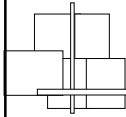


Wireless Communications and Security Issues Associated with the Wireless Application Protocol (WAP).



By: Ilkay Cubukcu

cubukcu@cs.fsu.edu

10/01/2002

Overview

■ WAP/WTLS

■ WTLS Protocols

■ WTLS Report Protocol

- ✧ Handshake Protocol
- ✧ Alert protocol
- ✧ Application Protocol
- ✧ Change Cipher Spec Protocol

■ WTLS vs TLS

■ WAP and CPAL

■ Some other wireless protocols and CPAL

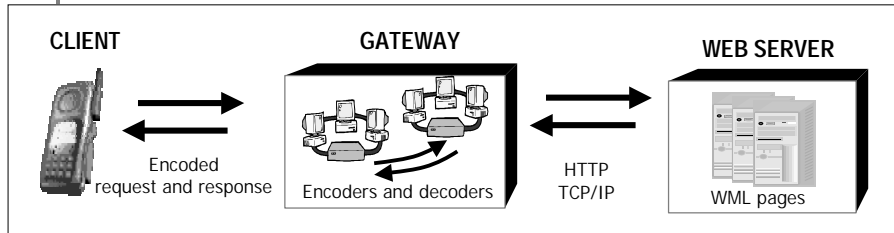
I. What is WAP?

- **WAP (Wireless Application Protocol)** is an open specification which offers a global standard method to develop applications over wireless communication networks.
- It is useful for enabling fast and easy information delivery and service to the mobile users.

I. What is WAP(continued)?

- **The devices which uses WAP:** Handheld digital wireless devices such as,
 - ❖ *mobile phones*
 - ❖ *paggers*
 - ❖ *two-way-radios*
 - ❖ *smart-phones*
 - ❖ *communicators from low-end to high-end.*

I.WAP Network Programming Model



- WAP connects the wireless domain and the Internet. The main function acts as a protocol gateway, encoder and decoder.
- The gateway translates request from the WAP stack to Internet protocol stack.
- Encoders translate WAP content into compact encoded format for reducing the size of the data.

10/1/02

ilkay Cubukcu

5

I. End-to-End Security in WAP

- The WAP security is ensured by two protocols:
 - ❖ **WTLS** (*Wireless Transaction Layer Security*): the WAP Gateway encrypts the content before it is sent over the wireless Network and then mobile phone can decrypt it and display the information to the user.
 - ❖ **HTTPS** (*Hypertext Transport Protocol Security*): The WAP Gateway connects to the web servers via the secure port in the same way that desktop Internet browsers (Netscape or IE) can also do.

-- The HTTPS component is the SSL-enabled equivalent of the IP*Works! HTTP component. The main difference is the introduction of a set of new properties and events that deal with SSL security

10/1/02

ilkay Cubukcu

6

I.WAP Protocol Stack

- Application Layer (WAE)
- Session Layer (WSP): Provides the ways to establish a session from client to server, agree on used protocol functionality, exchange content, suspend and resume sessions.
- Transaction Layer (WTP): Delivers request from client to the server and responses from server back to client. Runs at the top of datagram service.
- Security Layer (WTLS): Operates above transport protocol layer and provides upper level layer of WAP with a secure transport service interface.
- Transport Layer (WDP): This is supported by various types of network. Upper layers utilize the interface which is offered by WDP.

10/1/02

ilkay Cubukcu

7

WTLS Internal Architecture overview

- WTLS Record Protocol:
 - ❖ It is a layered protocol that accepts raw data from upper layers and applies the encryption algorithms to the data.
 - ❖ After this process, received data is *decrypted*, *verified*, *decompressed* and then sent to the higher layers.

10/1/02

ilkay Cubukcu

8

1- Change Cipher Spec Protocol:

It consists of a single message which is encrypted and compressed under the current connection state (not pending). The message consists of a single byte of value 1.

```
Struct {  
    Enum { change_cipher_spec(1), (255) } type;  
    } ChangeCipherSpec;
```

- It is sent either by client or server to notify the other party. Sending this message means, the sender has set the current write state to the pending state and, when a ChangeCipherSpec is received, the receiver should set the current reading state to pending state.
- Change cipher spec message is sent during the handshake and after the security parameters are agreed upon.
- To protect the finished and subsequent messages under the newly negotiated Cipher Spec and keys, implementations must check that this message is sent or received before sending and receiving the finished message verify.

10/1/02

ilkay Cubukcu

9

2- Alert Protocol :

Connection is closed when using alert messages. Alert messages are sent using the current secure state, compressed and encrypted, or if NULL cipher spec, no compression and encryption.

There are three types of alert messages:

Warning messages

Critical messages: termination of the current secure connection. Other connections using the secure session may continue and the secure identifier may also be used to establish a new secure connection.

