On Smartphone Users’ Perception of Smart Lock for Android

Masoud Mehrabi Koushki
University of British Columbia
Vancouver, B.C., Canada
mehrabi@ece.ubc.ca

Konstantin Beznosov
University of British Columbia
Vancouver, B.C., Canada
beznosov@ece.ubc.ca

Borke Obada-Obieh
University of British Columbia
Vancouver, B.C., Canada
borke@ece.ubc.ca

Jun Ho Huh
Samsung Research
Seoul, South Korea
junho.huh@samsung.com

Abstract

Deployed on millions of Android smartphones, *Smart Lock* is the first commercialized solution to leverage a combination of implicit (i.e., context-based) and explicit (e.g., biometric-based) authentication factors to unlock the phone. Given its unique capabilities, we conducted a mixed-method study, involving cognitive walkthroughs, think-aloud sessions, and interviews, to understand how the security, utility and privacy of SL is perceived by smartphone users. Our results suggest that there are various misconceptions regarding Smart Lock and its methods as our participants found it difficult to understand the semantics of context-based unlocking. The semantics of inter-operation of SL methods was even harder to grasp. Our findings provide evidence for the importance of clear semantics communication in smartphone unlocking and can inform the design of future context-based unlocking schemes on smartphones.

Author Keywords

Smart Lock; User Perception; Cognitive Walkthrough; Think aloud; Usable Security

Introduction

Users’ attitude towards smartphone unlocking has been well studied, demonstrating that smartphone users perceive unlocking as a burden. A study by Harbach and colleagues [11] found their participants to be spending around 2.9% of their smartphone interaction time with unlocking alone. Consequently, inconvenience is among the main reasons that cause nearly 40% of smartphone users to not use an unlocking mechanism on their phones [12, 16, 6, 11, 19].

To lessen this unlocking burden, the research community have proposed Implicit Authentication (IA) schemes which leverage behavioural biometrics such as touch gestures [7], gait patterns [5], body movement [18], and biomedical signals [17] to automatically and implicitly unlock the phone, without requiring any explicit action.

Smart Lock (SL) is the first commercialized solution that enables implicit unlocking on smartphones. It is also the first to combine implicit and explicit unlocking methods on smartphones. SL can leverage both implicit data, such as location, Bluetooth signals, and body movement, or explicit data, such as user's facial or vocal features, to unlock the phone. Since SL is part of Google Play Services, it is deployed on hundreds of millions of Android devices.

Surprisingly, while SL has been part of Android for nearly 5 years and while there exists theoretical evidence of efficacy of IA on smartphones [3, 13, 2, 1], no in-depth evaluation has ever been done to understand how implicit unlocking or a mixture of implicit and explicit unlocking, as provided by SL, is perceived or understood by smartphone users.

To the best of our knowledge, there are no studies evaluating Smart Lock, in any regard. We found that the usability and user perception of face [4] and voice [20] unlock (used by SL methods TF and VM, respectively) has been studied before, but we didn't find any existing literature that evaluates the perception of commercialized location- or device-based unlocking on smartphones.

As such, our study is the first to provide insight into how location- and device-based authentication and a mix between different implicit and explicit authentication methods is perceived by smartphone users. Our findings can inform the design of future implicit and mixed-method unlocking schemes.

Smart Lock for Android

Labeled as a "Personal Unlocking" experience by Google, Smart Lock for Android was first introduced during Google's annual I/O conference keynote in 2014 [8]. In its essence, Smart Lock is designed to reduce the number of times users have to unlock their phones by automatically unlocking the phone (or at least keeping it unlocked) when the surrounding environment is "deemed" secure. Some SL methods have the ability to automatically lock the phone as well. The following five unlocking methods are included in Google's implementation of SL:

- **On-body Detection (BD)** is a context-based method that can keep the phone unlocked while it is "on-person" (a.k.a., in movement).
- **Trusted Places (TP)** is a context-based method that uses location signals to automatically unlock the phone at certain locations (based on GPS coordinates).
- **Trusted Devices (TD)** is a context-based method that uses Bluetooth signal to automatically lock and unlock the phone when a certain Bluetooth device is nearby.
- **Trusted Face (TF)** is an explicit unlocking method that uses face recognition to unlock the phone.
- **Voice Match (VM)** is an explicit unlocking method that uses voice recognition to unlock the phone.

SL is considered an important part of the Android's user experience as its existence is actively advertised on Android smartphones. For example, whenever a new Bluetooth device is paired with an SL-capable Android phone, a notification is shown, encouraging the user to add the device as trusted to automatically unlock the phone.

Methodology

Research Questions

Our methodology design was focused on answering the following research questions:

RQ1 How well does SL UI support exploratory learning?

