Sudan University Of Science and Technology

College Of Engineering

School of Electronics Engineering

Configuration of Secure Wireless Application Protocol Gateway

A Research Submitted In Partial fulfillment for the Requirements of the Degree of B.Sc. (Honors) in Electronics Engineering

PREPARED BY:

1. Ayat Abbas Alsheikh
2. Nashwa Ali Naser
3. Nusaiba Mahgoub Mohammed
4. Wigdan Ahmed Hammad

SUPERVISED BY:

Dr. Sami Hassan Omer

OCT 2015

بسم الله الرحمن الرحيم

قال تعالى:

(قَالُواْ سُبْحَانَكَ لاَ عِـلْمَ لَنَا إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ)

سورة البقره(32)

صدق الله العظيم

الاهـــــــــدا ء

الى ملاكي في هذه الحياة..الى معنى الحب والتفاني..الى بسمة الحياة وسر الوجود..

الحبيبه أمي..

الى من علمنا كيف نقف ونبدأ الألف ميل بخطوه وعلمنا الصعود وعيناه تراقبنا..والدنا الحبيب..

الى الأخوات اللاتي لم تلدهن أمي..الى من تحلو بالاخاء وسعدت برفقتهم في دروب الحياة الحلوه والحزينه..

الى من تعلمنا منهم معنى الصبر والبذل والعطاء، وغرسوا حب العلم بعقولنا ، وكانوا أولى عتبات سلم الأمجاد، اساتذتنا الكرام..

نهدي اليكم فرحتنا علنا ننشرها لافاق بعيده ،،أيام جميلة قضيناها نعيشها الان لحظة بلحظة ، وكأنها شريط يمر بمخيلتنا يوما بيوم،لن ننسى هذا المكان الذي جمعنا بمقاعده ،لن ننسى وطننا المعبق بأريج الحب.

الشكر والعرفان:

الشُـــــــــــــــكر لله اولاً واخراً ،ومن ثَم الشُكر موصول الي كل من وضع بصمته ولو بكلمه وساهم في إنهاء هذا البحث والى من تحمّل مسؤوليه الإشراف علي هذا المشروع .

لانـــــــــــــــنسى من كان لها الدور الأعظم في تهيئه البيئه المناسبه واتاحه فرص العمل والانجاز الا وهي الأُسره الكريمه والأُم خاصه واسره جامعه السودان للعلوم والتكنولوجيا.

Abstract

The wireless application protocol(WAP) is a protocol stack for wireless communication network.WAP uses WTLS, to secure the communication between the mobile phone and other parts of the WAP architecture. This project describes the structural that is the security of critical applications by WAP. example of critical applications we used the implementation of the bank.

And as a solution to some of the security problems related to WTLS, which is a gap security while the basic gate sends data to the service provider and allow each customers cross through it, so we prefer to use Additional Gateway which sets to allow some users to access the server to get service with internet protocol, and blocks any IP address which is undefined inside it. we have developed additional gate near the internet service provider to make the connection from the client to the service provider's security.

Practically, we used Wireless Markup Language(WML) to design the implementation of the bank application. which was placed in a laptop and considered it as a service provider. We used an access point to create a local area network(LAN) connection through which small mobile device allowed him access to the provider for receiving the service, which has its request and that appear in the form of cards on a mobile screen.

المستخلص

بروتوكول التطبيقات اللاسلكيه عباره عن مجموعه من الطبقات ،يستخدم مع شبكات الإتصلات اللاسلكيه. يستخدم هذا البروتوكول طبقة الارسال اللاسلكي الامن لعمل السريه والأمن بين الموبايل وأي جزء آخر داخل هيكليته.

هذا المشروع يصف الهيكليه التي يتم بها امن التطبيقات الحساسه بواسطه بروتوكول التطبيقات اللاسلكيه وكمثال للتطبيقات الحساسه قمنا باستخدام تطبيق البنك.

وكحل لبعض المشاكل الأمنيه المتعلقه ببروتوكول طبقة الإرسال اللاسلكي الآمن وهي وجود ثغره أمنيه أثناء قيام البوابه الأساسيه بـإرسال البيانات لمزود الخدمه والسماح لكل المستحدمين بالعبور من خلالها، لذلك يفضل إستخدام بوابه إضافيه يتم ضبطها بحيث تسمح لبعض المستخدمين بالوصول الي المخدم للحصول علي الخدمه المعينه بواسطه برتوكول الإنترنت وتحجب بقية العناوين غير المعرفه داخلها، وقد وضعنا البوابه الإضافيه بالقرب من مزود خدمه الإنترنت لجعل الإتصال من العميل لمزود الخدمه آمن.

تطبيقا؛ قمنا بإستخدام لغه الترميز اللاسلكيه في تصميم تطبيق البنك والذي تم وضعه في جهاز اللابتوب باعتباره مزود خدمه . إستخدمنا نقطه وصول لخلق شبكه محليه صغيره يتصل عن طريقها جهاز الموبايل المسموح له بالوصول للمزود لحصوله على الخدمه التي قام بطلبها والتي تظهر في شكل كروت على شاشة الموبايل.

TABEL OF CONTENTS

CHAPTERS TITLE PAGE

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

Abbreviations:

ASP	Active Server Pages
HDML	Handheld Device Markup Language
HTML	Hyper Text Markup Language
IP	Internet Protocol
ISP	Internet Server Provider
MAC	Media Access Control
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
SSL	Secure Session Layer
TCP	Transmission control protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAP	Wireless Application Protocol
WML	Wireless Markup Language
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security

WTP	Wireless Transaction Protocol
WDP	Wireless Datagram Protocol

Chapter One

Introduction

1.Introduction

1.1.Preface

The number of mobile phones in the world is increasing every day at an astonishing speed. These means increasing of applications that used with it. Also we have come to take for granted the availability of information. There are many ways to provide application access on mobile devices , and these applications want to be available for a long time. Some of these applications must be more sensitive, the security consideration in sensitive application must be implemented on mobile banking .

Mobile banking can be broken into three key areas: Informational, Transactional, and Service[1]. The Gateway secreting physically so only authorized users have access to the system.WAP can be used for this type of applications. WTLS is convenient protocol with WAP to make encryption of users data on gateway that connected with mobile client and content provider . In this project we implemented Elex Bank as a sensitive application, and used the own gateway to secure customers data which allocated on the content provider.

1.2. Problem Statement

Internet in general does not provides end-to-end security, WAP devices communicate with a server through an intermediate WAP gateway. WTLS is only used between the device and the gateway, while SSL/TLS can be used between the gateway and the server on the Internet. This means that the WAP gateway contains, at least for some period of time, unencrypted data and this break the security between two parties.

1.3. Propose Solution

To solve breakage of end-to-end security caused by the gateway, WAP Gateway is to be implemented near contents provider premises.

1.4.Methodology

WML language is used to write the code of Elex Bank and then by using IIS features to help open the page in the browser of laptop, and also in the browser of mobile phone by using wireless connection.

