

SCREENLOCK CRACKER: ETHICAL HACKING TOOL FOR ANDROID DEVICES

Shilpa R B¹, Dhanalakshmi M P²

¹Student, Dept. of Computer Science, ER & DCI institute of Technology, Trivandrum, Kerala, India

²Assistant Professor, ER & DCI Institute of Technology, Trivandrum, Kerala, India

Abstract – Screenlock Cracking is mainly referring to cracking or discovering screen lock present in android touch devices. Here which is developed as a tool. This tool recovering password from data stored in device, transport it into the tool. Screenlock Cracking is done by continues guessing, or through an algorithm or based on certain dictionaries. The tool tries numerous combinations until successful discovering of password. In sometimes this kind of cracking tools are misused by hackers for gaining unauthorized access to a device without owner's awareness. This kind of gaining result to cybercrimes included stealing personal information, banking details, personals pictures etc. Uses of such kind of devices are, forgotten a password or someone has misplaced. Some other activities such as owner or administrators conduct testes for checking password strength in the point of information security. So, hackers cannot easily crack the password protection of android touch devices. This can be implemented by root access and usb debugging mode enabled. Need to extract gesture and key for pattern and password, key and salt number for pin or password on the device. This tool supports cracking Screenlock such as password, pin and patterns.

Key Words: Android, Pin, Pattern, Password, Screenlock, Cracker

1. INTRODUCTION

The android touch screen devices are secured by using screenlock like security feature. This Kind of features are implemented in device like mobile device to prevent unauthorized access into the others personal devices. Screenlock is also known as lock screen. This security features required specific sequence of actions or specific action to perform action on the android device. Nowadays Screen locks contain password or passphrase which manually entered by users, specific actions for gesture or motion on the touchscreen of the device, biometric readers such as users' fingerprint, scanning of their eyes or similar analysis for user's recognitions [1].

Android screen locks are different kind, but here mainly focusing on pin, pattern and password only. Pin is a screenlock which was found on basic devices even in keypad devices. After introduction of touch screen mobile devices first implemented screenlock was pin. After development of touchscreen devices, they introduced password like screen locks, which was based on the security improvement. This password screen locks are the combinations of letters, numeric, and special characters. So, guessing of this is very difficult. New improvement of screen lock after password was patterns. The patterns are the lines go through the points shown on the screen. The points are the form of matrix 3X3. In which can draw the patters only combinations available in 3X3 matrix of points. The main difference between pattern and password is that combinations, which can guess in patterns but difficult in passwords. After this pattern biometric readers are introduced [2].

In first android did not use lock screens or any locks, it contain only menu button to open the home page of the android device. Gesture based lock screen was introduced on android 2.0, which was based on two button one for unlocking the phone and another one for volume button. The rotary dial was introduced on android 2.1 instead of two tabs. On android 3.0 introduced ball with a padlock icon for dragged to the outside of an area. Android 4.0 to unlock straight to the camera and on android 4.1 unlocks into google search by dragging up [3].

Android 4.2 had swiping from the left edge of the screen and also can add widgets to pages on the lock screen. Android also support devices to be locked using passcode, passwords, patterns, fingerprint sensing or facial recognition [4].

2. EXISTING SYSTEM

Among all existing system, screenlock cracking done through different attacks such as malware, offline cracking, shoulder surfing, video recording attacks etc.

These attacks have some limitations i.e. this are attacks and crack only if after done by authorized user[5].

2.1 Video Recording Attack

In video recording attack, attack done by help of video camera on mobile phones. The recorded video on the device was analyses, which contain video of users who enter passwords [6].

2.2 Guessing

Based on prediction of user password. It is very risky one, because cracking is implemented through guessing. It requires more time and more chances for finding correct password. In some of the devices have only limited attempts to unlock the device [7].

2.3 Brute Force Attack

In brute force attack, non-dictionary words are use for finding passwords. Which is the combination of alpha-numeric from aaa1 to zzz10. It also took time to find successful password [8].

