Forensics Analysis of Mobile Financial Applications Used in Myanmar

Htar Htar Lwin
Faculty of Computer Systems and Technologies,
University of Computer Studies, Yangon, Myanmar
htarhtarlwin@ucsy.edu.mm

Wai Phyo Aung
Department of Automation Control System,
Moscow Automobile and Road Construction State Technical University, Russia
myfamily46123@gmail.com

Abstract

This paper aims to analyze digital forensics of specific Android mobile financial applications such as m-banking and m-pay applications used in Myanmar. Some applications may store customer's credentials on the phone's internal memory. As sensitive data can be recovered through mobile forensic, sensitive user information is at vulnerability. Thus, we investigated on mobile financial applications to become aware of how tons touchy statistics may be recovered. Android application usually stores data in /data/data/package_name, thus analysis focuses primarily there. The selected Android applications are three mobile banking applications and five mobile money applications which are popular in Myanmar. We used popular open source forensics tools for data extraction and analysis. After analysis, finding indicates that some applications do not store data on user's device. Some applications store encrypted user credentials on device. Some applications not only store user information on device but also upload signature and photo of customer in cleartext.

Key Words- Forensics, Android mobile financial applications, sensitive data, data extraction and data analysis.

1. Introduction

In Myanmar, the ascent in mobile subscribers started after the government opened up the telecommunications segment in 2014, however implemented strong guidelines and point-of-sale (POS) installment arrangements are as yet lingering behind. [1]

Myanmar plans to increment financial inclusion from 30% in 2014 to 40% by 2020, and grown-ups with more than one product from 6% to 15%, by supporting the advancement of a full scope of reasonable, quality and successful financial services. Since the arrangement was propelled in 2013, Myanmar has seen a noteworthy increment in financial access. A report released in 2018 as a part of the Making Access Possible (MAP) program found that grown-ups with access to in any event one formal financial product expanded from 30% in 2013 to 48% in 2018, a right around 66% expansion in financial inclusion, outperforming the underlying 2020 objective of 40%. A few components have added to rising financial inclusion in Myanmar including developing Internet and mobile phone infiltration, with the mobile phone availability rate became from under 10% in 2014 to 95% in 2019. Today, Myanmar is encountering huge innovation drove changes in its banking and finance segment, with individuals step by step moving ceaselessly from money towards setting aside cash in banks and utilizing installment cards, for example, Automatic Teller Machine (ATM) cards and Myanmar Payment Union (MPU) cards. MPU is the national payment network. Additionally, the proliferation of mobile phones and Internet access is giving people access to digital financial services via mobile technology such as mobile applications and web platforms. [2]

Mobile banking is an innovation that gives banking services such as balance enquiry, money transfer, billing, and transaction statement utilizing a customer's mobile device. Mobile banking is characterized as an event when clients get to a bank's systems utilizing telephones or comparable gadgets through media transmission systems. Mobile money is an innovation that enables individuals to get, store and go through cash utilizing a cell phone. It's occasionally referred to as a 'mobile wallet' such as Wave Money, OK$, MyTel Pay, M-Pitesan and many more. Mobile money is a mainstream option in contrast to both money and banks since it's anything but easy to utilize, verify and can utilized anyplace there is a cell phone signal. The expanded utilization of cell phones in this manner, applications, has made the requirement for application security. The need to create secure

applications that ensure client's data without discarding a help is basic. The most recent Android Operating System adaptation offers Application Programming Interface (API)'s and rules for designers with the aim to advance the reception of secure practices, while most of new gadgets incorporate a segregated equipment/programming framework named Trusted Execution Environment (TEE) to verify information very still even in the event that the cell phone is established. In this way, it appears to be persuading to look at whether versatile applications safely store delicate data or permit the revelation of significant proof in a scientific examination. [3]

We made a forensic analysis on Android mobile financial applications in order to obtain sensitive information concerned with the mobile device's owner. The eight selected applications belong to the following categories: mobile banking and mobile money or mobile wallet. Various open source and commercial tools were used for forensics extraction and analysis in this study. The remainder of the paper is organized as follows. In section 2 literature review on application forensics focusing on Android Operating System was presented. In section 3 we explored the methodology used to analyze the selected financial applications. In section 4 we presented implementation and analysis results. Section 5 is about future works and in section 6 we concluded our findings with discussion.