1.5.Thesis Outlines

Chapter Two contains background of WAP and literature review. In chapter Three deeply information of WAP supported by figures, also contains gateway background. In chapter Four introduction about internet security in general and then security on WAP specifically in different concepts. Chapter Five illustrated small introduction about IIS, ASP and the code and at last contains the results. Chapter Six contains conclusion and recommendations.

Chapter Two

Literature Review About Wireless Application Protocol

2.Literature Review About Wireless Application Protocol

2.1.Background

The Wireless Application Protocol (WAP) is an emerging standard for the deployment of data oriented applications in wireless environments. Although some components of the WAP suite have been developed. The protocol stack consists of miniaturized versions of UDP, TCP and HTTP protocols with reduced header sizes and complexity to make the protocols usable in wireless sensor networks.

A general architectural framework to develop and deploy portable applications and services accessible by WAP compliant mobile terminals, extending end-to-end services between terminal and business applications. A micro browser (WML) hosted by the mobile terminal (client side), a WAP gateway allowing the inter working operation between the wireless network and others kinds of data networks (TCP/IP networks) , a layered stack of (WAP) protocols specifically designed for wireless environments [2].

2.2. Related Studies

The author Juul ,Niels Christian and Niels Jørgensen on the section of gateway represented that the WAP gateway is a piece of software.

Typically, it runs on a computer in a building under the control of the mobile service provider, MSP.   the security weakness of WAP discussed means that all data exchanged may be available to people with privileged access to the WAP gateway.

The Wireless Application Protocol (WAP) is a suite of evolving standards for browsing the web with a thin client browser, a mobile phone. The standard describes a full suite, sometimes referred to as a “stack” of protocols, basically in compliance with the ISO-OSI model for network protocols.

Then authors talked about the technical rationale for the WAP gateway ,they found that WAP was designed to work not only with GSM but most other digital wireless telephone networks. Compared to the well known Internet, mobile wireless networks are characterized by: limited communication capacity (bandwidth), higher latencies, higher variation in packet loss (jitter), and variation in long term connectivity or availability (on/off).

On the field of WML , The WML document asks the user to provide a credit card number, using elements of WML that correspond to a so called form in HTML. For security, WAP provides a secure protocol for data transport: WTLS, Wireless Transport Layer Security.

For encryption over the wireless path, WAP uses WTLS which is in essence an adoption for wireless communication of the TLS protocol. The changes to TLS embodied in WTLS do not weaken security. They are also talked about the combination of WTLS and TLS provides secrecy (indeed, also integrity) over both halves of the WAP client and web server connection. The crucial weakness is, of course, that all data transferred between the WAP client and the web server is decrypted at the WAP gateway. To make solution to unencrypted data is Moving the WAP gateway to the web server.[3]

The authors, Singel´ee Dave and Bart Preneel make a simple background for WML and said that just as for the WWW, the user interface to WAP is via a mini browser in the mobile phone. WAP has its own Mark-up Language WML (Wireless Mark-up Language). WML is the WAP equivalent of HTML. WML also includes scripting (WML Script).they also talk about The communication between the mobile phone and the WAP gateway which has to be secured by using WTLS. The TLS protocol cannot be used for this purpose because of the constraints of the mobile phone. A mobile phone has very limited bandwidth, memory, computational power and battery power and cannot perform heavy (cryptographic) computations. For the use of WAP they illustrate architecture which has some security consequences.

They explained the WAP protocol stack, the WTLS protocol and the Wireless Identity .Also they illustrate WAP protocol stack and its layers. The authors specifies basic issues with WTLS and all steps of communications between mobile client and server. Then they specified security problems with WAP and the most important security problems will now be discussed. One of these problems WAP gateway. WAP does not offer end-to-end security.

WAP devices communicate with web servers through an intermediate WAP gateway. WTLS is only used between the device and the gateway, while SSL/TLS can be used between the gateway and the web server on the Internet. so, gateway has unencrypted data at some times. The gateway vendors have to take steps to ensure that the decryption and re-encryption takes place in memory, that keys and unencrypted data are never saved to disk, and that all memory used as part of the encryption and decryption process is cleared before handed back to the operating system .also they make a look about physical security and said that , The weakest link of the system will be the mobile phone itself. It easily gets lost or stolen and it is likely to be used more and more for the storage of sensitive data.

The solution which they made to pervious problems was use trusted and secure gateway instead of using default gateway. the problem with this solution is that it’s not always very easy for user to switch to another gateway. Also upgrade all WAP gateways. in this way the WTLS encrypted data stream travels from the mobile phone to the server without being decrypted. upgrading WAP gateways and WAP servers is much easier than upgrading all WAP devices. These solutions have some disadvantage is that the user has to configure his own system(choose the WAP gateway) or all the WAP gateways and servers have to be upgraded[4].

The author Kaur , Parminder made the primary definition of WAP forum and WAP itself as a worldwide standard for providing Internet communications and advanced services on digital mobile devices, such as handheld phones, pagers, and other wireless devices. He talked about the architectural goals and mentioned them in eight points. Then made architecture overview of WWW after that WAP model.WAP enables a flexible security infrastructure that focuses on providing connection security between a WAP client and server. WAP can provide end-to-end security between protocol endpoints. If a browser and origin server desire end-to-end security, they can communicate directly using the security protocols. Moreover, the WAP specifications include support for application level security, such as signed text. In a security on WAP1.1 said that the main security initiative in WAP 1.1 is the Wireless Transport Layer Security protocol (WTLS). WTLS provides similar functionality to that of the Internet's transport layer security protocol (TLS), the standard for securing Internet browsing and this, is based on Secure Sockets Layer (SSL) Internet Protocol. [5].

The authors Anders Hessel and Paul Pettersson are presented experiences from applying a model based approach to perform testing of a gateway developed by Ericsson. The gateway is used to connect mobile phone clients using the Wireless Application Protocol (WAP) with the Internet. They defined WAP as a global and open standard that specify an architecture for providing access to Internet services to mobile (handheld) devices. The WAP standard specify both a protocol and a format, named Wireless Markup Language (WML) . A WAP gateway converts between the WML content on the HTTP side, and WML/Binary on the mobile side. It also serves as a proxy for translating WAP requests to Internet protocols (HTTP). The WAP side of a gateway typically consists of the following protocol layers. The WAP specification defines two roles in the protocol. The part that starts a transaction is called initiator, and the other part is called responder[6] .

The authors A. K.Muruganandam, B. V.Palanisamy, C. A.Krishnan and D.R.Rajesh talked about existing architecture and problem with WAP. To deploy applications for wireless terminals it is not sufficient to simply guarantee access to data (web or database contents), but it is necessary to take into account the constraints of wireless connections, both in architectures and applications. Wireless terminals are available in different models (handheld, laptop, communicator, smart phone) and architectures, which can cause interoperability problems. They also talked about the basic component of WAP. One of these component micro browser represented in WML, it hosted by the client. a WAP gateway allowing the inter working operation between the wireless network and others kinds of data networks a layered stack of (WAP) protocols specifically designed for wireless environments.WML is a simplified data description language able to face the constraints of wireless environments, its document is a deck composed by a set of cards, a card is a unit of interaction between user and application[7].

