EmojiAuth: Quantifying the Security of Emoji-based Authentication

Maximilian Golla, Dennis Detering, and Markus Dürmuth
Horst Görtz Institute for IT-Security
Ruhr-University Bochum
Bochum, Germany
{maximilian.golla,dennis.detering,markus.duermuth}@rub.de

***Abstract*—Mobile devices, such as smartphones and tablets, frequently store confidential data, yet implementing a secure device unlock functionality is non-trivial due to restricted input methods. Graphical knowledge-based schemes have been widely used on smartphones and are generally well adapted to the touch-screen interface on small screens. Recently, graphical password schemes based on emoji have been proposed. They offer potential benefits due to the familiarity of users with emoji and the ease of expressing memorable stories. However, it is well-known from other graphical schemes that user-selected authentication secrets can substantially limit the resulting entropy of the authentication secret. In this work, we study the entropy of user-selected secrets for one exemplary instantiation of emoji-based authentication. We analyzed an implementation using 20 emoji displayed in random order on a grid, where a user selects passcodes of length 4 without further restrictions. We conducted an online user study with 795 participants, using the collected passcodes to determine the resistance to guessing based on several guessing strategies, thus estimating the selection bias. We evaluated Markov model-based guessing strategies based on the selected sequence of emoji, on its position in the grid, and combined models taking into account both features. While we find selection bias based on both the emoji as well as the position, the measured bias is lower than for similar schemes. Depending on the model, we can recover up to 7 % at 100 guessing attempts, and up to 11 % of the passcodes at 1 000 guessing attempts. (For comparison, previous work on the graphical Android Unlock pattern scheme (CCS 2013) recovered around 18 % at 100 and 50 % at 1 000 guessing attempts, despite a theoretical keyspace of more than double the size for the Android scheme.) These results demonstrate some potential for a usable and relatively secure scheme and show that the size of the theoretical keyspace is a bad predictor for the realistic guessability of passcodes.**

I. Introduction

Smartphones store security and privacy sensitive data, so it is commonly advised to use an access protection mechanism based on knowledge, possession, or biometric authentication. While modern fingerprint recognition systems provide a convenient way to unlock a smartphone [1], they require specialized hardware components, which increase the price and limit the use of fingerprint readers to high-end models. Furthermore, biometric schemes on smartphones, such as Apple's TouchID, always provide a knowledge-based fallback authentication solution [1], if the sensor readings are inconclusive. Consequently, there is a need for knowledge-based authentication schemes on mobile devices.

Emoticons ":-)" are the predecessors of the colorful emoji graphics 🙂 we use in instant messaging and e-mail to express emotions and moods. The pictogram-like characters we use nowadays were invented by Shigetaka Kurita in 1998 [23] and range from symbols for food items to more complex emotions like "smiling face with open mouth and closed eyes" 😆. Today, emoji are part of the Unicode standard, and special emoji keyboards are available on all major mobile platforms. In 2015, a new graphical knowledge-based scheme that utilizes an emoji-based passcode was proposed [12]. Based on the possible combinations, the authors stated that the scheme is more secure than a 4-digit PIN. The basic idea underlying emoji-based authentication is rather straightforward. The user selects a sequence of emoji, usually from a grid showing all available emoji. For authentication, the user needs to reproduce the same sequence of emoji. The interesting idea here is that most users are very familiar with emoji and use at least a small set of emoji on a daily basis [18]. Furthermore, emoji can be used to express complex feelings in a single character, and thus enable users to tell rich stories with very few characters.

Previous work [15] indicates that emoji-based authentication schemes can offer login times comparable to classical PIN entry, and reasonable memorability, at the same time offering a larger theoretical keyspace and thus potentially more security against guessing attacks. However, it is well-known that user-chosen authentication secrets are usually not distributed uniformly over the theoretical space of secrets (cf. [30]). Thus, user studies are required to estimate how strong the bias of user-selected authentication secrets is for a particular scheme.

A. Contributions

We conducted an online user study to evaluate the security of a prototypical emoji-based authentication system. We consider guessing attacks against the user-chosen secret, and leverage Markov models trained on the emoji, their position on the grid, as well as fused models. To the best of our knowledge, this is the first work to provide security estimates for emoji-based authentication. While there are many limitations to

USEC '17, 26 February 2017, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2017.23024

comparing data collected in different studies and circumstances (see Section V-C), we compare our results with similar estimates for other schemes. We find that our implementation with 20 emoji offers better resistance against guessing than Android Unlock patterns [30] (despite its smaller theoretical keyspace), but lower resistance than uniformly chosen 3-digit PINs for very small number of guesses. Furthermore, our results provide valuable insights on users passcode selection strategies and explain how they differ from classical PIN selection.

B. Outline

In Section II we will review some material about graphical passwords and their security. In Section III we provide details about the conducted user study, as well as participants. In Section IV we describe the attacker model that we consider and explain our guessing approach based on three different Markov models. In Section V we provide and discuss the results and give some insights on the provided security level of emoji-based authentication. We discuss some properties of the studied scheme and directions for future work in Section VI, and conclude with Section VII.

II. Related Work

In this section, we review prior work on related graphical authentication for mobile and desktop devices.

A. Graphical Passwords

Graphical passwords have the potential to offer easier-to-use authentication, as there is the indication that graphical information is remembered with less effort by humans [8]. Recently, they found widespread adoption, especially on mobile devices. While there is a loss in usability with text-based passwords, if used on devices without a physical keyboard [19], graphical schemes are particularly well-suited for touchscreen use.

A popular example for a *recall*-based graphical password scheme is the Draw-a-Secret scheme (DAS) [14], where one draws free-handed on a grid. In 2007, Tao and Adams [25] modified the original idea by snapping the drawn lines to the intersections of a grid, thus removing many of the problems of ambiguities of the DAS scheme and making it much easier to use, calling the resulting scheme Pass-Go. This scheme was adopted, with some restrictions, for use in Android-based mobile phones in 2008.

Moreover, examples for *cued-recall*-based schemes include BDAS (Background Draw-a-Secret) [10] and PassPoints [34], [35], [36]. Presumably, the most widely used cued-recall based scheme is the Windows Picture Password [24], which is based on the PassPoints idea.

Finally, *recognition-based schemes* are, instead of recalling information, based on recognizing a previously seen object. One of the classical examples is the PassFace scheme [22], where the user selects several pictures of faces, and has to select these faces among a number of decoy images for authentication. Several related schemes have been explored, but to the best of our knowledge, there is no scheme with significant adoption.

B. Graphical Passwords Security

For the DAS scheme, Thorpe and van Oorschot [26] analyzed the security based on mirror symmetric (reflective) fragments. They constructed dictionaries that improve guessing attacks against graphical passwords and estimated the realistic space of passwords being smaller than the theoretical space. Further, they explored relationships between the number of composite strokes and password length and found security reductions depending on how users choose their strokes [27]. Jermyn et al. [14] analyzed the security of the DAS scheme for computer-generated passwords. However, computer-generated passwords are in practice only used for very few accounts, problems being user acceptance and low usability.

For the PassFace scheme, Davis et al. [7] measured user's bias when selecting faces and found substantial bias based on gender, race, and subjective beauty of the face. For the PassPoints scheme, Dirik et al. [9] investigated the distribution of user's choices and found substantial bias based on data collected from human users. Thorpe and van Oorschot [28] used a more involved method and used click-points collected in a user-study to seed automated methods for predicting likely click-points, further facilitating and improving this kind of attack. Zhao et al. [37] evaluated the security of the graphical password scheme used in Windows 8 and proposed effective guessing algorithms against them.

The most widely deployed graphical password scheme is the Android Unlock pattern, which is a successor of the Pass-Go scheme. Its security has been well studied. Uellenbeck et al. [30] evaluated the security of Android Unlock patterns and found substantial bias both in the starting point as well as the path chosen by users. They precisely quantified the security of the scheme and found its security to be lower than that of a uniformly chosen 3-digit PIN.

