# Analysis and Bypassing of Pattern Lock in Android Smartphone

V. Venkateswara Rao
Computer Science and Engineering
JNTUK, Kakinada
vvrao@cert-in.org.in

A. S. N. Chakravarthy
Computer Science & Engineering
JNTU Kakinada
asnchakravarthy@yahoo.com

***Abstract*—Android enabled mobiles/devices are high in use by huge number of users for various purposes. Other than for just calling, most of the users are using these devices for storing and maintaining important data such as personal information, calendar schedules, photos, videos, office documents and much more. These devices are also used for chatting through various instant chat messaging and social networking applications, emailing and internet browsing. In the investigation of many of the cyber crime cases, digital devices enabled with an android operating system are found as prime evidence at the crime scenes. With these devices an investigator can get the handful of information to track the call records, chat messages and activities on the device links to crime happened. This evidence is very useful in tracking down the culprit or criminals involved in the cyber crimes. In order to analyze the found devices, the devices lock must be bypassed to access the available sources of evidence in the digital form. This paper discusses the rooting of the android devices and methods to bypass the pattern lock.**

***Keywords— Android forensics; investigation; SHA-1; pattern lock; cryptography; rooting***

## I. INTRODUCTION

Android is the fast growing and mostly used operating system in smart phones, tablets and other electronic devices in this current era. The Smartphone bearing a lot of personal data in the form of SMS, call log, photos, videos and other personal information. Android provides six different options to provide security for accessing all these resources. Pattern lock is one of them and has a higher level of security among all the available mobile screen lock options. This will restrict unauthorized users from accessing our mobile devices and personal information.

The forensic analyst may find a Smartphone at the crime scene, where the phone is secured with a screen lock. In this scenario, the security of the device should be bypassed in order to analyze the evidence. This paper illustrates how to bypass the pattern lock security within the android mobile. In android devices, screen lock settings are enabled at the location *settings → security*. In this, select the "Screen lock" then enter the pattern input to be used for screen lock. The given input is recorded as the secret phrase for opening the screen lock.

## II. PATTERN LOCKING MECHANISM IN ANDROID

The *screen / pattern* lock is enabled in *settings → security* option as shown in "Fig 1". In an Android operating system different ways of security mechanisms available to secure the device from unauthorized access. Screen lock is one of the mostly used security mechanism in which a pattern is used to form a secret phrase with numbers arranged in a 3x3-matrix format. The matrix is formed with numbers starting from 0 to 8 and these numbers are joined together to get some secret phrase to unlock the device in the next subsequent accesses by authorized users when the device is locked. The matrix representation of the numbers is shown in “Fig 2(a)” and “Fig 2(b)”. According to these figures, the pattern which used is 6 – 3 – 0 – 1 – 2 – 5 – 8 – 7.

The combination of digits is not directly stored in plain text format in the device database. The secret phrase formed by combining a pattern of digits is stored as SHA-1 hash value without any salt in the devices system database file *gesture.key* located in the */data /system* directory shown in "Fig 3". SHA-1 is a one-way cryptographic hash function, where we cannot get the plain text from the hashed one. This SHA-1 value does not use any salt to generate a hash. The SHA-1 hash value is equivalent to 1cb3629a723f5d287e990a2ac4becc48568777fc and is stored in the *gesture.key* file.

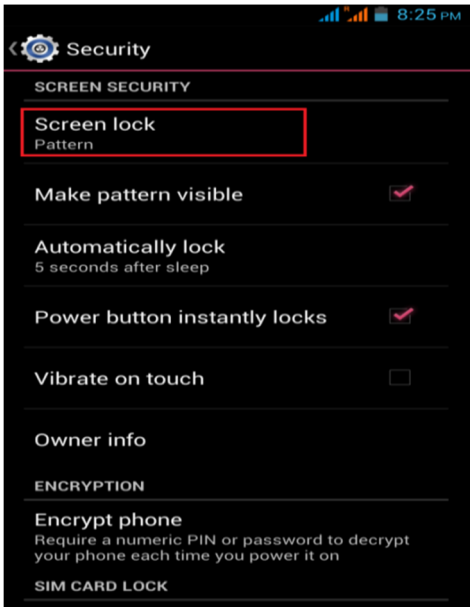
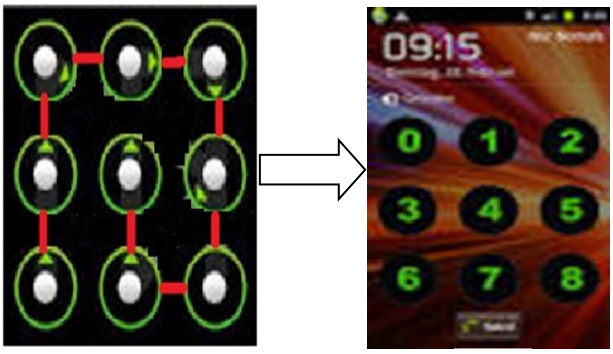



