International Journal of Computing and Business Research

ISSN (Online) : 2229-6166

Volume 2 Issue 2 May 2011

INADEQUACIES IN THE USE OF PRESENT MOBILE BANKING IMPLEMENTATIONS

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

ABSTRACT

In the recent years, the number of online banking users has increased swiftly. This has led many developers to investigate extra convenient methods for customers to perform mobile banking transactions. 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 over the General Packet Radio Service and Short Message Service by means of Wireless Internet Gateway. 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 some of the security deficits

1. INTRODUCTION

Mobile banking is actually very fascinating as customer can find it very convenient approach to perform banking transactions, but there are safety shortfalls in current mobile banking implementations. This paper discusses some of the security insufficiencies, such as security problems with the GSM network, GPRS protocols etc. This paper discusses the proposed solutions for these problems implementing SMS and GPRS. These proposed solutions provide secure communications between the user's mobile application and bank servers. The proposed solutions permit the users to bank using the secure SMS and GPRS. Many banks provide mobile banking through these two systems: through the Wireless Application Protocol via General Packet Radio Service and Short Message Service using the Wireless Internet Gateway. In this paper, we walk around the security fears in mobile banking implementations using Global System of Mobile network. The purpose of this plan is to build applications for the portable devices that ensure that users can securely perform transactions and can send banking information via the GSM network securely.

2 EXISTING SMS BANKING SERVICES

Nowadays most of the banks use the Wireless Internet Gateway for their mobile banking. Some banks use the Unstructured Supplementary Services Data along with the SMS approach. These banks requires the user to first send a USSD string along with the user's PIN to the server of the bank.[1] Then the server of the bank returns a message to report the user that the server is now ready to accept the banking SMS message. This approach is also not secure because every user's detail is transmitted in

International Journal of Computing and Business Research

ISSN (Online) : 2229-6166

Volume 2 Issue 2 May 2011

plaintext during this process. The mobile network operator has almost full access to these banking details sent by the user to bank.

3 SECURITY DILEMMAS WITH SMS

Actually, the preliminary idea for SMS usage was anticipated for the subscribers to send their non-sensitive messages across the wide open GSM network. Common authentication, plain text encryption, end-to-end security, non- refutation were lost during the design of GSM architecture [2]. In this section we argue some of the security problems using SMS approach.

3.1 Counterfeit Originator s Address

It is possible to amend the originator s address field in the SMS header to some other string. SMS spoofing is an attack that engross third party sending out SMS messages that look as if it is from a legit sender. It actually hides the original sender's address [3] and the sender can now send out hoax messages and performs masked attacks as per his wish.

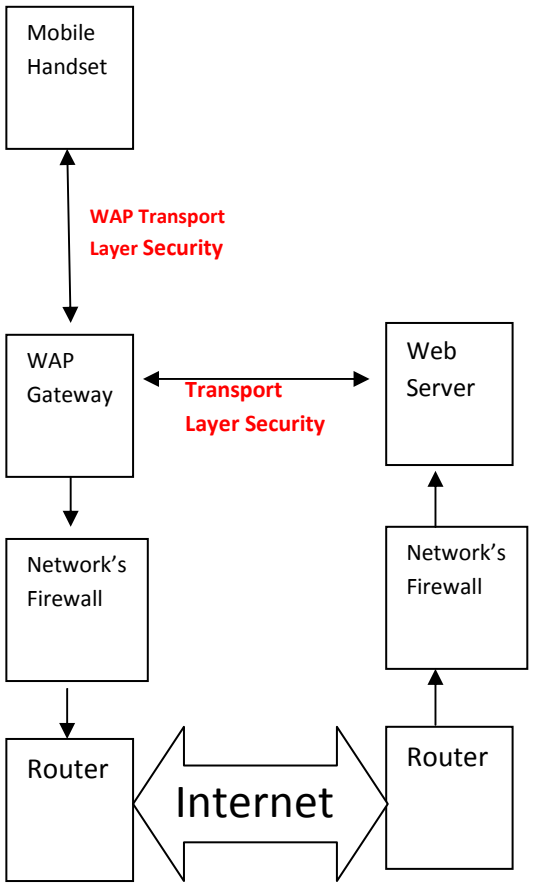
3.2 SMS Encryption

End to-end encryption is not available yet. The encryption algorithm used is A5 which is confirmed to be susceptible [3]. That's why, a more secure algorithm is needed. The for SMS message's default data format is also in plaintext. The only encryption engrossed during transmission is the encryption only between the base transceiver station and the mobile station.

