International Journal of u- and e- Service, Science and Technology
Vol. 7, No. 6 (2014), pp. 107-116
http://dx.doi.org/10.14257/ijunesst.2014.7.6.10

Systematic Literature Review: Security Challenges of Mobile Banking and Payments System

Md. Shoriful Islam

University Putra Malaysia, Dept. of Computer Science and Information Technology
Serdang, Darul Ehsan, 43400, Kuala Lumpur, Malaysia
sohel.upm.my@gmail.com

Abstract

Mobile banking is more easily and fast banking today, but its challenges to payments security system. Many organization or financial institutions are now incorporating mobile banking and financial services as a key component of their growth strategy, and use of the mobile phone to conduct banking and financial services tasks continues to rise among early adopters. Large number of security challenge of mobile banking and payment system have been proposed in to the current research issues, our goal is to gain insight into the current status of mobile banking and payment system security challenge research issues published to date, conducted a systematic literature review mobile banking security challenges that have been claimed between January 2008 to December 2012.this paper presents the result of the systematic review, 10 publication and 20 were selected as primary studies, from which a large number of challenges were elicited. By applying qualitative data analysis methods to extracted data from the review. However among the majority of consumers, security threats are most commonly listed as the primary reason for not trying mobile banking. This review will attempt to technically address these largely unfounded consumer security fears while helping to lay a roadmap for financial institutions successful implementation of mobile banking technology. A clear and emerging new channel in the space of banking and payments is mobile. A key challenge with gaining user adoption of mobile banking and payments is the customer's lack of confidence in security of the services. Understanding the mobile banking and payments market and ecosystem is critical in addressing the security challenges. There are new security risks introduced with mobile banking and payments that must be identified and mitigated.

Keywords: *SLR, Online threats, Mobile Banking, security challenge payment system, mobile network GSM & CDMA, Security Best Practices, Mobile Operating system*

1. Introduction

Socio-economic impacts of mobile-banking systems in the developing world is scarce .Even less attention has been paid to the social, economic, and cultural contexts surrounding the use of these systems. Mobile banking is a revolution that is driven by the world's one of the fastest growing sectors mobile communication technology. Like in any emerging technology, there exist barriers to the adoption of mobile banking services. This study explores the issues in mobile banking perceived critical for adoption by both mobile banking users as well as non-users. The study identified certain issues pertaining to banks, mobile handsets and telecom operator's viz. mobile handset operability, security/privacy, standardization of services, customization, Downloading & installing application software and Telecom services quality. For this a descriptive design was adopted to empirically

ISSN: 2005-4246 IJUNESST

explore the Security challenges. Study suggests that from consumers' perspective mobile handset Operability, security/privacy and standardization of services are the critical issues and security challenges. The implications of the results provide practical recommendations to the all concerned mobile banking security and payment challenges. This paper reports on the results of our systematic review aiming at identifying and classifying Mobile banking payment security challenges. We provide an overview of the-state-of-the-art of mobile banking security challenges, and a key for reading and interpreting them. In addition, this paper presents a number of interesting findings, including mobile banking challenges of payment security and application of mobile banking, and the importance of inter-relationships between financially as well as our smart phone security challenges. Our findings also ring a bell to the research community. A large number challenges Javelin Strategy & Research and Vanessa Pegueros focused research agenda is necessary to current mobile banking security challenges research efforts. Number of workshops, conferences, project are establish challenges of mobile banking security to make payment via online. The studies that have been analyzed in Javelin Strategy and Vanessa Pegueros review were published between 2009 and 2012.All conference and workshops, journal on mobile banking challenges time to perform an update systematic review security challenges of mobile banking payments system.

2. Research Methods

2.1. Systematic Review

A systematic process of formulating study objectives, selecting, critically appraising, synthesising information and drawing conclusion from relevant studies in order to provide a reliable review using either quantitative or qualitative approach (Oxman, 1994; Boynton et al., 1998). A review of the evidence on a clearly formulated question that uses systematic and explicit methods to identify, select and critically appraise relevant primary research, and to extract and analyse data. Statistical methods (m-a) may/not be used. To conduct the systematic review constituting three main phases planning the review, conducting the review, reporting the review. The main part of planning are to specify research question and develop a review protocol, review protocol most important part of systematic review.