Attacks beyond probabilistic guessing were considered by Aviv et al. [2], who used "smudges" left on the smartphone screen while entering a pattern to reconstruct the user's secret. The accelerometer built into basically all modern smartphones was shown [3] to leak (partial) information about PINs and patterns entered on a smartphone. Von Zezschwitz et al. [32] measured and compared the usability of (assigned) PINs and Android Unlock patterns under a realistic setting over a timespan of three weeks. Recently, von Zezschwitz et al. [33] analyzed the choice of Android Unlock patterns by observing the impact of human interest in geometric properties of the resulting shapes. To influence the starting point of the unlock pattern, they proposed different background images showing, among others, emoji to increase the diversity in the user choice.

III. Study Design and Data Collection

In this section, we describe the details of the studied EmojiAuth scheme, the design of the user study, the data collection methods, and the participant recruitment process.

A. EmojiAuth Prototype

We developed an instantiation of an emoji-based authentication scheme to evaluate its security. Previous instantiations were studied by Kraus et al. [15] (abbreviated KS) and announced by Intelligent Environments Ltd. [12] (IE) to enable consumers to log into their banks using four emoji characters.

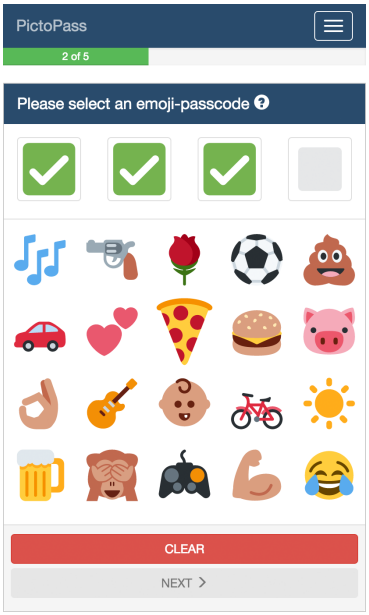


Fig. 1. Emoji entry form as used in the user study. Every entered emoji is covered with a white check on a green background. A "Clear" button allows resetting the form. A user is allowed to continue after selection four emoji.

The number of emoji offered to the user varies widely between both schemes (KS offers 12 emoji, while IE offers 44 emoji). We chose to provide a choice of 20 emoji, as these were still easy to select even on smaller screen sizes, it was possible to select 20 emoji that were simple to distinguish, and it offered a substantially higher theoretical keyspace than PINs of the same length. We selected emoji of different categories (flora and fauna, music, food, transportation, weather, and leisure), by selecting a subset of the emoji used in the proposal of IE. We were specifically interested in studying selection strategies based on the emoji content and the position, so we chose a random order to display emoji on the screen, but this order was fixed for one user over the entire experiment. KS used a fixed layout but suggested to use a user-specific keyboard or even a user-specific selection of emoji, and IE seems to use a fixed layout.

Users were supposed to choose 4 emoji, where the order is relevant and the same emoji could be selected multiple times. We wanted to study the security of user selected passcodes, so restricting the user's choices would have hindered us to obtain a reasonable baseline for further comparisons (in potential follow-up work). Please note that practical implementations would likely implement such restrictions, and from our results, we recommend to apply such restrictions. While KS seems to allow repetitions of emoji, IE does not.

PIN and password entry on mobile devices usually implements a simple measure against shoulder surfing, where the letters or digits are displayed for a short while after input only, and then replaced by a generic placeholder. We displayed the emoji for half a second before showing the placeholder (see Figure 1).

The interface for enrollment is shown in Figure 2(f), the interface for authentication only differs in the green progress bar and is shown in Figure 2(h).

All proposed emoji-based authentication schemes offer a higher theoretical keyspace compared to PINs of the same length. (KS's keyspace is larger by a factor of approx. 2, ours by approx. 16, and IE's by approx. 350. At the same time, at least KS reports that authentication times are comparable to PIN-based logins and that emoji-based schemes provide reasonable memorability. However, the size of the theoretical key space is not a good measure of the resistance to guessing attacks, as users are not selecting their passcodes truly uniform, and thus some passcodes are more common than other passcodes. Quantifying this selection bias and thus estimating the security against guessing attacks is the goal of this work.

B. Study Design

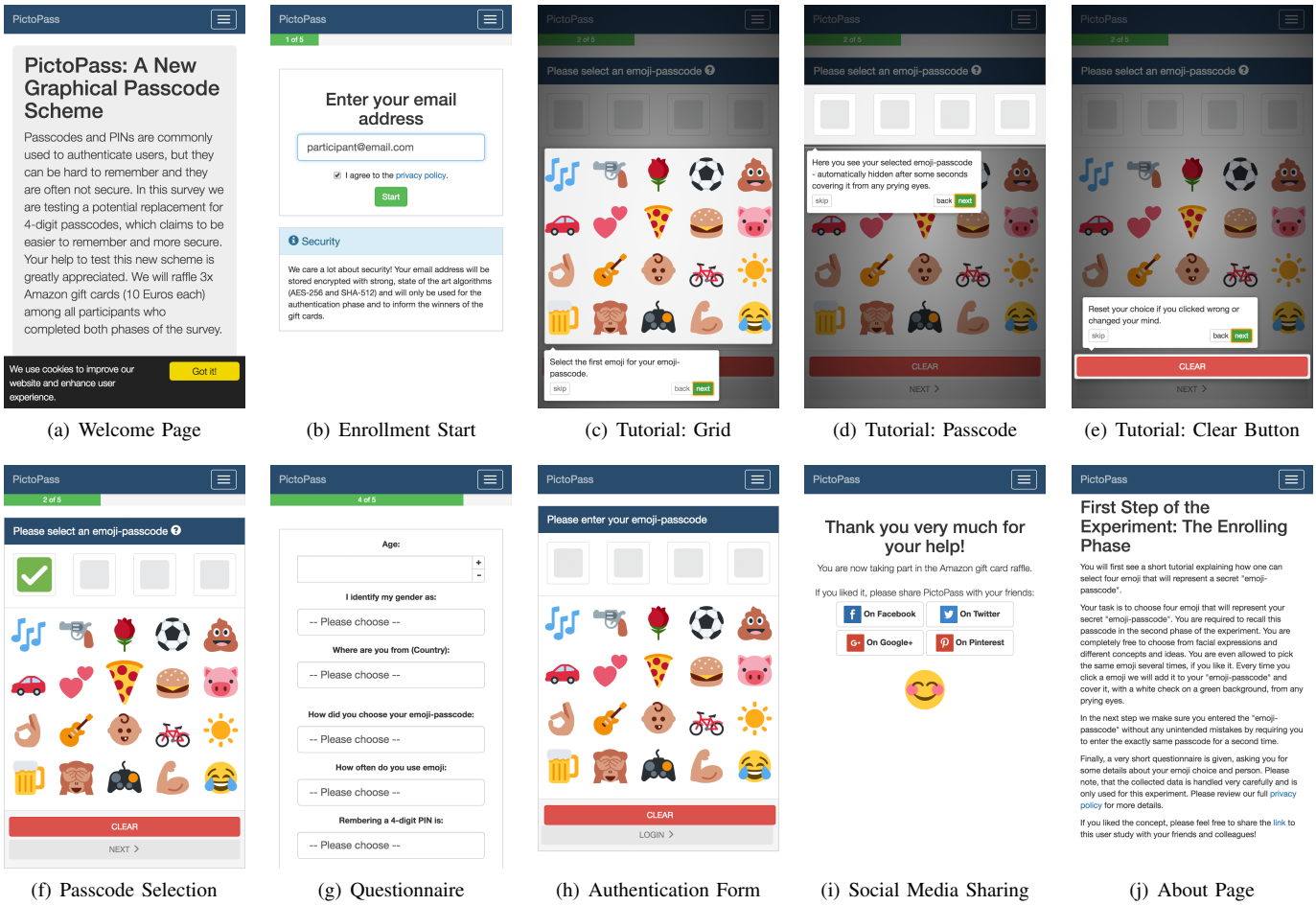
We developed a web-based prototype implementation (at the time using the name "PictoPass"). Participants first went through a *welcome* page that described the idea, then *enrolled* by choosing a passcode and answered a brief questionnaire. After 2 days we re-invited them to the *authentication* where they were supposed to reproduce their passcode.

