Exploring the Adoption of Physical Security Controls in Smartphones

Nasser O. Alshammari[1,2(✉)], Alexios Mylonas[1,3], Mohamed Sedky[1], Justin Champion[1], and Carolin Bauer[1]

[1] Staffordshire University, Beaconside, Stafford, ST18 0AD, UK
nasser.alshammari@research.staffs.ac.uk,
{alexios.mylonas,m.h.sedky,j.j.champion,c.i.bauer}@staffs.ac.uk,
nashamri@ju.edu.sa, amylonas@aueb.gr
[2] College of Information and Computer Science, Aljouf University, Sakaka Saudi Arabia
[3] Information Security and Critical Infrastructure Protection Research Laboratory, Department of Informatics, Athens University of Economics and Business, 76 Patission Ave., GR10434 Athens, Greece

Abstract. The proliferation of smartphones has changed our life due to the enhanced connectivity, increased storage capacity and innovative functionality they offer. Their increased popularity has drawn the attention of attackers, thus, nowadays their users are exposed to many security and privacy threats. The fact that smartphones store significant data (e.g. personal, business, government, etc.) in combination with their mobility, increase the impact of unauthorized physical access to smartphones. However, past research has revealed that this is not clearly understood by smartphone users, as they disregard the available security controls. In this context, this paper explores the attitudes and perceptions towards security controls that protect smartphone user's data from unauthorized physical access. We conducted a survey to measure their adoption and the reasons behind users' selections. Our results, suggest that nowadays users are more concerned about their physical security, but still reveal that a considerable portion of our sample is prone to unauthorized physical access.

Keywords: User acceptance of security policies and technologies · Smartphone · Security control · Authentication · Anti-Theft · Biometrics

1 Introduction

Smartphones as multi-purpose and ubiquitous devices have managed to change the users' everyday life. Users carry smartphones throughout the day in different, and often insecure locations, accessing a plethora of heterogeneous data. Usually, the same device is used for both personal and business purposes [19, 22] thus smartphones store and/or have access to important data, which must be protected from unauthorized access.

At the same time, smartphone users tend to forget their devices in public places [5] and, as a study from Symantec suggests, device finders tend to try to access sensitive data that are stored in a lost device, e.g. personal data (e.g. social media accounts) and

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 287–298, 2015.
DOI: 10.1007/978-3-319-20376-8_26

business data (e.g. corporate human resource files) [8]. As such, the risk of unauthorized physical access to user's data (in a permanent or temporal device loss) is significant, both for individuals and organizations. Moreover, nowadays the request for more security controls against device theft has been implemented by smartphone vendors reducing the number of device theft [4] and unauthorized access to smartphone data. However, this protection is rendered useless unless the respective security controls (such as encryption, remote wipe, etc.) are activated in the device.

In this context, we conducted a user survey in order to explore the attitudes and perceptions towards security controls that protect against unauthorized physical access to the device data (hereinafter referred to as unauthorized physical access). Our study focuses on Android and iOS, which currently hold 95 % of the smartphone market share [6]. Our results, suggest that nowadays users are more concerned about their physical security, but still reveal that a considerable portion of our sample is prone to unauthorized physical access.

The paper is organized as follows. Section 2 presents related work and Sect. 3 provides the methodology of our work. Section 4 presents our results. Finally, Sect. 5 includes a discussion of the results and concludes the paper.

2 Background

2.1 Adversary Model and Assumptions

In this work, we assume the following adversary model. The malicious attacker has gained temporary (i.e. the device owner has not had his device stolen or lost) or permanent access to the smartphone. We assume that the attacker has the knowledge, skills and hardware in order to access device data either with a logical or a physical acquisition. An attacker, however, can access user data remotely (e.g. malicious applications that violate user privacy [20]), but this falls outside the scope of this paper. Finally, we assume average users, i.e. not technically and security savvy ones.

2.2 Related Work

Smartphone users can authenticate and access their device with traditional passwords (PINs (Personal Identification Number) or alphanumeric strings). Unfortunately, users prefer usability, thus choosing memorable passwords that are easy to recall [12], but easy to recover with dictionary attacks [15]. The proliferation of smartphones made other authentication mechanisms popular, e.g. graphical passwords and biometrics (e.g. facial recognition, fingerprint reader).

