WAP and the WTLS

Presented by Mark A. Shaw
CS 522 Final Project Report
Professor Chow
Due: 12-10-04

Abstract

The Wireless Application Protocol (WAP) is a communications protocol for small, wireless and mobile devices e.g. Mobile Phones, Personal Digital Assistants (PDA's), Pagers etc. that allow these devices to connect to the Internet as part of the "Mobile Computing" revolution that has exploded since 1997. Many of these wireless and mobile devices are being used to handle sensitive data such as financial information making security one of the most important factors in controlling the growth and development of the underlying WAP technology. Although WAP is still an evolving protocol, its popularity has diminished in favor of 802.1x technology. The hardware restriction of the devices in which WAP is used adds to the complexity of the design of the perfect wireless protocol. Since WAP is seen as a way to get Internet to small wireless and mobile devices, all the security concerns currently involved with wired internet should also be considered along with the ones that are particular to wireless communications in general. Because of this, efforts are being put into developing new and more powerful secure alternatives. The Wireless Transport Layer Security (WTLS) is the security layer in the WAP protocol and bears close resemblance to the Secure Sockets Layer (SSL) and its successor, the Transport Layer Security (TLS) but takes into account the specific features of the wireless environment.

1. Introduction

The WAP protocol bridges the gap between the wireless mobile world and the Internet and offers the ability to deliver an unlimited range of wireless services to mobile subscribers independent of their network, bearer and terminal. Mobile subscribers can access information from a pocket-sized device as they would from a desktop PC. This paper is an attempt to understand the WAP and the WTLS. This paper is structured as follows: First section gives a brief overview of WAP and the WAP forum. The next Section covers the WTLS security layer for the WAP from a fundamental and technical viewpoint. Since WAP is still an evolving protocol, an attempt is also made to highlight the security related problems present in old version (WAP 1.0) and steps taken to solve some of it in the latest release (WAP 2.0), some security issues due to gateway based design, and implementation of security through WTLS are explained. Finally, I give my interpretations on the future of WAP followed with my conclusion and a list of my resources.

2. Introducing WAP

2.1 The WAP Open Mobile Alliance

The WAP Open Mobile Alliance is the industry association that is responsible for developing and nurturing the growth of the specification of the Wireless Application Protocol (WAP), the communications protocol that allows mobile users of wireless hand-held devices to securely access and interact with Internet-based content, applications and services. It was founded in 1997 by SonyEricsson, Motorola, Nokia and Phone.com. It is currently comprised of hundreds of members from worldwide device manufacturers, carriers, infrastructure providers, software developers and wireless solution providers. The latest specification version is WAP 2.0 released in July of 2001.

2.2 The WAP Architecture

Figure 1. illustrates what may be considered the typical WAP networking environment based on gateway-based implementation of WAP.

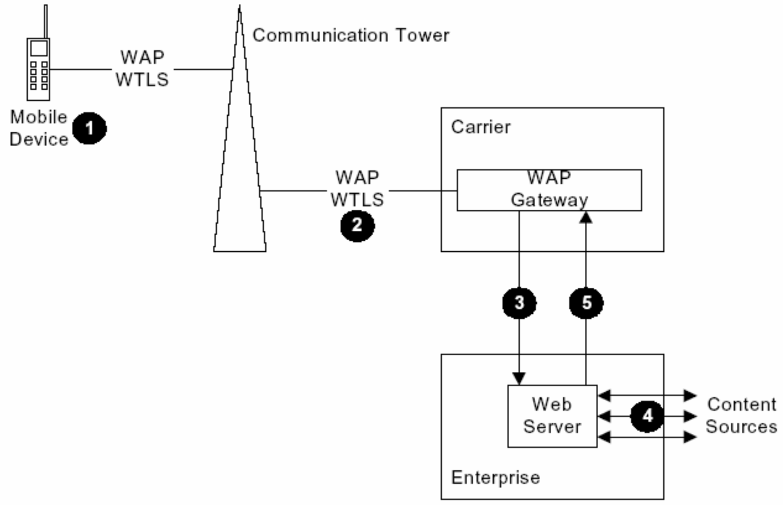

Figure 1.

