Sensitive Data Protection on Mobile Devices

Fan Wu
Department of Computer Science
Tuskegee University
Tuskegee, Alabama, USA

Chung-han Chen
Department of Computer Science
Tuskegee University
Tuskegee, Alabama, USA

Dwayne Clarke
Department of Computer Science
Tuskegee University
Tuskegee, Alabama, USA

***Abstract*—Nowadays, many mobile devices such as phones and tablets are used in the workplace. A large amount of data is being transferred from one person to another. Data transfer is used for several different fields. Many companies and institutions are focusing on research and development on the way to further protect sensitive data. However, sensitive data still get leaks on mobile devices. To analyze how sensitive data get leak, a simulation on transferring sensitive data is developed. In this paper, we present the analysis of mobile security problem dealing with sensitive data from getting out. The goals in our research are for users to have a greater understanding on how data is being transferred and prevention sensitive data from being stolen. Our work will benefit mobile device users and help to prevent sensitive data from being stolen. Our experiments show different ways to safely transfer information on mobile devices by testing three methods types, which are back-up, encryption, and lock plus wipe data.**

Keywords—Mobile Security; Sensitive Data; Data Protection

I. Introduction

Mobile Security is a very important field in the security world. Computer data transfer plays a very important role in daily life. The importance of the transfer data can range from business, schools, companies, and government documents. The process of transfer data is to focus on finding answers for life problem by transfer information from one person to another. In order to analysis how data being transfer from the mobile device and to prevent sensitive data from getting out there, we need to simulate several different ways how data can be transfer on the mobile device. Data transfer is achieving by safely copying or moving important data from one location to another. Some examples are, computer to computer, computer to mobile device, mobile device to mobile device, mobile device to the server, and computer to the server. Now it is much easier and faster to transfer data today than it was in the past few decades.

Nevertheless, it is even easier for hackers to get sensitive data from the users. As a result, many researches are needed to find safer ways to transfer data and information on the mobile device.

In this paper, we present analysis of mobile security problem dealing with sensitive data from getting out there. Data transfer is copying data from a storage device to memory also copying data from one computer to another [1]. As a result transfer data has increased it range for transfer data it just not only are computer, but are phones, tablets, and server.

Data transfer has many benefits, which include, offloading server work, robustness support environment, transferring only relevant data, backup data, and balancing resources in an application development environment. A redistribution of work load boosts response time for production systems that run on servers.

Increasing robustness to the decision support environment works in the case of a network failure that would temporarily eliminate access to the server's data. Transfers Only Relevant Data can transfer only the data that you need to use. Model of a Centralized Control Point automated jobs that can run during non-peak hours can distribute data and applications to multiple computers that need the data and the applications for the next day's work. Back-Up Client Data and applications can be copied from a client that has limited memory resources to a server that has more memory resources. This provides a backup in case of loss on the client. Balances Resources in Application Development Environment programmers can use Data Transfer Services to make efficient use of network resources [2].

This paper focuses on three solutions on how to prevent sensitive data from getting out on the mobile device. They are back-up, encryption, and remote lock plus wipe data. These solutions can be used for many different applications not only for personal use but for the business world as well also can be used on a number of mobile devices such as, phones and tablets. Although many approaches were use on the computer and had been applied with advantage to the solutions of some of these problems, we will explored this issues on an Android phone or tablets to see if one or both can be prevent sensitive data from getting taken from the user.

The rest of the paper is organized as follow: Section II introduces some previous related work; Section III describes the background on Sensitive Data on mobile device briefly; Section IV presents the experiments and research on prevent sensitive data from getting out there; and our experimental results are presented in Section V; Finally Section VI concludes this paper with our future directions.

II. Related Work

The smart mobile devices, such as smartphones and tablets, are becoming an essential tool in people's personal and business activities. A large amount of personal data and even more sensitive important company data are stored in these devices, which also exposes a severe risk to device users when their devices are lost or stolen. If no defense mechanisms were enforced a prior, the lost or stolen devices would leak user information: your passwords can be broken, your emails could be seen, e-commence data such as online purchasing or banking transaction might be viewed; The situation would be worse when a device has the access right to Enterprise networks, e.g., via VPN, in which company networks will be exposed to malware or could be hacked It is one of major focus of security concerns for Android mobile device [3].

