Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 2, No. 2 February, 2000

Wireless Application Protocol (WAP) Security: How does it work?

This issue of *Wireless Security Perspectives* is the first of a two-part series on the security of the Wireless Application Protocol, or WAP (see www.wapforum.org). WAP is the rapidly emerging de-facto world standard for the presentation and delivery of wireless information and telephony services on mobile phones and other wireless terminals. Because WAP is designed to provide applications over a broadcast, inherently insecure radiopath to the web, it requires a secure communications path between the client and the application server. The WAP specification provides a secure protocol for these transactions from a wireless handset or terminal.

WAP uses the Wireless Transport Layer Security (WTLS) protocol for providing security end-to-end security over a radio-link and interim networks. WTLS is based on the IETF (Internet Engineering Task Force: www.ietf.org) Transport Layer Security (TLS) protocol. TLS is based on the Secure Sockets Layer (SSL) protocol. This article focuses on the fundamentals of the SSL Version 3 upon which, therefore, WTLS is based. The second part in this series will focus on how WTLS has been optimized for use over narrow-band communication channels and how it differs from SSL and TLS. We will also discuss any known vulnerabilities. This issue of WSP is written to give the reader a detailed overview of the SSL protocol and its security capabilities. It should not be considered a comprehensive tutorial on the protocol. For a complete review of SSL, consult one of the numerous network security texts available.

Overview of WTLS

The WTLS protocol operates at one of the six layers of the WAP protocol stack. The WAP stack is a 'lightweight' protocol stack developed to minimize radiopath bandwidth requirements and guarantee that a variety of wireless networks can run WAP applications. The WAP protocol stack and the location of WTLS within this stack is shown in Figure 1. WTLS is the security layer sandwiched between the transaction layer and the transport layer. If the WTLS security protocol, is used, it operates above the transport layer that handles

We Now Accept Diners Club

We now accept Diners Club credit cards for subscriptions, back issue orders and other products. We will continue to accept American Express, Visa and MasterCard, as well as checks, money orders and bank transfers. Please choose the method of payment that is most convenient for you. The rumor that those that pay with Diners Club will get their monthly issues on rice paper is simply not true.

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security Perspectives* is $250 for one year (12 issues) for delivery within the US or Canada. International subscriptions are US$300 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees for more readers.

Current subscribers to *Cellular Networking Perspectives* receive a discounted price – only $200 for delivery within the US and Canada or $250 elsewhere.

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Month's Major Topic

WAP security, Part II.

Next Issue Due…

March 20th, 2000.

Future Topics

Voice over IP security • Public Keys & Wireless • Kerberos • Public Key Infrastructure • IP Security • IKE

Write to Us!

Tell us what you would like to see in future articles.

Wireless Security Perspectives is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada.
Contact Information: Phone: 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/wsp.html.
Subscriptions: $200 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$250 elsewhere. Non-subscribers pay $250/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery:** Email or 1st class mail. **Back Issues:** Available individually for $20 in the US and Canada and US$25 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

UDP or IP (Internet Protocol) datagrams and can be used to secure operations over several bearer networks including TIA/EIA-136 (D-AMPS), CDPD, and TIA/EIA-95 (CDMA). The availability of security layer will be critical for many applications such as e-commerce.

Figure 1: The WAP Protocol Stack

Layer	WAP Protocol
Application Layer	Wireless Application Environment (WAE)
Session Layer	Wireless Session Protocol (WSP)
Transaction Layer	Wireless Transaction Protocol (WTP)
Security Layer	Wireless Transport Layer Security (WTLS)
Transport Layer	Datagrams (WDP)
Network Layer	Wireless Bearers, including TIA/EIA-136 D-AMPS, TIA/EIA-95 CDMA, CDPD, iDEN, PDC, PHS and others.

WTLS Security Services

WTLS offers four basic security services for transactions between a client on a wireless handset connected to an application server:

- Authentication;
- Confidentiality;
- Data Integrity; and
- Denial-of-service protection.