Graphical passwords are vulnerable to 'traditional' password attacks (e.g. shoulder surfing [21, 25] and brute force attacks [13]), as well as attacks that are unique to graphical passwords due to traces and oily residues left on the screen (i.e. smudge attacks [9–11]. Andriotis et al. [9, 10] focused on human factors that might affect the choice of graphical passwords on a smartphone (such as sub-patterns and starting points), which in combination with smudge attacks can be used to infer the graphical passwords. Finally, in [23] the authors studied the effect of pattern layout on the strength of graphical passwords.

Biometrics as a means of authentication was introduced in the fourth version of Android, with the use of the smartphone's camera for face recognition. However, this security control is not popular, as it can be bypassed with a photograph of the device owner. Modern and more expensive smartphones offer fingerprint readers to provide user authentication to the device. Although, the use of this security control is convenient, it has already been proven to be vulnerable to various attacks [7].

Smartphone vendors have introduced several security controls against device theft to increase post-theft data control, such as Find My iPhone of iCloud and Android Device Manager (ADM) of Google Play. Other third party apps offer similar functionalities such as Prey, Theftie, Avast Anti-Theft and Norton Mobile Security.

All these anti-theft apps support locating a smartphone on a map, playing a sound on a smartphone to help finding it, locking and tracking a smartphone, as well as remotely wiping the data on a stolen or lost smartphone. Remote wiping mechanisms allow owners to remotely delete sensitive data by sending a wipe command to the lost devices through the Internet or SMS [24]. Although, the majority of these anti-theft apps require the smartphone to be online, Find My iPhone suspends all credit and debit cards in Passbook for Apple Pay immediately, even if the iPhone is offline. Some anti-theft apps allow the user to wipe confidential files by sending a special SMS, such as Avast Anti-Theft and Norton Mobile Security.

With iOS 7 (released Q3 of 2013) and later, Find My iPhone is activated by default and includes a feature called Activation Lock, which is turned on automatically. Activation Lock makes it harder for anyone to use or sell an iPhone if it is lost or stolen. This is true, as an Apple ID and password are required before anyone can turn off Find My iPhone, sign out of iCloud or erase and reactivate the smartphone. On the other side, Android Device Manager (released Q4 of 2013) is part of Google's system application suite for all Android devices (version 2.2 and newer). Unlike, other Android third-party applications, where permissions are granted manually by users during installation, ADM can be manually enabled via the user's Google account.

In the user study that was conducted in Q4 of 2011 [19] it was found that smartphone users in the UK and Greece do not use available security controls that can protect smartphone data from unauthorized physical access, namely device locking, remote device locator, encryption and remote data wipe. Moreover, the analysis in [18] revealed that even security savvy users did not protect their data from unauthorized physical access. Moreover, the authors in [16] also studied in Q4 of 2013 the adoption of device locking, as well as the reasons for (not) using this control. Also, their results suggest that less than half of the sample used device locking and that the participants underestimated the time that they spend to unlock their device.

Chin et al. [14] carried out a user study to gain insights into user perceptions of smartphone security, in Q4 of 2011 and Q1 of 2012. Their study shows that both Android and iPhone participants seem equally concerned about phone loss and damage. Kraus et al. [17] examined how privacy and security knowledge and global information privacy concern of a user, influence mobile protection behavior. They found that low knowledge and low global information privacy concern can serve as predictors for not using the protection methods, whereas high knowledge and high concern can serve as predictors for the usage of the evaluated protection methods.

3 Methodology

To explore the adoption of physical security controls in smartphones we conducted a survey with an online questionnaire. The survey took place from November 2014 to January 2015 and targeted smartphone users who are based in the United Kingdom. The questionnaire was distributed via word of mouth, social media, and groups and societies in West Midlands. Before launching the survey we completed a pilot survey in the lab with 6 participants in order to validate the questionnaire.

The survey starts by asking the participants demographic questions (c.f. Appendix). Then, users are asked whether they use a locking mechanism (e.g. password, biometric) in their device. According to their responses, the participants are asked for the reasons why they do so, as well as the type of locking mechanism that they use. Next, the sample is asked if they use a password for an individual application on their device and according to their responses, the reasons why they do so. The last part of the survey asks users whether they have had their device stolen. Also, the participants are asked whether they use any anti-theft mechanism (such as remote data wipe, remote device locator, encryption, etc., c.f. Appendix) and the reason for doing so. The questionnaire uses open ended questions to collect from the participants the reasons why they use a security control or not. The participants directly expressed their reasons either directly, e.g. "the control is not useful to me", or indirectly "to protect my stuff from people who want to snoop me".

