ISSN:0975-9646

Vikash Yadav et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3527-3534

A Survey Paper on Wireless Access Protocol

Vikash Yadav[1], Monika Verma[2], Nisha[3]

[1,2]*Department Of Computer Science & Engg.,*
Harcourt Butler Technological Institute Kanpur, India,

[3]*Department Of Information Technology,*
Dr. Bhimrao Ambedkar Engineering College Bijnor, India,

Abstract -The Wireless Application Protocol (WAP) is a protocol stack for wireless communication networks. WAP uses WTLS, a wireless variant of the SSL/TLS protocol, to secure the communication between the mobile phone and other parts of the WAP architecture. Originally, WAP was designed with a gateway in the middle, acting as the interpreter between the Internet protocol stack and the Wireless Application Protocol stack. The WAP gateway forwards web content to the mobile phone in a way intended to accommodate the limited bandwidth of the mobile network and the mobile phones limited processing capability. However, the gateway introduces a security hole, which renders WAP unsuitable for any security-sensitive services like Banking.

Keywords: WAP gateway, WTLS, WML, WML Script.

1. INTRODUCTION

The Wireless Application Protocol (WAP) is a new advanced intelligent messaging service for digital mobile phones and other mobile terminals that will allow you to see Internet content in special text format (WML Wireless version of HTML) on special WAP-enabled mobile phones. Enabling information access from handheld devices requires a deep understanding of both technical and market issues that are unique to the wireless environment. There is a constraint on the use of mobile devices or terminal in the internet due to limited CPU, memory, battery life etc. Wireless network in which it is working is constraint by limited bandwidth, high latency. WAP specification addresses these issues by the use of best of existing standards and developing new extensions when needed.

Need for WAP:

- WAP enables any data transport
  - TCP/IP, UDP/IP, GUTS (IS-135/6), SMS, or USSD.
- It optimizes the content and air-link protocols
- It utilizes plain Web HTTP 1.1 servers
  - leverages existing development methodologies
  - utilizes standard Internet markup language technology (XML)
  - all WML content is accessed via HTTP 1.1 requests
- WML UI components map well onto existing mobile phone user interfaces
  - no re-education of the end-users
  - leveraging market penetration of mobile devices
- Several modular entities together form a fully compliant Internet entity

WAP: "Killer" Applications

- Location-based services
  - Real-time traffic reporting, Event/restaurant recommendation
- Enterprise solutions
  - Email access, Database access, "global" intranet access
  - Information updates "pushed" to WAP devices
- Financial services
  - Banking, Bill-paying, Stock trading, Funds transfers
- Travel services
  - Schedules and rescheduling, Reservations
- Gaming and Entertainment
  - Online, real-time, multi-player games
  - Downloadable horoscopes, cartoons, quotes, advice
- M-Commerce
  - Shopping on the go
  - Instant comparison shopping
  - Location-based special offers and sales

In section II of this paper we are going to discuss the principle on which WAP is designed. In section III we will discuss the WAP model and working of WAP i.e. how mobile client communicate with the server with the help of WAP gateway. In section IV we will discuss WAP Protocol Stack that is required for communication in wireless network. It shows protocols that are required for communication in wireless environment. In section V we will discuss WAP architecture that shows how communication is going to takes place between the client and server. In section VI we will discuss security problems associated with the WAP like use disclosure of unencrypted data at WAP Gateway. In section VII we will discuss security services provided by WAP. In Section VIII we will discuss security solutions for security hole at the WAP like placement of gateway at that location where the server is placed there by providing the same security them as with the server and at the end we will conclude this paper.

2. PRINCIPLE

The WAP uses a client-server approach. It incorporates a relatively simple **micro browser** into the mobile phones, requiring only limited resources on the mobile phones. This makes WAP suitable for thin clients and early smart phones.WAP puts the intelligence in the **WAP Gateway** whilst adding just a micro browser to the mobile phone

themselves. Micro browser based services and applications reside temporarily on servers, not permanently in mobile phones. The WAP is aimed at turning **"mass-market"** mobile phones into a "**network based smart phones**". The philosophy behind the Wireless Application Protocol's approach as per WAP Forum is to utilize as few resources as possible on the handheld device and compensate for the constraints of the device by enriching the functionality of network.

WAP Micro browser:

To browse a standard internet site you need a web browser. Similar way to browse a WAP enables website, you would need a micro browser. A Micro Browser is a small piece of software that makes minimal demands on hardware, memory and CPU. It can display information written in a restricted mark-up language called WML. Although, tiny in memory footprint it supports many features and is even scriptable. Today, all the WAP enabled mobile phones or PDAs are equipped with these micro browsers so that you can take full advantage of WAP technology.