Sensitive data have always been important but sensitive data on a mobile device just gaining attention. Also there is some work related to sensitive data on a mobile device. Here we just refer to some recent work closely related. University of Cincinnati and Southern Polytechnic focuses on the development of Mobile Security Lab ware which shows users on how to protect and prevent sensitive data before and after a device is lost or stolen. The different between their and our work is that what type of data can be prevented on the mobile device.

Another related work was from Dimensional Research. They mainly focused on is how many mobile devices store sensitive customer and business data. The statistics results show that users reported a significant level of very sensitive information was on their mobile devices, including customer data (47%), network login credentials (38%), and corporate information made available through business applications (32%) [4].

The Ponemon Institute research focuses on [5] conducting high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations. In addition, only 27% of users regularly update their passwords, again, leaving them vulnerable to security attackers [6]. Ernst & Young research was explaining that sensitive information or application configurations maybe accessible to users or unauthorized parties through various means [7]. American Health Information Management Association takes sensitive data on mobile security to medical point of view.

By saying, mobile devices are easily lost or stolen and thus pose increased risks to the confidentiality and security of patient health information. Loss or theft of a device could easily result in the need for patient breach notification and subsequent reporting to the Department of Health and Human Services and media as required under the American Recovery and Reinvestment Act [8].

III. System Architecture

The Android system that we used in our research and implementation is the API (Application Programming Interface), which connects with the devices to build functions program and create application to do many things. As the API level rises up the more add-ons. All Android system compatibles devices support 32 and 64 bit processing. This platform interacts with such mobile devices as phones and tablets.

The Sensitive Data Architecture is in Fig. 1 shows sensitive user data is only available through protected APIs [9]. The components of a sensitive data on the mobile device are personal information, input device, and metadata. Those are the types of sensitive User Data. API is the only way that another user can access sensitive data from the user.

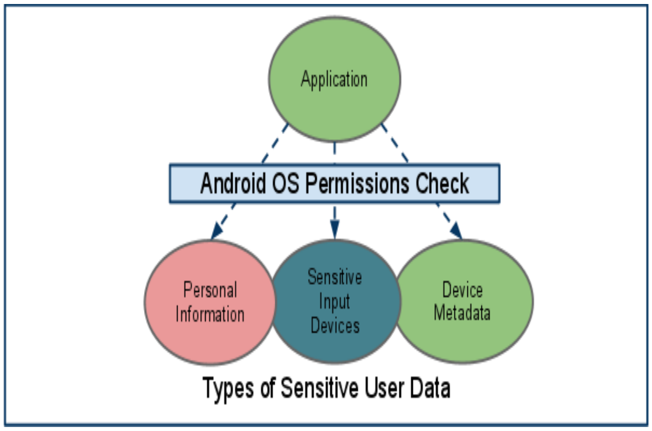


Fig. 1. Sensitive Data Architecture [9]

A. Personal Information

Personal Information is the information that identifies who you are. It will admission the user information and set it in a protected API. For example are contacts and calendar information on the device.

B. Sensitive Data Input Devices

Sensitive data inputs allow the applications or program to interact with the nearby environment, such as camera for taking pictures, microphone for speaking into or GPS for look for location. In order for third-party to gain access it needs the user permission for it.

C. Device Metadata

Device Metadata restricts access to data that is not natural, but also reveal some information about the user, user options, and the user method on the mobile device. For example are phones, logs, browser history, and text messages on the device.

IV. Protect Sensitive Data

Sensitive data has always been important not only for mobile security but computer relative issues. Some of the common problems with protect sensitive data on the mobile device are if your device get stolen, hacked, or damage. These are three methods that can be used to help the user protect sensitive data from getting out there which are back-up, encryption, and lock plus wipe data. Now for the programming, testing, and application parts to see if protect multiple types of sensitive data.

A. Back-Up

Back-Up is a copy of a file, program, or entire computer system in an event for the original get stolen, hacked, or damage. We are going to test if we can backup file such as, calendar, contacts, SMS, and even phone calls on the mobile device. To see how fast the process and where backup files will go. The way we are going to back-up files is by using a backup agent.

The algorithm 1 labeled "Back-Up Agent Code" shows class name for your backup agent, which is declared in your manifest with the android:backupAgent attribute in the <application> tag [10].

