 ISSN: 2321-8169
965 – 970

A Survey on Lock Screen for User Authentication Method in Android

Yash Thakur
PG Student, Department of Computer Science & Engineering,
Parul Institute of Engineering & Technology, Vadodara.
Email:thakur.yash514@gmail.com

Ravi Raj Chauhan
Associate Professor, Department of Computer Science & Engineering,
Parul Institute of Engineering & Technology, Vadodara.
Email:chauhanraviraj21@gmail.com

Abstract –1973 Motorola makes the first handheld mobile device. A gap was given until current smart phones started coming up in the 90s. Since then, it has been an avalanche of smart phones, with every manufacturer trying to fight for the greater market share. With Android at the helm of all the buzz, nobody gives a thought to the fact that these would resume of one's identity. Take away somebody's smartphone, and you have taken away a greater part of his life. This brings us to the whole security aspect of it. The measures which Smartphone manufacturers have taken to ensure their safety probably in the wrong hands still leaves a lot of questions and calls for analysis.

Keywords: *Security, User Authentication, Android Lock Screen.*

*****

I. INTRODUCTION

Hacking and data theft are the order of the 21st century. With the incoming of social media, online financial transactions,etc., it has become a categorical imperative for some Android framework users to secure their Smartphone. For some people it is just a matter of privacy, adding a thin layer of protection on their information, keeping it from the prying eyes of friends, colleagues and other acquaintances. For others, it is a very serious matter, because traversing from the outside past their screen lock into the privacy of their smartphone is unthinkable. As such there exist many forms of screen lock authentication methods on Android which a user could pick from. There are android applications which perform this security task, but most users settle for the options build into the Android system. We will examine some of these methods of screen lock authentication.

II. BACKGROUND

The Android operating system is based on the Linux kernel. It comprises of a software stack which is made of the following components: and operating system, a run-time environment, middleware, services, and libraries. Each of these elements listed is engineered and developed in such a manner that they give a high-performance output. All the components interact in a closely tied unit to bring out the power of the operating system. The listed components are shown in the diagram below.

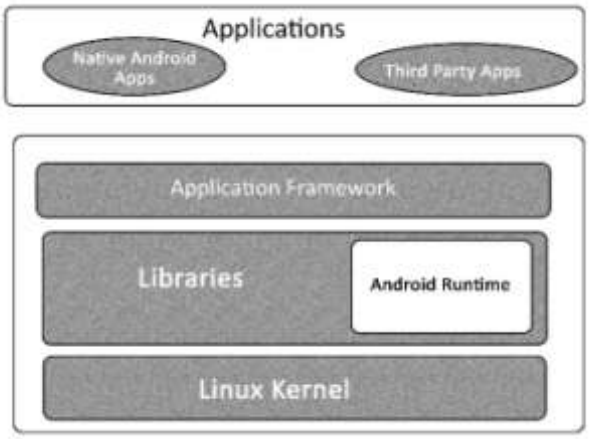

Figure 1.Basic Framework of Android

The Linux kernel:It was developed originally in 1991 by Linux Torvalds and can be found at the bottom of the Android software stack and provides a sort of link between the top stack components and the device hardware. It provides multitasking and system services such as memory, power management and also provides a network layer and device drivers for audio, Wi-Fi and screen display.

Android Runtime - Dalvik Virtual Machine:This is the virtual machine on which Android the Android system runs applications. It enables each Android application to run within its instance, making use of the multitasking capabilities of the Linux kernel. Each application runs directly on the Linux kernel.

Libraries: These are native c and C++ libraries and also Java Framework APIs that are used in the building of Android applications. It also includes core Android system components like ART and HAL

Application Framework: This stack element is made up a group of services which work together to form the platform on which applications run. These stack elements enablereusability in Android components. Individual components can be called and reused for different purposes, keeping its core functions and just using them to build other components possibly.

III. METHODOLOGY

Let's now examine the different screen lock methods provided by the Android system.

