Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 37 (2014) 451 – 456

Procedia Computer Science

International Workshop on Intelligent Techniques in Distributed Systems (ITDS)

Technical Requirements Of New Framework For GPRS Security Protocol Mobile Banking Application

ElBahlul ElFgee[a,*], Ahmed ARARA[b]

[a]*High Institute of Vocational Studies, Yafren, Libya*
[b]*College of Eng.- Comp.Engin- Dept-University of Tripoli, Libya*

Abstract

GPRS stands out as one major development in the GSM standard that benefit from packet switched techniques to provide mobile subscribers with the much needed high bit rates for bursty data transmissions. It is possible theoretically for GPRS subscribers to use several time slots (packet data channels) simultaneously reaching a bit rate of about 170kbit/s.
To meet our demands, the GPRS service has evolved from GSM to make high-speed data transmission possible, it offers high data rate packet switched connections and improves the utilization of the network and radio transmission resources, compared to the circuit switched radio transmission, GPRS allows multiple users to share one physical channel.
One of the facilities that GPRS offers is connection to the Internet. Because of this facility, some banks now offer their clients access to their banking networks through GPRS as medium for switching packets to different networks that have its own security implementations. Such security implementations have been cracked and proven vulnerable. At present Wireless Application Protocol (WAP) as a data bearer protocol is the prevalent protocol offering the extra layer of security, with WAP using WTLS (WAP Transport Layer Security) as a security protocol. In this paper, we have looked into this extra layer and the security shortfalls in this layer. A framework that includes the GPRS architecture, a set of security policies, and a set of mechanism shall be proposed. Also a handshake algorithm is presented that can be used to establish a connection between MS client and MS server.

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.

Keywords: ***Information Security, security framework, and handshake algorithm***

1. Introduction

In the past few years, fixed networks have witnessed a tremendous growth in data traffic, due in good part, to the increasing popularity of the Internet. Consequently new data applications are emerging and are reaching the general public**.** At the same time the market is witnessing a remarkable explosion of cellular and mobile technologies

* Corresponding author. Tel.: +218 92 735 4149;
E-mail address: fgeeee@dal.ca

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.
doi:10.1016/j.procs.2014.08.068

leading to demand that data applications become available to mobile users. GSM (Global System for Mobile communications) is the European standard for cellular communications developed by ETSI (European Telecommunications Standards Institute).Throughout Europe and the rest of the world (including North America), GSM has been widely adopted. GSM already offers data services but they have been constrained by the use of circuit Switched data channels over the air interface . For this reason, the GSM standard has continued its natural evolution to accommodate the requirement for higher bit rates. The HSCSD (High-Speed Circuit-Switched Data) is one solution that addresses this requirement by allocating more time slots per subscriber and thus better rates. It remains however insufficient for bursty data applications such as Web browsing. In a circuit switched mode (see figure 1), a channel is allocated to a single user for the duration of the connection. This exclusive access to radio resources is not necessary for data applications with the use of packet switched techniques. GPRS stands out as one major development in the GSM standard that benefit from packet switched techniques to provide mobile subscribers with the much needed high bit rates for bursty data transmissions. It is possible theoretically for GPRS subscribers to use several time slots (packet data channels) simultaneously reaching a bit rate of about 170kbit/s [1].

To meet our demands, the GPRS service has evolved from GSM to make high-speed data transmission possible, it offers high data rate packet switched connections (see figure 1) and improves the utilization of the network and radio resources, Compared to the circuit switched radio transmission, where single users occupy a complete traffic channel for the entire call period, GPRS allows multiple users to share one physical channel [2].

