INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

**ISSN: 2454-132X**
**Impact factor: 4.295**
***(Volume2, Issue6)***
Available online at: www.ijariit.com

# A Review on Wireless Transport Layer Security

**Chandan Sharma**
*Department of Computer Science*
*Career Point University*
*Hamirpur (H.P.)*
chandan786p@gmail.com

***Abstract - Wireless Application Protocol (WAP) is one of the technical standards for information over a mobile wireless network. Mobile devices such as mobile phones that use the protocol have a WAP browser as a web browser. WTLS (wireless transport layer security) inherited from TLS (Transport Layer Security). WTLS uses similar semantics adapted for a low bandwidth mobile device. As compared to TLS main changes are compressed data structures where possible packet sizes are reduced by using bit-fields, discarding redundancy and truncating some cryptographic elements. WTLS defines a compressed certificate format. This broadly follows the X.509 v3 certificate structure, but uses smaller data structures. Packet based design TLS is designed for use over a data stream. WTLS adapts that design to be more appropriate on a packet based network. WTLS design is based on a requirement that it be possible to use a packet network such as SMS as a data transport. There are number of WTLS security issues. WTLS processing more is fast as compared to using SSL. So it is suitable for wireless system. WTLS uses modern cryptography tools to enhance security. WTLS can provide different level of security for privacy, data integrity and authentications***

***Keywords— WTLS, WAP, WCMP, WAE, SSL.***

## I. INTRODUCTION

Wireless transport layer security can be integrated into WAP architecture on top of WDP (Wireless Datagram Protocol). WTLS can provide different level of security and has been optimized for low bandwidth, high delay bearer networks. WTLS is designed to use with low processing power and limited memory capacity of mobile devices. Cryptographic algorithm can be easily implemented with wireless transport security. WTLS uses key refresh mechanism to update keys in secure connection without using handshaking It also support datagram and connection oriented transport layer protocol. WTLS is required for wireless devices because mobile devices have much limitation. They have low processing power, low memory and small display. There are many problems faced in wireless communication such as less bandwidth, high latency and connection are unstable.

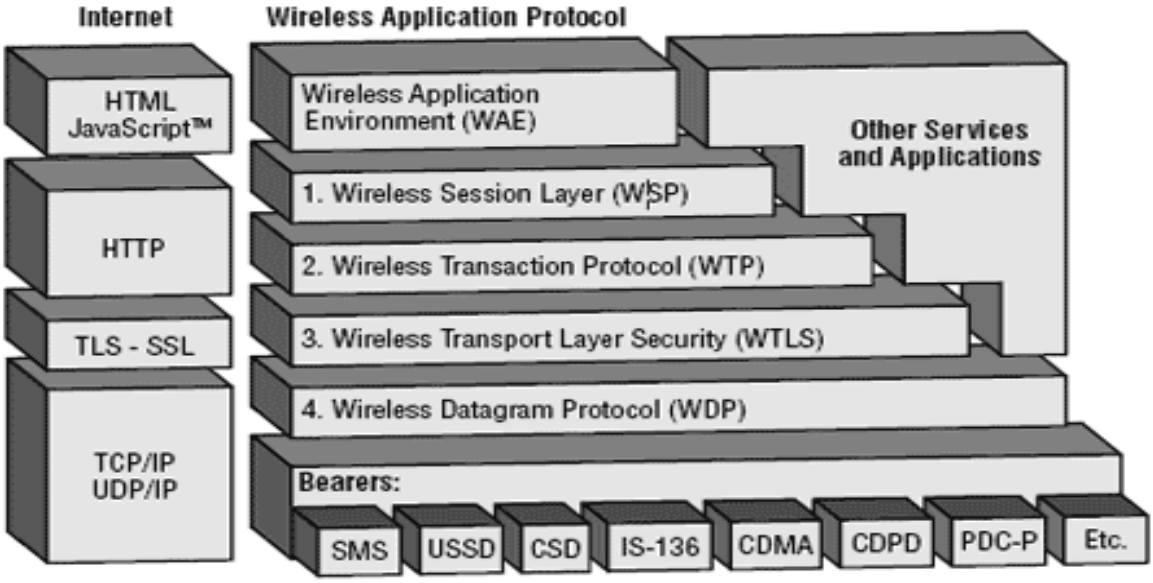
## II. WHAT IS ENCRYPTION

Encryption is method which encodes information or message in a way that unauthorised users can not access the data. In encryption data which is used for communication is called as plaintext. Encryption algorithms are applied on plaintext results in cipher text. Cipher text can be read by decrypting the data. Only authorized receiver can decrypt the data by using key provided by originator of message [5].TLS and SSL are both cryptographic protocols which provide encryption over internet. But TLS can apply same level of security without the requirement of dedicated TCP protocol [3].

