Issues and Security Measures of Mobile Banking Apps

Sameer Hayikader [*], Farah Nurafiqah Hanis binti Abd Hadi [**], Jamaludin Ibrahim[***]

[*] sameer797.kader@gmail.com, [**] farah.nurafiqahhanis@yahoo.com, [***] jamal55@gmail.com

Department of Information Systems, Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia

Abstract- Mobile apps is a used to designate the act or process by which application software is developed for handheld devices, such as personal digital assistants or mobile phones. These applications can be pre-installed on phones during manufacturing platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an "application-like" experience within a Web browser. However there are some cases where the mobile internet banking apps occurred some problems that might cause loss of money. Therefore, In this paper we will examine issues on the architecture, and some security issues of mobile internet banking apps. And then we will explore some security measuras to deal with the associated security challenges.

Index Terms- Mobile banking apps, security, meaures

I. INTRODUCTION

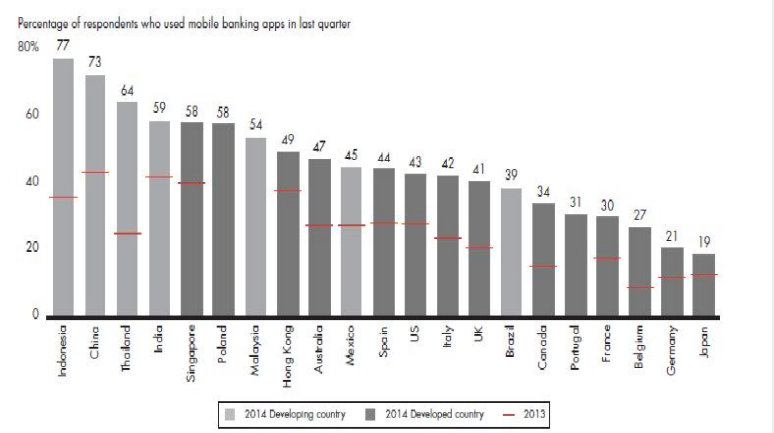
Financial services and transactions through mobile device are called Mobile banking. Mobile banking security will include data transmission which is important to secure the data of the users to prevent the hacker to attack and steal the data. Authentication is also important which is only allowed authorized users to have access to the data. Also avoiding complex authorization is crucial in order to make quickly for the data [1].

The protocol translation and compression of contents from mobile devices are working through online banking architecture. The architecture of online banking can be at variance by subject on outline by the panel of bank bodies; in-house services and third parties hosted services [2][3]. These online banking architectures were applied into mobile internet banking application since the bank has application servers that involve e-mail server, website server and others. Then the router will direct the transaction request by the user into those application servers. But the process for each architecture will be differ.

Recently, the communication of internet banking application in smartphone will be asynchronous through back-end system. To work on back-end system, Service Oriented Architecture (SOA) is needed for all application components provide services to other components by the use of a communications protocol, usually an Internet. It compromises bank bodies with option in involving old application with the current internet banking [4]. It is due to the advanced technology and wireless technology users are more convenience to do their financial services through mobile. Mobile banking based on WAP (Wireless Application Protocol) and SMS (Short Message Service) is popular [5]. Through SMS the customers can know the details about their account balance.

However, there still many security problems when making transaction through SMS. The data are not secure while transmitting through SMS because sending and receiving SMS have no encryption technique. Using mobile devices to access to the internet through WAP (Wireless Application Protocol) is insecure as WAP is vulnerable to hacker's attacks due to its protocol translation and compression of contents which is insecure. Thus, Intrusion Detection System (IDS) is introduced into internet banking security system for safety on online transaction processing [2][6]. Basically, IDS is used to review, analyze and record report of the system and network activities. Although IDS is not an obligatory in online banking architecture but by placing IDS might help in detecting any occurrence sabotage.

