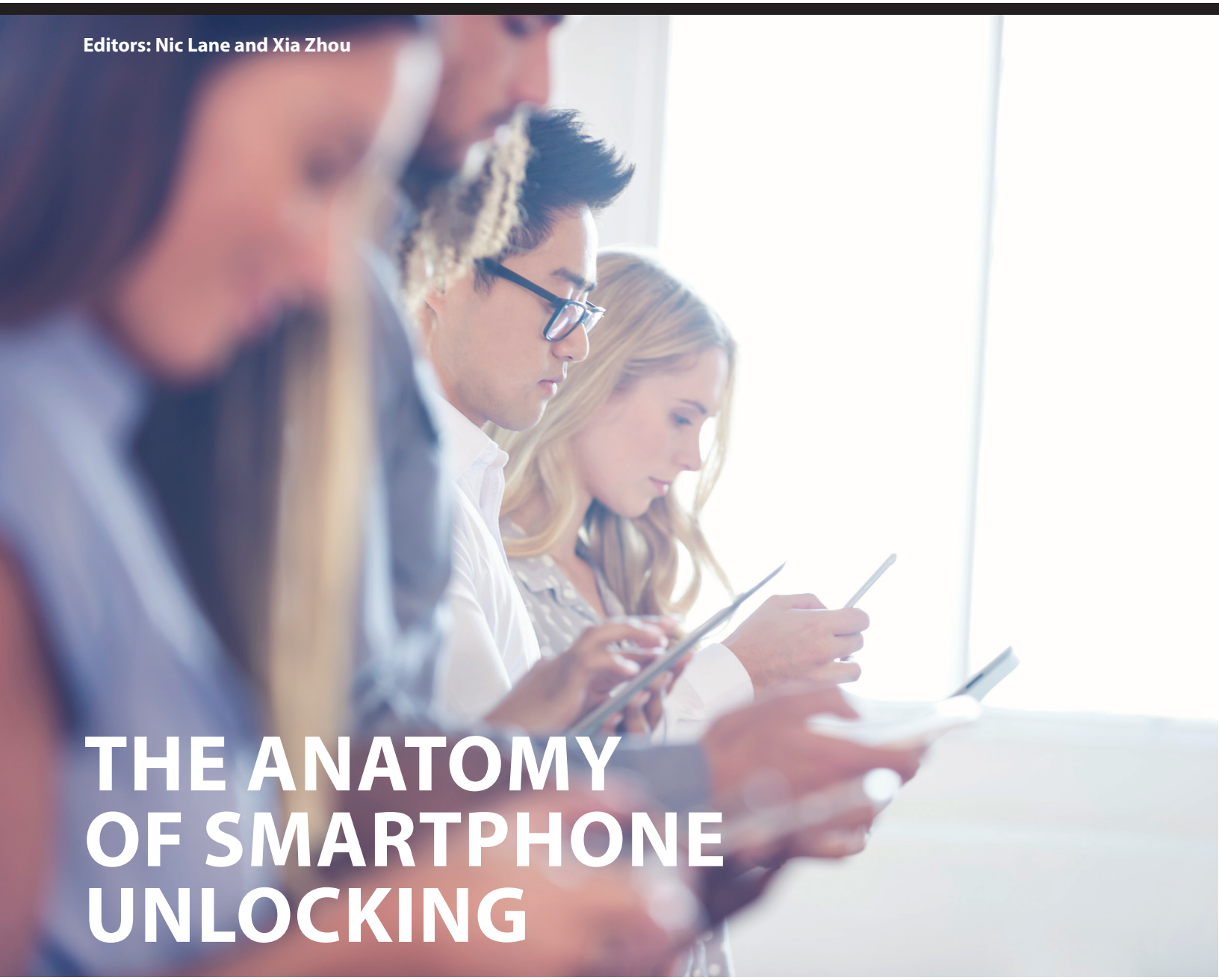
Nathan Malkin *University of California, Berkeley*
Marian Harbach *International Computer Science Institute, Berkeley, CA*
Alexander De Luca *Google, Zurich, Switzerland*
Serge Egelman *University of California, Berkeley, and International Computer Science Institute, Berkeley, CA*

