Class: Electronic Payment System

Final Report

2001, Spring

Professor: Kim Kwang Jo

" Wireless Technology: Comparative Study on WAP "

2001031 Kim Jina
2001070 Yoo Min Young
2001071 Yoo Jae Heung
2001139 Han Yumi
2001142 Hong Jinki

Dept. Electronic Commerce, ICU
mailto: behappy@icu.ac.kr (Yoo Jae Heung)

Submit Date: June 14, 2001

한국정보통신대학원대학교
Information and Communications University

Contents

Abstract

Mobile Commerce have highlighted in recent days. Many companies have been trying to find lucrative business opportunity in mobile industry. By developing middle-ware technology like e-payment system or security, and making contents like animation and compact online games, they are struggling to survive in mobile business area. It is important to understand mobile technology for using appropriate techniques to provide more efficient and secure services. So, we'd like to compare current mobile technologies focused on WAP/WML technology, which is de-facto standard in mobile commerce area. We are going to cover mainly three topics: wireless application protocols, markup language for developing mobile contents and WAP security issues at network level. By comparison of those protocols and markup languages, developers can get some perspectives to choose appropriate technologies, which are fit to their business. They also can either obtain some awareness about WAP security hole in network level and find some solutions to overcome the security problems.

KEY WORD: mobile commerce, markup language, end-to-end security, WAP

1. Introduction

Mobile Commerce is not unfamiliar word today. According to MetaGroup research by 2003, over 50% of Internet access will be by Non-PCs and by 2001, 78% of people will be using cell phones for wireless data ComputerWorld says. This mean the opportunities of mobile business also will be tremendously increasing.

So, it is necessary to understand wireless technology. Wireless technology is somewhat different from traditional Internet-based technology. The technology must be available in low-bandwidth and small-capable devices. Protocol must be simple and markup language must be easy to understand for developing data contents to mobile users. Security is another critical factor that make more customer join the wireless world.

In this context, we believe that understanding various mobile protocols and markup languages is inevitable for providing more effective contents services. And also understanding security-related issue is useful to support more reliable mobile services. That's why we are going to compare the various technologies of protocol, markup languages, and security.

WAP is de-facto standard of wireless application protocol. Most of mobile commerce based on this protocol. So, we are going to focus WAP technologies and try to find its pros and cons, especially the weakness of security and its solutions.

We expect that readers can get some useful information about overall wireless technologies, and they also get some perspectives, which are helpful to decide to adapt an appropriate technology for mobile service regardless of they are content providers or middle-ware developers. Wireless technology is highly dependent on company, which has the technology. This paper compared the technologies by various classifications so that readers could find each technology's pros and cons.

2. Comparative Analysis

2.1 Comparison of Application Protocol

(1) Why this comparison is needed?

Nowadays, M-commerce market is growing rapidly as wireless communication technology is developing. It is expected that infrastructure for wireless data communication will provide various multimedia services such as music downloads and video/graphics services in the near future. At that time, those multimedia services are going to satisfy customer's needs so that mobile commerce market will be more activated. In other words, growth of mobile commerce market absolutely depends on wireless technology. In this point of view, it is worthy to study an important factor in wireless technology.

As a matter of fact, one of the most important factors in wireless technology is wireless Internet application protocol that brings Internet contents and advanced data services to wireless phones and wireless terminals. Currently, many wireless Internet application protocols such as WAP, MME, I-mode, and Anyweb are implemented. By comparison, we can know the trend of application protocols and features to be required and improved. Especially, we are able to know the shortages of WAP as a worldwide standard for wireless Internet.

(2) What are characteristics of each Application protocol?

1) WAP

The Wireless Application Protocol (WAP) is an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly. The purpose of WAP is to enable easy fast delivery of relevant information and services to mobile users.

a) Optimized For Handheld Wireless Devices

The WAP specification defines a microbrowser that is the ultimate thin client, able to fit in a limited amount of memory in the handheld device. The use of proxy technology and compression in the network interface reduces the processing load at the handheld device so that an inexpensive CPU can be used in the handset. This further helps reduce power consumption and extends battery life, meeting the needs of both handset manufacturers and wireless subscribers.

b) Leverages Proxy Technology

The WAP specification uses standard Web proxy technology to connect the wireless domain with the Web. By using the computing resources in the WAP Gateway, the WAP architecture permits the handset to be simple and inexpensive. For example, a WAP Gateway will typically take over all DNS services to resolve domain names used in URLs, thus offloading this computing task from the handset. The WAP Gateway can also be used to provision services to subscribers and provide the network operator with a control point to manage fraud and service utilization.

A WAP Gateway typically includes the following functionality:

• Protocol Gateway – the protocol gateway translates requests from the WAP protocol stack to the WWW protocol stack (HTTP and TCP/IP).

• Content Encoders and Decoders – the content encoders translate Web content into compact encoded formats to reduce the size and number of packets traveling over the wireless data network.

This infrastructure ensures that mobile terminal users can browse a variety of WAP content and applications regardless of the wireless network they use. Application authors are able to build content services and applications that are network and terminal independent, allowing their applications to reach the largest possible audience. Because of the WAP proxy design, content and applications are hosted on standard WWW servers and can be developed using proven Web technologies such as CGI scripting.