II. THE USAGE OF MOBILE BANKING APPS



Source: Bain/Research Now NPS survey , 2014

The number of mobile banking apps users are increasing as shonw in the statistics above from Bain / Research survey in 2014, which Indonesia on the top following by China and Thailand. As we can see from the statistics more user in asia pacific use mobile banking apps. That shows us how people in this pacific are more conviniece with mobile banking apps although research has shown that hacking or malware has been the predominant method of Credit Card data breaches that occurred from 2005 to 2014 [7]

III. MOBILE BANKING ARCHITECURE

Client, application server and database are the major components of basic architecture of online banking system. For instance, customer send a request in viewing their balance through online banking, an application server will be responsible in monitoring server script and check for the ODBC bond for mapping to the correct database while the database will stored the latest activity of the client and bank data [8]. Literally, with support from iOS, Android, Windows, etc platform online banking application can be integrated with retail banking system. The interfaces are customizing user experience, high secure and scalable [9].

There are various technology interfaces that directly connect customers banking services. Figure 1 illustrates layered framework on how customer communicate with banking services via a set of networks and gateways that route requests to channel specific applications and services. SOA services and business processes of integration layer are important component that channel specific applications leverage the shared core banking functions [10] .

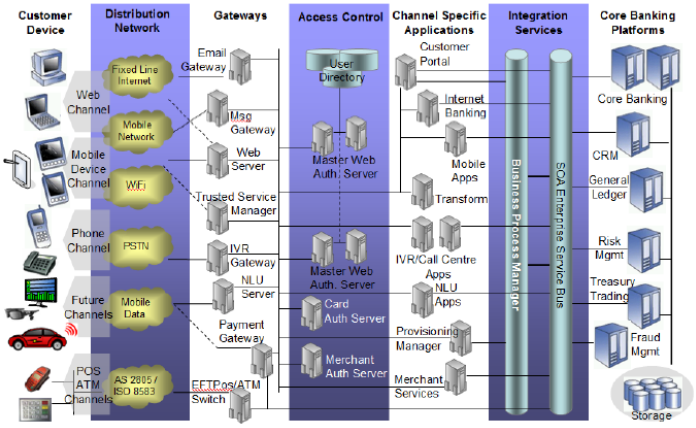


Figure 1: Various architures on Multi-Channel Banking [10]

IV. SECURITY AND THREATS IN MOBILE BANKING APPS

- **Issue with WAP (Wireless Application Protocol)**

New technology has made people to access to the internet much easier. Users connect the mobile devices to WAP and GPRS to have access to a wide range of banking services like transferring money from one account to another account, making payments for purchasing items. Security and convenience are the key factors for the growth of mobile banking and mobile commerce [11].

WAP allows more functionality of internet banking. There has been process on encryption for secure data transmission between bank and customers but when using mobile devices in banking services the encryption process is weaken for the protection of sensitive data between bank and customer because to secure any data it requires more powerful devices and high storage capacity. In internet banking there are powerful computer systems and complex encryption process to ensure the security. However, Mobile devices have low computational capacity which makes it unable to apply complex cryptographic system [12]. End to end security through WAP is crucial but it's not easy to provide it as the data is not encrypted at gateway during the switching of protocol process [13]. When using mobile devices in making services online information will be accessible on gateway which will make it possible for the attacker to access the information [14].

- **Virus Attacks in mobile banking apps**

There are different types of computer viruses, internet malicious program and TrojanZeus Trojan targeted mobile bank users. Virus Zitmo has been commonly used by attackers to defect SMS banking. As well as virus Zeus is commonly used by the hackers to access to mobile transaction authentication number or password [15].

- **Speng malware:**

According to Kaspersky Lab it discovered that a breed of malware targeting mobile devices called Svpeng. The malware, which targets Android devices, looks for specific mobile banking apps on the phone, then locks the phone and demands money to unlock it. Speng breaks into a mobile device through a social engineering campaign using text messages. Once it's wormed its way into a device, the malware looks for apps from a specific set of financial institutions. The Trojan also contains code that could be used for file encryption; it could, therefore, encrypt files stored on the mobile device and demand money to unencrypt them [16].

The threats of mobile banking apps security include Trojans, root kits and viruses. There are some well affected malware on mobile bank apps include Zitmo, Perkel/Hesperbot, Wrob, Bankum, ZertSecurity, DroidDream and Keyloggers. Cyber criminals have been refining these malware to target mobile devices for access to bank accounts and make them more resilient to security defenses. Below are some common malware that affect mobile banking apps. .(Webroot, 2014; Shih et al., 2008) [17].