1) Introduction: On the welcome page of the user study website users were informed about the objective of measuring the security of a potential replacement for a 4-digit passcode scheme, which possibly would be easier to remember and more secure (see Figure 2(a)). We collected user's email addresses to be able to contact them again. We requested all users to read and explicitly agree to the data collection. We informed about which data is collected and stored, how the contributed data will be managed, and that they can leave the study at any time.

2) Enrollment: The enrollment phase started with a short tutorial explaining how one can select four emoji that will represent a secret emoji passcode. An excerpt of this short tutorial is depicted in the Figures 2(c), 2(d), and 2(e). We first explained how to select an emoji, then showed that the selected emoji will be a part of a 4-digit passcode. After this, we introduced the "Clear" button and explained how one could proceed to the next page. On a separate page, we explained the process in more details. We asked to choose four emoji that will represent a secret emoji passcode. The users were informed that they need to be able to recall this passcode in the second phase of the experiment. Further, we explained that a user is completely free in choosing the emoji. Every time a user selected an emoji, we added it to the emoji passcode shown above the keyboard, displaying it for half a second and then covered it with a white check on a green background (a commonly used countermeasure against shoulder surfing). The user could reset the current selection by pressing the "Clear" button and start again.

After completion of the passcode, the user was requested to enter the passcode a second time, both to verify that no mistypes had happened, and to provide some light training on the code by repeating it. (This is a common technique for entry of PINs, Android Unlock pattern, and passwords).

3) Questionnaire: Afterward, we provided a short survey asking for some details about the age, gender, country, strategy for choosing the emoji passcode, and how much effort the user usually spends to protect personal data. To reduce the required time to complete this form, we provided convenient



(a) Welcome Page (b) Enrollment Start (c) Tutorial: Grid (d) Tutorial: Passcode (e) Tutorial: Clear Button

(f) Passcode Selection (g) Questionnaire (h) Authentication Form (i) Social Media Sharing (j) About Page

Fig. 2. Various screenshots of the online user study. Starting with a welcome page introducing the concept, participants consented to a privacy policy and provided their email address. On the next page, we showed a short tutorial explaining the user interface. After the passcode selection process the participants were requested to complete a brief survey. During authentication, users were asked to enter their passcode and encouraged to share the user study if they enjoyed it via social media. An additional project description, as well as a contact and privacy policy page, was provided (not depicted).

input methods like drop down lists and also enabled users to provided own answers via free text fields. However, most of the questions were answered by using 5-point Likert scale drop down lists, with a default position on a "Please choose" element. After the questionnaire users had an additional option to write some feedback and to submit wishes, suggestions, and criticism in a feedback form.

4) Authentication: Two days after the enrollment participants were invited by mail to the registered email address to start the authentication phase. The email provided a link (unique for each participant) to the authenticating page. By visiting this link a user was redirected to an individual passcode entry form. Users were prompted to enter the passcode that was provided during enrollment into the form to login. Upon falsely entering the passcode users were given up to two additional tries to enter the correct code, after three failed login attempts the login was deemed not successful. Finally, the user was encouraged to share a link to the study with friends, we thanked them for their time, and informed them (again) that they will now enter a raffle for gift cards.

The prototype was optimized for use on mobile devices, and participants were encouraged to use it on a mobile device, but we did not enforce this and let non-mobile devices participate as well. While the scheme seems most plausibly used for a mobile device unlock, the interaction does not appear to be specific for mobile devices, and it could be used on desktop-class devices as well.

C. User Participation

The EmojiAuth user study took place in March 2016 and lasted 21 days. We invited people via email distribution lists and social media to participate in the study. Additionally, participants were encouraged to spread the link via their social media accounts. This is the first study on the selection bias of emoji-based authentication, and we wanted to establish a first baseline with as many users as possible. Our study can serve as a starting point for more directed studies.

795 participants completed the first phase (introduction, enrollment, and questionnaire). We sent out an email invitation to the second phase (authentication) two days after the participant has registered, and sent out a reminder after four days to those who had not clicked the link at that time. 22 invite emails could not be delivered successfully (e. g., due to registering a fake email address or a typo in the email address). 141 participants

did not come back, an expected number for an online study without any confirmation.

632 participants started the authentication phase by visiting the link from the invite email, and 535 successfully authenticated (464 in the first, 58 in the second, and 13 in the third attempt). The remaining 97 participants did not authenticate successfully. 9 participants did not try any passcode at all, 8 gave up after the first attempt, 14 gave up after two attempts, and 66 failed in all three attempts.

D. Demographics

While participants from all age groups participated, most of them (73 %) were between 20 and 30 years old. Around 37 % were female, 62 % male, and 1 % did not feel to belong to one of these two groups. Most participants were from Germany (90.7 %), Austria (1.3%), and Finland (1.3%), while participants from over 39 countries registered. Most participants (33 %) use emoji frequently, e. g., for text messaging and enjoyed the use of emoji in this new context.

We observed a bias towards IT security aware participants, as most of them estimated their technical understanding as above average to excellent and assessed that they spend a substantial effort to protect their data. Furthermore, for most of the participants remembering a 4-digit PIN feels easy to moderate. Moreover, we asked all participants that used the "Clear" button why they pressed it. In most cases, the participants spontaneously changed their minds or accidentally tapped the wrong emoji. However, we also observed motivations like: "I instantly forgot the passcode / forgot the ordering" (4 participants), "I wanted to ensure myself that there is no typo" (3 participants). The detailed statistics are listed in the Appendix in Table III.

E. Limitations

The user study suffers from limitations typical of small-scale online studies. For instance, 37 % of the participants are female. Further, one can observe a distinct bias towards young participants ($20 - 30$ years) with more than average technical background (self-reported). We acknowledge that a more balanced user base would be preferable. However, a bias in the direction of young, technically interested, and security involved participants might not harm but protect the study from overestimating the offered security level of emoji-based authentication.

A further limitation is that recall of passcodes was tested after two days only, and results after longer time-spans may be different. But we believe that confirmed recall after two days is already a good indication for memorability of the passcodes, and should be sufficient for a first study exploring the topic.

F. Ethical Considerations

While there is no ethics committee covering this type of studies at the organization involved in this research, there are strict laws and privacy regulations in place that must be obeyed, and we discussed the study design with peers to ensure proper design. The data we collected about a participant cannot be linked back to a respondent, as the data is in quite broad categories only. We did not collect any personal identifiers (IP address, device identifier, name, or similar), and did not use third-party components that may still log such data. Users consented with the data collection for research purposes and were informed they can request deletion of their data.

IV. Measuring Guessability of Passcodes

In this section, we discuss the guessability of passcodes for emoji-based authentication and describe the construction of our Markov model-based guesser in detail.

A. Threat Model

To provide a lower-bound on the security of emoji-based authentication, we consider a *trawling* [4] attacker, where the attacker tries to guess the passcode of *any* user. This is in contrast to a *targeted* attack, where the adversary tries to gain access on behalf of *one particular* user.

