Using Graphics and Gestures to Improve Knowledge-based Authentication for Mobile Devices

Emanuel von Zezschwitz

INTRODUCTION AND PROBLEM STATEMENT

Since smartphones and tablets nowadays store huge sets of potentially sensitive data, user authentication has become an elemental part of mobile interaction. Despite biometric approaches, like Apple's *Touch ID*[1], knowledge-based authentication like PIN or Patterns are widely used. Drawbacks of biometric approaches are expensive hardware, the need for personal information (e.g. finger print) and the risk of false-acceptance which makes even state-of-the-art solutions relatively easy to circumvent[2]. Even Apple's iPhone 5s still relies on knowledge-based authentication for fallback, after restarts or when more than 48 hours have elapsed since the last unlock[1].

Therefore, knowledge-based authentication could notionally be very secure and superior to biometric approaches. However, the human factor can downgrade these theoretical advantages and can make password-based solutions ineffective.

For example, most people choose trivial numbers as passwords (e.g. birthdays) which are easy to remember, but also easy to guess [2]. Furthermore, password disclosure is a serious problem, since people write down their secrets [2] or the authentication process is easy to observe [3]. Since device unlocks happen many times a day, good performance and ease of use are prerequisites of every mobile authentication system.

To summarize, a great authentication system must provide passwords which are (a) easy to remember, but at the same time (b) hard to guess. Interaction must be designed in a way that the authentication process does (c) not reveal the actual secret. In addition, such a system must be (d) fast and easy to use on mobile devices.

RESEARCH GOALS, APPROACH AND METHODOLOGY

The direct interaction style of touchscreen-based mobile devices makes graphical and gesture-based passwords a promising alternative to the solely use of PIN [6]. Exemplary advantages of such authentication systems are improved memorability [6] and a larger password space [1]. One prominent representative of gesture-based graphical passwords is the Android pattern. Though, serious drawbacks of this method have already been shown [10].

The goal of my work is to analyze the impact of visualizations and interaction strategies on system security and usability. Based on the evaluation of current authentication systems and user behavior, novel concepts are developed and analyzed to overcome current issues. Thereby, a deep understanding of gesture-based user authentication is gathered.

The design space implies password aspects as well as visualizations and user interactions during enrollment and authentication. Special attention is paid to the evaluation of such systems. Following a structured user-centered approach, I started analyzing specific problems (e.g. password exposure) and developed specific solutions. The process utilizes prototyping, lab- and field studies as well as focus groups and questionnaires. Based on my findings, I will be able to formulate generalized statements on the design and evaluation of gesture-based graphical authentication methods and the impact of human factors.

RELATED WORK

Graphical authentication can be classified into searchmetric, locimetric and drawmetric systems [8]. The widespread system on current devices, Android's pattern-unlock, is a drawmetric system. It is based on simple touch gestures and can be seen as a usability-optimized version of the Draw-a-Secret (DAS) [7].

Up to date, only a few papers deal with specific aspects of graphical and gesture-based authentication for mobile devices. Most of them are concerning password disclosure and are therefore based on lab studies. For example, Bianchi et al. [3] propose a PIN entry method, which is resilient against shoulder surfing and Aviv et al. [1] analyzed smudge attack vulnerability of Android patterns. Overall, research still lacks a generalized evaluation and design approach and a deeper understanding of real-world aspects (e.g. password selection) of such systems.

PRELIMINARY RESULTS

Understanding User Behavior

These studies were conducted to get deeper insights into the problems with current authentication systems on mobile devices and to analyze user behavior and risk perception.

Patterns in the Wild

In this project, we performed a real world longitudinal study of PINs and Patterns [10] to simulate the time period after the assignment of new credentials. Key results were a

[1] http://support.apple.com/kb/ht5949, accessed: 31.03.2014

[2] http://www.ccc.de/de/updates/2013/ccc-breaks-apple-touchid, accessed: 01.04.2014

taxonomy for pattern-based input errors, insights into the relationship between error prevention and error recovery as well as interesting conflicts between perceived and measured performance.