2.2. Research Question

Mobile banking security challenge of payment system addressed in different studies perspectives simultaneously challenges fragmented. While consumers continue to express concern over using their mobile phone to conduct banking and financial services transactions, it is a fear born more of perception than reality. There are threats, but the security controls available to mitigate risk at this level are substantial and effective. However, security practices will need to continue to evolve as more and more smart phones enter the market running more and more applications, creating an ever growing opportunity for security threats. Mobile banking challenges described in different studies at various level of abstraction, making challenges fictively independent or isolated, typically challenges describe high level about proposing requirements for engineering activities or resulting products. Review is not only to identify all the claimed mobile banking security challenges, but also to classify them so that inter related and inter depended challenges can be grouped. The purpose of this paper is to educate the reader on the security threats and vulnerabilities for mobile, especially in the context of the financial services industry. This report highlights the most popular strategies for deploying mobile services, including SMS, client-based applications and the mobile Web, and the benefits and risks to each type of service. Security Challenges of Mobile Banking and Payments system: Key questions explored in this paper

Q1) Mobile payment over online threats challenges?
Q2) Operating systems on mobile devices security challenges?
Q3) Network and transport challenges mobile banking security?

2.3. Review Protocol

The main components of the review protocol include data sources, search strategy, study selection strategy, data extraction method, and data synthesis. The first three components define the scope of the study and explain the motivation behind it. The last two components describe how the results and concluded.

2.3.1. Data Sources: Therefore use these libraries as our main resources:

- IEEE Explore
- ACM Digital Library
- UCL Library
- Science Direct
- Wiley International Science journal Finder

Also helps of this two Search engine, Google and yahoo

2.3.2. Data Selection: Data selection is the most imported thing to systematic review any existing research review, lot of thing are irrelevant to our research questions. Study selection has to be including only studies that contain useful information for answering Mobile banking payment security system challenges. Limits of study that are strongly related to mobile - banking security system challenges. In our future work plan to another systematic review which on the studies that are presented in form than scientific paper.

2.3.3. Data Extraction: Each primary study is analyzed on identifying mobile banking security challenges. All identified challenges are documented in a spread sheet in terms of their names, description and rationale.

3. Overview of the Systematic Studies

Mobile banking is fast banking all over the world compare to other banking. Rapidly increased the user of mobile banking, New challenge of this sectors is Online threats, Smartphone user always active on online downloading various application and picture movies, song and official mail or other personal files, playing games over internet. More than 5 million users around the world regularly use their mobile phones to make various payment or transactions on their online banking accounts or view various payment, pay utilities bill and account balance. Most customers receive this information in the form of text messages, but a number of banks now allow customers to download secure software that can access on banking system and perform transfer money between accounts and third party. But the question is that how secure is this payment system, In February 2011 by Bill Gajda (Head of Global Mobile Product at Visa Inc.) written in his research paper over the past decade, mobile phones have emerged as one of the most ubiquitous technologies in human history. Today, billions of people in virtually every corner of the world have mobile phones. These devices shape their interaction with their communities, countries and economies.

3.1. Online Threats Challenge of Mobile Banking

Today mobile phone uses different forms, common from used of SMS spread phony URLs, and VOIP, the using of telephone number to lead victims to bogus voice service like IVR that fool victim into taking with their financial institution. Attackers send information via SMS or web-based banking when message including a URL or a phone number. When a calling a user may interact with an actual person or a voicemail system which is security threat challenge to mobile banking payments system. To review the threat security in mobile banking we can classify man three categories.

Broad threats	**Phone or handset threats**	**Online or Internet treats**
Unauthorized access Malicious hacking, Malware. Mobile viruses,	Memorycards,Downloads,Various,Application,Mobile Browsers, Smart card.	Mobile E-mail, SMS, Mobile IM (MIM) , Voice , Online Games. Gateway

Figure 1. Table of Threats

3.1.1. Broad Threats: Unauthorized access to services in mobile banking channel is broad threats, Various damage, hacking or web-based service attacks are creating some threats profile on the mobile as Personal computer or laptop. Malware is currently big factor on mobile banking as well as payment system challenge in mobile banking; Cross platform malware is example of challenges. Matt Swider written in his article april'2013 Smartphone is more effect present day, falling victim to 163% more malware in 2012 the previous year according to a new report. Especially 95% of malware found on Google hardware and Android operating system. In this research 32.8 million devices infected in 2012 when 10.8 million were host to malware in 2011. The app repackaging was most common method using for malware. In present day in mobile banking system really challenges to security for mobile threats.

