International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 3 Issue 1 2012

AN INVESTIGATION OF GSM ARCHITECTURE AND OVERLAYING WITH EFFICIENT SECURITY PROTOCOL

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

ABSTRACT

The Global System for Mobile Communications (GSM) network is a standard structure used by most of the mobile phone networks all around the world. According to facts gathered by an organization known as the GSM Association, approximately 80 percent of all mobile phones all around the world are branch of this network. In recent years, M-banking has emerged as the main division of e-commerce and m-commerce. Nowadays, Mobile banking services comprises of information inquiry, notifications as well as alerts, payment transfer etc. Mobile application handset is used for linking customer handset with the server of the bank for all above mentioned services. Present Mobile-banking applications used by most banks are facing security challenges basically due to the security architecture of GSM network. The security architecture of the cellular network is not completely secure. Global System for Mobile communication network infrastructure is proven to be unsafe and many types of possible attacks have been exposed. So that sending sensitive banking information

across the open mobile phone network is totally insecure.

In this paper, we first discuss GSM architecture and then present SMS based secure mobile banking approach which improves security with lowest possible cost. In this method bank hides customer transaction data via secure SMS using AES symmetric cryptographic algorithm. Customer application decrypts data in safe manner.

1. INTRODUCTION

In this project, first we investigate GSM architecture and then we will discuss security issues with the GSM architecture. Finally we will present method to improve security of M-banking using SMS based secure approach. The aim is to construct portable device applications that ensure client can securely send their banking information via the mobile network. The main

problem with the current mobile banking system is that they send data directly to clients in plain text form and compromising with the security.

Present M-banking applications used by most of the banks are facing security challenges for payment transfer[1]. Mostly banks are using secure payment gateway as well as security measures, which increases their cost and infrastructure for their bank. But major day-to-day banking activities are not only payment transfer but inquiries, notifications and alerts as well.

In section 2, we discuss GSM architecture and then in section 3, we will present security mechanisms in the GSM network. In section 4, we will present SMS based secure mobile banking approach to improve security on this GSM architecture.

2. GSM ARCHITECTURE

As earlier stated, According to facts gathered by an organization known as the GSM Association, approximately 80 percent of all mobile phones all around the world are branch of this network. Phones on this type of GSM network actually use a Subscriber Identity Module (SIM) card. One of the main objectives of the GSM network is to facilitate effortless access to cellular and satellite systems across international lines.

Using present digital technology, it makes use of both speech and data channels [2]. Figure 1 shows the fundamental structure of the GSM architecture; GSM offers both SMS and GPRS services.

The GPRS is an integrated part of basic GSM network; it is encrusted over the underlying GSM network. GPRS also employ some of the already offered GSM network elements like Mobile Switching Centers (MSC), Base Station Subsystems (BSS), Home Location Registers (HLR) and Authentication Centers (AUC).

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 3 Issue 1 2012

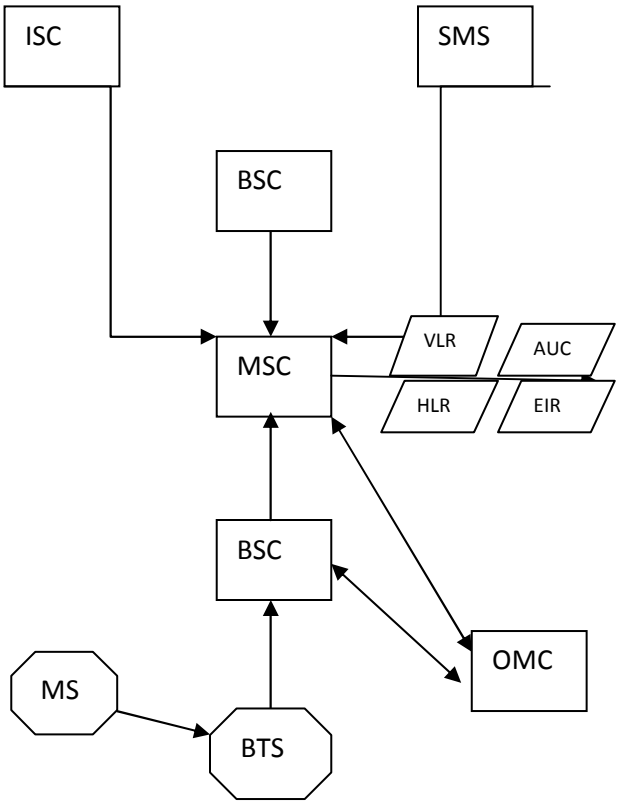


Figure 1. GSM Architecture

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 3 Issue 1 2012

BSC – BASE STATION COTROLLER

MSC – MOBILE SWITCH CENTRE

OMC- OPERATION AND MANAGEMENT CENTRE

MS - MOBILE STATION

BTS - BASE TRANSCEIVER STATION

SMSC – SHORT MESSAGE SERVICE CENTRE

ISC – INTERNATIONAL SWITCHING CENTRE

EIR- EQUIPMENT IDENTITITY REGISTER

AUC- AUTHENTICATION CENTRE

HLR – HOME LOCATION REGISTRY

VLR - VISITOR LOCATION REGISTRY

Key Terms

The supplementary GPRS network elements to the already existing GSM network include; GPRS tunneling protocol (GTP), GPRS Support Nodes (GSN), (Packet Data Protocol) PDP Context as well as Access points.

