On the Use of Emojis in Mobile Authentication

Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, Sebastian Möller

On the Use of Emojis in Mobile Authentication

Lydia Kraus[1] ✉, Robert Schmidt[1], Marcel Walch[2] ✉, Florian Schaub[3], and Sebastian Möller[1]

[1] Quality and Usability Lab, Technische Universität Berlin, Germany
lydia.kraus@qu.tu-berlin.de, mail@robschmidt.de,
sebastian.moeller@tu-berlin.de
[2] Institute of Media Informatics, Ulm University, Germany
marcel.walch@uni-ulm.de
[3] School of Information, University of Michigan, USA
fschaub@umich.edu

Abstract. Mobile authentication methods protect smartphones from unauthorized access, but also require users to remember and frequently enter PINs, passwords, or graphical patterns. We propose the EmojiAuth scheme with which we study the effects of Emoji use on the usability and user experience of mobile authentication. We conducted two between-subjects studies (lab study: n=53; field study: n=41) comparing EmojiAuth to standard PIN entry. We find that EmojiAuth provides good memorability for short passwords and reasonable memorability for longer passwords. Moreover, we identify diverse Emoji-password selection strategies and provide insights on the practical security of Emoji-based mobile authentication. Our results suggest that Emoji-based authentication constitutes a practical alternative to traditional PIN authentication.

Keywords: Mobile authentication, Security, Usability, User experience, Emoji.

1 Introduction

Usability of mobile authentication is an active research topic [1,2,3], given that users spend a considerable amount of time unlocking their phones [2]. Knowledge-based authentication mechanisms, such as PIN and unlock pattern (on Android), have been widely deployed for smartphone locking; alphanumerical passwords are also a common option. While PINs, especially 4-digit PINs, are susceptible to user choice [4] and shoulder surfing [5], they balance short log-in time and good memorability with sufficient protection against casual attackers [5]. Biometric authentication, such as fingerprint and face recognition emerged recently as alternatives, but still rely on knowledge-based authentication as a fallback [6]. Therefore, knowledge-based authentication remains relevant for smartphones and is unlikely to be replaced soon. However, if users need to spend mental effort and time to protect their smartphone, the required interactions should be as pleasant and positive as possible.

Designing positive interactions has gained considerable attention in user experience research. Concepts such as hedonic (product) qualities, joy of use, and stimulation evolved as important aspects of user experience design [7]. We argue that considering positive interaction aspects is also relevant in the design of usable security mechanisms.

An interesting direction for positive interaction in mobile authentication is the use of Emojis as password characters. Emojis are largely used in positive contexts [8] and are popular among users. Thus, providing potential for offering positive user experiences. Emoji-based passwords have recently been introduced by a commercial application [9].

In this paper, we study opportunities of Emojis for creating a positive mobile authentication experience. We further study how Emoji-based authentication influences password selection and shoulder surfing. To gather insights, we developed an Emoji-based authentication scheme (EmojiAuth) and evaluated it in a lab study (n=53) and a field study (n=41), including a shoulder-surfing experiment (n=38). Our contributions include (1) the identification of five main Emoji-password selection strategies; (2) a comparative evaluation of PIN- and Emoji-based passwords regarding their susceptibility to shoulder surfing, indicating a slight improvement with Emojis; and (3) an analysis of the user experience of Emoji-based passwords. While Emoji and PIN show similarly high usability, users indicated that they would prefer Emoji over PIN as a screen lock.

2 Related Work

Mobile authentication has received considerable research attention [1,2,3,10]. A multinational survey showed that 50.4% (Italy) to 76.4% (UK) of users use a screen lock on their phone [10]. Authentication schemes can be divided into knowledge-based, token-based, and biometric schemes [11]. The Emoji-based password scheme belongs to the class of graphical authentication schemes which is a subclass of knowledge-based authentication. In the following we detail related work on these two areas.

PINs and passwords are commonly deployed knowledge-based authentication schemes. While PINs can be entered quickly and accurately [5,3], they lack entropy. With a 4-digit PIN the password space is constrained to about 14 bit. Users tend to weaken PINs by choosing easy-to-remember numbers, e.g., birth dates [4]. Random passwords are more secure but harder to remember [12]. PINs generated under a security policy are more secure, but also harder to remember than freely-chosen PINs [13].

Graphical authentication schemes are motivated by the fact that graphics are easier to remember than alphanumeric passwords [14]. As for PINs and passwords, major issues of graphical passwords arise from the susceptibility to capture and guessing attacks [14]. For instance, image-based cued-recall schemes are prone to hotspots [14], i.e., image regions users are likely to select, which can be used in guessing attacks. Graphical passwords can also take longer to enter. A study with Android pattern unlock found that participants needed twice as long to enter a pattern and made more mistakes compared to a PIN [3]. Yet, users tend to rate pattern usability and likability similar to PIN, likely due to easy error recovery [3]. However, to be practical, a login attempt should not take longer than for a PIN or a pattern lock mechanism [2]. Patterns have a smaller theoretical password space as PINs and their security is considered low in general [15].

