Brute Force Attack on Mobile Keypad

Vishal Singh
Department of Computer Science & Engineering
MANIT, Bhopal

Namita Tiwari, PhD
Department of Computer Science & Engineering
MANIT, Bhopal

ABSTRACT
In recent years, mobile is a very useful and important device for everyone because of it's functionality. By the end of 2016 smartphone users are more than 2 billions according to the times of new York. Smartphone contain sensitive data so if they loss or hacked a big problem may arise directly or indirectly so mobile devices should be secure from different-different type of attacks. So security is a big issue. Basically there are 2 major attacks happens on mobile keypad locks. First one is brute force attack and the second one is smudge attack. Smudge attack also known as passive attack because in smudge attack attacker first have to collect and analyse the data.

Keywords
Brute force attack(BFA), Smudge attack(SA), Completion rate(CR), error rate(ER), average(avg).

1. INTRODUCTION
A smartphone offers variety of features like phone call, gps, images etc. smartphone users are increasing day by day because it provides variety of features. There are basically four types of lock. First one is numeric lock. In this type of lock user have to enter digits to unlock the smartphone. The second type of lock is pattern lock. In this type of lock user have to draw pattern to unlock mobile. Third one is biometric authentication in which registered finger print or iris scan is required for unlock the mobile phone. Last one is graphic lock in which user have to choose four images out of nine images to unlock the mobile phone.

1.1 Anti Theft Program
F-secure is a anti theft program. F-secure is used prevent misuses of a smartphone by finder or hacker. User can remotely lock the mobile phone with the help of F-secure. When attacker try to unlock the mobile phone F-secure sense his fingerprint and matches with the registered fingerprint if not matches then send an alert message to the registered mobile number.

1.2 Smudge Attack
Smudge attack is the first type of attack. This type of attack happens on the mobile pattern lock on a touchscreen only. When user is unlocking their mobile phone then attacker capture that movement using a camera. Then attacker hack the password by using a good image processing technique on that image. There is 68% chance of success rate in smudge attack.

Smudge attack is passive attack because attacker first have to collect and analyse the data.

Fig.1 Snapshot of smudge attack.

1.3 Brute Force Attack (BFA)
The second type of attack is brute force attack. brute force attack is a trial and error method to obtain the password or pin. BFA always give result if successful completed. If the mobile password is set to four digit then the attacker will start guessing form 0000 to 9999. Thus he will able to crack the passcode within 10,000 attempts on average he will crack the password in 5000 attempts.

$$T_T = 5000NT_IT_P$$

Here T_T defines the total time taken to crack the password by the attacker. T_I denotes the time taken for attacker to identify the position of the number, T_P denotes the time taken to press the button and N denotes the total number of button press. Thus the avg completion time for guessing the password is 3.4 seconds so it will take total 4.7 hours to unlock the mobile phone.

1.4 Problem with Fixed Keypad
If the password length is set to four digits then brute force attack easily takes place in mobile keypad. There is some way to make brute force attack more difficult on mobile keypad. First one by using 8 bit code. By using 8 bit brute force attack is more difficult because guessing 8 bit number is not easy. But in this type of lock scheme user have to memorize 8 bit code which is not easy and it is time consuming. The second scheme is pattern lock. By using pattern lock brute force attack is avoided but smudge attack is easily happens on mobile screen lock. Third one is biometrics authentication. Biometrics authentication is a good solution for brute force attack on mobile keypad. But sometime it is difficult to owner to authenticate himself when his finger is sweat or damages.

In section II, various algorithms are explained for mobile keypad security from brute force attack. In section III, a comparative analysis of algorithms is given. In section IV, The conclusion and some future research options are given.

2. LITERATURE REVIEW
There are various algorithms given to make brute force attack more difficult. The basic problem with fixed keypad is that if it is four digit pin then attacker will crack it within average 5000 attempts.

2.1 Randomized Keypad [Young Sam Ryu, do hyong kho et al, 2010]
Young Sam Ryu proposed randomized keypad to make brute

force attack more difficult in smartphones. In fixed keypad the sequence of all keys are always same whenever user whats to enter the keys. But in randomized keypad the sequence of key are always different. Every time a new sequence of key present on keypad. So the brute force attack on this type of keypad is more difficult and time consuming because attacker have difficulty to follow a sequence.

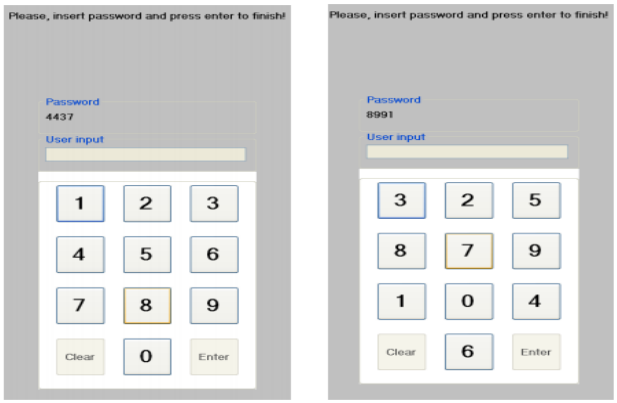

Fig.2. Fixed vs Randomised Keypad

Fig. 2 shows a comparison between fixed and randomized keypad. The avg. completion time for randomized keypad is higher than fixed keypad.