WAP gateway:

WAP gateway is a software system that helps WAP-enabled wireless devices to communicate to Internet Web sites and applications. Web sites deliver pages in special format called Wireless Markup Language (WML) that is compiled and forwarded by the WAP gateway. In order to access Internet resources from a WAP-enabled wireless device you need a WAP gateway service.

WAP tunnel:

WAP tunnel provides a free public WAP gateway service that works with all compatible WAP browsers. WAP tunnel allows WAP-enabled wireless devices to communicate to Internet Web sites and applications.

3. WAP MODEL

Before we describe WAP model, first we would like to describe how Standard Internet works.

The Internet Model:

The Internet model makes it possible for a client to reach services on a large number of origin servers, each addressed by a unique Uniform Resource Locator (URL). The content stored on the servers is of various formats, but HTML is the predominant. HTML provides the content developer with a means to describe the appearance of a service in a flat document structure. If more advanced features like procedural logic are needed, then scripting languages such as JavaScript or VB Script may be utilized. The Figure 1 shows how a WWW client request a resource stored on a web server. On the Internet standard communication protocols, like HTTP and Transmission Control Protocol/Internet Protocol (TCP/IP) are used.

The content available at the web server may be static or dynamic. Static content is produced once and not changed or updated very often; for example, a company presentation. Dynamic content is needed when the information provided by the service changes more often; for example, timetables, news, stock quotes, and account information. Technologies such as Active Server Pages (ASP), Common Gateway Interface (CGI), and Servlet allow content to be generated dynamically.

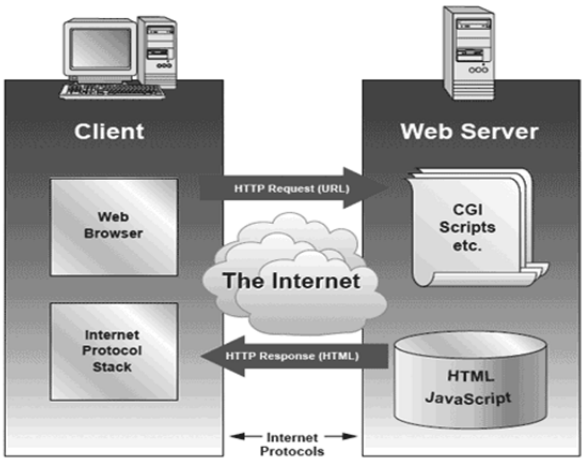

Figure 1: Processing of Client request to web server

The WAP Model:

The Figure 2 shows the WAP programming model. Note the similarities with the Internet model. Without the WAP Gateway/Proxy, the two models would have been practically identical.WAP Gateway/Proxy is the entity that connects the wireless domain with the Internet. You should make a note that the request that is sent from the wireless client to the WAP Gateway/Proxy uses the Wireless Session Protocol (WSP). In its essence, WSP is a binary version of HTTP.

A markup language - the Wireless Markup Language (WML) has been adapted to develop optimized WAP applications. In order to save valuable bandwidth in the wireless network, WML can be encoded into a compact binary format. Encoding WML is one of the tasks performed by the WAP Gateway/Proxy.

Working of WAP model:

A WAP request is routed through the WAP gateway, which acts as an intermediary between the bearer used by the client (GSM, CDMA, TDMA, etc.) and the computing network that the WAP gateway resides on (TCP/IP in most cases).

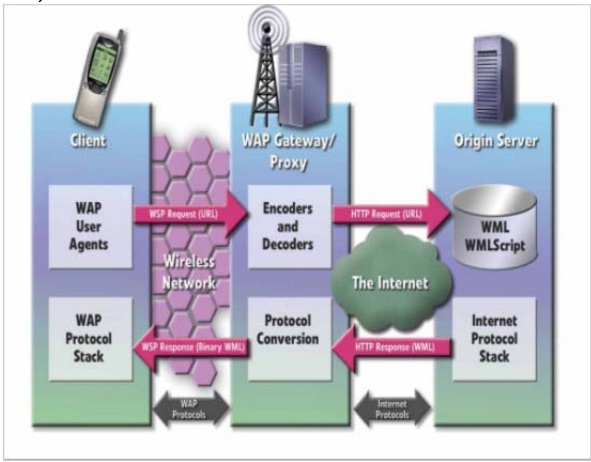

Figure 2: WAP Programming Model [4]

