Implications of the Use of Emojis in Mobile Authentication

Lydia Kraus
Technische Universität Berlin
lydia.kraus@telekom.de

Robert Schmidt
Technische Universität Berlin
robert-schmidt@telekom.de

Marcel Walch
Ulm University
marcel.walch@uni-ulm.de

Florian Schaub
Carnegie Mellon University
fschaub@cs.cmu.edu

Christopher Krügelstein
Technische Universität Berlin
c.kruegelstein@campus.tu-berlin.de

Sebastian Möller
Technische Universität Berlin
sebastian.moeller@tu-berlin.de

1. INTRODUCTION

Mobile authentication has attracted considerable attention in the usable security research community, given that users spend a considerable amount of time unlocking their phones – one hour per month on average even without considering authentication overhead [6]. A variety of mobile authentication methods for screen locks are available in today's smartphones. Knowledge-based authentication mechanisms, such as PIN, passwords and unlock pattern (on Android), have been widely deployed; Biometric authentication methods, such as fingerprint recognition (e.g., Apple's TouchID) and face recognition (mainly deployed on Android devices) emerged recently as alternatives to knowledge-based mobile authentication methods, but they typically rely on PINs or passwords for fallback authentication [1]. Thus, knowledge-based authentication mechanisms for smartphones are not likely to be replaced in the near future depite their shortcomings: PINs have a small theoretical password space and are susceptible to user choice [4]; random passwords are more secure but harder to remember [15]; and unlock patterns have a long entry time compared to PINs [14].

The use of Emojis has been proposed for use in mobile authentication [8]. Emojis are small icons, e.g., smileys or objects, that are often used in digital communication to express emotions [9]. Our interest lies in better understanding the implications of Emoji-based passwords. Can they potentially enhance the user experience of knowledge-based authentication or is their use just a gimmick? In the following, we reflect on the implications of using Emojis to create a positive mobile authentication experience for users. We further present the results of a user study for which we developed a study artifact named EmojiAuth (cf. Figure 1).

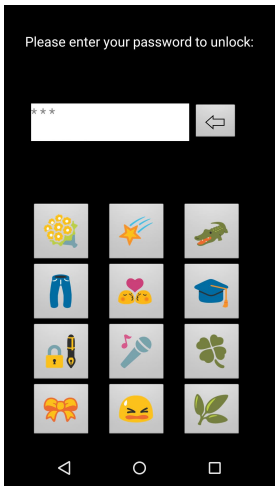

Figure 1: EmojiAuth: Each user has an individual keyboard. Emojis for EmojiAuth are depicted in the Noto Emoji fonts (`https://github.com/googlei18n/noto-emoji`).

2. EMOJIS IN AUTHENTICATION

2.1 Opportunities

Positive user experience: We hypothesize that using Emojis in authentication will lead to a positive and pleasing user experience and a positive perception of an emoji-based authentication method because Emojis are very popular among users [7]. They give text-based communication meaning [5], as they enable people to express moods, emotions and nuances in written text. Even without text, Emojis convey meaning. A smiling face can express joy or happiness, a sad face sadness or grief. Thus, they provide meaning per se and do not need to be made meaningful by users by connecting them with personal information, as it is often done for PINs [4].

High memorability: We expect that Emojis can leverage the opportunities of graphical authentication: graphics are easier to remember compared to alphanumeric passwords [3]. Moreover, Emoji passwords can leverage small stories. Constructing stories (similar to mnemonic phrases [15]) should help to increase memorability.

High theoretical password space: Regarding security, the large amount of available Emojis (currently more than 1,200 [13]) results in a large theoretical password space.

2.2 Requirements

Short login time: Authentication time in the mobile context should be kept short, i.e. not longer than PIN entry time [6]. However, while using more Emojis on the keyboard results in a larger theoretical password space, password entry time for keyboards with many keys is quite high [10]. Thus,

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

there needs to be a trade-off between theoretical password space and short login time. Also fixed keyboard positions for Emojis are preferable [11] as fixed positions lead to shorter login times [12].

