Analysis and Improvement of Security Features of WTLS Protocol in WAP Environment

A
Dissertation submitted to
JAWAHARLAL NEHRU UNIVERSITY, New Delhi
in partial fulfillment of the requirements
for the award of the degree of

Master of Technology
in
Computer Science & Technology

By
DEEPAK NIGAM

Under the Guidance of
PROF. P. C. SAXENA
&
PROF. C. P. KATTI

SCHOOL OF COMPUTER & SYSTEMS SCIENCES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI - 110067
JANUARY - 2002

SCHOOL OF COMPUTER & SYSTEMS SCIENCES

जवाहरलाल नेहरू विश्वविद्यालय

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI-110067 (INDIA)

CERTIFICATE

This is to certify that that the dissertation entitled *"Analysis and Improvement of Security Features of WTLS Protocol in WAP Environment"* which is being submitted by Mr. Deepak Nigam to the School of Computer & Systems Sciences, JAWAHARLAL NEHRU UNIVERSITY ,NEW DELHI for the award of Master of Technology in Computer Science & Technology is a bonafide work carried out by him under my supervision.

This is original and has not been submitted in part or full to any university or institution for award of any Degree.

4-01-02	Katti	4/1/2k+2
Dr. K.K. Bharadwaj	Prof. C.P. Katti	Prof. P.C. Saxena
Dean	Supervisor	Supervisor
SC & SS, JNU	SC & SS, JNU	SC & SS, JNU

ACKNOWLEDGEMENT

I wish to convey my heartful gratitude and sincere acknowledgements to my Supervisors Prof. P. C. Saxena and Prof. C.P. Katti for their constant encouragement, guidance and affection throughout my work.

I am grateful to them for providing me enough infrastructures through Data Communication and Distributed Computing Group (DCDCG) laboratory to carry out my work. It is great honour for me for being a member of DCDC Group and I am thankful to all the members for their cooperation and understanding.

I would like to thank all my faculty members for their help and useful suggestions during my work. I am also thankful to all of my classmates for their constructive criticism and useful suggestions.

DEEPAK NIGAM

ABSTRACT

The WAP (Wireless Application Protocol) is used for the presentation and delivery of the wireless information on mobile devices, handsets and other wireless terminals. WAP bridges the gap between the mobile world and the Internet and offers the ability to deliver an unlimited range of mobile value-added services to subscribers. These services are independent from Network type and the bearers. From the security point of view, the most significant WAP Specification is Wireless Transport Layer Security (WTLS) protocol. WTLS is integrated into WAP Architecture on top of the WDP. To provide secure communication WTLS should be implemented on both client (i.e. Microbrowser) and WAP Gateway (i.e. Proxy Server). WTLS exists between client and WAP Gateway and SSL exists between Gateway and Web server. The translation between SSL and WTLS takes milliseconds and occurs in memory of WAP Gateway, allowing for a virtual secure connection between two protocols.

Although WTLS provides good security solution but still there exists some problems. The key idea behind this Dissertation Work is to study security issues like Privacy, Authentication , Integrity and Denial of services and also to uncover those security threats that occurs in transmission in WAP Environment. In this work firstly we will provide the concept of security : What are the different Security Issues that a security systems must fulfill . Then the Architecture and the Specification of WAP will be discussed .

One rule for the effective secure system is that it should implement layers of security, the more layers you put, the more security in system. But in the case of WTLS in WAP environment, one cannot increase number of layers because of limited memory, limited supply of power and low processing power of CPU. Hence in last we implemented Encryption/Decryption algorithm that deals with the Limitations of WAP enabled handsets and discussion of effect of this algorithm i.e. how it improves the security features of WTLS.

CONTENTS

CHAPTER I

INTRODUCTION

Internet is the easiest and most efficient way of delivering services to wired users. As users become more and more dependent of services offered on the Internet, one shortcoming becomes increasingly evident – the need for a wire to connect to the Internet. This shortcoming makes itself especially evident to the millions of users that spend a substantial amount of their time on the move. The mobility fills the needs that the user might have to access the information wherever and whenever they fell like it. In terms of value added services , the mobile networks available today do not provide the same level of flexibility like wired networks. WAP addresses this issue by being designed to meet the constraints of a wireless environment.

The development of WAP is being driven by the mobile phone industry who see the merger of mobile and Internet technologies as the logical next step in adding value to their existing cellular networks. The kinds of services that WAP has been developed for include: news and information resources, e-mail, e-commerce (or m-commerce as it is becoming known), banking services, online address books, weather and traffic alerts, mapping and locator services, directory services.

BackGround The Wireless Application Protocol (WAP) is a result of joint efforts taken by companies teaming up in an industry group called WAP Forum. WAP could roughly be described as a set of protocols that has inherited its features, characteristics and functionality from Internet standards and standards for wireless services developed by some of the world's leading companies in the business of wireless telecommunications.

Key features offered by WAP are:

- **A programming model similar to the Internet's**

  Re-use of concepts found on the Internet enables a quick introduction of WAP based services since both service developers and manufacturers are familiar with these concepts today.

- **Wireless Markup Language (WML)**

  A markup language used for authoring services, fulfilling the same purpose as Hyper Text Markup Language (HTML) does on the World Wide Web (WWW). In contrast to HTML, WML is designed to fit small handheld devices.

- **WML Script**

WML Script can be used to enhance the functionality of a service, just as for example JavaScript may be utilized in HTML. It makes it possible to add e.g. procedural logic and computational functions to WAP based services.

- **Wireless Telephony Application (WTA)**

The WTA framework defines a set of features that provides a means to create telephony services. This is accomplished by introducing an in-client interface to the mobile network, handling of network events, a repository that allows real-time handling of services, and a mechanism supporting server initiated services.

- **Optimized protocol stack**

The protocols used in WAP are based on well-known Internet protocols such as Hyper Text Transport Protocol (HTTP) and Transmission Control Protocol (TCP), but have been optimized to address the constraints of a wireless environment, such as low bandwidth and high latency.

The protocol family works across different wireless network environments and makes web pages visible on low-resolution and low-bandwidth devices. WAP phones are "smart phones" allowing their users to respond to e-mail, access computer databases and to empower the phone to interact with Internet-based content and e-mail.

This latest endeavor of integrating handheld wireless devices into today's wired Internet has also brought about many challenges as the proliferation wireless communications and demands increases. And as wireless technologies grow so does the demand for a trustworthy secure environment.

In fact it wasn't until about 1998 with the advent of the Secure Sockets Layer (SSL), now the widespread de facto standard known as the Transport Layer Security (TLS) that sparked a dramatic increase in electronic commerce. The very presence of SSL/TLS instilled a more reliable security environment within the fixed the Internet architecture.