As shown in fig. 2 the gateway then processes the request, retrieves contents or calls CGI scripts, Java Servlets, or some other dynamic mechanism, and then formats data for return to the client. This data is formatted as WML (Wireless Markup Language), a markup language based

directly on XML. Once the WML has been prepared (known as a deck), the gateway then sends the completed request back (in binary form due to bandwidth restrictions) to the client for display and/or processing. The client retrieves the first card off of the deck and displays it on the screen. The deck of cards metaphor is designed specifically to take advantage of small display areas on handheld devices. Instead of continually requesting and retrieving cards (the WAP equivalent of HTML pages), each client request results in the retrieval of a deck of one or more cards. The client device can employ logic via embedded WML Script (the WAP equivalent of client-site JavaScript) for intelligently processing these cards and the resultant user inputs.

When it comes to actual use, WAP works like this:

- The user selects an option on their mobile device that has a URL with Wireless Markup language (WML) content assigned to it.
- The phone sends the URL request via the phone network to a WAP gateway using the binary encoded WAP protocol.
- The gateway translates this WAP request into a conventional HTTP request for the specified URL and sends it on to the Internet.
- The appropriate Web server picks up the HTTP request.
- The server processes the request just as it would any other request. If the URL refers to a static WML file, the server delivers it. If a CGI script is requested, it is processed and the content returned as usual.
- The Web server adds the HTTP header to the WML content and returns it to the gateway.
- The WAP gateway compiles the WML into binary form.
- The gateway then sends the WML response back to the phone.
- The phone receives the WML via the WAP protocol.
- The micro-browser processes the WML and displays the content on the screen.

4. WAP PROTOCOL STACK

WAP is designed in a layered fashion in order to enable the communication of browser requests from the mobile terminal to the web (content) server. As a result, the WAP protocol stack is divided into five layers as shown in Figure 3:

4.1. Application Layer:

Wireless Application Environment (WAE) is the top most layer in the WAP Architecture. It provides the general-purpose application environment based on a combination of WWW and mobile telephony technologies. It defines the user interface on the phone.WAE includes a micro-browser (Client software designed to overcome challenges of mobile handheld devices that enables wireless access to services such as Internet information in combination with a suitable network) and server environment which provides

1. Wireless Markup Language
2. WML Script
3. Content Format

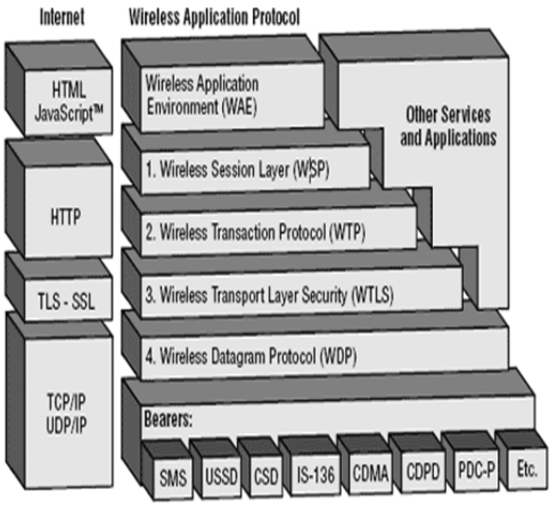

Figure 3: The WAP Protocol Stack

Various components of WAE:

- **Addressing model**
  Syntax suitable for naming resources stored on servers. WAP use the same addressing model as the one used on the Internet that is Uniform Resource Locators (URL).
- **Wireless Markup Language (WML)**
  A lightweight markup language designed to meet the constraints of a wireless environment with low bandwidth and small handheld devices. The Wireless Markup Language is WAP's analogy to HTML used on the WWW. WML is based on the Extensible Markup Language (XML).
- **WML Script**
  A lightweight scripting language. WML Script is based on ECMA Script, the same scripting language that JavaScript is based on. It can be used for enhancing services written in WML in the way that it to some extent adds intelligence to the services; for example, procedural logic, loops, conditional expressions, and computational functions.
- **Wireless Telephony Application (WTA, WTAI)**
  A framework and programming interface for telephony services. The Wireless Telephony Application (WTA) environment provides a means to create telephony services using WAP.

This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WML Script.

