Forensic Analysis and Security Assessment in Android m-Banking Applications : A Survey

** K. Khavya*
*** N. Hema Priya*

Abstract

Data is today's gold. Preserving data is important and it is vital to secure one's private information but nowadays, attackers are stealing users' information and selling it to others for various purposes. In today's world, 57% of digital population is using its smart phones and tablets for all bank related transactions and storing its important credentials. However, majority of people prefer android mobile phones due to its low cost. However, as per recent studies, the Android mobiles are 47% prone to high risk vulnerabilities and 76% of the password credentials can be easily traced. Almost 89% of the vulnerabilities can be exploited through malwares. This survey paper investigates forensic analysis and security assessment in Android mobile banking applications and lists a few measures to safeguard the devices from malicious attacks.

Keywords : Android, credentials, digital population, malicious attacks, malwares, preserving data, private information, vulnerabilities

I. INTRODUCTION

This survey paper depicts the forensic and security assessment of Android mobile banking applications and suggests few methods to safeguard one's private information.

II. NEED FOR SECURITY

Data security is simply defined as securing one's important data. It is also called information security or electronic information security. The need for securing the data is described as follows:

a. Information which is kept confidential is an important asset.
b. The data needs to be kept safe from unauthorized access, to protect it from tampering, destroying, or disclosing to others.
c. Securing the data retains integrity.
d. It enables data availability any time.
e. Avoids security breaches and lowers the chance of hacking of information.
f. Protects user credentials, important information like banking transactions, location history, etc.

III. SECURITY ISSUES IN ANDROID OPERATING SYSTEM

Android operating system is the most widely used operating system but it is more vulnerable to attacks than any of the other mobile operating systems like IOS, blackberry, etc. The security in Android devices is compromised due to its low cost and security issues in its architecture. The security issues in Android operating systems are:

a. Poor server-side controls
b. Inefficient binary protection
c. Insecure data storage
d. Inefficient security in network and transport layer
e. Poor authentication and authorization
f. Broken cryptography
g. Untrusted inputs and improper session handlings
h. Prone to security breaches and easy to modify android packages.

Manuscript received September 3, 2019; revised September 15, 2019; accepted September 18, 2019. Date of publication October 5, 2019.
* K. Khavya is Post Graduate student wirh Department of Information Technology, PSG College of Technology, Coimbatore, Tamil Nadu - 641 004, India. (email : khavyakannappan97@gmail.com)
** N. Hema Priya is Assistant Professor, Department of Information Technology, PSG College of Technology, Coimbatore, Tamil Nadu - 641 004, India. (email : nhemapriya@gmail.com)
DOI : 10.17010/ijcs/2019/v4/i5/149457

IV. RELATED RESEARCH WORKS

A. Forensic Analysis and Security Assessment of Android m-banking Apps

In [1], the security and forensic of m-banking applications is assessed. The experiment was held on different devices such as rooted Samsung Galaxy GT-I9500 and unrooted Galaxy S4 mini GT-I9190 device in order to analyze the forensic nature of mobile banking applications. Seven Android banking applications from Thailand were selected for the analysis and the results found that few applications were insecure, some did not detect the rooted device, data encryption was poor, and it was also easier to modify the existing packages. Thus, banking applications were found to be vulnerable and on securing these applications with rooting and employing algorithms like Secure Socket Layer (SSL), Advanced Encryption Standard (AES), Cipher Block Chaining (CBC), Secure Hash Algorithm (SHA), and Public Key Cryptography Standards 5 (PKCS5) Padding, the applications could turn to be reliable and more secure.

B. Forensic Analysis of Mobile Banking Applications in Nigeria

In [2], the forensic nature of five mobile banking applications in Nigeria is analyzed. Techniques like Universal Forensic Extraction Device (UFED) Touch and Forensic Recovery of Evidence Device (FRED) were adopted. On the basis of the results obtained, it was evident that the applications did not retain users' data, such as the user credentials, bank transactions etc. The testing was carried out in Samsung GSM SGH-i747 Galaxy SIII with Android operating system. The Cellebrite UFED Touch 4.0 tool was used to check the forensic nature. The results obtained by this tool were used to decode and analyze the data and was accepted by court of law. The mobile application was tested both manually and using tool and found unreliability in banking applications and also found that the application standards was not met.