3.1.2. Handset & Mobile IM (MIM): In mobile banking system some time customer saved in his personal data on his mobile such as money payment receipt or other various payment this information keep into mobile memory, Sometime mobile phone are effected by virus and hacker can get his information to payment system or personal information, Skulls is a Trojan horse that arrives as an installer for a normal application. Trojan is can overwrite existing files. The client-side environment includes the applications downloaded and installed on the device. These can be signed by either the carrier or the financial institution. Often the applications are sandboxed on the device. The most secure choice for financial institutions is not to send sensitive data to the handset at all. The next best is to delete it at the end of each session, or if sensitive data is stored on the handset, to encrypt the data. Mobile banking Application software developers must be development secure software that can be despite testing of mobile application on varies carriers and platforms When customer downloading application software from app store customer cannot identifying this one real or not. This is a big challenge with open source software, such as designed for android or Linux platforms. Mobile browser are the same as pc browser like scripts, cross site script (XSS) and cross site request forgery (RSRF) both are smaller feature.

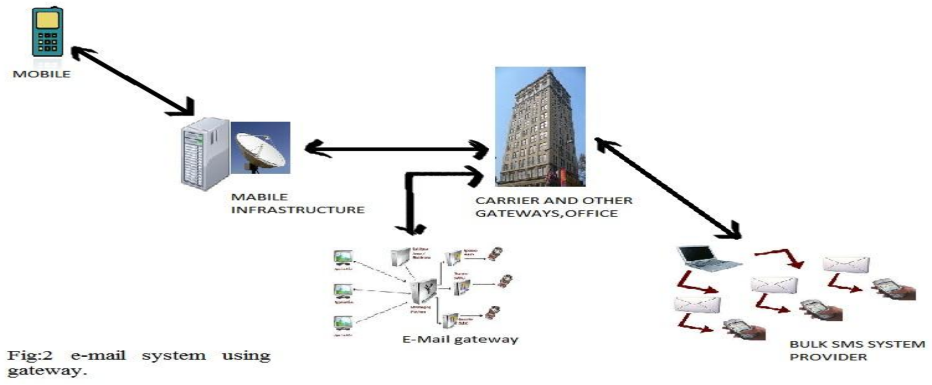
MOBILE
MABILE INFRASTRUCTURE
CARRIER AND OTHER GATEWAYS,OFFICE
E-Mail gateway
BULK SMS SYSTEM PROVIDER
Fig:2 e-mail system using gateway.

Figure 2. The System Mobile e-mail Clients using Gateways

4. Operating Systems on Mobile Devices Security Challenges

Operating system of mobile phone is new challenges of mobile banking payment system. Different mobile company used different types OS in smart phone, Mobile phone operating system is designed especially for mobile devices, Mobile OS is a software platform that a application program ran into on a mobile devices. Today mostly uses OS are Windows, Palm, Android, Apple, In some ways the open-source Android platform is more secure than other operating systems. By design, its OS uses the sandbox approach, which isolates code injected into the browser from other parts of the mobile system. That hasn't stopped research into vulnerabilities. In early 2009, security researcher Charlie Miller discovered a way that allows criminals to take control of the phone's Web browser. If compromised, the browser’s credentials and history could be visible to a remote hacker. No word on whether this vulnerability has been patched. The kernel of android mobile Operating system has defects, according to new research. In early 2008, a new WinCE Trojan called InfoJack insidiously appeared inside legitimate installer packages like Google Maps as an option. This Trojan disables Windows’ mobile security so that other unaccredited applications can be installed without permission.

