Conceptualizing Common Security Protocol for Wireless Client and Wired Server

Kamini
Lovely Professional University
School of Computer Applications, Systems and Architecture Domain

ABSTRACT
When mobile device want to connect to the internet all the communication goes through the WAP gateway. The WAP gateway act as an intermediate between the wireless client and www server. The WAP gateways translate the protocols between the wireless client and wired server. Two protocols are used in between the WAP client and www server. One protocol provides the security between the WAP client and gateway by using the wireless transport layer security. Other protocols provide the security between the WAP gateway and www server by using the transport layer security. The problem is related to providing the end to end security between the WAP client and www server. The focus of this paper is to analyze the security problem and also provide possible solution for the end to end security by designing a CSP (common security protocol) for wireless client and wired server).

General Terms
Transport Layer, Wireless Client

Keywords
WAP, Security, Client, Server, Communication

1. INTRODUCTION
WAP is the worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants and other Wireless terminal.WAP means Wireless Application Protocol. Wireless means Lacking or not requiring a wire or wires: pertaining to radio transmission.

Application means a computer program or piece of computer software that is designed to do a specific task. Protocols mean a set of technical rules about how information should be transmitted and received using computers. WAP is the set of rules governing the transmission and reception of data by computer applications on, or via, wireless devices like mobile phones. WAP allows wireless devices to view specifically Designed pages from the Internet, using only plain text [1].

Wireless devices provide the computing device with limited CPU, memory and battery life and a simple user interface. The WAP specification addresses these issues by using the best of existing standards and developing new extensions when needed.

The WAP solution leverages the tremendous investment in web servers, web development tools, web programmers and web applications while solving the unique problems associated with the wireless domain.

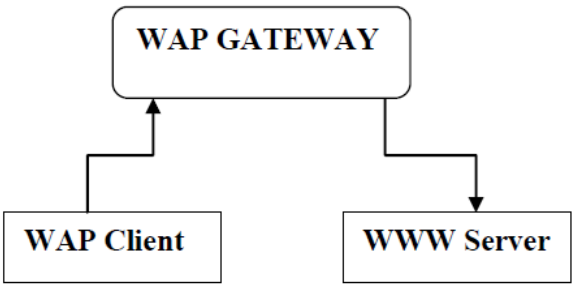

Fig 1: Basic Structure of WAP

In the above Fig1 the WAP client 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 [2].

The Wireless transport layer security protocol is used by WAP Gateway to provide communication between the WAP client and WAP gateway. The Transport layer security protocol is used to communicate between the gateway and www server. Modern day mobile phones have limitations that disable its ability to optimize WAP feature and the advantages of using WAP .The WAP is a binary encoded protocol .The request of WAP client go through the WAP gateway then gateway translates that request into HTML [3] .After this the gateway send this request to www server .The www server process the request, after processing the www server returned the processed request to the WAP gateway .Then again WAP gateway encode the message into binary form so that the micro browser display the requested page to user screen. .At client side the WML is used by WAP and server side HTML is used for processing the client request into server. Both markup languages are used at client side and server side processing.

2. PROTOCOL STACK FOR WTLS & TLS
The WAP protocol stack divide into five layers like application, session, transaction, security and transport layer each of these layers provides well design interface.

First we have Application layer which is the highest layer in the hierarchy which includes Wireless Application

Environment (WAE) and Wireless Telephony Application (WTA) [4].

