The role and the application of cryptography in the realization of electronic transactions in m-banking

Florim Idrizi, Ilia Ninka

Abstract— Banking systems are one of the most complex systems in the field of information technology, where besides their functionality, speed, optimization and auditing, it is required a high level of security. This is expressed more in situations where the interaction with customers is obligatory, such as balance check, checking the executed invoices, etc. In this way, data security ensures privacy and the protection of personal data. Frequently, data is exposed to a threat by users who are not supposed to be. In this article we will explain the cryptography role in mobile banking by analyzing the enhancement of security in electronic transactions execution through cell phones. Further, we propose an idea for implementing new application using authentication parameters, such as, username and password, and an additional parameter of SIM card, where the encryption and decryption of messages takes place.

Index Terms— Mobile baking, cryptography, SIM card, encryption, decryption

1 Introduction

A key area of concern for consumers and financial service providers is the security of mobile banking and payments. There are new technologies and new entrants as well as a complex supply chain that will increase the security risks. There is no real standard for technology that has captured the market and regulations relative some of the new entrants are non-existent. Customers have increased control of their device in terms of application downloads, OS updates and personalization of their devices. This will lead to new challenges relative to privacy and will take some time before the younger generation realizes the implications of privacy violations. Compounding the challenge is the fact that traditional security controls such as AV, firewalls, and encryption have not reached the level of maturity needed in the mobile space [1].

Mobile banking is a way for the customer to perform banking actions on his or her cell phone or other mobile device. It is a quite popular method of banking that fits in well with a busy, technologically oriented lifestyle. It might also be referred to as M-banking or SMS banking.

The amount of banking you are able to do on your cell phone varies depending on the banking institution you use. Some banks offer only the option of text alerts, which are messages sent to your cell phone that alert you to activity on your account such as deposits, withdrawals, and ATM or credit card use. This is the most basic type of mobile banking.A more involved type of mobile banking allows the user to log into his or her account from a cell phone, and then use the phone to make payments, check balances, transfer money between accounts, notify the bank of a lost or stolen credit card, stop payment on a check, receive a new PIN, or view a monthly statement, among other transactions. This type of banking is meant to be more convenient for the consumer than having to physically go into a bank, log on from their home computer, or make a phone call. While all of this is true, some are concerned about the security of mobile banking[2].

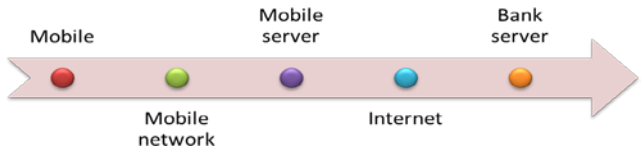

Fig. 1. Archtecture mobile Baking.

2 Mobile-Commerce Advantages and Disadvantages

- Mobile commerce involves all kind of electronic transactions by the use of mobile phone.
- By the use of mobile commerce enterprises can improve and widen their market reach, cut down on cost and give customers better service
- Users can benefit from m-commerce by the convenience the m-commerce provide to them and organizing personal data
- Examples of m-commerce are mobile parking meter

payments and buying ringtones and games online.

- Those kind of services are recognized as Micropayments: any transaction cost lower than $10
- High value purchases such as land, houses and cars will be more convenient in the future [3]
- It saves time, It saves energy, A person can easily locate the mall via GPS It can be carried anywhere and anytime, A person can text and email the shop and ask questions about it.

Disadvantages of m-commerce:

- Consumers fear for their privacy.
- Easier for information to get stolen.
- It has taken a while for businesses/consumers to accept m-commerce
- It prevents face-to-face customer service.
- Not all cellphones are capable of m-commerce yet.

3 Mobile user requirements

- Ubiquity: Mobile users must have the ability to receive information and perform transactions in realtime, regardless of location. M-Commerce can be present in any location or several places simultaneously.
- Personalization: The huge amount of information, services and applications presented on the Internet is of great importance, but users of mobile devices require different services and applications that should be personalized according to their preferences.
- Flexibility: Users of mobile devices should be able to engage in activities such as, receiving information, and conducting transactions with ease.
- Localization: Mobile users should have access to local information and services. This can be accomplished by having service providers know the location of mobile users in order to promote their products and services directly to their customers in a local environment[8].