Palm OS updated, new version is also security risk for mobile banking system smaller footprint worldwide was issues address denial of service when the user clicked over long URLs (greater than 4,063 characters). Attackers could have distributed an exploit for this through e-mail, MIM, or SMS. At Black Hat USA 2009, researchers showed how one could use a malicious SMS message to shut down the Com Centres in the Apple iPhone, Mac OS can be risk when the used wifi and connected by 3g or 4g internet system. Criminals to take control of the servers running BlackBerry systems, It worked by sending e-mails with tainted attachments within Adobe Systems’ PDF format. Customer may be at risk when they read PDF format file. Widows OS also risk, WinCE Trojan called Info Jack insidiously appeared inside legitimate installer packages like Google Maps as an option. This Trojan disables Windows’ mobile security so that other unaccredited applications can be installed without permission.

5. Network and Transport Frequencies Challenges

Mobile devices communication data over network system, Wireless carrier is primary interface between the mobile and radio communication system, the radio component of the mobile device communicates to the mobile sites. The cell sites then communicate through dedicated circuit or microwave to the mobile switching center which contains both the voice processing and data processing equipment and systems. The switching centre contains the gateway to the Internet and other carrier networks. If there is a security weakness in any part of this network, it can put the customer's data at risk. Figure 3 network system.

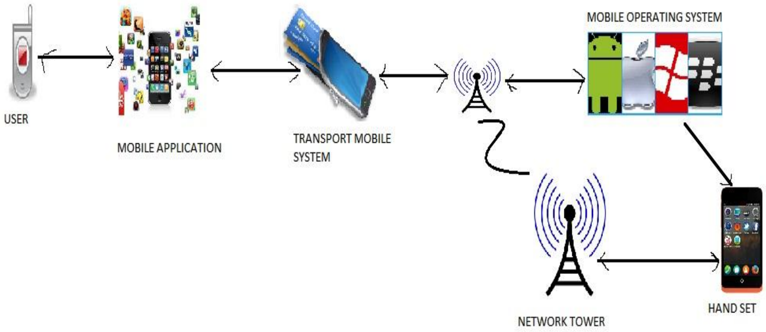

Figure 3. Network and Transport System

5.1. Network Challenges

Today mobile system is used commonly GSM and CDMA , Mobile weakest network is another challenges to mobile banking challenge, when Attacks this system the mobile network not working properly, This time the attacker directly access gain to mobile channel system. In 2007 Vodafone Greece was hacked. Software extensions installed on the Ericsson AXE switching equipment permitted eavesdropping on government phone calls.

5.1.1. GSM: Without North America recent cracking of the encryption used on GSM. The researchers and organizations have published research showing A5/1 and A5/2 encryption algorithms to intercept and decrypt traffic through such encryption. Active and passive techniques both are exist; the passive technique is much harder to detect because it avoids sending any additional traffic and only listens. As well as Third parties sell devices such as the "Passive GSM Interception System (SCL-5020)," to spy on communications when they use weak or no encryption (A5/0 and A5/2), however, the cost to hack GSM is still substantial. For this type attack is challenges to mobile banking challenges' to payment system.

5.1.2. CDMA: CDMA transmission is harder creak then GSM, In CDMA system used a code, the multiplexer used to multiplexing the code and it is transmitted on same channel, CDMA system handle more user on fewer cellular Network tower.

5.2. Transport Challenges

Mobile transport system is including HTTP, WAP, TCP/IP, SMS, BLUETOOTH, OTA, USSD, It is important that how the data sent by user or financial organization to make payment also challenges mobile banking payment system.5.2.1 HTTP and WAP browser. Smartphone can use HTTP protocol to access internet and take some advantage communication protocol to system security. Include SSL, the method manual authentication. That includes encryption. Wireless application protocol (WAP) is an open data communication protocol used in mobile system, it main used access internet via a mobile devices. A WAP browser of mobile system including all basic operation as a pc browser, but mobile have some restriction of the mobile ecosystem, when a mobile screen minimize the web site dynamically converted WML (Wireless Markup languages) and optimized the view as WAP browser, So the pc security cannot apply the mobile security system it is a security challenges of mobile banking system.

