International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Survey Paper on Wireless Transport Layer Security

Parmar Paresh B.[1], Ketan Patel[2]

[1]G.M.F.E, Himmatnagar

[2]Professor, G.M.F.E, Himmatnagar

Abstract: ***WAP is the protocol that is a secure data communication for the wireless environments developed by the WAP Forum. WTLS(Wireless Transport Layer Security) is the proposed protocol for secure communication in the WAP. The purpose of WTLS is to provide secure and efficient services in the wireless Internet environment. However, the existing WTLS handshake protocol has some security problems in several active attacks. Therefore, in this paper, we analyze the securities of the existing protocol, and then propose a security enhanced WTLS Handshake protocolWTLS was specifically designed to conduct secure transactions in the mobile devices,without requiring desktop levels of processing power and memory. WTLS processes security algorithms faster by minimizing protocol overhead, and enables more data compression than the traditional SSL approach. As a result, WTLS can perform security within the constraints of wireless networks. These optimizations mean that smaller, portable devices can communicate securely over the Internet. WTLS also provides a key refresh mechanism to update keys in a secure connection without handshaking. The frequency of the key refresh is agreed on during the handshake. In the key refresh, a new key block is generated using the master secret key, the message sequence number and other parameters.***

Keywords: WTLS

1. Introduction

WTLS was specifically designed to conduct secure transactions in the mobile devices, without requiring desktop levels of processing power and memory. WTLS processes security algorithms faster by minimizing protocol overhead, and enables more data compression than the traditional SSL approach. As a result, WTLS can perform security within the constraints of wireless networks.All Algorithm mine only Sequence Database or in terms of WTLS also provides a key refresh mechanism to update keys in a secure connectionwithout handshaking. The frequency of the key refresh is agreed on during thehandshake. In the key refresh, a new key block is generated using the master secret key.

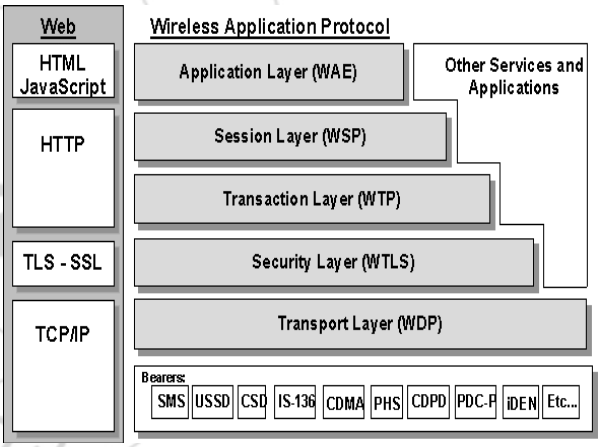
2. Wireless Requirement & WAP

Mobile terminals have several fundamental limitations. They have less powerful CPUs and memory, restricted power consumption, smaller displays, and different input devices than the typical desktop computers. Moreover, the mobile networks also have limitations that must be taken into account. These include less bandwidth, more latency, less connection stability and less predictable availability.

3. WAP Architecture

The WAP is developed by the WAP Forum to provide specifications for developing applications that operate over wireless communication networks. The WAP is a five layerprotocol stack that contains an application layer, a session layer, a transaction layer, asecurity layer, and a transport layer. The WAP defines a set of protocols in each layer. The main purpose of having a layer protocol stack is that the communication with a certain layer is made through well-defined interfaces. Thus, changing something in one layer does not imply changing all other layers.

The WAP has a layered architecture, which can be easily compared to the web model.

