The Seybold Report

ISSN 1533-9211

DOI 10.5281/zenodo.6686420

# A COMPARATIVE STUDYBETWEEN PIN-CODE AND PATTERN-BASEDSECURITYLOCK IMPLEMENTATIONSON ANDROID DEVICES

**FELICISIMO V. WENCESLAO, JR.**

College of Information and Computing Studies, Northern Iloilo State University, Estancia, Iloilo.

**ABSTRACT**

Today's Smartphone has the capacity to store a variety of sensitive information for personal and professional use. However, despite of the abundance of features to secure one's phone, many users still leave their devices unprotected putting them at risk. Several vendors of smart phones started to offer different security features for privacy and protection. Two of the most common methods used are PIN and Pattern locking mechanisms. This study aimed to determine the Smartphone security preference of the respondents, the reasons for choosing such facility and which between the two locking mechanisms provides better security based on the number of failed attempts. There were 192randomly selected participants of the study who were students enrolled in the Bachelor of Science in Information Technology at Northern Iloilo Polytechnic State College in Estancia, Iloilo during the second semester of school year 2020-2021. Among the participants, 162 were surveyed of their preferred Smartphone security lock using a researcher-made questionnaire while 30 participants were requested to take part in an experiment of cracking the pre-set security codes. They were to by-pass the four-dot Pattern-based code and the four-digit PIN-code. The numbers of attempts were recorded accordingly. One hundred (61.73%) respondents opted to use the pattern-based while 62 (38.27%) respondents chose the PIN-code. Regardless of the type of locking mechanism, the main reason for choosing the facility is for privacy and protection. Finally, it was found out that the Pattern-based locking mechanism is more secure than the PIN-code locking mechanism because there were more failed attempts made by the participants for the Pattern-based as compared to the PIN-code. However, the results of the study further revealed that there was no significant difference between the two locking mechanisms as to the number of failed attempts.

**Keywords:** Smartphone, Smartphone security, PIN code, Pattern-based

## INTRODUCTION

A Smartphone is a handheld electronic device that provides a connection to a cellular network. Smartphone’s allow people to make phone calls, send text messages, and access the Internet [1]. Even though it wasn't that long ago when it was introduced to the general public, it seems about everyone owns a Smartphone. In fact, according to fintechnews.sg (2016), the Philippines is the third largest and fastest growing market for Smartphone’s in Southeast Asia [2].

Smartphone’s today contain a lot of contents such as pictures, videos documents, messages, audio files, games and many more. These contents are important to users, and as such, would make sure that they are protected from unauthorized individuals.

Most of the users tend to use common security locks found in their Smartphone. On Android phones, users can select from Swipe, Pattern, PIN-code and password to secure their personal information. Some advance methods include Fingerprint, Facial recognition, Iris scanning

ISSN 1533-9211

DOI 10.5281/zenodo.6686420

and Voice detection [3]. Passwords and PINs are very similar in nature. The user needs to enter a predefined password or PIN to unlock the device. A password can be a combination of numbers, letters, and special symbols, while a PIN consists of only numbers. Pattern unlock is a gesture-based entry protection mechanism introduced by Google in 2008. To unlock the device with pattern unlock, instead of typing a password/PIN into a text box, the user is asked to draw a user-defined path by connecting dots in a 3x3 grid [4].

Mathematically, a four-digit PIN code has 10,000 possible combinations from 0000 to 9999[5] with the most popular PIN (i.e., 1234) accounts for 10.71% of all the 3.4 million PINs collected, followed by 1111 (6.01%), and 0000 (2%) [6]. On the other hand, a four-dot pattern has 1,624 possible patterns [7].Several studies showed that around 44% Smartphone users would select patterns that start in the upper left corner when creating their pattern [8][9]. Moreover, highly predictable shapes (e.g., Z and N), which usually starts from the corner, are easy to guess.

There can be many reasons when one chooses for his or her security lock preference. Some consider the aesthetics element while some would always consider the best level of security they can get. For others, they would simply opt for a straight-forward alternative. Harbach, De Luca, and Egelman (2016) found out that PIN users take longer to enter their codes, but commit fewer errors than pattern users, who unlock more frequently and are very prone to errors [10]. However, a recent study found out that 40% of the Android users use patterns to protect their devices instead of a PIN [11].