The WAP Gateway decreases the response time to the handheld device by aggregating data from different servers on the Web, and caching frequently used information. The WAP Gateway can also interface with subscriber databases and use information from the wireless network, such as location information, to dynamically customize WML pages for a certain group of users.

c) Addresses the Constraints of a Wireless Network

The protocol stack defined in WAP optimizes standard Web protocols, such as HTTP, for use under the low bandwidth, high latency conditions often found in wireless networks. A number of enhancements to the session, transaction, security and transport layers provide HTTP functionality better suited to the wireless network environment. Here are a few examples of these improvements:

• The plain text headers of HTTP are translated into binary code that significantly reduces the amount of data that must be transmitted over the air interface.

• A lightweight session reestablishment protocol has been defined that allows sessions to be suspended and resumed without the overhead of initial establishment. This allows a session to be suspended while idle to free up network resources or save battery power.

• WAP provides a Wireless Transaction Protocol (WTP) that provides reliable transport for the WAP datagram service. WTP provides similar reliability as traditional TCP does, but without behaviors that make TCP unsuitable in a wireless network. For example, TCP transmits a large amount of information for each request response transaction, including information needed to handle out-of order packet delivery. Since there is only one possible route between the WAP proxy and the handset, there is no need to handle this situation. WTP eliminates this unnecessary information and reduces the amount of information needed for each request-response transaction.

• WAP's WTP solution also means that a TCP stack is not required in the phone, which allows for significant savings in processing and memory cost in the handset.

2) MME

Microsoft® Mobile Explorer™ is an operating system independent, air-link agnostic, browser-based solution. Mobile Explorer enables secure mobile access to corporate or personal e-mail, corporate networks, and the Internet when connected to a wireless network. It includes the world first dual mode micro-browser that can display both WAP 1.1 and HTML Internet content.

Also, Microsoft Mobile Explorer is a unique browser-based solution that delivers rich Web services to a wide range of mobile handsets. Integrated into award-winning mobile phones across Europe and Asia, Mobile Explorer currently ships in products from leading manufacturers including Samsung, Sony, Hyundai, and Benefon with many more phones expected to come to market in 2001.

a) Revenue Generation

Mobile Explorer guarantees mobile operators a secure way to offer value-added services such as personal e-mail, access to corporate networks, and Web services to customers. It has been built as a flexible platform with revenue-generating personalization options for both operators. Users can download a wide range of home screen skins, ring tones, and personal

information to their handsets via the browser. These services can substantially increase data and SMS traffic accelerating the return on networks investments.

b) Future-Proofed Investment

Microsoft is the first manufacturer to ship a multimode micro-browser giving end users unlimited access to content marked up in HTML, WML (wireless mark-up language), and c-HTML used in the popular I-Mode Service. Microsoft Mobile Explorer has been designed from the ground up to support end-to-end services based on Internet standards. A protocol foundation of HTTP, TCP/IP, and SSL allows Mobile Explorer to connect with today Internet services and tomorrow WAP 2.0 services.

c) Enhanced Services

When used in combination with server technologies such as Microsoft Mobile Information Server, Microsoft Exchange Server, Microsoft BackOffice family, and MSN Mobile Service, Mobile Explorer enables a wide range of new data services to end users connected to mobile networks. With popular services such as Hotmail and MSN Instant Messenger, e-mail can be delivered as part of a branded solutions platform allowing operators greater flexibility to differentiate and build new revenue streams. Mobile Explorer also supports over-the-air configurations of WAP gateway and e-mail settings as well as provisioning of services and information by WAP push. Users are no longer required to enter complicated provisioning information such as IP and gateway addresses.

d) Secure Solutions

Mobile Explorer makes mobile commerce a reality for your users. It goes beyond the base protection offered on most Web-enabled phones by offering full end-to-end security for e-commerce transactions with support for both WTLS class 3 (WAP 1.2.1 specification) and SSL 3.0. Phones with integrated Mobile Explorer can also take advantage of Microsoft Passport, which is a sophisticated Web technology that speeds the authentication process for secure data transfer via the Web. Cookies residing in the phone's read-only memory authenticate the user ID, enabling the user to perform multiple e-commerce transactions without having to retype long passwords.

3) i-mode™

i-mode is the child of NTT DoCoMo. This solution lies at the completely proprietary and completely closed end of the spectrum, since it is entirely operated by NTT DoCoMo, and all content providers have to register with the company. The success of the user-based technology,

however, has created many suggestions that i-mode is a more appropriate path than WAP.

For one it is easy to establish a robust system if it is entirely closed. Many of the interoperability problems that the first version of WAP faced had never been an issue for i-mode.

Secondly, i-mode phones are designed with i-mode in mind. This means that the ser experience is much more enjoyable. Perhaps the biggest advantage of i-mode is the billing mechanism used. Instead of billing users based on the amount of time they are online, which is how current WAP network providers operate, the billing is based on the amount of data that users download to their phone. This makes using the phone much more cost effective because of the packet-based billing technology (PDC-P) it employs.

As opposed to WAP that defines WML for developing WAP sites, i-mode uses a subset of HTML called c-HTML. This makes development of content much easier since there is no need to learn a new language. Furthermore i-mode is based on a TCP/IP framework making the posting of information more straightforward and familiar.

Which is currently hard to implement in WAP, the capability of pushing content to the mobile phones so users can have true updates about the information they are interested in, be it stock values or weather reports.