2. Related Work

In [3], the researchers performed a forensic investigation to Android mobile applications aiming to find sensitive information of the mobile phone user. These applications were chosen based on these facts: (i) popularity on Google Play Store, (ii) handling sensitive privacy information, (iii) have not been researched by past works and (iv) free to download and install. The three chosen applications categorized by bank, mobile network carrier and public transport. The assessment of the security of the applications was performed using two techniques: code and disk analysis. In light of their discoveries they concluded that these applications neglected to protect user's sensitive data and a forensic analysis can reveal crucial and significant information from a forensics perspective.

In [4], exhausted portable entrance in Africa offers unbelievable potential to quicken money related consideration through extended determination of versatile banking by individuals at the Base of the Pyramid (BOP) on the mainland. This article gives results from an efficient audit of existing examination discoveries on the troubles, points of interest and selection elements of versatile banking at the BOP in Africa. The orderly survey, which sought after preferred reporting items for systematic reviews and meta-analyses (PRISMA) rules, perceives the going with key troubles for versatile financial dissemination at the BOP on the mainland: poor portable availability; absence of attention to versatile financial administrations; ignorance; destitution; absence of trust because of saw security dangers; lawful and administrative systems; and social components. In view of investigation of these difficulties, and of the advantages and appropriation elements additionally distinguished, the article gives recommendations on how versatile financial administrations can be all the more economically actualized to help individuals at the BOP in Africa.

In [5], they investigated how much sensitive user and app-generated data are put away on the mobile device after a user registers and banking transactions are finished. As indicated by App code examination, Bank A, Bank F, and Bank G do not implement root device detection. Although Bank D, Bank F, and Bank G have built-in encryption class, the latter is not implemented to encrypt user data. Bank A, Bank D, and Bank E implement SSL printing to check trusted certificate prior to app running with hard-coded public key for Bank A and Band D. In App repackaging analysis, when they installed their repackaged apps to catch SSL traffic and install third party certificate on the rooted device, they are able to intercept SSL traffic and capture sensitive information from Bank C, Bank D, Bank F, and Bank G (e.g. clear text PIN code, account number). Being able to use the same session ID to login to Bank D while another device running this app used in this session ID.

3. Methodology

The main purpose of this work is to determine whether activities performed through smartphone financial applications are stored on the internal memory of the device and whether these data can be recovered. The goal of this study was achieved by conducting experiments on a number of popular financial applications used in Myanmar. Forensic examinations and analyses were performed on three popular mobile banking applications and five mobile money applications.

The experiments were conducted using forensically sound approaches and under forensically acceptable conditions to fulfill a crucial rule in digital forensics, which is to preserve the integrity of the original. We followed the experiment procedure laid down from the Computer Forensics Tool Testing program guidelines established by National Institute of Standards and Technology (NIST).

We used forensically sound methods for data acquisition and data analysis which are implemented as forensics tools. These tools are open source tools and commercial tools.

3.1. Experiment environment and requirements

Prior to conducting the experiments, a forensic workstation was set up and configured. Once the forensic workstation was ready, it was isolated from the network. Table 1 and Table 2 show a list of software and hardware used to conduct the experiment:

Table 1. Software Tools

Tool	Name	Version
Root	CF-Auto-Root	
	Odin3	3.10.6
	Busy Box.apk	v1.20.1-Stericson
Forensics Acquisition	Magnetic Acquire	2.22.0.18775
	Android SDK	3.4.1
Forensics Analysis	Autopsy	4.13.0
	DB Browser for SQLite	3.11.2
	Belkasoft Evidence Center	9.9.4611

Table 2. Hardware List

Hard	Specification
Android Phone	Samsung Galaxy Note4, Model: SM-N910H, Android version: 6.0.1, Kernel version: 3.10.9-7284779
Laptop	Intel (R) Core i7 CPU, 8.0 GB RAM

3.2. Experiment procedure

The experiment procedure consisted of three stages: scenarios, logical acquisition, physical acquisition and analysis. The following sections describe each stage in details.

3.2.1. Scenarios. This stage involved conducting common user activities on financial applications on the smartphones. The applications were installed on device if they were not already integrated with the device. Applications were chosen based on their popularity in Myanmar.

For the purpose of the experiments, our own accounts were used on each service. For each application, a predefined set of activities were conducted. The activities were chosen to represent common activities, such as balance inquiry, money transfer, mobile top up, calendar remind setting, ATM/Branch Search and Bill Payment.

