A Survey: Online and mobile banking risks, security issues and challenges on mobile devices and its user awareness

Anum Abbas
MS Computing,
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology
90 and 100 Clifton
Karachi -75600
aabbas1988@yahoo.com

Naveed Dilber
Assistant Professor, Department of Computer Science
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology
90 and 100 Clifton
Karachi -75600
naveed.dilber@szabist.edu.pk

Abstract—— **With the growing use of mobile devices, it is a known fact that more people use internet from mobile devices than the conventional desktop PCs. Specifically, mobile devices are gaining popularity and with ease of availability its usage is a global phenomenon, creating a market and eco system of its own. Similarly online and mobile banking facilities have made a mark of its own, as consumers can now easily access their financial information from anywhere in the world and commit transactions without physically being present in financial institution of their choice. Combining the above two technologies opens a new arena of challenges, where a balance of functionality and security is to be carefully considered. Using online and mobile banking systems from mobile devices, either via browser or mobile business application, both the consumer and the institution are required to adopt a paradigm shift with respect to understanding the risks and required controls to mitigate those risks. In this research we attempted to study security issues and risks related to mobile devices faced by the banking industry, more particularly, mobile banking. Further, we shall look into the current trends, future challenges and solutions available in order to secure the communication between mobile devices and business application and how they can be mitigated. Furthermore, we will conduct a survey within the banking industry to understand the current security mechanisms adopted by these institutions. Moreover, consumer awareness, their thought process and views related to security threats shall be studied to identify their understanding of the risks and challenges and their comfort level while using mobile devices for financial transactions.**

Keywords*—— *Mobile device, online banking, mobile banking, information, security

I. INTRODUCTION

In the mobile technology world there is an emerging technology i.e. mobile devices, usage of these devices is dramatically increased in the recent years. In mobile devices there are different operating systems used which are Android, iOS, Symbian Nokia and Windows operating systems. The mobile devices are used in both private and corporate areas and its security becoming the main concern as the mobile device users are performing, accessing and managing different task such as communication with friends and family, managing bank account, accessing business or work related sensitive/critical data or information. As the sensitive and critical information are being accessed from the mobile devices, this makes it more vulnerable to security threats and attractive target for attackers.

The online and mobile banking is from where user can manage bank accounts and perform transactions by using business application, web or SMS. In online banking, users are given access to their personal critical financial data, making security a prime area of concern. To provide secure communication and to protect the critical data and information enabled many banking industries to rethink about their current security mechanism due to mobile device mobile nature.

This paper will provide an overview of current security issues and risk faced by the banking industry in online and mobile banking from mobile devices. Further, we will also study the solutions available in order to secure the mobile devices communication and how the risks can be mitigated. In this paper we will perform survey research in order to acquire information from banks about their current security mechanism to secure the online banking communication, Moreover, we will also perform survey to acquire information from users about the security concerns and how much they are aware about the online banking and mobile devices security issues and risk.

II. PROBLEM DOMAIN

As the usage of mobile devices and internet increases day by day, the risk related to the mobile devices and internet are also increasing.

In this paper, we have focused to aware the user about the online and mobile banking risk if it is used in mobile devices. The purpose of this research is to analyze that, are both the consumers and financial institutions have understood, analyzed and sufficiently mitigated the risks that have evolved with new technologies used to access critical financial data.

III. PROBLEM STATEMENT

"Are user aware from the risks of online and mobile banking while using it on mobile devices?"

IV. Related Work

There are many researches related to this work have already been conducted and there are more to come as this topic is related to the emerging technologies that how can we securely access our critical financial information and perform transaction through mobile devices. In this paper we have studied all the mentioned papers and then have compared the different mechanism and measures to securely use online banking through mobile devices. Further, we have compared their analysis and local banks survey that are providing online banking services in order to provide the awareness to users and point out best possible solution for securing the critical financial data.

V. Introduction to mobile banking, online banking and mobile devices

A. *Mobile banking and Online Banking*

Mobile banking allows the people to perform financial transaction through mobile devices by the use of special client programs or applications, SMS and mobile web. Mobile banking provides various types of services to customers that include checking account, payments, deposits, withdrawals and transfers. In earliest days mobile banking services are offered through SMS which was called as SMS banking. But in today's world introduction of smart phones and devices make the mobile banking a significant amount of boost. Some banks nowadays provide different applications that are compatible with different versions of operating system of mobile devices.

Whereas, online banking is same as mobile banking but it allows the customer to perform financial transactions through a secure website (browser based) and can be called as virtual banking. In order to access the services of online banking customer should have to register itself with the internet banking website with login credentials. Further, online banking provides almost same services as per mobile banking.

But in today's world, the introduction of smart devices like smart phone and tablets that provides almost same functionality as desktop PC's or laptops which narrowed the online or internet banking and mobile banking difference as the users can access their internet banking account through their smart devices.

