# INTEGRATION OF SECURITY PROTOCOL IN BETWEEN THE NETWORK GATEWAY

Kamini
Lecturer
Lovely Professional University
School of Computer Applications
Phagwara (Punjab)

Rajiv Mahajan
Professor
Global Institute of Management
and Emerging Technolgy
Amritsar (Punjab)

Rachit Garg
Associate Professor
Lovely Professional University
School of Computer Applications
Phagwara (Punjab)

***ABSTRACT*- Accessing the use of internet in mobile phones has been popular day by day just because of its features like portability, small in size. In nowadays mobile phones interfaces becoming very user friendly just because of its interactivity. In the past time when the people have the choice whether they want to use internet on the personal computer or in mobiles phones .At that time most of the people try to use internet on their desktop when they are browsing the internet and mobile phones is used only for the purpose of mail checking but today mobile technology is growing very fast now surfing on mobile phone is becoming very easier as similar to desktop. when any user want to access the internet on mobile phone the WAP (wireless application protocol)browser is available .All the communication are passed from mobile browser to www server with the help of gateway. The gateway acts as intermediate between the mobile devices and web server. This paper discusses about the protocol used in mobile devices and server side and how the communication take place from one end to other end. This paper focuses on the technique of integrating the security protocol together so that problem facing at the gateway can be resolved. The paper also presents the comparative analysis of security protocol.**

***Index Terms*- Transport Layer, Wireless Client**

***Keywords*- WAP, Security, Client, Server, Communication**

## I. INTRODUCTION

Today most of the e-commerce transaction is made possible with the help of wireless devices. People from different areas like manufacturing, marketing, banking, education and others are using mobile phones in their daily life. Wireless devices include PDA, mobile phones because of its features like low bandwidth, small in size, portable in nature. All communication takes place from WAP devices to web server through the gateway. A WAP is a small mini browser available for mobile phones where user can run their application. In WAP browser WML language is supported .The WML is called as wireless mark-up language used for mobile devices but on the other side of server the HTML language is supported which stands for hyper text mark-up language .both language like WML and HTML are scripting language .The scripting used for mobile phones is called as WML script and the scripting language used for HTML is called as HTML scripting which is used for design any kind of web application. There are some risks which are associated with WAP applications like personalized information can be share, access control to the personal information through mobile devices, viruses can harm the information, location detection and operating system problem. Two types of security protocols are required while transferring the data from mobile devices to web server. The security protocol used by the mobile devices is known as WTLS (Wireless transport Layer Security) and the other security protocol used at server side known as TLS/SSL (Transport Layer Security/Secure Socket Layer).The gateway acts as the intermediate which transferring the language of used by one system to another server. Both markup languages are used at client side and server side processing.

In this paper we focused on various problem faced at client side and server side .Here client is known as WAP client who is using the mobile phones for web browsing and server is known as web server from where we are going to access the internet. The end to end security can be improved only when there is Common pathway exists from WAP client to web server .The remainder of the paper is organised in the following manner. In Section II we discuss about the literature review of various papers. Section III we discuss about the problem defined with two security protocols. Section IV we discussed the comparative analysis of security protocols.

## II. WTLS/TLS LITRATURE REVIEW

[1] Discussed about the efficient architecture for the hardware implementation of WTLS is proposed. [2] Discussed about the security between the WAP client and gateway by using the wireless transport layer security. [3] Discussed about the web service used for the mobile phones is and secure communication for today world of online transaction. [4] Has Discussed about the current specification of WTLS does not provide total end-to-end security because WTLS-enabled gateway will leak plaintext during data transmission to the server. ITLS was created based on fixing WTLS security holes. A comparison of ITLS and WTLS demonstrates that ITLS provides stronger protection in gateway and offers a more secure channel than WTLS.[5] has discussed about the communication from the mobile phone to the Internet passes through the WAP gateway. The communication between the mobile phone and this WAP gateway has to be secured. The SSL/TLS protocol cannot be used for this purpose because of the constraints of the mobile phone. [6] Has discussed about the security model with reasonable assumption on the underlying TLS pseudo random function, thereby addressing concerns about its construction in terms of two hash function .The result is extended to a wide class of constructions that denoted as tagged key encapsulation mechanism. [7] discussed about the development of the wireless Internet, where cell phones, PDAs, and laptops let us receive and send e-mails, and perform all the activities that we are currently performing over the wire line Internet. [8] Discussed about the WTLS is a security protocol based upon the industry-standard Transport Layer Security (TLS) protocol, formerly known as Secure Sockets Layer (SSL). WTLS is intended for use with the WAP transport protocols and has been optimised for low-bandwidth bearer networks with relatively long latency. The primary goal of the WTLS layer is to provide privacy, data integrity, and authentication between two communicating applications.[9] Discussed about the WAP was designed to work not only with GSM but most other digital wireless telephone networks. Some bearers are illustrated on Figure 3. Compared to the well-known Internet, mobile wireless networks are characterized by: limited communication capacity (bandwidth), higher latencies, higher variation in packet-loss (jitter), and variation in long-term connectivity/availability (on/off). [10] Discussed about the WTLS handshake protocol which is implemented using c++ and performance measurements are done using the mobile phone which Would be twice .The protocol can be integrated for getting the same concept. In the below diagram the act as client ad open source WAP gateway. [11] Discussed about the WTLS handshake protocol is a cryptographic protocol designed for establishing the authenticated key in WAP environment. [12] Discussed about the protocol algorithm uses multiple data compression algorithm to provide doe data compression and decompression during communication. [13] Discussed about the data transfer during the transaction, number and size of messages exchanged during the secure session establishment and cryptography consumption during a secure wireless session. [14] Discussed about the supported ciphers performance is compared with previously published works and it has been proven superior to them. [15] Discussed about the security hole was a product of the so called WAP gateway.