Fatal messages: After this message sent, both parties terminate the secure connection.

Other connections using the secure session may continue but, failed connection is not used for establishing new secure connections because the session identifier must be invalidated.

- ❖ Handling errors in WTLS is based on the type of the alert messages. When an error is detected, then the detecting party sends an alert message with the occurred error. Other processes depend on the level of the occurred error.

10/1/02

ilkay Cubukcu

10

3- Handshake Protocol:

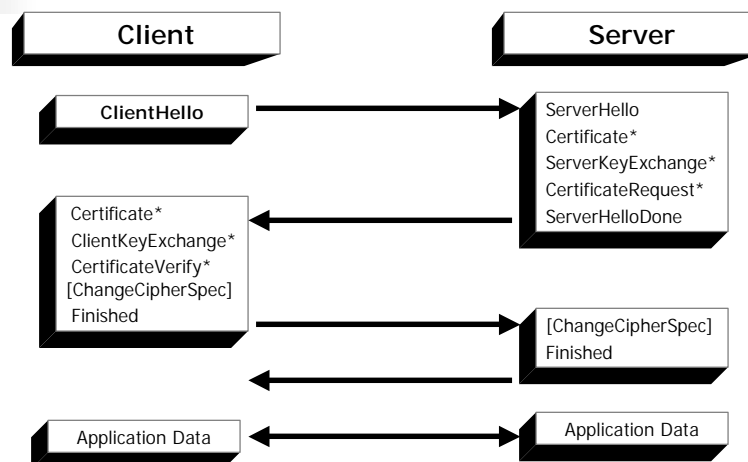
All security related parameters agreed on during the handshake. After the communication started between client and server, they use the same protocol version, select cryptographic algorithms, authenticate each other, and use public key encryption techniques to generate a shared secret.

$A \rightarrow B : E_{PK_B} (I_A, A)$
 $B \rightarrow A : E_{PK_A} (I_A, I_B)$
 $A \rightarrow B : E_{PK_B} (I_B)$

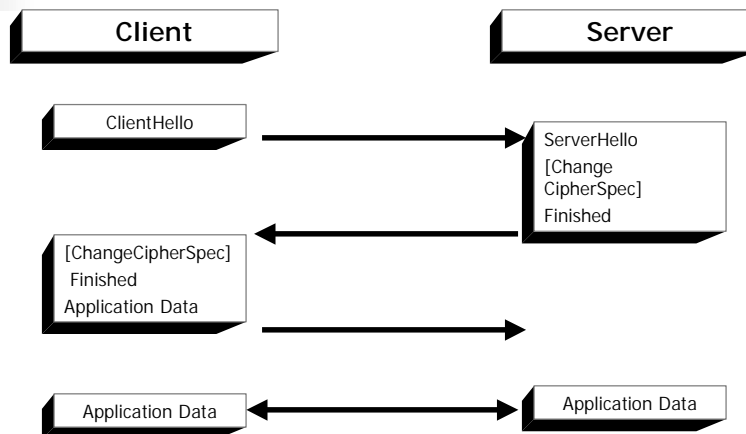
Handshake Protocol: The client sends a client hello message to which the server must respond with a server hello message, or else a *fatal error* will occur and the secure connection will fail. The ClientHello and ServerHello are used for security enhancement capabilities between client and server.

ClientHello and ServerHello establish the attributes, Protocol Version, Key Exchange Suite, Compression Method, Key Refresh, and Sequence Number Mode. The random values ClientHello.random and ServerHello.random are generated and exchanged.

Message flow for a full handshake



Message flow for an abbreviated handshake



10/1/02

ilkay Cubukcu

13

Abbreviated Handshake

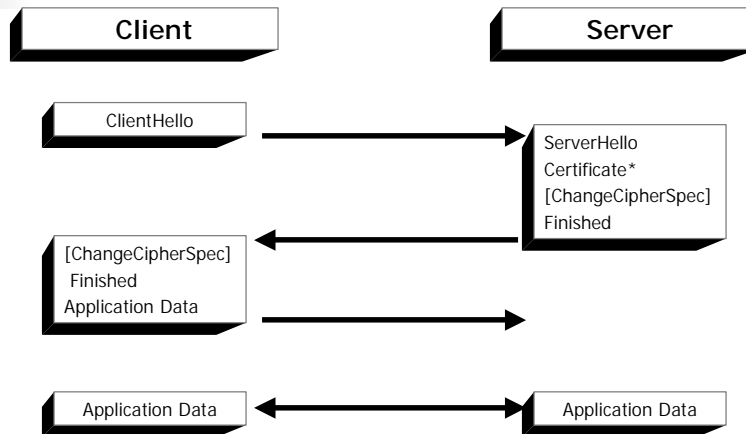
- If the client and server decide to resume a previously negotiated session then the handshake can be started by sending a ClientHello message where the SessionIdentifier is initialized with the identifier of the previous session.
- If both parties share a common session identifier then they may continue the secure session.
- Parties can start using the connection after they have confirmed the session informed the party with the change CipherSpec message.
- Only the Hello and Finished messages are sent
- Both parties must have a shared secret which is used as a pre-master secret.

