A NEW TAXONOMY OF MOBILE BANKING THREATS, ATTACKS AND USER VULNERABILITIES

Saman Mirza Abdullah[1], Bilal Ahmed[2], Musa M.Ameen[3]

[1]Koya University, Koya, Iraq
[1,2&3]Ishik University,Erbil, Iraq
[1]saman.mirza@koyauniversity.org, saman.mirza@ishik.edu.iq
[2]bilal.ahmed@ishik.edu.iq ,[3]musa.ameen@ishik.edu.iq

doi:10.23918/iec2018.29

ABSTRACT

Mobile banking becomes an interested technique within the modern bank establishments. It facilitates the transactions and day lifestyle of customers. It minimizes the impact of location and time for doing bank activities and communicate with bank servers. However, the process is not less risks from attackers and hackers, especially, user behaviors that opens and creates many vulnerabilities in this system. This work presents a new taxonomy for mobile banking attackers and threats. Through this taxonomy, this work will identify the important user vulnerabilities that attackers may misuse them for penetrating systems and steal privacy and sensitive date. The main contribution of this work is providing important suggestions for mobile banking users so that they can take them as precaution for protecting their privacy and financial aspects. The work concluded that there are many user behaviors of mobile banking leading to bring threats inside to systems. The work presents many suggestions for users so that their systems be protected from malicious activities and malwares. Many future aspects have been presented.

Keywords: Mobile Banking, Threats and Attacks, User Vulnerabilities.

1. INTRODUCTION

Mobile malwares (MM) are considered as a new and unlike threats for the mobile users. It is a growing security concern and expected to be continue as users perform sensitive actions on their smartphones. Most mobile users have no idea about different ways that thoroughly MMs (attackers and intruders) are penetrating their mobile systems without their privileges and prior knowledge. The worst case is the users consider themselves immune from such threats and they don't have enough knowledge about the rapid growth in the number and the type of mobile malwares[1] . According to a report from the McAfee Labs, 1.5 million of new incidents have been detected in the first quarter of the year 2017. With such increase, the landscape of the mobile threats and attacks are evolving in such a way that makes financial institutions (such as banks) and their customers always worry about the risks that expected from the process of online and mobile banking [2]. Therefore, it is necessary to study the feature(s) of every new mobile malware soon they have been propagated and defected systems. It is also necessary to conduct researches to find precautions for future possible threats and increase users' awareness towards such MMs.

New malwares, which are also known as the zero-day threats and attacks, are coming with different features and they follow varieties of policies and techniques. Malware analyzers need to perform reverse engineering processes on each new malware as they appear, so that they can reveal their secrets, such as the group that they belonged to. However, each malware has different policy in the design. The common point between malwares is that they misuse wide range of vulnerabilities to penetrate targeted systems. To simplify the revealing process, researchers are always grouping malwares based on the similarity among some defined features [3]. The most common grouping, is classifying malwares based on the technique(s) they are using while they penetrate mobile systems. In the other hand, researchers are grouping malwares based on the device type and the software platform. Other groupings are done based on the goals and purposes that MMs has been designed for. As an example, some malwares aimed to disclose privacy on the victim mobile, by steeling sensitive information or money, and in some cases attackers are penetrating mobile systems just for fun. At the end, breaking the defense systems of the mobile devices or the banks by bypassing the security solutions is the main target for all MMs in each group. Understanding the MM features through grouping them under different categories may help the task of mobile defense systems much easier, better analyze and evaluate malwares, and mobile users can understand their behaviors more, which will consequently, minimize the impact of malicious codes on the mobile systems[4]. this work describes the environment of the MMs in a form of some interrelated assets. Each asset covers some parts or elements that are essential in performing the mobile banking or transaction communication. This paper consist of six sections. The first section is introduction to the field of the mobile banking in the view of security. Section two is describing the fundamental framework of mobile banking and briefly states some differences between online banking and mobile banking. Section (3) is proposing a new taxonomy for the mobile vulnerabilities that misused by the MMs. Section (4) gives some examples of threats and attacks that are related to user vulnerability asset with a brief description on the policies of each MM family. Finally, some recommendations, suggestions, and advices have been explained on how to be on the safe side while enjoying using mobile banking facilities.