Alphanumeric Authentication on Mobile Devices

This project evaluated the impact of mobile devices on alphanumerical authentication performance and password composition [12]. Key results were that passwords are increasingly created on mobile devices and that users opt for weaker passwords, when authentication has to take place on mobile devices.

Unlock Risks and Authentication Efforts

With this project, we analyzed real world (un)locking behavior and risk perception of smartphone users [5]. Key results are that users perform many unlocks a day and shoulder surfing is possible in many scenarios. However, it was considered a risk in only 11 out of 3410 occurrences.

Password Exposure

The goal of these projects was to protect knowledge-based authentication against password exposure.

Smudge Attacks

Multiple authentication methods were designed to leave smudge traces that are not easy to interpret [9]. Key results were insights into the feasibility of randomization in user authentication. The kind of randomization has significant impact on the perception and the performance of such systems. To get further insights into the learnability of randomized authentication mechanism the systems were improved and tested in the wild.

Shoulder Surfing

We developed an authentication concept for shoulder surfing resistant PIN-entry using of-the-shelf smartphones. User interaction is based on simple gestures which make the deduction of the input difficult. The system is significantly more secure against shoulder surfing and comparable fast to already deployed concepts. Key results are based on unexpected user behavior which was triggered by specific design decisions. In addition, a concept for back-of-device authentication was proposed to counteract shoulder surfing [4].

CURRENT AND FUTURE PROJECTS

[redacted]

[redacted]

[redacted]

CONCLUSION

The results indicate that graphical and gesture-based password systems are a usable and secure alternative to alphanumeric authentication. Based on graphical representations and touch gestures, I am able to exploit a large design space to find usable and secure solutions against current threats. My PhD thesis will contribute to the field of usable security by showing ways to (a) design such secure and usable authentication methods and by (b) specifying best practices in evaluating novel concepts in the lab and in the field.

REFERENCES

1. Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. In *Proc.* WOOT'10. USENIX Association, Berkeley, CA, USA, 1-7.
2. Adams, A., and Sasse, M. A. Users are not the enemy. Commun. ACM 42, 12 (Dec. 1999), 40–46.
3. Bianchi A, Oakley I., Kostakos V., and Soo Kwon D. 2010. The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In Proc. TEI '11. ACM, New York, NY, USA
4. De Luca A., von Zezschwitz E., Nguyen N. D. H., Maurer M., Rubegni E., Scipioni M. P., Langheinrich M. 2013. Back-of-Device Authentication on Smartphones. In Proc. CHI '13. ACM, New York, NY, USA, USA, 2389-2398.
5. Harbach, M., von Zezschwitz, E., De Luca, A., Smith M. 2014. It'sa Hard Lock Life: A Field Study of Smartphone (Un) Locking Behavior and Risk Perception. In Proc. SOUPS '14, USENIX Association, Menlo Park, CA, USA, 213-230.
6. Schaub, F., Walch, M., Könings, B., and Weber, M. Exploring the design space of graphical passwords on smartphones. In Proc. SOUPS '13, ACM (New York, NY, USA, 2013), 11:1–11:14.
7. Jermyn I., Mayer A., Monrose F., Reiter M. K., and Rubin A. D. 1999. The design and analysis of graphical passwords. In Proc. SSYM'99, Vol. 8. USENIX Association, Berkeley, CA, USA, 1-1.
8. Renaud, K., and De Angeli, A. Visual passwords: cure-all or snake-oil? Commun. ACM 52, 12 (Dec.2009), 135–140.
9. Standing, L. Learning 10,000 pictures. The Quarterly Journal of Experimental Psychology 25 (1973), 203–222.
10. von Zezschwitz E., Koslow A., De Luca A., Hussmann H. 2013. Making Graphic-Based Authentication Secure against Smudge Attacks. In Proc. IUI '13. ACM, New York, NY, USA. 277-286.
11. von Zezschwitz E, Dunphy P, and De Luca, A. 2013. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In Proc. MobileHCI '13. ACM, New York, NY, USA, 261-27
12. von Zezschwitz, E., De Luca A., Hussmann H. 2014. Honey, I Shrunk the Keys: Influences of Mobile Devices on Password Composition and Authentication Performance. To appear in Proc. NordiCHI '14. ACM