УДК 004.9
МРНТИ 81.93.29

UNLOCK SECURITY DEVELOPMENT FOR SMART PHONE SECURITY IMPROVEMENT

A. RAZAQUE, S.T. AMANZHOLOVA, O.S. TOKANOV, R. DAVLETOV, T. MOLUTBEKOV, A. KANTSELYARISTOV

International IT University

Abstract: *With emergence of new technology, the influence exerted by telephone communication gadgets on our daily lives is increasing. Due to the fact that the information contained on such small gadgets is becoming highly confidential and sensitive. In United States of America alone, over 2012 there were more than 1.6 million thefts of smartphones. And, every year, this number continues to grow. In this situation, the first question that comes to mind about the protection of the personal information.*
One of the better solutions is the creation of new, or the improvement of the existing blocking systems of smartphones. In this paper, we introduce the keyboared saftety algorithm for improving the static unlock systems for smartphones. The proposed keyboad safety algorithm randomly allocates number in the keyboard that helps protect safety of the keyboard. The proposed algorithm is implented by using real device. Based on the testing result, we confirm the validity of the proposed algorithm.

Keywords: *Smartphone, unlock, algorithm, development, Biological characteristics*

СМАРТФОН ҚАУІПСІЗДІГІН ЖАҚСАРТУ ҮШІН ҚАУІПСІЗДІК ДИЗАЙНЫН АШАДЫ

Аңдатпа: *Жаңа технологиялардың пайда болуымен бұл мәселенің барған сайын маңыздылығы артуда. Осындай шағын гаджеттердегі ақпараттың құпиялы және өте құпия болып табылатындығына байланысты. 2012 жылы Америка Құрама Штаттарында тек 1,6 миллионға жуық смартфонның ұрланғаны тіркелген. Бұл сан жыл сайын өсуде. Мұндай жағдайда ақылға қонатын бірінші мәселе – жеке ақпаратты қорғау.*
Ең тиімді шешімдердің бірі смартфонды блоктау үшін бар жүйелерді дамыту болып табылады. Біз бұл мақалада смартфондар үшін статикалық құлпын ашу жүйелерін жақсарту үшін қауіпсіз пернетақта алгоритмін ұсынамыз. Енді осы айтылған пернетақта қауіпсіздігі алгоритмі пернетақта қауіпсіздігін қорғауға көмектесетін пернетақта нөмірін кездейсоқ түрде таратады. Берілген алгоритм нақты құрылғы арқылы жүзеге асырылады. Сынақ нәтижелері бойынша ұсынылған алгоритмнің жарамдылығын растаймыз.

Түйінді сөздер: *смартфон, құлпын ашу, алгоритм, даму, биологиялық сипаттамалары*

РАЗБЛОКИРОВКА РАЗРАБОТКИ БЕЗОПАСНОСТИ ДЛЯ УЛУЧШЕНИЯ БЕЗОПАСНОСТИ СМАРТФОНА

Аннотация*: С появлением новых технологий это становится все более важной проблемой. В связи с тем, что информация, содержащаяся на таких маленьких гаджетах, является конфиденциальной и конфиденциальной. Только в Соединенных Штатах Америки за 2012 год было зарегистрировано более 1,6 миллиона краж смартфонов. И с каждым годом это число продолжает расти. В этой ситуации первый вопрос, который приходит на ум – это защита личной информации.*
Одним из лучших решений является разработка существующих систем блокировки смартфонов. В этой статье мы представляем алгоритм безопасной клавиатуры для улучшения систем статической

разблокировки для смартфонов. Предложенный алгоритм безопасности клавиатур случайным образом распределяет номер клавиатуры, что помогает защитить безопасность клавиатуры. Предложенный алгоритм реализован с использованием реального устройства. На основании результатов теста мы подтверждаем правильность предложенного алгоритма.

Keywords: *смартфон, разблокировка, алгоритм, разработка, биологические характеристики*

Introduction

The smart phones have dramatically attracted the people to use for several applications including routine things. Therefore, the smart phone is not fully secure due to several security threats. [1] The unlock security gains popularity due to privacy and sensitive date.

The popular unlock methods on smartphone include the number unlock which is the basic, fingerprint unlock, iris unlock and other biometric ways. [2] [3] [4] In order to ensure the user experience, smartphone makers always allow the use of number unlock keyboard, which indicates that the number unlock is the basic thing in terms of smartphone security.