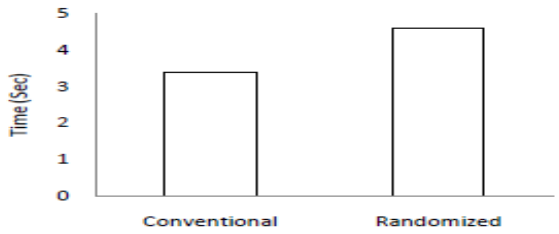

Fig.3. avg. completion time

The avg. CT with randomized keypad is 4.5 sec. and avg. CT with convention keypad is 3.4 sec. The error rate with fixed keypad are higher than fixed keypad.

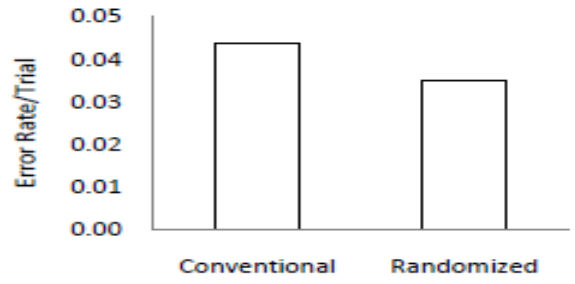

Fig.4. avg. error rate

The avg. error rate with fixed keypad is 0.04 sec. and avg. error rate with randomized keypad is 0.03 sec.

2.2 [I. Kim, 2010]

A new randomized keypad is suggested by I. kimin 2010. In which 5 keys out of all 10 keys are arranged on random positions. Here is seletion of random key and random position are determined using a random function. The key are selected and stored at random places without repetition using random function and stored in sequence in an array memory.

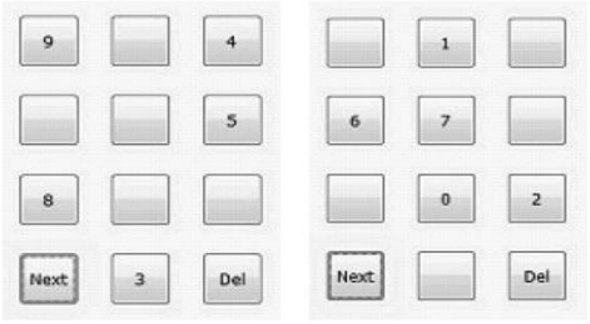

Fig.5. Proposed Randomized Keypad

In this type of keypad 5 key are selected out of all 10 keys using random function. Let assume user's password is 6549.first user have to enter 6 but 6 is not there in initial keypad so he will press next key so that remaining 5 keys are shown to the user which is stored in array. If the key is present in initial keypad then press the key if it is not present in initial keypad then press the next key so that remaining keys are visible to user.

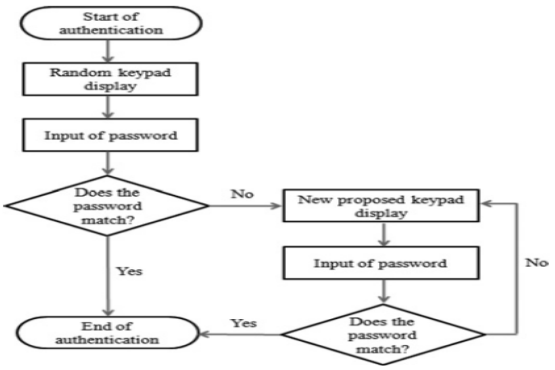

Fig.6. flow chart of proposed randomized keypad

Here is flow chart of authentication process of randomized keypad if user gives correct password in first attempt then screen will unlock otherwise new randomized keypad will displayed until he enter the correct password.

2.3 [Klein et al, 2012]

klein suggested a little bit modification in randomized keypad for making brute force attack more difficult by using penalty p. each time whenever user enter a wrong password he has to wait till penalty p time because keypad is disabled till p time. By using this lock scheme attacker needs approx 9.62 sec. for guessing one four digit password. If we set 25 sec. penalty then attacker needs more then 2 days to crack the password. In this type of lock scheme the time required for unlocking the mobile phone using brute force attack is depends on the penalty.

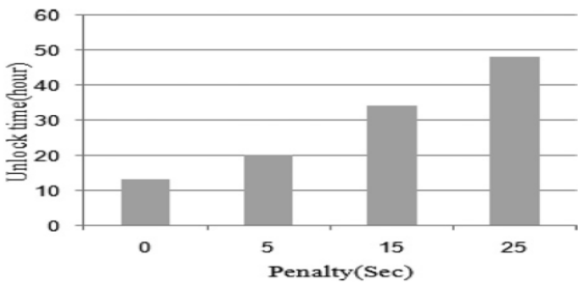

Fig.7. Time Required According to Penalty

Here time is given according to penalty. As much as penalty time increases the required time for unlocking the mobile phone is also increases.

