Don't Use Fingerprint, it's Raining! How People Use and Perceive Context-Aware Selection of Mobile Authentication

Sarah Prange*
Bundeswehr University
Munich, Germany
sarah.prange@unibw.de

Lukas Mecke*
Bundeswehr University
Munich, Germany
lukas.mecke@unibw.de

Alice Nguyen
LMU Munich
Munich, Germany
alice.nguyen@gmx.de

Mohamed Khamis
University of Glasgow
Glasgow, UK
Mohamed.Khamis@glasgow.ac.uk

Florian Alt
Bundeswehr University
Munich, Germany
florian.alt@unibw.de

ABSTRACT

This paper investigates how smartphone users perceive switching from their primary authentication mechanism to a fallback one, based on the context. This is useful in cases where the primary mechanism fails (e.g., wet fingers when using fingerprint). While prior work introduced the concept, we are the first to investigate its perception by users and their willingness to follow a system's suggestion for a switch. We present findings from a two-week field study (N=29) using an Android app, showing that users are willing to adopt alternative mechanisms when prompted. We discuss how context-awareness can improve the perception of authentication reliability and potentially improve usability and security.

CCS CONCEPTS

• **Human-centered computing** → **Field studies**; Smartphones; • **Security and privacy** → *Biometrics*.

KEYWORDS

Biometrics; Fingerprint; Context-Aware Authentication; User Perception; Field Study; Mobile Devices; Android

ACM Reference Format:
Sarah Prange, Lukas Mecke, Alice Nguyen, Mohamed Khamis, and Florian Alt. 2020. Don't Use Fingerprint, it's Raining! How People Use and Perceive Context-Aware Selection of Mobile Authentication. In *International Conference on Advanced Visual Interfaces (AVI '20), September 28-October 2, 2020, Salerno, Italy*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3399715.3399823

1 INTRODUCTION

Users protect access to a plethora of personal data on their smartphones, using authentication methods such as knowledge-based or biometric schemes. However, authentication on mobile devices is error-prone [10, 18] and perceived as time-consuming – in particular, because interactions on smartphones are usually short [10].

*Both authors contributed equally to this research.

AVI '20, September 28-October 2, 2020, Salerno, Italy

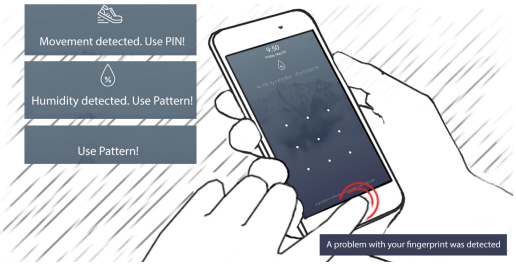

Figure 1: We investigate how people use and perceive context-aware suggestions to switch mobile authentication mechanisms. This is useful when the primary mechanism is likely to fail (e.g., wet fingers when using fingerprint).

Beyond improving the security of existing mechanisms [15, 31], concepts have, hence, been suggested to reduce authentication overhead (e.g., [4, 13]). One option is to use *context*, which refers to any (explicit or implicit) information that characterises the user's current situation [27]. Factors include environmental properties (e.g., location), but also human factors [28]. Context can be leveraged to a) skip authentication in certain situations (e.g., *Google Smart Lock* [8]) or b) choose adequate (e.g., biometric) authentication [32].

While related work suggests that this is technically possible [32], we look into how context-aware selection of authentication is used and perceived by mobile users in the wild. In a two-week field study (N=29), we tested an Android app, suggesting users of fingerprint authentication to switch to their knowledge-based fallback based on context information. Our results show that users are willing to switch and found our app helpful and beneficial in daily use. We discuss context factors, authentication switches and use cases.

2 CONTEXT-AWARE AUTHENTICATION

In this section, we report on results from our literature review on context-awareness and results of an online survey (N=35) and focus group (N=5) informing our design of a prototype to suggest switches to a fallback based on context factors (e.g. rain, see Figure 1).

Adapting mobile authentication based on context is very useful as we authenticate around 40 times a day [10] in varying contexts in daily life [12]. Authentication could thus leverage context-awareness to be more usable as well as more secure. Several authentication models consider location [11] or proximity [14]. Patented models consider potential risks as context [30]. Google's context-aware authentication on Android, *Smart Lock* [8], allows users to

choose contexts in which their phones stay unlocked. Wójtowicz and Joachmiak [32] presented a generic model that allows choosing the "optimal biometrics" for mobile authentication based on contextual factors (e.g., no voice biometrics in silent mode).