3. PROPOSED SYSTEM

The proposed system uses to crack screen locks in android devices. Screenlock cracking is implemented by using rainbow table, brute force and wordlist for comparing hash value of present screenlock and hashes stored in database. The rooted android devices are used for screenlock cracking. This screenlock cracker is mainly focused on cracking patterns, pins, and passwords.

3.1 Modular Description

The proposed cracking tool for cracking the screen locks of rooted android phone would mainly work on three modules.



Fig -1: Block Diagram of Proposed System

3.1.1 Rooting

Rooting is the process of gaining access of user's smartphones, tablets and other android devices, which

contain android operating system and it has kernel layer. If its rooted device then we can enter into the kernel layer and can dump sensitive data from phone. The advantage of rooting is that complete control of the device can gain and can use the device freely. Rooting is possible only in android devices and in some device which is difficult. Higher versions of android are also difficult to rooting. Such devices are rooted through flashing.

Input: An android phone connected via USB and enable USB debugging mode, KingoRoot.

Output: Rooted phone.

3.1.2 Dumping

Dumping means pulling required files and database from android phone to pc with the help of adb tool.

Input: ADB tool, rooted android phone.

Output: Files and database from phone.

3.1.3 Rooting

Cracking is the process of recovering passwords from data that have been stored in or transmitted to a computer system. Here attack, rainbow table and wordlists are used to crack password and also use available cryptographic hash of the password.

Input: Dumped files and database, Hash of the password.

Output: Password

4. SYSTEM DESIGN

The flow chart diagram is shows that overall design of the tool. First of all, choose an android phone whose USB debugging mode must be enable. After that it check the device is rooted or not. If it is not rooted then with the help of KingoRoot start to root. After complete rooting, adb tool is use to dump the files and database which required for cracking the screenlocks. The required files age password.key and gesture.key. The required database is locksettings.db. One more file is required which is device_policies.xml which is used to find the length of pin and password and also used to distinguish pin and password. Locksettings.db file is used to extract salt value from the database. Directly we cannot see the salt value for that sqlite3 is used to extract salt value. Gesture.key contain values which is not manually readable form. So gesture.key file open hex for seeing the hex value. This hex value is to crack

the password. Password.key contain 72 bits length long string. In which first 40 bits represents SHA1 and remaining 32 bits represents MD5. In cracker can choose any algorithms for cracking password. Different techniques are also use to crack password such as rainbow table, wordlist use for dictionary attack, and also brute force.

Step 5: Successfully root the device.

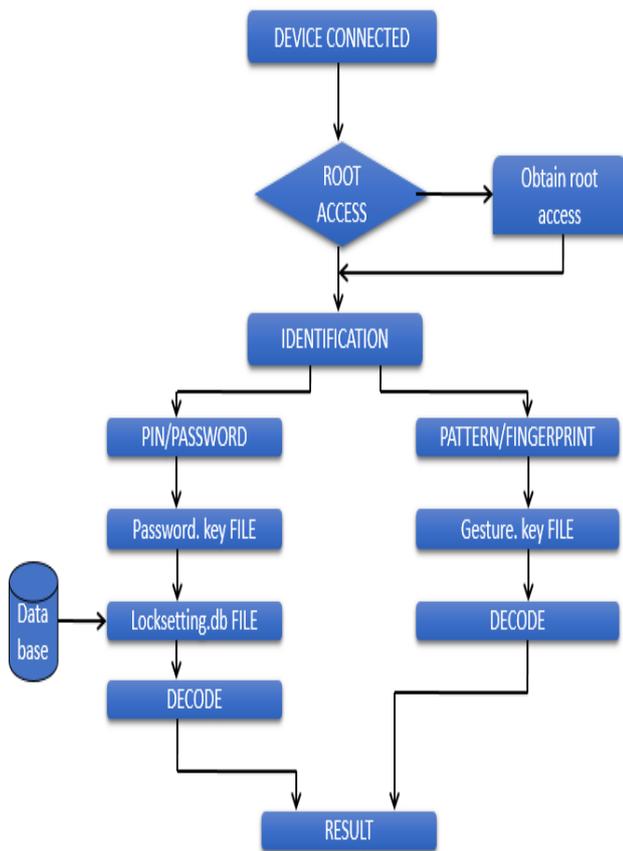


Fig -2: Flow of the System

5. IMPLEMENTATION

Rooting is the process to attain privileged control of android mobile operating system over various android subsystems. Android is a Linux kernel based, rooting in android devices is gaining super user permission on mobile device. Rooting is performed to overcoming limitations that present in hardware manufactures put on the devices. Thus, rooting helps to alter or replace such settings present in the kernel of the device.