3.2.2. Data acquisition. Data acquisition is the way toward imaging or generally extracting data from a digital device and its fringe hardware and media. Obtaining information from a mobile phone is not as simple as a standard hard drive forensic acquisition. The accompanying focuses separate the three sorts of forensic acquisition methods for mobile phones: physical, logical, and manual. These techniques may have some cover with a few levels talked about in the mobile forensics tool leveling framework. The sum and sort of information that can be gathered will shift contingent upon the kind of acquisition technique being utilized.

In this examination, physical acquisition of mobile phones was performed utilizing mobile forensic tools and methods. Physical extraction obtains data from the device by direct access to the flash memory. The procedure makes a bit-for-bit copy of an entire file system, like the methodology taken in PC forensic examinations. A physical acquisition can obtain the entirety of the information present on a device including the erased information and access to unallocated space on most devices.

3.2.3. Analysis. The third stage included performing forensic examinations to the obtained physical image of device, to decide if the activities conducted through these applications were put away on the device's internal memory. Provided that this is true, the amount, location, and importance of the information that could be found and recovered from the physical image were determined. The examinations were conducted manually utilizing various tools to see the gained images, search for data related to the mobile financial applications, and decide how these information were put away on device.

4. Implementation and analysis

The first stage of the experiment involved installing the financial applications and conducting the predefined activities on each device. These applications were downloaded from the App Store and installed on the devices. For experiment purpose, all financial applications were updated to latest version.

Once the applications were installed on the devices, the predefined activities were conducted on each device. These activities included balance inquiry, money transfer, mobile top up, calendar remind setting, ATM/Branch Search and Bill Payment.

Similar activities were conducted on each application except some services which are not supported by applications. After conducting the financial activities on the tested phones, a physical image of the internal memory of device was acquired and analyzed for evidence of the conducted activities. The following sections describe the procedures used for the acquisition and analysis of each application. The stages of the experiment are shown in Figure 1.

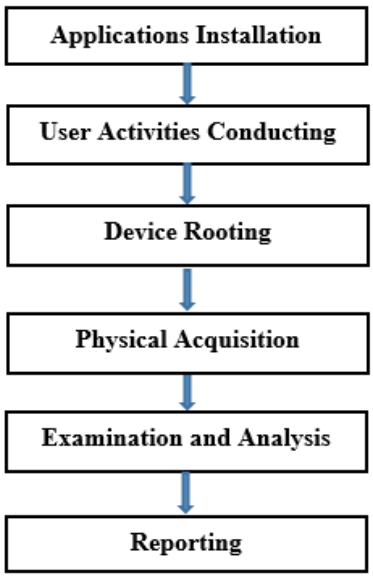

Figure 1. Stages of the experiment

4.1. Rooting

This section describes the procedure of the physical acquisition and forensic analysis of the Android phone (Samsung Galaxy Note4 – Kernel version 3.10.9-7284779). Except if the Android phone was rooted, many data files could not be accessed. Therefore, the tested Android phone was first rooted utilizing Odin3 (version 3.10.6) to upload the root-kit (CF-Auto-Root).

Installing a root-kit enables the user to gain privilege access the Android OS, permitting him/her to bypass a few restrictions that the manufacturers put on the device. A rooted Android phone enables the user to access protected directories on the system that hold user data (e.g., /data/data directory) and the entirety of the files in these directories. These data files can hold a lot of that may support an ongoing investigation.

4.2. Physical acquisition

To get physical image of the phone, we used two methods. The first one is using Linux commands 'dd' (Duplicate Data) and the next one is using Magnetic Acquire commercial tool. Extraction time depends on capacity of phone.

We used the following methods to get physical image of the tested phone. Firstly, we need to know which partition holds the data. So we used 'mount' command in first command window to take a look at the location of our desire data partition.

adb –d shell
su
mount

From output of 'mount', we knew that data is located in partition 'mmcblk0p21'. In second command window, we did TCP port forwarding in order to transfer extracted data image to the forensics work station.

adb forward tcp:8888 tcp:8888

In first command window again, we used 'dd' command to get image of data partition.

dd if=/dev/block/ mmcblk0p21 | busybox nc -l -p 8888

In second command window, we used netcat.exe to transfer acquired image file to the forensics work station. Our image file was named as dd_data.dd.

