International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013
http://www.ijeemc.com

SECURE GPRS SOLUTION FOR MOBILE BANKING: AN EFFICIENT SECURITY PROTOCOL

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

ABSTRACT

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. 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[1]. Still a lot of work has to be done on the authentication process. As there are so many security issues in case of SMS approach, so banking world has to look around for some other measures. In this paper, we assess secure GPRS solution in mobile banking as security measure.

INTRODUCTION

Mobile banking is a new system for customers to perform transactions, and is predicted to increase more rapidly in future also. At the moment most of the banks provide mobile banking through these two channels: First, through the Wireless Application Protocol(WAP) over the General Packet Radio Service (GPRS) and Short Message Service(SMS) by means of Wireless Internet Gateway(WIG)[2]. Mobile banking is appealing as it is a convenient approach to perform banking transactions, but there are security shortfalls in current mobile banking implementations.

This paper discusses the GPRS based solutions for problems of security issues with GSM architecture[3]. These proposed solutions provide secure communications between the user's mobile application and bank servers. The solutions permit the users to bank using the secure SMS and GPRS.

As we know that security of banking transactions is not the issue, with which one can compromise. But the problem with GSM is that, without overlying security protocols over it, it has proven susceptible to many types of security attacks.

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013
http://www.ijeemc.com

As with GSM in mobile banking, most of the authentication as well as confidentiality procedures have been rifted[4]. As mobile banking is a new system for customers to perform transactions, which is by far a convenient method for banking transactions and this practice is going to increase more rapidly in future also. This has force us to the implementation of overlying protocols like WAP and WIG to impose the security of transporting information over GSM networks.

Most of the banks, nowadays have taken benefit of these protocols to secure transactions upto some extent. In this paper, idea is to use secured GPRS over GSM networks in mobile banking to knob security concerns.

MOBILE BANKING SECURE GPRS SOLUTION

To cure the security problems mentioned above, two effective solutions were proposed. The first solution is to impart the security features in the present WAP based implementations and the second solution is a totally new GPRS security protocol[5]. To offer the bank with full control of the WTLS protocol, the solution lets the bank customers attach to its bank network through a personalized WAP gateway which operates in its network realm[6]. The personalized WAP gateway disallows the following handshake alternative:

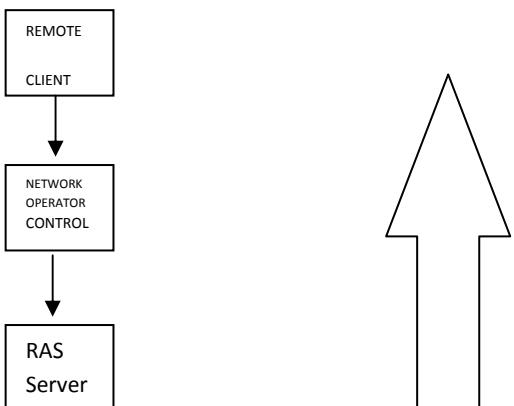
- Truncated handshake
- complete handshake Server authenticated
- Anonymous key exchange suites

NEW SECURE GPRS PROTOCOL

This Secure GPRS protocol is a tunneling procedure that is designed to look out of security in M-commerce applications. Protocol is used to create and conduct secure and safe connections between mobile devices as well as bank servers[7]. This Secure GPRS protocol comprises of two main components; an basic client server handshake and the second is, transfer of data packets (SGP record protocol) using the already created secure tunnel and exchanged cipher suites for the same[8]. Every SGP message sent between the client and server has total 3 components i.e. the message timestamp, message as well as the message type.

Figure shows the standard location of the WAP gateway for mobile banking.

Figure. Ideal WAP Gateway setup for the bank server



International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013
http://www.ijeemc.com

The message timestamp is utilized by both the client and server to avoid replay attacks, and the message type is again used by both the client and server to identify the message already sent[9]. Figure below shows this message structure.

Error message
Handshake message
Go-Ahead message

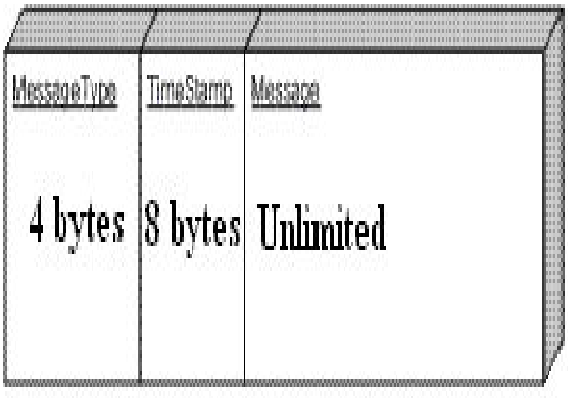


Figure .Structure of message sent

CLIENT PROTOCOL INITIALIZATION

When a client begins the mobile application, a one-time 512bits RSA key pair is created[10]. Once the keys have been created, the client sends its public key first to server.