B. *Mobile Devices*

Mobile devices in modern world are multi-functional devices capable of performing multiple tasks at a time and handle various range of applications for business, education, entertainment and etc. In mobile devices evolution smart phones and tablets is the most significant growing category through which people can access the internet and perform different task like accessing email, instant messaging, web browsing or even office documents. The mobile devices help the people to synchronize with their personal computers in order to exchange the information. The most critical part which questions the security of mobile devices that they are being using for the critical financial and corporate date and its usage is increasing day by day due its mobility and convenience nature. The users are performing financial transactions through their mobile devices and save the critical corporate data in their mobile devices.

There are many types of mobile devices which uses different types of operating system and every operating system have their unique functions. Following are the types of mobile devices and types of operating system.

C. *Types of Mobile Devices:*

There are many types of mobile devices but some major types are as follows:

- PDA (Personal Digital Assistant);
- Smart phones; and
- Tablet.

D. *Types of Operating System:*

Following are the types of operating system using in mobile devices:

- Symbian OS;
- Windows Mobile;
- Android;
- iOS; and etc.

VI. Security risk and issues of mobile devices

In today's world mobile devices gain the popularity and capture the electronic market and its usage is increasing dramatically. People can now use mobile devices for communication, entertainment, office work, shopping, banking and etc.

As the usage of mobile devices increases so as its risk are increasing due to the significant changes in the nature of mobile devices. There are many types of risk associated with the mobile devices but the main risk which we have highlighted and discussed here is data loss and data theft as the mobile devices are using for financial transactions contains very critical data and information which can be used by a hacker.

Many researchers have found out that people are bypassing the iPhone and android security admin restrictions which allowed the user to install the unofficial firmware and software which leads to malicious software running on that mobile device this is a major risk involved with the mobile devices nowadays which causes mobile devices damaged and corrupted. Further, portable nature of mobile devices causes many issues as the users are accessing their critical data and information related to finance or business without the limitation of location which leads to physical issues which are loss or snatch of mobile devices. The mobile devices are capable to secure the information or encrypt them but the unaware user does not implement any type of security measure in order to protect the critical information contain in the mobile device which causes mobile devices more vulnerable for data loss and theft. Moreover, mobile devices are susceptible to spamming, electronic tracking, cloning and etc.

There is also another and the most critical risk and issue in the mobile device is the communication medium as the mobile devices uses Wi-Fi technology to connect with the internet and exchange the information which can be easily hacked by publicly available tool as the mobile devices are less secure than the traditional PC's. The most common and famous attack which is called 'Man in the Middle' attack can be used in order to hack the mobile device.

So in order to protect the mobile devices from the highlighted risk and threats mobile devices users should be educated and aware about the security concerns in order to protect the critical data and information from going into wrong hands.

VII. Risk and Security Challenges in Online and Mobile Banking

Online banking was introduced in mid of 90's when internet popularity was increases and it was spreading rapidly all around the globe. Now, mobile banking is introduced which uses applications for banking purpose like check account balance, account transfer, perform transactions on mobile devices (iPhone, Blackberry, Android and etc.)

Many researches have been done on online and mobile banking risk in order to aware the user who are using these services but threat and risk always remain as the mobile devices nature is gradually changes. Due to rapidly change in the nature of mobile devices it is really difficult to educate the user as the technology is improving more and more risk and threats are increasing. However, many researchers concluded that the mobile banking is much more secured than the online banking as the mobile banking uses specific type of secure application as compared to the normal web browser.

There are many risks associated with online banking some of them are communication risks, client authentications, human factor and etc. Hackers can use many ways to hack the current online banking system like botnets, phishing, Trojan and etc. As per the internet crime report the internet crimes are not limited online banking it can effect client-server internet applications. The most emerging attacks nowadays are through the web browsers by the use of Trojan viruses. The attacker can easily hack the system if proper security measures are not taken like antivirus, antispyware, firewall and etc.

The financial institutions should be aware from the mobile banking risk in order to secure it from the threats which may affect mobile banking services. Cloning is the most significant threat which gives hacker to access the victim's financial accounts. The other risk in mobile banking is malware which came by installing unofficial application and software from third party which can compromise the confidentiality, integrity and availability of the victim's critical data. Further, malicious code came with the software can also create a backdoor causes financial damage and through phishing, hacker can trick the victim and get the account information or force them to download some application through email contains malicious code or malware.

VIII. Solutions for Online and Mobile Banking Security Risk and Issues as per International Banking Sectors

In order to secure the above mentioned security issues and risk many solutions have been introduced by researchers and IT security organizations in order to secure the online and mobile banking. Following are some of the security mechanisms and measures discussed below:

- Analyze the business reports and transaction trends;
- Uses alerts and notifications through which user updated about the transactions through email, SMS, voice or internet and etc. with transaction time, date and location;
- PIN codes, user name and passwords;
- Encrypting the mobile device;
- More robust communication encryptions;
- User awareness;
- More secure network infrastructure like firewall, IDS, IPS, DLP and etc. (Defense in depth);
- Introduction of antivirus and anti-spyware tools in mobile devices;
- Certificate verification or digital signatures;
- Multi-factor authentication;
- Device identification;
- Exception reports;
- More secured mobile banking application and etc.