3 SECURITY MECHANISMS IN THE GSM NETWORK

GSM has techniques to authenticate and encrypt data exchanged on GSM network. The GSM network has some safety mechanism to check activities like Subscriber Interface Module (SIM) cloning, and to put off unlawfully used handsets.

3.1 GSM Authentication Center

The SIM card authentication is performed when a mobile station in the beginning attempts to connect to the network, or in other words, when a terminal is switched on. The GSM authentication center is in operation to authenticate each SIM card which makes an attempt to

connect to GSM network. If in case, authentication fails then no services will be offered by the GSM network operator, otherwise the SGSN and HLR are allowed to administer the services associated with the SIM card.

3.2 Problems with the A3/A8 authentication algorithm

A3/A8 is the algorithm used to authenticate a handset on a mobile network. In A3/ A8 the generally used algorithm is COMP128[3]. COMP128 was cracked by Wagner and Goldberg almost effortlessly. This raises apprehension of having GPRS as a secure mechanism. By cracking COMP128 Wagner and Goldberg proved that it is possible to attain the Ki value, so making it possible to achieve SIM cloning[4]. There has been a publish of COMP128-2 and COMP128-3 to deal with the SIM cloning issues, but still, the majority of the SIMs are using COMP 128.

3.3 Problems with A5 algorithm

To prevent unfussy eavesdropping by encrypting the communications between mobile station (handset) and the BSS, the A5 algorithm is used. Kc is actually the Ki and RAND value put into the A5 algorithm[5]. This Kc value is basically a secret key used along with A5 algorithm for encryption in between the mobile station and BSS.

4. SMS SOLUTION FOR SECURE BANKING

The secure messaging protocol overcomes the on hand security deficits in the GSM architecture. The solution for the above mentioned problems is to impart a secure messaging protocol which actually uses SMS. The secure messaging protocol has been integrated along with mobile banking system to improve the security of M-banking.