4.2. Session Layer:

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection i.e. WSP provide connection-based services to the application layer. Generally a session is started, content is exchanged and later on the session is closed. The session can also be suspended and resumed. WSP is the WAP equivalent of HTTP. Within WSP (and HTTP) is the concept of a request and a reply WSP also defines a server ”push” transaction where the server can send information to the client without the client requesting it. This may be used for broadcast

messages or for real-time services such as stock quotes or news headlines.

4.3. Transaction Layer:

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

WTP is the WAP equivalent of TCP or UDP. The Wireless Transaction Protocol (WTP) provides a lightweight transaction-oriented protocol that reliably delivers requests from the client to the server and responses from the server back to the client. WTP is message oriented Protocol.WTP operates efficiently over secure or non-secure wireless datagram networks. When the connection is unreliable it is the responsibility of WDP for retransmission to make the connection reliable. WTP is also responsible for packet segmentation and reassembly and for acknowledgment of packets and retransmission of lost, unacknowledged or corrupt packets. In order to avoid duplication WTP numbers each packet so that a retransmitted packet is not mistaken for a new packet. It provides Class 0, Class 1, Class 2 types of services.

- class 0: unreliable message transfer
  - unconfirmed Invoke message with no Result message
  - a datagram that can be sent within the context of an existing Session
- class 1: reliable message transfer without result message
  - confirmed Invoke message with no Result message
  - used for data push, where no response from the destination is expected
- class 2: reliable message transfer with exactly one reliable result message
  - confirmed Invoke message with one confirmed Result message
  - a single request produces a single reply

4.4. Security Layer:

Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

The WAP Transaction Layer Security, WTLS, is a session oriented, secure protocol layer patterned after the web's Secure Session Layer (SSL) and Transaction Layer Security (TLS) protocols.. One unique feature of WTLS is the ability of both client and server to independently recalculate encryption key information based on an embedded sequence number. WTLS is based on Transport Layer Security (TLS) 1.0 but optimized for narrowband communication channels. Key features of WTLS includes Integrity of message through the use of Message Authentication Codes (MAC), Confidentiality through the use of encryption, Authentication and non-repudiation of server and client using digital Certificate, .WTLS contains facilities for detecting and rejecting data that is replayed or not successfully verified (Denial-Of-Service protection).

4.5. Transport Layer:

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

WAP Datagram Protocol, WDP, is a datagram oriented, network layer Protocol that has came after the User Datagram Protocol (UDP) used on the Internet. WDP and UDP are identical for those networks where Internet Protocols are present. On networks where UDP is not available, WAP defines a UDP equivalent. These UDP equivalents are known as "mappings". The currently defined mappings create the equivalent of UDP over SMS, USSD, and other mobile data transports. WDP makes no attempt to confirm delivery, resend lost packets, or correct errors in transmission. This is left to the higher layer protocols.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilize the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

Note that the mobile network bearers in the lower part of the fig. 3 are not part of the WAP protocol stack.

5. WAP ARCHITECTURE

The WAP [2] model closely resembles the Internet model of working. In Internet a WWW client requests a resource stored on a web server by identifying it using a unique URL, that is, a text string constituting an address to that resource. Standard communication protocols, like HTTP and Transmission Control Protocol/Internet Protocol (TCP/IP) manage these requests and transfer of data between the two ends. The content that is transferred can either is static like html pages or dynamic like Active Server Pages (ASP), Common Gateway Interface (CGI), and Servlets.

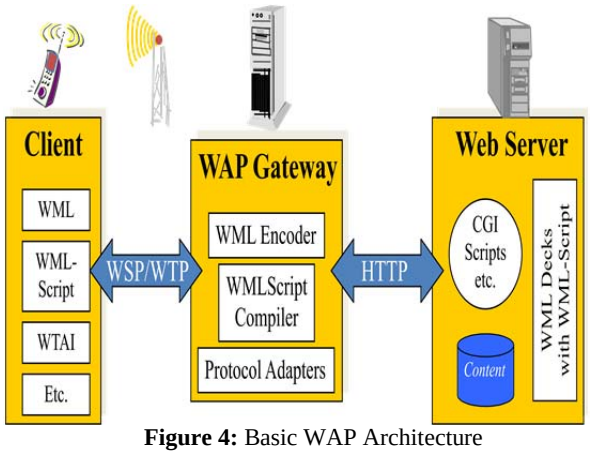

Figure 4: Basic WAP Architecture

Figure 4 shows the basic architecture of WAP. There are three participating entities: the WAP browser, the WAP gateway (also called WAP proxy) and web server. When the mobile device wants to connect to the Internet, all the communication must passes through the WAP gateway.