When WAP is compared to i-mode the winner, based on user acceptance, has to be i-mode. Just the fact that everyday people in Japan were immediately hooked on it, while in the rest of the world, WAP is having a hard time proves that i-mode provides a better service. However, WAP is available in the rest of the world while i-mode is only in Japan. In addition WAP has been designed with the rest of the world in mind while i-mode is entirely proprietary. Even though there are talks about i-mode networks elsewhere, network providers have made a huge investment in WAP and will not readily let go. In technological terms WAP is a far more advanced, albeit complex, solution that provides a more scaleable approach. Eventually, as WAP and mobile devices advance, we can hope that some of the best features such as the billing mechanisms and the instantaneous connection will be available to WAP users as well.

4) Anyweb™

The characteristics of Anyweb can be summarized as ten features, that is, inexpensive calls, web touch and call, PersonalJava compatible, faster connection, fear-free internet transaction, automatic program download, largest screen with easy-to-use interfaces, HTML-based off-line rest-page, plug & play, and call & web-surfing simultaneously.

a) Inexpensive Calls(VoIP: Voice over IP)

It works on both IP and traditional telephony networks giving you a lot of saving on your

telephone bill. It is noteworthy that you cannot save your money with other screenphone yet. By complying with H.323, it can inter-operate with PC S/W such as MS Netmeeting and multiple vendors' products. (VoIP function will be available upon customer's request).

b) Web Touch and Call

When the user connects to a designated corporate home page, he or she can read product information and simultaneously contact a salesperson with a PC at the company. Anyweb™ is also designed to make a call simply by touching icon on the company web site. Meanwhile, the company can save lots of cost for toll free number with increased sales opportunities.

c) PersonalJava Compatible

It is also the first Java enabled phone having fully passed Sun MicroSystems' certification tests last year. It supports downloading Java Applets and running Java applications and it will play an increasingly important role, allowing developers the freedom to work with a number of development tools, and gives consumers easy access to versatile applications such as e-commerce, Internet game, advertising, and etc.

d) Faster Connection(ISDN, LAN)

Anyweb™ is suitable for both residential and business use. It comes with a built-in modem and, uses 10 Base T Ethernet protocol for the corporate environments. High performance can also be enjoyed in the home via the multimedia networks such as ADSL or cable telephony networks. Fully approved for ISDN connection, Anyweb™ will allow Telecom Operators to offer high speed ISDN services to customers as well as ISDN supplementary services such as MSN (Multi Subscriber Numbering) providing up to five different numbers all with different ringing tones.

e) Automatic Program Download

Sophisticated but simple, the new multimedia device, Anyweb™ is smart enough to download new program automatically after version-check. It enables Telecom Operators or Service Providers can support media-rich applications and various new services with a single device.

f) Largest Screen with easy-to-use Interfaces(8.2 Inch)

Anyweb™ combines the Internet features of a PC, such as e-commerce, web surfing and e-mail, with Internet and the simplicity of a regular telephone. An 8.2 inch/15cm screen gives access to the Internet while a normal telephone handset and retractable keyboard provide

easy- to-use interface.

g) HTML-based Off-line Rest-page

The Rest-page (first page on the screen after power on) is based on Off-line html file enabling easy customization for different users, groups or even companies. Dynamic Advertisement, Customer-Targeted Marketing, Personalized Portal page are available as well.

h) Plug & Play

It is enable to help customers do not have to be web or Internet literate. It is designed to setup automatically initial connection and registration with the network. So users can use Anyweb™ just like a friendly telephone.

i) Call & Web-surfing simultaneously

The built-in IP telephony technology or fully approved ISDN connection can help you enjoy web-surfing and telephone call simultaneously. So you don't need to stop your web-surfing or to disconnect Internet for telephone call and vice versa. Also, it can handle double phone line, that is, you can connect one line for the Internet and another line for the telephone. (2 PSTN lines will be available upon customer's request).

<Table: Comparison of WAP, MME, i-mode, and Anyweb>

Category	WAP	HTML Series		
		MME	i-mode	Anyweb
Players	Motorola, Ericsson, Phone.com, Nokia, 011, 017, 019	Microsoft, 016, 018	NTT Docomo	Samsung Electronics
Service Location	Europe, Asia, USA	Korea	Japan, Hong Kong	Korea, Israel
Language	WML	m-HTML	c-HTML	s-HTML
Efficiency	• Every technology should be redefined for wireless environment • Suitable for low transmission speed • Programming factor by card unit editing	• TTP, TCO/IP based • Strong designing factor by page unit editing		

Compatibility & Expandability	• Use unique technical language •Can not be compatible with HTML contents	• Compatibility with HTML-based site • Scalability of PC-based Script
Security	• Insecurity feature	• Easy Implementation of end-to-end security

2.2 Comparison of Markup Languages

(1) Why this comparison is needed?

Globally there are many different mobile Internet specifications. The most of them based on WAP protocol, which mainly uses WML and HDML as markup languages. There are other markup languages that are designed for company's special service specification. cHTML is used by NTT Docomo's I-MODE in Japan, sHTML was developed by Samsumg, and mHTML was developed by Microsoft. Other HTML based markup languages has difference device capability and protocol environment that is noted above.

This comparison of markup language will be useful to those who have a plan to start Content Business via mobile network. They have to decide what kind of technologies and services they will provide. To select a markup language is important in that functions and interface will be limited by depending on the markup language. Through analyzing the characteristics of each markup language, business starters can get some help to select an appropriate technology to carry out their business.

(2) What are characteristics of each Markup Language?