The algorithm shows the user how it works.

```
<manifest...>
...
 <applicationandroid:label="MyApplication"
          android:backupAgent="MyBackupAgent"
>
        <activity...>
             ...
             </activity>
      </application>
</manifest>
<applicationandroid:label="MyApplication"
            android:backupAgent="MyBackupAgent">
 <meta-data
android:name="com.google.android.backup.api_key"
        android:value="AEdPqrEAAAAIDaYEVgU6DJnyJdBm
U7KLH3kszDXLv_4DIsEIyQ"/>
</application>
// Get the oldState input stream
FileInputStream instream = new
FileInputStream(oldState.getFileDescriptor());
DataInputStream in = new
DataInputStream(instream);

try{
    // Get the last modified timestamp from the state file and
data file
    long stateModified = in.readLong();
    long fileModified = mDataFile.lastModified();

if(stateModified!=fileModified){
       // The file has been modified, so do a backup
       // Or the time on the device changed, so be safe and do a
backup
 }else{
    // Don't back up because the file hasn't changed
  return;
 }
}catch(IOExceptione){
    // Unable to read state file... be safe and do a
backup
}
public class MyFileBackupAgent extends
BackupAgentHelper{
  //The name of the file
         static final String TOP_SCORES = "scores";
         static final String PLAYER_STATS = "stats";
    // A key to uniquely identify the set of backup data
    static final String FILES_BACKUP_KEY =
"myfiles";

     // Allocate a helper and add it to the backup agent
   voidonCreate()                                          {
       FileBackupHelper helper = new
FileBackupHelper(this, TOP_SCORES,
PLAYER_STATS);
 addHelper(FILES_BACKUP_KEY,                  helper);
 }
}
```

Algorithm 1. Back-Up Agent Code [10]

B. Encryption

Encryption data is another way to protect your mobile device from leaks sensitive data. Encryption data transforms data into a secret code or message that unreadable form that uses algorithms. We tested to see what type of data can be encrypted and where the data is going to be storage. The process we are going to encryption data is by using encryption application which is call universal encryption app and show some coding for SMS encryption. The algorithm 1 labeled "SMS Encryption Code" shows how the encryption and decryption works with RSA encryption and decryption algorithm [11].

```
public static void generateKey() throws Exception
    {
     KeyPairGenerator gen =
KeyPairGenerator.getInstance(RSA);
     gen.initialize(512, new SecureRandom());
     KeyPair keyPair = gen.generateKeyPair();
     uk = keyPair.getPublic();
     rk = keyPair.getPrivate();
    }
   private static byte[] encrypt(String text, PublicKey
pubRSA) throws Exception
    {
     Cipher cipher = Cipher.getInstance(RSA);
     cipher.init(Cipher.ENCRYPT_MODE, pubRSA);
     return cipher.doFinal(text.getBytes());
    }
   public final static String encrypt(String text)
    {
     try {
      return byte2hex(encrypt(text, uk));
     }
     catch(Exception e)
     {
      e.printStackTrace();
     }
     return null;
    }

   public final static String decrypt(String data)
}
```

Algorithm 2. SMS Encryption Code [11]

C. Lock and Wipe

If all else failed the user have to option to lock or wipe all sensitive data for their mobile device. We tested to see if all sensitive data can be lock or if not at least wipe all sensitive data from the mobile. The application we use for our research is Lookout. The algorithm 3 labeled "Lock and Wipe Code" shows the DevicePolicyManager method wipeData() to reset the device to factory settings [12].

```
// Set device lock
```

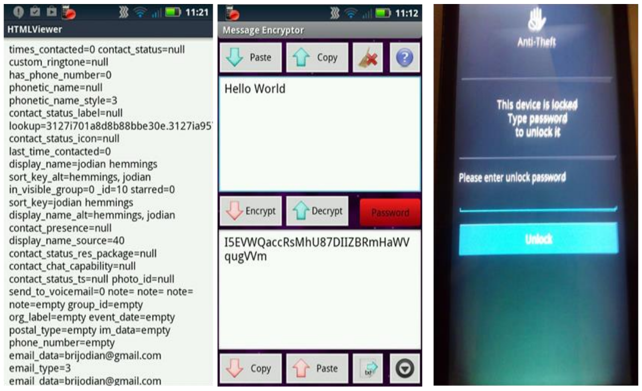
```
DevicePolicyManagermDPM;
ComponentNamemDeviceAdminSample;
long       timeMs=
1000L*Long.parseLong(mTimeout.getText().toString());
mDPM.setMaximumTimeToLock(mDeviceAdminSample,
timeMs);
DevicePolicyManager      mDPM;
mDPM.lockNow();

//Perform data wipe
DevicePolicyManager      mDPM;
mDPM.wipeData(0);
```

Algorithm 3. Lock and Wipe Code [12]

