07. Banff, Alberta, Canada: ACM, 2007, pp. 657–666. ISBN: 978-1-59593-654-7. DOI: 10.1145/1242572.1242661. URL: <http://doi.acm.org/10.1145/1242572.1242661>.
- [20] Saranga Komanduri et al. «Of passwords and people: measuring the effect of password-composition policies». In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2011, pp. 2595–2604.
- [21] Richard Shay et al. «Encountering stronger password requirements: user attitudes and behaviors». In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM. 2010, p. 2.
- [22] Blake Ives, Kenneth R Walsh, and Helmut Schneider. «The domino effect of password reuse». In: *Communications of the ACM* 47.4 (2004), pp. 75–78.
- [23] Yinqian Zhang, Fabian Monrose, and Michael K Reiter. «The security of modern password expiration: An algorithmic framework and empirical analysis». In: *Proceedings of the 17th ACM conference on Computer and communications security*. ACM. 2010, pp. 176–186.
- [24] William Melicher et al. «Usability and security of text passwords on mobile devices». In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM. 2016, pp. 527–539.
- [25] Patti Bao et al. «Smart phone use by non-mobile business users». In: *Proceedings of the 13th international conference on human computer interaction with mobile devices and services*. ACM. 2011, pp. 445–454.

- [26] Google, LLC. *What are extensions?* <https://developer.chrome.com/extensions>. Last accessed: 08.05.2018.
- [27] Lionel Standing, Jerry Conezio, and Ralph Norman Haber. «Perception and memory for pictures: Single-trial learning of 2500 visual stimuli». In: *Psychonomic Science* 19.2 (1970), pp. 73–74.
- [28] A Paivio. «Imagery and verbal processes. Holt, Reinhart, and Winston. [WMP, aZWP] (1975) Perceptual comparisons through the minds eye». In: *Memory and Cognition* (1971).
- [29] Brandon A Ally, Carl A Gold, and Andrew E Budson. «The picture superiority effect in patients with Alzheimer’s disease and mild cognitive impairment». In: *Neuropsychologia* 47.2 (2009), pp. 595–598.
- [30] Allan Paivio and Kalman Csapo. «Picture superiority in free recall: Imagery or dual coding?» In: *Cognitive psychology* 5.2 (1973), pp. 176–206.
- [31] Raymond S Nickerson. «Short-term memory for complex meaningful visual configurations: A demonstration of capacity.» In: *Canadian Journal of Psychology/Revue canadienne de psychologie* 19.2 (1965), p. 155.
- [32] Roger N Shepard. «Recognition memory for words, sentences, and pictures». In: *Journal of Verbal Learning and Verbal Behavior* 6.1 (1967), pp. 156–163.
- [33] Greg E Blonder. *Graphical password*. US Patent 5,559,961. 1996.
- [34] Susan Wiedenbeck et al. «Authentication using graphical passwords: Effects of tolerance and image choice». In: *Proceedings of the 2005 symposium on Usable privacy and security*. ACM. 2005, pp. 1–12.
- [35] Pointsec Mobile Technologies. *Pointsec for Smartphone*. https://hk.nec.com/en_HK/pdf/solutions/DLFE-1314.pdf. Last accessed: 04.05.2018.
- [36] Passfaces Corporation. *Passfaces*. <http://www.realuser.com/>. Last accessed: 07.05.2018.
- [37] Passfaces Corporation. *About Passfaces*. http://realuser.com/enterprise/about/about_passfaces.htm. Last accessed: 07.05.2018.
- [38] Darren Davis, Fabian Monroe, and Michael K Reiter. «On User Choice in Graphical Password Schemes». In: *USENIX Security Symposium*. Vol. 13. 2004, pp. 11–11.
- [39] Sacha Brostoff and M Angela Sasse. «Are Passfaces more usable than passwords? A field trial investigation». In: *People and Computers XIV—Usability or Else!* Springer, 2000, pp. 405–424.
- [40] Encyclopædia Britannica, Inc. *Android*. <https://www.britannica.com/technology/Android-operating-system>. Last accessed: 07.05.2018.