The authors Viehland, Dennis and John Hughes talked about a technical introduction to WAP and the WAP architecture is available from the WAP Forums Web site (Hubbard 1999). WAP has been the subject of most articles over the last fifteen years (Goldman 2001; Frederick 2000; Jackson 2000; Schwartz 2000; Shah 2000; Johnson 1999) or demise (Dooley 2000; Lewis 2000; Loken 2000; McGrath 2000; Sims 2000) of the protocol.

The technical barriers are the limitations of the handhelds (Banan 2000), the translation of HTML pages at the WAP gateway (Bannan 2000), lack of security (Sims 2000) and the incompatibility of WAP with other Internet standards (Khare 1999) [8].

Chapter Three

Overview About Wireless Application Protocol (WAP)

3.Wireless Application Protocol (WAP)

3.1. Preface

In 1997, several wireless phone manufactures organized an industry group called the wireless application protocol forum [10]. This group defined the WAP specification, describes technical document series that defines standards for implementing wireless network applications.

In recent years, wireless telecommunications have become a common subject of technical papers. The new trend in technology is to provide users with the ability to have all they could possibly need in a device that fits in their pocket.

Smaller and smaller PDAs (Personal Data Assistants), laptop computers and mobile phones are hitting the market, incorporating brand new features designed to let the users work and access documents in whatever situation they are in. The Internet is considered with particular interest, given the fact that it is widespread and easy to access from almost anywhere in the world.

One of the latest innovations in the field and the one that has shaken the telecommunication world from its roots is WAP.WAP gives ability to access information and services any time, anyhow, anywhere this know as a mobility services and there is another services of a WAP represented in location information services. So, if we are going to allow Internet access from a mobile phone, we first need to take into account these limitations of the client device. The Internet protocols (TCP/IP and HTTP) are far from being suitable for use with mobile phone communications. They introduce far too many overheads, requiring many messages between clients and server just to set up a connection. These overheads call for a high processing power on the client device.

Furthermore, there is a second limitation connected to the internal structure of wireless networks. This is the sustained waiting time, called latency. Basically, the information coming from the Internet and going to the mobile phones has to go through various elements in the mobile network, each one introducing a little delay. Also there is another limitations such as bandwidth , mobile screen size and keyboard.

3.2. WAP definition

The Wireless Application Protocol (WAP) is an emerging standard for the deployment of data oriented applications in wireless environments. It is communication protocol and application environment for the deployment of information resource, advanced telephony services, and internet access from mobile devices. Its protocol stack consists of UDP, TCP, HTTP protocols with reduced header sizes and complexity. WAP forum was created by phone.com, Ericsson, Nokia and Motorola.[9]

3.3. Goals of WAP

1. To Make Communication between content providers and mobile device more efficient and less time.

2. To provide protocol that is able to adapt to any type of mobile network[9].

3.4. WAP Internal Structure

The internal structure of WAP consist of group of protocols and layers, we may make definitions for all let us begin with protocol. A protocol defines the types and structure of messages that two devices have to use when they are communicating with each other. We will look at how the WAP protocol is structured and how the different WAP layers map into internet protocol layers. As shown in figure (3.1).

1.Application Layer

WAE provides application environment intended for the development and execution of the portable applications and services.

2.Session Layer

WSP supplies methods for the organized exchange of content between client/server applications.

3.Transaction Layer

To provide different method for performing transactions, to a varying degree of reliability.

4.Security Layer

WTLS is an optional layer that provides, when present, authentication, privacy and secure connection between applications.

5.Transport Layer

WDP is the bottom layer of the WAP stack, which shelters the upper layer from the bearer services offered by operator.

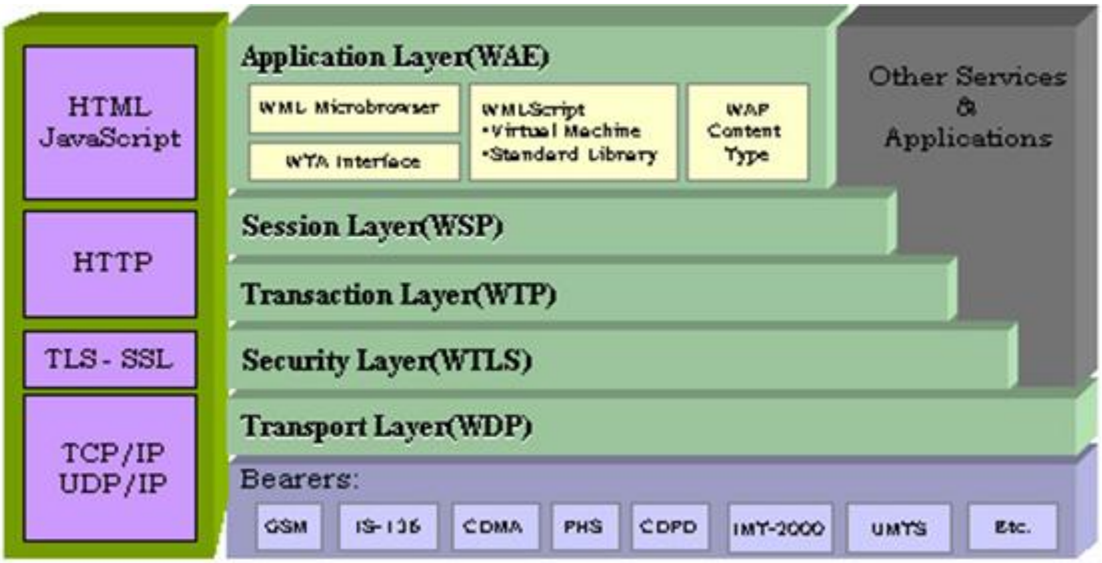


Figure (3.1): WAP Stack[9]

3.5. The Work Method of WAP

The content provider must be delivered WML content to mobile devices over related technology network. However, the delivery of many protocols and technologies takes the same route namely through a proxy server. This proxy server manages the communication between the wireless client and the Internet server(s), acting as a gateway to the wired Internet. It caches content and in some cases even translates raw HTML into WML. Many mobile devices have a built in wireless browser.

Although several different browsers are in use today among the various wireless providers, most browsers support WML. WML is becoming the most widely used mobile markup language. the figure (3.2) shows how WAP client find his URL by using WAP gateway.