We collected data from 208 survey participants. After the removal of participants who were not Android or iOS users and/or any incomplete questionnaires or data that failed our data validation, we ended up with 192 participants. Among them, 48 % used Android, ~65 % were male and 82 % were aged [18–35] ($\min_{age} = 18$ $\max_{age} = 67$). Regarding their IT skills the respondents classified themselves: (a) 11 % non-technically savvy ('moderate' IT), (b) 42 % with good IT skills, and (c) 47 % technically savvy ('excellent' IT). Finally, 17 % of the participants had their device stolen.

The next section presents our findings from descriptive and inferential statistics (χ^2 tests and φ coefficient). We compare our common results with the UK sample, which was collected in [19] and is referred to as *UK2011* sample. It is worth noting that compared to *UK2011* [19], the users have more options with regards to locking their devices, and the threat of unauthorized physical access is more well-known [4, 5, 8].

4 Results

4.1 Results Regarding Device Locking

An early finding in our analysis is that currently smartphone users, lock their device more frequently (76 %) than in the past (compared to the ~61 % in the UK sample in [19], c.f. Fig. 1). The results revealed that 40 % of the participants used application passwords, which is a considerable amount of participants if one considers that this is a third-party app that the user has to find and install on his own.

More specifically, the analysis revealed that 67 % of the Android participants and 84 % iOS participants lock their device. As summarized in Fig. 1, while PIN is the most

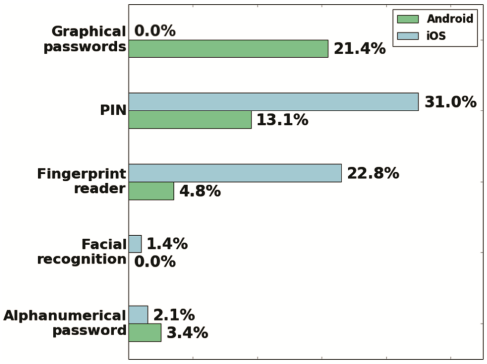

Fig. 1. Distribution of device lock mechanisms in Android and iOS users

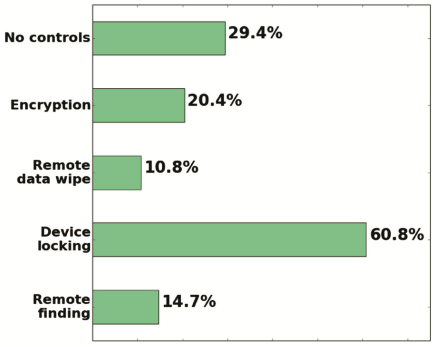

Fig. 2. Adoption of security controls by the *UK2011* sample in [19]

popular authentication mechanism in our sample, a considerable number of our participants used patterns and fingerprints for their authentication.

Our results suggest that in Android, patterns or graphical passwords are popular and user friendly alternatives to PINs, whereas fewer participants used fingerprint readers for their authentication and none used facial recognition (Fig. 1). On the other hand, the results suggest that iOS users opt for PIN and fingerprint readers. It is worth noting that, currently, fingerprint readers are only provided by expensive smartphones and, as a result, the popularity of this control might increase in the future, when the cost of the devices drops.

When the participants were asked about the reasons for using the abovementioned controls, they attributed security and privacy as the main reason (79 % of the sample) for using a particular device locking control. The rest of the reasons that were identified were: ease of use (41 %), organization policy (3 %) and default settings (8 %). Moreover, our results suggest that the participants who use the fingerprint reader, selected the control because of its ease of use ($\chi^2 = 16.452$, $p = 0.00005$, $\varphi = 0.337$). We did not find any statistically significant correlation between the rest of the reasons and device locking controls.

