International Journal of
Science and Engineering Investigations vol. 2, issue 18, July 2013
ISSN: 2251-8843

Security Protocol Design for Mobile Banking

Reihaneh Khorsand Motlagh Esfahani[1], Seyyed Mohsen Hashemi[2]
[1]Computer Engineering Department, Science and Research Branch, Islamic Azad University, Tehran, Iran
[2]Dean of the Software Engineering & Artificial Intelligence Dept., Science & Research Branch, Islamic Azad University, Tehran, Iran
([1]Reihaneh_khm@yahoo.com, [2]Hashemi@isrup.com)

Abstract- Accessing banking services on a mobile device give customers a great deal of independence. Not only does it put them in charge, it also enables them to do their banking independently of their location and time. A main worry for consumers and financial service providers is the security of mobile banking. In providing mobile banking services, it is very important to take the proper security authentication and authorization, because these services, while offering very good mobility and facility, can be easily exposed to diverse violation threats. In this paper, a novel security protocol for secure mobile banking applications is proposed to address security worries. The presented protocol permits customers to authenticate with the banking services with least user interactions but with new advance security characteristics.

Keywords- *mobile banking; security protocol; Risks; challenges; security*

I. INTRODUCTION

Mobile trade has some definitions in the published works but can be commonly defined as a type of e-commerce transaction, governed through mobile devices using wireless telecommunications networks and other wired e-commerce technologies [1]. A survey describes mobile banking as "using a mobile phone to access your bank account, credit card account, or other financial account. Mobile banking can be done either by accessing your bank's web page through the web browser on your mobile phone, via text messaging, or by using an application downloaded to your mobile phone." [7]. The development of mobile technology has caused great changes in the way people use mobile devices in their everyday lives. The rapid advancement in mobile commerce applications has transformed traditional banking services to form mobile banking activities. Mobile banking gives distinct, simple businesses and corporate customers rapid access to a diversity of products presented by financial organizations anywhere and at any time. users can access their accounts, do banking and bill payment transactions or receive information from different access devices such as mobile phones or PDAs. Almost 28 percent of mobile phone users in the survey report that they utilized mobile banking in the past 12 months [7]. Worries about the security of mobile banking stay one of the principal problems to more adoption. Moreover, consumers reported less trust in the security of mobile banking in the 2012 survey than they did in the 2011 survey [7].In the paper directed by the Federal Reserve, 48% of interviewees said their most important reason for not using mobile banking was "I'm concerned about the security of mobile banking". Information Security is most important priority to the business of mobile banking and its basic operations. Thus, technology used for mobile banking must be invulnerable and should ensure confidentiality, integrity, credibility and non-repudiation [8].

This research includes the following contributions:

- Benefits of mobile banking
- Security in mobile banking
- Security protocol design for mobile banking
- Conclusion

II. BENEFITS OF MOBILE BANKING

Mobile banking enables customers to do their banking activities everywhere, any time and at a cheaper manner and they do not have to go to a branch anymore. Mobile banking increases the advantages which electronic banking offers to the bank .A paper describes mobile banking services as reorganized version of existing banking services. The most important success factors of mobile trade are its accessibility, trust, and ease of use [2]. Let us review some benefits that banking mobile applications provide:

- Time efficient: Whereas paying visits to banks is no longer necessary, it saves up on time for a customer.
- Easy to use: The banking mobile applications are implemented in such a way as will allow even a non-technical customer to direct financial operations anytime and from anywhere.
- Reduces overall cost undertake by customer: The financial companies present mobile banking services as cheaper than what the customer would have to undertake if he/she had to be involved in normal banking transactions where visiting the financial company would be required.

- Mobile banking is more suitable than internet banking: The appearance of banking mobile applications has transformed the face of banking similar even internet facilities could not. This is due to the fact that in the case of the recent, having a computer with an internet connection is essential. But in the earlier, just having a smartphone is enough. The cost is lower in the case of banking with the help of mobile applications; in addition, the system is moreover portable.

III. SECURITY IN MOBILE BANKING

With the rapid development of mobile Internet, mobile technology is potentially vulnerable to an increasing number of malicious threats [9]. A customer should be able to rely on a mobile application producer that his or her credit or debit card information cannot be abused. Also, when these transactions become documented customer privacy must not be missing in the sense that the credit histories and spending methods of the customer must not be in public available for public investigation. Mobile payments have to be as unnamed as cash transactions. In addition, the system should be preserved from error and failure, unaffected by attacks from hackers and terrorists. This can be given utilizing public key infrastructure security passwords consolidated into the mobile payment architectures.

