World Journal of Research and Review (WJRR)
ISSN:2455-3956, Volume-2, Issue-4, April 2016 Pages 05-09

Design and Implementation of Privacy Retrieving and Forensics Reversing System Based on Android OS

Zhangyu Wang, Weiwei Huang, ZhenHua Tan

Abstract— **With the Mobile Communication Technology getting mature, mobile phone with full feature and comfortable user experience has become the indispensable part of communication tools in our daily life[1]. Mobile phone has been accepted and loved dramatically by many users due to open environment and abundant platform applications. However, mobile phone is likely to be lost or stolen because of its portability, that is to say, how we should do to protect or retrieve and recover private data from remote is of great concern, such as images, videos, documents, some private tools as well as the password of online payments and bank cards. Once it was lost, the important private data will be accessed by others intentionally or unintentionally, which may dramatically increase the risk of property loss. As all these issues, we adopt bleeding technology to design and implement a new type of Android-based forensics reversing and dynamic privacy management system in the cloud environment, so that we could obtain evidence by the real time monitor and remote control on either mobile phone or PC. As well as many other features, includes One Key Recovery, One Key Forensics and One Key Data Protection. The experiment and analysis show that, the Forensics and Dynamic Data Protection System is full-reatured and high performance comparing to the existing products in domestic and foreign market.**

Index Terms— **Dynamic Privacy Management, Remote Privacy Retrieving, Screen Locking, Ahttpd Asynchronous Network Communication Framework**

I. Introduction

The openness of the application environment and the diversity of application software makes the Android system security issues have been concerned about all the time, scholars at home and abroad have studied the security design of the application of Android system and Android system.2010,Y.Fledel, Y.Elovici, A.Shabtai et al. Published the paper Android-Powered Mobile Devices Using SELinux Securing, the strategy of using SElinux to enhance the security of Android system kernel is proposed 2013, Mishra, Jeter put forward the method of identifying the risk exposure of Android device users in the paper Identifying And Quantifying The Android Device Users'Security Risk Exposure.2013, Wang Lingli, Li Wenlong in the paper Android security mechanism and application of software security research analysis of the hidden dangers in the Android security mechanisms and malicious applications to steal user information behavior in depth.Facing the security problem in Android application environment, major domestic and foreign security vendors take active measures to invest a lot of energy for the research of Android mobile phone protection software. The United States McAfee company released the WaveSecure software on the Android platform, which allows users and mobile phone to establish a remote connection, if the phone is lost or stolen , the device can be locked instantly , and clear the user's private data stored on the phone, and provide remote data backup, tracking phone calls, malicious software identification and other functions. But WaveSecure did not set up a black list, as long as it is recognized by the software malicious processes or virus program ، both false positives or harmless, it shall be isolated, the user knows the application is secure, but can not make it run. Domestic Tencent Inc, 360 Kingsoft Corp also launched a software QQ mobile phone housekeeper, Jinshan guards, 360 mobile phone security guards and other similar software but this type of application performs in a passive defensive way, If the user does not find the phone stolen and control it remotely at once, the finder will be able to unlock the phone and delete this kind of application services directly.

Zhangyu Wang, Software College, Northeastern University,Shenyang City,China, 18202429356
Weiwei Hua, Software College, Northeastern University,Shenyang City,China, 18524407457,
Zhenhua Tan, Software College, Northeastern University,Shenyang City,China,13478212785

II. Problem Analysis

Comparative analysis of Android security products at home and abroad, Hunter's new type of forensic system provides a more complete solution to user. The operation is more convenient, the purpose of remote control is stronger, Analysis of Android security products in the market, we found out these following functional defects:

1. In terms of network: Does not provide the mandatory network connection, once the device is lost, the device will be in a state of no network. Most Android security products fails[2]. Only through a single message sending to the target phone in order to perform this operation, this will lose the significance of personal mobile terminal security products. (As long as the target phone to meet certain conditions, any mobile phone can make it as long as it can send text message).

2. In the aspect of obtaining evidence: The speed of forensic is too slow, what's more, the evidence of address and the pick-up of the photo is sent to the third party mail. Controller get the evidence by PC or mobile terminal landing the third party mailbox. Open the browser and click the link ,and then you'll get the location information and finder's photo. Quite complicated operations and it is difficult to obtain the evidence.