Using the numbers in the black circles in Figure 1. the basic working architecture of WAP environment can be put in following words. (1) WAP devices call a dial-in server that gives them an IP address, either by using an ISDN or an analog modem protocol, PPP is the standard protocol that is used for Internet dial-up connections. (2) Over the RAS (Remote Access Services) connection, the telephone will send and receive packets via WAP over WTLS. It routes through the applicable communications tower to the carrier to interface with a WAP gateway. Gateways are similar to proxy servers in wired network implementations. The mobile phones are configured to use a certain one no matter what WAP site is being accessed. The WAP gateway is the entity that connects the wireless domain with the Internet via Secure Sockets Layer (SSL). (3) In the United States, the most common configuration for the gateway is to reside on the carrier's infrastructure. Elsewhere, the gateway commonly resides inside the enterprise. Frequently, this is a security response to the so-called WAP Gap, the brief point during which WTLS is converted to SSL and is therefore unencrypted (WTLS is incompatible with SSL due to the stripped down implementation to accommodate mobile devices with limited bandwidth). The gateway converts WAP to HTTP and WTLS to SSL and then forwards the request to the applicable Web server. (4) The Web server issues HTTP requests for content from other sources, which return Wireless Markup Language (WML). The Web server sends the WML (via HTTP over SSL) to the gateway. (5) The gateway converts the HTTP to WAP (and SSL to WTLS) before sending the WAP content back through the communications tower to the mobile device. (In configurations where the gateway resides in the enterprise, the protocol conversions take place in the same manner, but the WAP content is sometimes sent directly to the communications tower, depending on the requirements of the carrier.)

The WAP architecture follows the layering model similar to OSI. The following figure 2. compares the two protocol stacks.

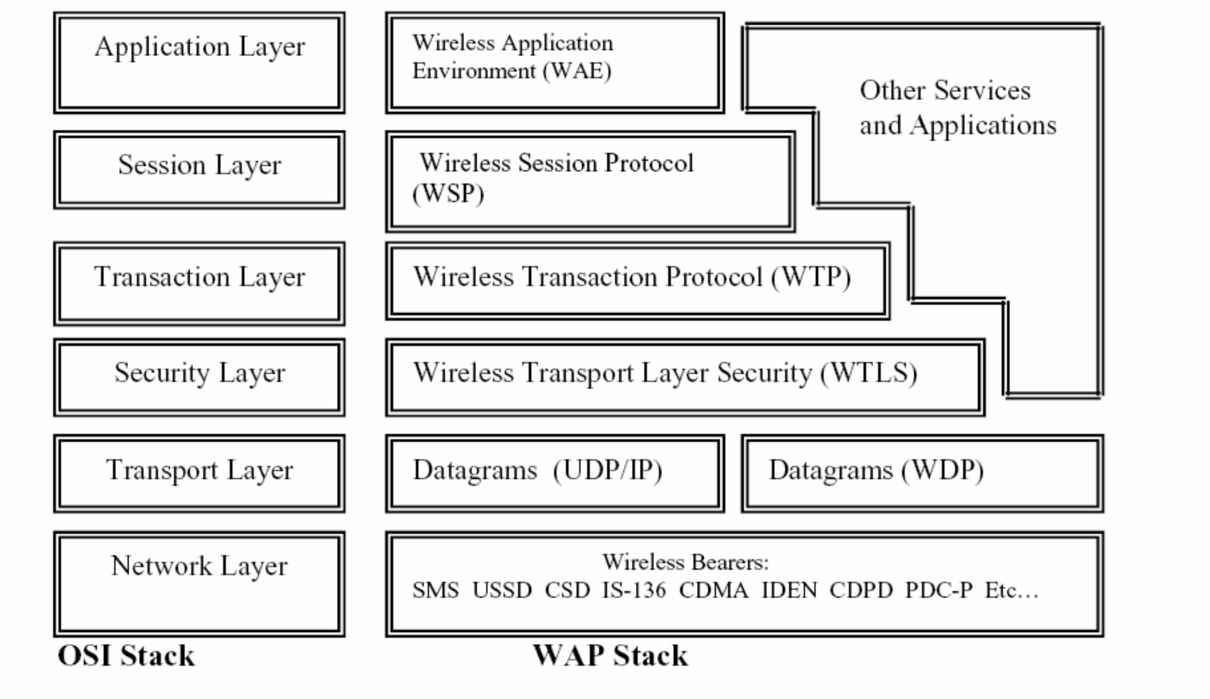
Application Layer
Session Layer
Transaction Layer
Security Layer
Transport Layer
Network Layer
OSI Stack
Wireless Application Environment (WAE)
Other Services and Applications
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
Datagrams (UDP/IP)
Datagrams (WDP)
Wireless Bearers:
SMS USSD CSD IS-136 CDMA IDEN CDPD PDC-P Etc…
WAP Stack

Figure 2.