REFERENCES

- [41] Sebastian Uellenbeck et al. «Quantifying the security of graphical passwords: the case of android unlock patterns». In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM. 2013, pp. 161–172.
- [42] Susan Wiedenbeck et al. «PassPoints: Design and longitudinal evaluation of a graphical password system». In: *International Journal of Human-Computer Studies* 63.1-2 (2005), pp. 102–127.
- [43] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. «Graphical passwords: Learning from the first twelve years». In: *ACM Computing Surveys (CSUR)* 44.4 (2012), p. 19.
- [44] Florian Schaub et al. «Exploring the design space of graphical passwords on smartphones». In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM. 2013, p. 11.
- [45] Deholo Nali and Julie Thorpe. «Analyzing user choice in graphical passwords». In: *School of Computer Science, Carleton University, Tech. Rep. TR-04-01* (2004).
- [46] SP NIST. «800-63-2–Electronic Authentication Guideline». In: *National Institute of Standards and Technology* (2013).
- [47] Paul A Grassi et al. «NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management». In: *Bericht, NIST* (2017).
- [48] Cambridge Dictionary. *emoji*. <https://dictionary.cambridge.org/dictionary/english/emoji>. Last accessed: 24.04.2018.
- [49] The Unicode Consortium. *FAQ – Emoji and Pictographs*. http://www.unicode.org/faq/emoji_dingbats.html. Last accessed: 24.04.2018.
- [50] Oxford Dictionary. *emoji*. <https://en.oxforddictionaries.com/definition/emoji>. Last accessed: 24.04.2018.
- [51] M Davis and P Edberg. *Unicode Emoji: Unicode Technical Standard# 51*. Tech. rep. Technical Standard 51 (5), 2017.
- [52] The Unicode Consortium. *About the Unicode Standard*. <https://www.unicode.org/standard/standard.html>. Last accessed: 24.04.2018.
- [53] The Unicode Consortium. *Basic Questions*. http://www.unicode.org/faq/basic_q.html. Last accessed: 25.04.2018.
- [54] Instagram Engineering. *Emojineering Part 1: Machine Learning for Emoji Trends*. <https://instagram-engineering.com/emojineering-part-1-machine-learning-for-emoji-trendsmachine-learning-for-emoji-trends-7f5f9cb979ad>. Last accessed: 25.04.2018.

- [55] Xuan Lu et al. «Learning from the ubiquitous language: an empirical analysis of emoji usage of smartphone users». In: *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM. 2016, pp. 770–780.
- [56] Matthew Rothenberg. *emojitracker*. <http://www.emojitracker.com/>. Last accessed: 25.04.2018.
- [57] Emoji+, LLC. *Emoji Stats*. <http://emojistats.org/>. Last accessed: 30.04.2018.
- [58] Lydia Kraus et al. «Implications of the Use of Emojis in Mobile Authentication». In: *Who are you?! Adventures in Authentication Workshop*. USENIX Association. 2016.
- [59] Kemal Bicakci et al. «Towards usable solutions to graphical password hotspot problem». In: *Computer Software and Applications Conference, 2009. COMP-SAC'09. 33rd Annual IEEE International*. Vol. 2. IEEE. 2009, pp. 318–323.
- [60] Susan Wiedenbeck et al. «Design and evaluation of a shoulder-surfing resistant graphical password scheme». In: *Proceedings of the working conference on Advanced visual interfaces*. ACM. 2006, pp. 177–184.
- [61] Tobias Seitz, Florian Mathis, and Heinrich Hussmann. «The Bird is the Word: A Usability Evaluation of Emojis inside Text Passwords». In: *Proceedings of the 29th Australian Conference on Computer-Human Interaction*. ACM. 2017, pp. 10–20.
- [62] Jeff Yan et al. «Password Memorability and Security: Empirical Results». In: *IEEE Security and Privacy* 2.5 (Sept. 2004), pp. 25–31. ISSN: 1540-7993. DOI: 10.1109/MSP.2004.81. URL: <https://doi.org/10.1109/MSP.2004.81>.
- [63] Cambridge Dictionary. *qwerty*. <https://dictionary.cambridge.org/dictionary/english/qwerty>. Last accessed: 15.05.2018.
- [64] Erik Dahlström et al. «Scalable vector graphics (svg) 1.1». In: *World Wide Web Consortium Recommendation* 16 (2011).
- [65] Cambridge Dictionary. *mnemonic*. <https://dictionary.cambridge.org/dictionary/english/mnemonic>. Last accessed: 21.05.2018.
- [66] Richard Shay et al. «Can long passwords be secure and usable?» In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2014, pp. 2927–2936.
- [67] Colin Robson. *Real world research*. 2nd ed. Malden, MA: Blackwell Publishing, 2002.
- [68] Robert V Krejcie and Daryle W Morgan. «Determining sample size for research activities». In: *Educational and Psychological Measurement* 30.3 (1970), pp. 607–610.