In a trawling attack, the adversary guesses the n most likely answers a_i for a given challenge c. If unsuccessful, the attacker moves on to the next victim. An ideal attack requires the well-approximated distribution of the answer space a. We consider the trawling attack to be more realistic than a targeted attack, as no assumptions about the user-preference must be made. If a smartphone is lost, the attacker might not be able to identify the owner, thus is not able to perform a targeted attack to unlock the phone. Furthermore, emoji-based authentication might not only be used to unlock the device but to authenticate against a web service with a high number of users.

B. Introduction to Markov Models

Markov models have proven a useful tool to model user-chosen authentication secrets in the past, both for passwords [21], [17], [11] and Android Unlock patterns [30]. We expect them to provide reasonable predictions for the studied EmojiAuth scheme as well, specifically in the light of previous work by Kraus et al. [15] which found that common (self-reported) strategies for selecting passcodes were based on *creating a story*, *repeating events of my life*, and *visual patterns "A-B-A-B"*. (Note that other common strategies did not necessarily involve a specific order of emoji, such as *important things of their lives* or *tried to select a random passcode*, and are thus less well modeled by Markov models. Still, the relative frequencies of emoji are approximated by Markov models.)

In a Markov model, one models the probability of the next token in a string based on a prefix of length $n-1$. Considering a sequence of tokens $c_1, \ldots, c_m$, an n-gram Markov model estimates its probability as

$$\begin{aligned} &P(c_1, \ldots, c_m) \\ &= P(c_1, \ldots, c_{n-1}) \cdot \prod_{i=n}^{m} P(c_i | c_{i-n+1}, \ldots, c_{i-1}). \end{aligned} \tag{1}$$

The required *initial probabilities* $P(c_1, \ldots, c_{n-1})$ and *transition probabilities* $P(c_n | c_1, \ldots, c_{n-1})$ can be determined empirically from the relative frequencies from training data. One commonly applies further post-processing to the raw frequencies: So-called *smoothing* tries to even out statistical effects in the data, in particular, it avoids relative frequencies of 0, as these would yield an overall probability of 0

regardless of the remaining probabilities. We use Laplacian (add-one) smoothing, as previous work [30] has shown that more involved smoothing has little effect for other graphical password schemes.

We trained and tested different n-gram sizes between 2 and 4, and found 2-grams to perform best in this setting. While in general, larger n-grams mean more precise models, it also exponentially increases the size of parameters to be learned (in our case we have 20^{n-1} initial probabilities and 20^n transition probabilities). With our limited training set, we apparently do not have enough datapoints to estimate these parameters for larger values of n accurately.

We use the Markov model to estimate the probabilities of all possible passcodes, and then sort them in order of decreasing frequencies to obtain the "optimal" guessing order. Also, for those passcodes that appear more than once in the training set, i. e., which allow us to directly compute a reasonable estimate for their relative frequency from the training data, we use that estimate instead of the estimate of the Markov model (similarly to previous work [30]). We train Markov models both on the selected emoji, their position, and a hybrid model. Details can be found in the next sections.

C. Attack Model Based on Content

In the questionnaire (see Table III) we asked the participants for the motivation of their passcode choice. We observed that most users chose their emoji in a way to create a story (33.7 %) or to include important things of their lives (29.4 %). Thus, it is very likely that the passcodes do not follow a random choice, but are highly structured. Figure 3 visualizes the structure of 2-grams observed in the user study passcode data. As stated by Kraus et al. [15] there is a variety of emoji passcode selection strategies. Due to the questionnaire we identified the following strategies:

- Created a story (268)
- Used important things of their lives (234)
- Tried to selected a *random* passcode (83)
- Repeating event of my life (54)
- Emoji frequently used while texting (44)
- Visual pattern: "A-B-A-B" (31)
- Positions within the grid (19)
- Emoji I like the most (17)
- Emoji I find hilarious and funny (6)
- Emoji of the same color (3)
- Constructed a passphrase: "Super-Baby-Pig-Poo" (3)
- First letter of the emoji: "Baby, Ball, Beer, Burger" (3)
- Emoji related to the same category: "food" (3)

Motivated by the number of selection criteria that are focused on the object or emotion that is represented or expressed by the visualization of the emoji, we built a Markov model considering the emoji content to generate guesses in their most likely ordering. This way, guesses including related emoji like 🍔, 🍕 are made rather early, while passcodes containing unrelated combinations such as 🍔, ⚽ are guessed later.

D. Attack Model Based on Position

Choosing digits based on the position in a grid is a typically PIN selection strategy [5]. Similar are so called keyboard

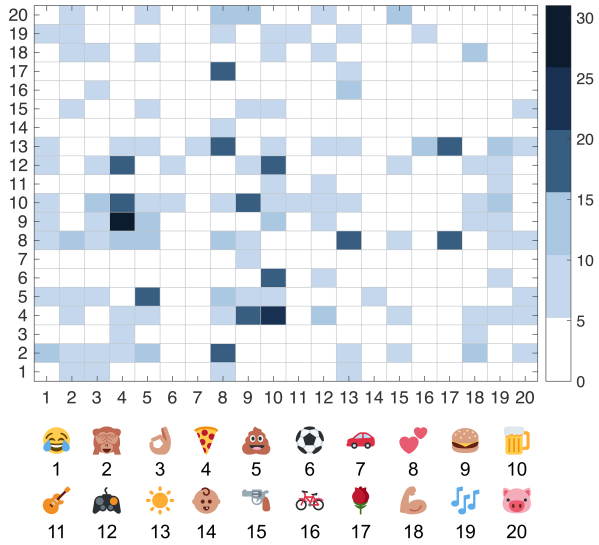


Fig. 3. Visualization of popular 2-grams in the user study data. One can observe structure but no uniform distribution in the emoji passcode choice. For example, related emoji like "Hamburger, Slice of Pizza" occur rather frequently, while unrelated combinations such as "Hamburger, Soccer Ball" do not occur in the dataset.

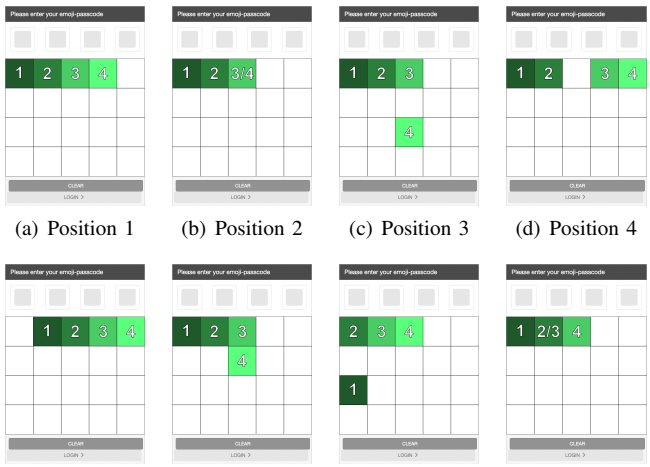


Fig. 4. Top 8 positions based on a 2-gram Markov model. Comparable to Android Unlock patterns we observed the upper left to be the most likely starting point of a passcode (a behavior that might be influenced by the cultural background of the enrolled participants).

walks in a password selection process [31]. In the user study around 2.4 % of the participants had chosen the emoji of their passcode based on the position within the displayed grid (see the Section III). To measure the influence on the security of such a selection strategy we built a Markov model on the chosen positions of the used emoji, i. e., positions like "3, 7, 15, 1", in contrast to the emoji content, i. e., 🌹, 💕, ☀️, 🎶. To account for interference between content and position all participants were assigned a random grid. However, the grid stayed the same for every participant between the individual enrollment and authentication attempts.

Figure 4 visualizes the 8 most likely user chosen positions based on a 2-gram model trained on the observed passcodes of the user study. Comparable to Android Unlock patterns we

observed the upper left to be the most likely starting point of a passcode (a behavior that might be influenced by the cultural background of the enrolled participants).