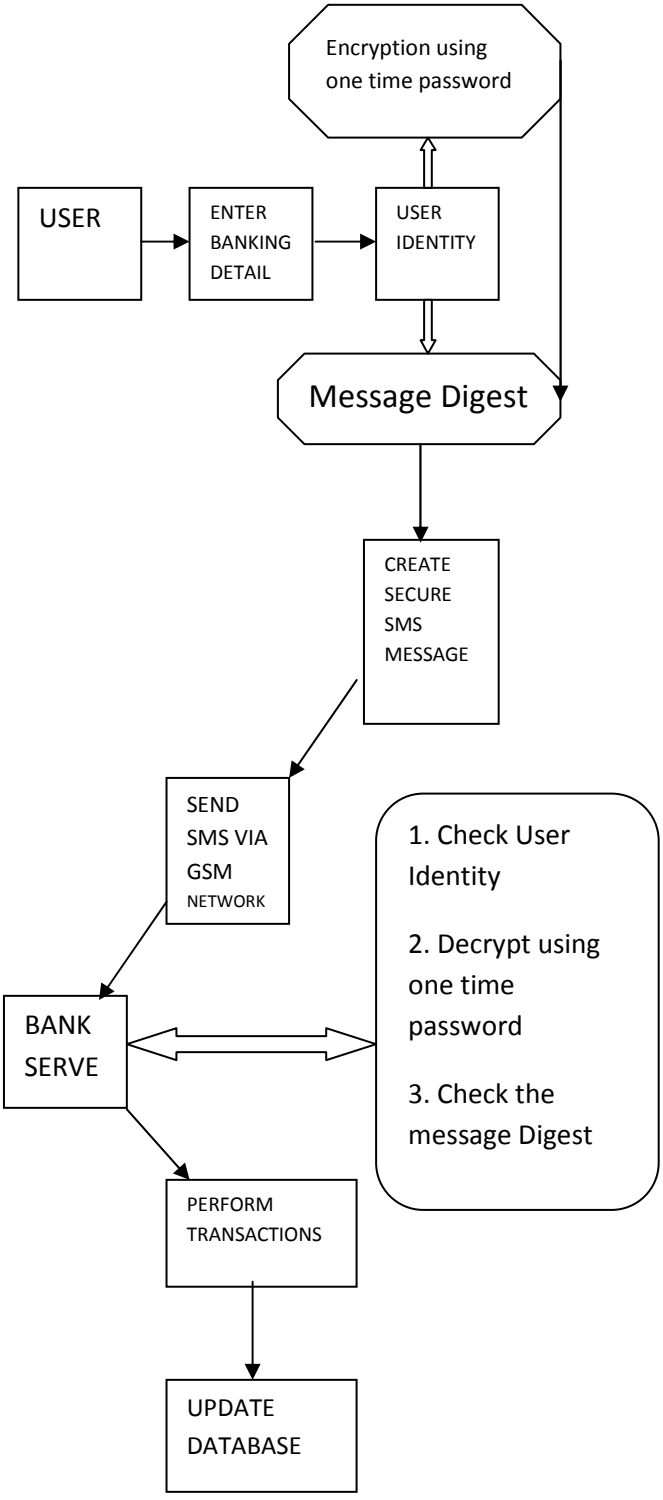
4.1 Protocol Sequences

Secure SMS protocol is basically divided in two parts[6]. The first part is mainly message generation. The mobile handset generates the message and sends it to the server of the bank. The second part is basically message security checks. The server of the bank, examines the received message, decodes the contents, present in it and carries out security checks. The subsequent subsections describe each part of the protocol in detail.

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 3 Issue 1 2012



International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 3 Issue 1 2012

4.2 Generating and Sending Secure SMS Messages

User put all the required security information in mobile device. This information is used to create the secure SMS message for sending to the server. The mobile device has a preset version pattern of bytes[7]. This pattern is also inserted while creating the message.

Hash value can ensure message integrity for the receiver side of the link[8]. Message integrity is needed to encrypt contents that are used for computing the message digest.

Now the message is intercepted and the intruder cannot use the encrypted contents to construct another digest. The integrity validation will not pass if any part of the original message is altered. Some identification details should not be encrypted to let the receiver identify the account holder.

The key used in this algorithm, for encryption is constructed from the one-time password of the client[9]. Only the server and the user have the knowledge of one-time passwords.

Figure 2. SMS based Protocol

4.3 Receiving and Decoding Secure SMS Message

After receiving the message, server breaks the message and first checks the pattern of the version bytes. By doing this server come to know that message is fit for the secure SMS protocol[10]. Next, the server checks if the account identifier is exist in the server database as well.

Now the server recovers the sequence number and checks if the sequence number recovered from the message matches with the seq. no. from the server's database. Now server gets the one-time password from the database.

This password is indexed by sequence number and the account identifier. So the server uses this password as the decryption key to decipher the encrypted contents. After successful decryption, one-time password is discarded[11]. After all this, the server uses the secure contents required for the computing message digest.

The message digest is computed using the same algorithm as used by mobile device. Now server compares the two digests for checking the message integrity[12]. After this, server takes the PIN from the message and then compares it with the account holder's PIN from the server's database. The server performs the requested transaction after all the above mentioned security checks.

5. CONCLUSION & FUTURE WORK

There are many fields that would benefit from SMS based security measures. Security solutions were restricted because of physical infrastructure of GSM network. The security architecture of the cellular network is not completely secure, as we have seen so many loopholes in the GSM architecture. Many of the inherent disadvantages of such networks can be treated with the use of SMS based security. Secure SMS approach uses the concept of One time password, hashing function, PIN no. and message digest computing etc, to provide the clients secure transactions using mobile banking. Still a lot of work has to be done on the authentication process. In a nutshell, idea is to use secured messages over GSM networks in mobile banking without worrying about security concerns in order to take full advantage of the facility provided by the banking sector.

6. REFERENCES

[1] Manoj V, Bramhe. Sms based Secure Mobile Banking. In International Journal of Engineering and Technology Vol.3 (6), 2011, 472-479

[2] Kelvin Chikomo and Ming Ki Chong. Security of mobile banking Project proposal

[3] Biryukov, A. Shamir, A. Wagner, D. Real Time Cryptanalysis of A5/1 on a PC. In *Fast Software Encryption Workshop,* 2000 Stallings, W. *Network Security Essentials Applications and Standards, international second ed.* Prentice Hall, 2003.

[4] 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

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

[6] SMSSpoofing: Everything you ever wanted to know about SMS spoofing. http://www.smsspoofing.com , 2008.

[7] Burak Bayoglu: Performance evaluation of WTLS handshake protocol using RAS and elliptic curve cryptosystems, 2004

[8]. Wagner, D. *GSM Cloning.* Smartcard Developer Association and ISAAC security research group. Available from: http://www.isaac.cs.berkeley.edu/isaac/gsm.html (1998); accessed 28 October 2006

[9] R. Chaudhri, G. Borriello, and W. Thies. FoneAstra: Making mobile phones smarter. In ACM Workshop on Networked Systems for Developing Regions. ACM, Oct. 2009

[10]. WAP Forum, Wireless Application Protocol Architecture Specification, Version 12-Jul-2001, from http://www.wapforum.org, 2001.

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

[12]. 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.