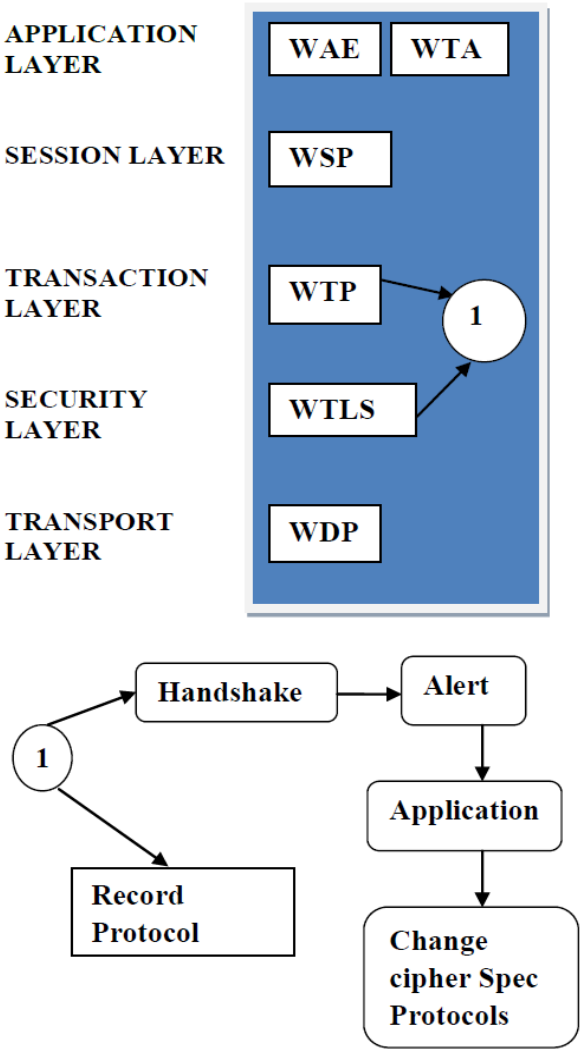

Fig 2: Protocol Stack For WTLS

These two are the main interface to the client device, which gives and controls the description language, the script language of any application and the specifics of the telephony. The client side is used for text messaging by using micro browser and WTA used for integration of telephone with scripting language. Second Session layer is used to provide the interface between the application layer and the transfer layer and delivers all functions that are needed for wireless connections.

The main purpose of session layer is to maintain state information about the parameter involved in the session state and communication state [5].A session mainly consists of 3 phases: start of the session, transferring information back and forth and the end of the session.

The WSP is used at session layer that provides the interface between the client and application server. Two types of connection can be supported by session layer .First is connection oriented service that guarantee reliable message exchange between the wireless device and server. Second connection less service which does not guarantee the reliable message delivery. Third Transport layer used which is used for transfer the data for both secure and no secure message exchange. The transport layer is responsible for reliable end to end data transfer [6].

The transport layer includes WTP runs at the head of the datagram service same like UDP. Both the UDP and the WTP are a part of the standard application from the TCP/IP to make the simplified protocol compatible to mobile terminals. WTP supports chaining together protocol data and the delayed response to reduce the number of transmissions. Fourth Security layer is providing security using WTLS .A secure transmission is crucial for certain applications such as E-commerce or WAP-banking and is a standard in these days. Furthermore WTLS contains a check for data integrity, user authentication and gateway security. Fifth Transport Layer represents the transfer or transmission layer and is also the interface of the network layer to all the above stacks/layers [7]. With the help of WDP the transmission layer can be assimilated to the specifications of a network operator. This means that WAP is completely independent from any network operator. The transport layer provide interface between the WAP protocol stack and network layer [8].

Benefits of WTLS

- The protocols works in conjunction with PKI (public key infrastructure) and wireless cookies for providing the security solution.PKI uses digital certificates to secure application platform and browsers.
- The WTLS provide data security, integrity, privacy, authentication of WAP devices.
- WAP provides the benefits to manufactures because of integrating a micro browser into their handsets which work on all WAP servers [9].

Drawbacks of WTLS

- Wireless devices consume less CPU power, less memory and more battery life when we used encryption techniques normally it consume a great deal of CPU usage, memory and bandwidth.
- Wireless networks provide less bandwidth, stability and reliability then the wired networks.
- The TLS protocols are used for providing secure communication over the internet. The TLS protocol stack divides into four layers – Application layer, handshake layer, record layer and transport layer each of these layers provides well defined interface.