Wireless security is not much different from wired security. You want several things from security, wired or not: authenticate whom you are talking to, secure the data as it travels from the handheld device to the destination host, and ensure that the traffic hasn't been altered route. In Wireless environment WTLS provides this kind of security .In the implementation of WTLS , it took TLS and tried to add datagram support , optimized packet size and select fast algorithms into algorithm suite. Notwithstanding, the Wireless Application Protocol (WAP) is one such technology that is paving the way to the future disconnected global environment [6]. Two options are becoming available for end-to-end WTLS security. The first is WTLS tunneling, which tunnels WTLS traffic through a service provider's network to a remote WAP gateway. WTLS proxy, meanwhile, proxies WTLS connections through the carrier's WAP gateway. Neither solution is widely deployed and each will require partnerships with carriers and phone manufacturers to implement. WTLS is all about adding security to low CPU-powered wireless devices by making the cryptography efficient

This Dissertation report is made to enlighten the new wireless technology and the purpose of this work is to examine the security problems and to develop an algorithm for encryption and decryption so that it would require minimum resources from handheld devices. In this report we first discuss in chapter II the different security issues that any communication system must have. Then in chapter III we discuss about Wireless Application Protocol . And then present the Internet model and compare it with the WAP model. After that we will discuss about different layers available in WAP Architecture. In chapter IV we discuss the Wireless Transport Layer Security Protocol which is responsible for the security in WAP enabled devices in Wireless Communication. In chapter V we discuss about the security problems in WTLS protocol and what will be the accepted level of security. And then we present the encryption and decryption algorithm. After that we will show the effect of this algorithm in WAP enabled devices i.e. what are the different problems in WAP Environment that will be solved by this algorithm . Finally in chapter VI conclusions based on the findings of earlier chapters is presented.

CHAPTER II

SECURITY ISSUES

Just as traditional web pages can be secured using the industry standard TLS (Transport Layer Security), an example of which is the commonly used SSL (Secure Sockets Layer) based security, WAP sessions can be secured by a similar means called WTLS (Wireless Transport Layer Security). Where TLS provides a secure session between the client and the Web Server, WTLS provides a secure session between the wireless device and the WAP Gateway. Similar to TLS, WTLS provides WAP with the key security elements, Privacy, Authentication, Integrity, Non-Repudiation and Denial of Services.

2.1 PRIVACY : Privacy ensures that only the sender and the intended recipient of an encrypted message can read the contents of that message. To guarantee privacy, a security solution must ensure that no one can see.

access or use private information, such as addresses, credit card information and phone numbers, as it is transmitted over the Internet.[7] . The main tool for providing privacy is cryptography. A plaintext is simply encrypted and decrypted to implement privacy. If the plaintext is encrypted using a strong encryption, it is almost impossible for eavesdropper to decrypt and read the original content.

2.1.1 Concept Of Cryptography : In practice, the domain and range of most cryptography functions are the same (that is, bit or byte sequences). We denote encryption with 'C = E(M)', and decryption with 'M = D(C)' ; where M is Message or Plain Text and C is Encrypted Message or Cipher Text . In order for encryption and decryption to do anything useful, the equality M = D(E(M)) will automatically hold (otherwise we do not have a way of getting plain text back out of our cipher text).

In real-life cryptography, we are not usually concerned with individual encryption and decryption functions, but rather with classes of functions indexed by a key. 'C = E{k}(M)' and 'M = D{k}(C)' denote these. For keyed functions, our corresponding automatic equality is M = D{k}(E{k}(M)). With different key indexes to our function classes, we do not expect equalities like the above (in fact, finding them would usually indicate bad algorithms): M != D{k1}(E{k2}(M)). This inequality works out nicely because all the folks without access to the key K will not know which decryption function to use in deciphering C.

2.1.2 Symmetric and Asymmetric Algorithm : There are actually two rather different categories of encryption algorithms. In a previous panel, you saw that it is possible to index encryption and decryption functions with a key. In such a case, we get the equality M = D{k1}(E{k1}(M)). That is, both the encryption and decryption functions use "k1." If this equality holds, the algorithm is a "symmetric."

In 1975, Whitfield Diffie and Martin Hellman proposed a different sort of relationship between encryption and decryption keys. What if we performed encryption and decryption using two different, but related, keys? The consequences turn out to be quite radical. What we get is what is known as "public key" or "asymmetric" algorithms.

2.2 AUTHENTICATION : Authentication is a technique to ensure that the stated identity of the user is correct. In the beginning, the other party introduces itself and claims to have some identity. This is not enough. The contacted party also needs to know for sure that the contacting party is the one it claims to be. The contacting party has to present some verification to prove its identity. It can be as simple as passwords, or more complicated digital signature or certificate. But then again, the contacting party also wants to be sure that the other end is valid. The contacted party has to present some identification about itself.

After the authentication, the service provider can be sure that the service is available to the user who has correct rights to use the service. On the other hand, the user can be confident about the service provider.

WTLS provides 3 levels of authentication:

1. Class 1 – Anonymous Access
2. Class 2 – Server Authentication Only
3. Class 3 – Client and Server Authentication (2 way authentication)

WAP provides encryption throughout all three classes mentioned above. The current implementation of WAP only supports classes 1 and 2. Part of the delay resides in the time to market for the devices which support the various WAP standards. [8] . It is implemented through Digital Certificates.[9]

2.3 INTEGRITY : Integrity ensures the detection of any change in the content of a message between the time it is sent and the time it is received. For example, when a user instructs a bank to transfer Rs. 1000 from one account to another, integrity guarantees that the account numbers and amount in the user's message cannot be altered without the bank or the user noticing. If the message is altered in any way during transmission, the security system must have a way of detecting and reporting this alteration. In many systems, if an alteration is detected, the receiving system requests that the message be resent [3] . In WTLS Integrity is implemented through Message Authentication Code (MAC).[9]

2.4 NON-REPUDIATION : It provides a method to guarantee that a party to a transaction cannot falsely claim that they did not participate in that transaction. In the real world, handwritten signatures are used to ensure this. When a consumer writes a check, presenting a driver's license ensures the identity of the writer (authentication), while the signature on the check ensures that the consumer was in fact present and agreed to write the check (non-repudiation). [3].