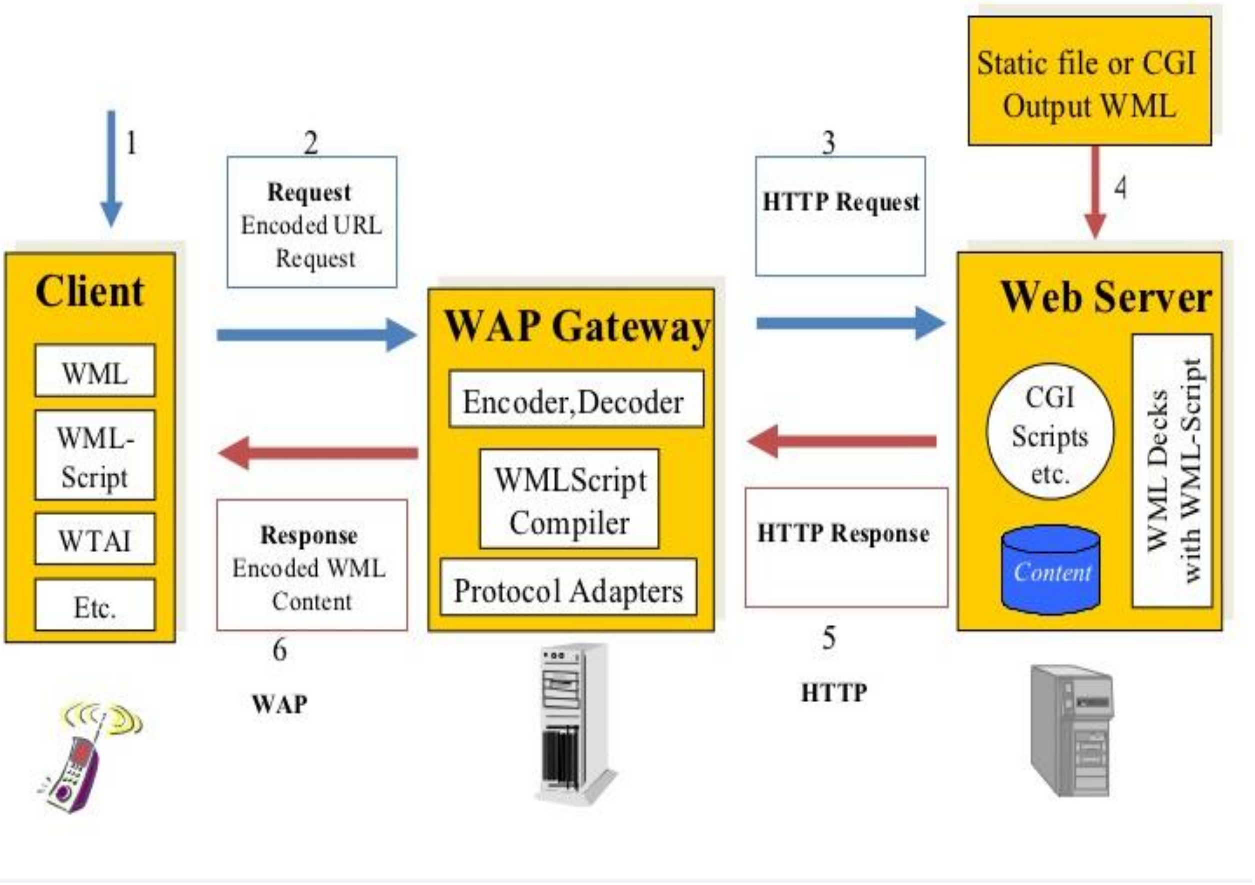


Figure (3.2): finding URL from a server[3].

3.6.The Technical Terms of WAP

3.6.1 WAP Device

This term indicates the physical device that you use to Access WAP applications and content. It doesn't necessarily have to be a mobile phone – it might be a PDA or a handheld computer. More generally, it's every WAP compliant device.

3.6.2 WAP Client

In a network environment, a client is typically the logical entity that is operated by the user and communicates with the 'server entity'. In the WAP world, the client is the entity that receives content from the Internet via a WAP Gateway. This is usually (but not necessarily) the WAP browser. Commonly, 'WAP client' and 'WAP browser' are often used interchangeably.

3.6.3 WAP Browser

This is software running on the WAP device that interprets the WAP content arriving from the Internet and decides how to display it on the screen of the WAP device. WAP browsers are available for all WAP devices, and are frequently referred to as micro browsers. There are also emulators available for some browsers, which run on PCs.

3.6.4 WAP Gateway

This is the element that sits (logically) between the WAP device and the origin server. It acts as an 'interpreter' between the two, enabling them to communicate. It usually resides within the operator network, but you can also install your own gateway, as we will see later. Unless otherwise stated, when a gateway is discussed, we mean a gateway residing in the operator network, since this is the more common situation that one encounters.

3.6.5 Content/Origin/Application Server

These three names are used interchangeably. They denote the element that hosts the Internet content that is sent to clients when they make a request for it. A web server is an origin server, providing HTML content (but also WAP content if properly configured)[10].

3.7. Difference Between WEP proxy and WAP gateway

Proxy is an intermediary element, acting both as a client and as a server in the network. It is located between clients and origin servers; the clients send requests to it and it retrieves and caches the information needed by contacting the origin servers. shown in figure(3.3).

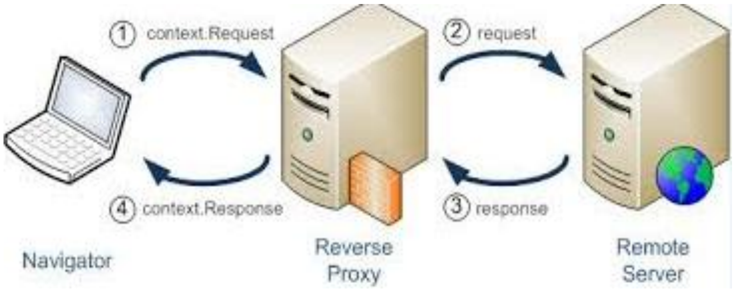


Figure (3.3):WEP proxy.[5]

Gateway connect between two different devices in different networks, but the proxy connect between devices in the same network. Shown in figure(3.4).

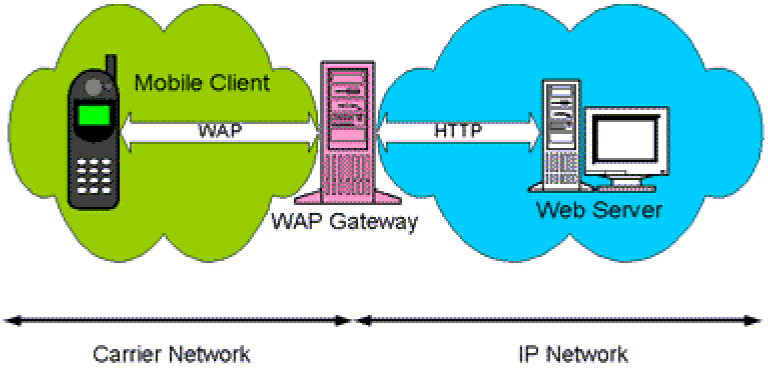


Figure (3.4): WAP gateway.[6]

3.8. Functionality of WAP Gateway

The gateway part of WAP proxy takes care of translating all the requests that are sent and received by the client using WSP to the protocol that the origin server is using (for example HTTP),it's has many functionalities represented in:

3.8.1 Implementation of WAP Protocol Stack Layer

This is the most obvious function of a WAP Gateway and it contributes to most of the functionality of a WAP Gateway. Depending on whether type of the service is connection–oriented or connectionless. Secure or not secure, the following stack layers need to implemented.