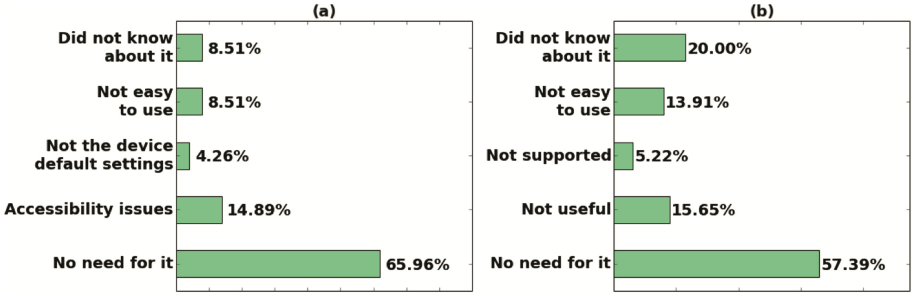

Fig. 3. **(a)** Reasons the participants do not use device locking **(b)** Reasons the participants do not use application password.

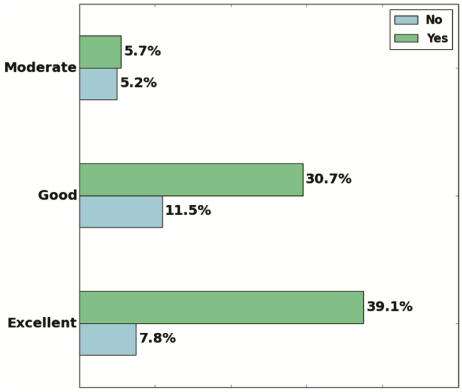

Fig. 4. Adoption of device lock versus the IT skills of the participants

Figure 3 depicts the reasons[1] the participants are not using the device locking and application passwords. In both cases the participants claimed that the security controls were not needed. In addition, as Fig. 3b suggests, currently a considerable amount of our participants are not aware of application passwords, which is somewhat expected as this control is only available as a third-party application.

Our analysis revealed that almost one third of the participants who had their device stolen (10 out of 32) did not lock their device, leaving their device and its data exposed to unauthorized access. Among them, 5 participants had both device locking and application passwords disabled.

Finally, as in [19] the analysis revealed that the IT skills of the participants affect the adoption of security controls. In this survey, as depicted in Fig. 4, the technical savvy participants tend to lock their device. However, we did not find such finding for application password.

[1] The reasons are self-explanatory, except for "Accessibility" that refers to any impairment that prevents the participant from using the control.

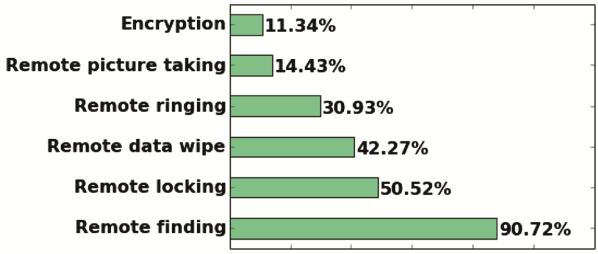

Fig. 5. Distribution of anti-theft security controls in the sample

4.2 Results Regarding Anti-theft Controls

The analysis revealed that 51 % of the sample used an anti-theft control. Our analysis suggests that remote finding the device was the security control that was mostly used by the participants, followed by remote locking and remote data wiping. Considerably less participants reported the use of encryption and remote picture taking. The aforementioned are summarized in Fig. 5. Also, the results reveal that the participants who use remote picture taking are more likely to be Android users ($\chi^2 = 8.402$, $p = 0.04$, $\varphi = 0.209$). We did not find any other statistically significant correlation between the adoption of the anti-theft controls and the participants' operating system, or their IT skills and the adoption of anti-theft controls.

It is worth noting that the analysis revealed the same misconception about encryption that was found in [19], stemming from the fact that in iOS the device is encrypted when the user enables device lock [3]. Specifically, in this work, we found 45 iOS participants who were using a PIN out of which 43 of them (96 %) reported that they are not using encryption. Similarly, 33 iOS survey participants used the fingerprint reader and 31 of them (94 %) did not know that they were using encryption.

When asked about the reasons of using anti-theft controls, again the majority of respondents identified security and privacy as their main reason (85 %), followed by default settings (11 %) and organization policy (4 %). Also, as Fig. 6 suggests, lack of knowledge about the existence of anti-theft controls was the main reason why the respondents ignored them.