1. *Slide Lock*

   The slide lock is a lock screen authentication method where the user slides his finger across the display of his phone depending on where theOS requests that he should do the sliding. The sliding gesture immediately unlocks the phone if done well. This is most often the default method of screen unlocking that Android provides. There are variants of this approach which include sliding to the left, right top or bottom. This is by far the weakest authentication method as anybody who gets the phone will be able to unlock it. It also has major disadvantages in the fact that error can unlock the phone. The user might put his phone in his pants pocket or his jacket, and a mere rubbing of the phone against his skin might unlock the phone [2]

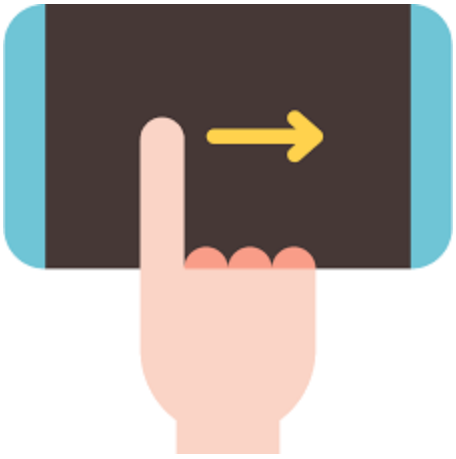

Figure 2.swipe lock

2. *Password Authentication*

   Since the dawn of computer systems, passwords have always been at the centre of authentication and will continue to be popular for a long time. This has been no different in the Androidworld. This method of authentication has been proven to be one of the surest methods, allowing users to put complex characters which hackers might find difficult to break. Password users are always advised to use a variety of characters including uppercase, lowercase alphabets, numbers and other characters. The trick here is to put in a password which is complex enough, but simple doesn't take long to type and is simple to remember. The user has to strike a balance between implementing a harder password and taking a longer time to unlock his phone and just setting a simple password and letting down his security.

   With this method, users can forget their password and would not be able to access their phones. Unfortunately there exist very few methods of recovering your data on your phone if you cannot get past the lock screen.

Figure 3.password authentication

For now, the easiest method would be to factory reset the phone [3].

3. *PIN Authentication*

   This screen lock authentication method is one which many people are fond of. All it requires is a four digit code. After configuration, the Android system prompts you by displaying the numbers 0 – 9. Using this method is a lot easier than using a password because of the minimal amount of data to retain, but a lot easier to crack for hackers. A simple password robot can decipher pin codes in a little while.

Figure 4.PIN authentication

4. *Pattern Authentication*

   Android has used pattern authentication since its early releases. It is an easy way to implement security on Androiddevices. The user has to draw a pattern within a 9 point grid and could go from just drawing two points on the grid to drawing complex patterns. This visual method of authentication is very popular amongst users because it

 ISSN: 2321-8169
965 – 970

is relatively faster than putting in a password and almost as quickly as putting in a pin.

Advantages of this method of authentication include the fact that users as spared the need of using passwords which hackers find easier to bypass than patterns.

There are also disadvantages of the using this method. Forgetting the pattern immediately after creation is easy. Unlike passwords or pins, patterns are not easy to retain immediately after creation and users often find themselves trying to remember their patterns as soon as 5 minutes after creation.

Figure 5.pattern authentication

5. Biometric Authentication

This method of authentication is the best so far; users use a natural identification like a fingerprint, facial recognition or iris scan to gain access to their Android devices. It goes without saying that this total frees the user from having to memorise his authentication (password or pattern). Hackers find it difficult to hack intoAndroid devices with biometric authentication, but real and determined hackers can still break through biometric authentication.

i. Fingerprint

Fingerprint reader technologies have now flooded the Android market. Every manufacturer is racing to incorporate this piece of technology on their Android devices. It safe to say that with time this technology has become very efficient. When it was just introduced not up to 3 years ago, it was quite slow and sometimes would fail to recognise the user's fingerprint. Users are more prone to this method of screen lock authentication. It is fast and practically easy to use.

Anybody intending to get into their device will just need to use their fingerprint at that time.

Fingerprint readers can be now found ontheback of Android devices, on the screen itself, on the home button and at the side of devices.

Figure 6.fingerprint authentication

I. Facial recognition

Facial recognition is also one of those relatively new user authentication methods introduced to the Android framework. The face of a human being has distinct features, ridges and furrows. The software uses these functions to store the unique characteristics of a user in a database, at the time, using a unique code. This is done during the process of enrollment.