5.2.2. TCP/IP and SMS: TCP/IP used all Smartphone to communication over internet, mostly Smartphone operating system are support TCP/IP network protocol.TCP/IP handles low level networking protocol such as UDP IP TCP the attacker attacks IP layer and Routing Information Protocol attacks which changes the data destination and passing data to other destination. Smartphone mobile banking TCP/IP another challenges to mobile banking system. SMS system is challenges to mobile banking system. Client SMS are automatic saved in personal mobile when user saved is SMS on his mobile set, Attacker attack the mobile and get important information about the organization and can log in to the organization system and important transaction is risk, many of attacker applying this kind of send sms and send E-mail to user.

5.2.3. BLUETOOTH, OTA, and USSD: Bluetooth protocols used to connect to a mobile device with unfortunate results when malware is involved. Bluejacking and bluesnarfing method used the attacker to connect using Bluetooth devices. Attacker can a phone call the user can not realized the phone number, for this region many mobile handset today disable Bluetooth by default. June 2004 attacker, at least fifteen variants, the original worm spread over Bluetooth connections on Symbian Series 60 mobile handset phones, in the inbox as a caribe.sis file. Accepting the file user and attack the user mobile phone. OTA is over the air programming allow the administrator to upgrade a new system over existing system. This is the new future of mobile programming various standards exist, including open mobile alliances (OMA). Unstructured supplementary services data (USSD) is a real time SMS service at GSM mobile system. When SMS change to Email the SMS change to a telnet, The organization and user check account balanced via USSD service. USSD not use the ameria

6. Security Best Practices

Mobile banking payment system is attack by handset, mobile operating system various application SMS or MMS and network transport data communication. Email and phone call have some create threats that may be attack on our mobile phone and lost personal information, User avoided the unexpected SMS can safe his mobile phone.SMS gateway provider to prevent spam and spoofing.

6.1. Best practise Handset

User mobile applications one of the most secures mechanisms for conducting critical payment system or do transactions but could still contain vulnerabilities and subject to mobile threats. Organization or Application have more control of network and transport protocols to use encryption. Client or User can Destroy temporary data and encrypt file locally stored sensitive data. Important and Critical applications may allow instituted or organizations to support special functionality such as profiling and registering a device and check or verifying the system integrity. Features system may be available through the mobile operating system than through a custom-designed and modify mobile application. While such control is potentially beneficial, it requires investment in multiple operating systems and platforms. Maintenance and development costs may be higher than other solutions and require more support.

6.2. Best Practices Network

ISP Providers can be block an unauthorized internet access site and SMS gateway provider because attacker to send spam or spoofed messages. Similarly, SMS service providers may monitor message contents and work with financial institutions to prevent such messages from reaching end devices. SMS filtering can help organizations that reach out to service providers to prevent threats at the network level. Many of the option can be applied the SMS gateway provider such as including Network option: End-user lists, Content-based detection, Legal action, Limit outgoing spoofed messages. Gateways always monitor the number or volume of SMS messages the customer send and organization received. SMS gateway can be many controls and serve a good service.

7. Conclusion

Mobile banking rapidly increase to make easy payment system, user can access any time banking to make any payment. Attacker always makes a new program to attacks our mobile and gets personal information. So, organization and mobile banking user must be concern about update mobile banking system. The mobile manufacturing company must working together with operating system and network provider company that make a most reliable and user trust security system. The Mobile banking Software organization and vendor must be communicating each other that ensure the system always updated. User education is very important way to mitigate the threat of mobile viruses. Network provider can be blocked some known SMS because Attacker used some commonly SMS send to spam and spoofed messages. Some organization used phishing and malware channel in to the mobile channel that is not good channel or not secure and trust channel. Organization implement to used the transaction this channel can be safer then online channel. The mobile banking payment system is more challenging and dynamic changes rapidly, mobile banking payment system ecosystem is more complex system. Security and perception of security system mobile banking can be play a role in who ends of dominating.

8. Key Finding

While consumers continue to express concern over using their mobile phone to conduct banking and financial services transactions, it is a fear born more of perception than reality. There are threats, but the security controls available to mitigate risk at this level are substantial and effective. However, security practices will need to continue to evolve as more and more smart phones enter the market running more and more applications, creating an ever growing opportunity for security threats.