2.1 Challenges of Daily Authentication

2.1.1 Online Survey. Related work found that fingerprint authentication is sometimes problematic, e.g., while walking, in dark environments or after using moisturiser [1, 2]. Only artificial environments were tested. To understand the contexts in which users encounter difficulties when authenticating on arbitrary devices, we conducted an online survey (N=35, 20 female, mean age=28). We did not limit this to biometrics to get a broad spectrum of experiences.

Respondents were asked to describe any problems they encountered in as much detail as possible, followed by open-ended questions about the context of the incident and the perceived reason behind the problem. We asked for time of day, weather and location as those might have an impact. Participants were recruited via university mailing lists and took part in a raffle for three 20€ vouchers.

We discarded one response since it did not contain a problem situation. In the remaining 34 responses, smartphone-related issues were predominant (22 out of 34). The majority of those were about issues with lockscreens (14) and fingerprint authentication (12). From those we identified wet or dry fingers as the main source of failed authentication attempts, e.g., P30: "*When [my] hands are sweaty the smartphone can't be unlocked using fingerprint. This mostly happens in crowded [public] transport.*". Reported contextual causes for wet or dry fingers were temperature (rain or muggy weather), location (kitchen, bathroom, or public transport) and activities (walking, applying moisturiser, washing hands, or exercising).

2.1.2 Focus Group. We conducted a follow-up focus group (N=4, 2 female, mean age=26.3) to further investigate problems with fingerprint and coping strategies. Participants were compensated with 10 €. We asked about *issues* encountered when authenticating using fingerprint authentication on mobile devices and their *coping strategies* to overcome said issues. We concluded by collecting feedback on the idea of *leveraging context to suggest switches to fallback*.

Named *problems* were dirty/wet fingers, similar to the online survey. Reasons were cooking, winter season (dry fingers) and neurodermatitis. The predominant *coping strategy* encompassed repeated scanning of the finger. Other options were registering multiple fingers, addressing the problematic state (e.g., drying or moisturising fingers) or using different methods (e.g., a fallback mechanism). Participants were very positive about the suggested switches to fallback based on context information. Their design priorities were saving time (e.g., by omitting the manual swipe gesture to get to the fallback), having visual indication of the currently used method and receiving (brief) explanations for system decisions.

In addition to confirming the online survey's results, we found that switches to fallback mechanisms is not among common coping strategies due to the required effort. However, participants thought positively about alleviating the need to actively switch the authentication method. Overall, participants favoured concepts that are transparent and save time, which aligns with previous work [10, 19].

2.2 Lessons Learnt

From related work we learn that fingerprint authentication is error prone (e.g., for wet or moisty fingers [2]), as also reported by our survey and focus group participants. However, switches to fallback are tedious. We further learn that context can be considered for authentication (e.g., location, proximity or other sensor values [11, 14, 17, 30, 32]) and that it is technically possible (e.g., choosing biometric mechanisms based on context [32]). Thus, several novel authentication mechanisms evolve (cf. this survey [29], examples include [5, 15]) to counteract threats (such as shoulder surfing [31]) and/or usability issues. Further directions have been suggested [21]. Context factors could be leveraged to further increase usability (e.g., use fingerprint when on the go or knowledge in case fingerprint might fail) or prevent threats (e.g., if possible observers are around, use fingerprint instead of knowledge). In addition to confirming prior work, our online survey and focus group show that there is a need for transparent and straightforward ways to switch to fallback mechanisms when authentication is not possible due to contextual factors, such as the user's state, location or activity.

3 PROTOTYPE: CONTEXTLOCK

As outlined in section 2, we see great potential in leveraging context to (proactively) suggest switches of authentication methods. As a prerequisite for this, the aim of our work is to evaluate user perception towards authentication switches in the wild. While related work showed that choosing an appropriate authentication scheme based on context is possible [32], it is not known whether users will follow derived suggestions *in the wild*. Participants of our focus group also wished for explanation, which was highlighted by prior work to be important for intelligent systems in general (e.g., [25]). Indeed, one of the usability heuristics is to maintain the "visibility of the system status" [22]. Thus, we also investigated in our field study if explaining suggested switches to fallback mechanisms impacts users' decision to follow this suggestion.