It is implemented through Digital Certificates. [9]

2.5 DENIAL OF SERVICES : WTLS contains facilities for detecting and rejecting data that is replayed or not successfully verified. WTLS makes many typical denial-of-service attacks harder to accomplish and protects the upper protocol layers. WTLS may also be used for secure communication between terminals, e.g., for authentication of electronic business card exchange. Applications are able to selectively enable or disable WTLS features depending on their security requirements and the characteristics of the underlying network (e.g., privacy may be disabled on networks already providing this service at a lower layer). [10]

CHAPTER III

WIRELESS APPLICATION PROTOCOL

WAP is an open industry-established world standard that is based upon successful Internet standards such as, but not limited to the eXtensible Markup Language (XML) and the Internet Protocol (IP). Internet technology could not be adopted because of the fundamental limitations of mobile terminals. As a result, the WAP architecture has to meet those requirements by optimizing protocols for narrow-band bearers with potentially high latency and efficient use of devices' resources. Now we will discuss limitations of handheld devices.

3.1 LIMITATIONS OF HANDHELD DEVICES : WAP is targeted at handheld devices of various kinds. Services should be accessible from a Handheld PC as well as from a small phone. WAP addresses this fact by taking the following issues into consideration:

Small Display: When accessing a service from a desktop computer, the size of the screen does not limit the user experience. Wireless devices might also have "big" displays, for example a Personal Digital Assistant (PDA). But many devices will have smaller displays, for example mobile phones, to provide larger portability. No matter how good these displays will be in the future, the size of the human hand will always limit the size of them. Instead of using the flat document structure HTML provides, WML structures its document in decks and cards. A card is a single unit of interaction with the end user, for instance a text-screen, a selection list, an input field, or a combination of them.

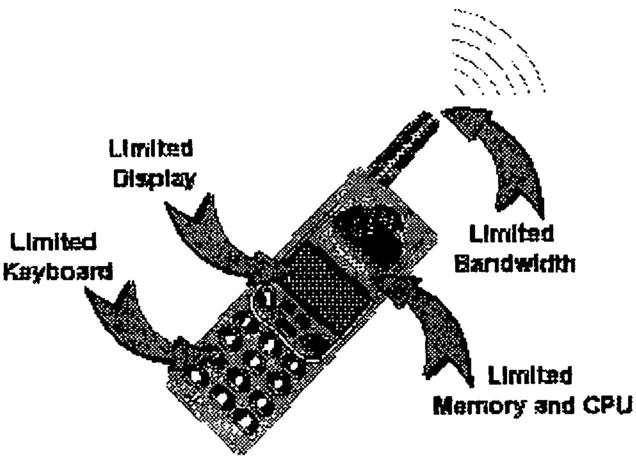

Fig. 1 Limitations of WAP Devices

Limited Input Facilities: Wireless devices do most often not have the same input facilities as their wired equivalents, that is, they lack QWERTY keyboards and have mouse-less interfaces. WML addresses this issue as well. The elements that are used in WML can easily be implemented so they make very humble requirements on the keyboard. The use of decks and cards provides a navigation model that call for minimum inter-page navigation since the user is guided through a series of cards instead of having to scroll up and down on a large page. Further, soft-buttons are supported by WML in order to provide the service developer with a means to couple desired actions to vendor specific keys.

Limited Memory and CPU: Wireless devices are usually not equipped with amounts of memory and computational power (CPU) comparable to desktop computers. The memory restriction is valid for RAM as well as for ROM. Even though the trend indicates that more memory and more powerful CPUs will be available in a foreseeable future, the relative difference will most probably remain. WAP addresses these restrictions by defining a lightweight protocol stack adapted to its purpose. The limited set of functionality provided by WML and WMLScript makes it possible to implement browsers that make small claims on computational power and ROM resources. When it comes to RAM, the binary encoding of WML and WMLScript helps keeping the RAM as small as possible.

Limited Battery Power: The stumbling block in wireless communication devices today is the operating time, i.e. the battery power restricts its usage. Access to wireless services will increase the utilization of bearers (radio interface), and thus will the power consumption also increase. This issue is solved by minimizing the bandwidth needed and thus keeping the bearer utilization as low as possible. In WAP environment there is also limit on Network Bandwidth .As network bandwidth increases the handset's power consumption will also increase, further taxing the already limited battery life of a mobile device. Wireless messaging uses more battery power than

CPU processing alone and WAP applications should take account of this [4].

Low Connection Establishment Time : WAP phones have slow connection establishment time. Majority of the wireless systems is based on circuit switches for data communications. But circuit switches can take up to 30s to establish a connection, just like data access via fixed telephone lines. Mobile users might not have enough patience to wait this long. The other issue faced in the current trend of mobile Internet access is access speed. The speed that is allowed by existing infrastructure makes it difficult for mobile Internet to become really popular.

3.2 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; i.e. the entire content of a page is shown simultaneously. If more advanced features like procedural logic are needed, scripting languages such as JavaScript or VB Script may be utilized. The figure 2 shows how a WWW client requests 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 may be static or dynamic. Static content is produced once and not changed or updated very often, for example a company presentation.

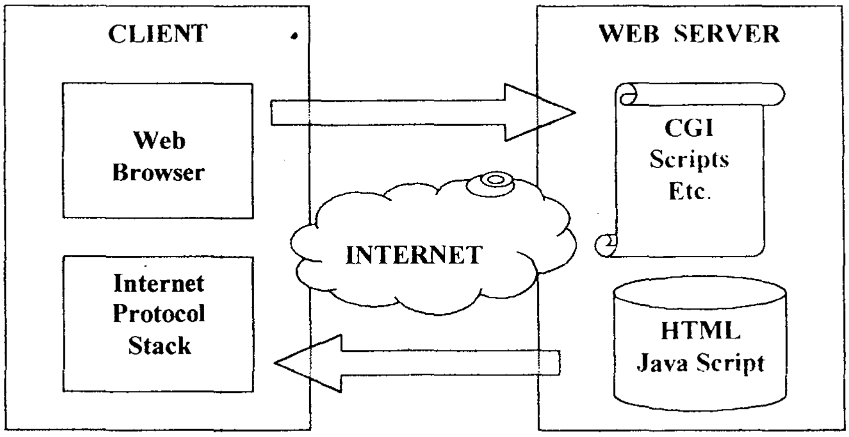

Fig. 2 Internet Model

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 Servlets allow content to be generated dynamically .