Several methods can be applied in order to by-pass PIN or Pattern based security lock in smart phones. These include guessing attacks, shoulder surfing attacks, smudge attacks, and side-channel attacks. In guessing attacks, attackers rank passwords from most likely to least likely and guess passwords in this order [12]. In a shoulder surfing attack, the attacker observes the login information which are being entered by the genuine user and later those credentials can be used to impersonate the actual user [13]. A smudge attack can happen when users swipe their fingers on a touch-enabled screen to form a pattern for unlocking the device and leave behind oily residues or smudges on the touch screen surface [14]. On the other hand, attacks that do not rely on brute forcing or exploiting a design weakness, but instead, are based on information gained from the physical implementation of a security scheme, are called side channel attacks [15].

**Under this attack scenario adversary observes the login information**

Which are being entered by the genuine user and later those credentials can be used to impersonate the actual user.

Under this attack scenario adversary observes the login information

Which are being entered by the genuine user and later those credentials can be used to impersonate the actual user.

Under this attack scenario adversary observes the login information

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.6686420

Which are being entered by the genuine user and later those credentials can be used to impersonate the actual user.

Under this attack scenario adversary observes the login information

Which are being entered by the genuine user and later those credentials can be used to impersonate the actual user

In [16], they found out that smudge attacks can be used that, for as long as the line of sight is not perpendicular; it is easy to observe entered patterns based on smudges. Their experiments revealed that under ideal conditions, 92% of the patterns entered were partially identifiable and 68% of the entered patterns were fully recoverable. Under less ideal conditions, 37% of the patterns were partially recoverable and 14% were fully recoverable. In another study, [17] investigate the effectiveness of combining Markov model based guessing attacks with smudge attacks. Their investigation showed that this combined method can significantly improve the performance of pure guessing attacks, cracking 74.17% of patterns compared to just 13.33% when the Markov model-based guessing attack was performed alone.

In [18], they developed novel video-based attack to reconstruct Android lock patterns from video footage filmed using a mobile phone camera. Results of their experimental showed that their technique can break over 95% of the patterns in five attempts and concluded that complex patterns do not offer stronger protection.

The purpose of this paper is to survey the preferred security lock among Smartphone users between PIN and pattern and identify the reasons why users preferred such. The security strength shall be determined by the number of unlocking attempts to be made before a successful breach is achieved and determine whether significant difference exists between the two lock implementations.

## METHODOLODY

We divided this study into two phases. The first phase was a survey on the demography of the target respondents. Survey questionnaires were provided to the selected participants. The survey determined the respondents' preferred security lock, Smartphone ownership, the content of the Smartphone and the reason of using the said security. The second phase included an experiment where the participants were requested to by-pass the Smartphone's security locks using known techniques.

### Respondents of the Study

There were a total of 192 respondents in this study. As previously mentioned, the study is divided into two phases. Thus, during the first phase, we have requested 162 respondents to answer the researcher-made survey questionnaires. For the phase 2 of the study, 30 respondents were requested to participate in the experiment.

They were students enrolled in the Bachelor of Science in Information Technology at Northern Iloilo Polytechnic State College, Estancia, and Iloilo during the Second Semester,

ISSN 1533-9211

DOI 10.5281/zenodo.6686420

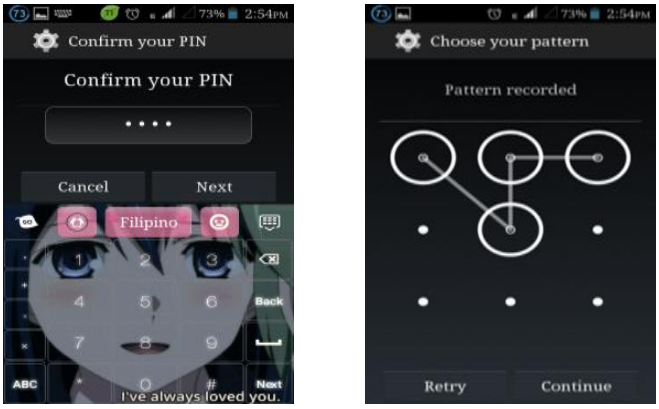
School Year 2020-2021. They were randomly selected using a simple random sampling technique from a population of 336 students.

