Transformation of WAP Gateway Server for Providing the Solution of Re-Encryption

Kamini
Research Scholar
Punjab Technical University
(Jalandhar), Kapurthala

Rajiv Mahajan, Ph.D.
Punjab Technical University
(Jalandhar), Kapurthala

Ravinder Singh, Ph.D.
Punjab Technical University
(Jalandhar), Kapurthala

ABSTRACT
Today mobility has been increased day by day through wireless devices because of small in size and portable in nature. Two different protocols are used at transport layer for transferring the data between mobile devices to web server. Wireless devices like mobile phones and PDA provides the facility to user for conducting the ecommerce transaction at any time at any place through a secure communication channels. The mobile communication is possible only when peoples are connected with internet. The purpose of this paper is to discuss about the security protocols at both side one for the WAP client to gateway and another for gateway to web server. The problem between the gateways is called WAP gap in which Re-encryption is required at gateway which leads to the problem of end to end security .This paper focuses on providing the solution of Re-encryption by changing the path of WAP gateway directed to route of web server.

General Terms
Wireless Transport Layer, Wireless Client

Keywords
Architecture, Client, Server, End to End Security

1. INTRODUCTION
The wireless and mobile devices are rapidly increased because of its features like small in size and use anywhere in the world. In various distributed application peoples communicate with each other through network communication channels. The end to end communication is possible only with the use of secured encryption and decryption techniques. Privacy, security and authentication is provided by security protocols. In today time all want to use mobile phones instead of desktop computers. When anyone want to access the internet through mobile phones all the communication is pass through a secured network protocol. Two way communication is provided at gateway one for the wireless devices and another for the wired devices. When a mobile device is used for internet transaction then WAP protocol stack is used for this purpose. The WTLS is named as wireless transport layer security used for wireless devices like mobile phone and PDA and another is TLS/SSl is used for wired devices. The gateway used as intermediate for transferring all the communication from mobile devices to www server. The wireless communication is transfer through the gateway to server. The path for the encryption and decryption used twice. First encryption is done at gateway for wireless devices and another encryption is done at web server. The structure is as follows.

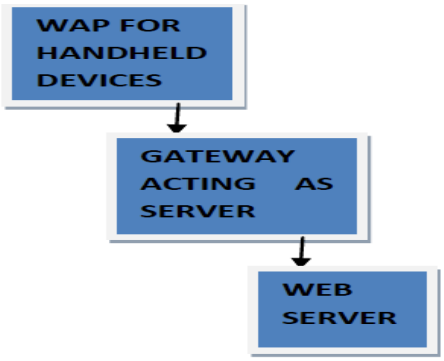

Figure 1: Structure of a WAP protocol

The remaining structure of paper is as follows Section 2 discuss about the review of literature. Section 3 discuss about the suggested proposed method for end to end security improvement between the gateway and web server. Section 4 discuss about the WAP security solution.

2. THE LITRATURE REVIEW
The wireless communication and the use of internet become very interoperable and every users want this communication channel to be very secure and available when it is required [1].Client and server authenticate each other with the concept of handshaking. Handshaking is a technique where the mutual understanding is made possible through secure communication channel. Three types of communication is there .In anonymous communication no exchanging of certificates between the client and server .In one way authentication server side authentication is made possible. In two ways communication server and client mutually exchanges certificates. The vital goal of the security solutions for MANETs is to provide security services, such as confidentiality, integrity, authentication, anonymity, and availability, to mobile users [2]. To achieve the goals, the security solution need for complete protocol stack is available. Digital certificates are based on public-key cryptography, which uses a pair of keys for encryption and decryption. With public-key Cryptography, keys work in pairs of matched. “Public” and “private” keys [3]. IPSec further differentiates between Transport Mode which is mainly used for point to point connections between two single hosts and Tunnel Mode which tunnels the traffic between two sub-networks that are protected by a security gateway [4]. Communicating in the wireless environment has its own issues and challenges. It is characterized by relatively low bandwidth and data rates, as well as higher error rates and the need for low power consumption (for mobile devices). The mobility of the nodes in cases such as ad hoc networks adds another significant layer of complexity and unpredictability [5]. WTLS uses the term key exchange suite to specify the Public-key

cryptosystem pair to be used for certificate validation and key exchange. WTLS supports several alternative key exchange suites. However, only two of them offer an acceptable level of security: ECDH_ECDSA and RSA key exchange suites [6]. Data transmission time model includes two components. The first component is the amount of time necessary to transmit the measured size of data with specified channel transmission rate. The second component is the traversal delay of the network that is added to the data transmission time regardless of how much data is sent [7]. A big advantage of WAP is that it is bearer independent. The most common bearer is currently GSM, but also a PDA or a third generation mobile phone can be used [8]. The WTLS handshake protocol is a cryptographic protocol designed for establishing an authenticated key in WAP environment. In an external view, the shape of the WTLS handshake protocol is similar to that of Secure Socket Layer (SSL) or Transport Layer Security (TLS). But it is reflected upon mobile environment, terminal's limitation, lower computing power, small user interface, lower data Transfer rate [9]. Take the WAP users nature and the conditions they are facing during accessing WAP sites through their WAP devices into consideration when designing wireless enabled sites [10].The various constraints on wireless networks like WTLS which becomes incompatible with TLS or SSL ,which is used for network planning and for the administration of end to end security[11].The gateway is used as server which transfers all the data from WAP client to web server machine [13].The three types of class types for WTLS. The WTLS is class 1 is implemented without exchange any certificates. The WTLS is class 2 is implemented where server certificates are sent to client. The WTLS is class 3 is implemented where client and server exchange the certificates [14]. In a full WTLS handshake, two round-trips are required before the client and server can start exchanging encrypted application data. In the first round-trip, client and server hello messages are exchanged [15].