3.1 Field Study

3.1.1 Apparatus. Informed by our survey and focus group we developed an Android application, *ContextLock*, to provide suggestions to switch to fallback based on context. Due to Android's security limitations and ethical concerns, we did not replace the lock screen, but simulated a failed fingerprint authentication attempt (by showing a fallback screen) after successful user authentication.

We built an Android fallback authentication screen allowing for PIN [26], pattern, and fingerprint [20] authentication. The presented fallback was determined by a question in the initial questionnaire to match participants' routine. Fingerprint was provided, as we did not want to force a switch but allow users to retry using fingerprint (which we found to be a common coping strategy) if they wished.

To acquire the user's context, we integrated OpenWeatherMap [23] and Google's activity recognition API [9]. If no fitting context data was available, we randomly chose either *"Humidity detected"* or *"Movement detected"* as mock context reason (see Figure 1).

3.1.2 Study Design and Procedure. We designed our study as a two week within-subject field study with the *presence of explanation* for suggested switch to fallback as independent variable (*generic*

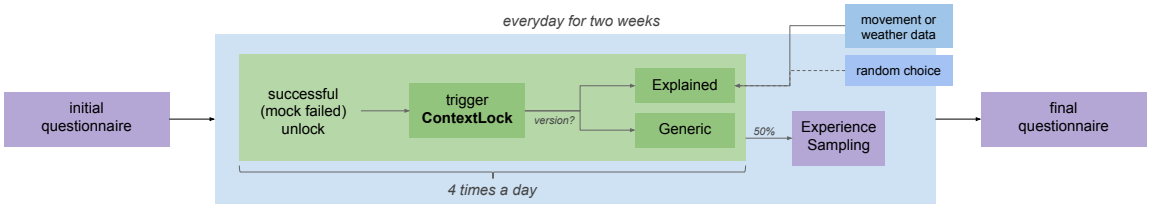

Figure 2: Procedure of our two week field study, including all data sources.

vs. *explained*, cf. Figure 2). Dependent variables were participants' subjective ratings from questionnaires and experience sampling probes as well as decisions on whether to switch to the fallback.

The study duration was initiated and concluded with a questionnaire, asking for demographics and a final comparison of the study conditions. During the study period, participants were presented with a proposed switch to their fallback four times (average authentication failures as reported in the initial questionnaire) in random intervals between 8am and 9pm every day. Explanations were given depending on the current study condition (see Figure 1), which would automatically switch midway through the study. After successful unlock (by either using the suggested fallback or fingerprint) a dismissable experience sampling (ES) questionnaire was shown with 50% probability. Conditions were counterbalanced.

3.1.3 Participants. We recruited participants via university mailing lists and social media. From a total of 42 installations, 29 participants (12 female) between 18 to 45 years (mean=23.6) completed the field study. Participants were located in the UK, Central America, Russia and Italy when using the app. The majority came from Germany. Participants used PIN fallback (16) and pattern fallback (13).

3.1.4 Limitations. Due to strict battery handling on Huawei phones, our application was sometimes terminated by the operating system. To counteract this, we showed an icon in the task bar to indicate that the app was active and kindly asked participants to manually restart it if the symbol disappeared. We analysed all records with at least four (of seven) days of data for each condition.

We decided to trigger our app in certain intervals rather than triggering based on context factors. We made this decision to ensure consistent data collection, though a real application would do it the other way round. Furthermore, our sample was self-selected and biased towards younger European students.

3.2 Results

Data sources were the initial and final questionnaire as well as experience sampling probes (compare Figure 2). Significance was determined using Wilcoxon and McNemar's tests and is reported at a significance level of p = .05.

3.2.1 Prior Authentication Behaviour. We found the most common coping strategy (stated by 24 of the 29 participants) with fingerprint failure to be switching to the fallback after *multiple* failed attempts. Less participants would switch immediately (2), try again later (2) or ignore it (1). Some participants reported lockouts (complete loss of access to their device) at least once a day (5) or more than once a week (4). Nine participants experienced lockouts once a month at most and eleven never encountered this problem. The responses about perceived fingerprint error frequency were also mixed, from once (8) or more than once (7) a day, once (7) or more than once (6) a week, to less than once a month (1).

Overall, this shows that fingerprint errors and, in some cases, resulting lockouts are indeed a problem and there is room for current coping strategies to be improved.