This WAP gateway translates all the protocols used in WAP to the protocols used on the Internet. For example, the WAP proxy encodes (and decodes) the content to reduce the size of the data that has been sent over the wireless link. The communication between the mobile device and the WAP gateway is secured with WTLS. WTLS is only used between the mobile device and the WAP gateway, while SSL/TLS can be used between the gateway and the Internet. This means that the WAP gateway first has to decrypt the encrypted WTLS-traffic and then has to encrypt it again (using SSL/TLS). This has some security consequences which we will discuss in next section.

6. SECURITY ISSUES IN WAP

Security issues in WAP generally occur due to WAP gateway and existence of some attacks like Denial of Service attack. These security issues are as follows:

6.1. WAP gateway:

Generally WAP does not offer end-to-end security [4].WAP devices communicate with web servers through an intermediate WAP gateway. WTLS is only used between the device and the gateway, while SSL/TLS can be used between the gateway and the web server on the Internet. This means that the WAP gateway contains, at least for some period of time, unencrypted data (which can be highly confidential). The gateway vendors have to take steps to ensure that the decryption and re-encryption takes place in memory, that keys and unencrypted data are never saved to disk, and that all memory used as part of the encryption and decryption process is cleared before handed back to the operating system. But there is no mechanism or standard that ensures these precautions are met or not. Therefore security of WAP gateway is more of concern in WAP environment.

6.2. Encryption v/s the functions of the gateway:

Since WAP gateway does not provide end to end security between the user and the server [4]. End to end encryption cannot be provided by retaining functionality of gateway because it is not possible to compile the WML Script code in encrypted form unless or until gateway first decrypt it and then compile there by breaking the end to end encryption. Also, it is not possible for the gateway to understand the encrypted WSP request (to decompress). That's why mobile devices have to use high latency occurring, more bandwidth consuming HTTP request. Finally, the gateways compression of ordinary WML documents are completely ruled out as if gateway cannot recognize the WML tags/ cards then it cannot perform the compression because characters of encrypted data is randomly distributed with no apparent pattern therefore such data cannot be compressed. Thus modifying the WAP standard to provide full end-to-end encryption as in TLS, conflicts with the compilation, decompression and compression functions of the gateway that serve to limit the amount of data that has to be transmitted over the wireless network.

6.3. Denial of Service Attack:

Denial of service attack [2] gains the benefit in a fault design of communication protocols to cause damage to network environment whether it is wired or wireless. The result of such attack can be temporary or permanent. Basically it involves two types of attacks:-

1. Resource allocation attacks
2. Resource destruction attacks

1) Resource Allocation Attack: Resource allocation attacks consume the targeted resources of the network environment hence cause other users to face a situation in which all or some of the resources necessary for the provision of the concerned services are engaged by the attacker[2]. As soon as the attacker terminates its attack, the engaged resources would become available again and the provision of service may be resumed to new clients Resource allocation attacks require flooding to the server with repetitive requests for a service by the attacker, and are based on the fact that the server has limited resources. There is no remedy if the attacker is serious and powerful enough. Of course, one can limit the damage by having the WAP gateway to monitor the traffic and if it exceeds a certain threshold, shut down the service in order continue the provision of mobile terminal connectivity to non-Internet users. WCMP echo request, Client Hello Request, Mail Bombs are the examples of Resource Allocation Attacks [2].

2) Resource Destruction Attack: In contrast, resource destruction attacks exploit weak spots in the structure and logic of the concerned protocols to make the service unavailable to innocent users [2]. It involves alteration or modification of configuration information, in which the attackers gain unauthorized access to the server and modify or destruct its configuration information in such a way that renders the m e r unavailable to other clients. It usually requires restarting of the affected server. This types of attack generally arises due to weak authentication of server so if we make authentication procedure more strong. The use of Internet technologies in the digital wireless networks and the interconnection of new mobile terminals to the Internet make it vulnerable to attacks similar to the ones that we have seen on the Internet. The number of mobile terminals far exceeds the number of Internet users and hence the impact of effective attacks on the mobile networks can potentially be more devastating. It is therefore necessary to devise procedures and solutions to make such attacks that target the mobile networks ineffective. Ping of Death, Teardrop [2], and Bonk are some of the examples of Resource Destruction Attacks.