RQ2 How clearly are the semantics of each SL method communicated to the user?

RQ3 How clearly are the semantics of inter-operation of SL methods communicated to the user?

RQ4 How do participants perceive Smart Lock's utility, security, and privacy?

Data Collection and analysis

The data collection and analysis of this study were approved by our university's ethics research board, before any data collection took place. We used a combination of cognitive walkthrough, think-aloud and interview sessions to address our research questions. We selected Cognitive Walkthrough (CW) [15, 21] as our main method of data collection due to it being task-oriented and focused on learnability of the UI (RQ1).

A traditional CW only involves HCI-proficient participants. However, as we intended to analyze users' perception (RQ2-RQ4), we believed it was necessary to also involve general smartphone users in the study. As such, we used an alternative variant of CW that also allows for participation of general smartphone users. The variant we selected is Cognitive Walkthrough with Users (CWU) [9, 14, 15]. CWU involves conducting traditional CW group sessions with HCI proficients, in addition to conducting think-aloud individual sessions with regular users (not proficient in HCI or usability).

Overall, we recruited 26 participants, 10 for cognitive walkthrough and 16 for think-aloud sessions. While all CW participants were graduate students, only about 1/3 were students among the participants of think-aloud sessions. There was a wide variety of occupations among non-students, ranging from a health consultant, to a physical instructor, and a flight attendant.

To analyze the data, We first transcribed the audio recordings from all the CW and think-aloud sessions, then anonymized and analyzed the transcripts. We also analyzed notes written by participants in the problem reporting forms. Overall, we analyzed the transcripts of approximately 14 hours of audio recordings. We chose Thematic Analysis [10] as our analysis method of these two datasets.

Results

In this section we report on how SL and its implicit and mixed-method unlocking capabilities were perceived by our participants.

Semantics and Mental Model

To evaluate whether participants understood the semantics of implicit unlocking and the mixture of different unlocking methods in SL, we specifically asked participants how they thought each SL method locked and unlocked the phone. Interestingly, while prior experience with the underlying biometric technologies helped some participants understand the semantics of explicit unlocking methods (i.e., VM and TF), but TP, which is an implicit unlocking method, showed to be the easiest to understand for participants. This does not mean however, that their mental models of TP were adequate as most of them were confused about the range of TP. In general, no matter implicit or explicit, troubling was the confusion about the precise conditions under which SL methods lock and unlock the phone. The semantics of the inter-operation of several SL methods was even more confusing for the participants as the UI does not specifically communicate how SL will behave if multiple SL methods are enabled at the same time.

Security and Privacy

Overall there was no consensus among participants on whether implicit SL methods were more secure than explicit ones. Some participants perceived SL as more secure than traditional unlocking methods because they thought it was more difficult to mimic a voice or hack a location unlocking system, than to guess a PIN or password. At the same time, other participants perceived SL as less secure for the same reasons (e.g., voice being easy to mimic). A similar division was observed in regards to the privacy of the data collected by SL methods (e.g., the possibility of voice or face data being leaked from the phone).

Utility

To evaluate participants' appreciation of implicit and mixed-method unlocking, as provided by SL, we asked participants directly about the benefits of SL. Most participants cited convenience as the main benefit of SL as they thought SL made it easier to unlock the phone. Some participants suggested it could be faster to unlock the phone using SL rather than a PIN or a password. Another utility benefit of SL was perceived to be the increase in the alternatives to the secret-based unlocking methods. In general however, in most contexts and environments, SL was perceived to be of not enough value as some participants commented that currently, (un)locking a smartphone isn't particularly a difficult task to accomplish. One of the most repeated concerns was that, participants were not sure about SL's use cases and when or where they could use each of the SL methods.

Reliability and Trust

The themes of perceived reliability of SL methods and, as a consequence, trust in the technology kept reappearing in the collected data. While inter-related with security and privacy and semantics and mental model, these themes deserve their own role in the relationship between SL and its users. Participants found SL lacking reliability, precision, and accuracy. Participants explicitly expressed on several occasions their distrust in SL or its specific methods.

Discussion

Through this study, we found that providing context-aware (un)locking for smartphones is tricky because:

1. It is challenging to make users appreciate the value of context-aware unlocking. For biometric methods, the convenience they provide over a PIN or a pattern is obvious. Finding use cases for context-aware methods however seems to be more difficult.

2. It difficult for users to understand how context-aware unlocking works, resulting in their inability to judge when their phone would be locked or unlocked. This lack of understanding can reduce users' trust and confidence in the technology as they might perceive unexpected behaviours as malfunctions.

3. Users' security and privacy needs need to be carefully considered. Most of our participants were worried that, by using context-based unlocking, family

members or co-workers might be able to access their private information. Some participants were also concerned with phone manufacturers' use of their data.