Icon-based graphical authentication schemes are a promising approach enabling fast log-in times [5], while potentially providing a theoretical password space similar to PIN or larger. The Story scheme [16] is somewhat similar to our proposed Emoji-based scheme as users create a password from a 3x3 set of photo icons from different

categories (objects, food, people). An interesting finding is that Story did not result in a skewed password probability distribution [16]. Emoji-based authentication has been recently suggested [9]. Shortly after our lab study was conducted, Golla et al. conducted an online study to investigate the susceptibility of Emoji-based passwords to guessing attacks [17]. Their Emoji-based authentication scheme features a keyboard with 20 Emojis. With their scheme, they found that the distribution of Emoji-passwords is skewed, but 4-digit user-chosen Emoji-passwords were still more resistant to guessing attacks than 4-digit user-chosen PINs.

User experience and authentication should be considered together. To create a positive user experience, psychological needs, such as stimulation and popularity, should be addressed in the interaction design of mobile authentication mechanisms [18]. Also, while mobile and graphical authentication schemes have been investigated intensively in terms of usability and security, user experience evaluations beyond usability, have received little attention [19].

While Emojis have been used in authentication, we are the first to study usability and user experience of an Emoji-based scheme in the lab and in the wild, as well as its resistance to shoulder-surfing attacks.

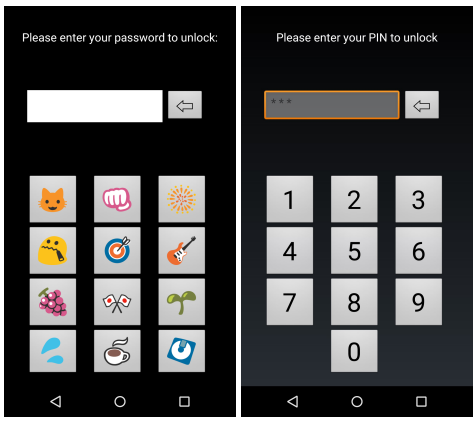
3 EmojiAuth: Emoji-based Authentication Scheme

The use of Emojis may lead to a positive and pleasing user experience and positive perception of EmojiAuth: Emojis have been shown to enable the expression of moods, emotions and nuances in written text [20]. Thus, Emojis may also make authentication more (personally) meaningful for users. Emojis further have positive associations which may lead to authentication being perceived positively as well. The most frequently used Emojis are rated significantly more positive than the remaining Emojis [8].

Similar to PIN entry, our EmojiAuth scheme features twelve buttons (cf. Figure 1(a)). We further designed a PIN lock as a baseline comparison (cf. Figure 1(b)). In both schemes, if users enter their password correctly, the entry field turns green and the screen unlocks automatically. If the password is incorrect, the phone vibrates and a respective message appears above the entry field. The use of a keyboard with twelve Emoji buttons is grounded in the advantages of PIN keyboards: PIN entry is easy and fast [3]. Simple keyboards have further been linked to authentication usability [21].

In EmojiAuth's keyboard generation, three Emojis are randomly selected from each of four categories (Person and Face: 226 Emojis, Object: 287 Emojis, Nature: 204 Emojis, and Activity: 44 Emojis) to support easy assembly of passwords. Once a user-specific keyboard has been initialized, the Emojis and their position remain static to reduce search time and thus enable shorter login times [5,22].

The theoretical password space of EmojiAuth is more than two times larger than the password space of PINs for 4-digit passwords (EmojiAuth: 20,736; PIN: 10,000), and almost three times larger than PIN for 6-digit passwords (EmojiAuth: 2,985,984; PIN: 1,000,000). However, that users favor certain Emojis is evident from rankings of currently popular Emojis [23] and has been also shown as an issue in related work on Emoji-based authentication [17]. To mitigate the issue of hotspot Emojis, EmojiAuth generates an individual keyboard for each user during password enrollment. Keyboards



(a) EmojiAuth (b) PIN

Fig. 1. EmojiAuth and PIN user interfaces. The original UIs were in German. Emojis are depicted in the Noto Emoji Font by Google Inc. `https://github.com/googlei18n/noto-emoji`.

generated from a large set of Emojis may increase the practical password space as specific Emojis have low probability to appear on individual keyboards, thus decreasing the probability that certain Emojis are favored across the whole user population.

We conducted a lab study and a field study, both between subjects, to evaluate EmojiAuth (treatment) in comparison to PIN entry (control). In the lab study, we evaluated memorability, selection strategies, and user experience of Emoji-passwords. In the field study, we validated our findings in the wild. We further conducted a shoulder-surfing experiment at the end of the field study.

4 Lab Study

4.1 Methodology and Procedure

In the lab study, the Emoji and PIN conditions were further divided into two subgroups to investigate effects of varying password length (4 and 6 digits). Groups are subsequently referred to as Emoji-4, Emoji-6, PIN-4 and PIN-6. The lab study was conducted in two sessions. The first session started with participants signing the consent form and completing an entry questionnaire on demographics and smartphone use. They were informed that passwords they create in the study will be stored in plain text to enable scientific analysis, but will not be linked to their identity. Participants were then assigned round-robin to an Emoji or PIN group. Participants who currently used a PIN (or fingerprint and PIN combination) on their smartphone were assigned to the Emoji group, in order to reduce the impact of prior habituation to PIN entry.