- Step 1: Download and install KingoRoot
- Step 2: Plug in android device into the computer using USB cable. Rooting device will detect automatically and make sure about internet connection.
- Step 3: Enable USB debugging mode.
- Step 4: To begin process. Click "ROOT".



Fig -3: KingoRoot Display

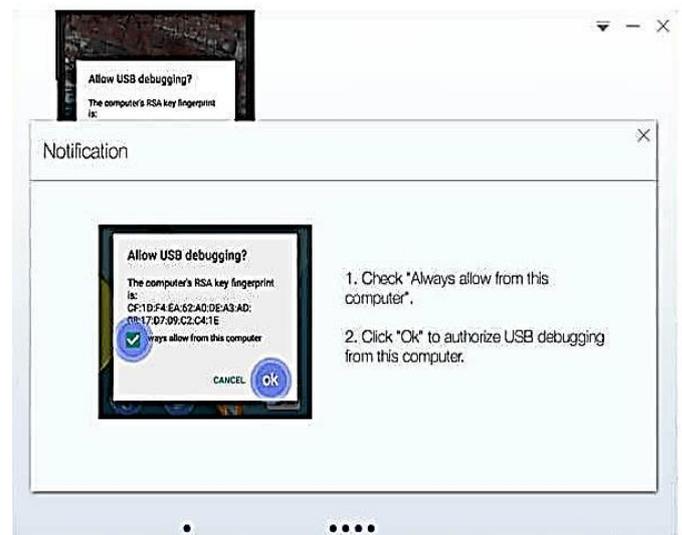


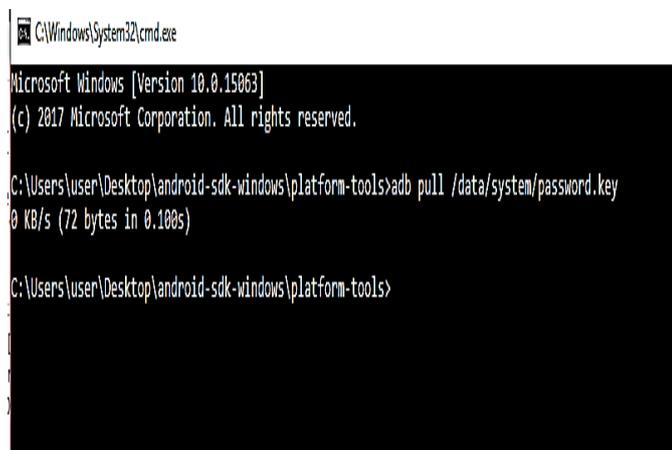
Fig -4: USB Debugging



Fig -5: Root Succeed

Android debug bridge (adb) is a command-line tool. Which use to communicate with devices. The adb commands use to perform various action on device such as installing, debugging etc. It also accesses UNIX/WINDOWS shell to run various commands on device. Here adb is use to dump files from android device to the computer for cracking password.

Password.key file want to be dump form rooted android device. So, we use adb shell to pull the file from device to system. The command for that is adb pull /data/system/password.key

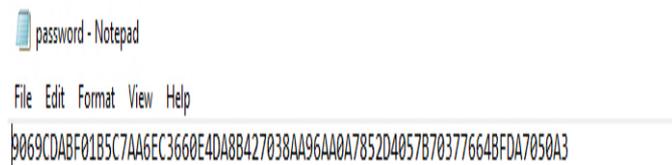


```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user\Desktop\android-sdk-windows\platform-tools>adb pull /data/system/password.key
0 KB/s (72 bytes in 0.108s)

C:\Users\user\Desktop\android-sdk-windows\platform-tools>
```