Ill-intentioned people guess the password by snooping on the gesture when others unlock the phone so that they can steal sensitive information from others' smartphone. It is a fact that the current number keyboard for unlocking is not safe enough to prevent voyeurism. Today, smartphone has been an inalienable part of our life. [5] There is no denying that it makes our life more convenient, it has lots of functions such as communication, payment, GPS and so on. Meanwhile, we often save and uploading our personal information through it and even be used as the authentication tool. Therefore, smartphone security is a significant issue worthy of re-search. The smartphones unlock are important now. Our aim is to introduce randomly generated keyboard to improve unlocking safety. In this keyboard, numbers from 0 to 9 can be randomly allocated so that others cannot guess what one has typed. In this condition, voyeur is no longer a problem for unlock problem of smartphone. This paper contributes to:

- Introduce the development of unlock security.
- Improve the unlock security.
- Make one number keyboard to increase unlock security.

The rest of the paper is organized as:

- Section 2 presents the related work.
- Section 3 introduces the proposed plan.
- Section 4 indicates the experimental result.
- Section 5 concludesentirepaper.

LiteratureReviews

In this section, salient features of existing approaches are discussed. As we stated, the unlock security of smartphone is one relatively new area for us to do research. While we still find some academic papers and white papers which are related to it. It is a fact that unlock of smartphone combines both ordinary digital unlocks and biometrics. Neither of them can be deleted. This literature can help quickly know the current findings in this area. What's more we give our evaluation and outlook. In the ACM database we reviewed two most relevant studies. The first one is about the salient feature of existing approaches is discussed. The anatomy of smartphone unlocking is analyzed in [6]. Excusive evaluation is conducted by addressing advantages and disadvantages including different methods to unlock the smartphone. Further, both smartphone unlock security improvement and reduction of complexity are discussed.

Another paper is about one new way to unlock smartphone. It [7] presents Glass Unlock, a novel concept using smart glasses for smartphone unlocking, which is theoretically se-cure against smudge attacks, shoulder-surfing, and camera attacks. By introducing an additional temporary secret like the layout of digits that is only shown on the private near-eye display, attackers cannot make sense of the observed input on the almost empty phone screen. This paper indicates one awesome way for us to improve the security of unlocking.

There are also a lot of white papers [3] and websites [4] which discuss about the unlock security methods that are worthy to explore. According to our current research, we have already found out that it is a fact that we should

refine our initial research topic so that we can have one considerable result at the end of the semester.

Based on the literature survey, we have figured out that the basic digital password keyword is one of the initial item for protecting the unlock process, since we can skip other biometrics methods to the digital keyword when in need. What's more, according to a recent funding, some computer science engineers have made one AI to record the action when people use the password to unlock. [8] It is also not hard for us to guess one's number password when looking their hands' action. Moreover, it is relatively impossible for us to help improve the algorithm of biometrics due to the lack of lack of background knowledge on the biological. In conclusion, our paper especially focuses on improving the safety of number unlock to avoid being cracked easily due to the motion of the hand. The most important reason that people with dangerous motivation and highly developed artificial intelligence (AI) can guess the password is that the numbers are located in specific place, which decrease the safety of the password.

Proposed Keyboard Safety Algorithm For Unlock Security Of Smartphones

As, the modern mobile phone has developed new defensive strategy so that when the attacker tries the pass-word for over 10 times, it automatically locks itself un-less the user asks the mobile phone manufacturer to un-lock it. The only concern we focus is to create one ease-of-use keyboard which can randomly show the number to protect the users' password. The keyboarded safety for static unlock system of smartphones is depicted in Figure 1.

Figure 1- Proposed keyboard safety for static unlock system

As shown in figure1, we create one demo which can show the keyboard randomly locating the number. We plan to use advanced programming language, such as Java, to implement our plan.

First of all, we should give user the choice, which can be one button connected to one Boolean value, to use our improvement or not, since some of users are not suited to change. If the user rejected our improvement, all the number can show in the keyboard in the original location. We can use the function random() to automatically create the number from one to ten. It is also true that we can create the random number on our own. Also, we create a list called 'list' to help avoid that the number is repeated. The following is the sample 'if sentence' to check the repetition. It is a fact that if we can create this kind of keyboard in java so that it can be used in some mobile operating systems. In conclusion, based on our proposed plan, we can build one demo to randomly allocate number in the key-board. The following part is the algorithm to implement this idea (Figure 2).

The algorithm 1 shows how to implement to create a save keyboard. The first step of this algorithm is to create a frame for users to make decisions if they need to create one save keyboard. Ff in this algorithm is one frame which appears so that the user can decide whether they need to use our method. L is a list where the number that has not been put in the keyboard stores, number Ns is from 0 to 9. Random() is one method which can generate number randomly, provided by all the advanced programming language. The result of users' decisions from Ef is indicated by the value UserDecision. If user chooses not to follow our method, it shows the common number keyboard Ckf and close the previous confirm page.