After a training task with randomly generated passwords, participants were asked to choose their own password and instructed that they will have to remember it. After creating their password, they had to enter it three times with a mental rotation task (MRT)

between attempts. The MRTs served to distract participants and clear their short-term memory between login attempts [24,5]. Participants then completed a usability and user experience questionnaire (AttrakDiff 2 mini [25]) and a five-minute semi-structured interview, in which they were asked to describe how they selected their password and their level of confidence in remembering their password. AttrakDiff 2 mini measures different aspects of user experience [25,26]: pragmatic quality (PQ), hedonic quality (HQ), and attractiveness (ATT). Each dimension is measured on a semantic differential with 7 rating levels between differentials. Pragmatic quality is related to usability, i.e., functional aspects of a product [27]. Hedonic Quality (HQ) relates to the capability of a product to address aspects of *personal relevance* [27, p. 38]. The hedonic quality scale is further divided into the sub-dimensions *Stimulation* and *Identity* [26]. Stimulation refers to a products' capability to provide stimulating experiences (e.g. in terms of providing *new impressions, opportunities, insights*), whereas identity refers to a products' capability to communicate identity [27, p. 35]. Attractiveness is related to the overall judgment of a product [26].

One week after the first session, participants returned to the lab for the second session. Participants had to enter the password they created in the first session and completed the same usability and UX questionnaire. They were also asked in a short interview how they memorized their password and whether they had written it down. All participants conducted the study on the same smartphone (LG Nexus 5, Android 5.1.1). The interviews were recorded and transcribed verbatim for further analysis. Participants received 4€ compensation for the first study session, and 8€ for the second one in order to incentivize participants to return and thus reduce drop-outs. Participants were recruited through a participant panel of TU Berlin, classified ads posted on an online service similar to Craigslist, flyers, and e-mail.

4.2 Results

In total, 53 smartphone users participated in the lab study: 14 in the Emoji-4 group, 13 in each of the other three groups. Participants were 18 to 70 years old (M=31, $Mdn.$=27); 28 were male, 25 female. The average time between sessions was 7 days (SD=1.2 days; range 3-12 days due to scheduling). Over half the participants were students (58.5%), despite not targeting campus populations. Other participants were employees (15.1%), self-employed (7.5%), retired (5.7%), and others (13.2%). Most (75.5%) did not have a professional or educational IT background. In the sample were 69.8% Android users, 22.6% iOS users, and 7.6% other smartphone users. Most participants (69.8%) reported to use authentication on their phone; most common were PIN (28.3%), unlock pattern (22.6%), and fingerprint with PIN as fallback (11.3%).

Password memorability The lab study results indicate high memorability of both EmojiAuth passwords and PINs. After one week all participants (EmojiAuth and PIN) were able to successfully authenticate within three attempts. Long Emoji-passwords seem to be slightly harder to remember after a week of non-use, as a lower number of participants managed to enter their password correctly for all three trials in week 2 (Emoji-4: 92.9% in both weeks; Emoji-6: 100% in week 1 and 69.2% in week 2; PIN-4:

100% in both weeks; PIN-6: 100% in week 1 and 92.3% in week 2). A Fisher's exact test did not reveal statistically significant differences between groups. Only four PIN participants reported writing down their passwords after the first session.

Password selection Interviews on password selection strategies were first coded openly by one coder, who created separate code books for Emoji and PIN with some overlapping codes. Two coders then independently re-coded all interviews with the code books. Multiple codes could be assigned. Interrater agreement was high for both groups (Emoji: Cohen's κ=.83; PIN: κ=.72). Coders subsequently reconciled the remaining cases. Participants in the PIN group relied on predictable password selection strategies, e.g., birth dates as PIN [4]. The selection strategies of the Emoji participants overlapped only partially with the PIN strategies. Emoji participants often selected passwords based on a preference for certain Emojis and remembered them by creating stories, memorizing spatial patterns or repeating characters. We identified five main password selection strategies each for Emoji passwords and PINs (frequencies are provided in Table 1):