References

[1] The State of Mobile Security in Banking and Financial Transactions Conducted by Javelin Strategy & Research September, (**2009).**

[2] B. X. Chen and N. Bilton, "Et Tu, Google? Android Apps Can Also Secretly CopyPhotos", (**2012**) March 1, http://bits.blogs.nytimes.com/2012/03/01/androidphotos/

[3] D. Danchev, "Fake Gmail Android application steals personal data", (**2012**) June 6, http://www.zdnet.com/blog/security/fake-gmail-android-application-stealspersonal-data/12308

[4] E. Eigdon, "US Mobile Banking Forecast", Forrester, (**2011)** January 31,

[5] L. Essers, "Untethered jailbreak for iOS 5.1.1 available for download", May 25th,2012,http://www.computerworld.com/s/article/9227495/Untethered_jailbreak_for_iOS_5.1.1_available_for_download

[6] G. Morgan, "Mobile malware rises by 155 per cent as Android platform risksgrow", (**2012**) February 16, http://www.v3.co.uk/v3-uk/news/2153026/mobilemalware-rises-155-cent-android-platform-risks-grow

[7] V. Niemi and K. Nyberg, "UMTS Security", John Wiley & Sons, England, (**2003**).

[8] J. D. Pitts, "Surfing the Payment Channels, Mastering the Fraud Tsunami", JDP Enterprises, Carrollton, TX, (**2010**).

[9] M. J. Schwartz, "New Android Malware Has Costly Twist", (**2012**) February 6,h ttp://www.informationweek.com/news/security/mobile/232600313.

[10] Q. Gu and P. Lago, "Exploring service-oriented system engineering challenges: a systematic literature review".

[11] R. Chaudhri, G. Borriello, and W. Thies, "FoneAstra: Making mobile phones smarter", In ACM Workshop on Networked Systems for Developing Regions, ACM, (**2009**) October.

[12] M. Pickens, "Mobile money by the numbers," *http://technology.cgap.org/2009/06/04/mobile-money-by-the-numbers/*, (**2009**) June.

[13] J. S. Cheney, "An Examination of Mobile Banking and Mobile Payments: Building Adoption as Experience Goods?", (**2008)** June.

[14] Mobile-based spam is becoming an increasing concern in many parts of the world. For example, the average mobile cellular phone subscriber in China receives six to 10 spam messages a day. See "Cloudmark: Mobile Operators Bracing for Global Surge in Mobile Messaging Abuse," *Wireless News*, February 17, 2008.For further reference, see Mark Furletti and Stephen Smith, "The Laws, Regulations, and Industry 13.Practices that Protect Consumers Who Use Electronic Payment Systems: Credit and Debit Cards," Payment Cards Center, Federal Reserve Bank of Philadelphia, (**2005**) June, (seewww.philadelphiafed.org/pcc/papers/2005/ConsumerProtectionPaper_CreditandDebitCard.pdf).

Author

MD.SHORIFUL ISLAM

Address: B3-07-01, Kepong Central Condominium, jalan puncak desa-2,Tman puncuk Desa,52100,kepong,kuala Lumpur, Malaysia. +60166757409(Malaysia),+8801721299559(Bangladesh).

Academic

M.sc in computer science and information technology
University Putra Malaysia.(UPM) ,Serdang, Selangor, Darul Ehsan ,43400, Kuala Lumpur, Malaysia**.**

Business Information Technology.(BIT).
FTMs College, Jalan Hang Kasturi,50000 Kuala Lumpur,Malaysia.

Computer Science and Engineering (B.sc)
Islamic University,Kushtia-7000,Bangladesh.

Project Work:
LIVE TRAFFIC MONITORING SYSTEM.
University Putra Malaysia.(UPM) ,Serdang, Selangor, Darul Ehsan ,43400, Kuala Lumpur, Malaysia**.**

ONLINE INSURANCE SYSTEM,
Islamic University,Kushtia-7000,Bangladesh.

Associate member (AM)
Bangladesh computer Society (BCS), Dhaka, Bangladesh.

Personal:
Country : Bangladesh
Passport No: BC0271733
Date Of birth: 09th September 1983

Statement: To work in a challenging environment with a scope of future progress, by applying my academic knowledge and working ability. I want to work as a part of a dynamic working where I can make a significant contribution to develop my skills yet further.