A brief summary of the layer functionality is in order:

1. WAE defines the user interface on the device.

2. WSP is the WAP equivalent of HTTP. This layer links the WAE to two session services a connection oriented service operating over WTP and a connectionless service operation above the WDP.

3. WTP is the WAP equivalent of TCP or UDP, it provides reliable or unreliable communication. WTP supports Protocol Data Unit concatenation and delayed acknowledgment to help reduce the number of messages sent.

4. WTLS incorporates security features that are based on TLS.

5. WDP allows WAP to become a bearer independent by adapting the transport layer of the underlying bearer. WDP presents a consistent data format to the higher layers of the WAP protocol stack.

2.3 The WAP Gateway

The functionality and design of the WAP gateway is important to know one of the major security issues concerned with WAP, a point I brought up earlier known as the WAP-Gap. WAP enabled devices are characterized by their limited capacities of processing power (CPU), storage capacity (memory), input/output and power (battery). Also, the mobile networks implemented for which these devices communicate are characterized by limited bandwidth, higher latencies, high packet-loss and long lasting sessions. The Open Mobile Alliance's only requirement pertaining to a document to be delivered from a web server to mobile device is that it should be written in WML, which is ordered and sent in a request-reply cycle. The WAP Gateway provides the following functionalities working with all the above constraints:

1. Encoding/Decoding transport protocols. Since the gateway connects wired and wireless devices, it has to convert requests, replies etc from one protocol format to another to pass message from source destination. Here it is done between the TCP/IP stack and WAP.

2. Data Compression: The gateway applies so-called loss-less data compression on the WML documents before sending it to the mobile device to reduce the data that is transmitted to and from the mobile device.

3. Compilation: If a WML document contains embedded source code (like WMLScript), the gateway compiles such a code into a bytecode format, something that relieves the mobile device the daunting of the task of parsing the code.

4. Decompression: The gateway reads and interprets the original WSP request, which is in a compact form that cannot be understood by the web server. It translates a symbolic Internet address to an IP number working as DNS for mobile devices.

2.4 The WAP-Gap

The basic security feature of WAP provides secrecy in the two parts. First part is on the path that connects the WAP client and the gateway and the second part is between the gateway and web server. The data stream is encrypted with WTLS between the WAP device and WAP Gateway, and then with SSL between the WAP Gateway and the Web server. SSL is not directly compatible with WTLS, so the WAP Gateway decrypts the SSL-protected data stream coming from the Web server and re-encrypts it using WTLS before passing the data on to the WAP device. This brief period when the data is unencrypted is commonly called the WAP Gap and is one reason why most WAP gateways would be installed inside a corporate firewall. While SSL uses 128-bit encryption, WTLS usually uses 56-bit (or more) encryption. The WAP Gateway uses the encryption size the WAP device reports during handshaking that it can support. The processing done on the un-encrypted data corresponds to the protocol layers above the security layer. The fact that the data exists in its "original un-encrypted" form though for a short amount of time is the problem. With the current technology and improvement in hacking methodologies it’s not difficult to gain access to the data when it is in un-encrypted form in gateway.

3 Wireless Transport Layer Security (WTLS)

WAP communications are protected using the WTLS protocol. WTLS provides entity authentication, data confidentiality and data integrity. It is based on the IETF SSL/TLS protocols with new functionalities like datagram support, optimized handshake and dynamic key refreshing.

There are three different classes of WTLS:

Class 1: Anonymous encryption. Data is encrypted, but certificates are not exchanged between the client and the gateway.

Class 2: Encryption with server authentication. Data is encrypted and the client requires a digital certificate from the server.

Class 3: Encryption with client and server authentication. Data is encrypted and the client and the server exchange digital certificates.