A. Risks Related To Mobile Banking For The Customers

- Risks in mobile device:
    - SMS are not encrypted form
    - SMS spoofing attack
    - Less storage capacity
    - Implementing complex cryptography is difficult
    - Hacker can get password from stolen devices
    - Slow processing speed makes a loophole
    - Digital signature is computational intensive and a signed template can be used with several unsigned values like date, amount etc.
- Risks in wireless application protocol (wap) :
    - Attacker can access unencrypted data
    - During switching of protocol process at gateway the data is not encrypted form
    - Modification or eavesdropping attack
- Risks in latest technology
    - Bluetooth: External protection is needed for detecting malicious
    - NFC: Non reputation problem
- Risks in server (bank system)
    - Server failure
    - System crash
    - Virus attacks
    - Malevolent intrusion

B. Some Common Security Threats For Mobile Banking

- Security issues related to WAP: WAP is applied for communication between devices similar to mobile phones, internet, etc. Encryption operation is lately utilized for secure data sending between bank and customers but the problem is that this encryption operation is not satisfactory enough for the protection of sensitive data between bank and customer. The reason is that mobile device have little computational capacity and therefore we can not to use complex cryptographic system [3].
- Password for identification: The security mechanism selected by the banks confronted various security issues like being attacked by unauthorized users which is of highest priority in security measures. If the device is lost then the hackers or unauthorized individuals can discover the password from the log files or saved draft files. A large number customers save their password in their mobile or they may maintain the password under auto fill settings of the form, this hole may be easily applied by the unauthorized person. Unlearned people are less informed of these issues and so cause loss of trust by customers [4].
- Password for recognition third party enrollment in mobile banking application: There is no confidence [5] in securing the data of customers such as bank account features and customer addresses as they are supervised by 3rd party service provider. Thus customer imagines no security to share their password and details to the stranger 3rd party.
- SMS based mobile banking: The primary good points of SMS are the facility and easiness to use. Because of plain text property, SMS is not acceptable for authentication. Thus shortage of privacy, integrity and security are the chief issues involve in SMS banking [6].
- Malware: Malware or malevolent software can find its way to the mobile device of a customer. malware may damage a mobile device or lead to damage to the owner without the owner's satisfaction. Instances of malware are viruses, worms, spyware, Trojan Horses, etc.
- Denial of Service: A denial of service attack is an attack that drowns a device so that all the resources are consumed thus that normal activity is no more possible. A denial of service attack can be much against a mobile device which can lead to the battery to drain or consume its limited resources, for example it's CPU, memory, available port numbers or bandwidth. A denial of service attack could endanger the availability of a mobile device. Users are also incapable to do banking on their mobile device.
- Device or application malfunction: there are two types of malfunctions. Malfunction produced by the user by mistake or wrong configuration and malfunction of the application because of inconsistency between the application and platform.

Cases mentioned before could endanger the reliability, integrity and availability of the mobile security assets. The security assets we determined for mobile devices are: device, application, personal information.

IV. SECURITY PROTOCOL DESIGN FOR MOBILE BANKING

The mobile service environment has three primary performers such as the mobile device, mobile manager and the bank. The proposed security protocol allows mobile users to use the SIM based authentication mechanisms at the bank to access the mobile banking services. The most current technology relevant to mobile devices and related to wireless carriers this day is based on 2G technology and 3G technology standards.

- The mobile device has an over-the-air installed application that utilizes the SIM card as one of its security components. This application is named as the mobile bank application (MBA). MBA functionality is presented in figure 1.
- The mobile manager presents the authentication service using the triggering architecture as specified by the 3GPP specification [10].
- The banking services content is given by the services provider in agreement with the Web services.
- International Mobile Equipment Identity (IMEI): The unique identity of the mobile device and this is issued by the mobile device producer.

Figure 2 presents detailed description of our security protocol in the mobile banking.

1- The mobile device requests to download MBA. MBA is a mobile bank application and it establishes the mobile device communication with the bank. Unique ID caused unique identification for MBA and it is un-accessible to the device users.
2- The MBA is downloaded and installed into the mobile device.
3- Mobile manager will generate a new shared secret key (SSK) between the mobile device and the mobile manager. The SSK is generated in the device and mobile manager sends the RSSK as a reference to the shared secret key (SSK).
4- MBA generates the HIMPI and hashed sim serial number (HSSN) using an internal hash function.
5- The bank sends the RSSK to the mobile manager and requests the SSK then generates service token as the authentication confirmation.
6- The user requests service and it is sent to the bank.
7- The bank generates execution token and it delivers the service to the user.