**Data Collection Procedure**

Prior to the actual conduct of the study, the researcher-made survey questionnaire were subjected to item validation and reliability testing using appropriate statistical treatment. When the total number of respondents for the study was ascertained, we immediately handed out survey questionnaires to them. They were oriented with the purpose of the study and were asked to answer as honestly as they can. The survey questionnaires were then retrieved, tabulated and analyzed.

Subsequently, thirty (30) students were asked to participate in the second phase of the study. These students were at their third year level in the BS Information Technology major in Network and Security Track. They were selected because of the theories learned in their previous courses.

We prepared five (5) Smartphone and lock those using 4-digit PIN. We then asked 30 participants, in a batch of five at a time, to try to unlock the smart phones. They were also instructed to record the number of attempts made until a successful unlocking. As soon as the device was unlock, the Smartphone owner would then change the PIN and have another participant to unlock it. The same processes were implemented for the 4-dot Pattern-based security lock. Figure 1 shows a typical Android Smartphone locked screen for PIN (a) and pattern (b)




(a) PIN-Code (b) Pattern-based

**Figure 1: A typical Android Smartphone Locked Screen.**

In theory, the more failed attempts were made, the better level of security the locking method can provide. For this study, we devised a scale to verbally interpret the mean failed attempts as follows: 258.41 or more (Most Secured), 193.81 to 258.40 (Moderately Secured), 129.21-193.80 (Average), 64.61-129.20 (Less Secured) and 64.60 or below (Not Secured).

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.6686420

## RESULTS AND DISCUSSION

### Distribution of Respondents by Smartphone Lock Preference and Sex

Based on the survey conducted with the respondents, it was found out that the most preferred security mechanism for Smartphone users was the Pattern-based. Sixty-two respondents or 38.27% opted to use the PIN-code while 100 respondents or 61.73% choose Pattern-based to secure their phones. Out of 62 respondents who used the PIN-code, 17 were males and 45 were females. Similarly, for those who chose Pattern-based, 28 were males while 72 were females. Figure 2 shows the distribution of respondents by Smartphone lock preference and sex.

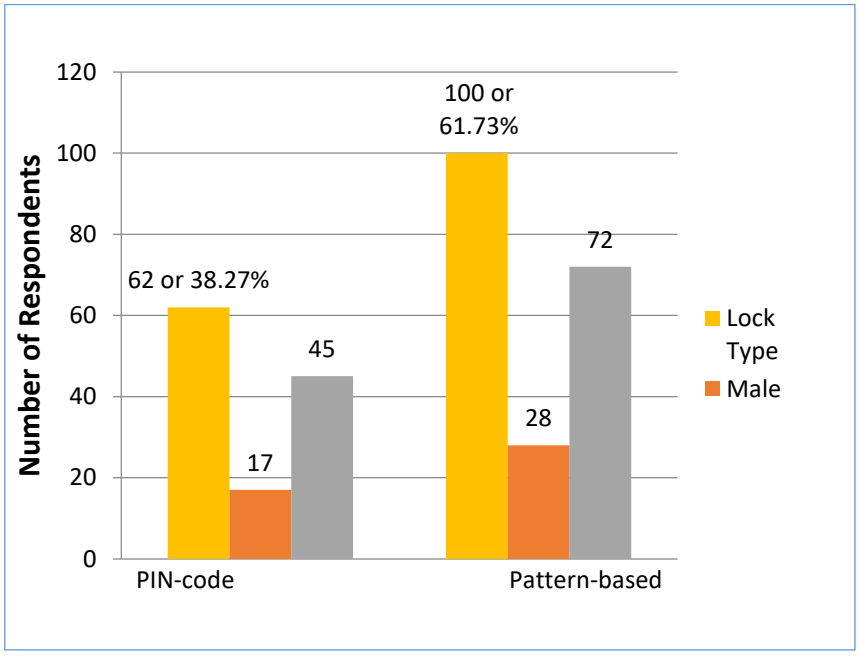



**Figure 2: Distribution of Respondents by Smartphone Lock Preference and Sex.**

### Distribution of Respondents as to Smartphone Ownership

Based from the survey being conducted it was found out that among the respondents, 133 (82.10%) respondents said that they owned one Smartphone device, 25 (15.43%) owned two smart phones while four (2.47%) respondents said they owned three or more Smartphone devices. Figure 3 shows the ownership of Smartphone's among the 162 respondents.