3.1 The WTLS Handshake

The WTLS handshake is very similar to the SSL handshake. The following figure 3. illustrates the most common form of the WTLS handshake that for WTLS class 2 optimized handshake. This involves the client authenticating the gateway, but not vice versa.

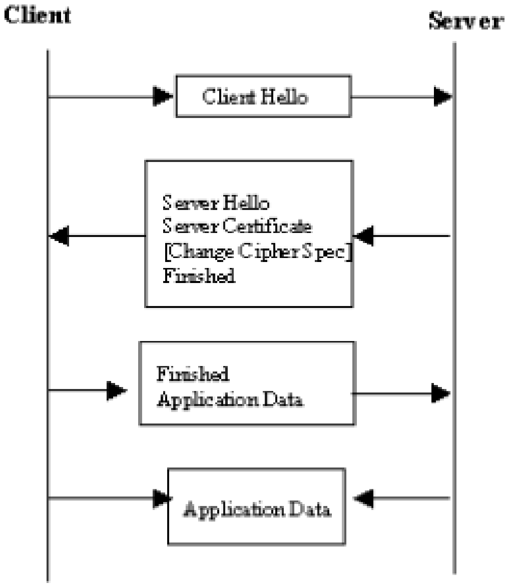

Figure 3.

The following figure 4. illustrates the WTLS handshake that is for the WTLS class 3 full handshake. This involves the client authenticating the gateway and the gateway authenticating the client.

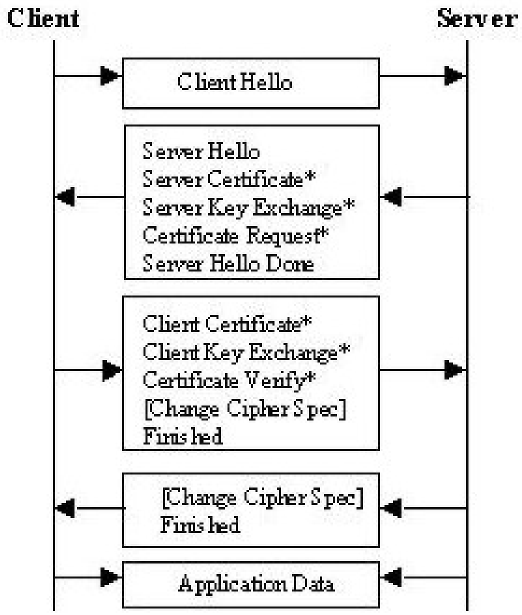

Figure 4.

The WTLS protocol is composed of three layers:

1) The WTLS handshake protocol manages secure connection, provides client and server authentication and is used to exchange key material.

2) The WTLS record layer provides privacy and data integrity.

3) The alert layer is used to report error conditions to each other and to handle the close alert.

The WTLS protocol defines the following key exchange algorithms:

1) Anonymous key exchange algorithms based upon RSA and Diffie-Hellman key exchange.

2) Key exchange algorithms with authentication based upon RSA key exchange with RSA based certificates or Elliptic Curve Diffie-Hellman key exchange with Elliptic Curve Digital Signature Algorithm based certificates.

3) Symmetric-key based handshake where both parties share a secret key that is used as the pre-master key as such.

WTLS uses an encryption technique called public key cryptography, in which the WAP Gateway sends the WAP client a public key for encrypting information that only the Gateway can decrypt with a private key it holds. To accommodate the unreliability and unpredictability of connectionless datagram communication (WDP), messages are always packed as one Record Protocol Layer packet when sent in one direction, to ensure that they are either received or lost on the other side. A Digital Certificate is very important for customer authentication and non-repudiation. The X.509 Certificate is the most widely accepted Internet standard. The WTLS certificate is similar to the X.509 certificate but is coded more compactly, and satisfies the high latencies and low bandwidth of wireless networks, as well as the limited processing resources of WAP Customer devices. The record layer provides data integrity by calculating and verifying message authentication code. Currently SHA-1, MD5 (HMAC based) and SHA-1 (XOR based) algorithms are used. The privacy is taken care by encrypting and decrypting data using bulk ciphers using algorithms like RC5, DES, 3DES and IDEA. One of the plus points that comes because of the way the WTLS protocol and its functioning has been designed is it makes it very less attractive for crypto analysis for the following reasons. In WTLS many connection state parameters can be recalculated during a secure connection. This feature is called key-refresh. It is performed in order to minimize the handshakes. In key refresh the values of MAC secret, encryption key, and IV will change due to change in sequence number.