REFERENCES

- [69] Creative Research Systems. *Sample Size Calculator*. <https://www.surveysystem.com/sscalc.htm>. Last accessed: 15.05.2018.
- [70] Mirta Galesic and Michael Bosnjak. «Effects of questionnaire length on participation and indicators of response quality in a web survey». In: *Public Opinion Quarterly* 73.2 (2009), pp. 349–360.
- [71] NSD. *Information and consent*. http://www.nsd.uib.no/personvernombud/en/help/information_consent/. Last accessed: 20.05.2018.
- [72] Centre for Social Development et al. *The World's Women...: Trends and Statistics*. United Nations, 2010.
- [73] NSD. *Personvernombudet for forskning*. <http://www.nsd.uib.no/personvern/>. Last accessed: 25.10.2017.
- [74] E.B. Goldstein. *Cognitive Psychology: Connecting Mind, Research and Everyday Experience*. Wadsworth Publishing, Jan. 2005, pp. 150–161.
- [75] Sonia Chiasson, Robert Biddle, and Paul C van Oorschot. «A second look at the usability of click-based graphical passwords». In: *Proceedings of the 3rd symposium on Usable privacy and security*. ACM. 2007, pp. 1–12.
- [76] Daphna Weinshall. «Cognitive authentication schemes safe against spyware». In: *Security and Privacy, 2006 IEEE Symposium on Security and Privacy*. IEEE. 2006.
- [77] Florian Schaub, Ruben Deyhle, and Michael Weber. «Password entry usability and shoulder surfing susceptibility on different smartphone platforms». In: *Proceedings of the 11th international conference on mobile and ubiquitous multimedia*. ACM. 2012, p. 13.
- [78] ISO 9241-11:1998. *Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)–Part II Guidance on Usability*. Standard. International Organization for Standardization, 1998.
- [79] Arnold M Lund. «Measuring usability with the USE questionnaire». In: *Usability interface 8.2* (2001), pp. 3–6.
- [80] Joseph Bonneau, Sören Preibusch, and Ross Anderson. «A birthday present every eleven wallets? The security of customer-chosen banking PINs». In: *International Conference on Financial Cryptography and Data Security*. Springer. 2012, pp. 25–40.
- [81] Ronald Aylmer Fisher, Frank Yates, et al. *Statistical tables for biological, agricultural and medical research*. 3rd ed. Oliver and Boyd, Edinburgh, 1963.
- [82] Matt Weir et al. «Testing metrics for password creation policies by attacking large sets of revealed passwords». In: *Proceedings of the 17th ACM conference on Computer and communications security*. ACM. 2010, pp. 162–175.

REFERENCES

- [83] Lee R Dice. «Measures of the amount of ecologic association between species». In: *Ecology* 26.3 (1945), pp. 297–302.