2. LITERATURE REVIEW

Based on the best knowledge of the author, the activities of the mobile banking have been started with SMS services, and the history of initiating such services is going back to 1999 [5]. Many countries at that time tried to employ the mobile devices in the financial and banking issues and they suggested better processor and communication facilities to cover more services. Soon developed countries encouraged the banks to provide customers with mobile services [6]. Even more, developed countries tried to include some multimedia services of the mobile in the banking issues [7]. Services, such as paying bills, payment transferring, online shopping and checking accounts were the expected and required services for the future of the mobile banking [8]. However, the security concerns became an important problem within the infrastructure of the mobile banking. Therefore, many works developed some security frameworks and others argued some security assessment processes [9, 10]. Within these frameworks and assessments, the mobile users and their behaviors were the most important security questions. User vulnerabilities still important in many recent works as they become the main vulnerabilities for the mobile attackers' penetration, beside system vulnerabilities. one of the recent works addressed an assessment of the mobile vulnerabilities within Android and iPhone OS[11]. The work argued some vulnerabilities of the mobile banking applications that released and certified by the banks. The work showed that some banks are using simple HTTP protocol without concerning to the security issues that related to the man in the middle attack. The work just focused on the vulnerabilities of those applications and forgot to analyze user vulnerabilities that also misused by attackers work in the middle way. Many works focused on securing the communication channels between customers and bank servers. In those works, stronger encryption methods are proposed [12]. However, the weak point of the mobile banking systems are the users themselves. Within any downloading of games or unknown applications, a Trojan malware could insert itself to the system and make itself active for opening a back door for attackers. The possibility of downloading Trojan is in increase as the work [13] reported that number of Trojan infected apps in the mobile application sources, such as Google Play Store and iOS app store, are increased unpredictably.

Another part that more concerned the security of the mobile banking systems are the security of the physical storage of data in bank sides. One of the most important attacks that related to the server security is SQL injection. Such attacks inject a malicious code inside the database of the bank and do activities they need. Many authors worked on that problem and they designed SQL Injection detection systems [14]. Although mobile users may not have impact on those database security, employers in the bank whom working on such dataset may be misused by attackers.

It seemed that all framework of the mobile banking needed to be securable. Moreover, a great part of the security breaching is the responsibility of the user vulnerability. Therefore, this work presents a new taxonomy of the mobile banking threats and attacks and discusses the impact of user vulnerabilities on each part.

3. SECURTIY PERSPECTIVES OF MOBILE BANKING

Today, banks in most developed countries offer mobile banking services for their customers. It is putting essential banking services as a mobile applications and let users (bank customers) to use them remotely either from their smartphones or tablets. The most common services that provided through mobile banking applications are bill payments, fund transferring, checking transactions and balance, and sending some security alerts or reminders [15]. The most important part of the mobile bank services is to ensure users that their communication with the bank is been transferred via a secure and protected channel. This will increase the trust of mobile bank users and their acceptance to the system, which is not really an easy matter as shown in some statistical figures. Researches been conducted for specific countries and bank. A paper found that 69% of German banks are providing m-banking services, and it showed that 79% of the people are using m-banking. Among all users and nonusers of mobile banking, only 77% of them are still worrying about the security of m-banking [16]. Therefore, securing the systems of the m-banking is becoming a very essential issue, however, it is not easy. the typical infrastructure of any m-banking is shown in Figure-1 [17] . The core idea is establishing a communication channel with the core bank systems using mobile communication system, Internet networks, and mobile banking servers. In the figure, the part of the mobile communication systems, implicitly, comes within the Internet network. Another implicit part of the m-banking systems is the users, or the bank customers that are performing banking transactions through their mobile devices.