## III. CONTRIBUTION OF THE PAPER

The problem with using two protocol is that the end to end security could not be improved because one protocol is used at client side when client is using the mobile phone and other protocol is used at server side when client want to access something from the internet. One communication is passed from wireless device to web server then two type of pathway would be followed .One pathway is required from WAP client to gateway and another pathway is required from gateway to server. There should be only one protocol so that instead of transferring the communication from two ways it should be transferred using a one way using common protocol. Before the WTLS only TLS/SSL protocol was used .The WTLS protocol has been derived from TLS.The TLS protocol has been derived from SSL .The TLS/SSL used for the wired networks where the bandwidth is much higher than the wireless network. The WTLS is used by the wireless devices. It is important to determine how much time is taken by WAP gateway to transfer the data from WAP browser to web server. When the connection established between WAP client to web server then the security algorithm also works .One security mechanism take place between WAP client to WAP gateway using WTLS security algorithm and other security algorithm take place between WAP gateway to web server using TLS. When two security algorithms are used between the gateway then two times of encryption and decryption algorithms are also required .one encryption and decryption algorithms required for WTLS and same for the TLS also. These two times encryption and decryption algorithms cause a problem of end to end security .The time taken for connecting the data from web server would be twice the time for using two protocols. integration is possible for two different protocol .One is possible through the client and server architecture model

Protocol called as WTLS and another protocol called as TLS.When we combine both of them then the common objectives can be achieved. The integration between the protocols can increase the benefits of time because the time would be decrease when one common path would be used instead of two different paths. When we talk about the security protocol three types of communication is possible .One communication is anonymous communication in which client and server communicate With each other without knowing which one is act as client and which one is act as server .Second type of communication is server side authentication in which server side certificates is used for the authentication but client side no certification is used for the verification. Third communication is called as client and server communication in which client and server communicate With each other through exchanging the certificates.

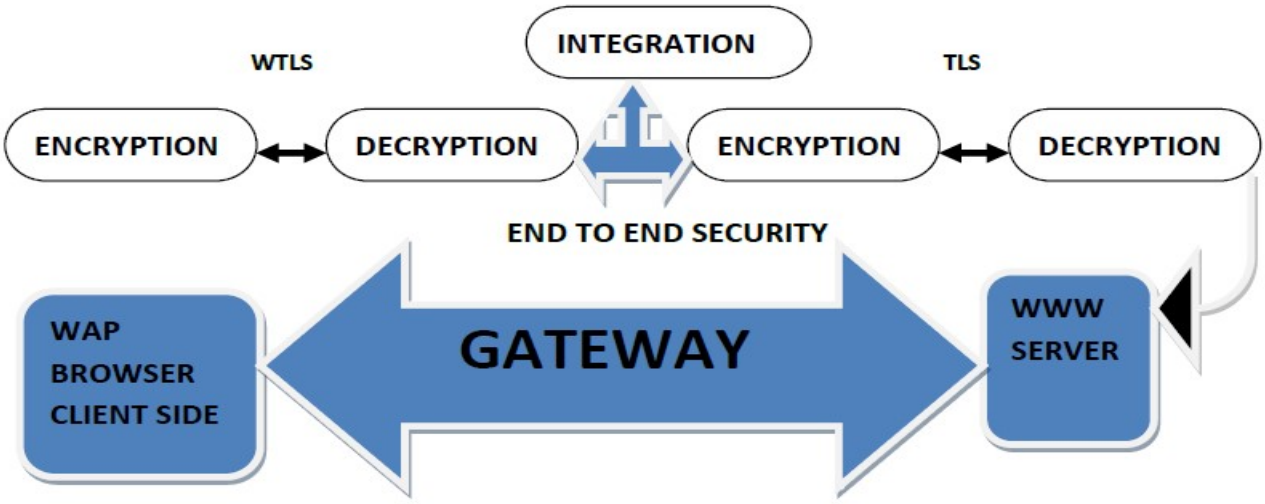


Fig 1: Integration of two security protocol

In the above figure 1 the WTLS (wireless transport layer security protocol is used as client side and client is going to use the mobile phone for accessing the information from the web server .The encryption algorithm used for encrypt the data and decryption algorithm is used for decrypt the data .These security algorithm are used in between the gateway and the gateway is acting as Intermediate. Other side for wired devices encryption and decryption technique is used again. When re-encryption is used twice in between the gateway then in the mean time this data can be hacked by any unauthorized user because the data is in air because of wireless devices. When we integrate two security protocols together then the security mechanism can be improved.Combination of both security protocols will perform better and it will provide the fast results.