E. Model Fusion

By combining the content- and position-based Markov models we tried to increase the guessing success rate further. Based on the observed selection strategies, it is likely that both features do not disturb but complete each other. A proper fusion of both features can be used to more precisely model the ordering of the emoji passcode guesses, thus increase the attacker's success rate.

In our experiments, we tested different fusion techniques, known, e. g., from biometrics [13]. While more comprehensive approaches exist, we limited ourselves to standard transformation-based fusion via combination rules, such as addition, multiplication, minimum, and maximum, and compared the results to the performance of the individual models, i. e., content-only and position-only.

We performed 5-fold cross-validation on the dataset: splitting the dataset into 5 subsets of approximately equal size, training the model(s) on 4 subsets, and evaluating the guessing success on the 5th subset. This process is repeated to use all 5 subsets as a test set once. We only used the 623 passcodes that were tried to be repeated in the authentication phase, to avoid working with passcodes that were selected by participants without the intention to reproduce. Thus, the size of the training set was approximately 500 in each fold, seemingly sufficient to estimate the 400 transition probabilities in a 2-gram model.

For the fusion, we trained two individual models per fold, one based on the content and the other one on the position of the emoji passcodes in the current training set. After this, given the grid layout of the currently attacked user in the set, we needed to translate every possible passcode into its corresponding position. This way we obtain an individual probability of a passcode in both models. Next, a combination rule is applied to fuse the two individual probabilities into a new hybrid probability and store the result in a new model. As we no longer require a single model per fold in the cross-validation, but need to compute a model for every user in the current test set, the fusion approach is computational more expensive.

V. Analysis and Results

Next, we give the results for the guessing resistance of emoji-based authentication and compare the resulting security with other user-chosen secrets.

A. Basic Statistics

First, we provide some basic statistics about the collected passcodes.

The most *frequently used passcodes* in the dataset are shown in Table I. One can see that only two passcodes occurred more than twice. Further, only 13 passcodes occurred more than once. We can see some tendency towards cheerful emoji, a tendency which is also reflected in the most common emoji (see below). Noteworthy is the choice to build passcodes consisting only of a single emoji, which apparently is reducing the security. We also see some tendency of selecting emoji for a common theme, e. g., food or love.

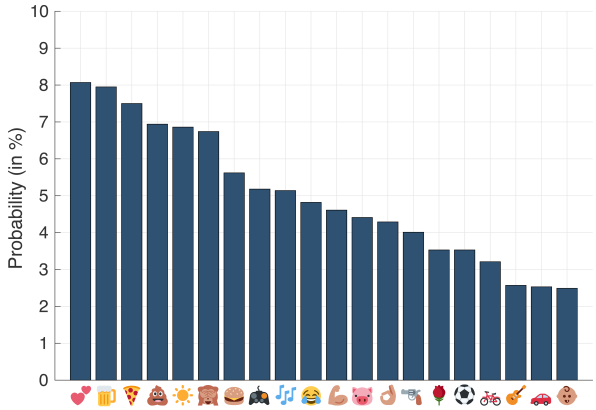
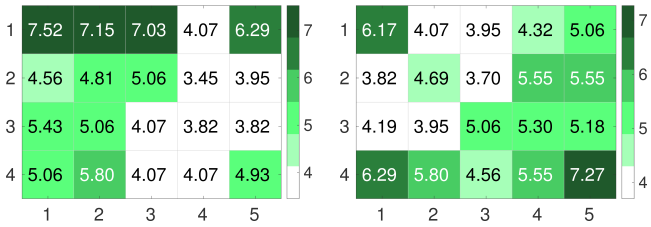


Fig. 5. The most frequently used emoji observed in the passcodes.



(a) Entry (b) Exit

Fig. 6. Visualization of the position distribution for the first (entry) and last (exit) emoji of the passcodes (in %).

TABLE I. Top 5 passcodes of all participants.

Occ.	P1	P2	P3	P4	Prob.
4	💩	💩	💩	💩	0.64 %
3	💩	💕	💩	💕	0.48 %
2	💕	😂	🎶	☀️	0.32 %
2	💕	💕	💕	💕	0.32 %
2	☀️	☀️	☀️	☀️	0.32 %

The most *frequently used emoji* are shown in Figure 5. The emoji "two hearts" (8.1 %) is the most common, while "baby" (2.5 %) is the least popular choice. We can see that emoji of the category "food" are rather popular.

The *entry and exit points* are shown in Figure 6. This data shows, similarly to other drawmetric schemes and specifically for the Android graphical password, a tendency to start at the upper-left and end at the bottom-right. The effect is much less pronounced than for other schemes, as the location aspects are only one part of the users' selection strategies. (As we will see later, the bias caused by the emoji content is more pronounced.)

TABLE II. ONLINE GUESSING SUCCESS, WHERE λ_N IS DEFINED AS THE PERCENTAGE OF PASSCODES CORRECTLY GUESSED WITH N GUESSING ATTEMPTS.

Scheme	λ_1	λ_{10}	λ_{100}	$\lambda_{1\,000}$
Emoji - Position	0.2 %	2.4 %	2.6 %	5.0 %
Emoji - Content	0.3 %	1.9 %	4.7 %	8.5 %
Emoji - Fusion (Add.)	0.2 %	1.6 %	6.6 %	10.8 %
4-digit PIN - All	2.6 %	9.2 %	17.7 %	38.0 %
Android Unlock pattern	0.9 %	3.8 %	17.0 %	50.0 %

B. Strength Estimates

Next, we provide the strength estimates for EmojiAuth, the main results of the study. We present strength estimates for the attacks based on content, position, and the hybrid attack, separately. The guessing success of all three models is shown in Figure 7, for the most interesting region of up to 300 guesses on the left, and for the full 160 000 guesses on the right. For reference, we add the guessing success against uniformly chosen PINs of length 3, 4, and 5.

1) Content-Based Guessing: First, we describe the results from the Markov model trained on the emoji content only. It is shown in blue (crosses) in Figure 7. For 10 guesses 1.9 % of passcodes are recovered (i. e., $\lambda_{10} = 1.9\,\%$), and for 100 guesses 4.7 % of passcodes are recovered (see Table II). This offers roughly a security of uniformly chosen 3-digit PINs, slightly lower for 10 guesses and slightly higher for 100 guesses.

2) Position-Based Guessing: The results from the Markov model trained on positions only are shown in green (boxes) in Figure 7. For 10 guesses 2.4 % of passcodes are recovered (i. e., $\lambda_{10} = 2.4\,\%$), and for 100 guesses 2.6 % of passcodes are recovered (see Table II). Again, this offers roughly a security of uniformly chosen 3-digit PINs, lower for 10 and higher for 100 guesses. What is interesting is that numbers hardly change between 10 and 100 guesses, and generally the curve turns out to be much flatter than the curve for other models. In Figure 7(a)(right) we see that the curve is quite close to the diagonal, i. e., to the curve for random guessing. This indicates that there is a small number of passcodes that were chosen according to the position, and the model has low predictive value beyond those passcodes. Recall that 2.4 % of the participants reported having chosen a passcode based on the position of the emoji (see Section IV-D).

3) Hybrid Guesser: Finally, we report the guessing success for the fused model, which takes into account both content and position. We tried different fusion techniques that are compared in Figure 9. We found the addition rule to perform best. Since this rule is robust to errors in the estimation of the probabilities, it works well in practice and is commonly used in multibiometric systems [13]. As one can see, using a rule that always picks the bigger probability (max rule) performs equally well. However, just multiplying the probabilities of both schemes, does not perform as good, especially for lower guess numbers. Noteworthy is that all fusion models, except the one using the min rule (always picking the smaller probability), perform better than the models built on a single feature, i. e., content or position. We only report the numbers for the addition-based fusion. The model slightly decreases the guessing success for very small guessing numbers (1.6 % for 10 guesses, as opposed to 1.9 % for the content-based and 2.4 % for the position based model). For larger guessing numbers, the success substantially increases, to 6.6 % for 100 guesses and to 10.8 % for 1 000 guesses.