## III. ARCHITECTURE OF WAP AND WTLS

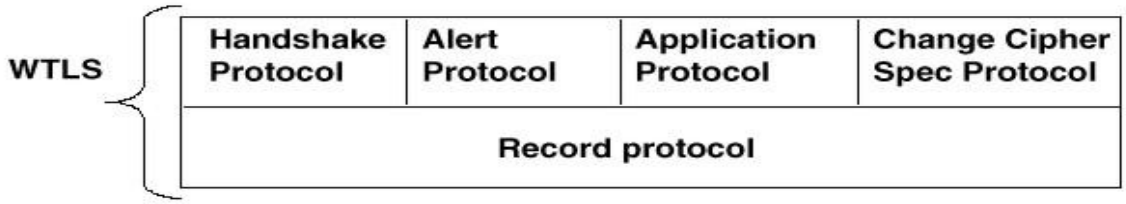
WAP architecture:-




WAP protocol architecture[8]

All communication in mobile devices is done using WAP gateway [6].In WAP, there are five different layers. First layer is Application Layer, this layer is also known as Wireless Application Environment (WAE). It is top layer in WAP architecture. By combining www and telephony services it provide environment for mobile devices. Devices can interact by using micro browser. Wireless session protocol support fast connection setup; suspend connection and reconnection [1]. Wireless transaction protocol is light weight protocol. Wireless transaction layer offer light weight transaction service. WTLS has been designed for use in wireless network system with narrow band width [2]. Wireless datagram protocol in transport layer protocol make WAP to independent of bearer services. WDP offers source and destination port numbers used for multiplexing and de multiplexing of data respectively. WCMP (Wireless Control Message Protocol) provides error handling mechanism for WDP [2].Main security problem in WAP is WAP gateway [6].WAP is advantageous to manufacturer because micro browser can be integrated into mobile devices

**WTLS architecture:** Main role of WTLS was to secure transaction in mobile devices without need of huge desktop level power supply and memory consumption. WTLS provide more data compression as compared to SSL. By these features mobile devices can securely communicate over internet. Without using handshaking technique, it can refresh keys in secure manner [3].




WTLS internal architecture [3]

In this architecture Change cipher spec protocol, Peer receives change cipher spec protocol sent by either client or server. Cipher spec message is sent during hand shake phase. Three types of alert message are used *i.e.* warning, critical and fatal. Critical alert message results in termination of current secure connection. All security related parameters such as cryptographic algorithms are agreed during handshake. Authentication in the WTLS is carried out with certificates. Authentication can occur between the client and the server or the client only authenticates the server [2]. WTLS is session oriented secure protocol layer pattern. In WTLS client and server can recalculate encryption key information. WTLS has facility to reject and detect data that is not successfully verified or data that is replayed. One of major difference between SSL (secure socket layer) and WTLS is that WTLS can be used only between

mobile devices and WAP gateway. While SSL can be used between internet and gateway [1]. Main role of WTLS protocol is in commerce applications to provide authentication, integrity and privacy protection [5]. By default WTLS uses elliptic curve cryptography (ECC) . Main benefit of using elliptic curve cryptography is that it uses small size keys. WTLS define its own certificate format optimized for limited bandwidth [6].WTLS can be used with PKI (Public key infrastructure) and wireless cookies to provide security. Digital certificates are used by PKI for security.[7]

## IV. ISSUES

WTLS provide different level of security level. End to end service is not provided by WAP. WTLS is used only between mobile device and gateway. But SSL is used between gateway and server. So data remain unencrypted for some time, which leads to privacy issues related to confidential data [1]. If application accesses another server by gateway, additional mechanisms are needed for security of end to end connection [2]. Some of messages sent in clear text and are not authenticated. An alert message is assigned a sequence number; an active attacker may replace an encrypted datagram with an unauthenticated plaintext alert message with the same sequence number without being detected by anybody [3]. Encryption provided in hand held device cannot be strong due to low power. If there is strong encryption requirement then extra encryption techniques are required. WTLS. Normally wireless devices consume less CPU and less memory, less battery. But using this type of encryption techniques lead to consumption of more CPU, memory and power.

## CONCLUSION

WTLS can provide different level of security for privacy data integrity and authentication and has been optimized for low bandwidth high delay network. WTLS takes into account low processing power and very limited memory capacity of mobile devices for cryptographic algorithms. WTLS took many features from TLS but it has optimized handshaking between peers. WTLS has some new features such as datagram support, dynamic key refreshing and optimized handshaking. WTLS may or may not be used depending on security level to be implemented. Future work include consistent support for application level security e.g. digital signatures and different implementation classes with different capabilities

## References

[1] V Yadav, M Verma and Nisha. 2015. A Survey paper on wireless access protocol. *International Journal of Computer Science and Information Technologies*, Vol. 6 (4): 3527-3534.

[2] J. Schiller. 2000. *Mobile communication*. Pearson Education Limited, Great Britain.

[3] B. Parmar Paresh & Ketan Patel. 2016. A Survey paper on wireless transport layer security. *International Journal of Science and Research*, Vol. 5(4): 1743-1745.

[4] S Jormalainen & J. Laine 1999. Security of WTLS. *Computer Science and Engineering* Helsinki University of Technology.

[5] V. A. A. S. Perera, E. A. M. K. B. Ekanayake, S. S. Shurane, P.A. I. Udayanga, J. P. Maharajage, R. M. C. Bandara and D. Dhammearatchi. 2016. Enhancement WPA2 protocol with WTLS to certify security in large scale organizations inner access layer Wi-Fi media associated devices. *International Journal of Scientific and Research Publications*, Vol. 6 (4): 197 -202.

[6] D Singelee & Bart Preneel, ESAT-COSIC, K.U. Leuven, Belgium. 2005, The Wireless Application Protocol. *International Journal of Network Security*, Vol. 1 (3): 161–165.

[7] Kamini. Conceptualizing Common Security Protocol for Wireless Client and Wired Server. 2012. *International Journal of Computer Applications*, Vol. 42 (5):14-18.

[8] https://www.tutorialspoint.com/wap/wap_architecture.htm