7. SECURITY SERVICES

7.1. Wireless Security:

Before discussing WAP Security, it would be instructive to become aware of security available in existing networks such as AMPS, GSM, CDMA, and CDPD. WAP runs on top of these bearer protocols, and hence may or may not be able to make certain assumptions about the level of security provided by these networks. Hence, it is necessary to have security mechanisms in place at the WAP application layer as well.

7.1.1. Link Layer Security:

AMPS is an analog cellular network, and does not offer a very high level of security. Since the technology is analog,

it is possible for an amateur radio hobbyist to eavesdrop on conversations by tuning their radio to the appropriate frequencies.

GSM allows the network to authenticate the mobile terminal using the A3 algorithm. In addition, key agreement can be established using A5, and connections are encrypted using A8. The A3, A5, and A8 algorithms are specified as part of the GSM protocol.

CDMA is a spread-spectrum technology that spreads a signal across a large spectrum range based on the code sequence associated with the mobile terminal. All mobile terminals in a cell share the same spectrum, and the mix of all signals manifests itself as noise. Base stations are aware of the code sequences of all the mobile terminals in the area, and are able to decode the spread-spectrum signals.

7.1.2. Application Layer Security: WAP achieves application layer security by taking advantage of WTLS (Wireless Transport Layer Security), access control features in WML and WML Script, and TLS (Transport Layer Security) / SSL (Secure Sockets Layer). NTT DoCoMo's I-Mode service does not offer any application layer security or HTTPS (HTTP over TLS/SSL) at this time.

7.2. WAP Security Models:

This section will review the architecture of WAP services, and the security trade-offs that result from locating WAP gateways at different locations and with different configurations in the network.

7.2.1. Network Operator Hosts Gateway:

In the US, most WAP gateways are hosted by network operators such as Sprint PCS, Verizon, or AT&T Wireless. WAP services may be deployed with or without public-key infrastructure (PKI) in place. In this section, we will look at the security-related advantages and disadvantages of having network operators host WAP gateways.

7.2.1.1. Without PKI: In a WAP architecture in which the network operator hosts the WAP gateway, and in which there is no PKI deployed, the mobile terminal is hardcoded to connect to the network operator's WAP gateway. The network operator's WAP gateway accesses content from web servers on behalf of the mobile terminal. The mobile terminal connects to the WAP gateway using WTLS or encrypted HDTP, and the WAP gateway connects to web sites using TLS / SSL.

The mobile terminal is hardcoded to connect to the carrier's gateway if no PKI or certificates are deployed in the system, as there is no way for the mobile terminal to authenticate the gateway.

The advantages of this architecture are as follows:

1)No extra work for Content Provider. Content providers do not need to worry about running gateways, and they can get their WAP applications up and running quickly.

2) No extra work for the mobile terminal user. Users can have their phones pre-configured by the network operator, and do not need to worry about what gateway they need to use to connect to various WAP applications.

3) One logical gateway. The WAP browser running on the mobile terminal only needs to worry about connecting to one logical WAP gateway. This simplifies the design of the WAP browser that needs to be running on the mobile terminal. While a network operator has the flexibility to run an entire farm of WAP gateway servers, the mobile terminal only needs to worry about connecting to one logical IP address for the entire farm of gateway servers.

The disadvantages of this architecture are as follows:

1) Content Providers must trust Network Operator. Although communication between the mobile terminal and the WAP gateway is being encrypted with WTLS, the communication is being decrypted at the gateway such that it can be re-encrypted using SSL to be sent off to web servers on the Internet. While some gateway manufacturers take precautions to ensure that decrypted information is in memory for the shortest amount of possible time, and that such information is never paged to disk, it is still the case that the content is in decrypted form on the network operator's gateway for some (hopefully small) amount of time. Hence, the content provider must trust that the network operator has taken appropriate precautions to ensure the physical and network security of the WAP gateway. Some content providers, such as large banks, require that network operators sign formal non-disclosure agreements and policy agreements before they make their WAP application available on a particular network.

2) Network Operator can control home deck. Since the network operator controls the gateway that the mobile terminal makes its first connection to, it gives the network operator the opportunity to control the home page, or home deck (in WML parlance), and that the user sees.

3) Network Operator can introduce advertising. In addition to controlling the home deck, the network operator could, subject to usability constraints, wrap advertising around every WML page that is returned by any content provider!

7.2.1.2. With PKI: With a PKI infrastructure in place, web servers can request certificates from a "PKI Portal" and can kick off secure communication with a mobile terminal by encrypting a message with the mobile terminal's public key. Hence, although all subsequent communication will take place through the gateway, the information transmitted will be opaque to the gateway.