Editors: Nic Lane and Xia Zhou



THE ANATOMY OF SMARTPHONE UNLOCKING

Why and How Android Users Around the World Lock their Phones

Excerpted from "The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens," http://dl.acm.org/citation.cfm?id=2858267 and "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* with permission. http://dl.acm.org/citation.cfm?id=2858273

Photo, istockphoto.com

To prevent unauthorized access to their smartphones, users can enable a "lock screen," which may require entering a PIN or password, drawing a pattern, or providing a biometric. We present the results of two studies that together offer a detailed analysis of the smartphone locking mechanisms currently available to billions of smartphone users worldwide. An online survey (N=8,286), conducted in eight different countries, sheds light on people's reasons for choosing their screen lock method and demonstrates significant crosscultural differences in attitudes towards this subject. In a separate monthlong field study (N=134), we studied how existing lock screen mechanisms provide users with distinct tradeoffs between usability and security, identifying areas where both could be improved.

With the growth in smartphone adoption around the world, threats to the personal information they contain are also increasing. To protect devices and their contents from unauthorized physical access, manufacturers offer locking mechanisms, such as PINs, passwords, and biometrics. However, from a security perspective, PINs and patterns are susceptible to guessing attacks [1, 4, 12] and shoulder-surfing [14]. Patterns are also vulnerable to smudge attacks [2].

Because of the limitations of existing locking mechanisms, a variety of novel techniques have been introduced in the academic literature. These include additional biometric security layers for PINs [15] and Android patterns [5], external hardware [3], and improving security by visual methods like indirect input [9, 11, 13]. However, for any alternative method to be successfully adopted, a detailed understanding of how real users interact with existing smartphone authentication mechanisms is needed.

As a result, the motivation for our research is twofold. First, we sought to understand the adoption and usage of current locking mechanisms: which ones are used, and what motivates people to use them. Second, we wanted to establish benchmarks for the current authentication mechanisms, against which future research can be compared: users are unlikely to switch to a mechanism that requires more time or effort than their current one.

To this end, we conducted two studies: an international survey [8] and a measurement-based *in situ* in study [7]. Both were conducted during the summer of 2015 and targeted Android users.

INTERNATIONAL SURVEY

Method

We conducted a survey with 8,286 participants in eight countries: Australia, Canada, Germany, Italy, Japan, Netherlands, the United Kingdom, and the United States. Each participant was asked about how they unlocked their phone, why they chose this unlock method, and how sensitive they considered the data on their phone.

Our survey was administered through Google Consumer Surveys (GCS), which allows Android users who have installed a dedicated app[1] to earn Google Play credits by answering short surveys.

The survey was translated into each country's primary language. To ensure the questions retained their meaning across different languages, we consulted domain experts who were native speakers of the target language and verified the results by having other native speakers translate each question and response back to English.

[1] Google Opinion Rewards. https://play.google.com/store/apps/details?id=com.google.android.apps.paidtasks

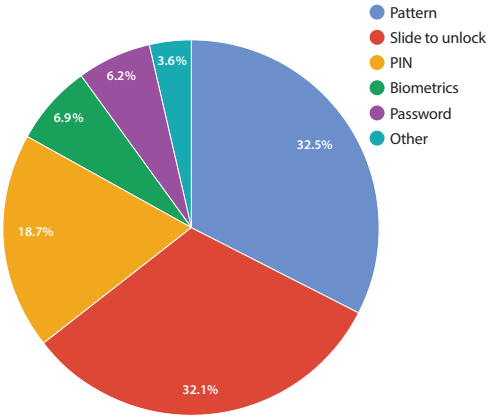


FIGURE 1. How do users unlock their phones?

Responses were translated and then coded into categories using a quantitative content analysis approach. To account for demographic covariates (age and gender), we fitted logistic regression models, with the US as the reference category.

Results

Locking methods

How many people lock their phones? Do locking techniques differ by country?

Worldwide, about two-thirds of those surveyed use a secure lock screen. However, this number varies significantly among the countries in our study, from 50.4% in Italy to 76.4% in the United Kingdom (see Figure 2). The United States has the second-lowest lock rate, at 64.6%.

How popular are the different locking methods?