This method was also not very efficient though and up till now, and though it is not still that popular, it remains a practical method for authentication. Users have been known to complain that during certain conditions they are not recognised by the phone software. For example, in dimly lit conditions the software would find it difficult to recognise the user. The user might have glasses on, or he might have drastically changed his hairstyle, and the software would also have difficulties recognising him.

Authentication also requires the user to put his phone up in front of his face for the software to do the calculations and matching of the features on his face. Users find this process very slow and inconvenient.

Figure 7.face reorganization

 ISSN: 2321-8169
965 – 970

II. Iris Scan

This is a process whereby thelight beam is projected into a user's eye so that the features of the iris are captured. The light beam enables the visibility of particular patterns of the iris so that camera can capture it. During enrollment, the model of the iris is captured and stored on the Android device. During authentication, the user has to hold up his device to his eyes. The scanner verifies the iris and matches it with that which is in the database.

Figure 8. Iris scanner

This form of authentication is very effective, but many users would probably choose not to use this method because of the length of the authentication process. One has to take out his phone, power it on, then bring it up to his eyes and wait for the verification. Most users do not have the patience to go through that process, so we can imagine this method would be unpopular [4].

6. *Android Smart Lock*

We cannot round this survey up without talking about the new AndroidSmart lock authentication method was introduced in Android 7 and is gradually gaining some popularity especially geeks who just love to make the most of their new Android features. This method involves connecting your device to a trusted Bluetooth device, or NFC tag or any other Android device. Lock screen authentication is immediately disabled each time the trusted device is onyourAndroid device.

Wi-Fi can even be used to unlock the screen of your phone through thesmart lock. Options are given to go further to unlock thephone via GPS. A user could configure his phone to unlock when he is in a particular location or to lock if he is in another place. This method of authentication might interest those who are not too concerned about security. With authentication methods like this, anyone can always get into the user's phone once he is within the required unlock range.

Using native smart unlock users can also configure their Android devices to unlock at certain times and automatically lock on other occasions[5].

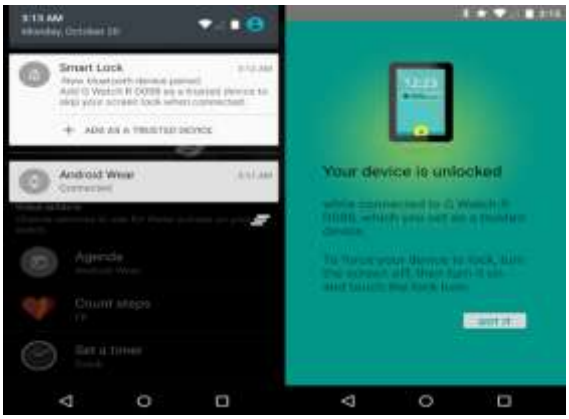

Figure 9. Smart Lock

7. *Puzzle Unlock*

Now, taking a look at other Android lock screen authentication methods which do not come with the Android OS, we can think have puzzle unlock. This means of unlocking is similar to that of pattern unlock; the simple difference is that images replace the grid, which needs to be assembled in a particular order. When arranged in the right order, the screen unlocks. This is method is not an easy method as the proper order of the puzzle should be memorised otherwise the phone will not unlock.

8. *Gesture Unlock (waving)*

Some manufacturers incorporate this into the Android OS making use of the proximity sensors of the phone to provide and authentication method where users can make gestures above the screen of the phone to unlock it. [6]. Gesture authentications, in general, mean any authentication which involves moving the hand or finger in a particular direction. To be precise in this case we are talking about gestures without touching the screen of the phone. For example a simple wave of the hand to unlock the screen of the phone. [7]

This method falls amongst those that work in some cases and does not in others. So we might have a situation here where the user tries it a few times before it works. This usually comes with options on third-partyAndroid launchers which make us of the proximity sensor.

9. *Shake Unlock*

This authentication method allows the user to shake the phone to unlock it. This methoduses the accelerometer sensor of the phone to detectmovements of a certain velocity.Identified as one of the options also provided by third party launchers on Android, this method, is not quite common.

This method is also almost always set up with the other methods of authentication because failure to unlock the screen through shaking would result in factory resetting the phone.

10. *Circular Lock Screen*

This screen lock comprises of six circles. Each circle changes its colour maximum of seven times by retouching the circle. There is no particular order for touching the circles. Once retouching is done a password string is then confirmed by tapping on the Ok button. If the string is matched, then the telephone is unlocked [8].

