Improved Authentication System for Android Smartphone

Shrabani Medhi[1], Pinky Saikia Dutta[2]

Assistant Professor, Department of Computer Science and Engineering, College, Guwahati, India[1]

Assistant Professor, Department of Computer Science and Engineering, College, Guwahati, India[2]

Abstract: The popularity of Smartphone is increasing day by day especially the one using android operating system. Since these devices contain increasing amount of personal information, it is important to have better security system. In this paper we try to see the different aspects that must be kept in mind while enforcing security in android Smartphone. We also discuss and compare the various authentication systems available and present a new improved authentication system that tries to remove the drawbacks present in the current authentication systems.

Keywords: Android, security, authentication lock screen, smart phone, color lock pattern.

I. INTRODUCTION

Most of the devices used in IT services are rapidly changing from PCs and laptops to tablets and smart phones. Since these devices contain important personal information, better security is required. Major problems could occur if the mobile is lost. So proper authentication system is very important. Different authentication schemes are available with both advantages and disadvantages. The authentication schemes must be made by keeping in mind the requirements of the users and the android architecture.

SECURITY ASPECTS OF ANDROID SMARTPHONE

There are many security related problems associated with android smart phone. So while solving the security issues these problems must be kept in consideration. These issues mainly arise because of the following characteristics of the android smart phone.

- Portable: There is a probability of the smart phone being lost because of its small size. This can lead to the leakage of personal and business information, such as social networking information, internet banking information, schedules, etc.

- Openness: There are some advanced features in android smart phone, using which user can easily share applications. Having a variety of external interfaces provides path for malicious code propagation and will leave the internal interface vulnerable [1].

- Low memory: Smart phones have relatively low memory compared to PCs or desktop. The application to monitor the security of the smart phone is limited by the size.

- Low efficiency: Smart phones have low efficiency and low power compared to PCs.

II. POPULAR AUTHENTICATION SCHEME FOR ANDROID SMARTPHONE

There are various authentication schemes available for android smart phone. Some of the most widely used schemes are—

- Slide lock: It is a touch-horizontal slide. [5] It is a lock screen provided by Android and IOS. It doesn't provide security. But the system is convenient for user. It is most commonly used and basically the default. There are no passwords or patterns. It is simply a way to keep the phone turned on. [3]
- Glass lock: It is based on Android OS and used by Samsung devices. It is same as slide lock and can be dragged in all directions. There is no security.
- Keypad lock: It requires a four digit password. The key space is from 0 to 9999. This scheme is not that convenient because it needs repetitive touching by the user. It provides normal security. [3]
- Pattern lock: It contains 9 dots on the screen. Each dot can be touched and dragged one dot at a time. Redundancy input is not available. Since 9 dots are available. It provides almost one million of key space = 9P4 + 9P5 + 9P6+ 9P7 + 9P8 + 9! It provides normal security. It provides for easy dragging by the user. So it provides normal convenience. If the user uses an easy pattern there is weak security. And if the pattern is complex it will be inconvenient for the user. If someone finds out the pattern from the oily residue left by stroking fingers on the phone screen, there won't be much security. This is called smudge attack. [3]
- Finger scan: This scheme is used by Atrix smart phone, made by Motorola. It provides a finger scanning system. It provides both good security and convenience. There is no chance of smudge attack. The main problems of this scheme are overlapping processes and low speed. [2].

Based on different researches in this field researcher have found that users don't prefer very complicated authentication schemes. But it is not suggestible to user a simple scheme compromising the authentication. Keeping this point as the basis we can conclude that pattern lock is the most popular and widely used authentication scheme. Users prefer it because of the easy dragging. However, there is always a possibility of smudge attack in this scheme.

III. PROPOSED APPROACH

We have developed an authentication system for android smart phone that is both user friendly and provide more authentication than the current authentication schemes that are available. We have developed the lock screen system that is based on pattern scheme.