3.3 WAP MODEL : WAP does also make use of the Internet paradigm to provide a flexible service platform. In order to accommodate wireless access to the information space offered by the WWW, WAP is based on well-known Internet technology that has been optimized to meet the constraints of a wireless environment. Services created using HTML would not fit very well on small handheld devices since they are intended for use on desktop computers with big screens. Low bandwidth wireless bearers would neither be suitable for delivering the rather extensive information that HTML pages often consist of. Therefore a markup language adapted to these constraints has been developed - the Wireless Markup Language (WML). WML offers a navigation model designed for devices with small displays and limited input facilities (no mouse and limited keyboard). 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, which is the entity that connects the wireless domain with the Internet. The solution in WAP is called WML Script. The figure 3 shows the WAP programming model. WAP model without the WAP Gateway/Proxy is practically identical to Internet Model.

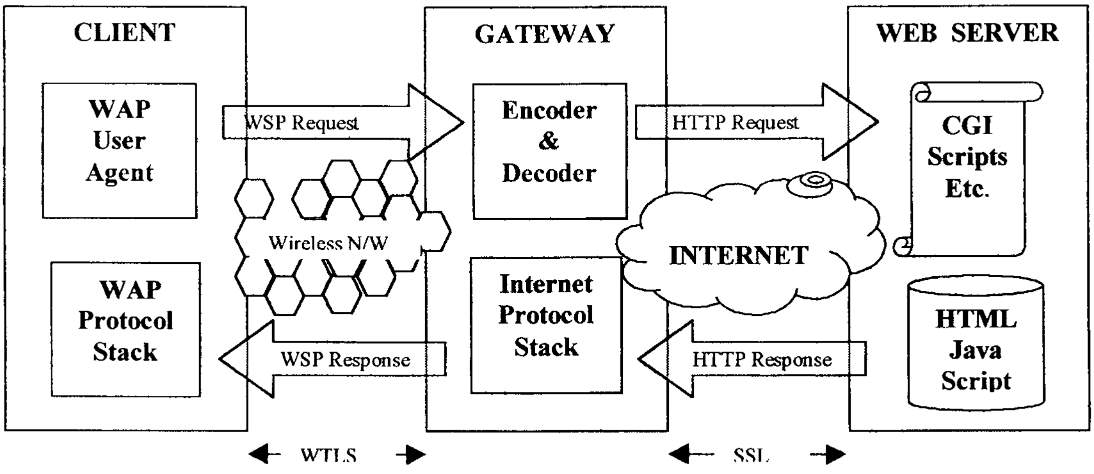

Fig. 3 WAP Model

The request that is sent from wireless client to WAP Gateway/Proxy Uses the Wireless Session Protocol (WSP) . In its essence WSP is A binary version of HTTP.

The main elements of WAP Model are

3.3.1 Client : It is usually WAP handset used to access WAP services. Software vendors are developing the browser so that one can use existing device to access WAP Services.

3.3.2 Gateway : The WML pages can't be delivered directly to WAP device. Instead they must pass through a WAP gateway, which translate them into a compressed "byte code" format that a WAP device understands. This compression helps to get the best performance from the WAP devices. Personal WAP users are likely to use their mobile operator's WAP gateway. The communication path between WAP device and the WAP gateway is referred as Bearers. The most common bearers are - SMS , CSD (Circuit Switched Data) and Packets.

3.3.3 Web Server : It takes the content (information) and formats it into WML that the WAP Devices can understood. WML pages are very similar to HTML pages.

"A secure WAP conversation occurs in two stages. First the transmission between the web server and' the WAP gateway occurs over SSL. The onward transmission of this message over the air interface to and from the WAP browser device is over wireless networks using WTLS. Essentially the WAP gateway serves as a bridge between the WTLS and SSL security protocols. There are considerations (some say limitations) in the introduction of a bridging protocol like WTLS. The current WAP security model requires a strong relationship between the network operator and the content provider. The WAP Forum has recognized that as the market for highly secure applications increases, a more flexible and extensible solution will be needed. When working across many different wireless networks, application developers must be assured that their content remains encrypted from the time it leaves their application server until it arrives at the WAP handset. As a result there is a process underway to develop this more advanced security solution, which must address the enterprise's need for higher security and the operator's need for proper integration with WAP gateways in the wireless network."[5]

3.4 WAP ARCHITECTURE : The lightweight WAP protocol stack is designed to minimize the required bandwidth and maximize the number of wireless network types that can deliver WAP content.

The layers in WAP architecture are as follows.

3.4.1 Application Layer resides at the top of the WAP stack. It has WAE (Wireless Application Environment) protocol. The WAE consists of two main parts, the Wireless Markup Language (WML) and WMLScript, which provides a software platform environment for the application software. The application environment is built into microbrowser and defines the user interface and programming language of the device. WML's integrated scripting language, WMLScript, allows programmers to embed executable logic in the applications to control many functions of the browser and the wireless device.

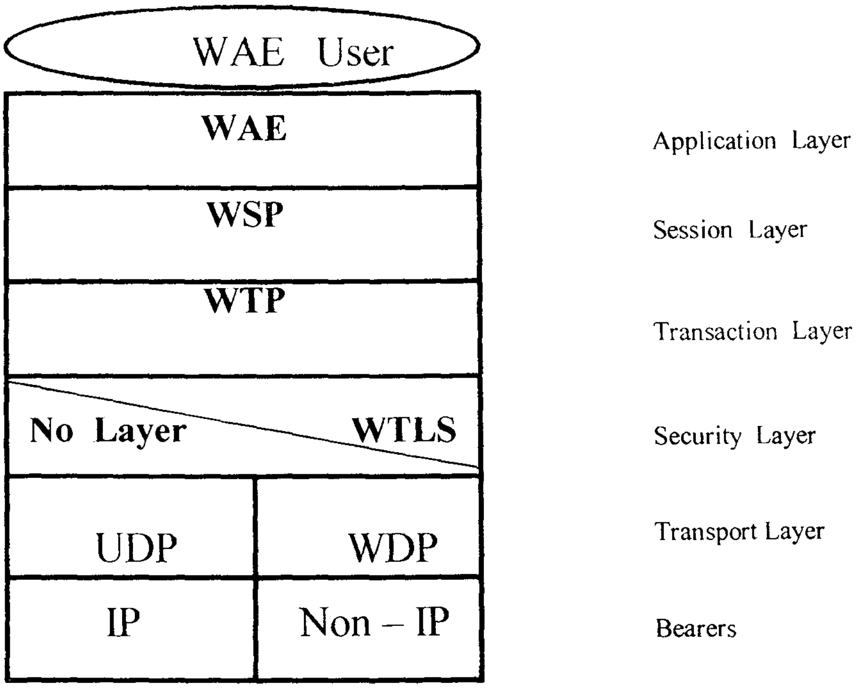

Fig. 4 WAP Architecture

3.4.2 Session Layer It has WSP (Wireless Session Protocol). WSP defines two protocols, one that provides a connection-mode session over a transaction service and the second protocol that provides non-confirmed, connectionless service over a Datagram transport service. In essence the protocol allows sessions to be suspended and then proceed without the overhead of re-establishing the connection. Secure sessions can be accomplished with the assistance of the security layer in combination with public/private certificates. WSP was designed specifically for low-bandwidth wireless networks.

