Research on Attack and Defense of Android Mobile Screen Password

Lei Wang

School of information technology, School of Jianqiao University, Shanghai, China.

03010@gench.edu.cn

Keywords: Graphic cryptography, PIN password, encryption algorithm.

Abstract: This paper mainly introduces the basic principle of screen graphics lock password and PIN password in Android system, and puts forward relevant protective measures, providing users with a better use of security experience.

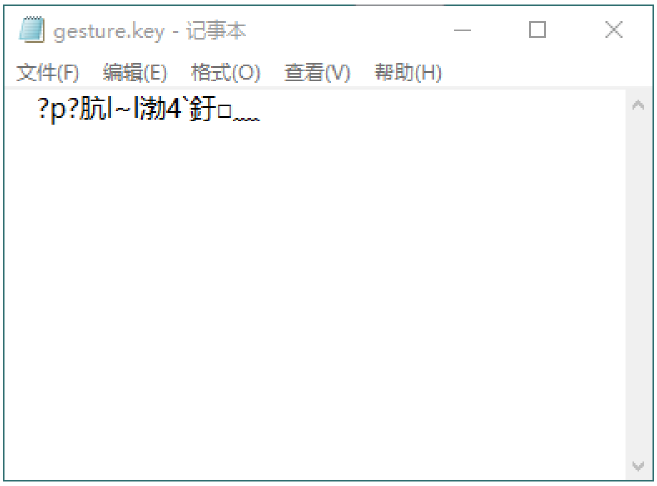
1. Preface

With the popularity of mobile devices, more and more people are accustomed to this kind of mobile network life, using mobile devices to surf the Internet, browse news, chat shopping, network financial management, etc., but the security problems are also particularly prominent, especially personal privacy issues, data security issues, etc. Android system screen is tight. As the first gateway to protect users'privacy, code lock is used by most users. At present, there are two most common ways of lock screen password, one is gesture password, that is, the common Nine-palace map password, the other is input password, which can be divided into PIN password and complex character password, and PIN password is the number. The password is relatively simple. Of course, there are also some more advanced password modes, such as fingerprint passwords and face recognition passwords. This paper mainly introduces the related content of gesture password and PIN password, including encryption principle, cracking methods and reinforcement measures.

2. Introduction to Graphic Lock Password

The graphics password lock in Android system is mainly composed of 9 points similar to the Nine Palaces. When setting the screen password, it is required to connect at least 4 to 9 non-repetitive points. These points and the sequence of connections constitute a path with direction. This path is the graphics lock password. By putting the Nine Palaces pattern into the screen password, it is required to connect at least 4 to 9 non-repetitive points. Transform to byte array, and then use SHA1 encryption algorithm to encrypt, so as to achieve the protection of the password [1]. The system will save the encrypted file to / data / system / gesture. key file. When you open the program with Notepad, you can see some random code, as shown in Fig 1.

SHA1 algorithm is used in graphic lock cipher encryption. This algorithm is briefly introduced below. SHA1 algorithm produces a 160-bit message digest. It is a data encryption algorithm. The idea of this algorithm is to receive a plaintext and convert it into a (usually smaller) ciphertext in an irreversible way. It can also be simply understood as the process of taking a series of input codes and converting them into output sequences of shorter length and fixed digits, i.e. hash values. Hash function value can be said to be a "fingerprint" or "abstract" of plaintext, so the digital signature of hash value can be regarded as the digital signature of plaintext. The characteristics of this encryption method are as follows: 1. The security of one-way hash function lies in its strong one-way operation process of generating hash value [2]. SHA1 algorithm is irreversible, anti-collision and has good avalanche effect. 2. Digital signature can be realized by hashing algorithm. The principle of digital signature is to convert the plaintext to message digest through a function operation (Hash). The message digest is encrypted and transmitted to the recipient together with the plaintext. The recipient generates a new message digest from the accepted plaintext and interprets the message digest from the sender. In close comparison, the results of comparison consistently indicate that the plaintext has not been altered, if not, that the plaintext has been tampered with.