2.4 [Yanyan Li et al , 2014]

A new approach for authentication is proposed by yanyan li. He proposed a 2 way authentication process in which 2 different kind of lock scheme are combined. This type of lock scheme are secure but time consuming because user has to enter password two times. User has to memorize two different-different type of password. Both the password are needed at the time of authentication.

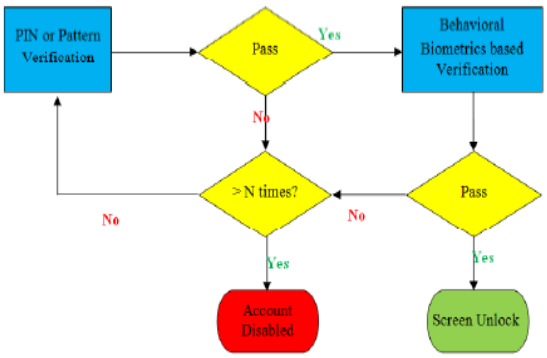

Fig.8. Flow Chart of 2 way Authentication Process

Here is the flow chart of 2 way authentication process. In which first type of password is pin or pattern and the second type of password is biometrics. If user give both the password correct then only screen will unlock. If user give correct pin then it will go to the second type of password which is biometrics. If user give wrong password then he will repeat the same process N times. If he attempts more then N time then user's account will disabled for a limited time.

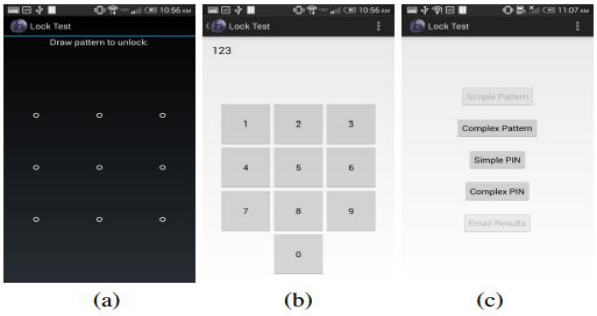

Fig.9. snapshot of 2 way lock scheme

Here is snapshot of 2 way authentication lock scheme. The first lock scheme is pattern and the second type of lock scheme is pin. If user enters both the password correctly then only screen will unlock.

3. COMPARISON AND ANALYSIS

The randomized keypad given given by young sam yu is a solution for brute force attack but BFA is also happens on this type of lock scheme. It will take some extra time to crack the mobilekeypad lock.

The second lock scheme introduce by I. Kim in 2010. This type of lock scheme is more secure against BFA because in this type of lock scheme only 5 keys are shown at a time next 5 keys are available to user by pressing next button.

The third type of lock scheme is proposed by klein in 2012. He suggested the penalty which is added each time whenever user enters a wrong password. By using this scheme attacker guess one password in 9.62 seconds which is better then previous one.

The fourth type of lock scheme is suggested by yanyan li in 2014. He proposed a 2 way authentication process. It is secure against BFA attack because two time authentication is needed for unlocking the mobile lock screen but it is time consuming.

4. CONCLUSION AND FUTURE WORK

The next generation of smartphone have in built projector, seamless voice control, 3d screens and important data so we need a good security scheme for keep the things safe because if we loss that data problem will arise directly or indirectly. The existing keypad lock schemes are not so good because every lock scheme has some drawbacks. So we need a secure keypad lock algorithm which is secure against all type of attacks.

5. REFERENCES

[1] [Young Sam Ryu,2010]"Usability Evaluation of Randomized Keypad" Department of Computer Science,Texas State University-San Marcos, Vol. 5, Issue 2, February 2010, pp. 65-75

[2] [I. Kim,2010]" Keypad against brute force attacks on smartphones", IEEE transactions on security, 2010.

[3] [Adam J. Aviv et al,2010], Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith,"Smudge Attacks on Smartphone Touch Screens",2010.

[4] [Yanyan Li et al,2014], Junshuang Yang, Mengjun Xie, Dylan Carlsony, Han Gil Jangz, Jiang Bian," Comparison of PIN- and Pattern-based Behavioral Biometric Authentication on Mobile Devices",IEEE transaction paper,2014.

[5] [K. K. Brajesh,2012],An Approach For User Authentication One Time Password (Numeric And Graphical) Scheme, Journal of Global Research in Computer Science, 3, 54-57.

[6] [Ihor Vasyltsov,2016], *Senior Member, IEEE*, Changgyu Bak," Method for Seamless Unlock Function for Mobile Applications",2016.

[7] [K. I. Shin et al,2012],"Design and Implementation of Improved Authentication System for Android Smartphone Users," in Proc. 26th Int. Conf. Advanced Information Networking and Applications Workshops (WAINA 12), 2012, pp. 704–707.

[8] [Hirsch, S.B. ,1982],Secure keyboard input terminal, United States Patent #4,333,090: United States Patent and Trademark Office, 305 Peck Dr., Beverly Hills, CA 90212.

[9] [Marian Harbach1 et al,2010],Alexander De Luca2, Serge Egelman1;3 1International Computer Science Institute, Berkeley, CA" The Anatomy of Smartphone Unlocking A Field Study of Android Lock Screens", 2010.