10/1/02

ilkay Cubukcu

14

Message flow for an optimized full handshake



10/1/02

ilkay Cubukcu

15

Optimized Full Handshake

- Server can retrieve client's certificate by using the trusted third party, based on the information provided in ClientHello.
- The provided information by certificates both parties are able to complete the shared secret values by using the Diffie-Hellman key Exchange.
- Server sends ServerHello, Certificate and Finished messages and Client sends ClientHello and Finished messages.

10/1/02

ilkay Cubukcu

16

Comparison between internet and WAP architecture

	<i>Internet</i>	<i>WAP</i>
Content Development	HTML JavaScript	WML WM script
Web Application Delivery	HTTP	Wireless Session Protocol Wireless Transaction Protocol
Secure Connectivity Protocol	TLS SSL	Wireless Transport Layer Security (WTLS)
Basic Transport Protocol	TCP/IP UDP/IP	Wireless Datagram Protocol Bearer Network: SMS, CDPD, CDMA, GSM, TDMA, etc

10/1/02

ilkay Cubukcu

17

WTLS

- **Wireless friendly version of TLS**
- **Several differences designed to:**
 - optimize bandwidth use
(low bandwidth bit/sec, byte/sec)
 - accommodate unreliable link
 - reduce client code size and processor requirements

10/1/02

ilkay Cubukcu

18

Major differences between WTLS and TLS

- **Datagram support**
- **No fragmentation**
- **Key refresh for long-lived connections**
- **Optimized handshaking**
- **Shared-secret handshake**
- **Compact certificate (WTLSCertificate)**

Shorter parameters

- **Shorter parameters**
- **Cipher suite negotiation**
- **Algorithms**

10/1/02

ilkay Cubukcu

19

III. CPAL-ES

(Cryptographic Protocol Analysis Language Evaluation System)

- CPAL-ES uses Dijkstra's Weakest Precondition(wp) for analyzing the security protocols.
- This method analyses the goals and actions of the algorithms for producing wp which will satisfy the given goals. Because security protocols are algorithms, we can use this technique for formally verifying the ability of principles in protocols to reach their goals.

10/1/02

ilkay Cubukcu

20

III. CPAL-ES (continued)

- The protocols which are analyzed with CPAL-ES are specified in CPAL which requires a formal specification of the protocol.
- The Protocols are described as the series of actions in CPAL.
- CPAL Protocol specification actions are assignments, encryption, decryption, hashing, verifying, signing, function operation, sending and receiving messages, assertions and conditional tests.

III.wp(Weakest Precondition)&CPAL

- In wp, the preconditions guarantee that the target will be reached after the last statement and iteratively finds the guaranteeing precondition of the previous statement which means the process analysis starts at the end of the protocol and proceeds to the beginning.
- Each statement in CPAL modifies the predicate and resulting predicate will be the verification condition for the protocol.
- The symbols used in CPAL describe the operations done by protocol participant.



III. BAN Logic and CPAL-ES

- BAN Logic is a combination of formula notation and some rules.
- The evaluation of CPAL-ES with BAN Logic is a very powerful, and useful tool.
- When CPAL-ES and BAN Logic techniques are combined, the principal actions in protocol will be used with CPAL operators for send, receive, encrypt, decrypt, etc.

10/1/02

ilkay Cubukcu

23



III. BAN Logic and CPAL-ES (continued)

- The protocol assumptions used as BAN Logic predicated or as operations on values are included as CPAL ASSUME statement.
- Protocol goals are denoted in CPAL ASSERT statement.
- The GOODKEY predicate is essential to the BAN Logic evaluation process, and its translation is much harder than the other predicates.
- wp definition of statement allows CPAL-ES to force sequencing on the steps in each protocol, solving the permutation problem of BAN Logic. CPAL-ES does not replace BAN Logic, but complements BAN Logic by analyzing protocols using BAN Logic constructs.

10/1/02

ilkay Cubukcu

24



Next:

- ~~PART-II : Atena/Strand Spaces, Graph Theory~~
- PART-II: Some wireless protocols and CPAL ?
 - 802.11 (*Mishra, Arbaugh*)
 - Privacy and Authentication for Wireless Local area Networks (*Aziz, Diffie*)
- PART-III : WAP and CPAL-ES/wp, BAN Logic