- Zitmo – attack and steals TAN codes which is sent by banks in text messages to the customer.
- Perkel/Hesperbot – JavaScript injection (JS) is used in this case on PC to request mobile number and then delivers Trojan using SMS. Trojan poses as a security app.
- Wrob – poses as the Google Play app and replaces installed banking apps with Trojan clones » Bankum – replaces legitimate versions of banking apps with fake ones.

- ZertSecurity – impersonates bank login, steals credentials Rootkits.
- DroidDream – uses rageagainstthecage exploit to root the device, steal data, install additional apps, execute remote commands
- Keyloggers – pose as third party keyboards that send keystroke and contextual information.

V. THE PROBLEM OF THE INHERENT SECURITY RISK INVOLVED IN TRANSFERRING INFORMATION OVER THE NETWORK

There are two components related to this problem. First, personal identification integrity and the second problem is message integrity. Digital signature is commonly used in mobile banking which refers to the identification integrity to know where the message is originating. The message integrity involved information and details of the message in order to establish the message is received and no third party to open, change the contents. Zhang and Lee have stated that, transferring information over the network seems to cause a lot of concern for both sender and receiver [18]. The sender risks is theft or misuse of their personnel information such as account and bank details, the receiver risks repudiation of the transaction and resultant nonpayment.

There are different security problem can happen one of major security breach in mobile banking is transferring the user's information from one mobile network to another [19]. In this case, all encrypted data needs to be decrypted for transparency. In mobile banking, when mobile devices make requests to web pages of a network server, some initial process will be made which means the requests arise from the originating Wireless Transport Security Layer (WTSL) protocol. And then the requests will be translated at Wireless Application Protocol (WAP) gateway. Once the requests have been translated they are sent to the standard

Session Security Layer (SSL) protocol of the destination network. And finally the translated information will be received by the Hyper Text Transfer Protocol (HTTP) modules in the new network in order for the requests to be processed. As the result the data will be decrypted and re-encrypted when translating a protocol from one to another and this process known as "WAP Gap" during this process it will be easy for an attacker to gain access to the mobile network, which will result to capturing the data when it is decrypted can compromise the security of the session.

Data is secured using encryption technology in the mobile environment. According to Ghosh, it has already been proven that the technology is vulnerable to attacks [20]. Hackers have broken some of the existing algorithms for encryption. As the result, technology is not completely secured. On the other hand, there is no international regulatory framework available to ensure and solve security related problems. As technology is advanced and more people are advance as well , no individual organization can guarantee security to consumers and people need to be aware of security in using mobile banking innovation [3].

VI. VULENABILITIES IN MOBILE BANKING APPLICATION

According to Ariel Sanchez security vulnerabilities in mobile banking applications which could be used by hackers to steal money from customers. Sanchez said that some banks have vulnerabilities identified as "70% of the applications did not use alternative authentication solutions, such as multi-factor authentication, which could improve the security aspect and to mitigate some risk which could lead to attacks to information.

Mobile banking apps which commonly used by users using their smart phones and tablets, have caused security concern for worldwide in terms of transaction. As the result The European Central Bank proposed the creation of a raft of new mobile payments security standards that payment service providers (PSPs) such as banks and 'mobile payment solution providers' (MPSPs) should have to adhere to in November last year [21].

VII. TWO FACTOR AUTHINTICATION PROBLEM

Two-factor authentication is not always used when conducting sensitive transactions on mobile devices. According to studies, consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices. Using static passwords for authentication has security drawbacks: passwords can be guessed, forgotten, written down and stolen, or eavesdropped. Two-factor authentication generally provides a higher level of security than traditional passwords and PINs, and this higher level may be important for sensitive transactions. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" something you know, something you have, or something you are before being granted access. Mobile devices can be used as a second factor in some two-factor authentication schemes. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Without two-factor authentication, increased risk exists that unauthorized users could gain access to sensitive information and misuse mobile devices [22].