## IV. COMPARATIVE ANALYSIS OF SECURITY PROTOCOLS

**Table 1**: Comparison Chart for the analysis of WTLS/TLS security protocols

| Type | Wireless Devices | Wired Devices |
|---|---|---|
| **User interface** | The user interface used for WAP is through the built in mini browser in mobile phone. | The user interface used for wired devices is through the internet explorer, Mozilla, opera etc used by web. |
| **Security Protocol** | The security protocol used for wireless devices is called WTLS. | The security protocol used for wireless devices is called TLS. |
| **Capacity** | The mobile phones has limited bandwidth and less memory .Due to this heavy computations does not performed by security devices | The wired devices has more capacity as compare to mobile phones .Due to this heavy computations is performed by security devices |
| **Use of Gateway** | The WAP communication is passing through the gateway to web server. | All the encrypted data of wired devices is passed directly to server. |
| **Language** | The WML language is used by wireless devices. | The HTML language is used by wired devices. |
| **Transport layer protocol** | The protocol used by transport layer is called WDP. | The protocol used by the transport layer is called UDP. |
| **Session layer protocol** | The protocol used for maintaining the session is called WSP. | The protocol used for maintaining the session is called HTTP. |
| **Transaction Layer protocol** | The WTP protocol is used at transport layer. | The TCP/IP is used at transport layer. |
| **Certificate** | The size of the certificate is small in case of WTLS | The size is large as compare to WTLS. |
| **Compression** | In WTLS the packet size is small as compare to TLS because of UDP | In TLS the packet size is large because of wired devices. |
| **Packet Type** | In WTLS the data is transferred in the form of packet stream. | In TLS the communication is done with data steam. |

## V. CONCLUSION

This paper has discussed about the how we can integrate two security models into on one common security model. The main benefits of integration of two model is that instead of travelling the data from two different path which is most time consuming process the communication would be possible by a common path. The comparative analysis of two different security protocols has done in this paper. The communication is done by a single protocol the time would be reduced .In future various simulators and Matlab software can be used for communication between two different protocols.

## REFERENCES


[1] Kamini; Sharma, P., "Algorithmic Review of WTLS and TLS for Recommending Measures for Implementing CSP in the Network Gateway," *Computing Sciences (ICCS), 2012* pp.286,290, 14-15 Sept. 2012 doi: 10.1109/ICCS.2012.11

[2] Kamini.:Conceptualizing Common Security Protocol for Wireless Client and Wired Server. International Journal of Computer Applications 42(5):14-18, March 2012. Published by Foundation of Computer Science, New York, USA

[3] Kamini. Article: Key Resolution of Reencryption by Providing Paging in Between the Gateway . International Journal of Computer Applications, March 2012. Published by Foundation of Computer Science, New York, USA, National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC 2012

[4] Younhee Kim, Chun-kit Wong, George Mason University," Comparison of WTLS and ITLS in Wireless end-to-end secure network (December 2002)

[5] Dave Singel´ee, Bart Preneel.The Wireless Application Protocol (WAP). COSIC Internal Report, September 2003, Pages 1-5

[6] Jakob Johnson Burton S.Kaliski Jr.On the security of RSA encryption in TLS.RSA laboratories, 20 Crosby Drive, Bedford, MA 01730.USA.

[7] Andres Liana, Jr (2001).Wireless Application Protocol (WAP) and Mobile Wireless Access", Auerbach Publication", CRC press LLC.

[8] "WTLS – The Security layer in the WAP Stack. Colloquium on Information Security Martin Christinat, Markus Isler, keyon

[9] Niels Christian Juul, Niels Jørgensen," Security Issues in Mobile Commerce using WAP" Bled, Slovenia, June 17 - 19, 2002

[10] Burak bayoglu,"Performance evaluation of WTLS handshake protocol using RSA and Elliptic Curve Crptosystem.

[11] Jongcheol moon,bongwan kim,sokjoon lee,yoojae won,"A handshake protocol analysis of WAP WTLS" Electronics and Telecommunication research institute.

[12] Hashmi Domun and Leckraj Nagowah. Article: An Intelligent Protocol Algorithm to improve the Performance of Enterprise Systems Communications. International Journal of Computer Applications 57(22):19-22, November 2012. Published by Foundation of Computer Science, New York, USA

[13] Ramesh Karri,Piyush Mishra,"Optimizing he energy consumed by secure wireless sessions:wireless transport layer security case study. April 2003, Volume 8 Issue 2

[14] N.sklavas,P.Kitsos,K.pepadopoulos,O.Koufopaviou,"Design ,Architecture and perfrom,April 2006,Volume 36 issue1

[15] Niels Christian juul,niels Jorgensen,"The security hole in WAP,An analysis of the network and business rationales underlying a failure", June 2003, Volume 7 Issue 4