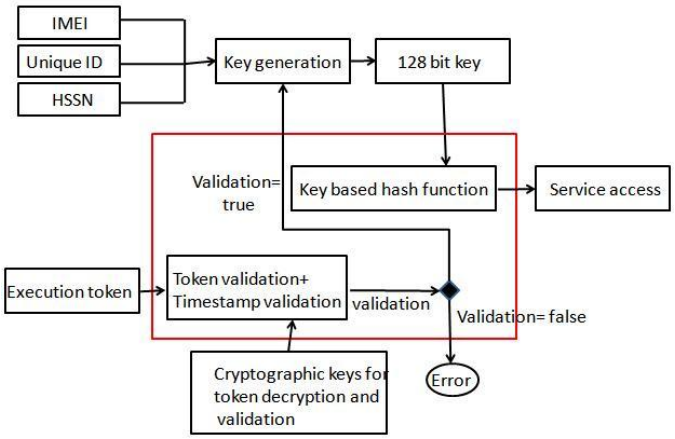

Figure 1. MBA functionality

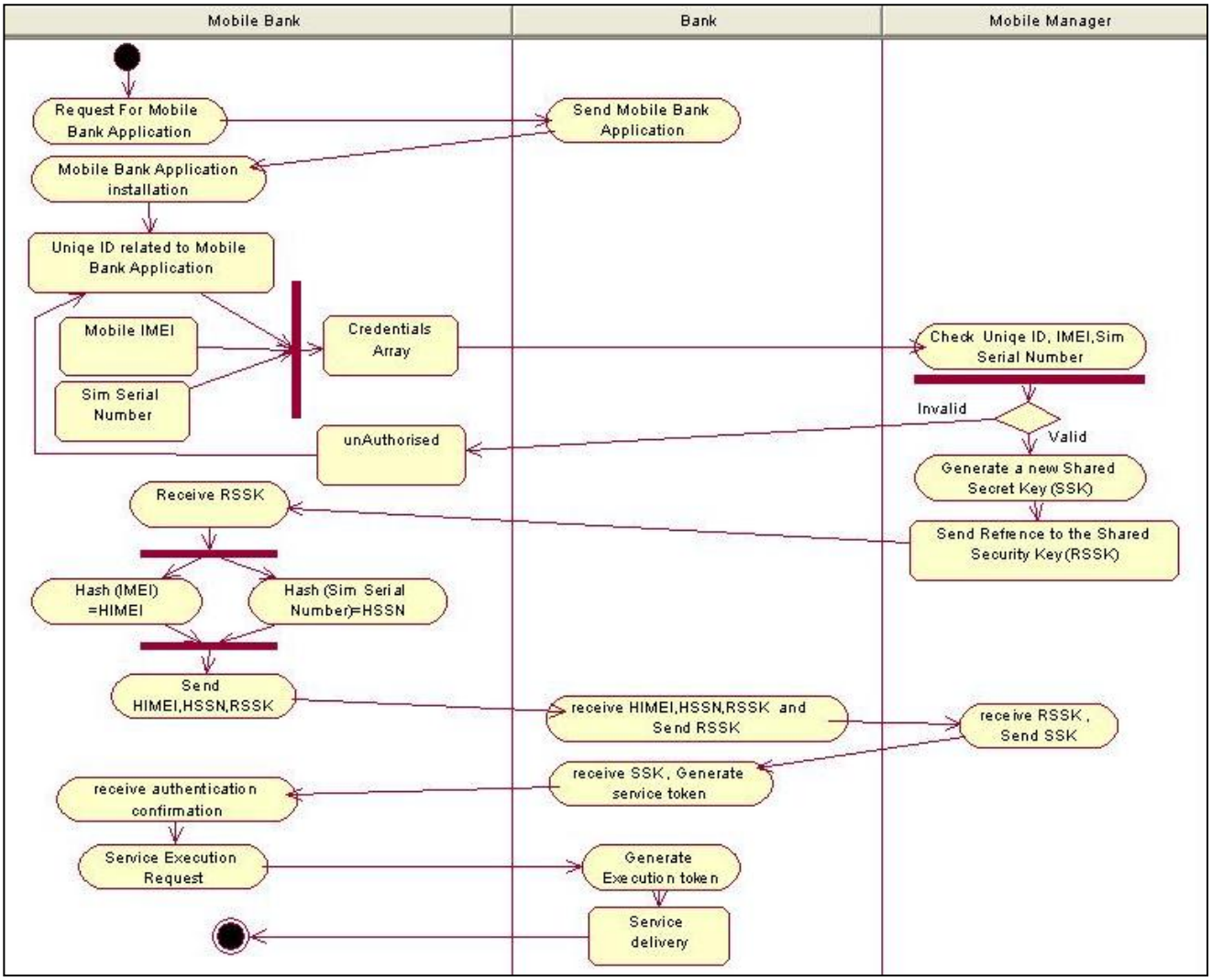

Figure 2. Security protocol design for mobile banking

V. CONCLUSION

A most important obstacle for the adoption of mobile banking technology and services is the awareness of lack of security. Understanding the mobile banking has high priority in addressing the security challenges. There are new security risks introduced with mobile banking and payments that identified. The research novelty discussed in this paper leads to a security protocol design for mobile users to access their banking services from anywhere. The current mobile banking solutions require number of user intrusive activities during the authentication but our solution presents effective and user friendly authentication solution for mobile devices. We have taken good care during the protocol design phase to reduce the complexity and size of the messages and tokens.

REFERENCES

[1] K. Siau, E.-P. Lim, and Z. Shen, "Mobile Commerce: Promises, Challenges and Research Agenda," ed: IGI Global, 2001, pp. 4-13.

[2] G. Xu and J. A. Gutierrez, "An Exploratory Study of Killer Applications and Critical Success Factors in M-Commerce", ed: IGI Global, 2006, pp.63-79.

[3] Jin Nie and Xianling Hu. Mobile Banking Information Security and Protection Methods, Computer Science and Software Engineering, 2008 International Conference , pp. 587-590, 2008.

[4] Suraj, sankaran, "Mobile Banking Architecture :Palisade", http://palisade.plynt.com / issues /2007May / mobile-banking / ,MAY, 2007.

[5] R. Fisher, Business aspects of trusted third party services in Europe, Information Technology Applications in Biomedicine, IT IS - ITAB ' 99. IEEE EMBS International Conference, pp. 38-39, 1999.