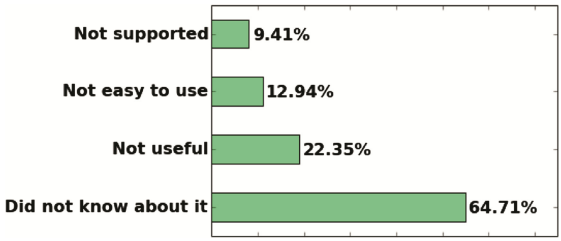

Fig. 6. Reasons the participants do not use ant-theft controls

When comparing our results with the *UK2011* sample, there are less participants (17 %) who did not lock their device and did not use anti-theft controls (c.f. Fig. 2). Amongst them, five participants have had their device stolen in the past, which increases their risk of unauthorized access to their device.

As in [18, 19], the analysis revealed multiple statistical significant correlations between pairs of security controls. More specifically, the participants tend to have disabled the following security controls: (a) remote finding and encryption ($\chi^2(1) = 9.550$, $p = 0.02$, $\varphi = 0.223$), (b) remote finding and remote device lock ($\chi^2(1) = 42.148$, $p < 001$, $\varphi = 0.469$), (c) remote ringing and remote locking ($\chi^2(1) = 62.520$, $p < 0.001$, $\varphi = 0.571$), (d) remote finding and remote picture taking ($\chi^2(1) = 17.847$, $p < 0.001$, $\varphi = 0.305$), (e) remote finding and remote wiping ($\chi^2(1) = 36.992$, $p < 0.001$, $\varphi = 0.439$), (f) remote wiping and remote locking ($\chi^2(1) = 62.273$, $p < 0.001$, $\varphi = 0.570$), (g) remote ringing and remote finding ($\chi^2(1) = 37.008$, $p < 0.001$, $\varphi = 0.439$), and (h) device ringing and device wiping ($\chi^2(1) = 57.202$, $p < 0.001$, $\varphi = 0.546$).

The analysis also revealed statistically significant correlations regarding the use of the controls, namely: (a) participants who encrypt their device are more likely to use remote device locator ($\chi^2(1) = 9.550$, $p = 0.02$, $\varphi = 0.223$), (b) participants who unlock their device with their fingerprint are more likely to use remote device locator ($\chi^2(1) = 7.476$, $p = 0.06$, $\varphi = 0.197$), (c) participants who enable remote locking tend to enable remote finding ($\chi^2(1) = 42.148$, $p < 001$, $\varphi = 0.469$), (d) participants tend to enable remote locking and remote ringing together ($\chi^2(1) = 62.520$, $p < 0.001$, $\varphi = 0.571$), (e) participants tend to enable remote locking and remote wiping together ($\chi^2(1) = 62.273$, $p < 0.001$, $\varphi = 0.570$), (f) participants who enable remote picture taking tend to enable remote finding ($\chi^2(1) = 17.847$, $p < 0.001$, $\varphi = 0.305$), (f) participants who enable remote wiping tend to use remote finding ($\chi^2(1) = 36.992$, $p < 0.001$, $\varphi = 0.439$), (g) participants who enable remote ringing tend use remote finding ($\chi^2(1) = 37.008$, $p < 0.001$, $\varphi = 0.439$), and (h) participants tend to enable device ringing and device wiping together ($\chi^2(1) = 57.202$, $p < 0.001$, $\varphi = 0.546$).

5 Discussion and Conclusions

The commercialization of smartphones has introduced threats with regards to the security and privacy of their users. The devices store and process heterogeneous data, which must be protected from unauthorized access. The owners of these devices are not necessary security savvy and thus may be unaware of the relevant threats and countermeasures.

In this paper, we have examined the adoption of security controls that protect users from unauthorized physical access. We have conducted a survey with participants from the United Kingdom in order to explore the use of security controls, as well as the reasons for (not) using device locking (such as PINs, graphical passwords, and fingerprint readers) and anti-theft controls (such as remote wipe and remote finding the device, etc.). Our findings suggest that, compared to surveys that preceded ours [16, 18, 19],

smartphone users tend to use the available controls more frequently, which is particularly true for device locking controls.