ISSN 1533-9211

DOI 10.5281/zenodo.6686420

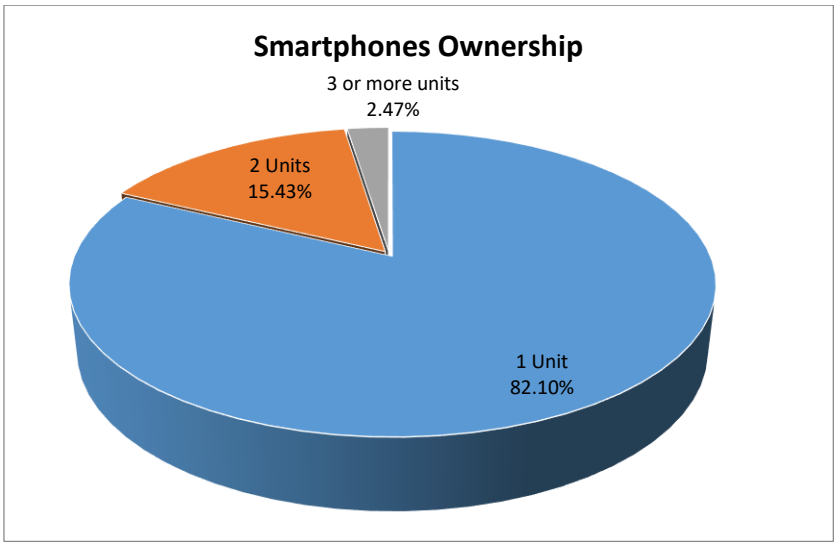



**Figure 3: The Distribution of Smartphone Ownership among Respondents.**

**Reasons for Choosing the Smartphone Security Lock**

The respondents were asked about the reasons as to why they chose to use the type of security locking mechanism. They were asked to select the primary reason for such. The options include 1) Ease of Use, 2) User-friendly, 3) For privacy and protection and 4) It provide better security.

For the respondents who chose Pattern-based, 50 respondents said that they chose it because they believe it can provide better security and protection; 24 said it is easy to use; 19 respondents said they felt that it can provide better security and 7 respondents thought that it is user-friendly.

Similarly, respondents who opted to use PIN lock, the most prevalent reason is that it can be used for privacy and protection for 33 respondents. To the 16 respondents, they said that the PIN lock can provide better security, 9 respondents said it is easy to use while 4 respondents said it is user friendly. Figure 5 shows the different reason for choosing PIN-code and Pattern-based as a Smartphone security. Figure 4 shows the various reasons of the respondents for choosing their preferred security lock.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.6686420