3. In the aspect of SIM card: Most of the mainstream market for personal mobile terminal security products does not support SIM card replacement reminder. This means that on the detachable hardware, once the SIM is replaced, in case of unknown load SIM card number on the target phone, can not send text messages from the control side to the target phone by instructions.

4. Over reliance on message control: The vast majority of Android security products did not support the cloud servers, so that they can not ensure that once the SIM card fails, the device is still in the good state of network, leading to the results that once the SIM card is pulled out, the vast majority of the evidence collector in the system will be completely ineffective.

5. On the lock screen: The mainstream personal mobile terminal security products in the market, especially Qihoo 360, Kaspersky , a small number of enterprises of mobile terminal security products to provide a screen lock feature. However, they don't Shield the Home key, the Menu key and the Power Key. Once the device is lost, the finder may immediately long press the power button to shut down the system, it will increase the obstacles for the subsequent evidence. Even make the personal mobile security products go failure.

6.Important APP lock aspect: Because of the user's habitual operation and lazy habit, causing a lot of APP running in mobile phone system background. After closed, login in the second time does not require entering the password again. This is a huge risk, once the phone is lost, and the phone is not in the lock screen state protection or cracked the lock screen password, may easily enter any application. For example, QQ, Wechat, Alipay, Online Banking, and there are lots of privacy information memorandum or information associated with a variety of bank accounts can be arbitrary operation. Many payment platforms provide quick payment, you can only get the verification code will be able to pay. And wanton operation of social networking applications, important personal privacy information easily exposed.

7. In terms of private data recovery: In the mainstream personal mobile terminal security products, the data recovery features is provided by sending SMS to the phone, in order to restore to a third party mailbox which is previously binded by the users. However, users get these data (such as text messages and contacts) by logging in to the third party mailbox, And then manually enter the new phone one by one, the tedious and monotonous mechanical operation process is not acceptable to people who are living in an environment with a fast pace of life.

III. Proposed Solution

1.In terms of network: The Hunter's new forensic system offers the ability of forcing to open the network，Just send the following instructions to the target phone ： " #*opennetwork*#+ Original phone login password" Can be forced to open any mobile phone with a hunter Forensics System，After connected to the network. you can follow the evidence and privacy management operations.

2. In the aspect of obtaining evidence: In the view of the complicated operation, the situation is not easy to do evidence collection,Achieve a key remote control,return the location information to the hunter's operation interface. No need to intervene in the third party mailbox,no need for third party APP intervention.

3. In the aspect of SIM card: Implement the replacement of SIM card to remind, get replaced SIM card number so that remote control can follow up, we implement a pre-binding reception number. Once the device is lost, the SIM card is replaced. The blinding number immediately received a notice, and get the latest mobile phone number to be replaced. Expand the channels of evidence collection, using the cloud server to use the Jpush API to control remote network directly.

4. In the lock screen and important APP: Achieve the built-in screen locking features, shielding Home key, MENU key and power key, and can not be shut down on the device that can not remove the battery. Achieve remote APP bulk lock, the selected APP is locked out immediately, unable to make a landing, The loss of privacy and financial caused by loss of user equipment is reduced to the maximum extent. Hunter's new forensic system provides APP remote locking,assure the APP which contains sensitive information will not used by others.

5. In terms of privacy data recovery: Hunter's new evidence system implements the feature of one key restoring data to the new phone, text messages and contacts can be one key restored, manually input is not required. The remote backup module implements the content specified by the control terminal upload directly from the lost device to the cloud server, to provide the required data at any time. The data recovery module can restore the required content directly to the corresponding position. For instance, all SMS of target phone restored to the control side SMS directory by one key.