One of the reasons for this is that nowadays smartphones offer controls that are easier to use, which - as our results suggest - gradually replace PINs and passwords (e.g. graphical passwords in Android and fingerprint readers in iOS). Another reason is that users have been trained to authenticate with passwords, e.g. before they access their computer/laptop or online services (e.g. social media) and, as a result, they are aware about device unlocking. However, as our results suggest, this does not hold for application passwords and the anti-theft controls, since a main reason behind not using these controls is users' unawareness of their existence.

The demographics of our sample introduce limitations to our work. Thus, it might be the case, that our findings are biased towards the demographics of our sample. Moreover, our survey used an online questionnaire, thus, it relies on self-reported data. However, we consider that our results give considerable insights regarding the attitudes and perceptions towards physical security controls. This holds true, as our results are validated from the common security findings of the most recent related survey [16], which studied the use of device locking and the reasons for (not) using this control. More specifically, in [16] participants also attributed security and privacy as the main reason for using the security control. Similarly to our results, the main reason for not using device locking was user perception that the control is not needed.

PIN is still the most popular device locking control as it has been revealed in this work, as well as in [16, 19]. However, in our work we found that other controls are getting more popular, such as the graphical passwords and the fingerprint readers. We consider that the latter will gain more popularity in the near future as the cost of the devices that are offering them decreases. This holds true, as we found that the participants who were using fingerprint readers identified ease of use as a reason for its selection. The fingerprint reader seamlessly authenticates the user and does not interrupt her from fulfilling tasks, especially when a task might last less time than the authentication attempt (e.g. in the case that the user needs to check the calendar and has to first enter a PIN/password). This is an important factor if one considers the amount of time that users spend in order to unlock into their devices [16].

Our results, as in [18, 19] reveal occasions in which users disable or enable together the controls that allow the user to remotely control her device (e.g. lock it, wipe it, find it, etc.). One obvious reason for this is that they are managed by the same software/configuration interface. Finally, as in [18, 19], this work revealed iOS users who had encryption enabled by default without knowing it. This is a security feature that could be adopted by Android to protect its user base, especially if one consider the low adoption of encryption by Android respondents.

As future work, we plan to repeat this user survey to examine if the attitudes and perceptions of smartphone users with regards to physical security controls will significantly change.

Acknowledgement. Nasser O. Alshammari receives funding from the Ministry of Education in Saudi Arabia.

Appendix

Questionnaire
Q1: What is your gender? *Only one choice of* {Male, Female}
Q2: What is your age? *(Open-ended question)*
Q3: How good are you with computers in general? *Only one choice of* {Excellent, Good, Moderate}
Q4: What is your smartphone operating system? *Only one choice of* {Android, Apple iOS, Windows Phone, Blackberry, I do not know, Other}
Q5: Do you use a mechanism on your smartphone to lock/protect it? *Only one choice of* {Yes, No}
Q5a: What type of locking mechanism do you use on your smartphone? *(Only shown if Q5 answer is "Yes", Multiple choices of* {Numerical password (PIN), Alphanumerical password (characters and/or numbers), Graphical password (patterns), Fingerprint readers, Facial recognition, Other}
Q5b: Why do you use this locking mechanism? *(Only shown if Q5 answer is "Yes") (Open-ended question)*
Q5c: Why you chose not to use a locking mechanism? *(Only shown if Q5 answer is "No") (Open-ended question)*
Q6: Do you use passwords for individual applications on your smartphone? *Only one choice of* {Yes, No}
Q6a: Why you use a password for applications on your smartphone? *(Only shown if Q6 answer is "Yes") (Open-ended question)*
Q6b: Why you chose not to use a password for applications on your smartphone? *(Only shown if Q6 answer is "No") (Open-ended question)*
Q7: Have you ever had your smartphone stolen? *Only one choice of* {Yes, No}
Q8: Do you use any anti-theft mechanisms on your smartphone? *Only one choice of* {Yes, No}
Q8a: What type of anti-theft mechanisms do you have? *(Only shown if Q8 answer is "Yes", Multiple choices of* {Remotely wipe data, Remotely find the device location, File encryption, Remotely take pictures using the smartphone camera, Remotely lock the smartphone, Remotely ring the smartphone, Other}
Q8b: Why you do have anti-theft mechanisms? *(Only shown if Q8 answer is "Yes") (Open-ended question)*
Q8c: Why you chose not to have anti-theft mechanisms? *(Only shown if Q8 answer is "No") (Open-ended question).*