11. *Tiny Pad Lock*

This screen unlocks method is similar to the pattern lock method. Infact, this approach is an upgrade of the pattern method. The idea originates from the fact that with the pattern method, the user left traces of the screen lock pattern with his finger, which any intruder can easily use to access the phone. \During the process of drawing the pattern, tactile feedback is felt by the user each time he draws on a dot, guiding him through the drawing process. When he is through, a circle appears in the place of the tinypad, and he either draws anti-clockwise or clockwise in the circle to wipe the finger traces. That is when the phone unlocks if the pattern he drew was right. This solves the problem an intruder guessing the pattern from finger tracing smudge marks.[9]

12. *Pingenie Screen Lock*

This is a screen lock which is sold by a third party vendor. The numbers which pop up always shuffle so that they are never in the same position. This makes it hard for somebody who is trying to have access to the phone to get past the screen lock. This method is very straightforward and secure. But this method only provides number password to be set.

Lock screen Type	Shoulder Surf Protection	Complexity	User Friendly	Hardware Dependent	Secure	Speed of Authentication	Duration of Configuration	Need to Memorise authentication
Slide Unlock	No	Low	YES	No	NO	Fast	Short	No
Password	No	Medium	YES	No	Yes	Medium	Medium	Yes
PIN	No	Low	YES	No	Yes	Medium	Medium	Yes
Pattern	No	Low	YES	No	Yes	Medium	Medium	Yes
Fingerprint	Yes	High	YES	Yes	Yes	Fast	Long	No
Facial Recognition	Yes	High	NO	Yes	Yes	Slow	Long	No
Iris Scan	Yes	High	NO	Yes	Yes	Slow	Long	No
Smart Lock	No	High	NO	No	No	Fast	Long	No
Shake Unlock	No	Low	YES	YES	NO	Medium	Short	No
Puzzle Unlock	No	High	NO	NO	Yes	Medium	Long	Yes
Gesture Unlock	NO	Low	YES	YES	NO	Medium	Long	Yes
Circular Lock	YES	High	YES	NO	YES	Medium	Long	No
Tinypad Lock	YES	Low	YES	NO	YES	Medium	Medium	Yes
Pingenie	YES	Medium	YES	NO	YES	Medium	Medium	Yes

IV. CONCLUSION

These screen lock authentication methods come with advantages and disadvantages. There are other upcoming methods of authentication which are only concepts like DNA authentication on Android systems. So far not much has been done in that light.

So far the biometric authentication is the most popular and most sought after though the technology can only be found in mostly premium Android devices and a few midrange devices.This is true for fingerprint readers who have proven to be the best in most categories when compared

with the other lock screen authentication methods. In the nearest future, it is believed that biometric systems will become very much advanced and more widely used both in the Android framework and in other systems.

REFERENCE

[1] Android Security Overview, Android open source project, http://source.android.com/tech/security/index.html
[2] Androidcentral.com
[3] Andriotis, P., Oikonomou, G., Mylonas, A. and Tryfonas, T. (2016) A study on usability and security features of the Android pattern lock screen. Information and Computer Security, 24 . pp. 53-72. ISSN 2056-4961 Available from http://eprints.uwe.ac.uk/29738
[4] http://www.pocket-lint.com
[5] JR Raphael: android intelligence analysis- computer world
[6] Schlöglhofer, R. and Sametinger, J. 2012. Secure and Usable Authentication on mobile devices. In Proceedings of the 10th
[7] International Conference on Advances in Mobile Computing & Multimedia (Dec. 2012). ACM New York, NY, 257-262.DOI= http://doi.acm.org/10.1145/2428955.2429004.
[8] https://www.xda-developers.com/unlock-yr-device-using-a-hover-gesture-with-magic-unlock/
[9] Kwang Il Shin, JiSoo Park, Jae Yong Lee, Jong Hyuk Park "Design and Implementation of Improved Authentication System for Android Smartphones Users",26th IEEE International Conference on Advanced Information Networking and Applications Workshops, 2012
[10] Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM. Smudge attacks on smartphone touch screens. In: Proc. 4th USENIX conference on offensive technologies (WOOT'10) 2010. pp. 1e7.Bicakci K, Atalay N