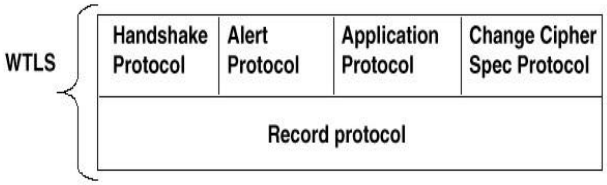


WEB & WAP Mode

4. WTLS Architecture

WTLS was specifically designed to conduct secure transactions in the mobile devices, without requiring desktop levels of processing power and memory. WTLS processes security algorithms faster by minimizing protocol overhead, and enables more data compression than the traditional SSL approach. As a result, WTLS can perform security within the constraints of wireless networks. These optimizations mean that smaller, portable devices can communicate securely over the Internet. WTLS also provides a key refresh mechanism to update keys in a secure connection without handshaking. The frequency of the key refresh is agreed on during the handshake. In the key refresh, a new key block is generated using the master secret key. The message sequence number and other parameters.

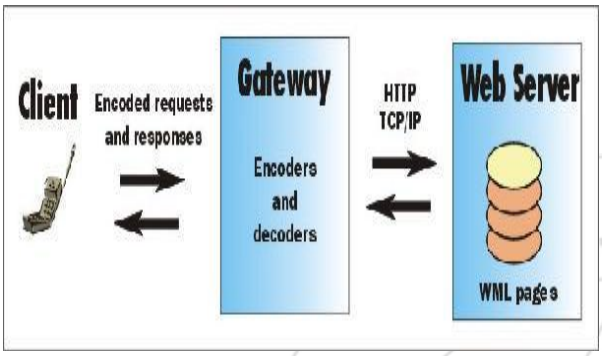
Licensed Under Creative Commons Attribution CC BY



5. WAP& WTLS Applications

5.1 WAP Gateway

The programming model used in Internet is adopted to WAP as much as possible.



WAP Gateway Functionality
The encoders translate WAP content into compact encoded formats to reduce the size of the transferred data over the network. This model allows the content and the application to be hosted on standard Internet HTTP servers and to be developed using existing Internet -------technologies like CGI, application servers, and servlets. The illustration below demonstrates the concept.

5.2 WAP Browser

In order to communicate with the WAP gateway, the mobile client must have some WAPbrowser. Many wireless devices use the generic WAP browser. A generic browser fulfils the mandatoryrequirements of the WAP specifications as well as most usable optional requirements, including WTLS. It is independent of bearer services and network technologies, and the device's operating system, so it can easily be integrated to any host environment. A typical browser usually requires the client to have at least 300KB of RAM. However, the browser uses about 25KB of RAM. The executable program uses static memory and can be stored in ROM. If the mobile device does not support ROM, persistent memory (hard disk, flash memory, etc.) is used instead. Persistent memory is not a mandatory requirement for the browser. If persistent memory is available, it can be used to store user preferences, application data, history list and favorites.

5.3WTLS Toolkit

There are many WTLS toolkits available for creating secure encrypted sessions between online-networked applications. Most toolkit allows the developer to integrate WTLS data encryption capabilities into any applications. This entails the ability to initiate and receive WTLS-secured connection and to configure the security parameters to be used for privacy, integrity and authentication. Most toolkits supports:

- Anonymous and authenticated Elliptic Curve Diffie-Hellman (ECDH) keyexchange and Elliptic Curve Digital System Algorithm (ECDSA) schemes at 163-
- bits,
- 768-bit and 512-bit anonymous and authenticated Diffie-Hellman,
- Anonymous and authenticated 1024-bit and 512-bit RSA,
- DES, Triple-DES (RC5 and IDEA are less commonly supported) for symmetric
- MD5 and SHA-1 for message authentication. They also support WTLS certificate and X.509 v3 certificates.

5.4 Security

A number of potential security problems have been identified in the WTLS.The adoption of TLS has at least partly led to some security problems including the chosen plaintext data recovery attack, the datagram truncation attack, the message forgery attack and the key-search shortcut for some exportable keys. [19], [22]