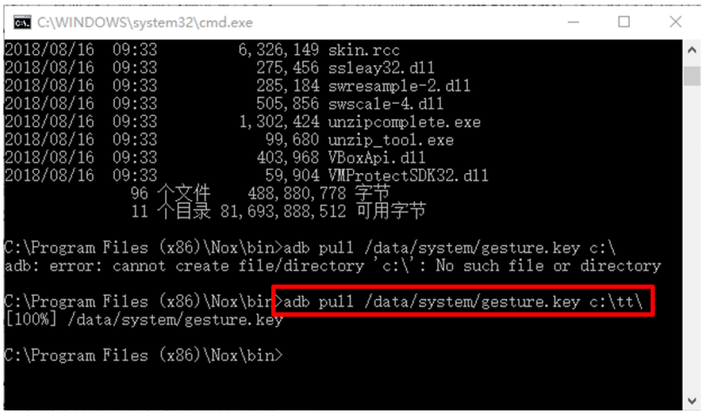


```
?p?肮l~l渤4`釪□....
```

Fig.1 Graphic Lock Password File

3. Graphic Lock Password Cracking

There are two most common methods to crack graphics lock password. The first is to clear the password directly. Because the file of graphics lock password is stored in a fixed location, that is, in the system/data/system/gesture.key file, as long as the file is deleted, it will naturally not need to input graphics password. Therefore, it is true that the file of graphics lock password is stored in the system/data/system/gesture.key file. In practice, we only need to build the ADB toolkit to build the debugging bridge of Android program, and then delete the password file directly by using the command line mode. The specific command behavior is rm/data/system/gesture.key [3]. The second method is to decode the encrypted file by parsing the encrypted file with third-party software. The specific steps are as follows. First, the graphics password file gesture. key is downloaded to the local area using ADB toolkit. The command behavior is ADB pull/data/system/gesture.key C:\ tt\ as shown in Fig 2. After that, use Gesture Cracker software to load graphical password files and crack them, as shown in Fig 3.



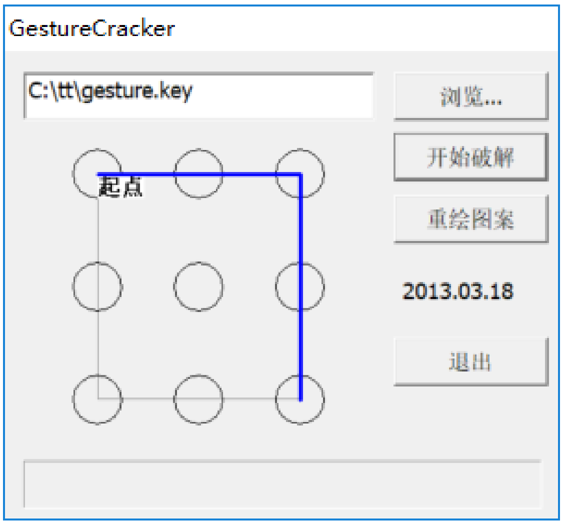
```
2018/08/16  09:33         6,326,149 skin.rcc
2018/08/16  09:33           275,456 ssleay32.dll
2018/08/16  09:33           285,184 swresample-2.dll
2018/08/16  09:33           505,856 swscale-4.dll
2018/08/16  09:33         1,302,424 unzipcomplete.exe
2018/08/16  09:33            99,680 unzip_tool.exe
2018/08/16  09:33           403,968 VBoxApi.dll
2018/08/16  09:33            59,904 VMProtectSDK32.dll
              96 个文件    488,880,778 字节
              11 个目录 81,693,888,512 可用字节

C:\Program Files (x86)\Nox\bin>adb pull /data/system/gesture.key c:\
adb: error: cannot create file/directory 'c:\': No such file or directory

C:\Program Files (x86)\Nox\bin>adb pull /data/system/gesture.key c:\tt\
[100%] /data/system/gesture.key

C:\Program Files (x86)\Nox\bin>
```

Fig.2 Download Graphic Password File



GestureCracker

C:\tt\gesture.key

Fig.3 Graphic Lock Password Cracking

Graphic lock password is a relatively simple password. Its essence is to convert the data in the Nine Palaces into byte arrays, and then directly encrypt SHA1. The encrypted file is finally stored in / data / system / gesture. Key. As long as the file is parsed, the deciphering operation of graphic lock password can be realized.