3. THE PROPOSED SOLUTION

We have given a proposed solution of end to end security problem. Two types of security protocols are used at two ends. The WTLS is used at wireless side and TLS/SSL is used at wired side. The problem with two security devices is that there is requirement for using encryption and decryption techniques twice. One for WAP client side to gateway side and another for gateway side to web server side. The idea is given here by changing the route of encryption from gateway to web server so can only one encryption and decryption is used. The proposed idea would work in following way.

1. The WAP client is sending request for accessing the data from the internet.

2. The request is arrived at gateway, but it will directly pass to web server and encryption technique will apply there.

3. The request is encrypted by using encryption technique .After checking the requested page from web server if page is available then it is ok.

4. The web server replies with sending the requested page to gateway.

Now data will not be decrypted by the gateway, it will be directly send to WAP client for accessing the internet. Now data would get decrypted using decryption technique the wireless and wired encryption commonly to be implemented on www server .The other side wired decryption and wireless decryption commonly to be implemented on WAP devices. When any client want to authenticate the server, certificate would be directly send from WWW server But it seemed like that the data is arrived from the gateway.

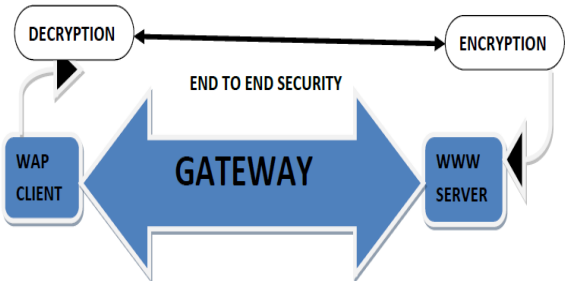

Figure 2: The encryption and decryption at only one end

WAP architecture is available for wireless devices like mobile phones and PDA. The WAP gateways encrypt all the Wireless traffic and send it to the main web server for the decryption. The end to end security problem was there because two security protocols were used for different devices. First WTLS is used wireless devices and then TLS/SSL is used for wired devices. The security protocols are used at transport layer of OSI model when it is used for transferring all the data from client machine to server machines. The gateway acts as intermediate which transfers all the WAP traffics to web server by transferring all the protocols used by wireless devices to wired devices. In the above Fig1 we have discuss about the encryption and decryption at only one end. A common pathway becomes possible with the help of proposed solution which leads to the improvement of end to end security. The WTLS term developed from TLS/SSL but the difference between both that WTLS is used for mobile devices and TLS/SSL is used for wired devices .The WTLS is only limited for small devices which lead to the problem of low bandwidth and small memory. A common algorithm would be design in such way so that Encryption and decryption could work on both ends. The encryption and decryption algorithm would design in such a way so that no unauthorised can access the data. The WTLS cryptography algorithm should be very strong for the purpose of security. But in case of wireless network the key size is very small as compare to wired networks. As large the key means security algorithm work for long time duration. Digital signature are used for authentication and integrity purpose .Authentication is used for the purpose of authenticate the server as well as client .When client and server exchanging the certificates with each other it means they are authenticate .The handshaking would directly be performed from WAP client to server instead of gateway. The handshaking protocol is used to negotiate all the session related information between the client and server. The WAP data encrypted directly as web server because a common pathway is required from the WAP client to server. When common path would be from WAP client to WWW server only one common security protocol would be used at transport layer which will work for wireless devices and wired devices. This is required for the improvement of end to end security between the client and server.

4. REFERENCES

[1] Boncella," WIRELESS SECURITY: AN OVERVIEW". Washburn University" AIS.

[2] Dr.G.Padmavathi1, Dr.P.Subashini2, and Ms.D.Devi Aruna3," ZRP with WTLS Key Management Technique to Secure Transport and Network Layers in Mobile Adhoc Networks" International Journal of Wireless &

Mobile Networks (IJWMN) Vol. 4, No. 1, February 2012.

[3] Allan Macphee," Understanding Digital Certificates and Wireless Transport Laye Security (WTLS).

[4] Andreas Steffen." Secure Communications in Embedded Systems" 2004 in the CRC Industrial Information Technology Handbook.

[5] Eduardo B. Fernandez, Imad Jawhar, Maria M. Larrondo-Petrie, and Michael VanHilst ." An overview of the security of wireless networks" Version of November 19, 2004.

[6] Albert Levi, Erkay Savas" Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol.

[7] BURAK BAYOGLU." PERFORMANCE EVALUATION OF WTLS HANDSHAKE PROTOCOL USING RSA AND ELLIPTIC CURVE CRYPTOSYSTEMS. Spring 2004.

[8] Dave Singel´ee, Bart Preneel." The Wireless Application Protocol (WAP)." COSIC Internal Report September 2003.

[9] Jongcheol Moon, Bonghwan Kim, Sokjoon Lee, Yoojae Won." A HANDSHAKE PROTOCOL ANALYSIS OF WAP WTLS".

[10] Ayma A. Issa, Munib A. Qutaishat," Dynamic Multiplatform HTML to WML Mobile Converter" Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

[11] Available at this link "http://www.crcnetbase.com/doi/abs/10.1201/9781420040012.ch6"

[12] "Amendment to PKCS#11 for support of WTLS and TLS PRF" RSA Laboratories November 2001

[13] Available at this link "http://www.tol.oulu.fi/users/ari.vesanen/Langaton_TT/luennot/kalvot/WAP.pdf"

[14] "Security Issues In Wireless Environments" October 12, 2000.

[15] Neil Daswani" Cryptographic Execution Time for WTLS Handshakes on Palm OS Devices"