We concluded that it is even trickier to combine multiple (un)locking methods because:

1. The semantics of inter-operation of different unlocking methods is difficult to understand. We found it was difficult for our participants to predict how SL would behave if multiple methods were enabled at the same time which could lead to misconceptions and inadequacy of mental models.
2. It is difficult to make the UI consistent, when implicit and explicit unlocking factors are combined. Such complications seem to be caused by difference in capability among such methods.

Conclusion

Smart Lock (SL) is the first commercialized smartphone unlocking scheme that can automatically unlock the phone using a combination of implicit factors (e.g., location and body-movement) and explicit biometrics (e.g., facial recognition), as alternatives to knowledge-based authentication (e.g., PIN and password). To understand how SL's combination of unlocking methods is perceived by smartphone users, we conducted a mixed-method study with 26 participants, consisting of cognitive walkthroughs, think-aloud sessions, and interviews. Results of our investigation suggest that while SL is a promising technology, there are certain requirements for a successful deployment of any SL-like unlocking scheme. Firstly, the technology's added convenience and utility need to be communicated to users in clear and accessible way. Secondly, the implementation needs to be reliable and trusted by users. And finally, the UI needs to help users develop and maintain adequate mental models, so that users can become proficient and comfortable with the technology, learn how to utilize it, and can avoid making dangerous security errors.

REFERENCES

1. Lalit Agarwal, Hassan Khan, and Urs Hengartner. 2016. Ask me again but don't annoy me: Evaluating re-authentication strategies for smartphones. In *Symposium on Usable Privacy and Security (SOUPS)*.
2. Heather Crawford and Karen Renaud. 2014. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management* 1, 1 (2014), 7.
3. Heather Crawford, Karen Renaud, and Tim Storer. 2013. A framework for continuous, transparent mobile device authentication. *Computers & Security* 39 (2013), 127–136.
4. Alexander De Luca, Alina Hang, Emanuel Von Zezschwitz, and Heinrich Hussmann. 2015. I feel like I'm taking selfies all day!: towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 1411–1414.
5. Mohammad Omar Derawi, Claudia Nickel, Patrick Bours, and Christoph Busch. 2010. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 306–311.

6. Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are you ready to lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 750–761.

7. Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security* 8, 1 (2013), 136–148.

8. Google. Google I/O 2014 Keynote. `https://www.youtube.com/watch?time_continue=1659&v=biSpvXBGpE0`. (????). Accessed: 2019-02-14.

9. T Granollers and J Lorés. 2005. Cognitive Walkthrough With Users: an alternative dimension for usability methods. In *Proc. HCI International, Las Vegas*.

10. Greg Guest, Kathleen M MacQueen, and Emily E Namey. 2011. *Applied thematic analysis*. sage.

11. Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *Symposium on usable privacy and security (SOUPS)*. 213–230.

12. Eiji Hayashi, Oriana Riva, Karin Strauss, AJ Brush, and Stuart Schechter. 2012. Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2.

13. Hassan Khan, Aaron Atwater, and Urs Hengartner. 2014. A comparative evaluation of implicit authentication schemes. In *International Workshop on Recent Advances in Intrusion Detection*. Springer, 255–275.

14. Wallace Lira, Renato Ferreira, Cleidson de Souza, and Schubert Carvalho. 2014. Experimenting on the cognitive walkthrough with users. In *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*. ACM, 613–618.

15. Thomas Mahatody, Mouldi Sagar, and Christophe Kolski. 2010. State of the art on the cognitive walkthrough method, its variants and evolutions. *Intl. Journal of Human–Computer Interaction* 26, 8 (2010), 741–785.

16. Ahmed Mahfouz, Ildar Muslukhov, and Konstantin Beznosov. 2016. Android users in the wild: Their authentication and usage behavior. *Pervasive and Mobile Computing* 32 (2016), 50–61.

17. Arsalan Mosenia, Susmita Sur-Kolay, Anand Raghunathan, and Niraj K Jha. 2017. CABA: Continuous authentication based on BioAura. *IEEE Trans. Comput.* 66, 5 (2017), 759–772.

18. Abena Primo, Vir V Phoha, Rajesh Kumar, and Abdul Serwadda. 2014. Context-aware active authentication using smartphone accelerometer measurements. In *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*. 98–105.

19. Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. 2012. Progressive Authentication: Deciding When to Authenticate on Mobile Phones.. In *USENIX Security Symposium*. 301–316.

20. Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. 2012. Biometric authentication on a mobile device: a study of

user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference*. ACM, 159–168.

21. Chauncey Wilson. 2013. *User interface inspection methods: a user-centered design method*. Newnes.