Among participants with a secure lock screen, the most popular locking mechanism was the pattern at 48%, with the PIN coming in second at 27%. Approximately equal numbers of people – around 6% – reported using a password and biometrics. The relatively low adoption of biometric authentication is likely because not many Android phones supported fingerprint scanners at the time of the survey, in 2015.

Are there demographic differences in locking behavior?

We found that a person's age group was a significant predictor of their locking behavior. In general, the older a person is, the less likely they are to use a secure lock

screen. In particular, respondents over the age of 55 were much less likely to secure their phone than younger users.

Locking reasons

Why don't people lock their phones? Inconvenience was the most commonly cited reason for not locking one's phone, mentioned by over 40% of respondents without a secure lock screen. One US participant exemplified this perspective: *"It's annoying to have to use a password every time I want to use my phone."* Some countries found lock screens more inconvenient than others: Australia, Germany, Italy, Japan, and the Netherlands cited inconvenience as a reason significantly more often than the US, Canada, and the UK.

Nearly one-third of those without a lock screen said that they did not lock their phones due to an absence of threat. For example, one respondent commented that they *"don't have anything on here worth stealing."* Respondents from the US and Canada were more likely to cite this as their reason than users in all other countries.

The third most-common response, though much less frequent than the first two, attributed the lack of a secure lock to the user's carelessness. *"I am always with my phone so I didn't think I needed to. Now that you ask, that seems kind of dumb,"* acknowledged one participant. Not all countries admitted carelessness at the same rates: Germany, Italy, Japan, and the Netherlands all cited it nearly half as often as other countries.

Other common reasons for using swipe-to-unlock included conflicts with existing usage patterns – for example, a public safety officer who treated their phone as a *"lifeline"* and a participant who left it unlocked in case first responders needed to access their contacts. Some mentioned that they relied on other security measures, such as in-app passwords, to protect the data they considered sensitive. These responses suggest that users' risk perception drives their locking decision, a finding that corroborates previous research on the subject [6].

Why do people choose to lock their phones? When discussing the reasons for locking one's phone, the unifying theme is protection. However, different people focused on various aspects of the protection goal in their responses.

One in every five participants mentioned someone specific they wanted to keep out of their phones. These included people they knew (for example, children and "nosy coworkers," but also partners) or strangers, such as potential thieves and hackers.

Another large subgroup focused on the data they did not want to fall into the wrong hands. Examples included bank information, personal files, and text messages or other communications. Respondents from Japan and the Netherlands were less likely to cite this reason than others.

Approximately the same number of respondents (13%) described a scenario they had in mind when locking their phone. Loss or theft of the device were most often mentioned, but some also worried about snooping partners and pranks by friends.

Two percent of respondents across the eight countries (though fewer in Italy, Japan, and the UK) reported that a secure lock screen was mandated by their employer's policy.

In their responses, many participants simply stated that they were locking their phones for privacy purposes. Participants in Germany, in particular, were much more likely to state that protection is necessary in general. *"Because it's nobody's business what text messages, photos, or other data I have on my phone,"* explained one respondent.

Do people consider the data on their smartphones sensitive? As we have seen, many people do not consider the data on their phones to be sensitive and do not lock their phones as a result. Indeed, when asked to rank the sensitivity of their data on a seven-point scale, participants without a secure lock mechanism rated themselves approximately in the middle. In contrast, those with a secure lock screen considered their data much more sensitive, averaging over a point higher.

Reported sensitivity of data varied by country. Notably, Canadians had among the lowest scores, while Japanese had the highest average in both subgroups, scoring over half a point higher than the international average (see Figure 3).