1) HDML vs. WML

Both languages share the same basic programming model and functionality; however, there are some notable differences to discuss. The main difference is that WML is XML-based, while HDML is not. The main benefit of being XML-based is that a company can use commercially available XML tools to generate, parse and manipulate WML, and they can also user XSL/XSLT to construct WML decks from XML meta-languages.

Another major difference between HDML and WML is that HDML does not allow scripting, while WML allows it's own version of JavaScript, called WMLScript. WMLScript allows the programmer to check the validity of user input, access other facilities on the device (make a call on a phone, add a number to the phone book, etc.), generates messages and dialogs, and other device-specific tasks. HDML has the functionality to do most of the same tasks;

however, using WMLScript reduces overall network traffic by performing the task locally.

HDML does not have a DTD (Document Type Definition) while WML does. As expected, there are also other smaller functionality and syntax differences such as WML's intrinsic events and the ways in which variables are set and passed.

<Table: Comparison of HDML and WML>

Feature	HDML	WML
XML-based	No	Yes
DTD available	No	Yes
Scripting	None	WMLScript
Display Cards	Yes	Yes
Choice/Select Cards	Yes	Yes
Entry/Input Cards	Yes	Yes
Nodisplay Cards	Yes	Yes
Images in Text and Anchors	Yes	Yes
Variables % 0 A	Yes	Yes
Deck Access Control	Yes	Yes
Deck Cache Control	Yes	Yes
Timers	No	Yes
Multiple Choice Lists	No	Yes
Bookmarks	Yes	No*
Nested Activities	Yes	No**
Images in Labels and Choices	Yes	No**
Mobile Originated Pre-fetch	Yes	No**
Key Accelerators for Links	Yes	No**

** UP.Browser supports this feature via WML meta tag*

*** Supported by Up.Browser 4.0 via Phone.com WML extended tag*

Based on the aforementioned facts, WML is going to live much longer and go farther than HDML. Unfortunately, Unwired Planet (now Phone.com) came out with HDML a tad before its time. When the HDML Spec was released, XML was so new, Unwired Planet did not know enough about it to make HDML based upon it. Although the Phone.com's UP.Link platform will continue to support applications written in HDML, they are recommending to its users to move to WML.

In Europe and Japan, some WAP devices already do not accept the HDML format. In the U.S. and Canada, many of the commercially available CDMA and CDPD phones only support HDML. It is most likely that the future US and Canadian phones will all support WML also.

Fortunately, it is not difficult to convert HDML to WML and the learning curve should be minimal.

2) c-HTML, s-HTML, and m-HTML

a) cHTML (compact HTML)

It is wireless Internet document format used in the i-mode™ and developed to overcome the limit of mobile device: low capacity of memory, low electric power CPU, limited display, single size/color and font, limited input way without keyboard or mouse. It also provides a service as a compressed language of HTML 2.0, HTML3.2 and HTML 4.0.

Its advantages are as follows; first, it is easy to develop and reuse of existing contents based on HTML second, more efficient function are provided by excluding contents such as Frame, Table. However, It still requires many memories, and provides only single color display in the limited hardware. It is manipulated by controlling basic four functions: Cursor forward, Cursor backward, Select, and Back/Stop.

b) mHTML (mobile HTML)

MicroSoft developed ME (Mobile Explorer) as a transient solution in the absence of standard of wireless Internet mobile device. ME adopted mHTML characterizing the subset of HTML to consider ease of making contents. It has limited display size (4 rows and 8 columns) and only single font and size is available due to lack of memory and limitation of device capacity, but it uses its own special tags. "Tel" tag is for calling, and "BTN" tag is for linking to other mobile site. And also supports vCard document format, which make it possible to exchange directory information set that contains telephone numbers, email address, postal address, and etc. A critical advantage of using mHTML is that it is based on MicroSoft's operating system environment. That means it supports compatibility with other MS's products and also can use a number of Micorsoft's customers. So, mHTML is becoming a competitor to WML, which is de-facto standard markup language in wireless environment.

c) sHTML (short HTML)

Samsung Electronics and Web Planet developed sHTML language based on HTML 4.0 in order to provide wireless Internet service and AnyWeb™ browser supporting it. sHTML has an advantage of technological independence , so that they need not to provide royalty. It provides single font and color just as other HTML based languages does. And It does not support any Script languages such as JavaScript, ActiveX, VBScript. It added some function to support Bitmap image, animation, and marquee function.

<Table: Comparison of HTML based Markup Languages>

Classification		ME	AnyWeb	I-MODE	Internet
Protocol	Application Layer	HTTP	HTTP	HTTP	HTTP
	Transport Layer	TCP/IP	TCP/IP	TCP/IP	TCP/IP
Markup Language		mHTML	sHTML	cHTML	HTML
Browser		MicroBrowser	AnyWebBrowser	CompactNetFront	Netscape/Explorer
Technology loyalty		Pay by number of users	No pay	No pay	-
Companies		KTF, HansolM.com	SamsungElectronics AI-NET	NTT Docomo	-

As a conclusion, cHTML and sHTML are good for providing more multimedia-related services among HTML based markup languages[1]. mHTML does not provide enough tags to include images and its alignment due to using TCP/IP, which make network overload.