VIII. MOBILE BANKING APPS ON RISKS BY HACKERS

Research has shown that hacking or malware has been the predominant method of Credit Card data breaches that occurred from 2005 to 2014 [23]

• Most apps have been hacked. The research of top fnancial apps reveals that: – 95% of Android apps have been hacked – 70% of iOS apps have been hacked.

• The research also reveals a growing trend of financial app hacking – Android app hacking increased from 76% to 95%, from 2013 to 2014 – iOS app hacking increased from 36% to 70%, from 2013 to 2014.

IX. COMPARISON BETWEEN iOS & ANDROID APPS

	iOS	Android
Distributed level	iOS apps are distributed only through the Apple App Store	primarily distributed through the Google Android Market, are legally distributed by other means
Third party	No third-party software APIs.	Android developers are free to add to the API, use third-party APIs.
Permission	iOS, Android applications can share resources and data through the declaration of permissions.	apps can access only its Unique User ID (UID) tagged data unless granted extra-sandbox permissions to other data sources.
Level of security	Apple's iOS model provides greater security out-of-the-box given Apple's total control over the device.	Google's Android provides greater potential for application-level security due to the extensive and open nature of the SDK.

Table 1: Differences between iOS & Android [24]

X. NATIONAL BANK OF ARIZONA

Some banks describe their privacy policy in using mobile banking apps to the customer to provide them a clear describtion about the privacy policy. Good example of describing privacy policy to the customer is National bank of Araizona which has set up apps privacy policy and described what information that can be shared.

Mobile apps stores personal information once the customer starts using the apps such as name and other activities. Contact information will be also stored and won't be shared with service provider and also will not be used for markting and profiling. Customer's financial information will be shared and known to every one in the bank as well as the service provider and the legal procces. The apps will track the customer's location and also the activities that have been done by the customers will be known to the bank such as the page the customer has visited on the apps and the email that has been sent to the company. However , the customer has no 100% privay when using mobile banking as some information is not encrypted and visiable to the third party. [25]

XI. MOBILE BANKING APP

I. VENMO APP

Venmo is mobile baking apps which has prominently advertised its security on its website. Venmo use encryption tool to encrypt all connections by applying SSL and "uses bank-grade security systems and data encryption to protect the information and to prevent the loss or any unauthorized transactions or access to your personal or financial information.

How private are Venmo transactions?

Venmo apps set its defult setting as online sharing to the public via social networking. Usualy the transaction information such as the name of the sender and the recipient will be mentioned and its taken from linked Twitter or Facebook accounts and other social networking, other information in the transaction such as the date of the transaction is shared to the public if the users do not read the privacy policy and do not change the defult setting [26].

II. STARBUCK APP

Starbuck mobile application is a convenient pay for purchases, earn stars, redeem rewards with My Starbuck rewards and much more. The mobile banking application can be downloaded by iPhone and Android smartphone. Ordering any drinks is faster without waiting line. Besides, customer can leave a tips for barista digitally. The app itself lets the customer pay at checkout with mobile phone. The customer can reload Starbuck gift card by inevitably drawing fund from his bank account or credit card.

How secure are Starbuck mobile application transactions?

Starbuck apps set pay at checkout with mobile phone. Usually customer will put amount of money into the Starbuck app and can reload Starbuck gift card. Then the customer will be notify about his transaction by a message or an email. It makes more convenient and faster in paying the drink, however, the level of security of Starbuck security system is just moderate. Several case happen when an intruder sneak into customer Starbuck's account online. One of the case happen to a customer who brought a drink at Starbuck in Sugar Land, Texas. He keep on getting notification from Paypal in mentioning he did reload into his Starbuck card. Besides, he got several email from Starbuck as well. From the case it shows that Starbuck did not ask confirmation of transaction to the customer before doing so [27].

III. BANK OF CHINA (HONG KONG)

Similar like Maybank, Bank of China (Hong Kong) or known as BOCHK has provides the personal mobile banking application for general banking and investment services. The application can be used throughout the world because user can use their smartphone in handling their finance anytime anywhere. The updated version of the application can be done whenever wherever a new update is available.