The system consists of nine dots arranged in a matrix of 3 × 3. Redundancy input is allowed i.e. retouching the dots. When the dots are touched it changes colors. Maximum of seven retouching is allowed, i.e. each time a dot is touched it changes color seven times. If the password is entered correctly then only the screen will be unlocked.
The security power depends upon the size of the key space. The bigger the key space, the more difficult is a brute force attack. Comparing our system to the Pattern Lock and number password systems, the Pattern Lock has about one million key spaces, the number password system has about 10,000 key spaces, and our Lock Screen system has about ten million (7^9 = 10077696) key spaces. It can also be made larger by increasing the number of repetitive touches.

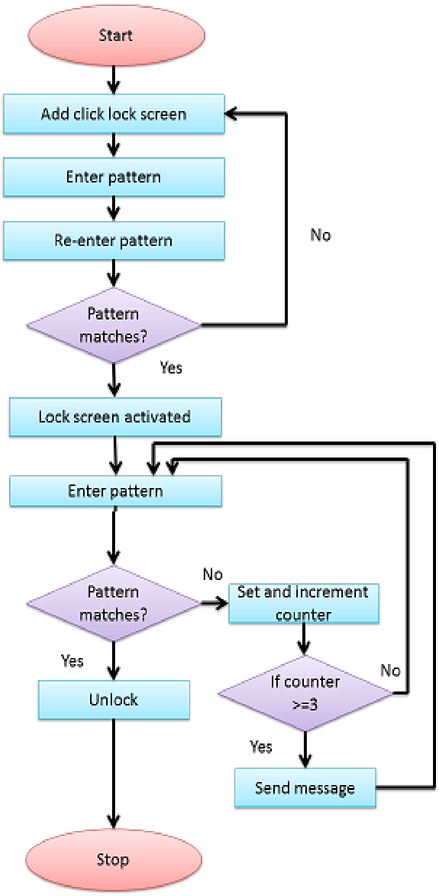

Fig.1. Workflow diagram for the proposed system

A. Setting Of Pattern as Password
First we will have to enter the color pattern that we want to use as password.

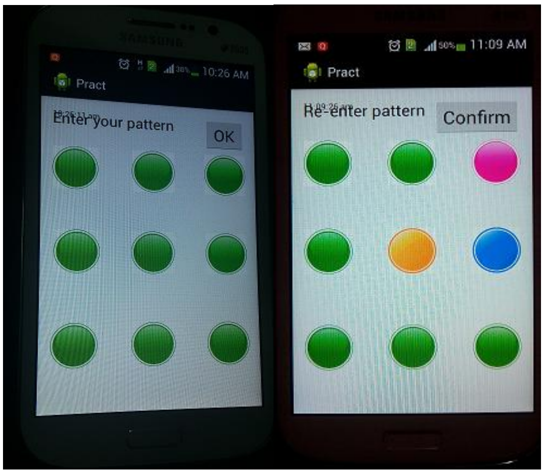

Fig .2. Pattern entry and confirmation

B. Setting Mobile Number

We need to give one phone number so that if some unauthorized person tries to unlock the phone, a message will be sent to that phone number. Message will be sent if the unauthorized user tries to unlock the phone three or more than three times.

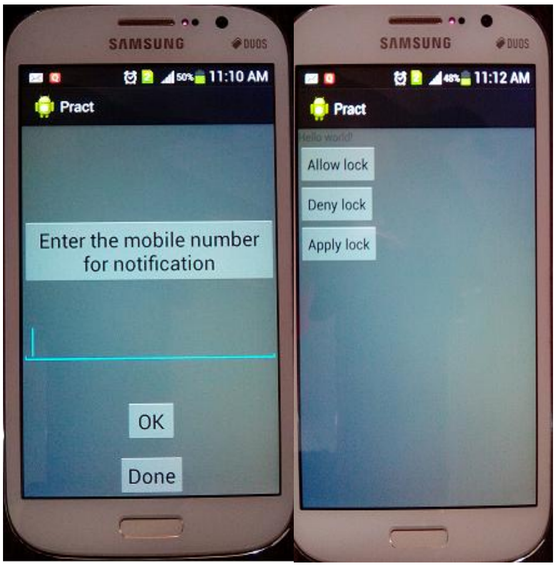

Fig. 2. Setting mobile number and applying lock

C. Unlock Password

When the user tries to unlock that pattern will appear. User will have to enter the pattern. If the entered pattern matches with the already saved pattern then only the phone will be unlocked else we will have to keep trying to enter the pattern. And Message will be sent to the previously registered number if the unauthorized user tries to unsuccessfully unlock the system for more than three times.