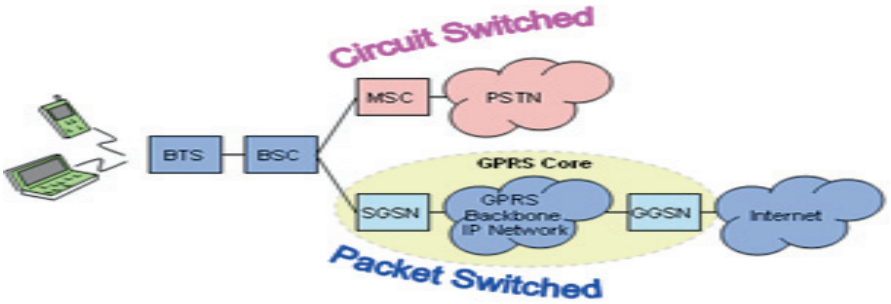

Figure 1 GPRS evolution via GSM

Figure 1 illustrates the packet switched path taken by GPRS instead of the circuit switched path. The main components of GPRS are:- (i) The Serving GPRS Support Node (SGSN) which is used for:- Mobility Management, Authentication, gathers charging information; (ii) Gateway GPRS Support Node (GGSN) which provides:- Gateway between UMTS (Universal Mobile Telecommunications System) Core Network and external networks, address allocation for MS, gathers, and charging Information, and filtering. (iii) Base Station Subsystem (BSS) which consists of BSC and BTS / Radio Network Subsystem (RNS). Despite the fact that there is no absolute secure system, but we shall propose a framework that includes:- a GPRS architecture, a set of security policies, and a set of security mechanisms. The proposed framework should conform to the objectives of secure mobile banking regarding integrity, confidentiality, non-repudiation, and authentication.

2. WAP Protocol Stack

The Wireless Application Protocol (WAP) is a protocol stack for wireless communication networks. WAP uses WTLS, a wireless variant of the SSL/TLS protocol, to secure the communication between the mobile phone and other parts of the WAP architecture as shown in Figure (2).

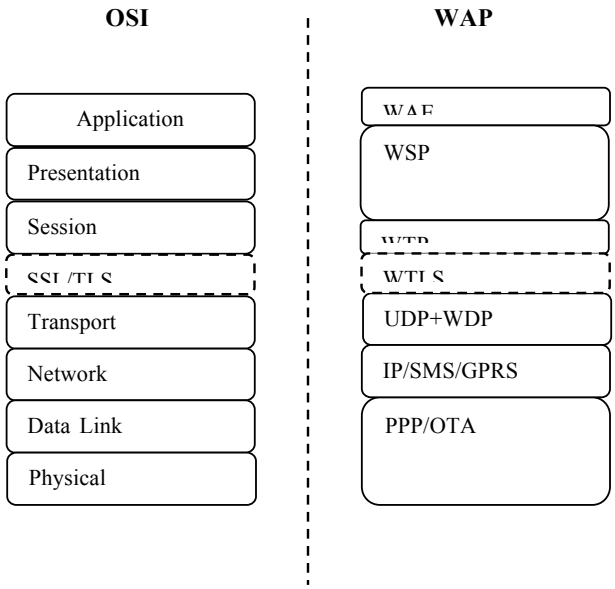

Figure (2) WAP protocol stack

There are three participating entities in the WAP architecture: the WAP browser, the WAP gateway (also called WAP proxy) and a web server. When the mobile device wants to connect to the internet, all the communication passes through the WAP gateway. This WAP gateway translates all the protocols used in WAP to the protocols used on the Internet. For example, the WAP proxy encodes (and decodes) the content to reduce the size of the data that has been sent over the wireless link. Another example is the WTLS protocol. The communication between the mobile device and the WAP gateway is secured with WTLS. WTLS is only used between the mobile device and the WAP gateway, while SSL/TLS can be used between the gateway and the Internet. This means that the WAP gateway first has to decrypt the encrypted WTLS–traffic and then has to encrypt it again (using SSL/TLS). The WAP protocol stack contains the following elements:

Physical and Data Link Layer: In WAP, Point to Point Protocols (PPP) are used over one or more Over–The–Air (OTA) bearer protocols.

Network Layer: IP is the network layer of choice. However, not all wireless networks are capable of transmitting IP. That is why SMS or some other non-packet network protocol can be used.

Transport Layer: The protocol used in the transport layer is UDP. However, this may not be feasible over non–IP networks. That is why (there are also other reasons) that WAP defines an additional transport layer protocol, WDP, which can be used when UDP is not possible to use.

Session Layer: The functionality of the session layer is partially included in WTP. Other aspects of the functionality are implemented in WSP.

Presentation Layer: The functionality of the presentation layer is included in WSP.

Application Layer: Some aspects of the functionality of the application layer are included in WSP; the others are implemented in WAE.