4. Introduction to PIN password

PIN cipher is an exponential cipher. Users only need to input four digits to unlock the cipher, so that the range of the cipher is limited to all digits between 0 and 9999. The principle of this cipher is to first input the original cipher + the salt value of the device, then use MD5 encryption and SHA1 encryption respectively, and then convert it into hex value. Finally, the two are spliced and saved to the local encrypted file. The local encrypted file storage directory is / data / system / password. key [4].

In this encryption mode, not only SHA1 encryption mode is used, but also MD5 encryption mode is applied. The following is an introduction to this kind of encryption mode. MD5 message digest algorithm, a widely used cryptographic hash function, can produce a 128-bit (16-byte) hash value, which can be used for this purpose. Ensure that information transmission is complete and consistent. Designed by American cryptographer Ronald Linn Rivest, MD5 was released in 1992 to replace the MD4 algorithm. The typical application of MD5 is to generate Message-Digest for a piece of information to prevent tampering. MD5 can produce an equally unique "digital fingerprint" for any file (regardless of its size, format, number). If anyone makes any changes to the file, its MD5 value, that is, the corresponding "digital fingerprint" will change. A brief description of the MD5 algorithm can be as follows: MD5 processes input information by 512-bit grouping, and each grouping is divided into 16 32-bit subgroupings. After a series of processing, the output of the algorithm consists of four 32-bit groupings. After cascading the four 32-bit groupings, a 128-bit hash value will be generated[5].

Comparison of SHA1 and MD5: Because both are derived from MD4, SHA1 and MD5 are very similar to each other. Correspondingly, their strength and other characteristics are similar, but there are still some differences as follows:

Security against forcible attacks: The most significant and important difference is that the SHA1 digest is 32 bits longer than the MD5 digest (SHA1:160 bits, MD5:128 bits). Using forcible technology, the difficulty of generating any message to make its digest equal to that of a given message digest is 2 ^ 128 orders of magnitude for MD5 and 2 ^ 160 orders of magnitude for SHA1. In this way, SHA1 is more powerful against forcible attacks.

Security for cryptanalysis: Because of the design of MD5, SHA1 is vulnerable to cryptanalysis attacks, and SHA1 is not vulnerable to such attacks.

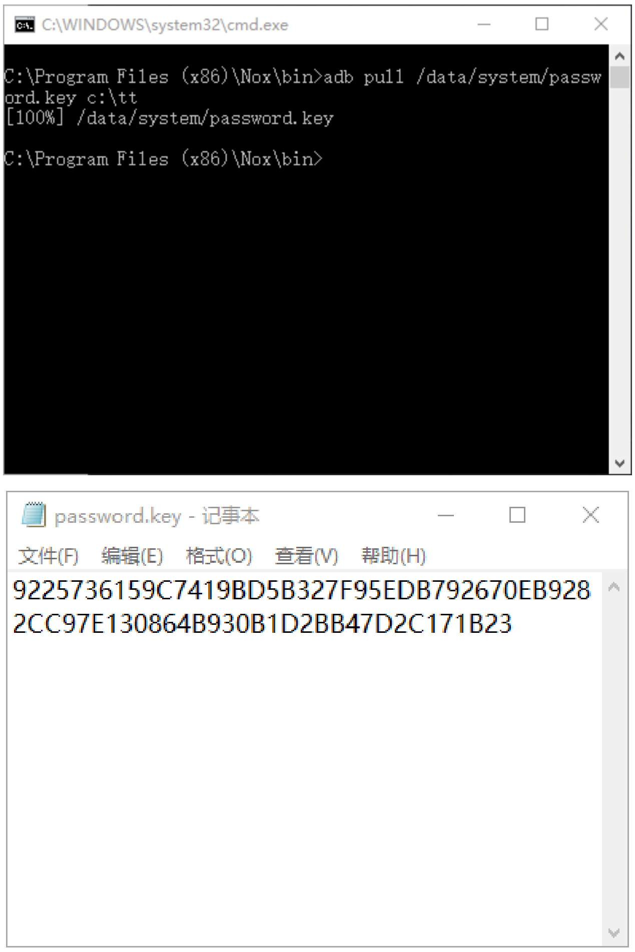
Speed: On the same hardware, SHA1 runs slower than MD5.