4 Mobile Payment Authentication

Public key cryptography is considered as a preferred architecture for mobile commerce and banking. The most notable illustration for this is Visa Three Domain Secure (3-D Secure) specification. Its architecture relies on the issuer's ability to authenticate a remote cardholder by a pre-determined mechanism, where necessary data may be collected during the enrollment process. The 3-D. Secure Wireless Authentication Scenarios specification presents several authentication methods relevant for the wireless environment, including shared secret, signature and biometrics. The most secure scenario is that of a signature, that relies on public key cryptography.Proximity transactions are also regarded as a future application of wireless phones[9].

5 Digital Signatures on Mobile Transactions

Digital signatures make public key cryptography a most practical tool in real-life applications, being the most reliable method for authentication and nonrepudiation. As , digital signatures are expected to become a fundamental element of mobile devices business applications, as they already are being used for signing transactions, taking place in online banking and payment applications. A new concept for mobile transactions is called actionable alerts. These are constructed by a service provider sending a message to the mobile user, and the mobile user responding with an alert. A secure version of actionable alerts application, based on digital signatures and encryption, allows the banks to facilitate mobile platforms to secure banking transactions. Similarly, other procurement transactions may be secured by engaging digital signatures, where the mobile user signs documents such as a contract, NDA, MOU, RFP, bids etc[9].

6 Telephone banking system

Phone banking is the provision of banking services using a classic telephone line. A bank client can obtain the necessary information on dialing a telephone number specified in advance. Before the requested banking service information is provided, the client's identity is determined using contractually agreed terms. Using this banking service enables bank clients to obtain information concerning active and passive banking products, but a client can also actively use the bank payment system and request, for example, a payment order or a collection order, open or cancel a term deposit or a current account. In this case a fax connected to the telephone serves as an output communication channel. The client advisor or so-called telephone banker is a bank employee capable of providing any information about products and services and, follow-

ing verification that he is speaking with an authorized person, can also perform any passive or active operation. He can provide advice to the client and offer further banking products.
One advantage of this service is that it requires no additional technical equipment apart from a telephone. As a rule bank telephone center (call center) operators work 24 hours a day nonstop and it is thus possible to use their services from any place at any time[7].

7 SMS BANKING

SMS banking uses short text messages sent through the client's mobile phone. SMS text messages can be used for both passive and active operations similarly as with classic telephone banking. A client can automatically receive information about his account balance: an SMS is sent to the client immediately after a certain operation is performed, or on request: a client sends the bank a correctly formatted message which processes it and answers the client's request by SMS. Information sent on request mostly concerns current interest rates or currency exchange rates. Providing these is simple for the bank because this is publicly accessible information that needs no protection. A client however can request information about the balance in his account, which is not public information and must be protected when it is provided. Passwords are
used for this purpose or technologies based on the principle of an electronic key. A client however is required to know the code of every transaction including constant and variable symbols. The whole message containing data separated by # symbols sometimes has up to fifty characters. Users can easily make mistakes. This is frequently a limiting factor for clients, reducing the comfort factor in this service[7].

7.1 SMS encryption

As default data format for SMS is plaintext. Currently end to end encryption is not available. The only encryption involved at base transceiver station and SMS bank server during transmission. The encryption algorithm used is A5 which is proven to be defenseless [10].

7.2 SMS Spoofing Attack

The most dangerous attack in SMS banking is spoofing attack where attacker can send messages on network by manipulating sender's number. Due to spoofing attack, most of the organizations are not adopting mobile banking through SMS [11].

7.3 Virus Attacks in mobile banking

There are more than fifty thousand different types of computer viruses, internet malicious program and Trojans [12]. Software like Trojan horses can easily take up password on the web browser or any cached information on operating system. Malicious codes are written for remote
communication [13]. Zeus Trojan targeted mobile bank users. Zitmo has been used by attackers to defect SMS banking. Zeus is commonly used to steal mobile transaction authentication number or password [14].

