International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

INSECURE GSM NETWORK AND SECURITY SOLUTIONS FOR MOBILE BANKING

Karun Madan, Surya World Institute of Engg. & Technology, Rajpura, Punjab

ABSTRACT

Out of the many revolutions in the current world, mobile banking is a new handy scheme for customers to carry out banking transactions without concerns about the location boundary. The usages of mobile banking are predicted to multiply as the number of cellular phone users are increasing day by day and mobile usage are foreseen to revolutionize payment banking for almost every fields and industries world-wide. But the fact is that the security architecture for cellular network is not totally secure. GSM (Global System for Mobile communication) network infrastructure, at times, was proven to be insecure and many possible types of attacks have been discovered and protection cautions were not considered at times, therefore sending protective banking information across wide open mobile phone network is totally insecure.

INTRODUCTION

In the last decade, a new trend has been developed in the banking sector as the number of online banking users has increased at a brisk rate. This has given an important work to developers investigate on more convenient as well as secure methods for bank customers to perform financial transactions.

As mobile banking becoming increasingly prevalent in last decade, still there are security issues within mobile banking by using the cellular phone network (GSM)[1]. The goal of the researchers is to build portable device applications that ensure clients of the banks can securely send their banking information via the mobile network.

In this paper, we try to investigate security issues in each level of the mobile network standards. At each level, we are interested in investigating how messages are sent across from customer's cellular phone to mobile network. This includes the overall security architecture of mobile network, message encryptions etc[2]. We inspect the defects of securities within cellular networks, the current standards and practices for mobile banking around. We investigate the security in SMS banking and GPRS banking. For each of these solutions, focus on its economical advantages and disadvantages, along with its cost factor is also important consideration[3].

MEDIUM FOR BANKING TRANSACTIONS

Mobile banking service is a advancement of internet banking using cellular technology and the GSM network mainly a medium to transfer request over the wireless network[4]. The basic idea of mobile transactions is to provide a convenient and cost effective method for customers to pay and perform banking transactions.

MOBILE TRANSACTION ARCHITECTURE

The mobile transaction architecture comprises of these main components i.e. the client, the device and the mobile transaction provider. The client requests for the service, the device is the mobile handset which connects the client and the service provider through some wireless network, and the mobile transaction provider is a cellular operator, may be a bank[5]. Figure 1 below shows tha architecture of cellular phone transactions.

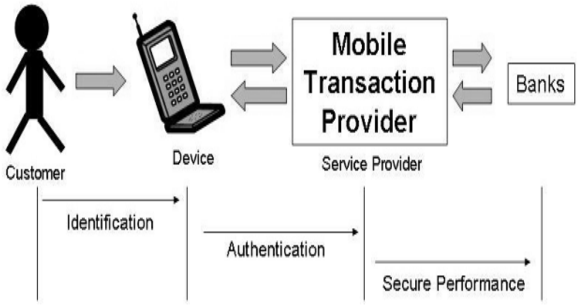


Figure 1. Modular Transaction Architecture with all three components

For a transaction to be safe and secure, it must consist of the following three modular processes[6]:

Identification, the user sends his unique id information to the server using a cellular device network for the process of verification. Identification component may consist of the user's password or any other bio-metrics information.

Authentication, the service provider will authenticate the transaction from customer via some identification process or any cryptographic mechanism.

Secure Performance, the transaction is actually performed on the service provider side. The service provider has the sole responsibility to ensure that the requested transaction from the customer is performed under the safe and secure environment and ensure a trustworthy protocol for payment transfer.

SMS BANKING SERVICES

GPRS based mobile banking is fairly new in most of the regions, with only most leading banks offering the service. Some banks have a similar kind of offering; they provide Mobile internet banking over GPRS and as well as EDGE technology[7]. Along with that their devices use HTTPS SSL 128-bit encryption for some mobile banking practices.