In other conditions, it shows the keyboard Skf which randomly arrange the number. This study also provides one way to randomly choose number based on the use of List. If one number was selected from the list, it will be removed so that the reputation can be avoided. The first ten lines of this algorithm helps to define the variable of this algorithm. From line 15 TO 24, it creates the common keyboard for the user to use. The last part of this algorithm creates the safe keyboard to increase the unlock safety.

```
1       Initialization
2       {
3       Ff : The first frame;
4       L: A list;
5       Random(): An encapsulated method.
6       Ns: The number selected from L
7       }
8       Input
9       {
10      UserDecision: A Boolean number which
indicates the user's decision;
11      }
12      Output
13      {
14      Skf: The frame that contains the save
keyboard;
15      Ckf: The frame that contains the common
keyboard;
16      }
17      Realization:
18      Fundamental: {
19      Create the Ff
20      Ff offers the choice so that user can decide
whether they follow our method or
not; (The result was shown by the variable
UserDecision)
21      If UserDecision == false
22      Then create the Ckf;
23      Else
24      Implement method improvement;
25      Improvement: {
26      Create the Skf (At this time, the skf does not
have number in it);
27      For t from 0 to 9
28      Use random() to create Ns;
29      Remove Ns from L;
30      Put Ns in the Skf;
31      End For
32      }
33      End If
34      Turn off the Ff
35      }
```

Figure 2-Pseudo code of save keyboard generation

Experimental Result

According to the proposed plan, we have built the prototype to help increase the safety. In this section, the performance of this tool is discussed. All experiments are per-formed under the same conditions. The device that performs the experiment has the same screen and processor. Volunteers who participated in the experiment did not know that they find a secure keyboard or a normal keyboard. Table 1 shows used tools in the experiment.

Table 1 – Used tools in the experiment

Tools	Specification
TCL Smart Phone	Qualcomm 610, 5 Inch Ips Display, Android 5.0
Lenovo Laptop	Win 10 8G Ram CPU: Intel Skylake I5
USB Line	OtgSupported
CasioStopwatch	Accuracyof measurement:0.01s

Based on testing, results are evaluated:

- Safety evaluation.
- Speed evaluation.

A. Safety evaluation

According to the proposed plan, we have built the prototype to help increase the safety. In this section, the performance of this tool is discussed. All experiments are per-formed under the same conditions. The device that performs the experiment has the same screen and processor. Volunteers who participated in the experiment did not know that they find a secure keyboard or a normal keyboard. Table 1 shows used tools in the experiment.

Table 2 shows the experimental result which only uses the common keyboard. It is a fact that volunteers can get a guess that is close to the original password. They have got most of the right password. If they could have more chances to try to unlock the phone, they certainly can get a right password.

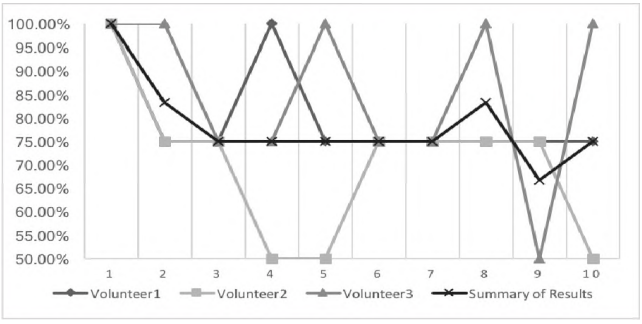

Figure 3 - Safety Evaluation Using Common Keyboard

In figure 3, it shows the line chart summarizing the experimental result, is shows that the volunteer who participated this experiment can guess most of the password with the common keyboard. About 75% of password can be got only at one time.

Table 3 shows the experimental result which uses the safe keyboard, it shows that the safe keyboard greatly improves the safety of unlocking. The volunteers get the guessed numbers which have little relationships with the password. No matter how many times they try, they cannot have the right password.