- **Emoji preference (Emoji):** Emojis are selected based on personal preference, e.g., "Well I clicked those Emojis I was interested in" (P33).
- **Association & story (Emoji):** Participants leverage an association between Emojis and their own knowledge or experience, and/or a password is selected or memorized by creating a story connecting the Emojis, e.g., "[I selected the password] after a song. [...] each Emoji stands for one word and depending on the song which words came first, I typed [the Emojis] in." (P22); "I just thought about the weekend [laughing]" (P3).
- **Pattern & position (Emoji):** A spatial pattern is used to create or remember the password and/or the position on the keyboard is used to remember certain Emojis, e.g., "And then I went from the upper left down to the bottom right" (P16).
- **Repetition & similarity (Emoji):** Either single characters or character sequences are repeated to create a password and/or a password is assembled from Emojis which are (subjectively) similar to each other, e.g., "[I chose the password so] that the pictures look similar" (P39).
- **Color & Shape (Emoji):** A Password is selected based on color or shape of Emojis, e.g., "Well... first I chose four symbols with the same color." (P16); "I chose [the Emojis] according to circular shape" (P18).
- **Date (PIN):** A date of personal importance (birthday, anniversary, etc.) is used to create a PIN.
- **Repetition & sequence (PIN):** Single numbers or number sequences are repeated to create a PIN and/or a PIN is created with consecutive numbers.
- **Re-use (PIN):** A PIN is selected by re-using a current or former PIN.
- **Pattern & position (PIN):** A spatial pattern is used to create or remember the PIN and/or the keyboard position is used to remember certain numbers.
- **Association (PIN):** An association between numbers and the user's knowledge or experience is used to select the password (e.g., choosing a name that contains a number or a phone number as PIN).

The PIN selection strategies are consistent with findings in related work. For instance, dates as PINs or parts of passwords are commonly observed [4,28] and were also

the most frequent selection strategy in our study. We further observed spatial patterns as PIN selection strategies, which are known user strategies to improve memorability [4,28]. The re-use of passwords is another well-known issue [28] that also surfaced in our study. Participants reported that they used former or current PINs.

The emergence of the Emoji-password selection strategy "Preference" suggests that passwords generated with EmojiAuth may also follow a skewed password distribution. We analyzed the set of Emoji-passwords created in both our studies to further explore this issue (cf. Section 5.3).

User experience Pragmatic Qualtiy (PQ) for Emoji was medium-high in week 1 (M =4.5, SD =1.4), but lower compared to PIN ((M =5.9, SD =0.77). A Kruskal-Wallis test revealed a significant difference between the groups, $H(3)$=16.25, p=.001, with PQ for Emoji-4 and Emoji-6 being significantly lower than for PIN-4. In week 2, PQ increased for Emoji (M =5.5, SD =1.2) and approximated the ratings for PIN (M =5.9, SD =0.71). The Kruskal-Wallis test did not reveal significant differences in PQ between groups in week 2. Hedonic Quality in terms of Stimulation was medium-high for Emoji (week 1: $M = 4.8$; $SD = 1{:}36$; week 2: $M = 4.9$; $SD = 1.38$) and medium-low for PIN (week 1: $M = 3.8$; $SD = 1.19$; week 2: $M = 4.0$; $SD = 1.13$). Differences were significant in both weeks (Mann-Whitney U; week 1: U=185;p=.003; week 2: U, U=209;p=.018). This suggests that Emoji users found the authentication more stimulating in both weeks compared to PIN.

5 Field Study

5.1 Methodology and Procedure

The field study consisted of a pre-study questionnaire, an introductory session, a field phase of 15-17 days, and an exit session. In order to ensure meaningful use of the authentication methods during the study, we deployed EmojiAuth and PIN as a protection mechanism for the participants' email app on their own phone. E-mails have been shown to often contain sensitive information [1] worth protecting. Consequentially, we recruited only Android users who use an email app on their device and verified this in a screening survey. Participants were recruited through a participant panel of TU Berlin and classified ads posted on an online service similar to Craigslist. Participants from the first study could not participate. Participants received 25€ compensation of which 5€ were paid at the introductory session and 20€ at the end.

During the introductory session participants received information about the study and were asked for consent. Then, either EmojiAuth or PIN was installed as a lock for their email app on their own devices. We used Android accessibility services to monitor whether the e-mail app is currently in the foreground. In order to activate this service, the participants had to select one or more e-mail apps which they currently use from the list of installed apps. After they created an Emoji-password or PIN (depending on the group), opening their email app required participants to authenticate with their password/PIN. Our apps had a 30 second time-out for an authentication session, i.e., if participants left their e-mail app for 30 seconds or more, they had to re-authenticate.

Participants were asked to pick their password/PIN at home. It had to be at least 4 digits. For the PIN group, only meta-data of the user-chosen PINs was collected (PIN length and number of differing characters).

Directly after creating the password, participants received a questionnaire asking about the importance of different password/PIN selection criteria, which were derived from the lab study results. Participants could change their password or PIN during the study (within our app) and EmojiAuth users could further generate a new Emoji-keyboard. In case that they had forgotten their password or PIN, users could enter a pre-defined backup-password in our app and select a new password/PIN. If the password/PIN was entered five times incorrectly in a row, users also had to provide their backup-password to unlock their e-mail app and to select a new password.

The field phase lasted 15–17 days, depending on when participants scheduled their exit session. Similar to Wechsung et al.'s study [29], participants received a daily reminder to complete a daily feedback questionnaire, which asked participants to rate on a Smiley-scale how they liked interacting with EmojiAuth or PIN that day. Participants could further explain their rating in a free-text field. On days 2, 8, and 14, participants further received the AttrakDiff2 mini-questionnaire to assess user experience.