3.4.3 Transaction Layer It has Wireless Transaction Protocol (WTP). WTP was designed for interactive browsing which incorporates a "content push" that would enable a server to send messages and documents to a device without the need for a specific request. The transaction protocol resides between the session protocol layer and the security protocol layer of WAP stack. WTP divides data packets into lower level datagrams and concatenates received datagrams into useful data. It also keeps track what packets were sent and received and when detected, performs re-transmissions and acknowledgments. There are three messages types that are supported by WAP's WTP. These consist of an unreliable one-way request known as a non-guaranteed push, a reliable one-way request known as a guaranteed push and last a reliable two-way request/response transactions.

3.4.4 Security Layer It has Wireless Transport Layer Security (WTLS) protocol . Which was formulated specifically to enable secure transactions and at the same time embrace the power and memory resource requirements necessary to implement secure solutions. As mentioned WAP's WTLS is based on the Internet de facto standard of the Transport Layer Security (TLS). WTLS compensates for the known wireless limitations by minimizing protocol overhead utilizing better compression, and employing more efficient cryptography, such as RSA or Elliptical Curve Cryptography (ECC). The WTLS provides privacy by using strong encryption, integrity using MACs, and provides a public/private key pair for authentication. WTLS also provides dynamic key refreshing which allows encryption keys to be updated on a regular and configurable basis during a secure session.

To insure an even tighter secure environment, it also offers private passwords in addition to the public/private key pair. The heart of WAP's WTLS protocol is the kernel, which responsible for ensuring trustworthy security in wireless communications. The kernel of WTLS is the Wireless Identity Module (WIM). WIM can be implemented on a smart card, in a SIM card or any tamper resistant device such a special memory segment. WIM enhances the security of wireless communications by providing the security elements like private keys and client certificates to verify a client's identity. WIM also supplies trusted CA certificates to verify servers. Another purpose of WIM is to store the vital WTLS session data that is used to continue a suspended session. This operation will only occur using a PIN private to the client. In addition, the WTLS kernel enhances security by performing optimized cryptography handshakes, which is necessary during client authentication, and creates long-term, secure WTLS connections.

3.4.5 Transport Layer It has Wireless Datagram Protocol (WDP) . At the base of the WAP stack lies the actual transport layer protocol, referred to as the Wireless Datagram Protocol (WDP). The transport layer is supported by a variety of network types and provides a consistent interface between the higher layers within the WAP architecture and the wireless networks. WDP processes datagrams from the stack's upper layers into various formats required by the different physical data paths. Therefore, the upper layers of the WAP stack are able to operate independently of the underlying wireless network because of the WDP. Therefore, the upper levels utilize the interface offered by the WDP to communicate transparently over one of the available services.

3.5 SECURING WAP : Security of WAP applications is dependant on three main objectives:

1. WAP Gateway Security
2. Transmission Security
3. Enabling certificate management through PKI
4. Security of the handset and bearer

WAP Gateway Security :

The security of the WAP Gateway is essential, since all the transaction-based content must traverse this server and the encryption in essence "goes away" when the packet gets to its gateway. This server, in many cases, will reside outside of the content providers perimeter. Many of the newer development efforts appear to be outsourcing the Gateway to a third party. When assessing the security of the WAP gateway, it is important to assess the level of protection provided in the following areas:

1. Physical Security of the server
2. Access control at the file, registry and application levels
3. Back-end security between the Gateway and the Web Server
4. Baseline for the permissions. roles and user abilities

Transmission Security :

Transmitting the information is another important area for protection. The Transmission of data can be observed by the third party. To prevent this kind of stealing the concept of "Frequency Hoping" comes. Under this , the data is transmitted over frequently changing frequencies with very less interval during change of frequency. It assures that if the eavesdropper has the ability to listen the transmission , they can't do it so long because you are OFF to the next frequency with in milliseconds. Fast frequency hopping avoids interference by third party. In WAP environment this method is expensive for both the company transmitting the data and user.

Enabling certificate management through PKI : The PKI (Public Key Infrastructure) allows the application provider and the user to authenticate to each other and to provide non-repudiation capabilities.

For PKI, WTLS uses two types of certificates.

"*WTLS server certificates*, defined as part of WAP 1.1, are used to authenticate a WTLS server to a WTLS client (handset) and to provide a basis for establishing a key to encrypt a client-server session. They are like SSL server certificates, except that two different certificate formats are defined - X.509 certificates (as in SSL) and WTLS mini-certificates, which are functionally similar to X.509 but are smaller and simpler than X.509 to facilitate their processing in resource-constrained handsets. The mini-certificate is mandatory to implement and the X.509 certificate is optional to implement.

WTLS client certificates, defined as part of WAP 1.2, are used to authenticate a WTLS client (handset) to a WTLS server. They also can be formatted as either X.509 certificates or mini-certificates. WAP 1.2 also defines an interesting PKI-based function that is not part of WTLS. This function, which allows a WAP client to digitally sign a transaction, is known as the WML2 Script Sign Text function, and is intended for applications that require non-reputable signatures from clients."

Security of handset and bearer : Use of mobile device certainly increases the productivity of the organization. Since wireless devices are highly mobile they can be easily stolen or may fall into wrong hands. Hence user authentication is required for the security of the handset. In the scheme of the authentication no one is allowed to share the keys.

WTLS, although providing a fairly complete security solution, lacks a mechanism for providing availability. Although WAP based viruses and other malicious code has not yet been discovered, be proactive in assuring protection from these types of threats. A strong PKI solution is imperative as overall security is based on the management of the certificates.

CHAPTER IV

WIRELESS TRANSPORT LAYER SECURITY

WTLS is designed to function on connection-oriented and/or datagram transport protocols and security is assumed to be an optional layer above the transport layer . The reason for saying it optional is that the security feature can be omitted from WTLS if it is already provided by Network. It provides the upper-level layer of WAP with a secure transport service interface that preserves the transport service interface below it. The session or application management entities are assumed to provide additional support to manage secure connections (e.g., initiate and terminate).