System feedback and shoulder surfing resistance: For entering a password, users need to know how many digits of their password they have already entered. Also feedback on the pressed button is preferable, as it allows users to notice mistakes and correct them if necessary. Former work shows that shoulder-surfing attackers who focus on the entry field have a higher success rate [10]. Thus, it is preferable that the entered charactered (i.e. the Emoji) is masked with an asterisk. Also, magnification of pressed buttons should be avoided as magnification has been linked to higher shoulder-surfing susceptibility [10].

User choice resilience: That users favor certain icons over others is evident from related work [2]. If similar popularity effects would hold in the user choice of Emoji-based passwords, the skewed password distribution would result in an increased vulnerability for guessing attacks, similar to image selection and image hotspot issues in graphical authentication schemes [3]. Thus, an emoji-based authentication method needs to address this issue. Bicakci et al. [2] proposed an icon-based authenticaion scheme for computer use. The user interface for password entry showed icons (similar to Emojis) from 15 different categories. Drawing the available icons from different categories was supposed to reduce the hotspot problem, but for self-selected passwords the study participants still favored some icons over others. Our suggestion is to address the problem of possible hotspots, i.e., salient icons being favored, by creating an individual keyboard for each user, which is initialized during enrollment. Individual keyboards generated from the very large set of Emojis enable a larger practical password space as single Emojis have a low probability to appear on each keyboard. Thus, the probability that single, well-known Emojis are favored across the whole user population decreases.

2.3 Practical challenges

Even though Emojis are available in Unicode [13], their graphical representation depends on the deployed Emoji font. On different platforms, different Emoji fonts may be installed, thus Emojis may look different on different devices and operating systems. This leads to a number of challenges in the implementation: First, users may prefer certain fonts over others, thus users may be annoyed if they cannot find their favorite font on their platform. Second, as different fonts look quite different, transferring passwords may be difficult as it might be impossible to recognize the password-Emojis in unfamiliar fonts. Furthermore, when individual keyboards are used, they need to be transferred between platforms in a secure way (similar to moving encryption keys between platforms).

3. USER STUDY

We developed a study artifact named EmojiAuth to explore the implications of Emoji-based mobile authentication (cf. Figure 1) addressing the described requirements. We conducted a between-subjects study (n=53) comparing EmojiAuth to PIN entry as a baseline. We find that EmojiAuth provides login times comparable to PIN and reasonable memorability. Our results indicate that once participants were familiar with EmojiAuth, they perceived EmojiAuth as providing a more positive user experience compared to PIN. Furthermore, the results suggest that users have a variety of password selection strategies which differ in a number of points from PIN selection strategies. This encourages further investigation into the topic of Emoji-based mobile authentication w.r.t. to user experience, password selection, and creative solutions for the practical challenges.

4. REFERENCES

[1] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. *Proc. USEC*, 2015.

[2] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz. Towards usable solutions to graphical password hotspot problem. In *COMPSAC'09.* , volume 2, pages 318–323, 2009.

[3] R. Biddle, S. Chiasson, and P. C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44(4):19, 2012.

[4] 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*, pages 25–40. 2012.

[5] P. Cocozza. 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: 2016-02-19).

[6] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith. It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Proc. SOUPS*, pages 213–230, 2014.

[7] A. H. Huang, D. C. Yen, and X. Zhang. Exploring the potential effects of emoticons. *Information & Management*, 45(7):466–473, 2008.

[8] 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: 2016-02-19).

[9] Oxford Dictionaries. `http://www.oxforddictionaries.com/definition/english/emoji`. (accessed: 2016-03-02).

[10] F. Schaub, R. Deyhle, and M. Weber. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proc. MUM*, 2012.

[11] F. Schaub, M. Walch, B. Könings, and M. Weber. Exploring the design space of graphical passwords on smartphones. In *Proc. SOUPS*, 2013.

[12] E. Stobert and R. Biddle. Memory Retrieval and Graphical Passwords. In *Proc. SOUPS*, 2013.

[13] The Unicode Consortium. UTR #51: Unicode Emoji (Revision 5). Technical report, 2015.

[14] 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 *Proc. mobileHCI*, pages 261–270, 2013.

[15] J. Yan et al. Password memorability and security: Empirical results. *IEEE Security & privacy*, (5):25–31, 2004.