Authentication

Authentication is the security service that ensures the proof of identity. Specifically, it ensures that a message sent in a transaction is correctly identified with an assurance that the identity of the sender is not false.

Confidentiality

Confidentiality, or privacy, is the security service that ensures that information in the transaction is accessible only for reading by authorized parties.

Data Integrity

Data integrity is the service that ensures that only authorized parties are able to modify information that is transmitted. Modification includes deleting, inserting or changing transmitted messages. Integrity ensures that data has not changed from its 'pure' or original state.

Denial of Service

Denial-of-service 'attacks' prevent or inhibit the normal use or management of a transaction or communications network, usually through overloading the system with phony transactions. This attack has become almost a household word with recent attacks against major websites such as Yahoo and Amazon.

Secure Sockets Layer (SSL)

Secure Sockets Layer is an open protocol designed by Netscape Communications Corporation after they recognized the need for a secure way to transmit data over the Internet. Netscape conceived of SSL and built it into their first web-browser in the mid-1990s. SSL is a protocol to protect communication between any SSL-enabled client and server software running on a TCP/IP network. SSL is most commonly used to secure data being exchanged between web browsers and web servers. SSL specifies mechanisms for providing data security layered between application protocols (e.g. HTTP) and TCP/IP. It provides data encryption, server authentication, message integrity, and optional client authentication for the TCP/IP connection.

SSL accomplishes its security goals between pairs of applications using three fundamental communication protocols:

- Handshake Protocol;
- Record Protocol; and
- Alert Protocol.

Handshake Protocol

The handshake protocol, the most complex part of SSL, allows the applications (client and server) to authenticate each other and to negotiate an encryption algorithm, MAC (message authentication code) algorithm and other cryptographic parameters to be used to protect the data during the session between the two entities. The handshake protocol is performed before any potentially sensitive application data is sent.

Record Protocol

The record protocol is used during the actual exchange of application data. During the record protocol, application data is first fragmented, or broken into smaller, more manageable blocks. Following the fragmentation step, the data is compressed (optionally) and sealed with a MAC. The integrity-protected data is then encrypted and transmitted to the receiving entity. The recipient decrypts the data, verifies the MAC (and decompresses the data) and reassembles the data for presentation to the application.

Alert Protocol

The Alert protocol is used simply to indicate any errors during the session or is used if the session is being terminated.

A simplified illustration of the Handshake protocol is depicted in Figure 2. This figure shows the initial exchange required to establish a connection between a client and server. This exchange of information may be viewed as having four phases:

1. Establishment of client-server security capabilities;
2. Server Certificate and Key Exchange;

3. Client Certificate and Key Exchange; and
4. The Finish.

Phase 1: Establishment of Client-Server Security Capabilities

The client and server exchange security capabilities used during their logical connection. This exchange, initiated by the client, includes: the highest SSL version understood by the client; a timestamp nonce (number used only once) and random number nonce used to protect against replay attacks; a session identifier to indicate a new or existing connection; a CipherSuite (cryptographic algorithms supported by the client), and compression methods supported by the client. After the client exchange, the server initiates a similar hello message with the same parameters. SSL allows for various well-known, standard, and robust cryptographic algorithms including Diffie-Hellman, triple DES, and SHA-1 (Secure Hash Algorithm) to be negotiated during the CipherSuite parameter flow at Phase 1.

Phase 2: Server Certificate and Key Exchange

During Phase 2, the server sends one or more (a chain of) X.509 public-key certificates. These are used by the client to authenticate the server. Also, the server exchanges a list of acceptable root certificate authorities (CA).

Phase 3: Client Certificate and Key Exchange

Phase 3 occurs after the client validates the server. The client sends its certificate if requested by the server and if available. The client also exchanges keys with the server as negotiated previously.