After the field phase, participants returned to the lab for the exit session in which they completed an exit survey (on paper) followed by the shoulder-surfing experiment. Furthermore, EmojiAuth/PIN was uninstalled from their devices.

5.2 Shoulder-Surfing Experiment

The field study's exit session contained a shoulder surfing experiment, modeled after similar experiments in related work [5,30], in which the threat model is a casual observer. Participants acted as shoulder surfers for either EmojiAuth or PIN (based on their field study condition), whereas the experimenter served as the observation target. In contrast to related work, our shoulder surfers were experienced with the authentication scheme they tried to observe after two weeks of use. Participants could position themselves either left, right or behind the experimenter who sat at a table to enter the password. Participants were provided with pen and paper for note taking. To ensure that passwords are entered with similar speed and in the same position, the experimenter trained password entry beforehand.

To test shoulder surfing susceptibility for passwords created with different password selection strategies, the procedure was repeated with five passwords in counterbalanced order. Emoji- and PIN-passwords used the same spatial position of keys on the keyboard in order to facilitate direct comparison between the two schemes. The first and second passwords were random 6-digit ('341779') and 4-digit passwords ('1706'). The third ('134679') and fourth passwords ('5802') were patterns lab study participants had created. The fifth password was an association based on the Christmas Eve date ('2412') for the PIN users and a Christmas-related story created by a lab study participant for the Emoji users ('bear - Christmas tree - snowman - heart' or '23#4' on a numerical keyboard). After a password was entered by the experimenter, the participant had three trials to enter the observed password on a LG Nexus 5 smartphone (Android 5.1.1).

5.3 Results

In total, 41 smartphone users participated in the field study: 21 in the Emoji group, 20 in the PIN group. Three PIN users had to be exluded (2 due to issues with participants' phones; one due to out of scope/inappropriate responses in almost all daily feedback questions). Thus, the PIN group decreased to 17.

Participants were 19–63 years old (M=34, $Mdn.$=28, SD=12.1); 24 were female (59%). Most were students (22), although we did not target students. The second largest group were employees (8), followed by job seekers (5), self-employed (2), and others (4). Most (80.5%) did not have a professional IT background. 19 participants currently used a PIN, 3 a password, 9 an Android pattern, and 11 did not use any locking method.

Success rates In both groups, few incorrect unlocks were recorded during the field study (Emoji: 3% of total unlocks; PIN: 1.5%). In total, 3,514 correct and 83 incorrect unlocks were recorded. EmojiAuth accounted for 1,924 correct (M=91.6, SD=66.1) and 58 incorrect unlocks (M=2.8, SD=4.2); PIN accounted for 1,590 correct (M=93.5, SD=70.4) and 25 incorrect unlocks (M=1.5, SD=1.6). Fisher's exact tests did not reveal significant differences in the number of correct and incorrect unlocks between the groups.

Success rates for PIN were high, suggesting that PIN performs well in the wild. This confirms related work that found PIN to be a practical authentication method with low error rates [3]. Emoji success rates were also high, suggesting that EmojiAuth is a practical authentication method, too.

Password length and changes The majority of participants in the Emoji group (19) initially picked a 4-digit password, whereas 2 participants picked a 5-digit password. Participants in the PIN group initially picked diverse PIN lengths: 10 picked a 4-digit PIN, 2 picked a 5-digit PIN, 3 picked a 6-digit PIN, and 2 an 8-digit PIN. A Mann-Whitney U test did not indicate significant differences in the mean password length between groups (Emoji: M=4.1, SD=.3; PIN: M=4.9, SD=1.4).

Four Emoji participants changed their password once, 3 changed their password twice. In the PIN group, 4 participants also changed their PIN once, 1 changed their PIN twice. A Mann-Whitney U test did not indicate significant differences in the mean number of password changes between groups (Emoji: M=.48, SD=.75; PIN: M=.35, SD=.61).

Password selection The same password selection strategies identified in the lab study also surfaced in the field study (cf. Table 1). Figure 2 provides examples of Emoji-passwords created by study participants in the lab and in the field study.

Based on the results of the lab study, we asked questions (available online at: `http://bit.ly/2imyb2H`) about Emoji and PIN password selection in the field. For EmojiAuth, the questionnaire contained 17 5-point items (1='does not apply at all'; 5='completely applies'), with 2–4 items to measure each selection strategy. For PIN, the questionnaire contained 15 items, with 1–6 items per selection strategy. Lab study frequencies for Table 1 were calculated by counting the occurrences of each interview

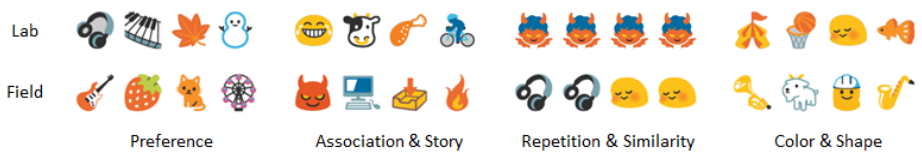


Fig. 2. EmojiAuth passwords created by lab and field study participants. Passwords are grouped according to password selection strategies.