- The predictable initiation vectors (IVs) in CBC can lead to chosen-plaintext attacks. In WTLS, the IV for encrypting each packet is computed by XOR'ing the original IV with the sequence number of the packet. Unfortunately, the sequence numbers are sent without encryption.
- The 40-bit XOR MAC in WTLS does not provide any integrity protection when stream ciphers are used, regardless of the key length. The XOR MAC works bypadding the message with zeros, dividing it into 5-byte block.
- Using PKCS#1 version 1.5 padding, RSA messages can be decrypted with 220chosen ciphtertext queries. The WTLS bad_certificate and decode_error may provide an oracle for an intruder. A system has an oracle if it tells the intrude whether the used key is correct. A brute force attack can be mounted because the correct key can always be recognized with the trial decryption.
- Some alert messages in WTLS are sent in clear text and are not authenticated. Since an alert message is assigned a sequence number, an active attacker mayreplace an encrypted datagram with an unauthenticated plaintext alert messagewith the same sequence number without being detected. This leads to a truncation attack that allows arbitrary packets to be removed from the data stream.
- Under some exportable keys, the IV of each packet can be determined from the Hello messages and the sequence number alone.
- An eavesdropper can determine the change of keys by reading the contents of this record_type field, which is sent unencrypted. The existence of error messages can also be determined from this same record_field, though the exact nature of the encrypted error messages cannot be determined.
- WTLS includes pre-defined primes along with generators that are used in Diffie-Hellman computations, but the group order is left specified. The absence of the group order makes it impossible to check that the give value belongs to the correct multiplicative subgroup

Licensed Under Creative Commons Attribution CC BY

6. What is TLS Encryption?

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocol thaprovide communication security over the Internet. Compared to SSL, TLS has the advantage of applying nearlthe same level of security without the need for a dedicated TCP port.

Advantages

- It is relatively simple, well-understood, standard technology.
- It applies to both a message body and its attachments.
- Implementation is inexpensive and simple
- Doesn't require any end user training, awareness, or changes to the desktop
- Works with self-signed (free) certificates
- TLS adoption is high compared with other encryption methods, especially in the financial services industry

Disadvantages:

- Only encrypts the message while in transit, not sender-to-recipient
- Cannot establish the identity of the sender, just the sender's gateway.

7. Conclusion

The Wireless Application Protocol (WAP) is a result of continuous work to define anindustry-wide specification for developing applications that operate over wireless networks. The security layer protocol WTLS operates above the transport layer protocol. The WTLS is optional so it may or may not be used depending on the required security level of the application. The WTLS layer provides data privacy, data integrity, and authentication between two communication parties. The WTLS provides functionality similar to TLS but incorporates new features such as datagram support, optimized handshake, and dynamic key refreshing. Additionally, it is optimized for low-bandwidth bearer networks with relatively long latency. The WAP PKI with WTLS will provide additional security services of authorization and non-repudiation. There are numerous technologies available for secure wireless communications. Among them are WTLS, Bluetooth, 3GPP, SIM Toolkit, Imode, SET, and IPSec. WTLS is the only one in the list that is both optimized for the wireless communication and nonproprietary.

References

[1] Radhamani, G., Ramasamy, K.: Security Issues in WAP WTLS Protocol. In: IEEE 2002 International Conference on Communication, Circuits and Systems and West Sino Expositions, vol. 1, pp. 483–487,2002

[2] Kwak, D.J., Ha, J.C., Lee, H.J., Kim, H.K., Moon, S.J.: A WTLS Handshke Protocol with User Anonymity and Forward Secrecy. In: Lee, J.-Y.,Kang, C.-H. (eds.) CIC 2002. LNCS, vol. 2524, pp. 219–230. Springer, Heidelberg ,2003

[3] WAP Forum, Wireless Application Protocol Wireless Transport Layer Security Specification version, February 18 ,2000

[4] Oh, S.H., Kwak, J., Lee, S.W., Won, D.H.: Security Analysis and Applications of Standard key Agreement Protocols. In: Kumar, V., Gavrilova, M.L., Tan, C.J.K., L'Ecuyer, P. (eds.) ICCSA 2003. LNCS, vol. 2668, pp. 191–200. Springer, Heidelberg ,2003

[5] Dierks, T., Allen, C.: The TLS Protocol version 1.0, IETF RFC 2246,pp.481-486,January 1999

Licensed Under Creative Commons Attribution CC BY