References

1. App Lock. http://www.domobile.com
2. iApp Lock. http://iapplock.thinkyeah.com/
3. Apple: iOS Security Guide. Technical report, October 2014
4. London Smartphone Theft Drops. http://www.theguardian.com/technology/2015/feb/11/london-smartphone-theft-drops-after-kill-switch-introduction-iphones/

5. Phone Theft In America. https://www.lookout.com/resources/reports/phone-theft-in-america/
6. Sales of Smartphones Grew 20 Percent in Third Quarter of 2014. http://www.gartner.com/newsroom/id/2944819
7. Spoofing Fingerprints. https://srlabs.de/spoofing-fingerprints
8. Symantec Smartphone Honey Stick Project. http://www.symantec.com/connect/blogs/introducing-symantec-smartphone-honey-stick-project
9. Andriotis, P., Tryfonas, T., Oikonomou, G.: Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 115–126. Springer, Heidelberg (2014)
10. Andriotis, P., Tryfonas, T., Oikonomou, G., Yildiz, C.: A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec 2013, Association for Computing Machinery, pp. 1–6. ACM, New York (2013)
11. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M.: Smudge attacks on smartphone touch screens. WOOT **10**, 1–7 (2010)
12. Bonneau, J.: The science of guessing: analyzing an anonymized corpus of 70 millionpasswords. In: 2012 IEEE Symposium on Security and Privacy, pp. 538–552. Instituteof Electrical & Electronics Engineers (IEEE) (2012). http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6234435
13. Botelho, B.A.P., Nakamura, E.T., Uto, N.: Implementation of tools for brute forcing touch inputted passwords. In: 2012 International Conference for Internet Technology and Secured Transactions, pp. 807–808. IEEE, New Yok (2012)
14. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring user confidence in smartphone security and privacy. In: Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS 2012. Association for Computing Machinery (ACM), New York (2012)
15. Ding, Y., Horster, P.: Undetectable on-line password guessing attacks. SIGOPS Oper. Syst. Rev. **29**(4), 77–86 (1995)
16. Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., Smith, M.: It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception. In: Symposium on Usable Privacy and Security (SOUPS), pp. 9–11 (2014)
17. Kraus, L., Wechsung, I., Möller, S.: A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior. In: Workshop on Privacy Personas and Segmentation (PPS) (2014)
18. Mylonas, A., Gritzalis, D., Tsoumas, B., Apostolopoulos, T.: A Qualitative metrics vector for the awareness of smartphone security users. In: Furnell, S., Lambrinoudakis, C., Lopez, J. (eds.) International Conference on Trust, Privacy & Security in Digital Business (LNCS), pp. 173–184. Springer, Heidelberg (2013)
19. Mylonas, A., Kastania, A., Gritzalis, D.: Delegate the smartphone user? security awareness in smartphone platforms. Comput. Secur. **34**, 47–66 (2013)
20. Mylonas, A., Theoharidou, M., Gritzalis, D.: Assessing privacy risks in android: a user-centric approach. In: Bauer, T., Großmann, J., Seehusen, F., Stølen, K., Wendland, M.-F. (eds.) RISK 2013. LNCS, vol. 8418, pp. 21–37. Springer, Heidelberg (2014)
21. Tari, F., Ozok, A.A., Holden, S.H.: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In: Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS 2006, pp. 56–66. Association for Computing Machinery (ACM) (2006)

22. Theoharidou, M., Mylonas, A., Gritzalis, D.: A risk assessment method for smartphones. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IFIP AICT, vol. 376, pp. 443–456. Springer, Heidelberg (2012)
23. Uellenbeck, S., Dürmuth, M., Wolf, C., Holz, T.: Quantifying the security of graphical passwords. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS 2013, pp. 161–172. ACM (2013)
24. Yu, X., Wang, Z., Sun, K., Zhu, W.T., Gao, N., Jing, J.: Remotely wiping sensitive data on stolen smartphones. In: Proceedings of the 9th ACM Symposium on Information Computer and Communications Security - ASIA CCS 2014, pp. 537–542. ACM (2014)
25. Zakaria, N.H., Griffiths, D., Brostoff, S., Yan, J.: Shoulder surfing defence for recall-based graphical passwords. In: Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS 2011, ACM (2011)