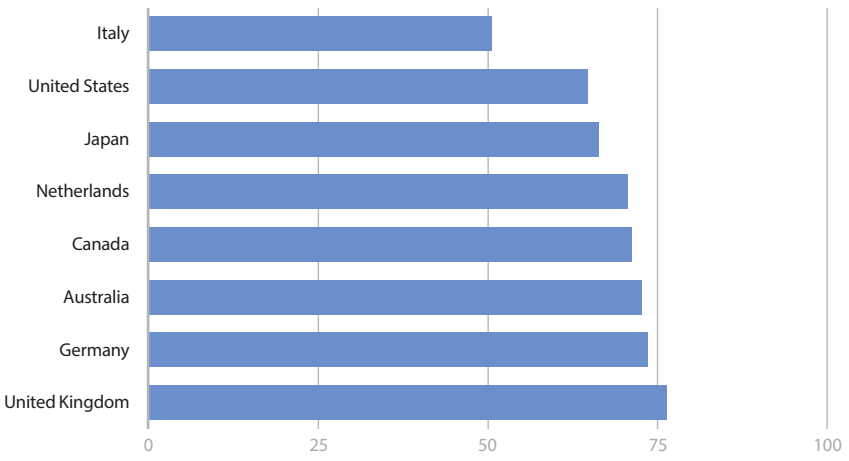


FIGURE 2. Fraction of users with secure lock screen.

LONGITUDINAL BEHAVIORAL STUDY

Method

In order to obtain fine-grained field data about unlocking behaviors, we instrumented participants' primary smartphones with a modified version of the Android operating system. We recruited subjects from the University of Buffalo's PhoneLab panel [10], consisting of more than 200 participants with customized Android phones, which receive over-the-air updates with experiment OS updates.

We limited our dataset to only those participants who were active for 30 consecutive days. We also excluded eight participants who used multiple types of lock screens during the study period, two who used a password, and one who disabled the lock screen altogether; their small numbers

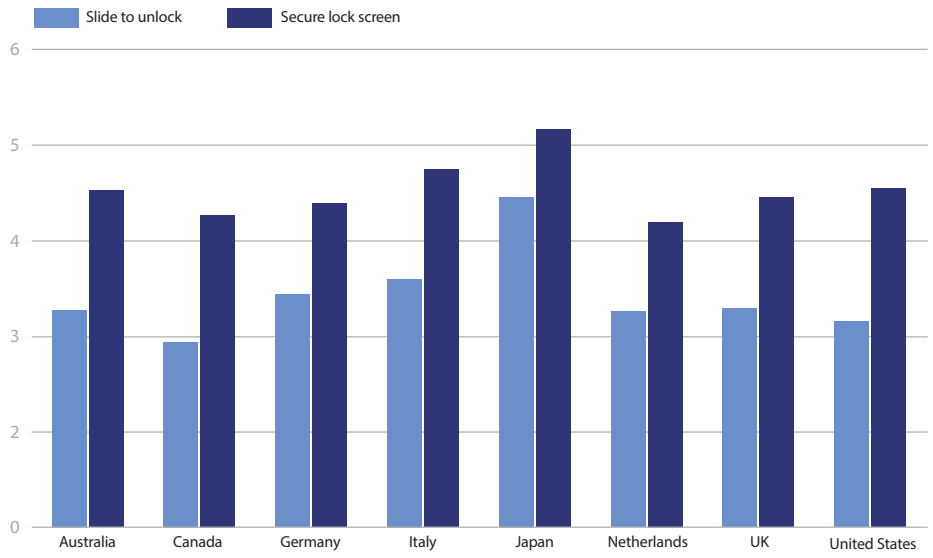


FIGURE 3. How sensitive is the data on your phone? mean scores by country.

precluded comparative analysis. This left us with 134 participants. Of these, half had a secure lock screen and half did not. Of those who did, 52% had a pattern lock, with the rest using a PIN. To collect qualitative information about the participants' unlocking behaviors, we also asked them to fill out a survey at the end of the study; this was answered by 71 of the participants.

When discussing differences between lock screen types, we rely on data that is first summarized per user.

Results

How do people use smartphones?

To truly understand the cost of phone unlocking, we need to know how often it happens. The median participant in our study unlocked their phone 31.8 times every day. We found, however, that this number differed significantly depending on the unlock method the participant had chosen. For example, those who used a PIN had around 10 fewer unlocks on average.

Do people always unlock their phone to use it?

It's important to understand how people engage with their smartphones. The median participant in our study activated their phone 57.1 times each day. But not everything we do requires unlocking the phone; people may just want to check the time or read their notifications. Accordingly, only 56% of these activations resulted in an unlock.

If people often use their phones to check the time, it follows that those with alternate means to do so (e.g., a watch) may do this less frequently. Indeed, the 33 participants who owned watches activated their phones significantly less frequently than participants without watches (median: 46.6 versus 64.6), providing further evidence of the phone's secondary uses.