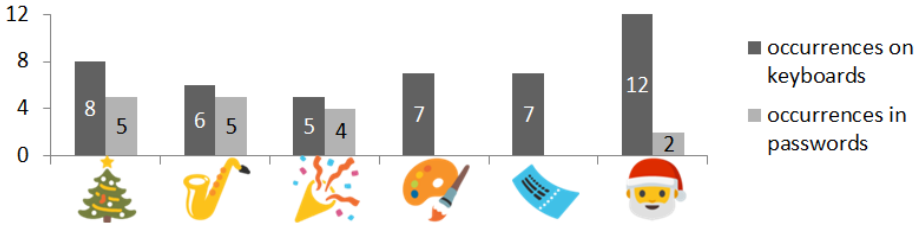


Fig. 3. Password-Emojis examples of the most popular (*left*) and unpopular (*right*) password-Emojis together with their occurrences on the keyboards.

code. Field study frequencies were calculated as the number of participants who rated at least half of the items of a scale (selection strategy) as important or very important.

The overlaps between selection strategies in both studies suggest reasonable validity of the identified strategies. The PIN selection strategies in both studies align with findings in related work [4]. For Emoji-password selection, *Preference*, *Pattern & Position*, and *Association & Story* played an important role in both studies.

The importance of the *Preference* selection strategy for Emoji passwords is also visible from the distribution of selected Emojis across passwords. Figure 3 depicts three examples of the most popular and three examples of the most unpopular Emojis together with their occurrences on the keyboards (lab and field study). Due to the different sizes of the category lists from which Emojis were selected in EmojiAuth, some Emojis appear more often on the keyboard than others. Although we expected the individual keyboards to decrease the probability of hotspots, Figure 3 suggests that the distribution of password-Emojis is skewed.

Shoulder surfing We calculated the minimal Levenshtein distance for each user ("attacker") and each password, i.e., the number of deletions, insertions, or substitutions, needed to obtain the correct password from the entered password [21,31]. There was a significant difference in the minimal Levenshtein distance between Emoji (M=2.45, SD=1.64) and PIN (M=.72, SD=.83) for the 6-digit random password (Mann-Whitney-U, U=289.0; p=.001; r=.53) with medium effect. Thus, the 6-digit random password was significantly harder to shoulder surf on the Emoji keyboard. For the other passwords, there were no significant difference between the authentication methods.

We also compared shoulder surfing susceptibility of passwords from the same scheme. For Emoji, a Friedman's test revealed significant differences in the minimal Levenshtein

Table 1. Frequencies of password selection strategies. Note that some participants used multiple strategies.

Strategy	Emoji		PIN	
	Lab (n=27)	Field (n=20)	Lab (n=26)	Field (n=17)
Color and Shape	2 (7%)	9 (43%)	-	-
Icon Preference	10 (37%)	12 (60%)	-	-
Repetition	9 (33%)	4 (20%)	7 (27%)	7 (42%)
Pattern and Position	12 (44%)	8 (40%)	5 (19%)	3 (18%)
Association and Story	10 (37%)	8 (40%)	5 (19%)	12 (71%)
Password re-use	1 (4%)	-	7 (27%)	4 (24%)
Date	-	-	13 (50%)	8 (47%)

distance between passwords (χ^2=40.44; $p<.001$). Post-hoc analysis with Bonferroni correction revealed that the 6-digit random password was significantly harder to shoulder surf than the 4-digit random password (M=.75, SD=.93; Z=1.45, p=.037, r=.46), the 6-digit pattern (M=.15, SD=.67; Z=2.75, $p<.001$, $r=0.72$), and the 4-digit pattern (M=.15, SD=.37; Z=2.2; $p<.001$, r=.70). All post-hoc results for Emoji had medium to large effect sizes. For PIN, a Friedman's test revealed significant differences between passwords (χ^2=10.78; $p<.029$), but post-hoc tests were not significant.

The post-experiment questionnaires revealed four different strategies attackers used to observe the password: paying attention to the numbers on the keyboard ("numbers"), the password's spatial pattern ("pattern"), a mix of both strategies ("mix"), or they reported observing password entry with high concentration ("observation"). The frequencies of strategies significantly differed between Emoji and PIN (p=.026; Fisher's exact). "Attackers" in the Emoji group were more likely to use the pattern observation strategy (Emoji: 16; PIN: 8). Not surprisingly, "attackers" in the PIN group were more likely to use the numbers observation strategy (Emoji: 0; PIN: 4).

In summary, the 6-digit random password was harder to shoulder surf with the Emoji keyboard compared to PIN and was also harder to shoulder surf with the Emoji keyboard compared to the 4-digit random password and the 4- and 6-digit pattern passwords on the Emoji keyboard. The casual "attackers" in the Emoji group largely relied on the pattern observation strategy which may make Emoji passwords that are based on spatial patterns more suscebtible to shoulder surfing attacks.