C. Baseline Comparison

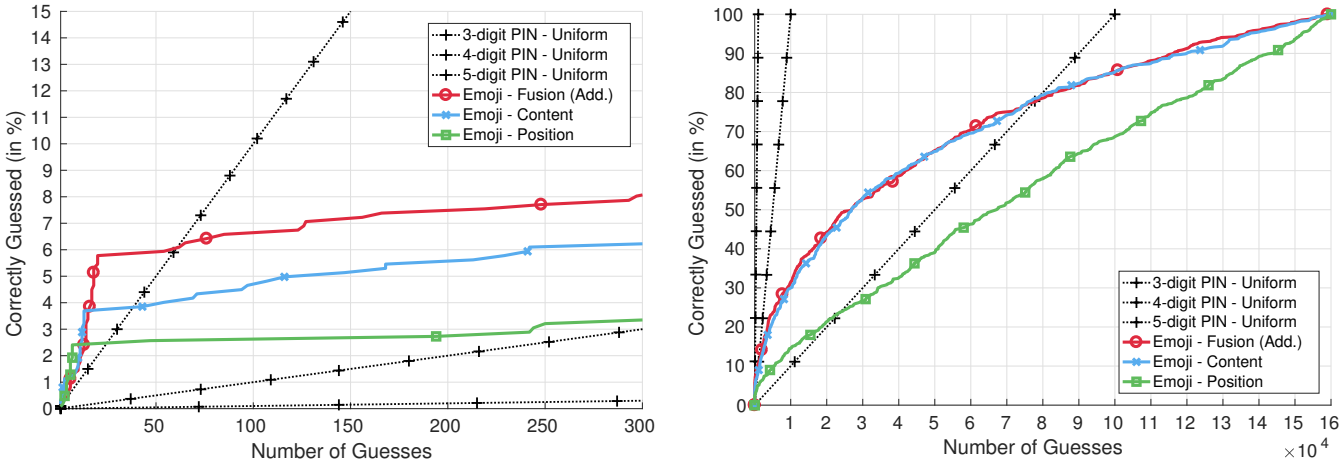
Next, we compare the strength estimates for the EmojiAuth scheme from Section V-B with strength estimates for other schemes, see Figure 8 and Table II.

Keep in mind that the guessing success against different schemes depends on the guessing algorithm used, on the quantity of samples available for training of the model, and may be influenced by demographic bias of the collected data. While using Markov models seems like a sound approach for predicting patterns for the EmojiAuth scheme, better models may exist. Thus the following comparison has some serious limitations.

One baseline we consider is the Android graphical password scheme, which has been well studied, and its security has been estimated before by Uellenbeck et al. [30]. To be able to compare their Android scheme results with the EmojiAuth results, we implemented the same Markov model-based guesser and model validation technique. Furthermore, we used a similar sized training set, see Section IV for details. The results indicate that EmojiAuth resists guessing attacks better than the Android scheme, despite the smaller theoretical password space (160 000 and 389 112, respectively).

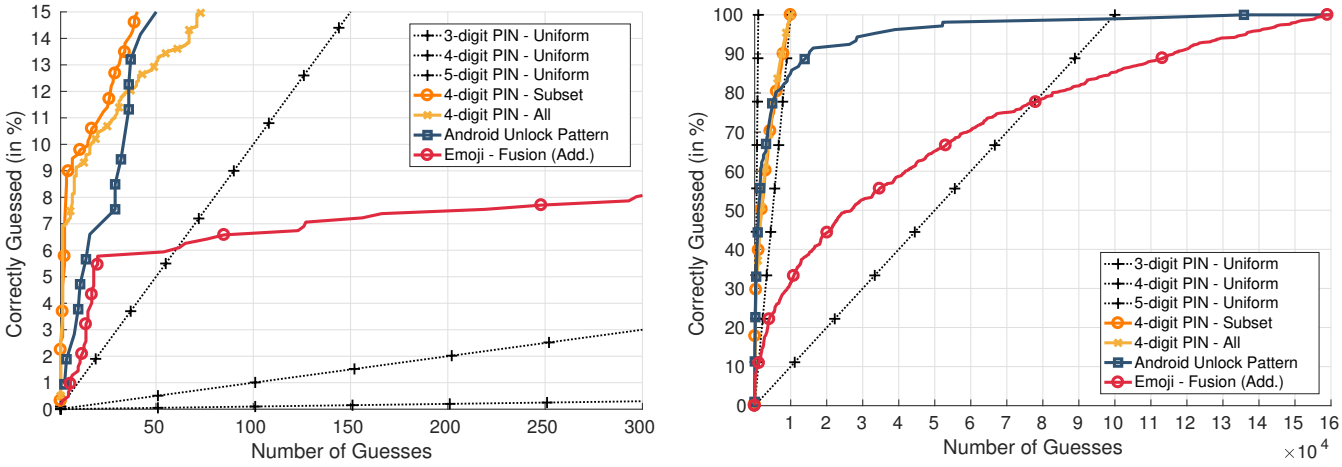
We also compare against a set of user-chosen 4-digit PINs, collected in 2011 by Daniel Amitay [6], using an iPhone application with a screen locking mechanism that required to enter a 4-digit PIN to unlock. Again, we used the same Markov model-based guesser, here trained on the 4-digit user-chosen PINs. As this dataset is much larger than the other datasets (it consists of 204 000 PINs), we tested two different sized datasets: i) the complete 204 000 PINs (All) available in the dataset, and ii) a small subset of 623 PINs (Subset), sampled randomly from the full dataset. As one can see in Figure 8(a), both the smaller and the larger sets of PINs behave very similarly, in fact the guessing success is slightly better for the smaller dataset, an effect most likely encountered by chance. This seems to indicate that the approx. 500 samples are more than enough to estimate the parameters for the Markov model for PINs, with 100 transition probabilities to learn. Overall, for PINs we find weaker resistance to guessing attacks as compared to EmojiAuth.

Overall the available data seems to indicate that EmojiAuth offers better resistance to guessing attacks than alternative schemes. It is important to recall the limitations of this comparison: Most importantly it is unclear how accurately Markov models model user choice in the individual schemes, which impacts the accuracy of the modeled attacker. The origin and the sampling of the three datasets is different, which may have an unknown effect on the strength of the patterns, and the specific parameters of the scheme (e. g., 4-digit PINs as opposed to other lengths, 20 Emoji as opposed to other sizes, 9 nodes as opposed to other grid sizes) influence the security as well.



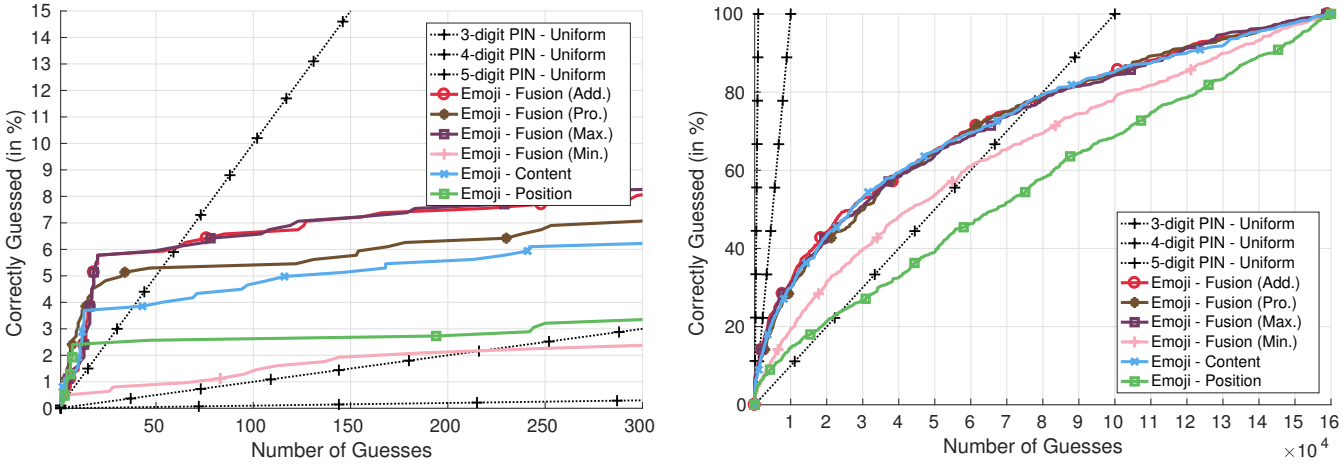
(a) EmojiAuth: 300 Guesses (b) EmojiAuth: 160 000 Guesses

Fig. 7. The user bias involved is substantial for the guessing success of the first approx. 5.7 % of the emoji passcodes. Afterward, a lower but continuous increase is observed. Further, one can see a benefit of fusing the content- and position-based Markov models depicted in the guessing success rate.



