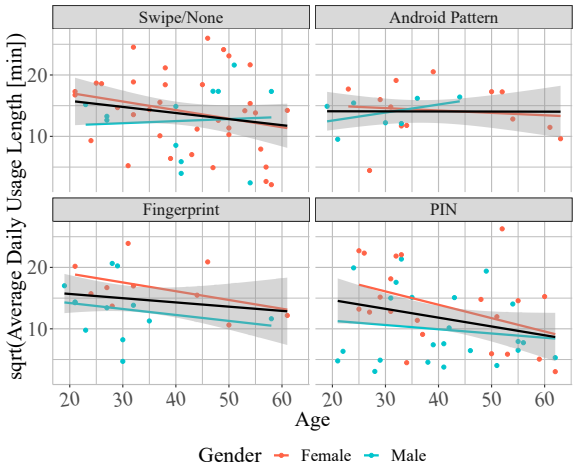


**Figure 5: Multiple linear regression model of the square root of average daily usage length on age, unlocking mechanism (base category "Swipe/None") and gender (base category "Female"):** $sqrt\,(AverageDailyUsageLength) = 18.869 - 0.108 * Age + 0.161 * (AndroidPattern) + 1.019 * Fingerprint - 1.256 * PIN - 2.867 * Male$, $N = 133$ **(*AndroidPattern*, *Fingerprint*, *PIN* and *Male* are binary variables with values {0, 1}). The black line represents the fitted model for participants in each unlocking mechanism group, and the grey area represents the 95% confidence interval. The other colored lines represent the simple linear regression models of the square root of average daily usage length on age for female participants and male participants in each unlocking mechanism group.**

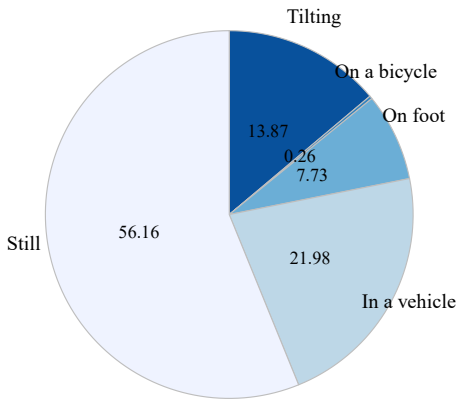


**Figure 6: Distribution of activities during unlock, $N = 116$.**

*Error Rates While At Still vs. On the Move.* To assess how error rates correlated with activity types, we again excluded participants who used "Swipe/None", as errors are not possible with this unlocking method.

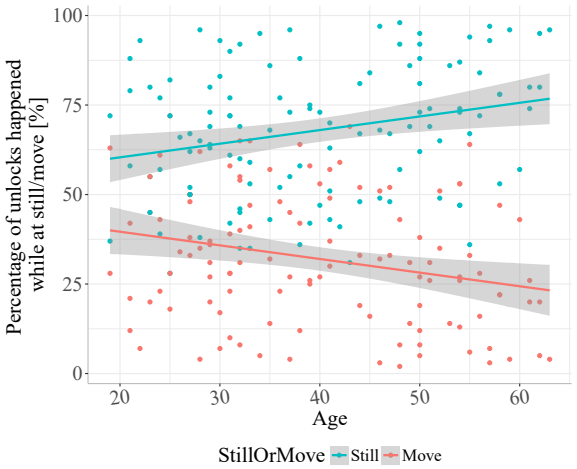


**Figure 7: Distribution of unlocks that happened while at still/move, $N = 116$. The lines represent the fitted simple linear regression model of the percentage of unlocks on age for each activity category, and the grey area represents the 95% confidence interval.**

We then counted the number of failed unlocking attempts and total unlocking attempts that each participant performed, while they were in "still" and "move" states. Afterwards, we calculated the likelihood of making an error, for each participant for each of the two activity categories. However, a paired-samples t-test did not reveal any significant differences in the likelihoods that participants would make an error, while their devices were *still* ($M = 4.37$, $SD = 7.16$) and *moving* ($M = 4.78$, $SD = 7.27$); $t\,(70) = 1.08$, $p = .28$.

*How Age Predicts Whether Authentication is Used While At Still vs On the Move.* To evaluate how often participants unlocked while they were in still and moving states, we calculated the percentage of unlocks for each activity category per user over the whole study period. Figure 7 shows the distribution of unlocks at still and on the move, with respect to participants' age. To further understand how age interacted with activity types (*still/move*), we fitted a binary logistic regression model to predict whether authentication would be used when users were at still and on the move based on age, with *move* as the reference activity category. The analysis revealed that age had a significant effect on predicting whether authentication happened while at still or on the move. Specifically, with one-year increase in age, participants were 1.5% more likely to use authentication when they were *still* than moving. Table 4 gives an overview of the fitted model.

| *Variable* | *Estimate* | *Std. Err.* | *z value* | *Odds Ratio* |
|---|---|---|---|---|
| Intercept | .078 | .024 | 3.268* | 1.081 |
| Age | .015 | .001 | 23.772* | 1.015 |

**Table 4: Binary logistic regression model: whether authentication is used while at still vs on the move by age. An "*" denotes significance ($p < .05$).**

## 6 DISCUSSION

The results presented in this paper provide the first real world data and detailed insights on the link between individual smartphone authentication patterns and age, thus, corroborating and extending on the previous study [6] that hypothesized that age might be an important factor. In addition, we investigated a broader scope of unlocking mechanisms, than previous work [5, 6, 10, 12], in terms of how participants' in-situ (un)locking behaviour differs among unlocking mechanisms. We are the first to extend these findings to "Fingerprint" users, despite that we had relatively smaller "Fingerprint" sample size (about 56% of participants' devices supporting such mechanism).