DOI 10.17148/IJARCCE.2016.55153

IV. COMPARISON WITH CURRENT AUTHENTICATION SCHEME

TABLE I Comparison with slide lock

SL NO.	SLIDE LOCK	PROPOSED AUTHENTICATION SCHEME
1	No security.	Security is present.
2	Personal information at risk.	Personal information not at risk.
3	Easily accessible by unauthenticated users.	Not easily accessible by unauthenticated users.
4	Necessitates extra security applications.	No need of extra security applications.

TABLE II Comparison with glass lock

Sl No.	GLASS LOCK	MODIFIED AUTHENTICATION SCHEME
1	No security.	Security is present.
2	Personal information at risk.	Personal information not at risk.
3	Easily accessible by unauthenticated users.	Not easily accessible by unauthenticated users.
4	Necessitates extra security applications.	No need of extra security applications.

TABLE III Comparison with keypad lock

Sl No.	KEYPAD LOCK	MODIFIED AUTHENTICATION SCHEME
1	Inconvenient for users.	Convenience is present.
2	Requires paying attention while inputting the password from keypad.	No need to use the keypad.
3	Consumes time before unlocking.	Doesn't consume time.
4	Key-space is less.	Key-space is much more. It is about ten million.

TABLE IV Comparison with pattern lock

Sl No.	PATTERN LOCK	MODIFIED AUTHENTICATION SCHEME
1	There is smudge attack.	There is no smudge attack.
2	Doesn't provide much security if simple pattern is used.	Even simple pattern provides security.
3	Not comfortable if complicated pattern is used.	Comfortable even if complicated pattern is used.
4	Key-space is less. It is about one million.	Key-space is much more. It is about ten million.
5	No repetitive use of dots allowed.	Same dot can be used repetitively.

TABLE V Comparison with finger scan

Sl No.	FINGER SCAN	MODIFIED AUTHENTICATION SCHEME
1	Overlapping processes on screen.	No overlapping processes on screen.
2	Speed is low.	Speed is fast.
3	Finger recognition takes time.	Pattern recognition doesn't take much time.
4	Not user friendly.	User friendly.
5	Changes in fingertip skin causes problem.	Works fine in all conditions.
6	Causes problem if skin condition varies enough from summer to winter.	Works fine in all conditions.

V. CONCLUSION

In this paper we have done a study of the security issues that must be kept in mind while designing the authentication schemes. We have studied the popular authentication schemes available along with their advantages and disadvantages. Here we have developed an improved authentication scheme that provides both authentication and convenience to user. We have made theoretical comparison of my system with the current schemes and suggest that it is better in terms of security, convenience, key-space and authentication. Here we have developed an authentication system for android smart phone that is both user friendly and provide more authentication than the current authentication schemes that are available. Our lock screen system is based on color pattern. The system consists of nine dots arranged in a matrix of 3 × 3. Each time a dot is touched it changes color seven times. If the password is entered correctly then only the screen will be unlocked. We give one phone number so that if some unauthorized person tries to unlock the phone, a message will be sent to that phone number. Message will be sent if the unauthorized user tries to unlock the phone three or more than three times.

REFERENCES

[1] DAI-Labor, "Malicious Software for Smartphones," Technical Report, 2008.

[2] Atrix, Motorola, http://www.motorola.com

[3] Android Security Overview, Android open source project, http://source.android.com/tech/security/index.html

[4] Design of Image Based Authentication System for Android Smartphone Users. International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013

[5] Design and Implementation of Improved Authentication System for Android Smartphone Users. 2012 26th International Conference on Advanced Information Networking and Applications Workshops