Fig 1: Screen Lock Settings

978-1-5090-0612-0/16/$31.00 ©2016 IEEE




(a) (b)

Fig 2: a) Pattern Lock , b) Number Assignment for Pattern Design

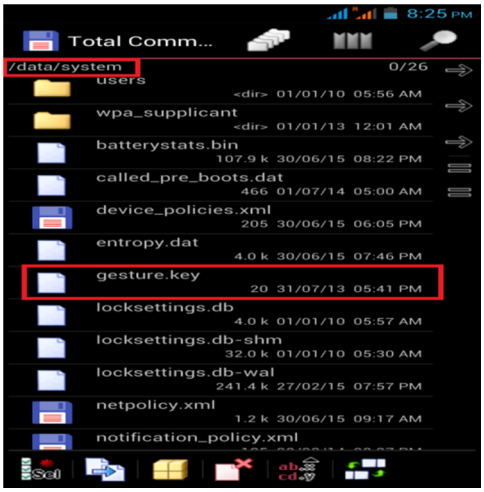



Fig 3: Screen shot showing the location of gesture.key file

## III. Rooting of Android Device

In android device the system files and */data* folder are not accessible to normal users. To access these files and folders user requires super or root user privileges. To gain root user privileges the device should be rooted. Rooting is a *jail breaking* process in android devices for gaining super user privileges and to get permission to access the root directory and other system directories and allow the user to customize functions and loading additional modules in the device [2].

For performing rooting of an android device, USB debugging mode must be enabled on the android device. The initial and basic setting for USB debugging mode is "disabled". It can be enabled from device settings by proceeding to "Developer Options" and enabling the USB debugging checkbox as shown in "Fig 4". Now connect the device to the computer by using USB/Data cable. Several manual and automatic methods are available for rooting android devices.

In this paper, "*Kingoroot*" is used for the rooting process. Android SDK and Kingoroot software should be installed on the system in order to perform the analysis process [3]. Kingoroot is a universal android rooting application, which supports almost any android device and versions from 1.5 to latest 5.0. This rooting application is very handy, it does not interact with any other mobile applications and there is no data loss during the rooting process.

Switch on the android device after connecting it to the computer. Now run the Kingoroot application on the computer and wait for some time to get the root access. During this process, the mobile device may get restarted several times.

## IV. Finding the Pattern Sequence by Comparison of Hash Values in Rainbow Table

After the successful device rooting the phone will be operated in super user mode and one can access mobile device system files and root directory. Using any of the file explorers (Total commander) copy the *gesture.key* from */ data / system* folder to computer. Using any of the Hex Editor open the *gesture.key* file and detect the contents of the file [4].

The following “Fig.5” shows the hex values stored in the gesture.key file as SHA-1 hash value equivalent to our pattern. For all the combinations of patterns from 0 to 8 numbers rainbowtable database is available with SHA-1 hash value and corresponding number sequence. This database is freely available on the Internet [5].

By using any of SQLite browser (Sqliteman) open the *Gesturerainbowtable.db* and open the *rainbowtable* table and explore the record. The *rainbowtable* contains two columns (hash, pattern). The hash column contains SHA-1 hash value of pattern and pattern shows the number sequence. The database and table details are shown in below "Fig 6".