User experience The daily feedback questionnaires answered during the field study indicate that the user experience of EmojiAuth and PIN was perceived similarly well. This is supported by the AttrakDiff 2 mini ratings, with the difference that EmojiAuth users perceived the authentication method more stimulating at the beginning of the study. In total, participants reported 342 (Emoji: 184) positive experiences, 99 neutral experiences (Emoji: 51), and 14 negative experiences (Emoji: 10). A Mann-Whitney U test did not reveal significant differences between distribution of positive, neutral, and negative experiences between groups.

To further analyze users' experiences, the free-text answers of the daily feedback were open-coded by one coder. This led to a code list of 17 codes. The qualitative data was then independently coded with the code list by another coder. Inter-rater agreement was high (Cohen's κ=.83). The coders jointly reconciled the remaining cases. A third of participants' comments (35%) expressed that everything was well (e.g., "everything's ok," "fine," "works"). The second most common comments (10%) concerned good usability of the methods (e.g., "really easy and not annoying", "fast [PIN] entry, no problems, I don't have concerns regarding memorability as long as the positions of the numbers don't change"). Six percent of comments indicated participants got familiar with the methods (e.g., "I've became accustomed to it," "it [the authentication] already belongs to my daily routine"). Thereby, Emoji participants reported this twice as much as PIN participants (14 vs. 7 comments). Four percent of codes concerned hedonic aspects. Hedonic aspects were mostly mentioned by Emoji users (11 out of 14, e.g., "I liked choosing the Emojis as I could select them on my own without restrictions," "it was fun to open the e-mail app with the Emojis while sitting next to my friends," "I changed my password twice today as I was curious which other Emojis are available"). A few comments (2.5%) also concerned perceived security vulnerabilities of the schemes ("when I open the app in quick succession, EmojiAuth didn't work properly" [participant was likely corollary not aware of 30 s time-out]; "it's relatively easy for others to find out the [Emoji] combination").

The AttrakDiff 2 mini ratings align with the daily feedback: Pragmatic quality was perceived as high ($M > 5$) for both methods at all measurement points (day 2, 8, and 14). Emoji users rated hedonic quality in terms of stimulation higher than PIN users on day 2 (Emoji: $M = 4.62$, $SD = 0.89$; PIN: $M = 3.22$, $SD = 0.60$; Mann-Whitney U, $U = 34$; $p < .001$; r =.70). However, this effect disappeared over time: there were no significant differences in stimulation between the groups for day 8 and 14.

Despite negligible quantitative differences in user experience, 17 of 20 Emoji users reported in the exit questionnaire that they would prefer using Emojis over PIN as a screen lock, mainly due to the high perceived memorability of Emoji-passwords (12 answers) and the appeal of the Emoji-based method (six answers).

6 Discussion and Conclusion

Limitations. Our study has a few potential limitations. Participants self-selected to participate in a study on mobile authentication, thus our participants may have higher technology affinity than the general population. As the sample size in both studies was limited, generalizations should be made with caution. However, our results facilitate a meaningful comparison of EmojiAuth to the current baseline: PIN entry. Furthermore, the consistency between lab and field study findings indicates a reasonable validity of our results.

Practical Emoji authentication. We have gained valuable insights into the practical aspects of Emoji-based mobile authentication. The results suggest that EmojiAuth may be a practical authentication method with a good password memorability of short passwords and a reasonable memorability of longer passwords. Study participants created their Emoji-based passwords with five different strategies: *Emoji preference*, *as-*

sociation & story, *pattern & position*, *repetition & similarity*, and *color & shape*. The results suggest that the distribution of Emoji passwords may be skewed, even with individual keyboards. We plan to conduct further studies to quantify the frequency of each selection strategy and its contribution to the practical password space. Results from the shoulder-surfing experiment suggest that EmojiAuth performs better for longer passwords that do not follow distinct spatial patterns. As the "attackers" in this experiment mostly focused on the *pattern* strategy, we recommend that spatial patterns should not be used for password creation. We also plan to conduct further studies to investigate whether password creation policies could help users create Emoji passwords that are resistant to guessing and capture attacks, as well as memorable. For example, such policies could blacklist most popular Emojis or spatial patterns.

The role of UX in mobile authentication. Both, EmojiAuth and PIN, were perceived as highly usable and as providing a good user experience in the lab and the field study. In the field study, EmojiAuth users mentioned hedonic aspects slightly more often in their daily feedback. However, for both methods, the overall number of experiences related to hedonic aspects was rather low. The Hedonic Quality/Stimulation ratings indicate that EmojiAuth users perceived their authentication method as more stimulating in the beginning of the field study compared to PIN users. The majority of EmojiAuth users (field) also indicated that they would prefer EmojiAuth over PIN as a screen lock, which is a promising result. We plan to conduct further studies to investigate how hedonic quality could be further increased and maintained in authentication methods and whether it contributes to long-term user "relationships" with the authentication method.