4. Security Flaws in WTLS

Though the WTLS is derived from TLS, changes made so that it works with wireless environment have resulted in many security flaws in WTLS. People have found many ways to attack WTLS.

1. Man-in-the-middle: These type attacks are possible since at least one anonymous key exchange is mandatory in WTLS. Any WTLS compliant client device must implement one of the anonymous handshakes.

2. Denials Of Service (DoS): These type attacks are very easy to carry out on WAP enabled devices using the WTLS because of the problem of IP spoofing is especially serious as UDP is used for transport.
client side port.

3. Predictable Initialization Vectors chosen for plaintext attacks against low-entropy secrets: Since WTLS should be able to operate over an unreliable datagram transport, when CBC mode is used, it is necessary for the IV (initialization vector) to be either contained in the packet itself (explicit IV, as in IPSec) or that the IV for that block is somehow derived from data already available to the recipient. WTLS uses a liner IV computation.

4. The XOR MAC and stream ciphers: The WTLS protocol supports among other MACs, a 40-bit XOR MAC. This works by padding the message with zeros, dividing it into 5-byte blocks and xoring these blocks together. If one inverts a bit position n in the ciphertext, the MAC can be made to match by inverting the bit (n mod 40) in the MAC. This can be repeated arbitrary number of times. Thus, when stream ciphers are used, the XOR MAC does not provide any integrity protection.

5. 35-bit DES encryption: The 40-bit DES encryption method is defined to use five bytes of keying material. Because of the parity bits contained in each byte of DES key, there are only 5 * 7 = 35 effective key bits in five bytes. This amounts to a reduction of the key space by a factor of 32. Therefore the strength of DES is not what is expected and key space need to be increased to make it more difficult for crypto analysis.

6. The PKCS#1 attack: The RSA signatures and encryptions are performed according to PKCS#1(Public Key Cryptography Standards) version 1.5. It has already been demonstrated that if the protocol includes an oracle that tells whether a given packet has correct PKCS#1 v1.5 padding, RSA messages can be decrypted with approximately 2^{20} chosen cipher-text queries.

5. Conclusion

The above material gives insight into some of the security issues present in WAP and WAP enabled devices. However, the position of WTLS in WAP protocol stack is somewhat perplexing, unlike the TLS, which is between the application layer and TCP layer. WTLS is between WTP and WDP. This implies the transfer of WTLS messages is not reliable and messages may be lost, duplicated, and re-ordered. But, the connection nature of a secure session requires the mechanism to guarantee reliability. Actually, I was somewhat surprised to see in the specification of WTLS that the Record Protocol even has sliding window protocol to deal with out-of-order messages. WTLS is far from a well-designed secure network protocol and WAP does have a looming technology that threatens to phase it out, and that is 802.1x. Many more areas, schools and businesses are embracing the new technology in favor of the high speeds and convenience. WAP was an interesting area of study, but I should have chosen a more recent technology like the 802.1x as the focus of my report.

References

[1]"*Security Issues in Mobile Commerce using WAP*", 15th Bled Electronic Commerce Conference, June 2002¸ Niels Christian Juul and Niels Jørgenson, < http://www.dat.ruc.dk/~nielsj/research/papers/wap-bled.pdf >

[2]"*Understanding WAP Security*", PC Network Advisor, Issue 131: June 2001,David Norfolk, < www.pcnetworkadvisor.com >

[3]"*Wired versus Wireless Security: The Internet, WAP and iMode for E-Commerce*". Paul Ashley, Heather Hinton, Mark Vandenwauver, IBM Software Group – Tivoli < http://www.acsac.org/2001/papers/61.pdf >

[4]"*Attacks Against the WAP WTLS Protocol*" Sami Jormalainen Jouni Laine, Helsinki University of Technology < http://www.hut.fi/~jtlaine2/wtls/ >

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

[6] "*Computer Networks*", Andrew S. Tanenbaum, fourth edition

[7] "*Secure Programming Cookbook for C and C++*", Viega and Messier