IV. Processes of Proposed Solution

Mobile phone screen lock: Replace lock screen of system, do not allow the system to display the screen lock. Shield off the Home keyboard, back key, menu key. Every time the screen light up can be able to show the custom screen lock. First step,adding permission settings to the Android system configuration file Manifext.xml can cancel system to lock screen. Second step,the way of using suspended window, and the suspension window occupies the entire screen, the suspension window level is set to LayoutParams.TYPE_SYSTEM_ERROR, other interfaces can be covered. Third step,through the way of receiving system broadcast, when the user's screen is off, the screen lock is started, Some events of Android system will send a system broadcast. Use BroadcastReceiver to receive the broadcast (Intent.ACTION_SCREEN_OFF).

Remote control uses Jpush API, after user logined, use users' name as a tag, If the user's mobile phone is lost, it can be verified on another phone, the server sends a specific instruction based on tag, after receiving instructions from the server, mobile terminal carries out related operations. we use Android corresponding API like TelephonyManager to obtain the SIM card's unique serial number[3]. Save in local via SHA-1 encryption. The way is to use the SharedPreferences. SharedPreferences is a lightweight storage class on the Android platform. Being used to save some of the commonly used configurations, and the data format is XML. When the

SIM card state transforms, Android system also has a corresponding broadcast, after receiving the broadcast, gets the serial number of the SIM card, compared with the original serial number. After getting the relevant data to be backed up by the user, encapsulate data in JSON format, and encoded by Base64, finally uploaded to the cloud based on user name.

Receiving through a broadcast receiver（BroadcastReceiver）code as follows:

```
public class LockScreenReceiver extends BroadcastReceiver {
    @Override
    public void onReceive(Context context, Intent intent) {
            if (intent.getAction().equals(Intent.ACTION_SCREEN_OFF)) {
            //do something..
        } else if (intent.getAction().equals(Intent.ACTION_SCREEN_ON)) {
            //do something..
        }
```

When the system receives the broadcast of the screen, a broadcast that can be displayed in some way（When the screen is put out, the efficiency of the interface is the highest, once again lit that is the screen lock interface, when the screen is lit and then display the interface needs a short period of loading process, the experience is poor）. Where to register the broadcast is also a problem, it is conceivable that when the user opens the switch of the screen lock,user is able to start a service, and then register the broadcast in the Service. Of course, in order to improve the priority of the service, the service can be set to the front desk service, to avoid the phone memory is not enough to be killed. Using **WindowManager** to display the lock interface is a better way. Many mobile applications, including 360, have a suspended window, the suspension window is activated by the interface. After testing, in MIUI, this type can even make the window on the shutdown option. The parameter code is as follows:

```
wmParams = new WindowManager.LayoutParams();
wmParams.type
|=WindowManager.LayoutParams.TYPE_SYSTEM_ERROR;
wmParams.flags |= LayoutParams.FLAG_LAYOUT_IN_SCREEN;
wmParams.width = WindowManager.LayoutParams.MATCH_PARENT;
wmParams.height = WindowManager.LayoutParams.MATCH_PARENT;
```

In forensics, the screen lock has played a crucial role, then how to obtain evidence? A simple idea is to call the front camera when the phone is unlock failed three times, take pictures in silence. At the same time, sending photos to the phone user's mailbox or allow the user to view in some way. Therefore, logical judgment when the user is unlocked, when the user fails to unlock the third time, call the API of Android to enable the front camera to take pictures. As shown in fig. 1.

One of the important functions of remote operation is the editor of the information, backup to server and delect, Then after receiving the push, how to delete the relevant information? Android provides the corresponding interface. ContentProvider is a way of sharing data across applications. Editing system contacts, text messages as well as album, Can also get the ContentResolver object by getContentResolver, interacting with the ContentProvider , which is provided by the system[4], simply call the corresponding URI. After obtaining the contentResolver object, using query and delete methods in contentResolve to query and delete the corresponding data. As shown in fig. 2.