After understanding the encryption algorithm, the most important thing now is to get the corresponding salt value of the device. By using the getSalt function, the first step is to get the salt value according to the field Key as lockscreen. password_salt. If this value is found to be 0, it is generated randomly, then saved to the database, and finally it will be transformed into hex. The value is OK. According to the analysis, the name of the database is locksettings. db. Now just look at the contents of the database, you can find the corresponding device salt value.

5. PIN password cracking

Through the analysis of PIN encryption mode, if you want to crack PIN password, just get the PIN password file password. key and the device's salt value, then you can directly explode the relevant digital password by using third-party software. The specific operation steps are as follows:

First, get the password.key file, because the path of the file is unchanged by default and stored in the / data / system directory, so as long as you use the ADB toolkit to build an Android program debugging bridge, you can download the file directly to the local, the command line is ADB pull/data/system/password.key C:\tt\. After you get the file, you can Open it as a text file, as shown in Fig 4.



C:\WINDOWS\system32\cmd.exe

```
C:\Program Files (x86)\Nox\bin>adb pull /data/system/passw
ord.key c:\tt
[100%] /data/system/password.key

C:\Program Files (x86)\Nox\bin>
```

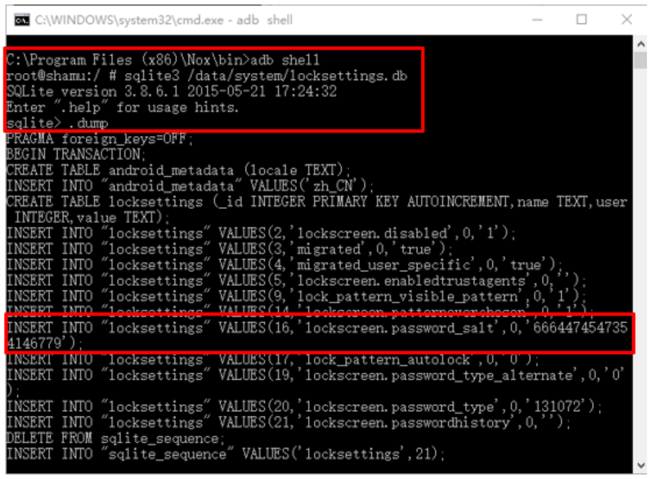
password.key - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
9225736159C7419BD5B327F95EDB792670EB928
2CC97E130864B930B1D2BB47D2C171B23
```

Fig.4 Obtain password.key

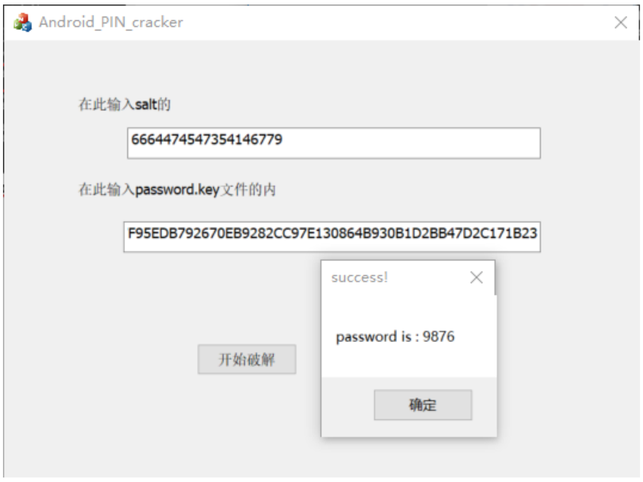
Secondly, after obtaining the password. key file, you need to use the command line ADB shell to rebuild the debugging bridge of Android program, and then look at the locksettings. DB database through the command SQlite tool to find the value of lockscreen. password_salt and download the record, as shown in Fig 5.

Finally, we need to use the third-party software Android_PIN_cracker to crack the PIN password, input the value of password. key and the salt value of the device into the software at the same time, and then directly crack it, as shown in Fig 6.