1. Non secure connection – oriented: WSP↔WTP↔ WDP

2.Secure connection – oriented: WSP↔WTP↔WTLS ↔ WDP

3.Secure connectionless: WSP ↔ WTLS ↔WDP

4.Non secure connectionless: WSP↔WDP

3.8.2 Access Control

This involves restricting specific content (like Subscription services or company intranet WAP services) Recognition of the device. Amore fine grained access control can be achieved by using user authentication.

3.8.3 Protocol Conversion(WSP ↔ HTTP)

The Gateway part of the WAP takes of translating all the requests that are sent and received by the client using WSP to the protocol that the origin server is using (HTTP for example). The Content provider sends its content using HTTP to the Gateway. It then forwards all the content received to the WAP devices, using the WAP protocol.

3.8.4 HTML to WML Conversion

Note that this optional feature. This conversion can never be perfect, and it can never generate that after conversion an HTML page will rendered properly on a wireless device.

3.8.5 Encoding of WML Conversion

The structure and content of the WML documents are encoded into standard binary that have been precisely defined into specification. Encoded WML can be directly used to vender the content on the device because a one to mapping exists between tags, attributes.

3.8.6 WML Script Compilation

WMLScript is compiled in a manner similar to compilation of programs in other programming languages and therefore all the phase of a compiler. The generated code is similar to Java byte code. It consists of assembly program instructions for a non-existent architecture.

The error detection during compilation need not keep track of the types of error that occur. Only the fact that there is an error is reported to the wireless device that made the request. The user of the device is not usually interested in understanding the error; they only want to know when one has occurred.

3.8.7 Security

This involves providing WTLS, between the Gateway and the HTTP origin server. Security illustrated in more details in chapter 4.

3.8.8Provide caching for frequently accessed contend

This functionality is very similar to that of proxy server, which found in various organizations, that cache Internet content regularly accessed by members of the organization.

3.9. Positioning of WAP Gateway in The Network

There are three possible location in which gateway can be suited, each one advantage and disadvantage.

3.9.1. A Gateway Provided by The Network Operator:

Here the gateway is part of the infrastructure, necessary for operator provided WAP services, one of the advantages is that the mobile device only needs a single gateway setting to access any internet content. Disadvantage illustrated in even if secure HTTP and SSL are used between WAP gateway and the application server, the request content will be an unencrypted form in the main memory, this could cause security problem. as is shown in figure (3.5).

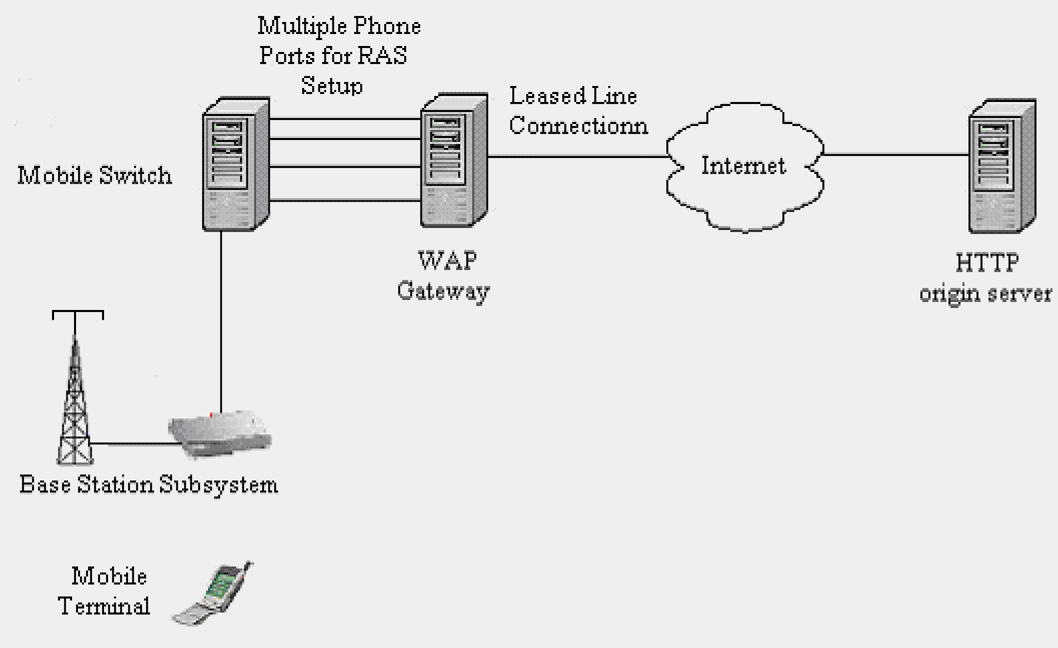


Figure (3.5): A WAP Gateway provided by the network operator[9].

3.9.2. A Gateway Provided by The Content Provider :

A content provider might decided to have its own gateway at its web farm, one advantage of this solution is access to the content on the origin servers through a WAP gateway other than the content providers own could be disabled for the sake of security, and disadvantage if every server has its own gateway, it will be impossible for the mobile user to have all necessary gateway configuration setup on their device. as is shown in figure (3.6).

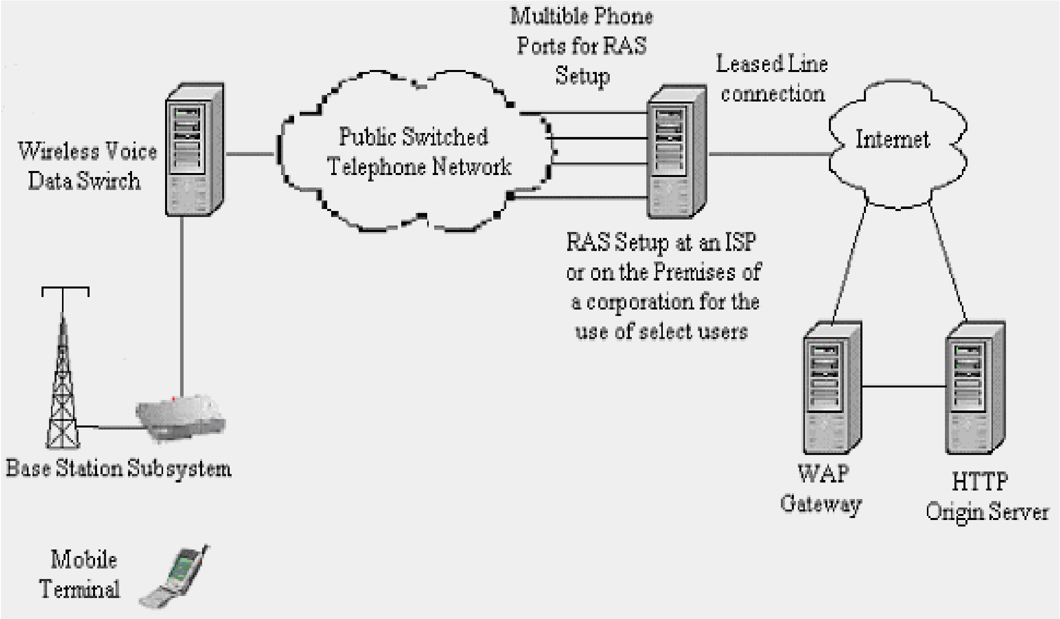


Figure (3.6): A WAP Gateway provided by the content provider[9]

3.9.3. A WAP Gateway Provided by The ISP:

The architecture is similar to previous case except for the position of gateway; the gateway will be closer to the RAS server and will be one of the nodes on the ISP's network.