### Age Makes a Difference

First of all, and most importantly, our data suggests that smartphone usage patterns, indeed, in many cases significantly correlate with age.

Specifically, we found a significant correlation of age with the following parameters: the choice of unlocking mechanism, session length, number of sessions per day, daily usage length, auto/manual lock, state of movement (at still vs. on the move), the choice of unlocking mechanism at still vs. on the move. In addition, we found that participant's gender also significantly correlated with their session length, daily usage length, and the choice of the unlocking mechanism.

That is, our results provide the first quantitative support (based on field measurements of real-world behaviour) for previous recommendations that, while designing new authentication systems for smartphones, demographic differences, such as age, should be taken into account [6]. Furthermore, we emphasize that our work not only confirms the link between age and in-situ authentication behaviour, but also extends the findings to gender. We thus invite more studies to investigate (other) demographic factors, and suggest future work could focus on recruiting even more representative (particularly age-wise) samples to provide further evidence.

### Age and Unlocking Security

One of our results related to age being a good predictor for some choices related to smartphone unlocking mechanism selection, is that older participants were less likely to enable "Fingerprint" authentication on their devices. In addition, older participants significantly more likely relied on the auto lock feature, despite the used unlocking mechanisms, which is in line with [5].

The auto lock feature very specifically represents a trade-off between security and usability. The related question is whether users make educated choices, when making these decisions, or whether other factors are more prominent in the decision-making process.

As a consequence, we argue that future research should look into the popularity of auto lock among older users and their awareness of respective security implications.

### Design and Evaluate for Movement

Another interesting result to highlight is that age was a good predictor for whether device unlocking was used on the move compared to at still.

Our results show that, overall, about 44% of unlocks happened with the devices moving. Furthermore, despite a trend in our data towards more authentication taking place in still states with increasing age, authentication on moving devices was a common task across all age groups.

While one might hypothesize that participants were more likely to make unlocking errors while moving, our findings do not support such a claim. The numbers of failed unlocking attempts when participants' devices were still and when they were moving were very similar, also across age groups. This might indicate that current unlocking mechanisms are robust against errors on the move.

A consequence of this and the fact that people do regularly authenticate themselves while moving, means that newly-designed unlocking mechanisms should be as robust in the presence of movement as existing mechanisms, in order to be acceptable for smartphone unlocking. This requirement not only influences how unlocking systems should be designed (e.g., constant eye contact might not be possible) but also how they are evaluated in studies (in-lab vs. in the wild).

### No One-Fits-All Solution

As mentioned before, we showed that age significantly correlated not only with the choice of unlocking mechanism but also whether and how features such as auto lock were used and whether authentication took place on still or moving devices.

Previous research [7] has concluded that due to user preferences, it is hard (or impossible) to find or build one authentication system that caters to all user needs. Our results add to these previous findings by providing evidence that these usage differences are also linked to age and gender.

While we cannot make claims about the cause of these differences, our findings suggest that these differences are important factors to consider. The findings further our understanding of why offering different unlocking mechanisms

for smartphones seems to be the right thing to do. Users have different preferences and usage behaviour, and this approach allows users to pick the mechanism that best fits their needs and the way they are using their devices.

## 7 LIMITATIONS

While we tried our best to mitigate any potential problems with the study setup, the study has a few limitations that need to be kept in mind when interpreting the results.

First, our server was silently down for 10 days at the end of May, when most of our participants were supposed to complete the study.This unexpected issue forced us to exclude those participants ($N$ = 43) whose data we failed to recover. This could have potentially biased our study sample. However, we do not consider this accident as a major threat to the validity of our results, since we did not find a significant difference between our sample demographics distributions and the US smartphone ownership distributions reported by Pew Research Center.

In addition, the use of MTurk for recruiting could potentially bias our study sample, since MTurk workers tend to be more privacy self-aware than average people [11]. However, we argue that avoiding "privacy" and "security" terms in our advertisement and only a small portion (about one fourth) of participants of the sample coming from MTurk helped limit this bias. Again, as our sample demographic distributions were not significantly different from the US smartphone population, we do not consider this affecting our results' validity either.

To determine session length, we measured the time between the screen on and off (with *keyguard* removed) events. Since this measurement did not remove the screen off timeout from the session length calculations, the reported length of sessions could potentially be longer than of the real sessions. Our comparisons on session lengths among groups might also be biased, as different participants would have set the screen off timeout to different values, varying from 0 seconds to 24 hours.