3.2.2 Experience Sampling. After data clean-up, we had a total of 253 complete sets of experience sampling data for the *generic* version and 261 for the *explained* version. On a 5-point likert scale (0=strongly disagree; 5=strongly agree) the situational *annoyance* level was rated as neutral for both versions (*generic*: M = 2.02, SD = 0.976; *explained*: M = 2.03, SD =1.126). We found no significant difference between the versions.

Though both were rated about neutral, a significant difference can be observed for the perceived *appropriateness* (Z = -3.031, p = .002). The *generic* design was perceived significantly more adequate (M = 2.13, SD = 1.073; *explained*: M = 1.85, SD = 1.143).

Participants were asked for possible reasons of fingerprint failure while using the *generic* version of *ContextLock*. Overall, wet (74) and dirty (62) fingers constituted the majority of perceived reasons. Weather and ambient influences such as rain (5), snow (2), humidity (14) and heat (14) were indicated as influential factors which is in line with prior work [32]. Other reasons were "movement" and "damaged fingers from climbing". This confirms our survey's results.

3.2.3 Switching Behaviour. We recorded if participants followed our suggestion to switch to their fallback mechanism. We collected 645 datasets for the *generic* (no explanation) and 611 for the *explained* design. Users showed no significant differences (p > 0.05) in following our suggestion with 67.13% (SD= 0.470) and 67.76% (SD = 0.468) of the cases, respectively.

3.2.4 Overall Rating. Figure 3 shows participants' overall rating of the two conditions with regards to understandability, appropriateness, increased success, less failures, annoyance and if they used the fallback. We found no significant impact of the conditions.

Besides conditional questions, we also asked for overall opinions. In summary, users found *ContextLock* somehow helpful (median=4), thought that the automatic recommendation was beneficial compared to their current lock screen (median=4) and would use a similar system in the future (median=4). The majority preferred the *explained* version (22) over the *generic* one (6); another six participants remained undecided.

15 participants made comments about situations in which they would have wanted *ContextLock* to activate (but it did not). Reasons

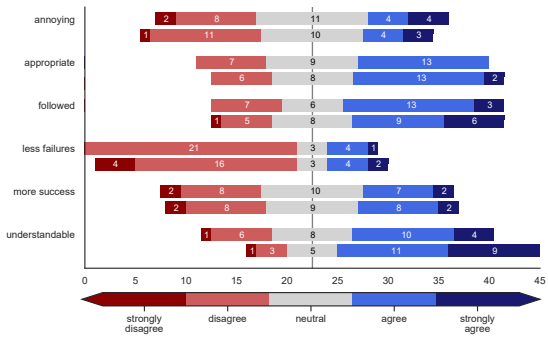

Figure 3: Responses for each Likert item in the final questionnaire for the *generic* (upper)/ *explained* (lower) version.

were "humid" environments, "wet fingers while walking in the rain" or "misplacement" of the finger on the sensor. Participants also mentioned increased battery usage and a wish to customise *ContextLock* to more closely resemble their real lockscreen. Three participants liked the usability of the app and two commented to have enjoyed the design. We saw no feedback indicating participants noticed some of the given reasons being random.

3.2.5 Summary. We found no significant differences between app versions but giving explanations was overall preferred. Participants liked the concept and found it useful and worth using in the future. This was also reflected in about 67% of the cases in which participants followed our suggestion and switched to their fallback.

4 DISCUSSION

For current biometric authentication mechanisms, users need to switch to a knowledge-based fallback in case the primary mechanism does not work (as expected). This takes time and is annoying to users, as reported in our focus group. We suggest to consider context to switch authentication mechanisms, not only in case fallback authentication is necessary, but on a per use case basis. We now discuss further aspects of our concept as well as opportunities for future work.

4.1 Appropriateness of Suggestions

Participants perceived suggested switches significantly less appropriate when they were given an explanation. However, this only holds true for the experience sampling and not the final rating. We believe the reason for this is the use of fake context information (when no real data was available), hampering trust in the system [16]. While we did not find significant differences, participants rated the explained version more understandable and perceived less failures. It was also rated as the preferred choice. This shows that participants generally appreciate explanations, though the use of real context data would be necessary to make the system transparent (as, e.g., suggested by Nielsen [22]). Specific use cases and related context factors are subject to future work.

4.2 Extending the Concept

From related work, we learn that environmental as well as technical factors [11, 27, 28, 32] may influence context-aware applications and, more specifically, the choice of authentication.