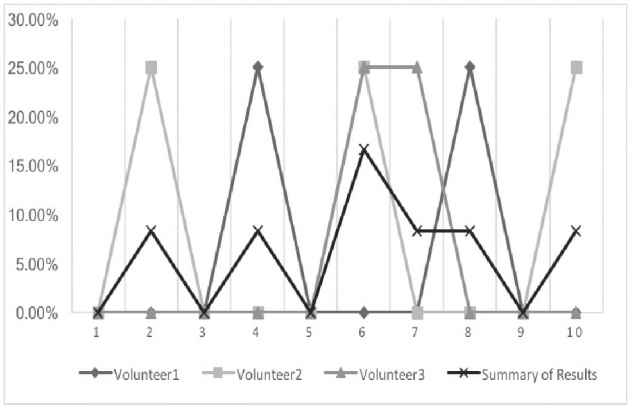

Figure 4 - Safety Evaluation Using Safe Keyboard

Figure 4 intuitively shows a lower hit rate. The volunteer can only guess about 5% of the password with their good luck. It is a fact that our safe keyboard can help increase the safety a lot.

B. Speedevaluation

It is a fact that everyone cares about the speed of unlocking the phone. [11- 12] In this case, our study should pay attention not to reduce the convenience of common number keyboard. To this extent, we let the volunteers type the password on both safe keyboard and common keyboard, comparing their time for inputting. The data obtained through common keyboard is shown in Table 4.

Since the user is familiar with the layout of the common keyboard, they can type the password in this kind of keyboard in a short time.

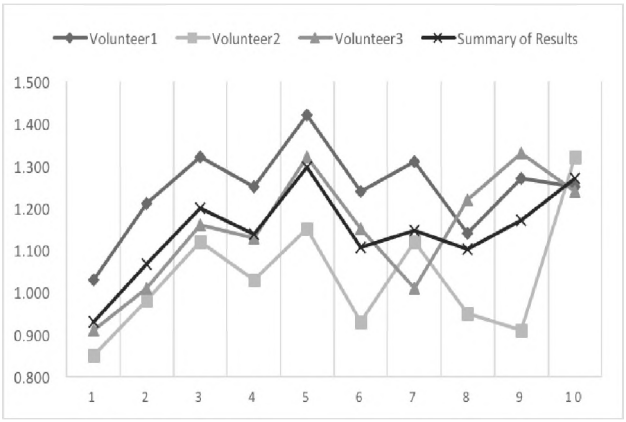

Figure 5 - Speed Evaluation Using Common Keyboard

Figure 5 shows that user can unlock the phone with common keyboard only in about 1.2 seconds. The experimental data obtained from safe keyboard is shown in Table 5.

Table 2– The Experiment Using Common Keyboard

Volunteer\ Password	0000	0124	2512	3241	2267	0042	0321	2231	1120	3210
Volunteer1	0000	0121	2511	3241	2277	0044	0331	2232	1129	3219
Volunteer2	0000	0125	3512	3442	2466	0041	0322	2233	1128	3318
Volunteer3	0000	0124	2522	2241	2267	0022	0322	2231	1139	3210
Summary of Results	100%	83.3%	75%	75%	75%	75%	75%	83.3%	66.7%	75%

Table 3 – The Experiment Using Safe Keyboard

Volunteer\ Password	0000	0124	2512	3241	2267	0042	0321	2231	1120	3210
Volunteer1	2222	3231	0789	5643	6641	5521	5433	2423	2231	5543
Volunteer2	5555	3321	0689	5623	6644	5532	5562	4443	3342	5511
Volunteer3	9999	3233	0888	5533	6652	5522	5501	3344	2241	5621
Summary of Results	0%	8.33%	0%	8.33%	0%	16.6%	8.33%	8.33%	0%	8.33%

Table 4– The Experiment Using Common Keyboard

Volunteer\Password	0000	0124	2512	3241	2267	0042	0321	2231	1120	3210
Volunteer1	1.03s	1.21s	1.32s	1.25s	1.42s	1.24s	1.31s	1.14s	1.27s	1.25s
Volunteer2	0.85s	0.98s	1.12s	1.03s	1.15s	0.93s	1.12s	0.95s	0.91s	1.32s
Volunteer3	0.91s	1.01s	1.16s	1.13s	1.32s	1.15s	1.01s	1.22s	1.33s	1.24s
Summary of Results	0.930s	1.067s	1.200s	1.137s	1.297s	1.107s	1.147s	1.103s	1.170s	1.270s

Table 5 – The Experiment Using Safe Keyboard

Volunteer\Password	0000	0124	2512	3241	2267	0042	0321	2231	1120	3210
Volunteer1	1.21s	2.22s	1.43s	1.59s	1.67s	1.94s	1.24s	1.65s	1.75s	1.73s
Volunteer2	1.01s	1.48s	1.52s	1.41s	1.45s	1.52s	1.71s	1.32s	1.42s	1.44s
Volunteer3	1.12s	1.28s	1.94s	1.72s	1.71s	1.85s	1.64s	1.15s	1.68s	1.63s
Summary of Results	1.113s	1.660s	1.630s	1.573s	1.610s	1.770s	1.530s	1.373s	1.617s	1.600s