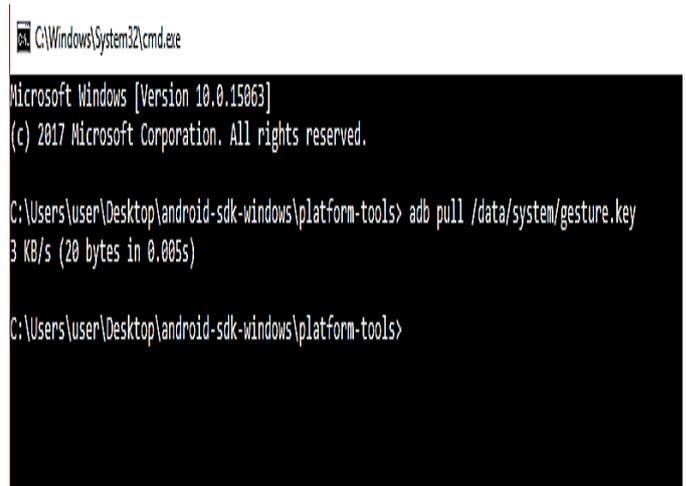
Fig -6: Password. key Dumping



```
password - Notepad
File Edit Format View Help
0069CDABF01B5C7AA6EC3660E4DA8B427038AA96AA0A7852D4057B70377664BFDA7050A3
```

Fig -7: Password.key File

Gesture.key file want to dump form rooted android device. So, we use adb shell to pull the file from device to system. The command for that is adb pull /data/system/gesture.key.

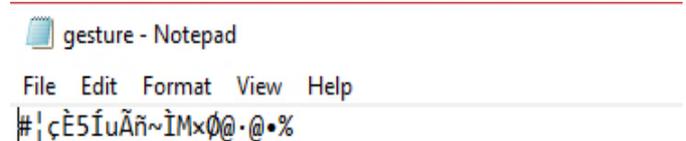


```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user\Desktop\android-sdk-windows\platform-tools>adb pull /data/system/gesture.key
3 KB/s (20 bytes in 0.005s)

C:\Users\user\Desktop\android-sdk-windows\platform-tools>
```

Fig -8: Gesture.key Dumping



```
gesture - Notepad
File Edit Format View Help
#;!çÈ5ÍuÃñ~Ìm×0@.@•%
```

Fig -9 Gesture.key File

Device policies file want to be dump form rooted android device. So we use adb shell to pull the file from device to system. The command for that is adb pull /data/system/device_policies.xml



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user\Desktop\android-sdk-windows\platform-tools>adb pull /data/system/device_policies.xml
1 KB/s (205 bytes in 0.111s)

C:\Users\user\Desktop\android-sdk-windows\platform-tools>
```

Fig -10 Device policies dumping

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<policies>
  <active-password nonletter="0" symbols="0" numeric="0" letters="0" lowercase="0" uppercase="0"
    length="9" quality="65536"/>
</policies>
```

Fig -11 Device policies File

Lock setting want to be dump form rooted android device. So we use adb shell to pull the file from device to system. The command for that is adb pull /data/system/locksettings.db