How risky are Bank of China mobile banking application?

There might be potential risk with man in the middle attacks since BOCHK mobile banking application do makes the entire process in HTTP. Not only general banking services can be done by using this application, there is a feature that make inquiries for electronic transaction records, opening and closing various electronic payment transaction functions and setting the transaction limits. By doing so, social engineering could be devastating because of the manipulating the confidence of this application [28].

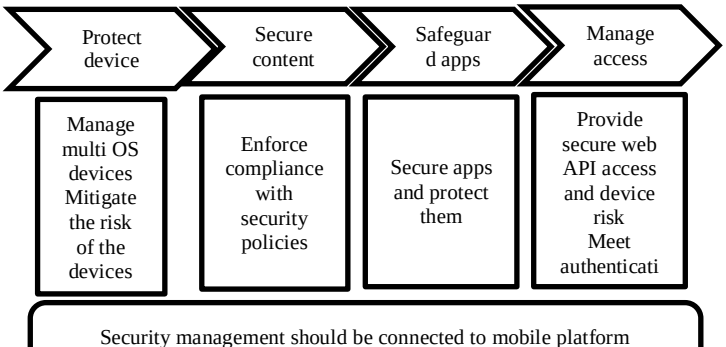
XII. SECURITY MEASURES

iOS and Android implement 5 security measures according to [29]:

- Traditional Access Control: seeks to protect devices using techniques such as passwordsand idle-time screen locking.
- Application Provenance: each application is stamped with the identity of its author andthen made tamper resistant (using a digital signature). This enables a user to decidewhether or not to use an application based on the identity of its author.
- Encryption: seeks to conceal data at rest on the device to address device loss or theft.
- Isolation: attempt to limit an applications ability to access the sensitive data or systemson a device.
- Permissions-Based Access Control: grants a set of permissions to each application andthen limits each application to accessing device data/systems that are within the scopeof those permissions, blocking the applications if they attempt to perform actions thatexceed these permissions.

XIII. CONTRIBUTION

In this paper, we have exmined the security issues on mobile banking apps and we found that malware and hacking are the threats for many people when using mobile banking apps. Therefore, in this paper we have come out with a framework which can improve mobile banking apps security. The framework is basically contains four main components which are protect device , secure content , safeguard application , and manage access. We have proposed to have security , Configuration and vulnerability management for each mobile apps platform to reudue the vulnerability and improve the security .



XIV. CONCLUSION

In this paper , we have discussed some security issues that related to mobile banking apps, examine issues on the architecture as well as some security measures to deal with the related security challenges. We found that mobile banking apps need to have a foundation to enhance app security and support future technologies. This ensures that mobile apps and their security framework remains future-proof and requires fewer resources to manage long-term.