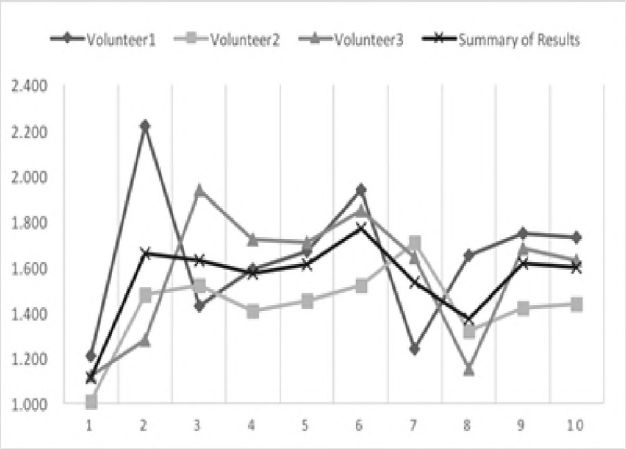

Figure 6 - Speed Evaluation Using Safe Keyboard

Based on the experiment, the safe keyboard, to some extents, reduced the convenience. This keyboard can result in a delay of approximately 0.5s seconds. However, there is no doubt that the losing 0.5s can greatly increase the safety of unlocking.

Conclusion

Unlock security for Smart Phone is introduced for improving the security of personal data and even privacy. Nowadays smartphones are used in every aspect of our lives. People also have been accustomed to save their important information such as personal information even privacy and some protected data in smartphones. The security problem attracted more and more attention in the society. Facing the security threats, this plan is aimed at improving the security from the perspective of the unlock way.

One common risk which is related to unlock is snooping. In this case, this study aims to rearrange the places of those numbers on the keyboard to improve the security. Every time you open the unlocking interface, those numbers' places are random. This method can effectively prevent people from guessing the password out through gestures.

In addition, several experiments also give the powerful support. When others are away from you 1 to 2 meters and cannot see the screen completely. Experiments indicate that others have probably 75% chance can guess out password when using the common keyboard with fixed places of numbers. But the possibility can be decreased to less 20% when using the improved keyboard. The trail comparison effectively shows the program reduce the possibility of being snooped. On the other hand, the other comparison show that people just need more 0.5s to input their password when using the new keyboard. It does not affect people experience a lot and within the acceptable range. And user can also decide whether to rearrange the keyboard or not. In this way, the program can availably increase the security and affect the experience as less as possible.

REFERENCES

1. Dunnewijk T, Hultén S. A brief history of mobile communication in Europe[J]. Telematics and Informatics, 2007, 24(3): 164-179.
2. Khan S, Nauman M, Othman A T, et al. How secure is your smartphone: An analysis of smartphone security mechanisms[C]//Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. IEEE, 2012: 76-81.
3. Mulliner C, Miller C. Fuzzing the Phone in your Phone[J]. Black Hat USA, June, 2009.
4. Jacob R J, Karn K S. Eye tracking in human-computer interaction and usability research: Ready to deliver the promises[J]. Mind, 2003, 2(3): 4.
5. Abroms L C, Westmaas J L, Bontemps-Jones J, et al. A content analysis of popular smartphone apps for smoking cessation[J]. American journal of preventive medicine, 2013, 45(6): 732-736.
6. Harbach M, De Luca A, Egelman S. The anatomy of smartphone unlocking: A field study of android lock screens[C]//Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. ACM, 2016: 4806-4817.
7. Winkler C, Gugenheimer J, De Luca A, et al. Glass unlock: Enhancing security of smartphone unlocking through leveraging a private near-eye display[C]//Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, 2015: 1407-1410.
8. Lindell A Y. Attacks on the pairing protocol of bluetooth v2. 1[J]. Black Hat USA, Las Vegas, Nevada, 2008.
9. Harbach M, Von Zezschwitz E, Fichtner A, et al. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception[C]//Symposium on usable privacy and security (SOUPS). 2014: 9-11.
10. Melnyk V. Simultaneous screen unlock and operation initiation: U.S. Patent Application 13/047,358[P]. 2011-3-14.
11. Minwook N A, Jongwoo S, Kangsik C, et al. Mobile terminal having a screen operation and operation method thereof: U.S. Patent 9,772,738[P]. 2017-9-26.
12. Cao K, Jain A K. Hacking mobile phones using 2D Printed Fingerprints[R]. MSU Technical report, MSU-CSE-16-2, 2016