Phase 4: The Finish

Phase 4 completes the establishment of a secure connection. This phase includes transmission of a change_cipher_spec message (using the simple SSL Record Protocol) to cause the two communicating entities to update their operational states to be that of their pending states. Last, finish messages are transmitted to both entities using the previously negotiated algorithms and keys. The finish message verifies that the key exchange and authentication processes completed successfully.

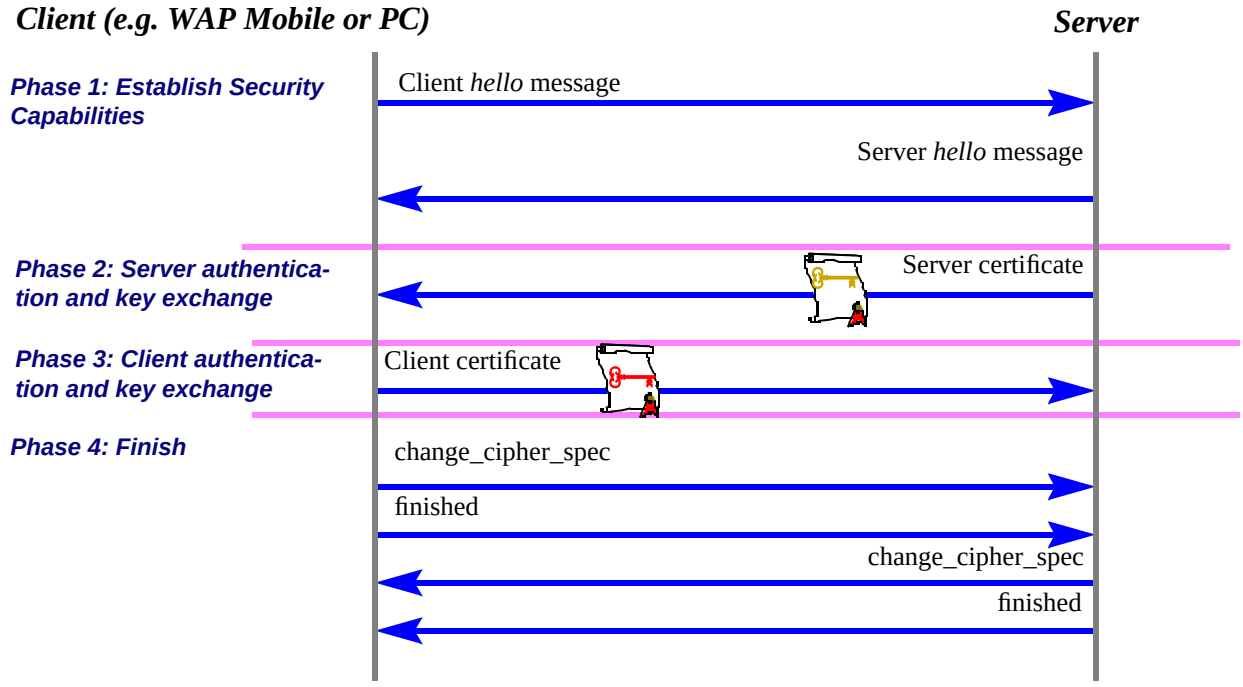
After both the client and server have completed the Phase 4 exchange, the SSL handshake is complete and the two entities may begin to exchange application layer data.

Advantages of SSL

SSL, the Secure Sockets Layer protocol has been used for securing web connections for more than five years now. As discussed above, it is fairly simple, flexible and has proven robustness against Net adversaries. SSL provides the following three basic security services:

- **Connection privacy**. Following the SSL handshake protocol, symmetric cryptographic protection between client and server is provided to prevent unauthorized listeners – prying eyes – from reading the application layer data, such as credit card numbers.
- **Peer Authentication**. Using asymmetric public-key cryptographic techniques, both the client and server can authenticate one another. The two ends of the link have assurance of the party to whom they are communicating.