How long does it take to unlock a phone?

Users do not immediately start entering their PIN or pattern when the screen turns on: preparation takes some time; the median is 3.4 seconds.

The actual unlock process takes around one second on average (the median is 0.82). The time a successful unlock takes is very different between lock screen types: slide-to-unlock takes on average 0.224 seconds, drawing a pattern takes 0.739 seconds, and entering a PIN takes 1.535 seconds.

Looking at the total time spent interacting with the unlock UI in an average day, slide-to-unlock users engage with it for just 6.8 seconds total, compared to 36.8 seconds for PIN users and 48.7 seconds for pattern users. But we saw earlier that patterns were faster to enter than PINs. What might explain the discrepancy?

Unlock errors

One-tenth of all unlock sessions experienced a failure. Pattern users experienced errors much more frequently (12.1%) than PIN users (3.1%). Over the course of a day, the median PIN user would therefore commit one error, while a pattern user would commit five. Given the average error rate, unlocking errors contribute 20.9% to each pattern user's daily unlocking time. For PIN users, this time amounts to 6.0%. Pattern users thus invest over three times as much time to compensate for errors.

How many tries does it take to unlock?

Where there was an error, in 70% of cases, the user was able to successfully unlock their phone on the second attempt. Interestingly, for both PIN and pattern unlock, single errors without successful unlocks happen frequently. Those most likely represent accidental inputs without the true intention to unlock (e.g., "pocket dialing").

Discussion

Usability remains a major challenge for secure smart device lock screens. Even among those survey respondents who did lock their devices, nearly half agreed that locking was sometimes annoying and could be easier. Over one-third agreed that the unlock process could be quicker. Speed, specifically, was also identified as a problem by those without a secure lock: 62% agreed that they would use a lock if the process were quicker. These results suggest that there is still room in the market for a more usable locking mechanism.

However, designers of such mechanisms must overcome a number of challenges. First, while users wish for even faster unlocking methods, our data shows that the existing ones are already quite fast. Consequently, slower alternatives are unlikely to be adopted.

Errors in the unlock process can also become a factor. As we saw, the unlock screen mechanisms that were available at the time of our studies provide users with a tradeoff between time and error rate. However, it may be possible to optimize this tradeoff. Concretely, pattern users may be able to save a lot of time, if we can help them commit fewer errors.

The lock mechanism can have implications beyond the unlocking process itself. Smartphone usage patterns as a whole seem to adjust to available mechanisms, including how often users engage with their phones and how they interact with it in the locked state.

In developing lock screens, designers also have to be cognizant of demographic differences. As we have shown, people vary systematically in their attitudes and behaviors, depending on their age and country. Potential explanations for these effects include differences in privacy attitudes, levels of trust, or technical ability. Further research is needed to disentangle these factors and understand their underlying causes.

Ultimately, the decision to secure one's phone will come down to whether the user thinks their effort is worthwhile. At present, many people around the world do not consider their phones to be particularly sensitive. Have they considered their data and its implications and made a rational decision? Or would additional information and messaging help convince them that a secure lock screen would be a prudent choice? ■

Nathan Malkin is a PhD student in computer science at UC Berkeley, where he is also a fellow with the Center for Long-Term Cybersecurity and the Center for Technology, Society and Policy. His research focuses on usable security and privacy; he has published at ACM CHI and presented his work at the Symposium on Usable Privacy and Security (SOUPS).

Marian Harbach is currently working on usable security for the connected car at Audi AG in Ingolstadt, Germany. He received his PhD at Leibniz University Hannover, Germany and has also performed postdoctoral research at the International Computer Science Institute in Berkeley, California. His main interests include human behavior around and perception of security systems with a focus on authentication.

Alexander De Luca has been working in the field of usable privacy and security for over a decade. He did his PhD at Ludwig-Maximilians-Universtität München, Germany, then worked for the German research center for artificial intelligence (DFKI) and for Fraunhofer FKIE. In March 2015, he started as a user experience researcher at Google, Zurich.