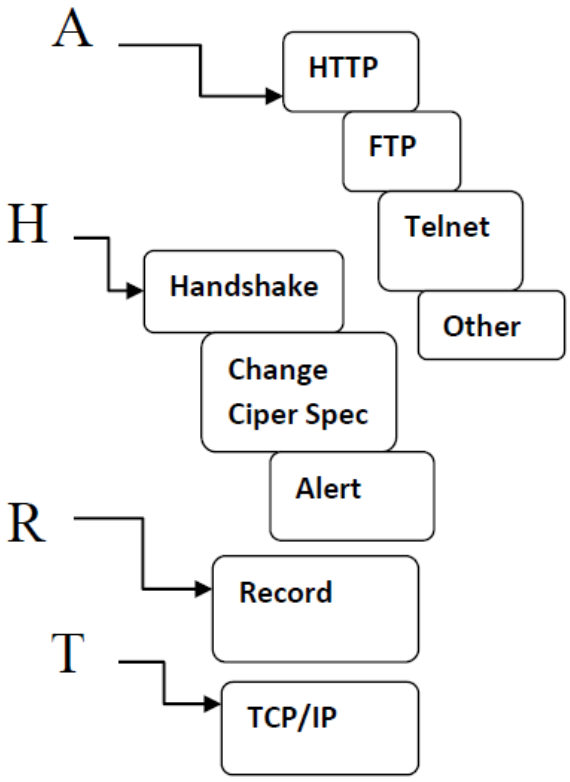

Fig 3: Protocol Stack for TLS

The TLS is used to provide data integrity and security for network communication. They use cryptographic methods to encrypt the data at the transport layer from end to end [9]. The application layer used HTTP, FTP, Telnet and others. The SSL/TLS operates on a layer between the transport layer and application layer [10]. In this position it can support multiple application layer protocols by securing the application data before sending it to transport layer. The TLS security protocol is divided into four specialized protocol. The Handshake protocol is responsible for the cipher suite negotiation, the initial key exchange and the authentication of the two sides [11]. The alert protocol offers some signaling to the other protocols. It can help informing the peer for the cause of failures and other error conditions the record protocol offers symmetric encryption, data authenticity and optionally compression.WAP provides failure in country like Japan and South Korea where only small amount of mobile users who are using mobile phones due to slow access speed [12].A WAP gateway is software which works as intermediate between the WAP client and www server [13].WTLS provided authentication, data integrity and privacy with low processing power [14]. WTLS generally uses RSA-based cryptography. However the protocol can also use elliptic-curve cryptography (ECC), which provides a high level of security with demanding fewer computing and memory resources [15].

request has to pass through gateway to www server the gateway would be act as a client. All the requests will be

3. MY CONTRIBUTION FOR PROVIDING END TO END SECURITY FROM WAP CLIENT TO WWW SERVER

My contribution in this paper is to provide the end to end security from WAP client to WWW server using Common Security Protocol (CSP). In the fig 4 there is no end to end security mechanism.

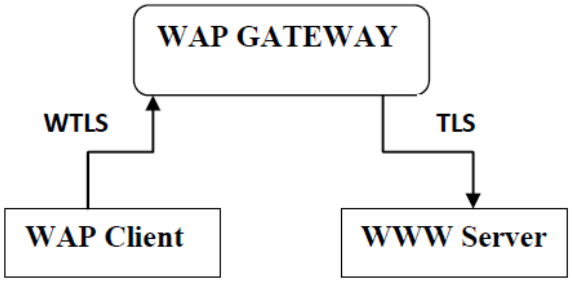

Fig 4: WTLS & TLS

When client encrypt the data and its is decrypted by WAP gateway by using the WTLS .At this time the communication is through the wireless media and again data is Re-encrypted by WAP gateway when it communicate through the wire. In this main time of Re-encryption any unauthorized person can hack the data because data is in air.

So it could be possible to design end to end security .In the below Fig 5 the WAP gateway working as sever when the communication go through the wireless media using the wireless transport layer security protocols and again the WAP gateway is working as a client when the communication go through the wired media.

4. PROVIDING SOLUTION OF END TO END SECURITY

A common security protocol (CSP) can be designed for providing end to end security from Wireless client to wired server.

CSP=WTLS+TLS

The common security protocol will work for wireless device and wired device. By using this technique, security mechanism can be improved and it could be possible to solve the problem of WAP gap. The common security protocol will help to provide security by using WTLS and TLS together. In table 1 security analysis of both protocols is done. When we combine the feature of both protocols, there will be common path between the wireless client and wired server.

In the Fig 5 the common security protocol (CSP) is equal to the WTLS and TLS .The WAP gateway is acting as server and client as well.

In Fig 5 when the request passes through WAP client to WAP gateway, the gateway would be act as server and when the

passed from wireless client to wired server with the help of gateway which act as intermediate between the both. After

responding to particular web page which is requested by client,

the requested response will be sent through www server to gateway. Now gateway would be act as a server. The gateway server would response the client request by opening the requested web page on micro browser in WAP enabled mobile phone.

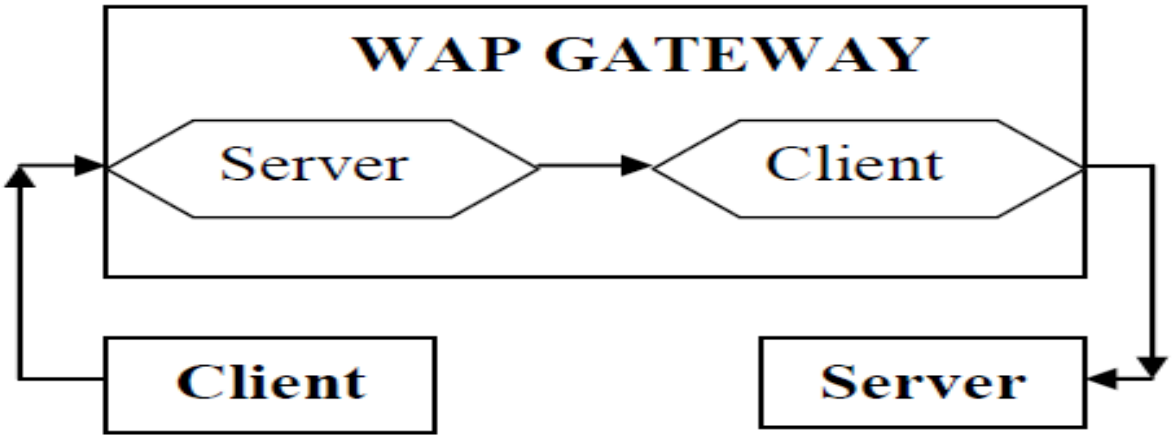

Fig 5: CSP=WTLS+TLS

In CSP,When the wireless sends a request to Gateway along with encryption technique, the Gateway will not decrypted there Then the request directly goes to www server and decryption algorithm will work there .This technique would be possible for removing the WAP gap and there would be a possibility of end to end security also.