3.10. Security

Mobile security standard such as TLS and WTLS are secure enough to allow most peoples and organizations to perform business transactions securely over the internet and wireless communications channel.

This does not mean that these technologies are impervious just that breaking the security is difficult enough to ensure that it's beyond the capabilities of most would be hackers, and costly enough to outweigh the benefit that could be gained.

Chapter Four

Wireless Application Protocol Security

4.Wireless Application Protocol Security

4.1. Overview

Security in general has five basics represented in:

4.1.1 Authentication

Is the process of making sure that another party is actual who they claim to be ,the purpose of authentication protocol is to try to catch an activity called spoofing, this is occurs when one party tries to hide their true identity and assume another .

4.1.2 Confidently

Is one of the most important aspects of security, to ensure the confidently of information it is usually encrypted.

4.1.3 Integrity

Message needs to be sure that was not change during transmission. This is what integrity is all about. In the world of computing message integrity is usually assured by driving the hash value for the message and transmitting that value either along with the message.

4.1.4 Authorization

Is the process of determining whether a particular party has the right to perform a particular action with respect to particular object, in a particular situation all of this (particulars) need to be taken into account in order to make and authorization decision.

4.1.5 E. Non-Repudiation

Non repudiation means implementing some sort of mechanism so that it is impossible for the parties to transaction to deny either that the transaction took place, or that they were party to it.

4.2. Security on The Internet

The client has to be make connection with the internet via an ISP; to begin with we can examine the connection between the client device and the ISP. the client will use a modem to connect the ISP and PPP can be assume to be the protocol use over this connection the encryption control protocol can also be used to negotiate for encryption to be applied to all packets exchange between the two peers.

For authentication we can use user ID and password or authentication protocol . Once the authentication is completed successfully the client device registered on the ISPs network and the RAS server will then act as a proxy for the client device transmitting IP packet received from the client and collecting packets addressed to the client and forwarding them over the PPP connection.

The ISP connected to internet through router or some sort, to protect ISP network from internet traffic use firewall. There are number of ways in which security can added in to the process, the most common in which is the TLS. Formerly known as SSL which is transport layer protocol when client request a secure session with server, the secure session establish the connection between client and server. TLS provides an end to end secure communication channel.

4.3.WAP Security model

Security in WAP has been implemented in such away as to provide maximum benefit with the least amount of pain, WAP is implemented most of security feature on WTLS, it based on TLS.

In this is model the connection is made via phone but handled by the network operator , rather than ISP the mobile device should use PPP.

The RAS server will perform authentication, instead of being routed over the internet to a web server the data is routed to the WAP gateway. The WAP gateway is responsible for the translation of WML and WML script. Also acts as the proxy server for the phone communicated with the web server on the phones using normal HTTP protocols to do so. The web server is not aware of the fact that is talking to the gateway it sees that the gateway as simply another client device.

Typically the web server will be the network operator's own web server and so the packets possibly will never leave the network operator's own network. However, you can usually access services that are provided by other organizations, should you want to, in which case the WAP gateway will simply send its HTTP packets through the firewall to a remote web server on another organization's network. Figure(4.1) shows the WAP security model.

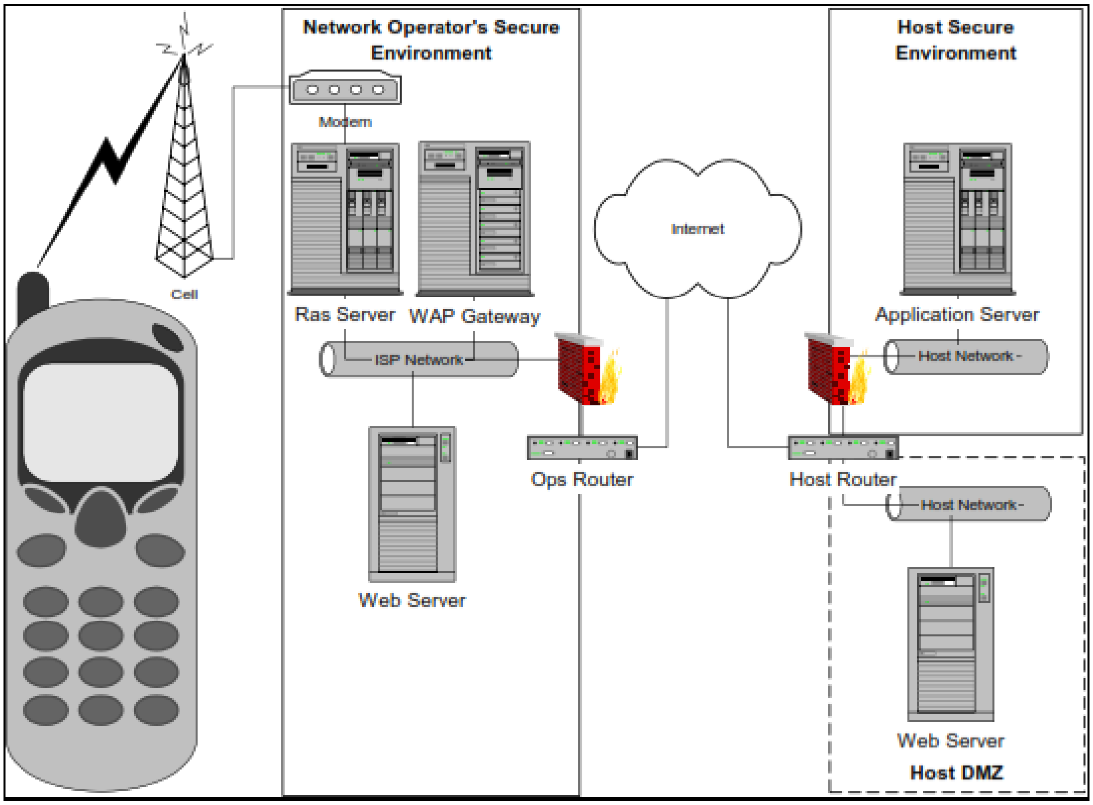


Figure (4.1): WAP security model[9]

If a WAP gateway acts as a proxy and use the HTTP then it used TLS to secure all communications between gateway and web server, but cannot be used to secure communications between mobile device and gateway, WTLS.