4.2.1 It's Raining vs I'm Tired. We propose to consider not only technical, but also further human factors. This may, on one hand, refer to users' concrete characteristics, as, e.g., hand size has an influence on accuracy of touch interaction [3, 24]. On the other hand, more abstract factors like users' current cognitive and physiological state may be worth considering when choosing authentication. As an example, using fingerprint may be more usable than entering a PIN for switching a song while doing sport. Users who are at home and tired may as well not want to enter a knowledge-based secret, but rather rely on their trusted environment.

4.2.2 Socially-Aware Authentication. Frankel and Maheswaran [7] showed that human social interaction is a feasible authentication factor, thus also social context could be leveraged for authentication switches. This may, on one hand, lead to a switch to an easier, potentially less secure mechanism, if trusted entities are present. On the other hand, users may want to hand over their device to someone else. While it is easy to share a knowledge-based secret, a biometric secret cannot be shared. Context-aware authentication could thus switch to knowledge-based models if the device is in the hands of a trusted, but foreign entity.

4.3 System vs User-Initiated Switches

Our prototype *suggested* the switch to knowledge-based fallback, but did not force users to do so. However, our participants did follow the recommendation in the majority of the cases (67%). Other approaches may provide users with the possibility to choose context-factors to be considered themselves (compare to, e.g., *Google Smart Lock* or aCapella [6]). At the same time, context-aware authentication could also force the switch of authentication mechanism based on appropriate factors. This would not leave the choice to switch to the user, but to the context-aware authentication system.

5 CONCLUSION AND FUTURE WORK

In this work, we presented *ContextLock*, which helped us to understand users' willingness to follow (mock) context-aware suggestions for authentication switches in the wild. From our 14-day field study (N=29), we found that users appreciated *ContextLock*'s suggestions and were wiling to follow them. We suggest to further evaluate context-aware authentication based on human factors to enhance both, usability and security, of mobile authentication mechanisms.

Future work could investigate deploying authentication mechanisms that are more secure but less usable only when there is a significant need according to the context (e.g., when a threat, such as shoulder surfing, is likely).

ACKNOWLEDGMENTS

This research was supported by the Royal Society of Edinburgh (Award number 65040) and by the Deutsche Forschungsgemeinschaft (DFG) under grant agreement no. 316457582 and 425869382.

REFERENCES

[1] Matthias Baldauf, Sebastian Steiner, Mohamed Khamis, and Sarah-Kristin Thiel. 2019. Investigating the User Experience of Smartphone Authentication Schemes-The Role of the Mobile Context. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. https://hdl.handle.net/10125/59918

[2] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. (2015). https://doi.org/10.14722/usec.2015.23003

[3] Daniel Buschek and Florian Alt. 2015. TouchML: A Machine Learning Toolkit for Modelling Spatial Touch Targeting Behaviour. In *Proceedings of the 20th International Conference on Intelligent User Interfaces (IUI '15)*. ACM, New York, NY, USA, 110–114. https://doi.org/10.1145/2678025.2701381

[4] Daniel Buschek, Fabian Hartmann, Emanuel von Zezschwitz, Alexander De Luca, and Florian Alt. 2016. SnapApp: Reducing Authentication Overhead with a Time-Constrained Fast Unlock Option. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 3736–3747. https://doi.org/10.1145/2858036.2858164

[5] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2937–2946. https://doi.org/10.1145/2556288.2557097

[6] Anind K. Dey, Raffay Hamid, Chris Beckmann, Ian Li, and Daniel Hsu. 2004. A CAPpella: Programming by Demonstration of Context-aware Applications. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04)*. ACM, New York, NY, USA, 33–40. https://doi.org/10.1145/985692.985697

[7] Andrew Dathan Frankel and Muthucumaru Maheswaran. 2009. Feasibility of a Socially Aware Authentication Scheme. In *2009 6th IEEE Consumer Communications and Networking Conference*. 1–6. https://doi.org/10.1109/CCNC.2009.4784910

[8] Google. 2020. Choose when your Android device can stay unlocked. https://support.google.com/android/answer/9075927. (2020). Accessed 17 January 2020.

[9] Google. 2020. Google Activity Recognition API. https://developers.google.com/android/reference/com/google/android/gms/location/ActivityRecognitionClient. (2020). Accessed 17 January 2020.