The different IT security organizations also introduced their security suite in order to provide more secure environment for online and mobile banking.

IX. Conclusion

After studying the general risk of mobile devices and compare the risk of online and mobile banking, we have concluded that mobile devices are not secure enough as compared to traditional PC's. Mobile banking is the future of banking as it uses secure application rather than web browser so in order to use the mobile devices for online banking customer should have to use mobile banking instead of online banking service.

Further, after conducting the survey at local banks and mobile devices users we have noticed many things like, first mobile banking application is not fully introduced yet in Pakistan. Moreover, users are not aware of the issues about the mobile devices and online banking. So in order to secure the critical data and information users should be aware and banks should conduct some awareness program locally in order to secure educate the user about how can user securely access their account and critical information.

My conclusion of this research is that mobile banking applications should be launched by the banks at Pakistan as it is more secure method due to its unique nature of application which makes it difficult for attacker to use general attack methods of web browsing. Further, the numbers of mobile devices users on online banking are increasing who are not aware of the issues of online banking which may cause critical data and information might be lost which in the end leads to or affects the bank's reputational risk.

Acknowledgement

First, I would like to thank Mr. Abbas Rajani (Chief Information Security Officer) of Bank Al-Habib who supported me in my independent study and share his utmost knowledge and information about this topic of research. He is very kind hearted person and helped me in developing questionnaire about my topic which helps me to understand research related things. Second, I would like to thanks Mr. Naveed Dilber (SZABIST Faculty) to be my supervisor in this research and have supported me throughout the research and provided his precious time from his busy schedule without his supervision this research never completed.

Further, I would like to thank to my parents, colleagues and friends who motivated and supported me during the entire research.

References

[1] Android OS Security: Risks and Limitations by Rafael Fedler, Christian Banse, Christoph Krauß, and Volker Fusenig, year 2012;
[2] A Land Mine Beyond the Internet: Mobile Banking Risk by Hicham S. Chahine and Luke Nordlie, year 2012;
[3] Meeting Today's Customer Needs with Internet Banking by First Data, year 2012; and
[4] Mobile Payments: Risk, Security and Assurance Issues by ISACA, year 2011.
[5] Awareness of Electronic Banking in Pakistan by Nouman Anwar Dar MCB Bank Limited year 2010
[6] Narendiran,Public key infrastructure for mobile banking security by C. Inst. for Dev. & Res. in Banking Technol. (IDRBT), Hyderabad, India Rabara, S.A.; Rajendran, N. year 2011
[7] Research on the Internet banking security based on dynamic password by Yazhou Xiong Sch. of Econ. & Manage., Huangshi Inst. of Technol., Huangshi, China year 2011
[8] Towards secure information systems in online banking by Karim, Z. Appl. Res. Centre for Bus. & Inf. Technol. (ARCBIT), Guildhall Coll., London, UK
Rezaul, K.M.; Hossain, A. year 2011
[9] The security of electronic banking by Yi-Jen Yang 2403 Metzerott Rd. Adelphi, MD. 20783 year 2011
[10] E-banking – impact, risks, security by Titrade Cristina Ciolacu Beatrice Pavel Florentina year 2010
[11] Users' Perception of Mobile Information Security by Liu Ying, Huang Dinglong, Zhu Haiyi, Patrick Rau year 2009
[12] Risk and inovation in e-banking by Cezar mihalcescu, Beatrice ciolacu, Florentina pavel, Cristina TITRADE Romanian – American University, Bucharest, Romania year 2009
[13] Phishing on Mobile Devices by Adrienne Porter Felt and David Wagner year 2009
[14] An Analysis of the Online Banking Security Issues Reported by Hole, Moen, and Tjostheim year 2010
[15] Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication Gunajit Sarma1 and Pranav Kumar Singh2 year 2012
[16] Mobile banking as technology adoption and challenges by Archana Sharma year 2012
[17] Relationship between Customer Satisfaction and Mobile Banking Adoption in Pakistan by Zohra Saleem and Kashif Rashid year 2012
[18] Understanding the Adaptation of Mobile Banking among consumers : An Empirical Evidence by Neha S. Shukla and Dr. Vimal K. Bhatt year 2012
[19] Preventing Spoofing Attacks in Mobile Banking Based on User Input Pattern - Based Authentication by K.Sujana, 2Md.Murtuza Ahmed Khan year 2012
[20] Mobile Banking in India: Practices, Challenges and Security Issues by Vishal Goyal1 , Dr.U.S.Pandey, Sanjay Batra year 2012
[21] An Analysis of Internet Banking Security of Foreign Subsidiary Banks in Australia: A Customer Perspective by Panida Subsorn and Sunsern Limwiriyakul year 2012
[22] A Practical Approach for Secure Internet Banking based on Cryptography by Syeda Farha Shazmeen, Shyam Prasad year 2012
[23] Online Banking: Information Security vs. Hackers Research Paper by Paul Jeffery Marshall year 2012
[24] Security of Mobile Banking by Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison year 2012