C:\netcat\nc64 127.0.0.1 8888 > dd.dd

Following is alternative to transfer image file to the forensics work station instead of TCP traffic.

dd if=/dev/block/mmcblk0p21 of=/sdcard/dd.img
bs=512 conv=notrunc, noerror,sync
adb pull /sdcard/dd.img

4.3. Examination and analysis

After extracting the image, we started analyzing the image using forensics analyzing tools. We used Autopsy, Belkasoft Evident Center and DB Browser for SQLite which are open source tools. DB Browser for SQLite is used for analyzing SQLite database.

Firstly, extracted image file was copied to the forensic workstation for forensics analysis. Application data is located at /data/data/app_package_name/. Under the folder with application package name, there are four subdirectories that held relevant data for this study: databases, files, cache and shared_prefs, which contains a number of files.

The 'databases' folder held SQLite files. Viewing each file through the SQLite Database Browser and examining its content yielded interesting results. These files hold the records that included significant information for the forensic investigator, such as the users' name, phone number, National Registration Card (NRC) number and account ID, contents of exchanged messages, Uniform Resources Locaters of uploaded photos.

The 'files' folder contained files with names that consisted of letters and numbers and that did not have any extensions. In our case, images contained within these files are screen shots of the customer profile. The 'cache' folder contains pictures that the user had used to register.

The ‘shared_prefs’ folder contains many xml file that hold a lot of information.

In our examination, the m-banking category includes three applications of major banks in Myanmar. The mobile money category comprises five applications that allow financial transactions. Analyzing results are reported as follows.

Application 1 (Bank 1): In this application, we found user ID is stored with clear text in two files of ‘Shared_prefs folder’ as follow.

string = “ht276***”
name = “USERID”

Application 2 (Bank 2): This application stored activate code length and pin key length in an xml file of ‘Shared_prefs’ folder as follow.

name = “activate_code_length”
value = “4”
name = “pin_key_length”
value = “4”

In ‘database’, we found the names of branches which the customer registered. Accont number is not mentioned in there. In our case, the customer registered two saving accounts in Lewe and Bogalayzay, and ATM card in Toungoo as follow.

title	**description**
SA-MMK-LWE	SA-MMK-LWE
SA-MMK-BKLZ	SA-MMK-BKLZ
ESA-MMK-TGU[ATM]	ESA-MMK-TGU[ATM]

We also found the name, phone number and NRC number of the customer in the ‘database’ as follow.
DAW *** +959797926*** 12/THAGANA (N)032***

Application 3 (Bank 3): In this application, we found the last updated location of the customer and last location updated time. It was stored in ‘Shared_prefs’ folder. We can locate the location of the customer in Google Map as shown in Figure 2.

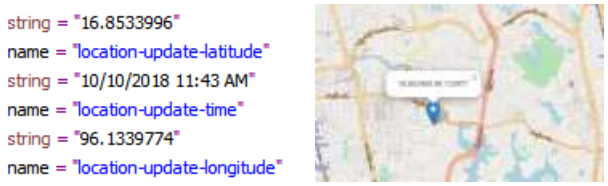

Figure 2. Location of the customer

Application 4 (Mobile Money 1): In this application, we found the balance of the customer mentioned in ‘Shared_prefs’ folder as follow.
<string nam=”Balance”>1121.00</string.

Application 5 (Mobile Money 2): No information was stored with clear text in device.

Application 6 (Mobile Money 3): This application takes care the customer information. It stored user data in encrypted database. Although we found the database, we couldn’t decrypt it. This is desirable for security purpose.

Application 7 (Mobile Money 4): This application cannot be installed on rooted device. So we couldn’t analysis it. It means this application takes care of security.

Application 8 (Mobile Money 5): This application stores the customer photo in ‘cache’ folder. In ‘files’ folder, we also found two screen shots as shown in Figure 3.

Figure 3. Customer photo in cache folder

This app stored a lot of user credential on local device and also uploaded signature and photo of customer to their server in clear text. URLs can be seen in an xml file under ‘shared_prefs’ folder as follows.

<string name="PROFILE_PIC_SIGN">https://s3-ap-southeast-1.amazonaws.com/***/Signpic00959974145***/079d4dcf-4d82-4183-9d8e-70cb8efc8339SignpicFebruary_14_2018 11_51_23 AM.jpg</string>

<string name="PROFILE_PIC">https://s3-ap-southeast-1.amazonaws.com/***/profilepic00959974145***/876a51be-6083-46d8-ad20-9ef554c67949profilepicFebruary_14_2018 11_51_23 AM.jpg</string>

We downloaded the photos using the URLs obtained from above as shown in Figure 4.