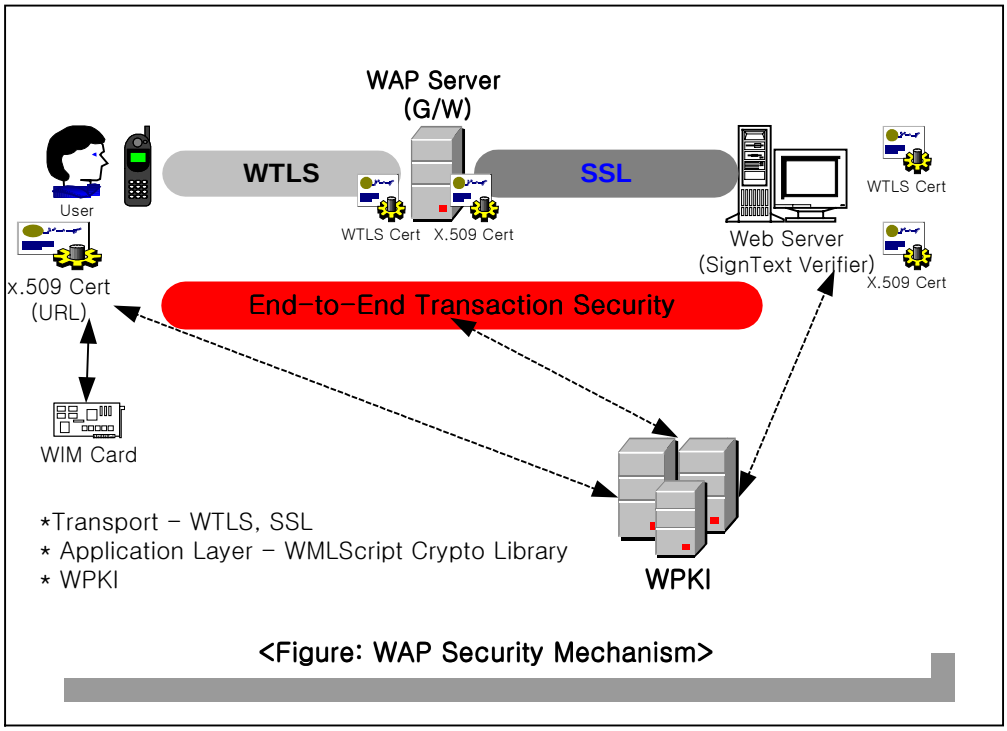
2.3 WAP Security Hole At Network Level

In this section, we are going to review security-related problems of WAP. The most vulnerable point is the Gateway system, which carries out protocol translation from wireless to wired network. Due to the weakness, WAP does not guarantee end-to-end security.

We'd like to survey some suggestions to solve the problem. Three ideas are introduced in this section. Each has both pros and cons. Understanding the security problem that WAP has and its solution is critical factor for success of business.

(1) Overall Mechanism of WAP Security

[1] I-BIZNET, http://www.i-biznet.com



<Figure: WAP Security Mechanism>

This picture shows how the security of mobile service works. Basically there are three components that make secure transaction: WTLS, SSL, WPKI.

WTLS is a special protocol, which is designed to run on mobile devices with relatively low hardware capacity. Its technology is based on SSL/TLS technology. SSL is generally used in traditional wired network. It usually works on TCP/IP transport layer and guarantee secure transaction between end-systems. The wireless public key infrastructure is not popularized, however, its specifications related to WPKI have introduced by WAP forum since 1999 and some companies have developed prototypes and succeeded commercialization. Let's review some basic components, which make WAP security mechanism.

(1) WTLS – the primary purpose of Wireless Transaction Layer Security is to provide privacy, data integrity, and authentication between two communicating applications. WTLS provides functionality similar to TLS1.0 and incorporates new features such as datagram support, dynamic key refreshing and optimized handshake. The WTLS protocol is optimized for low-bandwidth bears networks with relatively long latency[2].

(2) WMLScript Crypto Lib Spec – It provides cryptographic functionality of a WAP client. One way to provide authentication is to associate a digital signature with data generated as the result of a transaction, such as a purchase order or other financial document. To

[2] WAP Forum, WTLS Specification, 1999/11

support this requirement, the browser provides a WMLScript function, Crpto.signText, that asks the user to sign a string of text. The browser use special signature keys that are distinct from authentication keys used for WTLS. A WIM (Wap Identity Module) may be used for private key storage and signature computation[3].

(3) WIM- This is used in performing WTLS and application level security functions and especially, to store and process information needed for user identification and authentication. The functionality based on the requirement that sensitive data, especially keys, can be stored in WIM and all operations where these keys are involved can be performed in the WIM. An example of WIM implementation is a smart card. In the phone, it can be the Subscriber Identity Module (SIM) card or external smart card.

(4) WAP Public Key Infrastructure (WPKI) – It issues certificates for each users and gateway and manage the certificates and provide the verification services for requests. WAP defines an optimized certificate structures and provides the profiles of certificates revocation list.

In this section, basic WAP security elements have been reviewed. To guarantee a secure transaction in wireless environment, simple and optimized transaction protocol such as WTLS and tamper-proof security devices could be developed in occasion when independent mobile device itself cannot support perfect security. Finally, wireless public key infrastructure is necessary to provide authentication using digital signature that is going to be more popular and regarded as secure transaction functionality.

However, there is a problem in that WAP does not provide perfect security. The gateway system, which translates WTLS protocol to SSL protocol, is one of security hole. In the next section, we are going to review the characteristics of Gateway and its weakness and then find possible solutions.

(2) WAP Gateway

1) What is gateway and what is function?