This approach offers the advantage that Content Providers no longer need to have as much trust in Network Operators, but the downside is that PKI infrastructure must be deployed to support this architecture.

7.2.2. Content Provider Hosts Gateway:

In scenarios where PKI infrastructure is not deployed and content providers cannot comfortably trust network operators, content providers can opt to host the WAP gateway themselves. Some banks in the UK and in other non-US countries, for example, have opted to take this approach.

7.2.2.1. Static Gateway Connection: In the static gateway connection scenario, the mobile terminal is configured to connect to the content provider's WAP gateway. This can be accomplished by:

1) having the user enter the IP address of the gateway, as well as other necessary configuration information into the mobile terminal,
2) having the content provider pre-configure / provision mobile terminals for its users, or
3) the content provider can send a message to the user's mobile terminal OTA (over-the-air) with the appropriate configuration information. Not all mobile terminals have micro browsers burned onto them that allow for the above capabilities. Most mobile terminals deployed in the US, for example, currently do not support this capability, while models such as the Nokia 7110 deployed abroad do support this capability.

This approach has the following advantages:
- the content provider does not need to trust the network operator
- the content provider has the ability to control the home deck (or one of the home decks), and
- OTA can be used to simplify the configuration process if the mobile terminal supports it.

This approach has the following disadvantages:
- the mobile terminal may be limited in the number of gateways that it can access.
- the mobile terminal needs to be configured to talk to a gateway different than that of the network operator, which may introduce complexity for users, and for content providers.

7.2.2.2. Dynamic Gateway Connection:
The dynamic gateway connection model allows the user's mobile terminal to talk to the network operator's gateway most of the time, and "dynamically" switch to a content provider's gateway when a secure transaction needs to take place.
While this eliminates the need for the content provider to trust the network operator for secure transactions, the network operator needs to trust the content provider to the extent that it feels secure in directing the user's sensitive data to the content provider's gateway. Typically, a "lightweight" agreement will be in place between the network operator and the content provider to enable dynamic gateway connection.
This connection model was only approved by the WAP Forum as of the middle of this year, and is described further in the WAP Transport Layer E2E Security Specification. It may be some time before this connection model is available in live systems.

7.3. WTLS and SSL:
WTLS is the Wireless Transport Layer Security protocol designed to support the security requirements of authentication, privacy, and integrity in the Wireless Application Protocol (WAP) defined by the WAP Forum. The wireless mobile network introduces new challenges for implementing security architecture compared with the traditional connection oriented models like that used in Internet.

7.3.1. Authentication:
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. The latter procedure can happen only if the server allows it to occur [5]. The server can require the client to authenticate itself to the server. However, the WTLS specification defines that authentication is an optional procedure.
7.3.2 Key Exchange:
In order to ensure a secure communication channel encryption keys or initial values to calculate keys have to be exchanged in a secure manner. However, it is possible that the Server Certificate Message did not contain enough data to allow client to exchange the pre-master secret (pre-master secret is an initial value which is used to calculate the master secret). In this case a Server Key Exchange message is used to provide such data [5]. The key exchange mechanism of the WTLS also provides an anonymous way to exchange keys. In this procedure, the server sends a Server Key Exchange message which contains the public key of the server. The key exchange algorithm may be RSA, Diffie-Hellman, or the elliptic curve Diffie-Hellman. The message does not contain any certified information.
7.3.3 Privacy:
Privacy in the WTLS is implemented by means of encrypting the communication channel [5]. The used encryption methods and all the necessary values for calculating the shared secret are exchanged during the handshake.
7.3.4 Integrity:
Data integrity is ensured using the message authentication codes (MAC)[5]. The used MAC algorithm is decided at the same time as the encryption algorithm. The client sends a list of supported MAC algorithms where the preferred algorithm is the first in the list. The server returns the selected algorithm in the Server Hello message.

7.4. WIM
The **WAP Identity Module** specified by the WAP Forum provides a tamper-resistant environment in which cryptographic keys can be stored, and cryptographic operations using these keys can be securely carried out. A tamper-resistant environment is one provided, for example, by a smart card in which the device will "self-destruct" or be rendered useless if an adversary attempts to tamper with the card.