These keys are used in the protocol to produce digital signatures for the client. These digital signatures are confirmed by the server using the sent client public key; and with this, authentication of the messages sent by the mobile client takes place.

User Authentication

The authentication takes place in fact in two different sections; the first authentication is done by the mobile device and then the second by the bank. When a user registers to make use of the banking service, a server certificate get signed using the client's password is included as part of the application.

To complete the client protocol initialization, the client produces a PBE AES session key by making use of the client's password. This certificate is plays important role to authenticate the account holder on the phone. When a user places a password, the phone application produces an AES key using this password.

By making use of this key, the application attempts to get back the server's public key in the server's certificate, if the server's public key is recovered successfully, then the starting client authentication is complete; else, the client is inquired to re-enter the password.

More importantly, the client is only allowed for three login attempts at the most; if the login fails in all the three attempts, the account is blocked for some finite time.

The succeeding user authentication is now done by the server; the client sends its

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013
http://www.ijeemc.com

encrypted client account ID to server[11]. The server then acquires the password from the database and re-creates the AES key again; if it can effectively decode the encrypted message then it means that the client is authenticated now.

Packing of SGP packet on Client-side

The SGP handshake engrosses packing and transporting a *Full SGP packet* to the server so that the server would able to successfully decode the message and produce session keys[11]. Figure below explains the packing of the *Full SGP packet in detail.*

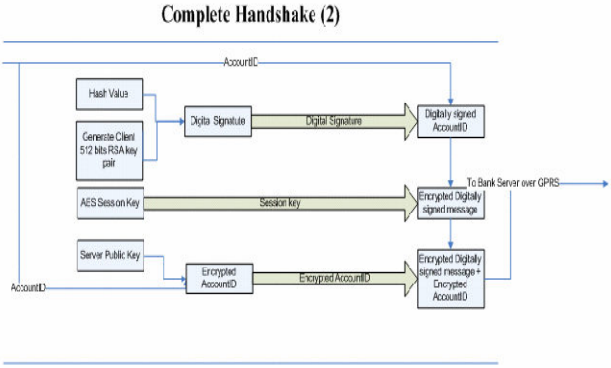


Figure. Packing of SGP message

Server Protocol initialization

When a server boot, it initializes the vital cipher parameters. Now administrator running the server must have to login using a password which is used to get back the server's private keys.

This must be done because all server private keys are get collected in the server's key-store marked using the administrator's password.

When a client makes a connection with the server, the first message the server gets, is the client's public key[11]. After getting the client's public key, the server expects to obtain the *Full SGP message.*

When the server obtains the full SGP message, it splits the message into the encrypted message digest as well as encrypted account ID.

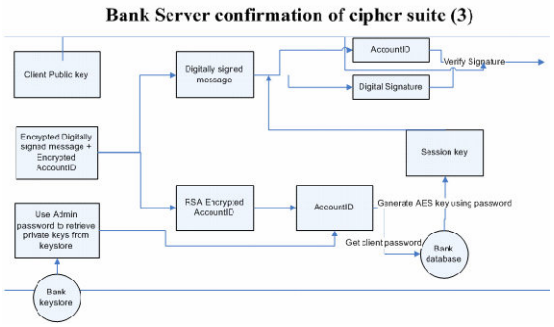


Figure. Server unpacking and verifying the Full SGP message

CONCLUSION & FUTURE WORK

As we have seen that security solutions were restricted because of physical infrastructure of GSM network. We have used GPRS protocol to generate secure connections between mobile devices and the banking servers. The Secure GPRS protocol formed up of two main components; an starting client server handshake and then the transfer of data packets (the SGP record protocol) using the

Volume 2 Issue 1 January 2013
http://www.ijeemc.com

already created secure tunnel and the exchanged cipher suites for the same. A lot of work has to be done on this field as mobile banking security is not a straightforward issue. By using this secured GPRS based protocol, we can take care of security concerns in mobile banking only up to some extent. So a lot of refinement needs to be done taking care of current cellular architecture.

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

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

[4]. 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

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

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

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

[8] 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.

[9] 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

[10]. A. Chaia, A. Dalal, T. Goland, M. J. Gonzalez, J. Morduch, and R. Schiff. Half the world is unbanked.

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013
http://www.ijeemc.com

Financial Access Initiative Framing Note, Oct. 2009.

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