

A Survey Paper on Authentication System in Android Phones

Mr. Gaurav R. Chimote, Prof. N.M. Tarbani

Abstract— Development and awareness of technology has lead to rapid increase in number of smartphone users around the world. These devices provide various facilities to us. These devices allow us to use internet including browsing and downloading, camera, play games, GPS tracking and many more. Smartphones also contains our personal stuff including photos, contacts, messages, personal information etc. Therefore security of smartphones is of utmost importance. Misuse of this information may result in privacy breaches and sensitive data leakage. The first line of defense is screen lock. Screen lock can be set by various methods. One such method is pin pattern. We have proposed a method that dynamically changes the pin pattern without user intervention.

Index Terms— Screen lock, Dynamic Pin Generation, Android Framework, Linux Kernel..

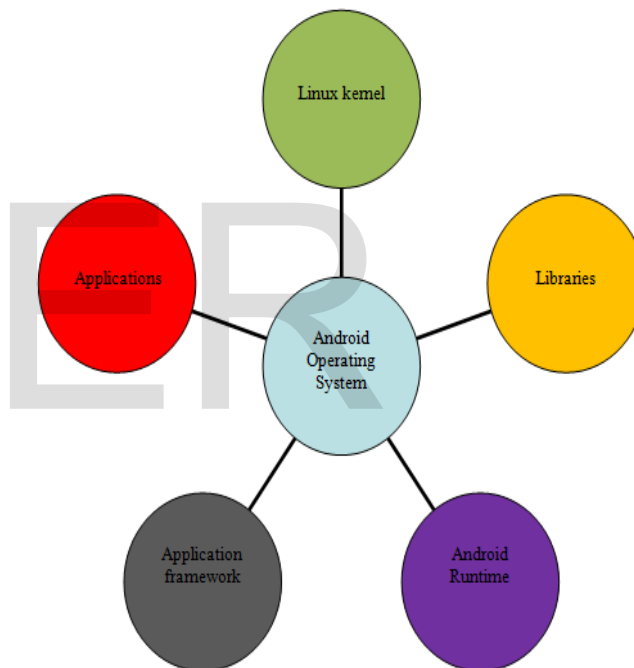
1 INTRODUCTION

The Emergence of android operating system in mobile phones has lead to a rapid increase in smartphone users [1]. An android phone runs on Google's open source android operating system. Currently a new version known as Marshmallow of android operating system has been launched. These versions are developed for increasing security and other features in an android based smartphones. A smartphone allows you to perform various activities. Therefore smartphones have become an important part of our life. These devices may contain all our personal information such as photos, contacts, messages, bank information etc. Therefore if these devices are stolen or left behind and fallen into wrong hands then it may lead to a grave problem.

If such condition arises then the first thing comes is a screen lock [2]. Screen lock protects our phones from unauthorized access by outsiders. But the problem still exists as the user needs to set pin or password manually. If the pin or password is seen by prying eyes then they can use smartphone maliciously unless the user again changes his/her pin or password. The problem with existing lock screen is that the user needs to change the pin or password regularly. The proposed system contains an upgraded Lock Screen system, which changes the pin or password dynamically without the user requiring changing it manually every time.

2 BACKGROUND

Detailed Android operating system is a stack of software components which is roughly divided into five sections as shown below in the architecture diagram.



2.1 Linux kernel

The first section is the Linux kernel. This provides basic system functionality like process management, memory management, device management like camera, keypad, display etc. Also, the kernel handles all the things that Linux is really good at such as networking and a vast array of device drivers, which take the pain out of interfacing to peripheral hardware.

2.2 Libraries

On top of Linux kernel there is a set of libraries including open-source Web browser engine WebKit, well known library libc, SQLite database which is a useful repository for storage and sharing of application data, libraries to play and record audio and video, SSL libraries responsible for Internet security etc.

• Mr Gaurav D. Chimote is currently pursuing masters degree at PRMIT&R Badnera, Amravati.
• Prof N.M.Tarbani is assistant professor at PRMIT&R Badnera, Amravati.

2.3 Android Runtime

This is the third section of the architecture and available on the second layer from the bottom. This section provides a key component called **Dalvik Virtual Machine** which is a kind of Java Virtual Machine specially designed and optimized for Android. The Dalvik VM makes use of Linux core features like memory management and multi-threading, which is intrinsic in the Java language. The Dalvik VM enables every Android application to run in its own process, with its own instance of the Dalvik virtual machine. The Android runtime also provides a set of core libraries which enable Android application developers to write Android applications using standard Java programming language.