C. Evaluating the Privacy of Android Mobile Applications Under Forensic Analysis

In [3] the recovery of the user's credentials from volatile memory of Android mobiles is investigated. The experiment dealt with 13 different mobile applications including banking, ecommerce etc. and it employed free and open source forensic tools like The Sleuth Kit (TSK) for evaluation. Thus, the results proved that user credentials stored in physical memory can be recovered. Secondly, it explored the exact position where the credentials were stored in memory and critically observed the privacy of Android mobiles. This work proved the existence of patterns and credentials at memory dump which was easy for a malicious attacker to steal the information. The solution proposed was that the developers should not allow hackers to trace the information and security must be enhanced.

D. Automated Forensic Analysis of Mobile Applications on Android Devices

[4] shows how forensic analysis of mobile applications on Android devices is automated. Fordroid, a fully automated tool was developed for Android operating system. This tool performs static analysis on Android application package (APK) and develops the control flow between the components. Dependency graph for the same is obtained. The tool analyzes the location where data is stored, traverses the path, and also identifies the data base topology to avoid Structured Queried Language (SQL) injection attack. The Fordroid tool was tested with hundred applications which contained 2841 components and it discovered sensitive paths in 36 applications, identified structures of 22 data tables. The duration of the total analysis tool was 64 hours.

E. A Forensic Investigation of Android Mobile Applications

In [5], how the owner's sensitive information from a set of android mobile applications is discovered. All the applications were chosen from Google play store which was easily downloadable and contained user's security credentials. The application included the banking, public transport, and mobile carrier domains. The security analysis had two types of techniques such as disk and code analysis. The results found that the security technique failed to protect the applications and hence, the secret information of the user could be retrieved. It retrieved information like password, location history from OLA, Uber, payment history, bank account related information, Whatsapp, Viber chats. From this result, it is evident that the proper security architecture must be devised in order to safeguard the information present in the Android device.

TABLE I.

SUMMARY OF RESEARCH RELATED WORK

S.No.	TITLE	REFERENCE	DESCRIPTION	EXPERIMENTAL SETUP	TOOLS /TECHNIQUES USED	INFERENCE
A	Forensic analysis and security assessment of Android m-banking apps	[1]	Assessed the security of 7 android mobile banking applications from Thailand.	Used Samsung Galaxy GT-I9500 (Rooted) and Galaxy S4 mini GT-I9190 (Unrooted) for testing the applications	SSL, AES, CBC, SHA, PKCS5 Padding	Updated the security of the mobile banking applications using various security algorithms.
B	Forensic Analysis of mobile banking applications in Nigeria	[2]	Analyzed 5 Android mobile banking applications from Nigeria.	Used Samsung GSM SGH-i747 Galaxy SIII with Android operating system for this experiment	Universal Forensic Extraction Device (UFED), Forensic Recovery of Evidence Device (FRED), The Cellebrite UFED Touch 4.0 tool	Performed manual and automated testing and found that the application was vulnerable, application security standards were not met.
C	Evaluating the privacy of Android mobile applications under forensic analysis	[3]	Evaluated 13 different mobile applications and found recovery of secret information from volatile memory.	Used devices that run on any Android operating system	The Sleuth Kit (TSK)	Found the location of secret credentials and recovered them using patterns. Hence, proven to be highly vulnerable and insecure.
D	Automated forensic analysis of mobile applications on Android devices	[4]	Automated the forensic analysis of hundreds of mobile applications on Android devices.	Used devices that run on any Android operating system.	Fordroid tool	The tool developed found the sensitive path to trace the credentials, identified the structure of data table and can be used for forensic analysis.
E	A forensic investigation of Android mobile applications	[5]	Discovered the owner's sensitive information from a set of Android mobile applications downloaded from Google play store.	Used devices that run on any Android operating system.	Disk and code analysis	Retrieved information like password, location history from OLA, Uber, payment history, bank account related information, Whatsapp, Viber chats to ensure safety.