4 EXISTING GPRS IMPLEMENTATION

4.1 Existing GPRS banking implementations

Nowadays some banks offer mobile banking using GPRS. Some banks are using the MTN mobile banking gateway. This MTN mobile banking allows the bank account holders to retrieve WAP sites and perform banking the similar way they would carry out internet banking for some purpose.



F f WAP to networks.

International Journal of Computing and Business Research

ISSN (Online) : 2229-6166

Volume 2 Issue 2 May 2011

4.2 Wireless Application Protocol (WAP)

Mobile terminals can access the internet using mostly WAP browsers; WAP browsers can only retrieve WAP sites. So instead of the usual HTML, XML or XHTML, WAP sites are constructed in Wireless Markup Language. WAP is an open international standard for all the applications that uses wireless communication. Its prime application is to facilitate access to the internet from a mobile phone [4]. The WAP protocol is only importunate from the client to the WAP gateway, and the connection from the WAP Gateway to the Bank Server is protected by either SSL or TLS.

WAP Transport Layer Security protocol and the WAP Identity Module is used by WAP to impart security of communications. WAP Transport Layer Security protocol gives a public-key based security mechanism analogous to TLS and the WAP Identity Module saves the secret keys[5]. In order to permit the interoperability of WAP equipment and software along with many different technologies WAP employs the WAP protocol suite.

Wireless Application Environment
Wireless Session Protocol
Wireless Transaction Protocol
Wireless Transport layer Security
Wireless Datagram Protocol
Network like IP or GPRS

Figure 2. Different layers in WAP Protocol Suite

5 SECURITY DILEMMAS WITH CURRENT GPRS IMPLEMENTATION

5.1 Security matters with present implementations using WAP

Use of WAP in the present mobile banking implementations, has proven to be very safe, but still there are some loopholes which could results in insecure communication. Some of these loopholes are following:
One of the problems with this implementations is that, there is end-to-end to encryption only between the client and the Gateway and then between the Gateway and the Server of the bank. There will be no end-to-end encryption between clients to bank server. To resolve this problem, the server of the bank could have its own Access Point Name (APN) in the GPRS networks. This APN would function as the WAP Gateway for the bank. So the client will be connected directly to the bank without any third parties in the middle of any communication.

WTLS standard offered the Public key cryptosystems key sizes.[6] These Public key cryptosystems key sizes are not well-built enough to meet today's WAP products security requirements. Taking into consideration, the low processing power of

the handheld mobile machines the key sizes have been limited.

Client and the server, both are not authenticated. Anonymous key exchange suites provided by the WAP Transport layer security handshake are also not considered safe. If possible, banks should make a system to prohibit this option of the handshaking.

2.4.2 Security concerns related with using basic GPRS network

There is no provision to avoid alteration of data and to guarantee the integrity of data for both the account holder as well as the Bank. The process to accommodate the confidentiality of information between the mobile station and the bank server has proven to be not strong enough[7]. This brings up security issues for the bank as well as the account holder. So the network operator can easily view account holder's sensitive information. The basic GPRS network is too general in reality; it does not serve for many banking security needs.

Lack of account holder's authentication or bank authentication is not a not-noteworthy issue. The Bank can supply a unique APN to access the information on Bank server, but without this or some additional authentication mechanism anyone can do fraud with the Bank[8]. All these matters raised worries of forgery of the bank information as well as account holder information. GPRS offers session handling services, but can't handle Bank specific sessions[9]; this results in unpredictability on the bank's side elevating security matters. The bank cannot verify any action performed by the account holder and same as the account holder cannot provide evidence that the bank carried out any particular transaction.

6. **CONCLUSION**

The present study examined GSM network for mobile banking. GSM is the solitary network for transporting data in mobile banking. But the problem with GSM is that, without overlying security protocols over it, it has proven susceptible to many types of security attacks. As with GSM in mobile banking, most of the authentication as well as confidentiality procedures have been rifted.

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 Even though WAP an WIG protocols provide security for banking transactions upto some extent but still there are some loopholes that could prove susceptible for transactions on mobile banking.

8. **FUTURE WORK**

With few exceptions, currently banks are using GSM networks overlay with certain security protocols for secured mobile banking. But as we have seen, these security protocols overlaid the GSM network for adding stronger authentication and confidentiality methods for secured communication, but these protocols are still

susceptible for security threats. Any third party can acquire sensitive information from bank or from client. In order to cure this problem, further work on authentication of mobile application is needed. As we know that security of banking transactions is not the issue, with which one can compromise. So some stronger protocols are needed to overlay the current GSM architecture.

10. REFERENCES

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

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

[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]. 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

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

[8]. 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.

[9] R. Chaudhri, G. Borriello, and W. Thies. FoneAstra: Making mobile phones smarter. In ACM Workshop on Networked Systems for` Developing Regions. ACM, Oct. 200