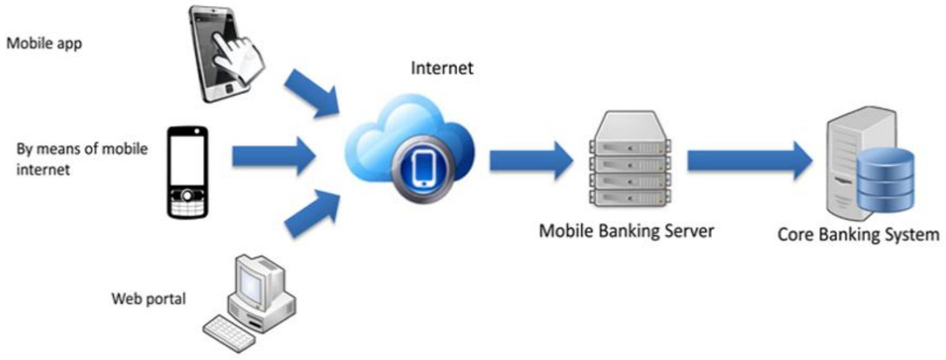

FIGURE 1. Typical Mobile Banking Systems

At each stage or part of the m-banking infrastructure, a special level of security defense systems are required and many security challenges will be there. According to this scenario, this work has divided the different parts of the m-banking systems, specifically from a security perspective, into four groups or assets; mobile user behaviors, mobile applications, hardware, and the mobile or the Internet network systems. Classifying the whole m-banking systems into four assets from a security perspective have been done according to the type and the policy of the attacks penetrating the m-banking systems. At each part (asset), special types of threats are misusing the vulnerabilities that could be found only in the corresponding part. To provide a full immune m-banking service, special defense systems should be designed. The proposed defense systems firstly need to know and analyze all threats and attacks at each part. Secondly, the defense system should be aware about the policies and vulnerabilities that might be misused by attackers and various threats to penetrate the corresponding part. Then, designing a fully protective system for securing m-banking system can be achieved [4]. next section explains in detail about the taxonomy of the MMs in the viewpoint of the above mentioned assets.

4. NEW TAXONOMY OF MM

The new MM taxonomy proposed in this work is considering each part of the mobile banking system as an asset, as shown in Figure 2.

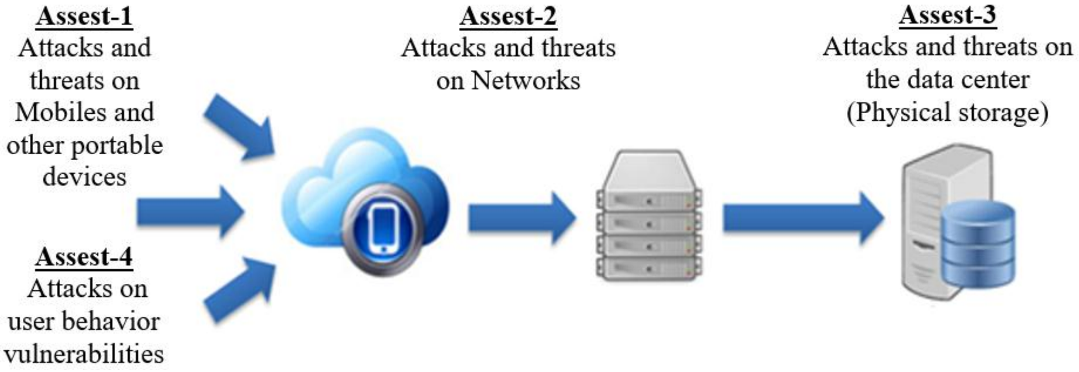
Assest-1
Attacks and threats on Mobiles and other portable devices
Assest-2
Attacks and threats on Networks
Assest-3
Attacks and threats on the data center (Physical storage)
Assest-4
Attacks on user behavior vulnerabilities

FIGURE 2. The main assets of the mobile banking systems

As shown in Figure 2, no part of mobile banking system is free from threats and attacks. Every single piece of the mobile banking system, from the device to the server, either physical or software are all entitled to different attacks through the vulnerabilities and flaws found in each asset. Table 1 lists the names of most known attack types under four different categories or assets. The mentioned attacks at each level can be considered as serious threats on mobile bank systems and customers.

TABLE 1.