WAP Gateway is a software Server, which makes connections between wireless network and TCP/IP based wired network. It has a function that translates WAP protocol (WSP, WTP, WTLS, WDP) to SSL protocol, which is based on TCP/IP packet network. Implementation of WAP gateway depends on vendors like Phone.com, Nokia and etc. It can be single server system or several distributed system. Let's take a close look at the functions.

In the wired network, the information is transmitted as text-based HTTP mode. Thanks to

[3] WAP Forum, WMLScript Crypto Library version 05-Nov-1999, 1999

enough bandwidth of wired network to transmit texts header it is relatively easy job. In contrast, it is difficult to transmit the information that is easily transmitted on the wired network in wireless network due to its low bandwidth. After all, it is necessary to translate the text based HTTP information to binary mode in wireless environment that has low bandwidth and long latency. The protocol conversion is from WSP to HTTP.

Another job of WAP gateway is encoding and decoding of contents that are expressed by WML. The gateway encodes elements tags and attributes that consist of WML to binary data. It also conducts error checking and handling while it is encoding or decoding the WML data or binary data.

2) What is the problem?

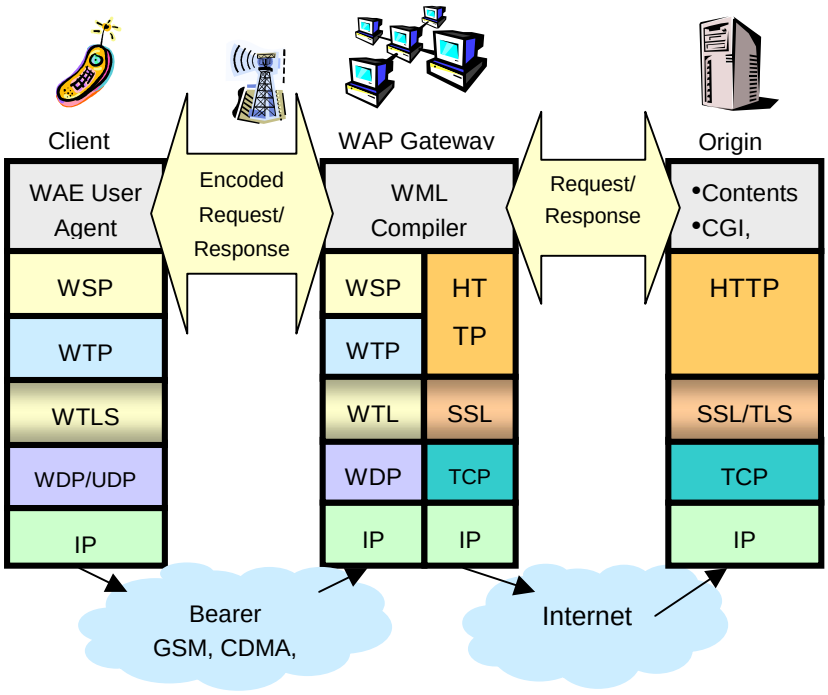


Figure: Security on Transport Layer

Problem happens at the time of protocol conversion.

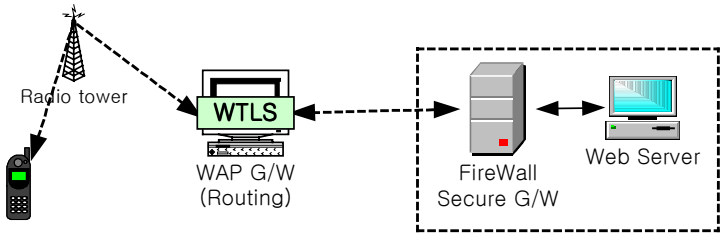
On the wired network, every data is encrypted by using 64bit-SSL protocol and there exists 40bit-WTLS standard for data encryption on the wireless network as well. However, it is necessary job of the gateway to decrypt the binary data from a mobile devices and it reencrypts the decrypted data by using SSL for transmit the data on the wired network. Due to these reason, the end-to-end security cannot be established. If users completely trust the WAP Gateway service provider, it might be possible to say there is end-to-end security between end clients and end content providers. But still, there is possibility of attack from outside. Now, this question

might be raised: are there any solutions to handle this problem? In the next section, some solution will be introduced.

(3) Enhancement of the weak points in network level[4]

1) Solution1: *Setting up Firewall System or additional Gateway Server in the service provider's domain*

This is to move G/W to contents provider. This model is used for somebody want to connect to a financial system like banking and stock system, which need high level of security. In this model user enters the IP address of the secure G/W system instead of entering the IP of WAP G/W. So, there is no work to translate from WTLS to SSL and to manipulate the encrypted data. However, the web server in service provider must translate the data that is transmitted from device to binary data because only binary data can be transmitted between base stations. It is very difficult for user to work with this model. In other words, whenever a user want to connect a secure gateway system, he/she has to input IP address of the system. And it is not allowed to input other IP address of g/w system in domestic[5].



Intra-Secure G/W Model

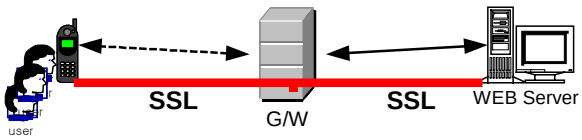
2) Solution2: MME Method for serving security

MicroSoft developed the Mobile Explorer to overcome the insecurity of WAP. ME does not need any protocol translating system like WAP G/W. It is possible to use HTML protocol in ME system. In version1.0, Gateway system is not needed and uses m-HTML as default markup language. SSL protocol is applied from mobile device to service provider. This guarantees end-to-end security. But it also has some disadvantages; there is too much overhead on browser and communication protocol (TCP/IP) and it needs high processing capability and it consumes a lot of electricity.