8. APPLYING CRYPTOGRAPHY IN MOBILE BANKING

The massive usage of smartphones and tablet PCs raises the need for creating mobile banking operations, where special mobile applications are needed by users to be downloaded. Thus, in mobile banking the number of channels must be equal to the number of clients that use mobile banking.
Our proposal is based on encryption and decryption of the message being sent to the central banking system (invoice execution), and received by the core banking system (balance chenking). With the use of authentication parameters, such as, username and password and the parameter of SIM card, we will encrypt and decrypt the messages that are sent and received from the bank.
The SIM card has some unified parameters, such as, ICCID and K(i), that are needed for authentication of the customer.
Ki or the authentication key is a 128 bit data used during the authentication process and the process of generating the coding key. Every SIM card comprises of an unique key provided by the provider, which is used for authorizing the card in the GSM network. Here, the most important role of the key will be its optimal use as a private key in the process of encoding the messages. ICCID identificator is made of seven data fragments:

- Provider identity
- State code
- Network code
- Fabrication month and year
- Configuration switch code
- SIM card number
- Control digit

The main idea:

a) The client

Encryption and decryption will be realized with these three parameters:

- Username and password (together form one encryption parameter)
- PoashtuSalt, which will be generated in random manner and will be sent as public key

- ICCID or Ki, which will be taken by the SIM card

b) The bank

Encryption and decryption will be performed with the same parameters. The difference is only to the third parameter whereby the username and password will be received by the respective provider, (there is no need for new protocol here, because banks already use services by providers. One such example is filling credits to prepaid customers through ATM machines).

9 CONCLUSIONS

Performing transaction through mobile banking is a new concept and is under development. What is important here is that the number of channels must be equal to the number of clients that use mobile banking. In this article we provided an explanation of cryptographic concepts applied for execution in the online transactions in m-banking. Afterwards, we proposed an idea for implementing new application using authentication parameters, such as, username and password, and an additional parameter of SIM card, where the encryption and decryption of messages takes place.

REFERENCES

[1] Security of Mobile Banking and Payments, Vanessa Pegueros, November 1, 2012, SANS Institute InfoSec Reading Room

[2] http://www.wisegeek.com/what-is-mobile-banking.htm

[3] A. S. Andreou, C. Chrysostomou, C. Leonidou, S. Mavromoustakos, A. Pitsillides, G. Samaras, C. Schizas, (MOBILE COMMERCE APPLICATIONS AND SERVICES: A DESIGN AND DEVELOPMENT APPROACH),(2003).

[4] Mark S. Ackerman and Donald T. Davis, Jr. Privacy and Security Issues in E-Commerce, (2008).

[5] Journal of Theoretical and Applied Electronic Commerce Research, (Special Issue on M-Commerce), AUGUST (2007).

[6] M-Commerce and its Security Issues - By SAMEER YADAV (2001).

[7] FORMS OF ELECTRONIC BANKING, Ing. Adriana Chovanová, PhD, BANKING SECTOR

[8] Mobile commerce applications and services: a design and development approach, A. S. Andreou, C. Chrysostomou, C. Leonidou, S. Mavromoustakos, A. Pitsillides, G. Samaras, C. Schizas

[9] Using Public Key Cryptography in Mobile Phones, http://discretix.com/wpcontent/uploads/2013/02/Using_Public_Key_Cryptography_in_Mobile_Phones.pdf

[10] C. Narendiran, S. Rabara, and N. Rajendran, —Performance evaluation on end-to-end security architecture for mobile banking system, ‖ W ireless D ays, 2008. W D '08. 1st IF IP, pp. 1-5,2008

[11] H. Harb, H. Farahat, and M. Ezz. SecureSMSPay: Secure SMS Mobile Payment model, Anti - counterfeiting, Security and Identification ASID, pp. 11- 17,2008

[12] [12] T. Wilson, — Malicious mobile ode, ‖ Internet Business, pp. 52-3, Feb.1999.

[13] F. de la Puente, S. Gonzalez, and J. Sandoval. Virus attack to the PC bank, Security Technology ,Proceedings. IEEE 33 rd Annual 1999 International Carnahan Conference , pp. 304-310,1999.

[14] T. Holz, M.Engelberth, F. Freiling," Learning More about the Underground Economy", ESORICS 2009, LNCS 5789, pp. 1–18, 2009