```
C:\Program Files (x86)\Nox\bin>adb shell
root@shamu:/ # sqlite3 /data/system/locksettings.db
SQLite version 3.8.6.1 2015-05-21 17:24:32
Enter ".help" for usage hints.
sqlite> .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE android_metadata (locale TEXT);
INSERT INTO "android_metadata" VALUES('zh_CN');
CREATE TABLE locksettings (_id INTEGER PRIMARY KEY AUTOINCREMENT,name TEXT,user
 INTEGER,value TEXT);
INSERT INTO "locksettings" VALUES(2,'lockscreen.disabled',0,'1');
INSERT INTO "locksettings" VALUES(3,'migrated',0,'true');
INSERT INTO "locksettings" VALUES(4,'migrated_user_specific',0,'true');
INSERT INTO "locksettings" VALUES(5,'lockscreen.enabledtrustagents',0,'');
INSERT INTO "locksettings" VALUES(9,'lock_pattern_visible_pattern',0,'1');
INSERT INTO "locksettings" VALUES(14,'lockscreen.patterneverchosen',0,'1');
INSERT INTO "locksettings" VALUES(16,'lockscreen.password_salt',0,'666447454735
4146779');
INSERT INTO "locksettings" VALUES(17,'lock_pattern_autolock',0,'0');
INSERT INTO "locksettings" VALUES(19,'lockscreen.password_type_alternate',0,'0'
);
INSERT INTO "locksettings" VALUES(20,'lockscreen.password_type',0,'131072');
INSERT INTO "locksettings" VALUES(21,'lockscreen.passwordhistory',0,'');
DELETE FROM sqlite_sequence;
INSERT INTO "sqlite_sequence" VALUES('locksettings',21);
```

Fig.5 lockscreen.password_salt



在此输入salt的

6664474547354146779

在此输入password.key文件的内

F95EDB792670EB9282CC97E130864B930B1D2BB47D2C171B23

password is : 9876

Fig.6 Android_PIN_cracker

6. Reinforcement measures

For Android system screen password existence of various possibilities to be cracked, the proposed reinforcement measures include three aspects, one is not to brush the machine privately, leading to the opening of root permission, because all the above-mentioned operations are premised on the first need to obtain the root permission of the system, so managing the root permission is to ensure the security of the system. Secondly, change the password regularly, whether graphics lock password or digital password, when setting graphics lock password, try to select complex graphics, connect as many points as possible, make the graphics path as complex as possible, increase the difficulty of cracking, and do not use daily numbers when setting digital password. For example, mobile phone number, ID card number, license plate number, etc., so as to prevent malicious snooping, trying, and thus cracking the code. The third is to use more advanced encryption methods as far as possible, such as fingerprint identification password and face recognition password.

Fingerprint identification technology [6] has been widely used in mobile devices such as mobile phones. Fingerprint identification technology matches a person's fingerprints with his fingerprints. By comparing his fingerprints with pre-stored fingerprints, we can verify his real identity and unlock all kinds of mobile devices. Capacitive fingerprint identification, optical fingerprint identification and ultrasonic fingerprint identification, etc. Capacitive fingerprint identification is based on the electric field formed by fingerprint sensor and conductive subcutaneous electrolyte. The fluctuation of fingerprint will lead to different changes in the pressure difference between the two, so as to achieve accurate fingerprint determination. The advantage of capacitive type is that it has strong recognition and adaptability, and has no special requirements for the use environment. Optical fingerprint identification may be familiar to you, such as the use of optical identification in the unit's attendance machine and entrance guard. Optical fingerprint recognition mainly uses the principle of refraction and reflection of light. However, this technology has not been widely used in the fingerprint unlocking of mobile phones, because of its poor penetration, easy to be affected by the light source and screen color, resulting in recognition errors. Ultrasound penetration is strong. Fingerprint module can be used to send a specific frequency of ultrasound scanning finger, using different fingerprints to reflect different ultrasound, so as to establish 3D fingerprint graphics; can penetrate metal, glass and other commonly used mobile phone materials, there will be no too many restrictions on the appearance of the mobile phone. Fingerprint recognition is shown in Fig 7.