---

[4] Hong Ki Yoong, Wireless PKI Technology Trend, KSIGN, 2001,5
Kim Bong Hwan, Security in wireless Internet service, ETRI, 2000/8
Kwon O Sung, WAP Gateway, MOSCA, 2000/10

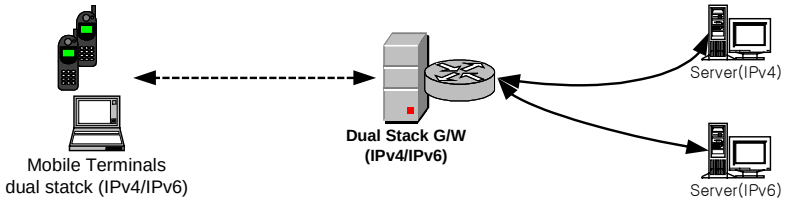
[5] http://matilda.snu.ac.kr/doc/column/security/wapsecurity.htm, 2000/Oct.



MicroSoft ME SSL Security Model

3) Solution3: Using IPv6 - Nokia's new strategy

IPv6 offers important advantages. The protocol will support more scalable network architecture, data integrity, autoconfiguration, mobile computing, data multicasting, more efficient network aggregation and improved security. Security is embedded and stadardized in IPv6, enabling seamless remote Intranet access, for example, as well as corporate virtual private network (VPN). All this is possible even when end users want to stay always connected to their corporate Intranet. This 'always-on' type of service is not readily achievable with IPv4 technology. IPv6 is necessary to maintain real IP-level Intranet presence for mobile workers. When it comes to security, IPv6 conforms to IP Security (IPSec) mechanisms and services. Along with mandated mechanisms that provide network layer security, IPSec comprises two services. An authentication Header (AH) is used to ensure data integrity and an Encapsulating Security Payload (ESP) Header, to ensure data confidentiality and data integrity. AH and ESP extension headers are optional in an IPv6 packet and can be used together or separately. Nokia has tried to transit from IPv4 to IPv6. There are three methods for achieving this goal: (a) IPv4/IPv6 dual stack in network elements and terminals (b) tunneling (automatic and configured) (c) translators[6].



Using IPv6: Nokia's Dual Stack Model

[6] NOKIA, IPv6 – Enabling the Mobile Internet, 2001/4

The use of IPv4/v6 dual stack is the main transition mechanism. On the network side, the implementation of dual stack, for example, is vital to enable both IPv4 and IPv6 access. The edge routers in the operator network should also be dual stack routers. Mobile terminals must be dual in order to access both IPv4 and IPv6 services without translators in the network.

Consequently, Using IPv6 is now quite costly. Additional dual systems are need to client, G/W and Web server side. It is also hard to define key exchange mechanism for large network, which need high-performing devices or system. Finally, It does not provide E2E security. It just guarantees network-level security; decryption of transmitted data is still to be happened in the Gateway system.

Table: Pros and Cons of the Solutions

	MME	Intra-Gateway	Using IPv6
Pros	E2E SSL TCP/IP Good for applying WPKI	E2E	Network layer security Direct communication links between users Cheaper W-VAN Good in long term view
Cons	TCP/IP load SSL Authentication RSA Calculation Overload (ECC)	Malicious CP Additional cost Hard to Access (Input IP address directly) Not feasible in domestic environment	E2E (X) Hardware cost (Dual system) Increasing Hardware complexity Hard to define key exchange mechanism for large network

3. Conclusion

(1) Application Protocol Analysis

While other technologies such as i-mode, Anyweb, etc. are implemented based on traditional TCP/IP and Internet; WAP is redefined from the ground for wireless environment in terms of protocol stack and description language. Its approach has two sides of coin. It is optimized only for wireless communications and mobile devices. WAP is suitable for low transmission speed and WML has a more appropriate structure, which is a card-and-deck structure, for mobile devices than any other HTML-like description languages. However, It is not compatible with HTML contents. It is not an industrial leader unfortunately but it is a worldwide standard for wireless Internet.

(2) Markup Language Analysis

WML is still de-facto standard in markup languages for mobile service while the mHTML has possibility to a dark horse in near future because MicroSoft uses mHTML. If MicroSoft integrates other Internet-based programs into mobile applications, mHTML will be more popularized. Core advantage of other HTML based markup language is that it is easy to develop a service in Internet environment because it is compatible with traditional HTML contents. However, all of markup languages do not support various multimedia services yet. It is only available to transmit low-size text or binary-based data.

(3) WAP Gateway Security

WAP Gateway can be attacked by insiders or outside hackers while it is translating WTLS to HTTP protocol. To avoid the exposure of translating problem and to guarantee end-to-end security, three models are suggested. The idea of first model is to let the service providers have the Gateway system in their domain. In this case, the service provider is responsible to keep the G/W secure. Client can connect to the G/W directly by inputting IP address of G/W but this model is not supported yet. In second model, end-to-end security is guaranteed by using SSL protocol in whole communication period. In this case, to guarantee E2E, lots of time and device capacity are necessary. It is quite costly model. Last model is using IPv6 that Nokia presented. Using IPv6 is good at direct linking between users and implementing wireless VAN because it guarantees network-level security, however, translating process is still needed. Therefore, using IPv6 does not support E2E.