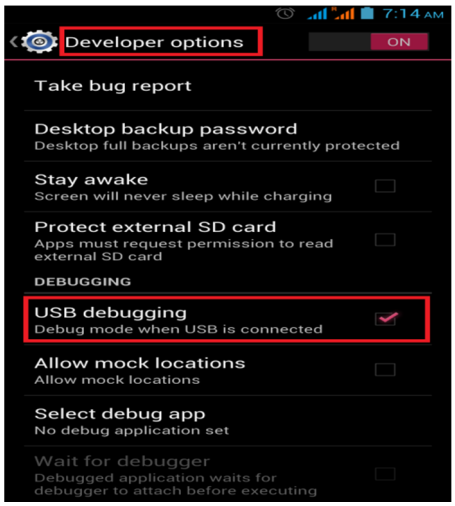



Fig 4: USB debugging mode in developer options

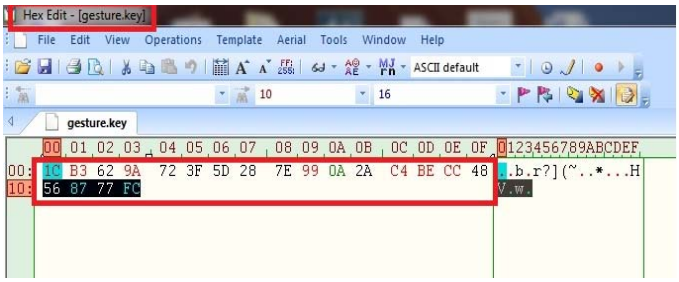



Fig 5: Hex Editor showing contents of the file gesture.key

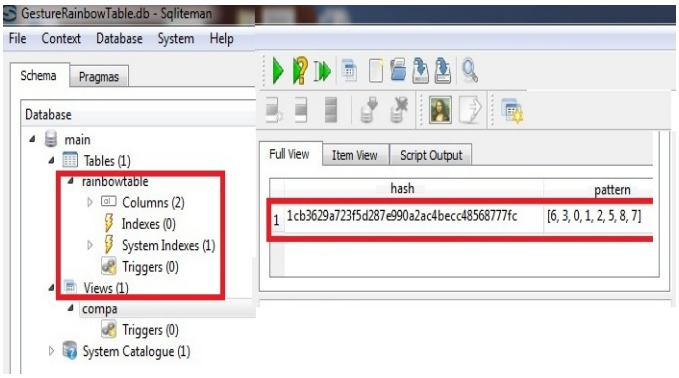



Fig 6: Validation of hash value in rainbow table

In the next step, find the hash sequence found in *gesture.key* file with rainbow table hash values to know the pattern (number sequence) for the matched hash value. Create a view with a hash matching condition to the hash value with the hash column. Create view comparison as,

*select * from rainbowtable where hash = '1cb3629a723f5d287e990a2ac4becc48568777fc';*

When this SQL statement is executed it will return one row containing the matched hash and the corresponding pattern value. The matched pattern value are given in "Fig 6" is {6, 3, 0, 1, 2, 5, 8, 7} which is same as the pattern lock sequence used by the user. Thus this process will be easy for the forensics analyst to investigate and analyze the unknown secure patterns of the android devices.

## V. DISCUSSION

This paper deals with the innovative forensics technique for providing a solution to the evidence detectors in crime scenes and investigations. This process makes simple to unlock the pattern of a mobile without the prior knowledge of the security locks to track the call records, chat messages and activities on the device links. In some cases, mobile phones may be the main evidence in trace out the crime evidence. In this paper, the procedure discusses how to root the android devices and methods to bypass the pattern locks. Rooting process will be done by Kingoroot application and make it run on the computer to get the root access after a short time. The pattern sequence will be found in an exceptional way by comparing with hash values in the rainbow table. Finally, a hash sequence will be found with the help of *gesture.key* to retrieve the pattern. Thus by this simple practice tracking down the culprit or criminals involved in the cybercrime is effortless.

## VI. CONCLUSION

This mechanism to investigate the critical cases for the evidences from the android mobile devices will be easy by breaking any critical security lock patterns. In this article, authors discussed how to bypass the pattern lock mechanism in android devices. This will help the forensic investigators to access and explore the mobile devices, which are under forensic investigation. Analysis and cracking of pattern lock in android Smartphone will be easy with this methodology. Bypassing mobile application specific locks (Applock) will be considered for future work.

## REFERENCES

[1] P. Dibb and M. Hammoudeh, "Forensic Data Recovery from Android OS Devices: An Open Source Toolkit", *2013 European Intelligence and Security Informatics Conference*, 2013.

[2] Jeff Lessard and Gary Kessler, "Android Forensics: Simpliying Cell Phone Examinations", *Small Scale Digital Device Forensics Journal*, vol. 4, no.1, pp1941-6164, 2010.

[3] K. Barmpatsalou, D. Damopoulos, G. Kambourakis and V. Katos, "A critical review of 7 years of Mobile Device Forensics", *Digital Investigation*, vol. 10, no. 4, pp. 323-349, 2013.

[4] S. Goetsch, "The Mobile Security Company | NowSecure", *NowSecure*, 2016. [Online]. Available: https://www.nowsecure.com/#viaforensics. [Accessed: 06- Jul- 2016].

[5] "UK's Leading Digital Investigation & Consultancy Company", *CCL Group Ltd*, 2016. [Online]. Available: http://www.cclgroupltd.com/. [Accessed: 16- Jul- 2016].