SMS COMMUNICATION PROTOCOL

A Security Mechanism for Secure SMS Communication is necessary as the current GSM network does not provide important security facilities like authentication, end-to-end security, non-repudiation[8]. In the GSM architecture standard, mobile SMS text content is sent over in normal text format or in a somewhat encrypted fragile format, which as a result, makes sensitive text messages sent across the network totally insecure. This enables an attacker with the right apparatus to eavesdrop on the information being sent, so a better SMS communication protocol is needed to send out text data between server and client.

It would be better, if we establishing an encrypted protocol connection by means of public keys and session keys between customers to the server. The client begins the connection by sending its username some secret number encrypted using the public key[9]. When the server receives the client message it is decrypted using the private key.

The server retrieves that secret number and username from the received message, and as a result retrieves the relative user PIN no. from its database; the server, then calculate a session key for the same client by using some hash functions[10]. As the session key is calculated, the server replies to and establishes connection with the customer.

The client then calculate the session key in parallel, as the client receives a reply from server, then a secure connection is established. The session key is generated by procedure like hashing the username, secret number and the shared PIN number as well[11]. Attackers cannot generate a session key with this procedure without knowing the PIN for the precise username. The secret value provides a more secure session key generation as the secret number is 128 bits long, it enhances difficulty for attacker to break the session key.

To check replays, a sequence number is used for that. This seq. number is incremented by one, each time as the message reaches the target. The client or the server may verify if SQ is incremented by one. In this way, protocol generates a secure communication channel between client and server using SMS. It also ensures confidentiality and integrity of SMS communication. But as a trade off, the encryption and keys generation root the protocol to operate very slowly and become the basis of inefficiency.

VOICE PATTERN AND BIO-METRIC SECURITY

Organizations can use alternative approach to provide security to their banking service like SMS alert, Person-to-Person alert payment, fund transfer, bill payment and etc. This approach uses a three layers security to attain protection against some fraud[12]. It needs the customer's SIM (Subscriber Identity Module), a PIN (chosen by the user) and the user's voice pattern. The transaction is dependent on these security measures. The customer's request is only when the user is authenticated by above process. These three layers of security offers a sole protection mechanism, the SIM card supply as a physical security key for the same, the PIN as a password security and along with that voice pattern verification that act as bio-metric security for the banking transaction.

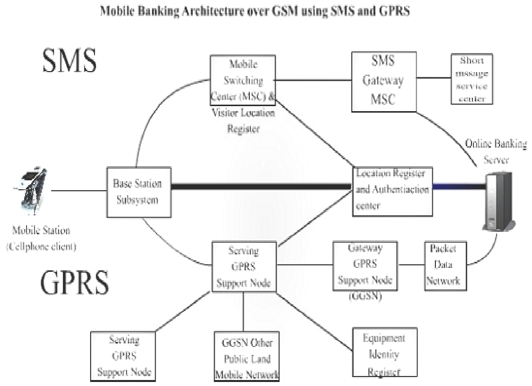
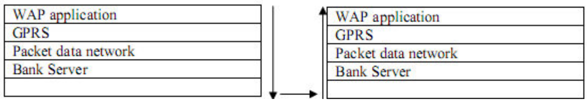

Mobile Banking Architecture over GSM using SMS and GPRS
SMS
Mobile Switching Center (MSC) & Visitor Location Register
SMS Gateway MSC
Short message service center
Online Banking Server
Base Station Subsystem
Location Register and Authentiaction center
Mobile Station (Cellphone client)
GPRS
Serving GPRS Support Node
Gateway GPRS Support Node (GGSN)
Packet Data Network
Serving GPRS Support Node
GGSN Other Public Land Mobile Network
Equipment Identity Register

Figure 2. Mobile banking architecture

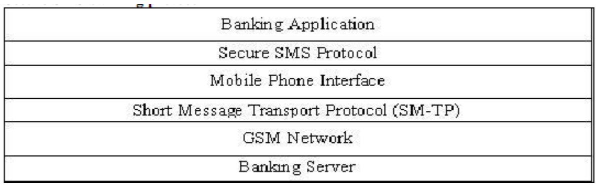
Figure 3 below shows a general banking GPRS protocol. secure banking protocol may be build on this protocol.