Wireless Transport Layer Security protocol (WTLS) establishes a session between a client (the mobile phone) and a server (the WAP gateway). This phase is called the handshake phase. During this handshake phase, security parameters used to protect the session are negotiated. These include the encryption protocols, signature algorithms, public keys, pre-master secrets, WTLS includes support for both a full hand shake, with negotiation of all security parameters, and for a lightweight handshake in which the security parameters of another session are reused. Once a session has been established, all the communication between the client and the server is encrypted. WTLS also support the feature to suspend a session and resume it later. WTLS also uses certificates. Because certificates were not really designed to be used by mobile devices, WAP defines a new format of certificate that is optimized for storage on mobile devices and transmission over wireless networks. These certificates have the same functionality as ordinary X.509 certificates, but rely on the server to perform more of the processing under some circumstances. WAP devices use a Wireless Identity Module (WIM) which contains the necessary private and public keys to perform digital signatures and certificate verification respectively. It is a tamper-proof device, which means that it is very difficult for an attacker to obtain the keys which are stored in this device. The WIM can be compared to the SIM of the GSM [3].

3. e-banking Security requirements

Security requirements and policies may include analysis and testing suites of the system for conformance to a set of security standards and best-practices. In order to conform to security objectives, GPRS need to be configured, and a set of security policies and security mechanism are to be devised. In this research, we shall look closely at the security requirements of GPRS based on GSM technology. Figure 3 illustrates the network and sub-networks that need to collaborate. A corporate 1 (a bank) need to permit a client to obtain e-bank services. Corporate 1 is also in need to communicate with corporate 2 via GPRS protocol. The communication corporate-2corporate and corporate-2-client and client-2-corporate must be done securely and conform to security measures and standards.

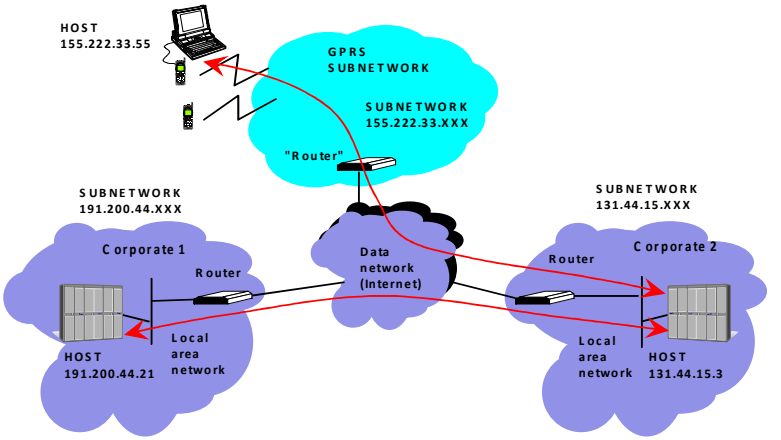

Figure 3 linking client and corporate via GPRS

3.1. Security threats requirement specification

Security can be defined as identifying potential threats and understanding that each threat presents a degree of risk. Security is about risk management and implementing effective countermeasures. All types of threats should be considered namely:- interception, interruption, modification, and fabrication [4][5]. Figure 4 shows the risk analysis tree. Each node in the tree represents a source or set of sources of risk. The tree is handy to develop security policies and related mechanism to overcome the m-banking system vulnerability. e-banking security threats require a complete risk analysis. The three sources of risk that must be analyzed are:- (i) MS (customer side):- authentication,

(ii) in networks:- Firewalls and routers, and (iii) in e-bank server side:- sensitive information such as encryption keys and customer information in transit [6][7].

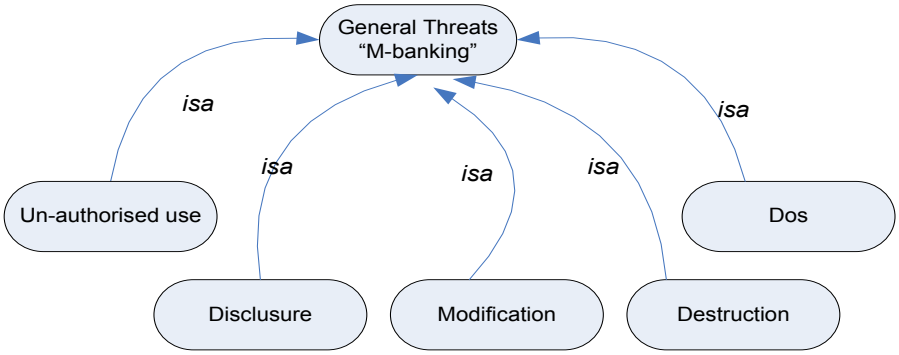

Figure 4 general risk- analysis-tree

3.2. Security policies, and mechanisms

A security policy describes precisely which actions the entities in a system are allowed to take and which ones are prohibited. Entities include users, services, data, machines, and so on. Once a security policy has been laid down, it becomes possible to concentrate on the security mechanisms by which a policy can be enforced [8]. There are four important security mechanisms to be considered:- (i) ***Confidentiality***, (ii) ***Integrity***, (iii) ***Authentication*** and ***Availability***. Ideally, these elements should not be susceptible to denial of service attacks [9].