V. WAYS TO SECURE ANDROID MOBILES

According to recent studies, about 22 applications were removed from Google Play Store since they had many viruses and had many vulnerabilities There were a few fake banking applications too. Recently, the most common application Cam Scanner was suspended from Google Play Store since it had lot of viruses and malicious code. Some ways to secure the Android applications are given next. Few of the points noted by developers to improve security standards are:

a. Setting application specific permissions which allow applications to perform only their own tasks on the device.

b. Setting up intent filters such that when two Android devices communicate without security, the intent could be read. This is given the highest priority, the least prioritized ones could be malicious and can be avoided.

c. Securing broadcast information using BROADCAST_STICKY messages which don't reads malicious messages.

d. Applications that avoid SQL injection attacks can be built.

e. Setting file permissions is important so that the intruder cannot locate the directory or memory location where important data is stored.

f. Avoiding insecure links in mobile code.

Few points noted by users to avoid malicious attacks are as follows:

a. Avoid downloading applications from untrusted sites.
b. Read and confirm the user agreement and request before installing any third-party software.
c. Do not trust any third-party software because the pirated version may contain malicious code or viruses.
d. Regularly update the security patches available in Google Play Store.
e. Protect the device with firewall and with a trusted antivirus software.
f. Do not save any passwords or any credentials in the application
g. Use strong passwords for any application with the combination of alphanumeric values.
h. Delete browsing history and cookies often from the web browser.
I. Don't use the links or spam links from any source.
j. Delete cookies frequently and do not save the passwords in any of the web browsers. Try using virtual keyboards for entering private information.

VI. CONCLUSION

Thus, this survey paper briefs about the need for security in today's world and security leaks in the Android operation system. This survey of forensic analysis and security assessment in Android mobile banking applications found that there are many vulnerabilities present in the Android applications which are found using various forensic tools. The effects include hacking entire user information, tracking the location of the user, stealing bank related information, and use for unethical and illegal activities. Thus, the solution proposed is increasing the security of the devices and securing the information present in the Android devices.

REFERENCES

[1] R. Chanajitt, W. Viriyasitavat, and K. K. R. Choo, "Forensic analysis and security assessment of Android m-banking apps," *Australian Journal of Forensic Sciences*, *50*(1), pp. 3-19, 2018. Doi: https://doi.org/10.1080/00450618.2016.1182589aa

[2] A. Andrew, O. Oluwafemi, O., I. Idris, and M. A. Shafi'I, "Forensic analysis of mobile banking applications in Nigeria," *i-manager's Journal on Mobile Applications and Technologies*, *6*(1), pp. 9,2019. Doi:10.26634/jmt.6.1.15704

[3] C. Ntantogian, D. Apostolopoulos, G. Marinakis, and C. Xenakis, "Evaluating the privacy of Android mobile applications under forensic analysis," *Computers & Security*, *42*, pp. 66-76, 2014. Doi: https://doi.org/10.1016/j.cose.2014.01.004

[4] X. Lin, T. Chen, T. Zhu, K. Yang, and F. Wei, "Automated forensic analysis of mobile applications on Android devices," *Digital Investigation*, *26*, S59-S66, 2018. Doi: https://doi.org/10.1016/j.diin.2018.04.012

[5] T. I. Kitsaki, A. Angelogianni, C. Ntantogian, and C. Xenakis, "A forensic investigation of Android mobile applications," in *Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, pp. 58-63, 2018.

[6] "Vulnerabilities and threats in mobile applications," [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

About the Authors

K. Khavya is pursuing M.Tech. (Information Technology) from PSG college of technology, Coimbatore. She completed B. E. (Computer Science and Engineering) in 2018. Her areas of interest include cloud computing and networking.

N. Hema Priya is Assistant Professor with the Department of Information Technology, PSG College of Technology, Coimbatore. Her areas of interest include distributed systems, web technologies, computer forensics, and open source computing.