It provides additional features from TLS such as dynamic key refreshing, optimized handshake and datagram support. The WTLS protocol is optimized for low-bandwidth bearer networks with relatively long latency. WTLS Connection management allows a client to connect with a server and to agree on protocol options to be used. The primitive sequence for establishing a secure session (full handshake) is shown in figure 5.

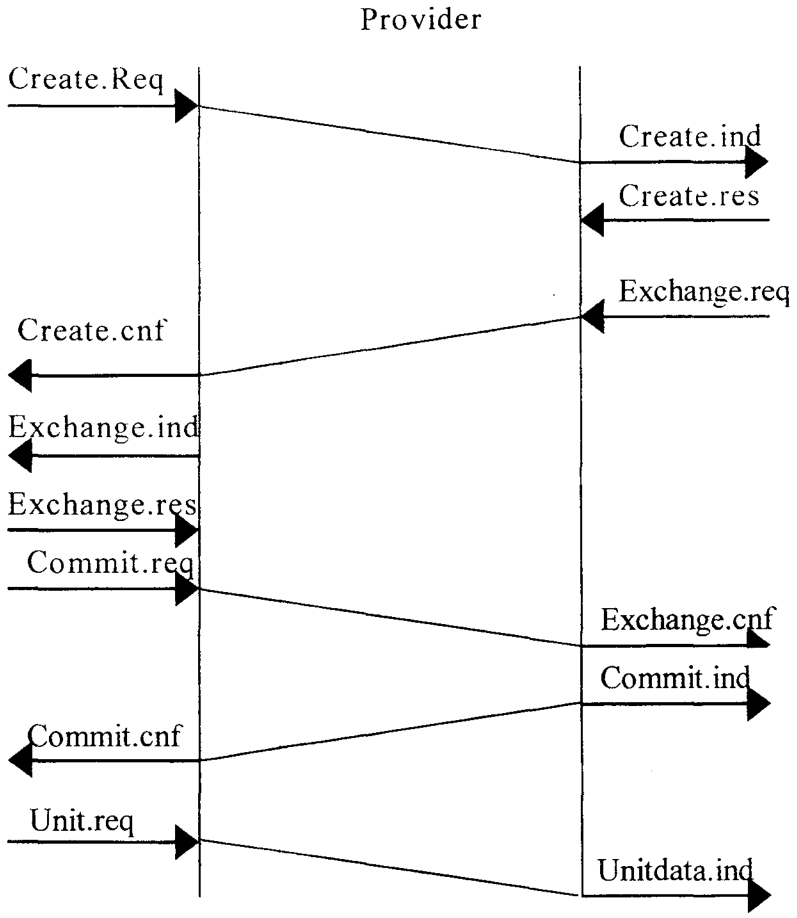

Fig. 5 Full Handshake

SEC-Create : This primitive is used to initiate a secure connection establishment.

SEC-Terminate : This primitive is used to terminate connection.

SEC-Exchange : This primitive is used in a secure connection creation if the server wishes to perform public-key authentication or key exchange with the client.

SEC-Commit : This primitive is initiated when the handshake is Completed and either peer requests to switch into the newly negotiated connection state.

SEC-Create-Request : This primitives is used by the server to request the client to initiate a new handshake.

4.1 WTLS INTERNAL STRUCTURE : The WTLS Record Protocol is a layered protocol which accepts raw data from the upper layers to be transmitted and applies the selected compression and encryption algorithms to the data. Moreover, the Record Protocol takes care of the data integrity and authentication. Received data is decrypted, verified and decompressed and then handed to the higher layers. The Record Protocol is divided into four protocol clients. The protocol stack is shown in Figure 6. The different clients are described in the following sections. The application protocol is not described here, since it is the interface for the upper layers.

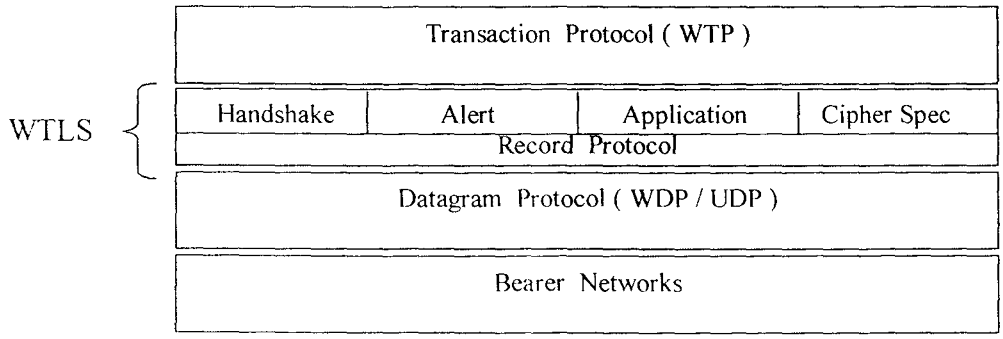

Fig. 6 WTLS Internal Architecture

4.1.1 Handshake Protocol The handshake protocol is responsible for negotiation a secure session. In the connection phase all of the necessary security parameters are agreed upon. This can include cryptographic algorithms, key lengths, key exchange. and authentication. When a secure connection is established the client has the possibility to send secure data over the net.

4.1.2 Record Protocol When the record protocol receives a record from the layer above that is going to be transmitted, it optionally compresses the data, applies a MAC to it and encrypts it, before the package is sent. When the record protocol receives a record it decrypt it, verifies and decompress it before sending it to higher-level clients. To optimize the transport of records, several of them can be transported in one Service Data Unit (SDU). This is normal to do with records that have a logic connection like the handshake records. Error handling in the WTLS is based on the alert messages. When a error is detected the detecting party sends an alert message containing the occurred error. Further procedures depend on the level of the error that occurred.

4.1.3 Alert Protocol Alert messages transport how critical the messages are and a description of the alert. Alerts use a four-byte checksum that are calculated from the last record received from the other party. The receiver of the alert should verify that the checksum matches with the message earlier sent. Alert messages are sent using the current secure state, i.e. compressed and encrypted . If the alert message, labeled as fatal, is sent, then both parties terminate the secure connection. Other connections using the secure session may continue but the session identifier must be invalidated so that the failed connection is not used to establish new secure connections.

4.1.4 Cipher Spec Protocol This protocol implements to signal transitions in the ciphering strategies. It consists of a single message, which is encrypted and compressed under the current connection state. The message consists of a single byte of value 1. The reason to send this protocol is to notify the other party that subsequent records will be protected under the newly negotiated Cipher Spec and keys. If the cipher spec is NULL, all security in WTLS is "turned off". Application Protocol Consists of the payload that the terminal wishes to send. The Change Cipher Spec message is sent during the handshake phase after the security parameters have been agreed on.