2.4 Application Framework

The Application Framework layer provides many higher-level services to applications in the form of Java classes. Application developers are allowed to make use of these services in their applications.

2.5 Applications

You will find all the Android application at the top layer. You will write your application to be installed on this layer only. Examples of such applications are Contacts Books, Browser, and Games etc

3 RELATED WORK

In this section we will study the existing screen locks. Firstly to access the screen lock, user has to go to setting option and then select Lock screen. Then the user can select from various lock screen options.

3.1 Slide lock

Slide lock is default lock screen that comes in every smartphone [1]. This is the simplest lock screen as the user has to either slide horizontally or vertically down the screen. This method is not secure at all because unauthorized user can simply slide to unlock and access the smartphone without the owner of the phone knowing about it.

3.2 Face lock

In Face unlock, the face of the user is used to unlock the phone. In this type of screen lock the phone must have front camera. Initially the user has to save his face as a password to open the screen lock. After this whenever the user tries to unlock his phone he has to look into the front camera and then if the face matches with stored image the phone unlocks [2].

3.3 PIN Pattern and Password

This method is secure method in screen lock. In this method the user has to set a pattern or numeric pin or alphanumeric password. Then to unlock the screen the user must enter the same pattern or pin or password. If the entered pin or pat-

tern or password matches the stored pin or pattern or password then the screen unlocks.

3.4 Biometrics Scanning

In Biometric scanning the user has to place his any of his finger on the fingerprint scanner and if it matches with already finger print then the phone is unlock. This method can be said as most secure screen lock method but this technology is provided only in high end phones which are costly.

4 PROPOSED WORK

The proposed method is based on the existing pin screen lock method. Although it is secured than other lock screen methods, it has a problem that every time the user has to set the screen lock manually. In addition to this, if while unlocking the phone somebody gets a look at the pin/pattern and gets hold of phone then he may perform malicious activities. In order to overcome this shortcoming, our proposed method changes pin/pattern every minute, or hour or day as per user's choice. In this way every time the user unlocks phone the pin will vary and the user may not worry of praying eyes around him [3].

Now to use the screen lock, firstly user has to install the .apk file of lock screen. After that the user will be asked to provide his details. Then the user will be tempted to provide a default password which will be use in case of emergency. Now the user has to choose a random number. This random number will be added to the current time of the smartphone. The result thus generated will be the new pin of the user. For example: suppose the user chose 20 as a random number and if current time of user's smartphone is 10:20 then the new pin will be the addition of 1020 and 20 i.e. 1040. Now user has to enter 1040 as his pin to unlock his smartphone. This method enables the user to let go off his worry of praying eyes as his pin will change from time to time. Even if some unknown eyes see the pin, they will not be able to unlock phone because they will be unaware of the mechanism of lock screen. In case the user is not able to unlock his phone, this is where the default password will come into play. The user can anytime enter the default password and unlock his phone.

5 CONCLUSION

In this survey paper, we have seen various screens lock methods and the problems associated with it. In numeric pin method while entering the pin if somebody sees the pin then he may access the phone provided if get the chance. Our proposed method overcomes this shortcoming by dynamically changing the pin at regular interval. Nowadays Smartphones plays a vital role in our day to day to life as it contains our personal as well as business information. So they must be protected from unauthorized access by unknown user.

REFERENCES

- [1] Kwang Il Shin, Ji Soo Park, Jae Yong Lee, Jong Hyuk Park "Design and Implementation of Improved Authentication System for Android Smartphone Users", 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, 2012.
- [2] Swapnil Waghmare et al. "Authentication System for Android Smartphones", International Journal of Computer Applications (0975 – 8887) Volume 87 – No.5, February 2014.
- [3] Bilal Shebaro et al. "Context based Access Control System for Mobile Devices", 1545-5971 (c) 2013 IEEE.
- [4] Sohail Khan, Mohammad Nauman, Abu Talib Othman, Shahrulniza Musa "How Secure is your Smartphone: An Analysis of Smartphone Security Mechanisms", IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012.
- [5] Te-en wei, Albert b. Jeng, Hahn-ming lee, Chih-how chen, Chin-wei tien "Android privacy", IEEE International Conference on Machine Learning and Cybernetics (ICMLC), 2012.
- [6] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication", IEEE Transaction On Information Forensics and Security, Vol. 8, No. 1, January 2013.
- [7] Ananda Kanagaraj S, Arjun G, Shahina A "Cheeka : A mobile application for personal safety", 9th IEEE International Conference On Collaborative Computing : Networking, Applications and Worksharing 2013.

IJSER