The New Taxonomy of Mobile Banking Threats and Attacks [1, 16, 18]

Assets-1 Devices	Assests-2 Network	Assets-3 Physical Storage	Assets-4 User Vulnerabilities
Phishing	Wi-Fi (No Encryption or Weak Encryption)	Platform Vulnerabilities	No Passcode/Weak Passcode
Framing	Rogue Access Point	Server Misconfiguration	iOS Jailbreak
Click Jacking	Packet Sniffing	Cross-Site Scripting (XSS)	Android Rooting
Man-in-the-Middle (MITM)	Man-in-the-Middle (MITM)	Cross-Site Request Forgery (CSRF)	Password and Data Accessibility
Buffer Overflow	Session Hacking	Weak Input Validation	User-Initiated Code
Data Caching	DNS (Domain Name Systems) poisoning	Brute Force Attacks SQL Injection	Sensitive Data Storage
No Encryption/Weak Encryption	SSL (Secure Sockets Layers)	Privilege Escalation	User skills and experience about security
Baseband Attack	Fake SSL certificate	Data Dumping	Phishing
SMIshing		OS Command Execution	
Improper SSL Validation			
Dynamic Runtime Injection			
Escalated privileges			

One of the best ideas of classifying mobile banking threats and vulnerabilities is to provide solutions that come fit with each asset. Therefore, this work will provide security solution(s) for each threats and attacks that more related to the user vulnerabilities.

5. USER RELATED ATTACKS IN MOBILE BANKING

Categorizing mobile banking threats makes the process of finding security solutions easier for security specialists and researchers. It divides the task of a fully immune mobile banking system on individual defense and protective systems. As shown in Table-1, assets of mobile banking are divided into four parts. Each part covers a group of attacks and threats, and of course, each individual attack has its own policy and technique to penetrate systems. In Table-2, most attacks that related to the user vulnerabilities have been described shortly. Next section, important suggestions for mobile banking users will be given.

TABLE 2.

Attacks, their policies and some solutions [1-4, 19]

Attacks and Threats	Definition and Policies
Phishing	It uses legitimate personation for stealing privacy or login credential information. It dose that through urgent emails to target victims.
Framing	It inserts some fake frames in a legitimate website for a bank or company for collecting privacy or login credential information.
Click Jacking	It is exactly like framing, but the attacker will put an invisible button on some interested button. The malicious activities will be done when a user clicked the interested bottom and it doesn't has idea that there is a hidden bottom
Man-in-the-Middle (MITM)	This type of hacking is done through a lot of malicious ways. The most popular ways are the email hijacking and WiFi eavesdropping
Buffer Overflow	Attackers try to write into some temporary memory locations more than they can hold.
Data Caching	This attack has some similarity with buffer overflow. They try to over follow the cache memory, breaking AES keys based on some timing or power consumptions, or sometime through provoking the eviction of recently accessed data
Baseband Attack	This attack can penetrate both Android and iOS based devices. It is usually attacking a device over the air. It starts through operating an adversary on a rough based station that somehow close enough to communicate with target device. It has ability to locate the position of the user and can break the privacy that stored on the device.
SMiShing	SMiShing is shorten of SMS Phishing. It sends an interested SMS thoroughly a user will be motivated to download Trojan Horse, virus, or other type of malwares.
Improper SSL Validation	It is very important to secure the communication between the bank and the client. This process done using a valid Secure Sockets Layer (SSL), which is standard security technology, and it depends on encryption. Using improper SSL makes the job of attacker easy to listen to these communications and steal privacies.
Dynamic Runtime Injection	It is the process of calling and controlling a library that permit a malicious code to be injected or replaced in a mobile device. It starts with clicking an unknown email then it controls the SSL communication process at run time.
Unintended permission	Many permission requests will be accepted set by applications and mobile users are accepting them. These permissions, after they allowed, they change the status of many private objects to public among applications.
Improper Certificate Validation	It comes with using or installing invalid, cracked, illegal software and applications. The attacker will try to overcome the SSL protocol and conduct an illegal communication with client.
Escalated Privileges	Is gaining the access to many parts of the mobile through different way, which one of them is rooting the devices
No Passcode/Weak Passcode	Passcode used to lock mobile devices and protect it from an authorized person.
OS Jailbreak and Rooting	These to apps used by mobile users (iPhone and Android) to get apps free.
Password and Data Accessibility	The most common way for protecting data is avoiding accessibility through using passwords.
User's Initiated Code	Quick Response (QR) Code becomes very come among mobile users.
Sensitive Data Storage	Sensitive data should be kept in a very secure storage (Strong password and Encryption algorithm). Attackers typically don't break crypto directly.
User skills and experience about security	Most attackers are penetrating systems because of unawareness of the users to the mobile devices and apps.