4.2 WTLS CLASSES : There are 3 types of classification of WTLS

Class 1 WTLS Implementation

- No certificates exchanged in secure negotiation
- Client and Server setup secure tunnel anonymously
- Secure session created, but who is talking to who?

Class 2 WTLS Implementation

- Server certificate sent to client during handshake
- Client authenticates server
- User (client) obtains server's identity before wireless transaction (e.g. shopping with credit card)

Class 3 WTLS Implementation

- Server & client certificates exchanged
- Client authenticates server
- Server authenticates client
- High security transactions (e.g. wireless banking) need client & server authentication

CHAPTER V

SECURITY IN WTLS PROTOCOL

A secure connection is set up with an establishment phase where negotiation such as parameter settings, key exchange and authentication is performed. Both parties can abort the secure connection during establishment or at any time later.

In the WAP architecture it is important to take into consideration the fact that the security layer, Wireless Transport Layer of Security (WTLS), is mandatory. To ensure the existence of WTLS in a system it is important to ensure the existence of WTLS in both , the terminal and WAP Gateway. WTLS is designed to function on connection-oriented and/or datagram transport protocols. The WTLS preserves the transport service interfaces. The session or application management entities are assumed to provide additional support to manage secure connections (e.g., initiate and terminate) . When implementing security into the applications the designer must take into consideration the functionality of the application compared to the level of security. WTLS provide Integrity, Authentication, Privacy and Denial-of-services. All these features certify that the sent data had not been manipulated by third party , privacy is guaranteed and the author of the message can be identified.

In the WAP-technology some of the security features may be mandatory, optional or not there at all. The none existence of security occurs when the cipher-suite is assigned to the value NULL. At the surface, the WTLS looks reasonably good. Regarding the research made by Markku-Juhani Saarinen, most of the text in the WTLS specification has been adopted, word for word, from TLS specification. However, many of the changes made by WAP Forum have led to security problems.

5.1 SECURITY PROBLEMS OCCOUR IN WTLS : In WAP environment , due to the limitation of WAP devices , the developers have to compromise between the security level and limitation of WAP Devices. These compromise may lead to following problems.

5.1.1 Man-in-middle Attack : Data can be modified during the transfer due to Man-in-the-middle attack. Anonymous authentication is main cause for the man-in-the-middle attacks. To prevent this problem to the client should define that during the handshake it will not support key exchange suites without authentication. In order to prevent man-in-the-middle attacks, the anonymous authentication should be denied, at least from the server side.

5.1.2 Denial-of-Service Attacks : Since WTLS operates on top of datagrams, the implementation should pay special attention to preventing denial-of-service attacks. It should take into account that some networks transport addresses may be forged relatively easy. To avoid this it is not possible for an attacker to break up an existing connection/session by sending a single message in plaintext from a forged address.

5.1.2 XOR-MAC with Stream Cipher : The WTLS supports a 40-bit XOR MAC, which works by padding the message with zeros, diving it into 5-byte blocks and XOR'ing these blocks together [2]. The XOR MAC does not provide any message integrity protection if stream ciphers are being used, regardless of the key length. A bit can be inverted in the ciphertext if the inverting is also done to the MAC. Thus the integrity check will be successful even when the content has been modified. This security problem affects integrity.

5.1.3 Unauthenticated alert messages : Some of the alert messages used in the protocol are sent in Cleartext and are not properly authenticated. Most of these messages are warnings and do not cause the session to be terminated. Since an alert message can take up a sequence number "slot" in the protocol, an active attacker may replace an encrypted datagram with an unauthenticated plaintext alert message with the same sequence number without being detected. This leads to a truncation attack that allows arbitrary packets to be removed from the data stream. We recommend that all messages affecting the protocol state should be properly authenticated. This security problem affects integrity.

5.1.4 No encryption at record_type field : The record_type field is sent unencrypted. The eavesdropper can determine the change of keys reading the contents of this field. The existence of encrypted error messages can be determined from this field. This security problem affects privacy.

5.1.5 Exhaustive Search On Symmetric Cipher : In order to mount an exhaustive key search on a symmetric cipher, one needs to have enough known or probable plaintext, so that the correct key can be recognized with trial decryption of one or more blocks. As symmetric ciphers are too fast they are implemented on most of WAP equipment. To solve this problem either increase key length or use asymmetric cipher. One solution for the exhaustive search is Key refreshing. Key refresh makes crypto-analysis less attractive for an attacker because keys will be invalidated regularly and the material that can be gained is limited. This is particular useful in environments, where export-restricted encryption is used and handshaking is expensive.[4]

If the Cipher Spec is NULL it is important to know that WTLS offers no security.

5.2 ACCEPTED LEVEL OF SECURITY :

When thinking of security in a system it is not just important to take care of security mechanism implemented into the system, but also the available infrastructure. One rule is to implement layers of security, the more layers you put in system the more effective will your security be. But in case of

WTLS , one can't increase the number of layers as it will require more memory and CPU power .

In the WAP infrastructure it is important to think of the layers of security when it comes to the WAP Gateway and WAP Server. From the WAP point of view the available security level is a compromise with the usage of limited resources. There is no point in using more than half of the available limited computing resources for encryption and decryption or create excess traffic to the narrow bandwidth. However, the WTLS has to ensure certain security level in order to be used for commercial purposes. It is not possible to maintain certain standards for a sufficient level of security because the level of security required is dependent on the information that is to be transmitted. The transmitted information always has some importance, hence, the owner of the information decides how much effort is put to preserve the confidentiality.

5.3 ENCRYPTION / DECRYPTION ALGORITHM : This algorithm is used for converting Plain Text to Cipher Text. It uses 4 registers for storing the Plain Text as well as Cipher Text. Here word size is w bits. Encryption consists of r number of rounds. b denotes the length of encryption key in bytes.

Encryption Algorithm

Input : Plain text stored in four w-bit input registers A, B, C, D .
r is number of rounds
w – bit round keys S[0,......,2r+3]

Output : Cipher text stored in A, B, C, D .

Algorithm :

```
B = B + S[0]
D = D + S[1]
    for I = 1 to r do
    {
        t = ( B x ( 2B + 1 )) <<< lg w
        u = ( D x ( 2D + 1 )) <<< lg w
        A = (( A ⊕ t ) <<< u ) + S[2i]
        C = (( C ⊕ u ) <<< t ) + S[2i + 1]
        ( A, B, C, D ) = ( B, C, D, A )
    }
    A = A + S[2r + 2]
    C = C + S[2r + 3]
```

Decryption Algorithm

Input : Cipher text stored in four *w*-bit input registers A, B, C, D .
r is number of rounds
w – bit round keys S[0,......,2r+3]

Output : Plain text stored in A, B, C, D .