4.4.Overview of WTLS

WTLS was specifically designed to conduct secure transaction in the mobile device, without requiring desktop level of processing power and memory. WTLS process security algorithm faster by minimizing protocol overhead**,** and enable more data compression than the traditional SSL approach.

WTLS provide key refresh mechanism to update keys in a secure connection without handshaking. In the key refresh a new key block is generated using the master secret key, the message sequence and other parameters.

The wireless transport layer security implements many features to ensure secure data transmissions and to protect the users, the network and service operators, and the functionality of the upper layers of the WAP stack. It provides safe data transmission that could support services requiring a high level of security such as mobile e-commerce.

WTLS sits above transport layer in the OSI protocol stack, it can operate over WDP and UDP and also differentiate between a session and a connection [2]. WTLS specification allows for authentication for both client (mobile phone) and server, and provides data privacy, data integrity between to communication parties.

To ease implementation , however, three classes of WTLS implementation are specified ,class one only require support of public key exchange, encryption and MACs, with client and server certificates and shared secret handshake being optional .For class two implementations support for server certificates is mandatory, and for class three support both client and server is mandatory.

The client begins the process of setting up a secure session by sending a message to the server to request the negotiation of secure session settings (this phase called handshake phase). During this handshake phase, security parameters used to protect the session are negotiated.

These include the encryption protocols, signature algorithms, public keys. Ones a session has been established, all the communications between the client and the server is encrypted.   as is shown in figure (4.2).

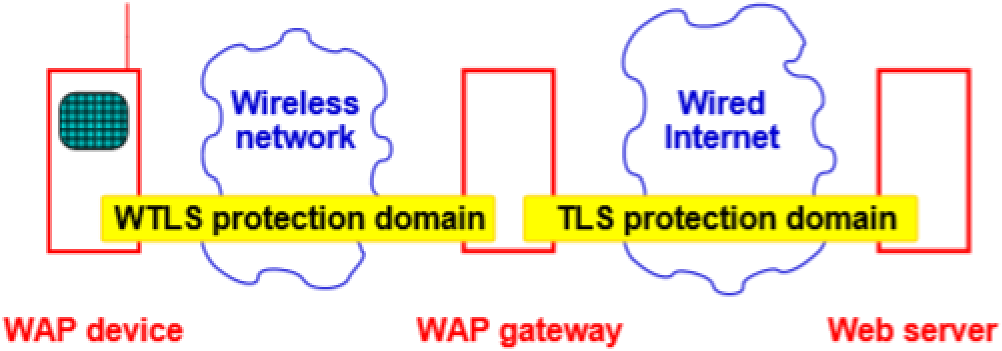


Figure (4.2): security zone using standard security services (WTLS and TLS).[3]

If the public key exchange mechanism that was agreed is not an anonymous, then the server must send the client certificate to identify itself. The certificate sent must obviously match key exchange algorithm agreed on.

4.5.Basics of WTLS Architecture

4.5.1. The Handshake Protocol:

All the security related parameters are agreed during the handshake these parameters include attribute such as protocol version, cryptographic algorithm and information on the use of authentication and public key techniques to generate a key.

4.5.2. The Alert Protocol:

The WTLS provides a content type of alert message; alert messages convey the severity of the message and a description of the alert. They are three descriptions of the alert messages: fatal, critical and warning.

4.5. 3. The Change Cipher Spec Protocol:

Change cipher spec is sent either by client or the server. By means of this message, both parties decide that they start using the negotiated session parameters. When the change cipher spec message arrives, the sender of the message sets the current write state to the pending state, and the receiver also set the current read state to the pending state. The change cipher spec message is send during the handshake phase after the security parameters have been agreed on. As show in figure(4.3)

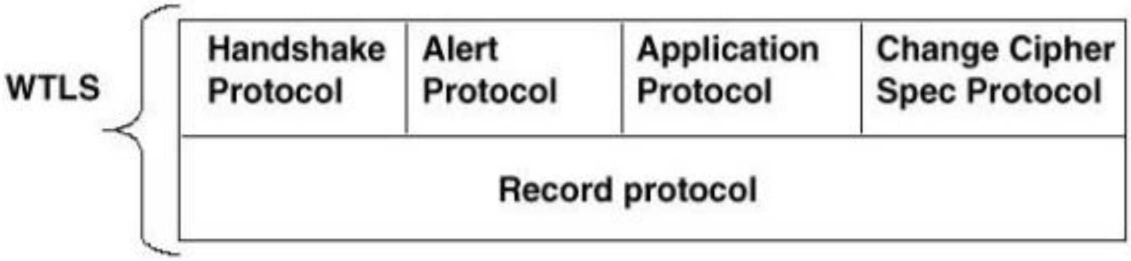


Figure (4.3): WTLS internal architecture.[8]

4.6. Gateway Security

There is a configuration that is allowing you to host your own gateway, and your own ISP. This is a secure model because WTLS is used effectively as a tunneling protocol to tunnel between the phone and the WAP gateway.

The WAP gateway and the web server are on different networks when the gateway is hosted by the network operator, the web server can be on a different network segment, or even in a different network accessed via the internet, because TLS is used to secure the connection between the gateway and the web server, so it is as secure as any other connection between a client server over the internet.

Because WAP does not provide end to end security it must implement trusted and secure gateway instead of using default WAP gateway. This important in sensitive services like electronic banking applications.

Chapter Five

Implementation of Elex Bank and Result

5. Implementation Of Elex Bank And Result

5.1.Internet Information Service(IIS)

Internet information service is a web server software package designed for windows server. It used for hosting websites and other content on the web. It created by Microsoft for use with windows NT family. it supports HTTP,HTTPS,FTP,FTPS. The IIS manager tool allows web administrators to modify website option, such as default pages , error pages, security setting and performance optimizations. It can serve both standard HTML web pages such as ASP,NET applications.

When a visitor accesses a page on a static website, IIS simply sends the HTML and associated images to the user's browser. When a page on a dynamic website accessed, IIS runs any applications and processes any scripts contained in the page, then send the resulting data to the user's browser. [11]

5.2. Overview of Active Server Pages (ASP)

Active Server Page is Microsoft alternative lets a web server usually (IIS) interact with databases and other systems , including email , file system and others . when IIS receives a request for a page with a . Asp extension , any server – side code that is embedded in the WML is executed and the resultant file is forward to the browser.

The Power of ASP Lies in

I. It makes building dynamic application easy .
II. It is simple.

III. It lets developers make use of component to and build complex web based services .[1]

5.2.1. Creating Dynamic Pages

HTML pages can be turned into active server pages simply by changing their file extensions to .ASP in a addition to changing the extension of WML files to .ASP they is one more thing to do . By default, IIS will forward the contents of an ASP to file to the browser using the MIME type for WML (text/vnd.wap.wml).