6. SUGGESTIONS FOR MOBILE BANKING USERS

The pillars' responsibility of security framework for any mobile banking system should be includes Bank Strategic IT Policy, IT technician beside the behaviors of the bank customers themselves. All involved parties in the system need to cooperate to have a safeguard zone and to minimize the risk of threats and attacks penetrations. In this section, this work provides the role of users in keeping the vulnerabilities as close as possible and increase their awareness about the possible open gates that thoroughly attackers may penetrating their systems. Although this work classified the attacks in the process of mobile banking into four assets (Figure 1), attacks due to user behaviors and vulnerabilities are more focused. In general, user vulnerabilities come in the first and fourth assets. While asset number two and three are more about the mobile communication and bank establishments. To avoid vulnerabilities in any mobile banking system, users should strongly consider the following recommendations and suggestions:

1. Users should not open any urgent notes or emails that originated by their banks, especially, if the email or note asks private information. Banks never send or ask privacies through mobiles or in urgent ways. Such messages or emails have high probability of containing phishing.
2. Many emails or note senders will ask customers some privacy information through filling sort of forms sent through a link. Once the link opened customers will see some frames added to the opened website. Or, the link will direct customers to a fake page where looks almost like the correspondence bank website. Any information given to such frames and websites will put users in the risk of stealing their privacy and financial information through a type of attack known as the man in the middle. Through such links the attacker can control the communication of customers and the corresponding banks.
3. Many mobile users are interested in downloading free apps and software through the process of rooting or jailbreaking their device. Such rooting processes will bypass the security and the permission controls that protecting the Kernel root of the mobile devices, thus the device becomes open for attackers to access any private and sensitive data that kept inside the mobile. Of course, stealing the credit card numbers and QR codes will be one of the

revealed data. Moreover, buffer over follow and data catching attacks will get advantages from jailbreaking mobiles for making devices working slowly and have bad respond.

4. Many attackers are working within the asset three, which is related to network part. However, users of mobile banking are also involving in this process of penetration. It is the role of the mobile users to give permissions to an app to escalate their privileges. Dynamic runtime injection attack is the most effective attacks that gets the advantages form the user permission. Users should be aware about the type of the access that an app is asking for controlling Kernel or other applications. For example, a game asking you to access your contact number list or read your SMS lists. Users should ask themselves about the relation between this app and contact list. If users couldn’t find any relation the requested access should be blocked.
5. SMS is the main gate of attackers toward the mobile devices in mobile banking apps.
    a. A type of phishing called SMIshing is the most popular attack that thoroughly many Trojans and worms are penetrating systems. Users should not open SMS messages from unknown or suspicious senders or should not click on any link that comes through an SMS from strangers.
    b. Another type of attack is called DDoS attack. This attack may come inside the mobile devices through opening and clicking a link inside an SMS came from stranger destination. The attack will control the communication or the SSL validation between the mobile and the bank server.
6. The fist access control type of any mobile devises is the passcode. All type of passcode should be strong and undetectable. When a mobile become physically with an attacker the first trial that the attacker will do is hacking the passcode. Mobiles that supporting bioinformatics access are much safer than others. There are many attackers use the track of keystrokes as type of breaking the access defense process. If the user depend on QR access, it should be aware that his/her QR could be extracted somewhere
7. Storage places of sensitive data should be strongly protected through a very powerful password. There are many recommendations about the formulation

of the passwords. Users should have knowledge about distinguishing weak passwords from strong one.