Figure 2: The SSL Handshake Protocol



- **Connection Reliability**. Message transport includes data integrity checking using a keyed message authentication code. As a result, 'active attacker' adversaries cannot delete, add, or modify messages that are communicated between the client and server.

Conclusions

In this issue, we have explored SSL, the underlying security protocol of WTLS, in some detail. As noted above, SSL provides three important security services for client-server connections. In the next edition of WSP, we will highlight the differences between SSL and WTLS and list additional salient characteristics specific to this protocol used in the wireless environment for WAP. We will also explore known vulnerabilities and comment on its use for the inherently insecure wireless world.

To Probe Further

For more information on SSL, go to:

home.netscape.com/eng/ssl3

For more information on TLS, download the IETF specification at:

ftp://ftp.isi.edu/in-notes/rfc2246.txt

For more information on WTLS, visit WAP forum at:

www.wapforum.org

List of Acronyms

DES	Data Encryption Standard
CA	Certificate Authority
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
MAC	Message Authentication Code
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WAP	Wireless Application Protocol
WSP	Wireless Security Perspectives
WTLS	Wireless Transport Layer Security

Book Review: *The Code Book* by Simon Singh

The Code Book (Doubleday, 1999, ISBN 0-385-49531-5) is an accessible history of the making and breaking of codes. With an eye on the current interest in the Elizabethan era, the author opens by describing how the use of codes and code-breaking resulted in the downfall of Mary Queen of Scots. If the title had not already been taken, perhaps the book should have been entitled *The Code Breakers*, because the author seems to find the breaking of codes more fascinating than the making of them. The continual tussle between code makers and code breakers throughout history makes for fascinating reading, particularly as many of the names are familiar to anybody with a background in world history.

It is the wealth of historical details (and absence of mathematical details) that make the book more than another dry history of codes. Who was the Man in the Iron Mask? Do the papers encoded with Louis XIV's "Great Cipher" reveal that the prisoner was a cowardly general? Or were they just a trap to convince future code breakers (200 years later) of a false identity? And, how did the British government advertise for code breakers in WW II without revealing what they were looking for, yet precisely target people with the right stuff?

Singh takes a segue out of the normal domain of code-breaking, via US soldiers who used Amerindian languages to communicate in a way that Germans or Japanese were unable to understand. Through this he cleverly branches into a discussion of the decoding of Egyptian Hieroglyphics and Linear B, using techniques very similar to those applicable to the breaking of intentionally secret codes. It is unfortunate that he did not also discuss the much more recent decoding of the Mayan alphabet.

The book covers all the bases in modern cryptology, including World War II's Enigma machine, Diffie-Hellman key exchange and Public-Key cryptography: both the establishment's RSA and the counter-culture PGP (Pretty Good Privacy).

The book ends with a discussion of the emerging field of Quantum Cryptography. This was the weakest part of the book, because it argues that this mechanisms is unbreakable, illustrating the same over-confidence that has plagued code-makers in the past. Since it has not been shown yet that Quantum Cryptography is even a practical technique, perhaps it would be safe to reserve judgment on whether implementations are as secure as the theory seems to be.

It is very easy to read a popular book on secret codes and understand it superficially, but never take time to put that knowledge into practice. The author tempts readers to try their hand at breaking various types of codes through "The Cipher Challenge", a series of interlinked, and progressively harder, ciphers. Starting with a Simple Monoalphabetic Substitution Cipher, he forces the would-be prize winner to decode a Caesar Shift Cipher, Monoalphabetic Cipher with Homophones, Vigenère Cipher, and on up to the famous World War II Enigma machine cipher. It is almost certain that anyone could make $15,000 more easily and more quickly by flipping burgers at Macdonalds, but think of the fame and glory of being the first to crack the complete series of codes!

The Code Book is highly recommended for anyone with an interest in cryptography, especially those who do not want to tackle the more precise, but more impenetrable mathematical descriptions of cryptography found in many other books.