REFERENCES

[1] K.Pousttchi, M. Schuring, "Assessment of today's mobile banking applications from the view of custmer requirements," in *Procedding of the 37th Annual Hawaii international Conference*, 2004.
[2] Joshi, M. B. & Patel, K. (n.d.). Enhanced Mechanism for Online Banking System through Cyber Crime Investigation, I (Vii), 242-246
[3] Mobile Banking Architecture. Retrieved October 27, 2015, from http://www.paladion.net/mobile-banking-architecture/
[4] Matei, C. M., & Silvestru, C. I. (2008). Internet Banking Integration within the Banking System. *Integration the Vlsi Journal*, 2(2), 55-59
[5] Li Ying , Zhang Can, "Customer's adoption decision analysis of Mobile Banking Services," in *Management and services (MASS), Inernational Conference*, 2010.
[6] Jadidoleslamy, H. (2012). Designing a New Security Architecture for Online-Banking: A Hierarchical Intrusion Detection Architecture and Intrusion Detection System. *Researchpub.org, 2*(2). Retrieved from http://www.researchpub.org/journal/cstij/number/vol2-no2/vol2-no2-5.pdf
[7] "Jakarta Globe," [Online]. Available: http://jakartaglobe.beritasatu.com/business/indonesia-world-leader-use-mobile-banking-apps-report/. [Accessed 22 11 2015].
[8] Darwish, S. M., & Hassan, A. M. (2012). Amodel to Authenticate Requests for Online Banking Transactions. *Alexandria Engineering Journal, 51(3)*, 185-191. http://doi.org/10.1016/j.aej.2012.02.005
[9] Digital Banking. Retrieved October 27, 2015 from http://www.isentric.com/index.php/business-divisions/enterprise-mobility/digital-banking
[10] C. Pavlovski, "A Multi-Channel System Architecture For Banking" *Journal of Computer Science, Engineering and Applications (IJCSEA).* Vol. 3, no. 5, pp. 1-12, 2013
[11] N.Mallat, M.Rossi and V.K.Tuunainen, "Mobile banking services," *Communication of the ACM*, Vols. 47, May, pp. 42-46, 2004.
[12] Jin Nie and Xianling Hu, "Mobile Banking information Security and Protection Methods," in *Computer Science and Software Engineering*, 2008.
[13] C.Narendiran,S. Albert Rabara and N.Ragendran, "Public key infrastructure for mobile banking security," *Global Mobile Congress*, pp. 1-6, 2099.
[14] Dai Wei and Tang Yanling, "Research on Security Payment Technology Based on Mobile E-Commerce," *e-Busuness and Information System Security*, pp. 1-4, 2010.
[15] S. a. J. F.de la Puente, "Virus attack to the PC bank," in *Seurity Technology Proceedings*.

[16] P. Crosman, "First Major Mobile Banking Security Threat hits the US," American Banker, 13 June 2014. [Online]. Available: http://www.americanbanker.com/issues/179_114/first-major-mobile-banking-security-threat-hits-the-us-1068100-1.html. [Accessed 26 October 2015].
[17] Webroot, "THE RISKS & REWARDS OF MOBILE BANKING APPS," Webroot, United States, 2014.
[18] Y. Zhang, and W. Lee, “Intrusion detection in wireless ad-hoc networks,” in ACM/IEEE MobiCom (2000).
[19] Zhang and Lee, “Intrusion detection in wireless ad-hoc networks.”

G. Hulme, “Services Seeks to Bring e-Business to Small Businesses,” in

Informationweek.com (2000), p. 21.

[20] Ghosh, Security and Privacy for E-Business.
[21] A. Sanchez, "Seurity Flaws in mobile banking apps identified by researcher," Out-Law.com, 13 Jan 2014. [Online]. Available: http://www.out-law.com/en/articles/2014/january/security-flaws-in-mobile-banking-apps-identified-by-researcher/. [Accessed 25 October 2015].
[22] M. Cooney, "10 common mobile seurity problems to attack," PC world, [Online]. Available: http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html. [Accessed 26 10 2015].
[23] Arxan, "State of Mobile App Security," 2014.
[24] “Which mobile operating system is the best? Andriod vs. iOS vs. Windows Phone,” Trusted Reviews, 10 June 2015. [Online]. Available: http://www.trustedreviews.com/opinions/which-mobile-operating-system-is-best, [Accessed 26 October 2015]
[25] N. B. o. Arizona, "Mobile Banking App Privacy Policy," 2014.
[26] Xiaoping Zhang and Cheng Zhong, "A Loss Reportable E-cash scheme," *Management of e-Commerce and e-Government*, pp. 354-358, 2008.
[27] “Starbucks (SBUX) on Wednesday acknowledged that criminals have been breaking into individual customer rewards accounts,” CNN Money,13 Jan 2015. [Online]. Available: http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/. [Accessed 26 October 2015]
[28] E. Filiol and P. Irolla, “(In) Security of Mobile Banking ... and of Other,” *BlackHat Asia*, pp. 1–22, 2015.
[29] Carey Nachenberg. A window into mobile device security. Technical report, Symantec, 2011.

AUTHORS

First Author – Sameer Hayikader, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and sameer797.kader@gmail.com.
Second Author – Farah Nurafiqah Hanis Binti Abd Hadi, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and farah.nurafiqahhanis@yahoo.com.
Third Author – Jamaludin Ibrahim, Adjunct Lecturer and Senior Academic Fellow, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and jamal55@gmail.com