V. Experimental Results

We tested malware program to see whether malware can be removed by looking at coding. The reason we took a look at the coding is to understand how sensitive data can be protected. The methods we used in our research are back-up, encryption, and lock plus wipe data. Fig. 2 shows each method on protecting sensitive data for the mobile device. Many data were tested to see if they can be back-up, encryption, and lock plus wipe data. The results successfully show most of data can work using these three methods such as text message, phone calls, contacts, and etc. However, there are possibility better methods to deal with sensitive data.



```
times_contacted=0 contact_status=null
custom_ringtone=null
has_phone_number=0
phonetic_name=null
phonetic_name_style=3
contact_status_label=null
lookup=3127i701a8d8b88bbe30e.3127ia95
contact_status_icon=null
last_time_contacted=0
display_name=jodian hemmings
sort_key_alt=hemmings, jodian
in_visible_group=0 _id=10 starred=0
sort_key=jodian hemmings
display_name_alt=hemmings, jodian
contact_presence=null
display_name_source=40
contact_status_res_package=null
contact_chat_capability=null
contact_status_ts=null photo_id=null
send_to_voicemail=0 note= note= note=
note=empty group_id=empty
org_label=empty event_date=empty
postal_type=empty im_data=empty
phone_number=empty
email_data=brijodian@gmail.com
email_type=3
email_data=brijodian@gmail.com
```

Hello World

I5EVWQaccRsMhU87DIIZBRmHaWV
qugVVm

This device is locked
Type password
to unlock it

Please enter unlock password

Fig. 2. Methods of protect sensitive data

VI. Conclusion and Future Work

A. Conclusion

In this paper we focus on and test sensitive data which can be protected from using a wide range options from back-up files encryption text, and lock plus wipe data. By using these methods and application was successful in protecting sensitive data from getting out in the open. It should not be too many problems to deal with sensitive data on the mobile device.

B. Future Work

There are some future problems in real world mainly in the business world. Since most sensitive data is protected from API. It is easily to avoid other users to get your information. However, it is difficult to tell how sensitive data will treat in the future and how it will change the mobile device. Future work will involve more and better methods on how to protect sensitive data on the mobile device by using more applications and different algorithms. We will focus on the applications such as Cosmos for Smartphones, and Super Backup for backup and protecting sensitive data. Also we will test if sensitive data can be protecting on mobile device using the cloud system.

Acknowledgment

This work has been supported in part by US. NSF grant # DUE-1241670 and US Department of Homeland Security Scientific Leadership Award grant # 2012-ST-062-000055.

References

[1] Inc, T.C., Data Transfer, 2014, http://www.pcmag.com/encyclopedia/term/40859/data-transfer

[2] SAS Institute, Data Transfer Services: Advantages, 2014, http://support.sas.com/documentation/cdl/en/connref/61908/HTML/default/viewer.htm#a000271140.htm

[3] University of Cincinnati., and Southern Polytechnic State University, 2013, https://sites.google.com/site/mobilesecuritylabware/1-threats-of-lost-or-stolen-mobile-devices/pre-lab-activity

[4] Dimensional Research., and Check Point Software Technologies LTD, 2014, http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

[5] Ponemon Institute, 2013, http://info.watchdox.com/rs/watchdox/images/WatchDoxWhite%20PaperFINAL2.pdf

[6] A. Lazou., and G. R. Weir, "Perceived Risk and Sensitive Data on Mobile Devices", UK. University of Strathclyde Publishing., pp. 183-196, 2011

[7] Ernst, & Young, Mobile devices security: Understanding vulnerabilities and managing risks, 2012, http://www.ey.com/Publication/vwLUAssets/Mobile_Device_Security/$FILE/Mobile-security-devices_AU1070.pdf

[8] G. Hughes, and C. A. Quinsey., Mobile Device Security, 2003, http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049463.hcsp?dDocName=bok1_049463

[9] Developer Android, Android Security Overview, 2014, https://source.android.com/devices/tech/security/

[10] Developer Android, Data Backup, 2014, http://developer.android.com/guide/topics/data/backup.html

[11] University of Cincinnati., and Southern Polytechnic State University, 2013, https://sites.google.com/site/mobilesecuritylabware/3-data-location-privacy/lab-activity/cryptography/cryptography-mobile-labs/encryption-decryption/2-lab-activity/lab1

[12] Developer Android, Device Administration, 2014,http://developer.android.com/guide/topics/admin/device-admin.html