7. CONCLUSION

This work concluded that responsibility for building a strong security framework of any mobile banking is not on the bank or just on the customer, it a pair responsibility. It is very important for users to understand their vulnerabilities and avoid them. To be more understandable, this work classified the attacks in the process of mobile banking into four categories. The work focuses more on the user vulnerabilities, as it is relevant to all categories. This work found that user behavior couldn’t be separated from the main framework of mobile banking security. Moreover, the only way for educating mobile users is through publishing some suggestions, which are not easy to be well understood as they required security skills and experiences. For the future work, this work preferred and designing a security framework for mobile banking that put all assets together in one frame. It will be great if some intelligent techniques as detection systems for each asset will be designed, and it will be better if an intelligent mobile banking systems could be presented in the viewpoint of smart cities, such as using the concept of Internet of Thing (IoT).

REFERENCES

[1] P. Y an and Z. Yan, "A survey on dynamic mobile malware detection," Software Quality Journal, pp. 1-29, 2017.

[2] MaCafee, "McAfeeLabsThreatsReport, "https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf2017 2017.

[3] F. Martinelli, F. Marulli, and F. Mercaldo, "Evaluating Convolutional NeuralNetwork for Effective Mobile Malware Detection," Procedia Computer Science, vol. 112, pp. 2372-2381, 2017.

[4] R. Unuchek and V. Chebyshev, "Mobile malware evolution: 2013," AO Kapersky Lab, 2014.

[5] D. irch, "Banking on the Move The internet isn’t the only new digital channel," 1999.

[6] B. Must and K. Ludewig, "Mobile money: cell phone banking in developing countries," Policy Matters Journal, vol. 7, pp. 27-33, 2010.

[7] M. H. Hasan and A. Khalid, "Development of Multimedia Messaging Service (MMS)-based receipt system for mobile banking," in Information Technology (ITSim), 2010 International Symposium in, 2010, pp. 1-6.

[8] N. Mallat, M. Rossi, and V. K. Tuunainen, "Mobile banking services," Communications of the ACM, vol. 47, pp. 42-46, 2004.

[9] D. Weerasinghe, V. Rakocevic, and M. Rajarajan, "Security framework for mobile banking," in Trustworthy Ubiquitous Computing, ed: Springer, 2012, pp. 207-225.

[10] L. Nosrati and A. M. Bidgoli, "Security assessment of mobile-banking," in Computing and Communication (IEMCON), 2015 International Conference and Workshop on, 2015, pp. 1-5.

[11] S. Bojjagani and V. Sastry, "VAPTAi: A Threat Model for Vulnerability Assessment and Penetration Testing of Android and iOS Mobile Banking Apps," in Collaboration and Internet Computing (CIC), 2017 IEEE 3rd International Conference on, 2017, pp. 77-86.

[12] H. N. Huxham, "Mobile banking system with cryptographic expansion device," ed: Google Patents, 2017.

[13] S. K. Shukla, "Trust and Security Must Become a Primary Design Concern in Embedded Computing," ACM Transactions on Embedded Computing Systems (TECS), vol. 17, p. 1, 2018.

[14] N. Shah, "Securing Database Users from the Threat of SQL Injection Attacks," 2017.

[15] K. Kavitha, "Mobile Banking Supervising System-Issues, Challenges and Suggestions to improve Mobile Banking Services," Advances in Computer Science: an International Journal, vol. 4, pp. 65-67, 2015.

[16] C.-. Insights, "Mobile Banking Security: Challenges, Solutions," USA, Report2015.

[17] mpss. (2018). Myanmar Paymnet Solution Services.

[18] A. Feizollah, N. B. Anuar, R. Salleh, and A. W. A. Wahab, "A review on feature selection in mobile malware detection," Digital Investigation, vol. 13, pp. 22-37, 2015.

[19] S. M. A. Ghani, M. F. Abdollah, R. Yusof, and M. Z. Mas’ud, "Recognizing API Features for Malware Detection Using Static Analysis," Journal of Wireless Networking and Communications, vol. 5, pp. 6-12, 2015.