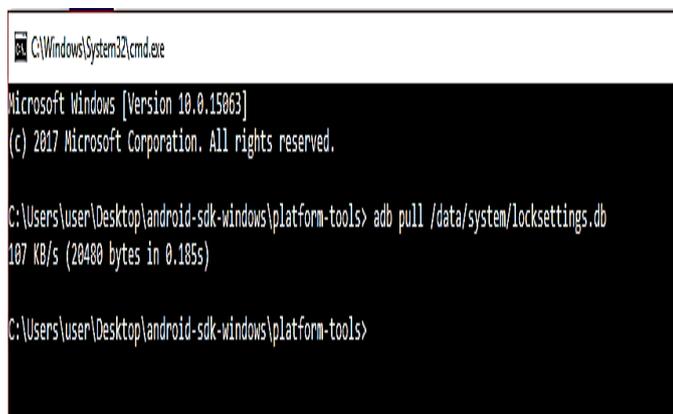


Fig -12 locksettings.db file Dumping

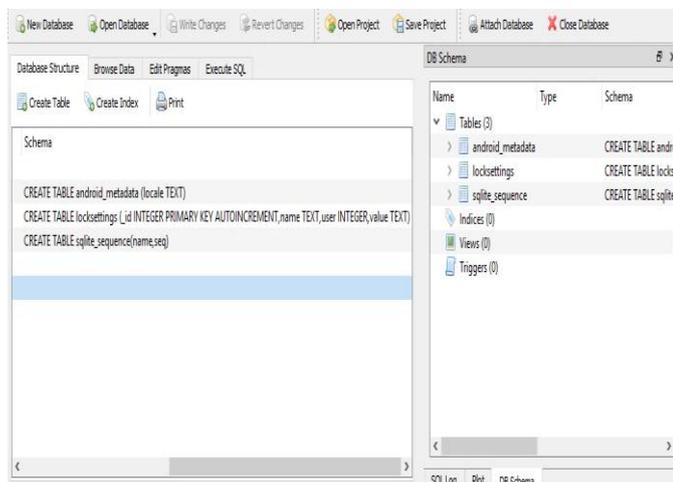


Fig -13 locksettings.db

5.1 Pattern Cracking

Pattern cracking is done by using gesture Rainbow Table.db database. Which is created with the help of rainbow generator. Gesture Rainbow Table.db database is read with the help of sqlite3. Gesture Rainbow Table.db contain hash values of all combinations of patterns and its pattern value. Hashes

of each pattern combination is set as primary key in database.

```
SELECT pattern FROM RainbowTable WHERE hash="C8C0B24A15DC8BBFD411427973574695230458F0"
```

SELECT pattern FROM RainbowTable



Fig -14 Cracker Tool Window

Pattern cracker window of cracking tool.

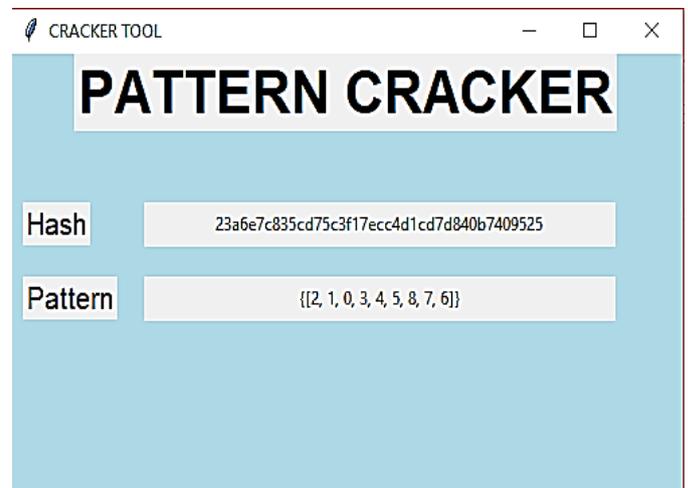


Fig -15 Pattern Cracker Window

5.2 Pin and Password Cracking

Pin and Password are cracked with the help of password.key file which dumped from android rooted phone. In addition to password.key device policies.xml file and locksettings.db files are also necessary. Password.key file fetch by using android debugging tool from location *data/system/password.key*. This file contain string is 72 characters long, which is a

strange number and not valid for most hash functions. It's actually two hashes, one SHA1 and one MD5 concatenated together.

```
1136656D5C6718C1DEF718431B2CB5652A8AD550E20BDCF52B00002C8DF35C963B71298
```

So this splits the above hash into:

SHA1:

```
1136656D5C6718C1DEF718431B2CB5652A8AD55
```

MD5:

```
0E20BDCF52B00002C8DF35C963B71298
```

Salt value is from:

Android Version	Location /strong>
Cupcake, Donut, Eclair, Froyo, Gingerbread, Ice Cream Sandwich	/data/data/com.android.providers.settings/databases/settings.db
Jelly Bean, Kit Kat, Lollipop	/data/system/locksettings.db

Table -1: Locations of salt value in rooted android phone

Database downloaded from locations now which can be viewed with help of sqlite3.

```
SELECT value FROM locksettings WHERE name = 'lockscreen.password_salt'
```

The salt value is 64bit long integer:

```
2146936913259450773
```

To use this, we need to convert it to hex and then lower case it.

```
1dcb73bf6600d195
```

Pin cracker window of cracking tool.