WAP application	WAP application
GPRS	GPRS
Packet data network	Packet data network
Bank Server	Bank Server

Figure 3.General GPRS banking protocol

Secure SMS banking protocol



Banking Application
Secure SMS Protocol
Mobile Phone Interface
Short Message Transport Protocol (SM-TP)
GSM Network
Banking Server

Figure 4. SMS banking protocol

Figure 4 above give you an idea about the overview layers of mobile banking by using SMS as communication protocol for the same.

- Banking Application is the application layer with which, the users interface work together with the bank server.
- Secure SMS protocol layer provides a secure exchange channel using SMS messages to transfer.
- Mobile phone interface is actually the cell phone specification specified by the mobile phone manufacturer.
- Short Message Transport Protocol layer is in fact specified by the GSM network, this layer is used to transmit SMS messages across the mobile network by using SM-RP (Short Message Rely Protocol) as well as SM-CP (Short Message Control Protocol).
- GSM network is the service provider for mobile phone.
- Banking server first authenticates users and accepts customer's banking transactions and then replies users with performed transaction status.

CONCLUSION & FUTURE WORK

In this paper, we have seen many security alternatives. One of the alternatives is to use a three layers security to attain protection against any kind of fraud. It requires the customer's SIM (Subscriber Identity Module) in mobile phone of customer, a PIN (chosen by the user) and the customer's voice pattern. The transaction is glued and dependent on these three security measures.

Another technique is suggested by establishing an encrypted protocol connection using some public keys and session keys between the clients to the server. The client commences the connection by sending encrypted information using the server's public key to that server. Server receives the client's encrypted message; it is decrypted by using the server's private key. The server finally retrieves the relative user PIN from its databas2.

Work has to be done to make a system from which, we expect to produce a completely secure protocol for every type of mobile banking transactions which will outfit all network security needs i.e. authentication, authorization, integrity, non repudiation, confidentiality, and access control. Based on the uncertainty of the existing protocol, we expect to produce tests and experiments that can unravel defects in existing mobile banking standards. Future work involves investigating the every possible alternative to mobile banking security, SMS banking, and how security objectives like confidentiality; integrity can be accomplished using these options.

REFERENCES

[1] Margrave, D. *GSM Security and Encryption.* Available from: http://www.hackcanada.com/blackcrawl/cell/gsm/gsmsecur/gsm-secur.html (1999); accessed 27 October 2006.

[2] Lord, S. 2003. Trouble at Telco: When GSM Goes Bad. Network Security. Issue 1, Page 10 -12.

[3] Cell phone Banking - How do I. (Website) https://www.fnb.co.za/personal/transact/accessyouraccounts/cellHowDoI.html

[4] Warwick, A. Banking via SMS. (Website) http://www.itweb.co.za/sections/business/2005/0503101110.asp?S=Telecoms&A=TEL&O=FRGN

[5] A. Chaia, A. Dalal, T. Goland, M. J. Gonzalez, J. Morduch, and R. Schiff. Half the world is unbanked. Financial Access Initiative Framing Note, Oct. 2009.

[6] Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison. Security of Mobile Banking

[7] Steve Lord, X-Force Security Assessment Services, and Internet: Trouble at the Telco When GSM goes bad. In *Network Security,* 2003(1):10 12, 2003

[8] Ratshinanga, H., Lo, J., Bishop, J. 2004. A Security Mechanism for Secure SMS Communication. Department of Computer Science, University of Pretoria, South Africa. (Online) http://polelo.cs.up.ac.za/papers/SecureSMS.pdf

[9] Herzberg, A. 2003. Payments and banking with mobile personal devices. Communications of the ACM .Volume 46, Issue 5 (May 2003) Wireless networking security Pages: 53 58 ISSN: 0001-0782

[10] MTN Banking - South Africa s first mobile bank runs on Fundamo. (Website) http://www.fundamo.com/index.asp?pgid=54

[11] INet-Bridge-Investec launches mobile banking. (Website) http://www.mybroadband.co.za

[12] Paul Vecchiatto and Tracy burrows - Mobile Internet banking spreads in SA