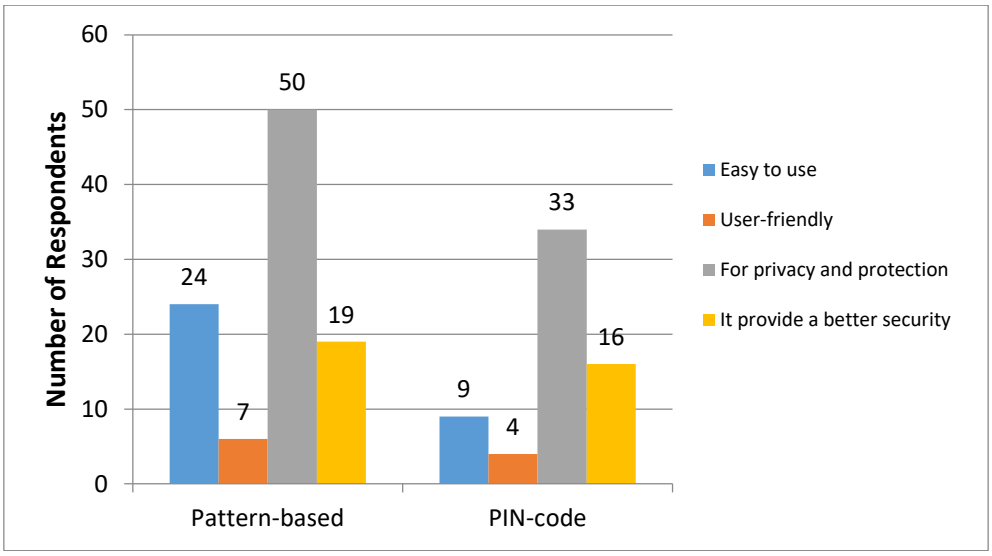



**Figure 4: Reason for Choosing PIN-code and Pattern-based as a Smartphone Security.**

**The Mean Unlocking Attempts Using PIN-code and Pattern-based Security Locks**

From the conduct of the unlocking experiment, it was found out that there were a total of 2,546 failed attempts made by the thirty respondents for the PIN-code. The failed attempts have yielded a mean of 84.87 (SD = 84.889) described as "less secured". On the other hand, in the pattern-based lock, the recorded failed attempts were 2,651 made by the same thirty respondents with a computed mean of 88.37 (SD = 72.269) which can also be described as "less secured". It is worth mentioning that at some point during the experiment, one respondent was able to unlock the PIN in just two (2) attempts while six (6) attempts were recorded as the fastest tries for the pattern-based. However, other participants were able to do it in more than 300 attempts. We described the strength in the security of locking implementations as Scale in strength258 or more attempts as “most secured”, 193 to 257 attempts as “moderately secured”, 129 to 192 attempts as “average security”, 64 to 128 attempts as “less secured” and 63 or less attempts are considered “not secured”. Table 1 shows the mean unlocking attempts using the PIN-code and Pattern-based security locks.

**Table 1: The Failed Attempts of PIN-code and Pattern-based Security Locks.**

| Type of Security | Standard Deviation | Mean | Interpretation |
|---|---|---|---|
| PIN-code | 84.889 | 84.87 | Less Secured |
| Pattern-based | 72.269 | 88.37 | Less Secured |

ISSN 1533-9211

DOI 10.5281/zenodo.6686420

**Difference between Pattern-based and PIN-code as to the Number of Unlocking Attempts**

When computed using the Mann-Whitney U statistics, the result showed that there was no significant difference between Pattern and PIN-code as to the number of unlocking attempts. The results revealed that the computed U value is 415.000 and the obtained Sig.(2-Tailed) value was .605 which is greater than 0.05 alpha level of significance. This suggests that whether a Smartphone user employs a 4-digit PIN or a 4-dot pattern, the level of their security lock is just the same. Our hypothesis stating that there is a significant difference in the level of security between the two methods is rejected. Table 2 shows the result.

**Table 2: Difference between Pattern-based and PIN-code as to the Number of Unlocking Attempts**

| U | z | P |
|---|---|---|
| 415.000 | -.518 | .605 |

*Significant at 0.05 alpha level

## CONCLUSION

This study aimed to determine the Smartphone security preference of the respondents, the reasons for choosing such facility and which between the two locking mechanisms provides better security based on the number of failed attempts. The results of this investigation revealed that 100 (61.73%) respondents opted to use the pattern-based while 63 (38.27%) respondents chose the PIN-code. Regardless of the type of locking mechanism, the main reason for choosing the facility is for privacy and protection. In the experiment conducted, the PIN-code was cracked with just two attempts while it only took six attempts for the Pattern-based to by-pass. This means that while attempts can go as many as more than 300, it is also possible to by-pass security locks with just few attempts. We conclude that the 4-dot pattern-based and the 4-digit PIN-code security locking features in Android smart phones can only provide less security. There was no significant difference between Pattern-based and PIN-code as to the number of unlocking attempts. Thus, our hypothesis stating that there is a significant difference between Pattern based and PIN-code as to the number of unlocking attempts is rejected.