Algorithm :

```
C = C – S[2r + 3]
```

```
A = A - S[2r + 2]
for i = r down to 1 do
{
        ( A, B, C, D ) = ( D, A, B, C )
        u = ( D x ( 2D + 1 )) <<< lg w
        t = ( B x ( 2B + 1 )) <<< lg w
        C = (( C - S[2i + 1] ) >>> t ) ⊕ u
        A = (( A - S[2i] ) >>> u ) ⊕ t
}
D = D - S[1]
B = B - S[0]
```

Where :

a + b integer addition modulo 2^w

a − b integer subtraction modulo 2^w

a ⊕ b bitwise exclusive OR of *w* bit words

a x b integer multiplication modulo 2^w

a <<< b rotate the *w*-bit word a to the left by the amount given by least significant lg*w* bits of b

a >>> b rotate the *w*-bit word a to the right by the amount given by least significant lg*w* bits of b

Key values are calculated as :

```
S[0] = $P_w$;
t = 2( r + 1 ) ;
for i = 1 to t do
```

$$s[i] = s[i-1] + Q_w ;$$

where P_w and Q_w are magic constant.

$P_w = odd((e-2)2^w)$ $e = 2.7182......$

$Q_w = odd((\phi-1)2^w)$ $\phi = 1.6180339......$

Odd (x) is odd integer nearest to x ,
rounded up if x is an even integer

(A, B, C, D) = (B, C, D, A) is used for the parallel assignment of values of registers at right side to the registers at left side.

Where A, B, C, D are four w bit registers

5.4 EFFECT OF ALGORITHM IN HANDSET : Implementation and characteristics of this algorithm shows the following results.

✓ As this algorithm is Asymmetric and Block Cipher algorithm. It will solve

the problem of

- XOR – MAC with Stream Cipher
- Exhaustive search on Stream Cipher
- Plain Text leaks etc.

✓ Also this algorithm is memoryless algorithm. It does all the operations on registers hence it solves the problem of Limited memory.

✓ This algorithm is designed in such a manner that by changing 1 bit in plaintext , the ciphertext will changed to complete different text. So the problem of man-in-middle attack can be resolved. The implementation of this algorithm causes the error-propagation . By changing the key length *w* and no. of rounds , it can be solved.

☞ **Solution For Gateway Security :** Since the encrypted request from the client is converted into plaintext and then it is forwarded to the web server. Before this request is fulfilled the plaintext remains in the memory of Gateway. An active attacker can access this information , which creates the problem for security system. "Some providers have worked around this problem by moving their wireless gateways behind their trusted network, or at the very least launched only less-sensitive applications for wireless use until a more robust fix can be implemented" [1] .

To get rid from this problem , it is necessary that the information should not kept in plain text form in the secondary media of WAP Gateway. And the process of decryption and re-encryption should be optimized for speed so that the \unencrypted data is erased from memory of Gateway ,and also it should be security conscious . WAP Gateway can also be secured by limiting the administrative access from the Remote locations.

CHAPTER VI

CONCLUSION

In the Wireless Application Protocol Environment , the WTLS was the first attempt to implement security. After the study of the security features available in WTLS we can say that the security features in WTLS are optional i.e. if Network itself provides some security feature like Privacy then this feature can be omitted from the WTLS to reduce the requirement of limited resources.

After the analysis of the problems that occours in WAP Environment , we came to conclusion that to achieve the sufficient level of security , Cipher Suit (i.e. all the algorithms like Encryption/Decryption , Compression , Key expansion etc.) should be combined properly i.e. Cipher Suit will decide the available level of security. Although WTLS provides the good security solution but the problems that occours are due to the limitations of available resources. The characteristics of given algorithm shows that it solves these problem.

Finally, my opinion about this technology is that it may be well on its way but this technology is extremely new and has not proven itself in industry as per user demands.

REFERENCES

[1] Mike McMurry , Wireless Security , SANS Institute , January 22, 2001 , http://www.sans.org

[2] Saarinen , Markku-Juhani , Attacks against the WAP WTLS Protocol, September 20,1999 , http://www.jyu.fi/~mjos/wtls.pdf

[3] Phone.com White Paper ,Understanding Security on The Wireless Internet , January , 2000, http://www.phone.com

[4] Tessella's Services. "Wireless Application Protocol (WAP)", WAP Technical Supplement, http://www.tssp.co.uk/literature/Supplements/WAP.htm, June,2000

[5] T. Dierks and C.Allen, "The TLS Protocol Version 1.0" , RFC 2246, 1999, ftp://ftp.isi.edu/in- notes/rfc2246.txt

[6] Sandra Laquina, "Wireless Application Protocol" , SANS Institute , September 4, 2000 , http://www.sans.org

[7] Algorithmic Research's WAP White paper, "Closing the Gap in WAP" ,2001

[8] Timothy P. Appleby , Global Integrity - White Paper , "WAP the Wireless Application Protocol" ,1999

[9] Burak Güçer. "Wireless Application Protocol and Security" , SANS Institute , August 15, 2000 , http://www.sans.org

[10] Marcus Cutts , "Secure Wireless Application Protocol (WAP) on the Enterprise , Ready or Not?" ,SANS Institute , September 5, 2000, http://www.sans.org

[11] "WAP-White Paper", AU-System Radio , February ,1999 .

[12] "WAP White Paper", Wireless Internet Today, October, 1999

[13] Ir. Chem Yuet Meng, "WAP – The Precursor to Wireless Internet?" , JURUTERA, Institution of Engineers-Malaysia, July, 2001.

[14] WAP Forum, Wireless Transport Layer Security Specification Version 1.1, 11.2.1999 , http://www.wapforum.org

APPENDIX

Definition of Common Terms Used

☞ Certification Authority : A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key .

☞ Dynamic key refreshing : It allows encryption keys to be updated on a regular and configurable basis during a secure session. This not only provides a higher level of security, but also provides considerable bandwidth savings on the relatively costly handshaking procedure.

☞ Handshake: The procedure of agreeing on the protocol options to be used between a client and a server. It includes the negotiation of security parameters (e.g., algorithms and key lengths), key exchange and authentication. Handshaking occurs in the beginning of each secure connection.

☞ PKI : A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual.

☞ Public key cryptography : It is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet.(The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)

☞ Secure Connection: The WTLS connection that has a connection state. Each secure connection is identified by the transport addresses of the communicating peers.