Due to technical limitations, we were not able to detect the used unlocking mechanisms and the states of auto lock setting programmatically for participants using Android 6 ($N$ = 64) and 7 ($N$ = 31) devices. Therefore, we asked those participants about their unlocking mechanisms (Android 6 and above users) and the auto lock settings (Android 7 and above) in the entry and exit surveys. As a consequence, the correctness of our collected data partially depends on the recollection of the participants. However, the data gives us no reason to believe that they would have incorrectly reported these attributes.

On average, the confidence level of detected activities (still, in a vehicle, on foot, etc.) is 73.31 ($SD$ = 25.16, $Min$ = 21, $Median$ = 75, $Max$ = 100). Therefore, the results of activity analysis are highly dependent on the accuracy of the Android activity recognition API.

Finally, the small "Fingerprint" sample size (75 participants' devices supported Fingerprint-based authentication) could limit the generalizability of our Fingerprint-related findings. Another caveat is that the awareness of biometrics authentication scheme among individuals, especially the seniors, could bias our results as well.

## 8 CONCLUSION

In this paper, we add to the research field of real world unlocking behavior by providing the first detailed look at how age correlates with smartphone users' in situ unlocking behavior. We conducted a longitudinal field study with 134 participants from North America, who installed our study app on their Android phones and ran it for 60+ days. The results of the study suggest that age does indeed significantly correlate with different factors related to smartphone unlocking. In particular, we observed that older users interacted with their devices less frequently. In addition, older participants relied more on the auto lock features and were less likely to enable "Fingerprint" authentication on their devices. We conclude that when designing new authentication systems, varying age-related usage patterns should be taken into consideration.

Based on our results, an interesting area for future work is to explore security perceptions of unlocking mechanisms across age groups. This would allow to identify whether the decisions that people make are conscious or whether they are influenced by other parameters such as usability related factors.

## 9 ACKNOWLEDGMENTS

This research was supported by funding from Google and the NSERC Engage Grant (EG). We would like to thank the anonymous reviewers for their helpful insights and suggestions.

## REFERENCES

[1] 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. http://doi.acm.org/10.1145/2858036.2858164

[2] Pew Research Center. 2013. Smartphone Ownership 2013. http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/

[3] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the Impact of Touch ID on iPhone Passcodes. In *Proceedings of the 2015 Symposium on Usable Privacy and Security (SOUPS '15)*. USENIX Association, Ottawa, ON, Canada, 257–276. https://www.usenix.org/conference/soups2015/proceedings/presentation/cherapau

[4] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*. ACM, New York, NY, USA, 750–761. http://doi.acm.org/10.1145/2660267.2660273

[5] 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. http://doi.acm.org/10.1145/2858036.2858267

[6] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. 2016. Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 4823–4827. http://doi.acm.org/10.1145/2858036.2858273

[7] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Proceedings of the 2014 Symposium on Usable Privacy and Security (SOUPS '14)*. USENIX Association, Menlo Park, CA, USA, 213–230. https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach

[8] Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, and Ian Oakley. 2013. CASA: Context-Aware Scalable Authentication. In *Proceedings of the 2013 Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, 3:1–3:10. http://doi.acm.org/10.1145/2501604.2501607

[9] Eiji Hayashi, Oriana Riva, Karin Strauss, A. J. Bernheim 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 2012 Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, 2:1–2:11. http://doi.acm.org/10.1145/2335356.2335359

[10] Daniel Hintze, Rainhard D. Findling, Muhammad Muaaz, Sebastian Scholz, and René Mayrhofer. 2014. Diversity in Locked and Unlocked Mobile Device Usage. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 379–384. http://doi.acm.org/10.1145/2638728.2641697

[11] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy Attitudes of Mechanical Turk Workers and the U.S. Public. In *Proceedings of the 2014 Symposium on Usable Privacy and Security (SOUPS '14)*. USENIX Association, Menlo Park, CA, USA, 37–49. https://www.usenix.org/conference/soups2014/proceedings/presentation/kang

[12] 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.

[13] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on Mobile Phones: Prevalence and Trends. In *Proceedings of the 2016 Symposium on Usable Privacy and Security (SOUPS '16)*. USENIX Association, Denver, CO, USA, 159–174. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/marques

[14] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2013. Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders. In *Proceedings of the 2013 International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*. ACM, New York, NY, USA, 271–280. http://doi.acm.org/10.1145/2493190.2493223

[15] Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. 2012. Progressive Authentication: Deciding When to Authenticate on Mobile Phones. In *Proceedings of the 2012 USENIX Security Symposium (USENIX Security '12)*. USENIX Association, Bellevue, WA, USA, 301–316. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/riva

[16] Daniel T. Wagner, Andrew Rice, and Alastair R. Beresford. 2014. Device Analyzer: Large-Scale Mobile Data Collection. *ACM SIGMETRICS Performance Evaluation Review* 41 (2014), 53–56.