(a) Scheme Comparison: 300 Guesses (b) Scheme Comparison: 160 000 Guesses

Fig. 8. Comparison of popular unlocking mechanisms and EmojiAuth over 300 and 160 000 guessing attempts. One can observe that the user bias involved is less pronounced than for the Android Unlock pattern and user-chosen PINs.



(a) Fusion Models: 300 Guesses (b) Fusion Models: 160 000 Guesses

Fig. 9. Comparison of different fusion mechanisms over 300 and 160 000 guessing attempts. We found the addition rule to perform best. Since this rule is robust to errors in the estimation of the probabilities, it works well in practice. We found all fusion models, except the one using the min rule, to perform better than the models built on a single feature, i. e., content or position.

VI. Discussion

In this study, we concentrated on the security of the EmojiAuth scheme, as previous work found that EmojiAuth (with 12 emoji) "provides login times comparable to PIN and reasonable memorability" [15]. We found that the security is substantially higher than for similar systems, specifically Android's graphical authentication scheme [30] and user-chosen 4-digit PINs [6].

We deliberately implemented the scheme without any restrictions on the selected passcodes. In particular, choosing the same emoji four times was permitted by our prototype implementation. The study has shown that a small number of passcodes was chosen by a relatively large number of users, specifically repeating the same emoji four times, and also some basic structures on the keyboard. So practical implementations should prohibit the usage of such simple passcodes to increase security. (As our study does not show how users will cope with such restrictions, further studies should investigate these aspects.)

Practical implementations need to take into account that emoji are unicode characters, and font developers provide their own implementation. Consequently, their actual representation differs between systems (cf. [16]), and can cause misleading interpretations by users [20]. This may have an adverse impact on the memorability, so using a fixed set of images instead of fonts is advised.

The studied scheme is, as most schemes implemented for mobile authentication, subject to shoulder surfing. We implemented a common basic defense against shoulder surfing by displaying the selected emoji for half a second only and replacing it with a checkmark after that time. We expect that this protects against shoulder surfing to a similar extent as it does for PIN and password entry, but due to the graphical nature of emoji they might be easier to recognize in a shoulder surfing attack. At the same time, as there are more emoji than digits, recognition might even get more difficult. Future research needs to clarify if this protection is sufficient, or if further protective measures are required.

VII. Conclusion

In this work, we studied a recently proposed authentication scheme using emoji. Specifically, we studied its resistance to guessing attacks for user-chosen secrets. To estimate the user bias when selecting emoji passcodes, we conducted an online study with 795 participants. We used Markov models based on the emoji content as well as its position on the grid and developed a hybrid model combining both features. We found bias in the collected passcodes, but this bias was less pronounced than in other schemes used on mobile devices, such as Android's graphical authentication scheme and user-chosen 4-digit PINs. We observed various passcode selection strategies, which are quite different from PIN selection strategies. Our results indicate that simple passcodes consisting of only one or two different emoji should be avoided to increase the resistance to guessing attacks.

Acknowledgments

This work was supported by the German Research Foundation (DFG) Research Training Group GRK 1817/1.

References

[1] Apple Inc., "Use Touch ID on iPhone and iPad," Jan. 2016, https://support.apple.com/en-us/HT201371, as of January 26, 2017.

[2] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," in *USENIX Conference on Offensive Technologies (WOOT '10)*. Washington, D.C., USA: USENIX Association, Aug. 2010, pp. 1–7.

[3] A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith, "Practicality of Accelerometer Side Channels on Smartphones," in *Annual Computer Security Applications Conference (ACSAC '12)*. Orlando, Florida, USA: ACM Press, Dec. 2012, pp. 41–50.

[4] J. Bonneau, M. Just, and G. Matthews, "What's in a Name? Evaluating Statistical Attacks on Personal Knowledge Questions," in *Financial Cryptography (FC '10)*. Tenerife, Canary Islands, Spain: Springer, Jan. 2010, pp. 98–113.

[5] J. Bonneau, S. Preibusch, and R. Anderson, "A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs," in *Financial Cryptography and Data Security (FC '12)*. Kralendijk, Bonaire: Springer, Mar. 2012, pp. 25–40.

[6] Daniel Amitay, "Most Common iPhone Passcodes," Jun. 2011, http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes, as of January 26, 2017.

[7] D. Davis, F. Monrose, and M. K. Reiter, "On User Choice in Graphical Password Schemes," in *USENIX Security Symposium (SSYM '04)*. San Diego, California, USA: USENIX Association, Aug. 2004, pp. 151–164.

[8] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems," *International Journal of Human-Computer Studies*, vol. 63, no. 1–2, pp. 128–152, Jul. 2005.

[9] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling User Choice in the PassPoints Graphical Password Scheme," in *Symposium on Usable Privacy and Security (SOUPS '07)*. Pittsburgh, Pennsylvania, USA: ACM Press, Jul. 2007, pp. 20–28.

[10] P. Dunphy and J. Yan, "Do Background Images Improve 'Draw a Secret' Graphical Passwords?" in *ACM Conference on Computer and Communications Security (CCS '07)*. Alexandria, Virginia, USA: ACM Press, Oct. 2007, pp. 36–47.

[11] M. Dürmuth, F. Angelstorf, C. Castelluccia, D. Perito, and A. Chaabane, "OMEN: Faster Password Guessing Using an Ordered Markov Enumerator," in *International Symposium on Engineering Secure Software and Systems (ESSoS '15)*. Milan, Italy: Springer, Mar. 2015, pp. 119–132.

[12] Intelligent Environments, "Now You Can Log Into Your Bank Using Emoji," Jun. 2015, http://www.intelligentenvironments.com/info-centre/press-releases/now-you-can-log-into-your-bank-using-emoji-1, as of January 26, 2017.

[13] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*, 1st ed. Springer, 2011.

[14] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in *USENIX Security Symposium (SSYM '99)*. Washington, D.C., USA: USENIX Association, Aug. 1999, pp. 1–14.

[15] L. Kraus, R. Schmidt, M. Walch, F. Schaub, C. Krügelstein, and S. Möller, "Implications of the Use of Emojis in Mobile Authentication," in *Who are you?! Adventures in Authentication Workshop (WAY '16)*. Denver, Colorado, USA: USENIX Association, Jun. 2016.

[16] P. Laperdrix, W. Rudametkin, and B. Baudry, "Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints," in *IEEE Symposium on Security and Privacy (SP '16)*. San Jose, California, USA: IEEE Computer Society, May 2016.

[17] J. Ma, W. Yang, M. Luo, and N. Li, "A Study of Probabilistic Password Models," in *IEEE Security and Privacy (SP '14)*. Berkeley, CA, USA: IEEE, May 2014, pp. 689–704.