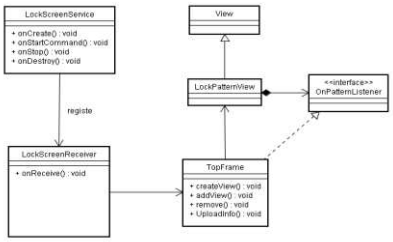

fig.1. Lock screen forensics module ideas

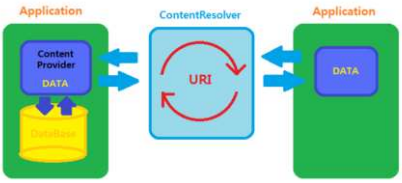

Fig. 2. Interaction process

As for how to achieve the alarm sound can not adjust the volume, forced open maximum sound. Specific ideas are as follows: The audio file of the alarm can be placed in the directory of the Android project res/raw, just call MediaPlayer to play. Volume adjustment can be carried out by AudioManager. As long as the audio playback continues to increase the volume, it is worth noting that opening a new thread to increase the volume is required. Because if the main thread in the Android (UI thread) for time consuming operation, will block the main thread, resulting in ANR[5].

A function of remote operation is to shield the application,refers the use of the user specified application, start a mask page of the Activity and can not enter the original application,the application is specified by the user in advance, when the phone received a push,then do the shielding actions. The method is as follows: Get installed App through PackageManager, allows users to specify the application in emergency situations, and the package name of each application is saved in the local by SharedPreferences, when the phone receives a push, starting a Service, the Service function is called through the Handler to call ActivityManager, gets the top running Activity on the Task stack and gets the package name of the Activity, compared with the stored package names, if match，just start an empty content of Activity, at the same time the Activity rewrite the onBackPressed () method, makes it impossible to return the Activity of the target application by returning the key.

How to achieve remote mandatory open network connection? When the system receives a message,system will release an action name for the android.provier.Telephony.SMS_RECEIVED broadcast Intent,the Intent stores the contents of the received text messages, use the name pdus to get the message content from Intent.Therefore,defining a BroadcastReceiver is required. When receiving text messages,read the contents of the message, according to the contents of the message to perform different operations.

Specific ***onReceive()*** method code is as follows:

```
public void onReceive(Context context, Intent intent) {
        Object[] pdus = (Object[]) intent.getExtras().get("pdus");
            for (Object pdu : pdus) {
                SmsMessage sms = SmsMessage.createFromPdu((byte[])
pdu);
                String content = sms.getMessageBody();
    }
```

Of course, if only by text messaging, it'll be in a low efficient state , while the cost is greater than the network operation. Open the mobile network through the ConnectivityManager is more efficient, that is, if system receives instructions to open the mobile network, then open the mobile data traffic and the network can be used directly by the remote control.

As how to implementation of monitoring in the SimCard transform, the idea of this function is: Users enter the phone number of their friends and relatives to bind, save the number on the phone,when the SIM Card changes to the phone, the

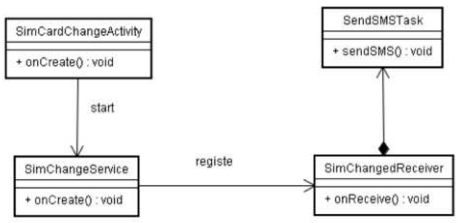

Fig. 3. SIM card replacement detection

bound phone is notified in particular way. The user's mobile phone card information can be obtained through the TelephonyManager[6],Due to security reasons, it can not get the user's SIM Card phone number, but to get the serial number of the SIM Card is also feasible. Code as follows: (TelephonyManager)getSystemService(Context.TELEPHONY_SERVICE) .getSimSerialNumber();The serial number is unique[7], so the sequence number and the number of binding storage by sharedPreference. When the SimCard state is changed, the system will send a broadcast, the broadcastactionandroid.intent.action.SIM_STATE_CHANGED , then calling SmsManager's SmsManager() method to send message. As shown in fig. 3.

V. System Test and Analysis

Ahttpd asynchronous network communication framework is based on independent development is the underlying architecture,the development of storage subsystem, subsystem and push mail system is on the basis of the architecture, these systems set up to achieve the function of obtaining evidence. At the same time, information security is also needed, server and client communications entirely uses SSL to ensure the security of data in the process of transmission.

On PHP (APACHE), Node.js and self-developed Ahttpd using siege(a web performance pressure test tool) to perform efficiency comparison test, the two set of tests were tested using only the Hello World string and Fibonacci Sequence, where n = 1000 returned to the client, from the complexity of the code is Ahttpd > Node.js > PHP, but the amount of Ahttpd code does not increase linearly with the complexity of the application. As shown in fig. 4.