Fig.7 Fingerprint recognition technology

Face recognition technology [7] has gone through many stages of development. The following is related introduction. The first stage is to get the basic contour of the face through the front-end camera of the mobile phone and unlock the system by plane recognition. It does not need any unique hardware support, but only related algorithms. This kind of elementary face recognition technology has the advantages of very low computational complexity, fast speed and almost no hardware requirements. But the disadvantage is that the security is so low that a photo can fool the security mechanism. In the second stage, through the improvement of the algorithm, it has the ability to learn, and uses structured light computing to obtain the facial depth information. The research cost of this algorithm is high, and the amount of computation is also increasing sharply. The advantage of this algorithm is that it improves the security on the premise of taking into account the recognition speed. At present, some mobile phone brands also use it. This recognition technology has its drawbacks. As long as a side face color print photograph with radian is prepared, the algorithm can still be deceived and directly recognized into the mobile phone. The third stage uses infrared or optical sensor scanning to generate a high-resolution human head model as recognition material, and uses deep learning to identify whether a real person is in front of the machine. By combining the algorithm with physical recognition, a safe and efficient face recognition technology has been achieved. Apple has produced the product. The iPhone X uses this recognition technology. But the disadvantage is that the related costs are relatively high, whether it is the development cost of the algorithm or the procurement cost of the hardware. As shown in Fig 8.

Fig.8 Face recognition technology

7. Summary

This paper mainly introduces the related contents of screen passwords in Android system, including graphic lock password, PIN password, fingerprint recognition technology and face recognition technology, and focuses on the detailed introduction of graphic lock password and PIN password, including the related encryption principle, the internal structure of password file, storage location and other issues. Detailed description is given, relevant cracking methods are put forward, and relevant password cracking is realized by using tools. Based on the above-mentioned password vulnerabilities, the defensive measures of password reinforcement are put forward, which provides better security for users to use devices safely for network life. In addition, the related theories of advanced fingerprint recognition technology and face recognition technology are introduced, their advantages and disadvantages are pointed out, and a better security scheme is given for users to choose better.

References

[1] Chen Zhaoyan, Huang Juncan. An Analysis of the Graphic Lock Problem of Android Mobile Screen [J] Strait Science, 2014 (10): 50-51B

[2] Zhao Yangyang, Qin Lijia. Identity authentication based on graphic password [J]. Digital technology and application, 2013 (2): 177-177.

[3] Ni Chaofan. Feasibility analysis of violent cracking of screen password lock in Android system [J].Journal of Hengshui University, 2014.1:12-14

[4] WangJiMo Research on lock screen password and cracking method of Android smartphone [J].Criminal Technology, 2015,40(02): 142-145.

[5] RenJieLin Security Analysis and Improvement of MD5 Encryption Algorithms [J].Journal of Agricultural Library and Information Science, 2017,29(07): 39-42.

[6] Liu Zhen, Wang Guoshi, Mo Yun, Huang Xiaojing, Zou Xiaojuan. Application and Research of Fingerprint Identification Technology in Identity Authentication [J]. Information Recording Materials, 2018, 19 (11): 93-94.

[7] Chen Siqi, Zhao Haoyue, Wang Jingyi, Jia Jingtan. Overview of Face Recognition [J]. Computer Fans, 2018 (12): 226.