[18] Megan Logan, "Where to Find That Missing Emoji You Neeeded," Jun. 2015, https://www.wired.com/2015/06/find-missing-emoji/, as of January 26, 2017.

[19] W. Melicher, D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin, L. F. Cranor, and M. L. Mazurek, "Usability and Security of Text Passwords on Mobile Devices," in *ACM Conference*

on Human Factors in Computing Systems (CHI '16). Santa Clara, California, USA: ACM Press, May 2016, pp. 527–539.

[20] H. Miller, J. Thebault-Spieker, S. Chang, I. Johnson, L. Terveen, and B. Hecht, "'Blissfully Happy' or 'Ready to Fight': Varying Interpretations of Emoji," in *AAAI Conference on Web and Social Media (ICWSM '16)*. Cologne, Germany: AAAI, May 2016, pp. 259–268.

[21] A. Narayanan and V. Shmatikov, "Fast Dictionary Attacks on Passwords Using Time-space Tradeoff," in *ACM Computer and Communications Security (CCS '05)*. Alexandria, Virginia, USA: ACM, Nov. 2005, pp. 364–372.

[22] Real User Corporation, "The Science Behind Passfaces," Jun. 2004, http://www.realuser.com/published/ScienceBehindPassfaces.pdf, as of January 26, 2017.

[23] Sternbergh, Adam, "Smile, You're Speaking Emoji," Nov. 2014, http://nymag.com/daily/intelligencer/2014/11/emojis-rapid-evolution.html, as of January 26, 2017.

[24] Steven Sinofsky, "Signing In With a Picture Password," Dec. 2011, https://blogs.msdn.microsoft.com/b8/2011/12/16/signing-in-with-a-picture-password/, as of January 26, 2017.

[25] H. Tao and C. Adams, "Pass-Go: A Proposal to Improve the Usability of Graphical Passwords," *International Journal of Network Security*, vol. 7, no. 2, pp. 273–292, Sep. 2008.

[26] J. Thorpe and P. C. van Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in *USENIX Security Symposium (SSYM '04)*. San Diego, California, USA: USENIX Association, Aug. 2004, pp. 135–150.

[27] ——, "Towards Secure Design Choices for Implementing Graphical Passwords," in *Annual Computer Security Applications Conference (ACSAC '04)*. Tucson, Arizona, USA: IEEE Computer Society, Dec. 2004, pp. 50–60.

[28] ——, "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords," in *USENIX Security Symposium (SSYM '07)*. Boston, Massachusetts, USA: USENIX Association, Aug. 2007, pp. 103–118.

[29] Twitter, Inc., "Twitter Emoji (Twemoji)," Mar. 2016, https://github.com/twitter/twemoji, as of January 26, 2017. Graphics are licensed under CC-BY 4.0 https://creativecommons.org/licenses/by/4.0/.

[30] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns," in *ACM Conference on Computer and Communications Security (CCS '13)*. Berlin, Germany: ACM Press, Nov. 2013, pp. 161–172.

[31] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, ""I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab," in *USENIX Symposium on Usable Privacy and Security (SOUPS '15)*. Ottawa, Canada: USENIX Association, Jul. 2015, pp. 123–140.

[32] E. von Zezschwitz, P. Dunphy, and A. De Luca, "Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices," in *Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '13)*. Munich, Germany: ACM Press, Aug. 2013.

[33] E. von Zezschwitz, M. Eiband, D. Buschek, S. Oberhuber, A. De Luca, F. Alt, and H. Hussmann, "On Quantifying the Effective Password Space of Grid-based Unlock Gestures," in *Conference on Mobile and Ubiquitous Multimedia (MUM '16)*. Rovaniemi, Finland: ACM Press, Dec. 2016.

[34] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Basic Results," in *Human-Computer Interaction International (HCII '05)*. Las Vegas, Nevada, USA: Mira Digital Publishing, Jul. 2005, pp. 1–12.

[35] ——, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," in *Symposium on Usable Privacy and Security (SOUPS '05)*. Pittsburgh, Pennsylvania, USA: ACM Press, Jul. 2005, pp. 1–12.

[36] ——, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," *International Journal of Human-Computer Studies*, vol. 63, no. 1–2, pp. 102–127, Jul. 2005.

[37] Z. Zhao, G.-J. Ahn, J.-J. Seo, and H. Hu, "On the Security of Picture Gesture Authentication," in *USENIX Security Symposium (SSYM '13)*. Washington, D.C., USA: USENIX Association, Aug. 2013, pp. 383–398.

APPENDIX

TABLE III. DETAILED RESULTS OF THE QUESTIONNAIRE

	No.	Percent
Age	795	100 %
< 20	78	9.81 %
20–30	580	72.96 %
31–40	97	12.20 %
41–50	20	2.52 %
> 50	20	2.52 %
I identify my gender as ...	795	100 %
male	492	61.89 %
female	292	36.73 %
other	11	1.38 %
Where are you from?	795	100 %
Germany	721	90.69 %
Austria	10	1.26 %
Finland	10	1.26 %
France	4	0.50 %
United Kingdom	4	0.50 %
Other	46	5,79 %
How did you choose your emoji-passcode?	795	100 %
Created a story	268	33.71 %
Repeating event of my life	54	6.79 %
Emoji I use the most while texting	44	5.53 %
Selection as random as possible	83	10.44 %
Important things of my life	234	29.43 %
Via the position within the grid	19	2.39 %
Via a visual pattern	31	3.90 %
Other	62	7.80 %
How often do you use emoji?	795	100 %
Very frequently	249	31.32 %
Frequently	266	33.46 %
Occasionally	154	19.37 %
Rarely	85	10.69 %
Never	41	5.16 %
Remembering a 4-digit PIN is?	795	100 %
Very hard	6	0.75 %
Hard	51	6.42 %
Moderate	248	31.19 %
Easy	294	36.98 %
Very easy	196	24.65 %
Working with emoji was enjoyable?	795	100 %
Strongly agree	152	19.12 %
Agree	359	45.16 %
Neither agree or disagree	187	23.52 %
Disagree	89	11.19 %
Strongly disagree	8	1.01 %
How do you assess your technical understanding?	795	100 %
Excellent	236	29.69 %
Above average	322	40.50 %
Average	212	26.67 %
Below average	22	2.77 %
Very poor	3	0.38 %
How much effort do you spend to protect your data?	795	100 %
Extreme	84	10.57 %
Substantial	361	45.41 %
Some	275	34.59 %
Little	67	8.43 %
None	8	1.01 %
Why have you cleared your passcode? [if pressed]	115	14.47 %
Clicked the wrong emoji	45	39.13 %
Spontaneously changed my mind	53	46.09 %
Other	17	14.78 %

TABLE IV. EMOJI AS USED IN THE USER STUDY.

No.	Unicode	Graphic	Description
1	U+1F602		“FACE WITH TEARS OF JOY”
2	U+1F648		“SEE-NO-EVIL MONKEY”
3	U+1F44C		“OK HAND SIGN”
4	U+1F355		“SLICE OF PIZZA”
5	U+1F4A9		“PILE OF POO”
6	U+26BD		“SOCCER BALL”
7	U+1F697		“AUTOMOBILE”
8	U+1F495		“TWO HEARTS”
9	U+1F354		“HAMBURGER”
10	U+1F37A		“BEER MUG”
11	U+1F3B8		“GUITAR”
12	U+1F3AE		“VIDEO GAME”
13	U+2600		“BLACK SUN WITH RAYS”
14	U+1F476		“BABY”
15	U+1F52B		“PISTOL”
16	U+1F6B2		“BICYCLE”
17	U+1F339		“ROSE”
18	U+1F4AA		“FLEXED BICEPS”
19	U+1F3B6		“MULTIPLE MUSICAL NOTES”
20	U+1F437		“PIG FACE”

We used the vector graphics version of the Twemoji [29] font to ensure the same representation on all devices.