[10] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 4806–4817. https://doi.org/10.1145/2858036.2858267

[11] Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, and Ian Oakley. 2013. CASA: Context-aware Scalable Authentication. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, Article 3, 10 pages. https://doi.org/10.1145/2501604.2501607

[12] Eiji Hayashi and Jason Hong. 2011. A Diary Study of Password Usage in Daily Life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2627–2630. https://doi.org/10.1145/1978942.1979326

[13] Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow. 2009. Implicit Authentication for Mobile Devices. In *Proceedings of the 4th USENIX Conference on Hot Topics in Security (HotSec'09)*. USENIX Association, Berkeley, CA, USA, 9–9. http://dl.acm.org/citation.cfm?id=1855628.1855637

[14] Andre Kalamandeen, Adin Scannell, Eyal de Lara, Anmol Sheth, and Anthony LaMarca. 2010. Ensemble: Cooperative Proximity-based Authentication. In *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services (MobiSys '10)*. ACM, New York, NY, USA, 331–344. https://doi.org/10.1145/1814433.1814466

[15] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 2156–2164. https://doi.org/10.1145/2851581.2892314

[16] René F. Kizilcec. 2016. How Much Information?: Effects of Transparency on Trust in an Algorithmic Interface. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 2390–2395. https://doi.org/10.1145/2858036.2858402

[17] Yuk L Li and Padmaja Ramadas. 2012. Context aware biometric authentication. (Aug. 28 2012). US Patent 8,255,698.

[18] 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. https://doi.org/10.1016/j.pmcj.2016.06.017 Mobile Security, Privacy and Forensics.

[19] George Musumba and Henry Nyongesa. 2013. Context awareness in mobile computing: A review. *International Journal of Machine Learning and Applications* 2, 1 (2013), 5. https://doi.org/10.4102/ijmla.v2i1.5

[20] Amirhossein Naghshzan and Akshay Pathak. 2020. Lock-Screen. https://github.com/amirarcane/lock-screen. (2020). Accessed 17 January 2020.

[21] Michele Nappi, Stefano Ricciardi, and Massimo Tistarelli. 2018. Context awareness in biometric systems and methods: State of the art and future scenarios. *Image and Vision Computing* 76 (2018), 27 – 37. https://doi.org/10.1016/j.imavis.2018.05.001

[22] Jakob Nielsen. 1994. Enhancing the Explanatory Power of Usability Heuristics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '94)*. Association for Computing Machinery, New York, NY, USA, 152–158. https://doi.org/10.1145/191666.191729

[23] OpenWeather. 2020. Weather API. https://openweathermap.org/api. (2020). Accessed 17 January 2020.

[24] Sarah Prange, Daniel Buschek, and Florian Alt. 2018. An Exploratory Study on Correlations of Hand Size and Mobile Touch Interactions. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia (MUM 2018)*. ACM, New York, NY, USA, 279–283. https://doi.org/10.1145/3282894.3282924

[25] Pearl Pu and Li Chen. 2006. Trust Building with Explanation Interfaces. In *Proceedings of the 11th International Conference on Intelligent User Interfaces (IUI '06)*. ACM, New York, NY, USA, 93–100. https://doi.org/10.1145/1111449.1111475

[26] Aritra Roy, Merab Tato Kutalia, shpp vsmaga, and Idan Ben Shalom. 2020. PINLockView. https://github.com/aritraroy/PinLockView. (2020). Accessed 17 January 2020.

[27] B. Schilit, N. Adams, and R. Want. 1994. Context-Aware Computing Applications. In *1994 First Workshop on Mobile Computing Systems and Applications*. 85–90. https://doi.org/10.1109/WMCSA.1994.16

[28] Albrecht Schmidt, Michael Beigl, and Hans-W Gellersen. 1999. There is more to context than location. *Computers & Graphics* 23, 6 (1999), 893 – 901. https://doi.org/10.1016/S0097-8493(99)00120-X

[29] S. W. Shah and S. S. Kanhere. 2019. Recent Trends in User Authentication - A Survey. *IEEE Access* 7 (2019), 112505–112519. https://doi.org/10.1109/ACCESS.2019.2932400

[30] Zhexuan Song and Jesus Molina. 2011. Method and apparatus for context-aware authentication. (Dec. 22 2011). US Patent App. 12/816,966.

[31] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1403–1406. https://doi.org/10.1145/2702123.2702212

[32] Adam Wójtowicz and Krzysztof Joachimiak. 2016. Model for Adaptable Context-based Biometric Authentication for Mobile Devices. *Personal Ubiquitous Comput.* 20, 2 (April 2016), 195–207. https://doi.org/10.1007/s00779-016-0905-0