Acknowledgement The authors thank Christopher Krügelstein and Felix Kaiser for their assistance to this research. This work was partially funded by the German Federal Ministry of Education and Research (BMBF) under the project Softwarecampus, grant no. 01IS12056.

References

1. Egelman, S., Jain, S., Portnoff, R.S., Liao, K., Consolvo, S., Wagner, D.: Are You Ready to Lock? In: Proc. CCS, pp. 750–761 (2014)
2. Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., Smith, M.: It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In: Proc. SOUPS, pp. 213–230 (2014)
3. Von Zezschwitz, E., Dunphy, P., De Luca, A.: Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In: Proc. MobileHCI, pp. 261–270 (2013)
4. Bonneau, J., Preibusch, S., Anderson, R.: A birthday present every eleven wallets? The security of customer-chosen banking PINs. In: Proc. FC '12, pp. 25–40. Springer (2012)
5. Schaub, F., Walch, M., Könings, B., Weber, M.: Exploring the design space of graphical passwords on smartphones. In: Proc. SOUPS, p. 11 (2013)
6. Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F., Savvides, M.: Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. Proc. USEC (2015)
7. Bargas-Avila, J.A., Hornbæk, K.: Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience. In: Proc. CHI, pp. 2689–2698 (2011)

8. Novak, P.K., Smailović, J., Sluban, B., Mozetič, I.: Sentiment of emojis. PloS one **10**(12), e0144,296 (2015)
9. Intelligent Environments: Now you can log into your bank using emoji. http://www.intelligentenvironments.com/info-centre/press-releases/now-you-can-log-into-your-bank-using-emoji-1. (accessed: 2017-03-02)
10. Harbach, M., De Luca, A., Malkin, N., Egelman, S.: Keep on lockin' in the free world: A multi-national comparison of smartphone locking. In: Proc. CHI, pp. 4823–4827 (2016)
11. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE **91**(12), 2021–2040 (2003)
12. Yan, J., et al.: Password memorability and security: Empirical results. IEEE Security & privacy **2**(5), 25–31 (2004)
13. Kim, H., Huh, J.H.: Pin selection policies: Are they really effective? computers & security **31**(4), 484–496 (2012)
14. Biddle, R., Chiasson, S., Van Oorschot, P.C.: Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR) **44**(4), 19 (2012)
15. Elenkov, N.: Android Security Internals: An In-Depth Guide to Android's Security Architecture. No Starch Press (2015)
16. Davis, D., Monrose, F., Reiter, M.K.: On User Choice in Graphical Password Schemes. In: USENIX Security Symposium, vol. 13, pp. 11–11 (2004)
17. Golla, M., Detering, D., Dürmuth, M.l.: Emojiauth: Quantifying the security of emoji-based authentication. In: Proceedings of the Usable Security Mini Conference (USEC) (2017)
18. Kraus, L., Wechsung, I., Möller, S.: Exploring psychological need fulfillment for security and privacy actions on smartphones. In: Proc. EuroUSEC (2016)
19. Kraus, L., Antons, J.N., Kaiser, F., Möller, S.: User experience in authentication research: A survey. In: Proc. PQS, pp. 54–58 (2016)
20. Cocozza, P.: Crying with laughter: how we learned how to speak emoji. http://www.theguardian.com/technology/2015/nov/17/crying-with-laughter-how-we-learned-how-to-speak-emoji. (accessed: 2017-03-02)
21. Schaub, F., Deyhle, R., Weber, M.: Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In: Proc. MUM, p. 13 (2012)
22. Stobert, E., Biddle, R.: Memory Retrieval and Graphical Passwords. In: Proc. SOUPS, pp. 15:1–15:14 (2013)
23. Rothenberg, M.: emojitracker: realtime emoji use on twitter. http://emojitracker.com/. (accessed: 2017-03-02)
24. Chiasson, S., Oorschot, P.C.v., Biddle, R.: Graphical Password Authentication Using Cued Click Points. In: Proc. ESORICS '07, pp. 359–374. Springer, Berlin, Heidelberg (2007)
25. Hassenzahl, M., Monk, A.: The inference of perceived usability from beauty. Human–Computer Interaction **25**(3), 235–260 (2010)
26. Diefenbach, S., Hassenzahl, M.: Handbuch zur Fun-ni Toolbox (2011)
27. Hassenzahl, M.: The thing and i: understanding the relationship between user and product. In: Funology, pp. 31–42. Springer (2003)
28. Fahl, S., Harbach, M., Acar, Y., Smith, M.: On the ecological validity of a password study. In: Proc. SOUPS, p. 13 (2013)
29. Wechsung, I., Jepsen, K., Burkhardt, F., Köhler, A., Schleicher, R.: View from a distance: comparing online and retrospective ux-evaluations. In: MobileHCI, pp. 113–118. ACM (2012)
30. Tari, F., Ozok, A., Holden, S.H.: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In: Proc. SOUPS, pp. 56–66 (2006)
31. Levenshtein, V.I.: Binary codes capable of correcting deletions, insertions and reversals. In: Soviet physics doklady, vol. 10, p. 707 (1966)