As for a high performance server, availability to reach 100% is essential.Concurrency: 428.31,Failedtransactions: 0,Longest transaction: 1.21 indicate that Ahttpd relative to the advantages of PHP and Node.js. In particular, the number of concurrent and the length of time spent on each transfer, these two indicators reflect the ability of a server's concurrency and data processing. The total time that Ahttpd handles all requests is not increased with the complexity of the business logic, this benefits from the use of C++ as a programming language with high efficiency and flexibility.

```
Transactions:                  10000 hits
Availability:                 100.00 %
Elapsed time:                  16.85 secs
Data transferred:              60.60 MB
Response time:                  0.84 secs
Transaction rate:             593.47 trans/sec
Throughput:                     3.60 MB/sec
Concurrency:                  497.25
Successful transactions:       10000
Failed transactions:               0
Longest transaction:            1.42
Shortest transaction:           0.00
```

figure 4 Efficiency of ahttpd (C++)

VI. Conclusion

In the overall design of the system, the combination of C/S mode and B/S mode is adopted. Not only remote control of the lost mobile phone through the mobile terminal，but also can be logged on the PC browser to the Web side of the mobile phone security management system to remotely control the target phone. During the development of the system, many problems and difficulties have been encountered. Because the various manufacturers to develop the second generation system with their own products on the basis of the Android system, then creates a screen adaptation problem, the problem is solved by using an interface layout file corresponding to each type of screen size. The realization of retrieve and forensics system can run smoothly in a variety of Android simulator and real machine. There still much left for improvement, and the prospect is as follows:

Mobile terminal and mobile terminal real-time screen monitoring can be realized with the aid of the streaming media technology, to remote monitoring of the behavior of any access to user privacy information[8]. And provide the corresponding privacy information recovery measures. Improve the judgment SIM binding basis by improving the algorithm, making the judgment more reasonable. Last but not least, basing on the Android system kernel to do more in-depth research is necessary.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No. 61572123;the Fundamental Research Funds for the Central Universities under Grant No. N151708005.

References

[1] Thimmarayaswamy K, Mary M. Dsouza, G. Varaprasad. Low power techniques for an android based phone[J]. ACM SIGARCH Computer Architecture News. 2011, 39(2):28-29

[2] Namheun Son, Yunho Lee, Dohyun Kim, Joshua I. James, Sangjin Lee, Kyungho Lee. A study of user data integrity during acquisition of Android devices. Digital Investigation, 2013, Vol.10, pp.S3-S11

[3] Antonio Corradi, Mario Fanelli, Luca Foschini,Marcello Cinque. Context data distribution with quality guarantees for Android-based mobile systems. Security Comm. Networks, 2012, Vol.6 (7)

[4] Ahmad, N.A.N.,Akhbariee, N.I.,Hafizuddeen, M. . Requirements analysis of android application using activity theory: A case study . Information and Communication Technology (ICoICT), 2013

[5] A. R. Beresford, A. Rice, N. Skehin,et al. MockDroid: trading privacy for application functionalityon smartphones[C]. In 12th Workhop on Mobile Computing Systems and Applications, 2011

[6] McClurg J, Friedman J, Ng W. Android Privacy Leak Detection via Dynamic Taint Analysis[J]. 2011

[7] Enck,W.,Ongtang,M.,McDaniel,P.Understanding Android Security[J] . Security & Privacy, IEEE.2009,7(1). 43~49

[8] Davi L, Dmitrienko A, Sadeghi A R, et al. Privilege escalation attacks on android[J]. Information Security, 2011, 324-356.

Zhangyu Wang ,majoring in Infermation Security and currently focusing on Complex Network Technology, Network Space Security Technology and Mobile Terminal Security Technology.

Weiwei Huang ,majoring in Software Engineering and currently focusing on Integrated Web Technologies, Distributed Systems and Container Technology. Northeastern University,China.

Zhenhua Tan ,received his ph.D degree in Computer Science and Technology form Northeastern University at Shenyang,China. He is a associate professor and vice director of Network Security Department. Focusing Academy of Information Technology.