Serge Egelman directs the Usable Security & Privacy Group at the International Computer Science Institute (ICSI), which is affiliated with the University of California, Berkeley. His research focuses on the intersection of privacy, security, and HCI. He received his PhD from Carnegie Mellon University, and has performed research at NIST, Brown University, Microsoft Research, and Xerox PARC.

REFERENCES

[1] Panagiotis Andriotis, Theo Tryfonas, and George Oikonomou. 2014. Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method. In Proceedings of the Second International Conference on Human Aspects of Information Security, Privacy, and Trust Volume 8533. Springer-Verlag New York, Inc., New York, NY, USA, 115–126. DOI: http://dx.doi.org/10.1007/978 3 319 07620 1_11

[2] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10). USENIX Association, Berkeley, CA, USA, 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009

[3] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2011. The Phone Lock: Audio and Haptic Shouldersurfing Resistant PIN Entry Methods for Mobile Devices. In Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '11). ACM, New York, NY, USA, 197–200. DOI: http://dx.doi.org/10.1145/1935701.1935740

[4] Joseph Bonneau, So ïren Preibusch, and Ross Anderson. 2012. A Birthday Present Every Eleven Wallets? The Security of CustomerChosen Banking PINs. In Financial Cryptography and Data Security, Angelos D. Keromytis (Ed.). Lecture Notes in Computer Science, Vol. 7397. Springer Berlin Heidelberg, 25–40. DOI: https://dx.doi.org/10.1007/978-3-642-32946-3_3

[5] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12). ACM, New York, NY, USA, 987–996. DOI: http://dx.doi.org/10.1145/2207676.2208544

[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 (CCS '14). ACM, New York, NY, USA, 750761. DOI=http://dx.doi.org/10.1145/2660267.2660273

[7] 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, 48064817. DOI: http://dx.doi.org/10.1145/2858036.2858267

[8] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. 2016. Keep on Lockin' in the Free World: A MultiNational Comparison of Smartphone Locking. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16). ACM, New York, NY, USA, 48234827. DOI: http://dx.doi.org/10.1145/2858036.2858273

[9] Sung-Hwan Kim, Jong-Woo Kim, Seon-Yeong Kim, and Hwan-Gue Cho. 2011. A New Shouldersurfing Resistant Password for Mobile Environments. In Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication (ICUIMC '11). ACM, New York, NY, USA, Article 27, 8 pages. DOI: http://dx.doi.org/10.1145/1968613.1968647

[10] Anandatirtha Nandugudi, Anudipa Maiti, Taeyeon Ki, Fatih Bulut, Murat Demirbas, Tevfik Kosar, Chunming Qiao, Steven Y. Ko, and Geoffrey Challen. 2013. PhoneLab: A Large Programmable Smartphone Testbed. In Proceedings of First International Workshop on Sensing and Big Data Mining (SENSEMINE'13). ACM, New York, NY, USA, Article 4, 6 pages. DOI: http://dx.doi.org/10.1145/2536714.2536718

[11] Tetsuji Takada and Yuki Kokubun. 2013. Extended PIN Authentication Scheme Allowing MultiTouch Key Input. In Proceedings of International Conference on Advances in Mobile Computing & Multimedia (MoMM '13). ACM, New York, NY, USA, Article 307, 4 pages. DOI:http://dx.doi.org/10.1145/2536853.2536944

[12] Sebastian Uellenbeck, Markus Du ïrmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13). ACM, New York, NY, USA, 161–172. DOI: http://dx.doi.org/10.1145/2508859.2516700

[13] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015a. SwiPIN: Fast and Secure PINEntry 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. DOI: http://dx.doi.org/10.1145/2702123.2702212

[14] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015b. Easy to Draw, but Hard to Trace?: On the Observability of Gridbased (Un)Lock Patterns. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 2339–2342. DOI: http://dx.doi.org/10.1145/2702123.2702202

[15] Nan Zheng, Kun Bai, Hai Huang, and Haining Wang. 2014. You Are How You Touch: User Verification on Smartphones via Tapping Behaviors. In Proceedings of the 2014 IEEE 22nd International Conference on Network Protocols (ICNP '14). IEEE Computer Society, Washington, DC, USA, 221–232. DOI: http://dx.doi.org/10.1109/ICNP.2014.43