[6] S. Alam, H. Kabir, M. Sakib, A. Sazzad, C. Shahnaz, and S. Fattah, A secured electronic transaction scheme for mobile banking Bangladesh incorporating digital watermarking, *Information Theory and Information*

Security (ICITIS), 2010 IEEE International Conference on, pp. 98-102, 2010.

[7] D. Buchholz,A. Cavazos-Wright, "Consumers andMobile Financial Services 2013", Board of Governors of the Federal Reserve System, Washington, DC 20551 , 2013.

[8] V. Chugh, "Master Circular - Mobile Banking Tansactions in India - Operative Guidelines for Banks",2013.

[9] V. Pegueros, "Security of Mobile Banking and Payments", SANS Institute InfoSec Reading Room, 2012.

[10] Davis, A., 2011, Securing consumer devices. *Information Security Forum*, (April). Esmaili, E. et al., 2011. The Role of Trust and Other Behavioral Intention Determinants on Intention toward Using Internet Banking. *International Journal of Innovation, Management and Technology*, 2(1), pp.95-100. Available at: http://www.ijimt.org/papers/111-E00102.pdf [Accessed January 3, 2012].

[11] M. Elkhodr, "A Proposal to Improve the Security of Mobile Banking Applications", 2012 Tenth International Conference on ICT and Knowledge Engineering, 2012.

[12] C. Jianmin, " Research on Behavior-based Detection Method for Mobile Application Security", 2012 International Conference on Industrial Control and Electronics Engineering, 2012.

[13] V. Goyal, D. Pandey, "Mobile Banking in India: Practices,Challenges and Security Issues", International Journal of Advanced Trends in Computer Science and Engineering, 2012.

[14] D. Weerasinghe, V.Rakocevic, M. Rajarajan, "Security Framework for Mobile Banking", book chapter, 2013.

[15] I. Ashraf, "Mobile Banking Security", Post Graduate IT Audit - Vrije Universiteit, Amsterdam Student number 2043068 Thesis number 1073 The Hague, The Netherlands, April 2012.