The Table1 given below shows the security analysis of WTLS and TLS .The common security protocol would be designed with both the features of security protocol like WTLS and TLS. When both features will be added in CSP then it can work for wireless client and wired media.

Security analysis

- TLS and WTLS both use handshake protocol for selecting cipher spec and generating a master secret which combines the primary cryptography parameters associated with secure session. The handshake protocol can also optionally authenticate parties who have certificates signed by a trusted certificate authority.
- TLS and WTLS support three authentication modes like anonymous, server authentication, client side authentication.
- TLS and WTLS support RSA and on the other hand, Diffie Hellman key exchange with authentication.
- TLS uses hash functions very conservatively. Both MD5 and SHA are used in tandem to ensure that non-catastrophic flaws in one algorithm will not break the overall protocol.
- TLS and WTLS both support markup languages .With the help of CSP,it would be possible to design a common markup language for WTLS and TLS security protocol

Feature	WTLS	TLS
Handshake Protocol	Y	Y
Authentication Mode like Anonymous, Server authentication, Client server authentication	Y	Y
Key Exchange like RSA, Diffie Hellman	Y	Y
Hash Function likeMD5, SHA support	Y	Y

Table 1: Security analysis of WTLS and TLS

The three major differences between TLS and WTLS are [15]

- **Compressed Data Structures** – The Packet size has been reduced by using bit-fields, discarded redundancy and truncated cryptographic elements whenever possible
- **Compressed Certificate Format** - The format follows the X.509v3 certificate structure but uses smaller data structures

- **Packet Based Instead of Stream Based** - TLS is designed to be used over a data stream and a significant part of the design of WTLS has allowed it to be used in a data packet environment so that protocols such as Short Message Service (SMS) would be used as data transport.

5. CONCLUSION

This paper has discussed about the CSP (common security protocol) for WTLS and TLS. The security architecture of WAP consists of three parts: the mobile phone, the WAP gateway and the Internet. In already developed system, The WAP gateway decrypts all the WTLS traffic and encrypts all the TLS traffic. The security analysis for both protocols, including WTLS for wireless communication and TLS for wired server has been discussed in this paper.. This paper focused on the protocols hierarchy for WTLS and TLS. In this paper The gateway is represented as server as well as client. The architecture and the implementation of CSP would be design further. More improvements would be design in future for providing the end to end security.

6. REFERENCES

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

[2] Mohamad Hairol Jabbar, Mohd Abd Wahab, Nor Aisah Sudin, Ariffin Abdul Mutalib (2009). Accessing Academice Related Materials through WAP protocols", IJWA, Volume 1 Number 3.

[3] WAP introduction. Website link http://www.psit.in/psit/deepesh/wap.pdf.

[4] Fawad Nazir, Aruna Seneviratne. Towards mobility enabled protocol stack for future wireless networks" Ubiquitous Computing and communication journal", Volume 2 Number4 ,pp. 68-69 .

[5] Saurabh Singh, Dr. harsh Kumar verma (2011) .Security for wireless sensor network", IJCSE, pp. 2395-2396, volume 3 No 6.

[6] Sami Jormalainen, Jouni Laine.Security in the WTLS.Computer Science and Engineering Helsinki University of Technology.

[7] Danielyan, Edgar. 2008. WAP: Broken Promise or Wrong Expectations? CISCO. The Internet Protocol Journal. Volume 6 Number 2. Accessed from http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-2/wap.html.

[8] Complete WAP Security from Certicom pages 5-12.

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

[10] Burak bayoglu, "performance evaluation of wtls handshake protocol using rsa and elliptic curve cryptosystems by burak bayoglu"2004.

[11] Kuljeet Kaur. Article: Fortification of Transport Layer Security Protocol. IJCA Special Issue on Network Security and Cryptography NSC (2):11-14, December 2011. Published by Foundation of Computer Science, New York, USA.

[12] Ilpo Koskinen, Petteri Repo, Petteri Repo (2006)," WAP and Accountability: Shortcomings of the Mobile Internet as an Interactional Problem", Vol. 2, Issue 1, November, pp. 22-38.

[13] Niels Christian Juul and Niels Jørgensen (2003).The Security Hole in WAP: An Analysis of the Network and Business Rationales Underlying a Failure", Vol 7, pp.73-92.

[14] Sandra Kay Miller (2001).facing the challenge of wireless security". Technology news.July.pp-16.

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