In particular, WIMs carry out the following operations:
- storage of both keys used to sign WTLS messages, as well as "signing" keys used to execute non-repudiable transactions using the WML Crypto API.
- storage of long-lived WTLS master secrets
- storage of CA, root CA, and user certificates and/or the URLs of these certificates
- "unwrapping of keys"
- computation of ECC-DH master secrets that take place in a WTLS handshake

7.5. WML Script Crypto API:

WAP 1.2 specifies a signText () WML Script function that can be used to execute non-repudiable transactions in WAP applications. The function takes a message to be signed, and the key with which the message should be signed as input, and returns a signed message as output.

7.6. WML Access Control:

Access to WML decks and WML Script libraries can be restricted to requests coming in from particular domain names and paths. An <access> tag can be placed in the <head> of a WML deck to restrict the set of referring domains and paths that may link to this deck. Similarly, WML Script libraries can prevent their external functions from being invoked by WML from untrusted domains and paths.

8. Security Solutions

In this paper we have given three solutions for the WAP gateway described below:

8.1. Switch to Trusted Gateway:

Switch to a trusted and secure gateway instead of using the default WAP gateway [4]. It is very important in sensitive services like electronic banking applications. The problem with this solution is that it is not always very easy for a (non-technical) user to switch to another gateway. Note that if WAP is deployed over GSM, switching from one gateway to another can be done by sending a SMS message. For e.g. in mobile commerce types of applications WAP gateway is generally placed where web server is placed there by protecting it in the similar manner as web server is protected. But it imposes additional overhead at the server to maintain the WAP gateway, update it according to new version of WAP.

8.2. Application level security on top of WAP:

Security at application layer on the top of WAP [4]. It leads to the introduction of security at the software layer above the WAP by considering WAP as an insecure medium for communication. In spite of providing the security through WAPs security protocol (WTLS), it is implemented by means of dedicated software running at two ends, mobile devices and web server as shown in Figure 5.

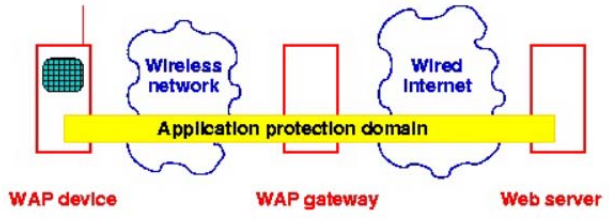

Figure 5: Security zones using application level encryption [4]

This software can perform the encryption in such a way that can eliminate the security hole at WAP gateway. Since it removes hole at security in gateway, it requires sophisticated cryptographic algorithm should be implemented at WAP enabled mobile devices. It also requires improvement in WML Script crypto library that presently contains only one cryptographic function to provide authentication (by Digital Signature). There is also the loss of compression, decompression and compilation facilities that is performed at the gateway in order to utilize the limited bandwidth availability of wireless network.

8.3. Solution for Denial of Service Attack:

We can limit the damage by having the WAP gateway to monitor the traffic and if it exceeds a certain threshold, shut down the service in order continue the provision of mobile terminal connectivity to non-Internet users [2]. But it required the WAP gateway to be equipped with additional functionality to monitor the traffic is whether it exceeds the certain threshold or not. Solution for Resource Destruction Attack of such problems require updates on the victims operating system that screen for the initiation of attacks and discard the packets that may cause harm to the system.

9. Conclusion

WAP enables mobile phones to browse on the internet. It is the wireless equivalent to TCP/IP and has the big advantage of being bearer independent. The security architecture of WAP consists of three parts: the mobile devices, the WAP gateway and the Internet. The communication between the mobile devices and the gateway is protected by WTLS, a wireless version of SSL/TLS, while the traffic from the gateway to the Internet can be protected by SSL/TLS. The WAP gateway decrypts all the WTLS traffic and encrypts all the SSL/TLS traffic. From a security point of view, this means that the gateway should be considered as an entity-in-the-middle. It is due to this fact that both the user and the web server on the Internet have to trust the WAP gateway. As this is not always the case, solutions have been searched to avoid this entity in the middle and denial of service attack prevents others users using the limited resources of server for the provision of the concerned services.

References

[1] Dave Singelee, Bart Preneel, The Wireless Application Protocol (WAP).
[2] Ahmed R Sharafat and Sahar Kosari, AN ANALYSIS OF DENIAL OF SERVICE ATTACK (DOS) IN THE WIRELESS APPLICATION PROTOCOL (WAP) ENVIRONMENT
[3] Complete WAP Security from Certicom
[4] A. Jaganath Swamy and D.Dinesh Reddy, WAP Collaboration and Security Issues in Mobile Communication
[5] Security Issues in WAP WTLS Protocol G.Radhamani, K Ramasamy Multimedia University