3.3. Handshake algorithm

In order to take measures of security requirements, an algorithm to show the handshake between Ms and bank server. Access control policies are needed to exploit the process of communication securely. Table 1 shows the algorithm of MS-Bank server handshake. This algorithm ensures Authentication, Integrity and Confidentiality.

Table 1 handshake algorithm

Name: ***MS –BankServerHandshake***
Input: ***MS BankTransaction event***
Output***: allow/provoke Transaction***
Steps:

1. *MS-RequestAuthentication(SGSN)*
2. *Generate Triplet(RAND, SRES,GPRS-kc)*
3. *SGSNgetTriplet ()*
4. *SGSNSend2MS(RAND)*
5. *MSCompute(SRES,GPRS-kc)*
6. *MSSend2SGSN(SRES)*
7. *If MS(SRES) is equal to Triplet(SRES)*
   AllowTransaction()
   Else
   ProvokeTransaction()
   Report2SecurityOfficer()

End// ***MS BankTransaction event***

Mobile banking can be accessed via two options i.e. through the Wireless Internet Gateway (WIG) or Wireless application Protocol (WAP) as in a figure (5). Bank account holders can access WAP sites and perform banking the same way they would carry out internet banking [6].

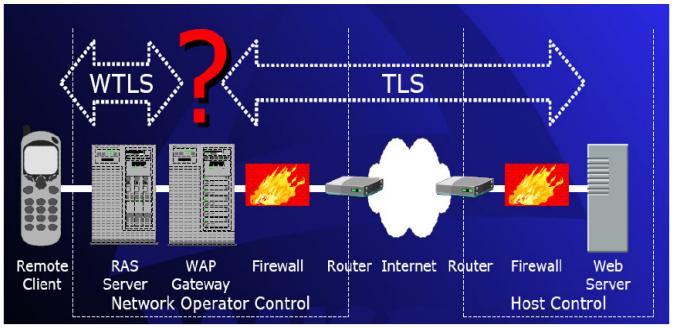

Figure (5) Wireless application Protocol

5. Conclusion

GPRS as a stand-alone medium for transporting packet data without overlying security protocols has proven vulnerable to some security attacks, with most of the authentication and confidentiality mechanisms having been cracked. This has led to the implementation of overlying protocols such as WAP so as to enforce the security of transporting data over GPRS. Even though this protocol provides solid security for banking transactions there are some slight loopholes that could prove susceptible for mobile banking. The authors presented a handshake algorithm of e-banking transaction between a client and a Bank Server and the transaction will be started after all security information received. In addition, a general risk-analysis tree is presented which indicates all possible risks that each node in the e-banking system can face. This can help to protect each element from possible attack and security measures can be taken.

References

[1] Gabhart, K. J2EE pathfinder: “Filtering with Java Servlets 2.4. Viewing, extracting, and manipulating HTTP data with Servlet filters .developer Works”, IBM’s resource for developers. 27 January 2004.

[2] Wesley, D. Microsoft Application Center 2000 Resource Kit: Chapter 1 - Scaling Business Web Sites with Application Center. 2000.

[3] Sterbenz, A., Lai, C. Secure Coding Antipatterns: Avoiding Vulnerabilities. JavaOne Conference, Sun Microsystem, Inc. 2006.

[4] Gegick, M., Williams, L. Matching attack patterns to security vulnerabilities in softwareintensive system designs. Proceedings of the 2005 workshop on Software engineering for secure systems-building trustworthy applications. 2005.

[5] ISO 310 00:2009. Risk management – Principles and guidelines.

[6] Microsoft Office Communicator Web Access Security Guide. Identifying Possible Security Threats. Microsoft TechNet. April 14, 2006

[7] ITGI. 20 09. Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework, Exposure Draft.

[8] Security Innovation, Inc. Application Security by Design. February 2006.

[9] Swiderski, F., Snyder, W. Threat Modelling. Microsoft Press. 2004.