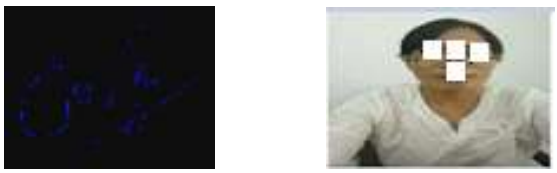

Figure 4. Signature and photo of customer

Another credential data were also found in 'shared_prefs' folder. There were a lot of information such as Name, Phone, mail, address, Balance, Location, NRC, Security Question (English and Myanmar) as follows.

<string name="number">09974145***</string>
<string name="walletbalance">8225.00</string>
<string name="SENDMONEYBANK_NRC">
12/THAGAKA(N)032***</string>
<string name="security_question_english">Who is your *** name?</string>
<string ame="MOBILENO">00959974145***</string>

Table 3 summarizes the report of our analysis for each application.

Table 3. Analysis Report

App Name	Database	Files	Cache	Shared_ prefs
App 1				User ID
App 2	Branch, name, phone, NRC			Code/key length
App 3				Location, time
App 4				Balance
App 5	No user information found			
App 6	Encrypted			
App 7	Cannot install on rooted device			
App 8		Photo	Photo	URLs

5. Future work

We analyzed non-volatile memory in this work. As a future work we will do on volatile memory where user credentials are usually stored. We will also analyze network traffic of application data in next work.

6. Discussion and Conclusions

In other countries, there are forensics investigations and analysis on financial applications used in their country. However there is no such works in Myanmar. This is the reason why we performed this work. This study focused on the recovery of artifacts and traces related to the use of applications of eight financial services used in Myanmar. The forensic analysis determined the amount, significance, and location of user credential data that could be found and retrieved from the physical image of device. The tested financial applications were three mobile banking applications and five mobile money applications. According to professional ethic, we could not mention the names of banks and payment services used in our investigation and analysis.

We used forensically strong methods and followed Computer Forensics Tool Testing program guidelines established by the National Institute of Standards and Technology. The results showed that most applications stored data in 'Shared Preferences' folder. Applications (1 to 4) stored a significant amount of valuable data that could be recovered and used by the forensic investigator. Application 5 did not keep any user information on the device. Application 6 stored data in encrypted database. Application 7 cannot be installed on rooted devices for security reason. The worse application which violence customer privacy is Application 8. It not only stored credential data such as profile photo and signature on device but also uploaded to server with clear text. Our analysis shows the nature of the credential data that could be recovered from device and their locations from physical image file. As indicated by our analysis, we can infer that these applications failed to secure user's sensitive information and a forensic analysis can uncover critical and noteworthy data from forensics perspective.

We would like to suggest financial application developers to follow privacy policies and have a great concern on security matters. Department of Consumer Affairs in Myanmar needs to take care of this issue because people from Myanmar is increasingly using mobile financial applications and they are still less awareness of security to protect their properties.

7. References

[1] Kyaw Soe Htet, "Growing mobile penetration gives Myanmar fintech a big boost", Myanmar Times, Myanmar, 21 August 2019.

[2] Thiha, "With 70% Unbanked Population Myanmar Bets on Fintech to improve Financial Inclusion", Consult-Myanmar, Myanmar, 19 November 2019.

[3] Theodoula-Ioanna Kitsaki, Anna Angelogianni, and Christoforos Ntantogian, "A Forensic Investigation of Android Mobile Applications", Proceedings of the 22nd Pan-Hellenic Conference on Informatics, Association for Computing Machinery, New York, NY, United States, November 2018. pp. 58-63.

[4] Richard Pankomera and Darelle van Greunen, "Challenges, Benefits, and Adoption Dynamics of Mobile Banking at the Base of the Pyramid (BOP) in Africa: A Systematic Review", The African Journal of Information and Communication (AJIC), LINK Centre University of the Witwatersrand (Wits), Johannesburg, South Africa, Issue 21, 23 November 2018. pp. 21-49.

[5] Rajchada Chanajitt, "Forensics Analysis of m-banking Apps on Android Platforms".