### REFERENCES

1) Franken field, J. (2018, Mar 1). Smartphone. Retrieved fromhttps://www.investopedia.com/terms/s/smartphone.asp
2) A Profile of Smartphone Users in the Philippines. (2016, September 4). Retrieved fromhttps://fintechnews.sg/5181/fintechphilippines/a-profile-of-smartphone-users-in-the-philippines/
3) Agomuoh, F. (2019, March 22). Common Smartphone Security Features and How They Work.Retrieved fromhttps://www.online-tech-tips.com/smartphones/common-smartphone-security-features-and-how-they-work/

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.6686420

4) Sun, C., Wang, Y. & Zheng, J. (2014). Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. Journal of Information Security and Applications. 19. 10.1016/j.jisa.2014.10.009.
5) Pinola, M.(2012, September 19). The Most (and Least) Common PIN Numbers and Numeric Passwords. Is Yours One of Them?.Retrieved fromhttps://lifehacker.com/the-most-and-least-common-pin-numbers-and-numeric-pas-5944567#:~:text=There%20are%2010%2C000%20possible%20combinations,3.4%20million%20passwords%20are%201234.
6) Wang, D. Gu†, Q., Huang, X. &Wang, P. (2017). Understanding Human-Chosen PINs: Characteristics, Distribution and Security. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications DOI: https://dl.acm.org/doi/proceedings/10.1145/ 3052973
7) Sinha, A. (2014). Rorschach Based Security Application for Android. International Journal for Scientific Research & Developmen 2 (07). Pp 554-557
8) Uellenbeck, S., Dürmuth, M., Wolf, C. & Holz, T. (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). Association for Computing Machinery, New York, NY, USA, 161–172. DOI: https://doi.org/10.1145/2508859.2516700
9) Løge, M., Drmuth, M., &Røstad, L. (2016). On User Choice for Android Unlock Patterns. In Proceedings of the European Workshop on Usable Security, Euro USEC ’16, Darmstadt, Germany, January 2016. DOI:10.14722/eurousec.2016.23001
10) Harbach, M., De Luca, A. & Egelman, S. (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). Association for Computing Machinery, New York, NY, USA, 4806–4817. DOI: https://doi.org/10.1145/2858036.2858267
11) Bruggen, D. V. (2014). Studying the Impact of Security Awareness Efforts on User Behavior. Ph.D. Dissertation. University of Notre Dame.
12) Liu, C., Clark, G. & Lindqvist, J. (2017). Guessing Attacks on User-Generated Gesture Passwords. In Proceedings of the ACM Interact. Mob. Wearable Ubiquitous Technol. 1, 1, Article 3 (March 2017). DOI: https://doi.org/10.1145/3053331
13) Chakraborty, N., Randhawa, G., Das, K. & Mondal, S. (2016). MobSecure: A Shoulder Surfing Safe Login Approach Implemented on Mobile Device. Procedia Computer Science. 93. 854-861. DOI: 10.1016/j.procs.2016.07.256.
14) Guerar, M., Merlo, A., & Migliardi, M. (2017). ClickPattern: A Pattern Lock System Resilient to Smudge and Side-channel Attacks. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 8, 64-78.
15) Andriotis, P., Tryfonas, P., Oikonomou, G. &and Yildiz, C. (2013). A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In Proceedings of the 6thACM conference on Security and privacy in wireless and mobile networks (WiSec '13). Association for Computing Machinery, New York, NY, USA, 1–6. DOI: https://doi.org/10.1145/2462096.2462098
16) Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M. (2010). Smudge attacks on smartphone touch screens. In Proceedings of the 4thUSENIX Conference on Offensive Technologies (WOOT’10), Washington, DC, USA, 1–7.
17) Cha, S., Kwag, S., Kim, H. &and Huh, J. (2017). Boosting the Guessing Attack Performance on Android Lock Patterns with Smudge Attacks. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17). Association for Computing Machinery, New York, NY, USA, 313–326. DOI: https://doi.org/10.1145/3052973.3052989
18) Ye, G., Tang, Z., Fang, D., Chen, X., Kim, K., Taylor, B. &Wang, Z. (2017). Cracking Android Pattern Lock in Five Attempts. 10.14722/ndss.2017.23130.