As the mobile commerce is growing, WAP Forum is preparing next version of WAP protocol. And adding new tags for multimedia service strengthens markup languages. Success of future mobile business depends upon keeping track of critical mobile technologies such as markup languages, protocol, and security-related technologies.

4. References

[1] WAP Forum, "WAP," white paper, http://www.wapforum.org, June 2000.

[2] Microsoft, http://www.microsoft.com.

[3] S. Allamaraju, et al., "JAVA E-Commerce," wrox, 816~872, 2001

[4] Samsung electronics co. LTD., "AnywebII: New Standard for Communications," white paper, 2001.

[5] ATLAS Research Group, http://www.atlasresearchgroup.org/.

[6] W3Schools.com: http://www.w3schools.com

[7] WAP Forum: http://www.wapforum.org

[8] W3C Submissions: http://www.w3.org

[9] Phone.com: http://developer.phone.com

[10] I-Biznet: http://www.i-biznet.com

[11] Hong Ki Yoong, Wireless PKI Technology Tren, KSIGN, May 2001

[12] Kim Bong Hwan, Security in Wireless Internet Service, ETRI, Aug. 2000

[13] Kwon O Sung, WAP Gateway, MOSCA, Oct, 2000

[14] http://matilda.snu.ac.kr/doc/column/security/wapsecurity.htm, Oct. 2000

[15] NOKIA, IPv6 – Enabling the Mobile Internet, Apr. 2001

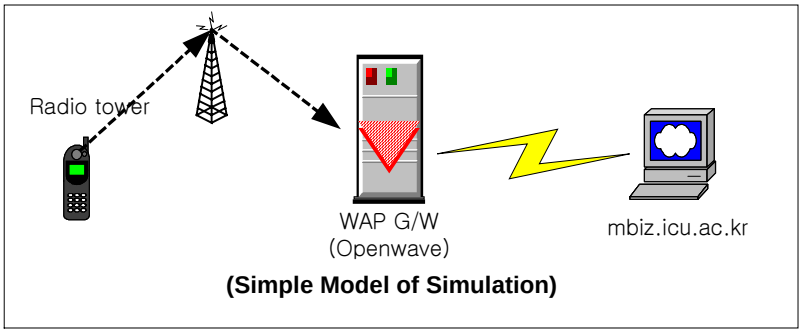
[16] WAP Forum, WMLScript Crypto Library version 05-Nov-1999, 1999

[17] WAP Forum, WTLS Specification, Nov. 1999

5. APPENDIX: Simple Implementation Using WAP/WML

Developing Environment:

Windows Server 2000, WML1.0, ASP3.0, UP4.0SDK, MS-Access2000



(Simple Model of Simulation)

Simulation: Step1----------Step2----------Step3---→ Calling

Source Code

Step1: Search.wml (Selecting a department)

```
<?xml version="1.0" encoding="euc-kr" ?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM/DTD WML 1.1/EN"
 "http://mbiz.icu.ac.kr/ec/wml_1.1.xml">

<wml>
        <card id="search">
                <p align="center">
                        <img src="Welicu.wbmp" alt="Nice Guys!! ICU EC"/>
                        <br/>
                </p>

                <p> 검색조건을 고르세요.
        <select name="type">
         <option value="1" onpick="bydepart.wml#searchbyeng"> EC공학 </option>
         <option value="2" onpick="bydepart.wml#searchbymgt"> EC경영 </option>
        </select>
                </p>
        </card>
</wml>
```

Step2: depart.wml (Select one who is in the list)

```
(중략)
<card id="searchbyeng">
                <do type="options" label="BACK">
                        <go href="search.wml"/>
                </do>

                <p> EC공학학생검색 <br/>


  <select name="search_value">
   <option   value="전진선"   onpick="display.asp?result=$(search_value)">전진선</option>

   <option value="정대민" onpick="display.asp?result=$(search_value)">정대민</option>

   <option value="조원철" onpick="display.asp?result=$(search_value)">조원철</option>

</select>
 </p>
        </card>
(이하 생략)
```

Step3: display.asp (Finding the Phone Number from database, ec.mdb and make a call)

```
<?xml version="1.0" encoding="euc-kr" ?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM/DTD WML 1.1/EN"
 "http://mbiz.icu.ac.kr/ec/wml_1.1.xml">


<%
        Response.ContentType = "text/vnd.wap.wml;charset=euc-kr"

        Set dbconn = Server.CreateObject("ADODB.Connection")
        strpath = Server.MapPath("./ec.mdb")
        dbconn.open("PROVIDER=MICROSOFT.JET.OLEDB.4.0;DATA SOURCE=" & strPath)
        svalue = Request.Querystring("result")
        SQLquery="SELECT depart_name, phone_no FROM depart where depart_name like
"&""""&svalue&""""&""
        Set rs = dbconn.Execute(SQLquery)
%>

<wml>
        <card id="info">
                <do   type="accept" label="전화걸기">
                        <go   href="wtai://wp/mc;<%=rs.fields("phone_no")%>"/>
                </do>

                <do   type="options" label="다시 검색">
                        <go   href="search.wml"/>
                </do>

                <p>
                        검색결과
                <br/>
                <%=rs.fields("depart_name")%>:<%=rs.fields("phone_no")%>
                </p>
        </card>
</wml>

<%rs.Close
  set rs = nothing%>
```

[END OF DOCUMENT]