Fig -16 Pin Cracker Window

Password cracking window of cracker tool

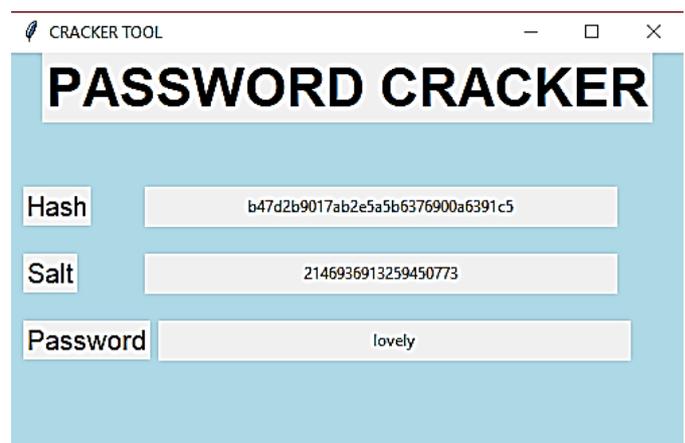


Fig -17 Password Cracker Window

6. CONCLUSIONS

This project mainly cracks pin, password and pattern. Limited tools are available for cracking screenlocks. While comparing to other available tools it is freely available. This tool can be run in versions of windows from 7 to higher versions. Cracking time of pin and password is similar to other tools. But in the case of pattern which can easily cracked because it is implemented with the help of rainbow table. This tool is applicable for rooted android devices. ADB tool is used to pull required files such as database file, file which contain hash values of screenlocks and device police files. Database file contain salt value which used for hashing the screenlock. Hash value stored files are contained hashes which are used to crack the

screenlocks. Device police file contain length and number of letters. Length is used for cracking pin and letters are used for password to. Sqlite3 is a database which used for collecting data from databases which created for cracking and dumped from android device. This tool is easy to handle because for cracking screenlock of rooted android device, just that device connected to the toll installed device. The tool automatically detects the device and dump required files according to the screenlock and crack it.

REFERENCES

- [1] Y.Guixin, T.Zhanyong, F. Dingyi, C.Xiaojiang, K.Kwang In, .B Taylorx, and Zheng Wang "Cracking Android Pattern Lock in Five Attempts," in School of Information Science and Technology, Northwest University, China, School of Computing and Communications, Lancaster University, UK, 2017.
- [2] C.Geumhwan, Jun Ho Huh, C.Junsung, O. Seongyeol, S. Youngbae and K.Hyoungshick, "SysPal: System-guided Pattern Locks for Android", in Department of Computer Science and Engineering, South Korea, South Korea, 2016.
- [3] Bh. Padma1 and GVS Raj Kumar, "A review on android authentication system vulnerabilities," in International journal of modern trends in engineering and research, 2016.
- [4] B.Remy de and K. Javy de "Offensive Technologies: Attacking Android's pattern PIN lock," in University of Amsterdam System & Network Engineering, 2013.
- [5] Jaewoo Pi and Pradipta De, "Using GPUs to Crack Android Pattern-based Passwords", in MSIP (Ministry of Science, ICT and Future Planning), Korea, under the "IT Consilience Creative Program" (NIPA-2013-H0203-13-1001) supervised by the NIPA (National IT Industry Promotion Agency).
- [6] Ms. Vidya Vijayan, Ms. Josna P Joy, Mrs. Suchithra M S, "A Review on Password Cracking Strategies", in International journal of research in computer and communication technology, 2015.
- [7] <https://android.gadgethacks.com/how-to/7-ways-bypass-androids-secured-lock-screen-0165540/>
- [8] https://www.fireeye.com/blog/threatresearch/2017/10/gocrack-managed_passwordcracking-tool.html
- [9] <https://www.guru99.com/how-to-crack-password-of-an-application.html>
- [10] <https://www.alphr.com/features/371158/top-ten-password-cracking-techniques>.