5.2.2 .Object Model

I. Request Object:

The request object encapsulates all the information that a user agent sends to the web server .the encapsulation statement is illustrated in box (1).

```
Request.Querystring("xxx")
```

Box(1)

II. Response Object:

ASP application builds the response message it can be regarded as a server response , to tell the server to use the right MIME type .the statement which it used to choose the right mime type illustrated in box (2).

```
Response.ContentType = "text/vnd.wap.wml"
```

Box(2)

III. Cookies:

Many gateways can store cookies on behalf devises .the main reason for cookies not to exist on a WAP device ,is that they are costly to implement. Cookies , allow as to create personalize application with ease. The information about the user can be stored in it .it can speed access to application. the information is held in a database that is linked with the user's name and password or PIN number.

III. connecting to a database:

First create a connection in the ASP page itself ,using the server.createobject method: the connection is made by the statements shown in box (3).

```
Dim conn

Set conn =Server.CreateObject("ADODB.Connect)
```

Box(3)

At the end each ASP page ,should close all the connections you have opened: this illustrated in box (4).

```
conn.close

Set conn = Nothing
```

Box(4)

5.3.Overview of Wireless Markup Language (WML)

Before start with WML let us take some information about extensible Markup Language (XML) , it is a technology for creating structure document that can be exchange between system . the DTD describes the tags that may be inside a document conforming to the DTD, what tags may be nested within each tag and other information. to examine this DTD it can be found at

http://www.wapforum.org/DTD/wml_1.1.xml.

5.3.1. Includes Major Functional Area

I. text presentation and layout , WML includes text and image support including a variety of formatting and layout command , on the WML all text to be displayed on the main part of the screen must be inside paragraph element .

II. deck/card all information in WML organized on to a collection of card and decks . card specify one or more units of user interaction card is grouped together into decks , WML dicks is similar to an HTML pages identified by URL , every WML deck start with the same XML header

5.4. XML Header

```
<?xml   version ="1.0"?>

<!DOCTYPE wml PUBLIC "-//WAPFOURM//DTD WML  1 . 1//EN"

"http ://www.wapfourm.org/DTD/wml_1 . 1 . xml">
```

The first line of this simply states in the previous box define an XML documents and the version number used , the next line select the document type and give the URL of the document type definition , WML browsers must implemented the URL schemes specified in [WEP] .the WML code of a deck is enclosed in the <WML> </WML> tag pair . this is the body of the document , and the card is defined within it using the<card></card> tag pair . tag pair encounter with attributes in WML . the id attribute gives a unique id for the card within the deck.

5.5. Understanding Decks

WML pages are structured within decks, allowing several pages (cards) to be defined in each WML file. This deck allows multiple pages to be delivered to the mobile client at the same time, minimizing the loading time between related pages, but he WAP device displays only one card at a time. However, the limited memory on most devices constrains the deck size. Visualizing a physical deck of cards structure can help in understanding the principles of WML. These cards together from a deck and are delivered to the mobile device in one file. Now suppose that each links to the next and that each card also has a back link to take the user to the previous card .Instead, used of tag tell the browser to remove the current page and display the pervious page in the history list.

5.6 An ASP Application in Practice

To make our application we need to use all the previous components starting from setting the features of IIS where we included the ASP which makes connection to the database. WML is considered to be suitable language with WAP applications because the limitations of mobile phones. so we here use it to writes the fields of bank such as services, currency value, etc…

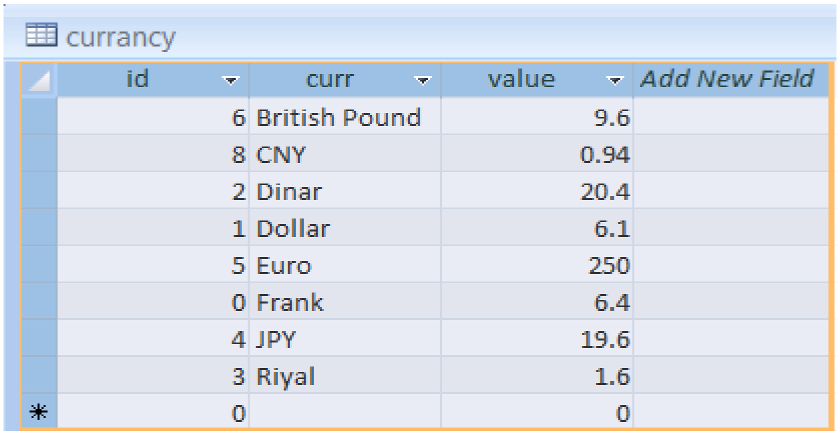
In security aspect we set one specific ID to a specific user in the authentication file, and this ID is found on the database, then when the user makes log in, it must be authorized firstly by the gateway and then give the possibility of accessing to the server database. The server also first make authentication form who the user is, if the ID is not identical with other one stored on database, the user must be denied from access, other case allowed to them for access.

5.7. The Database

In a serious WAP service we can use MS-Access for our application. before we delve to the code, first take a look at database. Its make of three tables: currency, account and customers.

The table called (currency) contains a full range of foreign currencies users can convert. table (5.1) include the currency database .

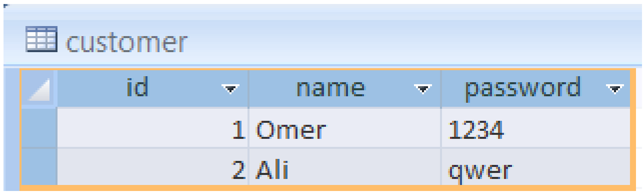
Table(5.1): shows the currency



	id	curr	value	Add New Field
	6	British Pound	9.6	
	8	CNY	0.94	
	2	Dinar	20.4	
	1	Dollar	6.1	
	5	Euro	250	
	0	Frank	6.4	
	4	JPY	19.6	
	3	Riyal	1.6	
*	0		0	

User access information is stored in separate table called(customer) as in table(5.2).

Table (5.2) :shows the customers

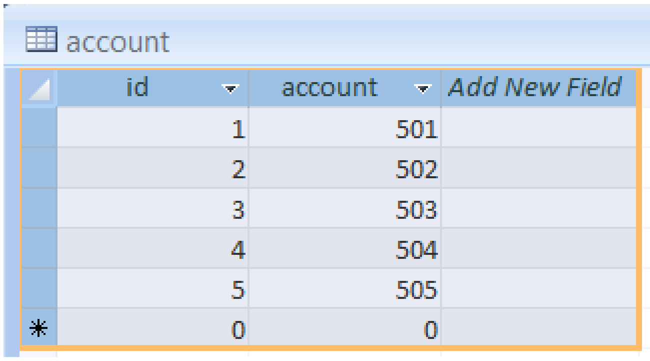


customer

	id	name	password
	1	Omer	1234
	2	Ali	qwer

user’s accounts information stored in table called (account) .

Table(5.3): shows the accounts.



account

	id	account	Add New Field
	1	501	
	2	502	
	3	503	
	4	504	
	5	505	
*	0	0	

We then have to run the configure script before we can build the binaries. You might want to pass some additional options so that the bin a installation. it’s done in home directory rather than the default /user/local directory for which. You might need root or administrative access .

5.8. Results

Figure (5.1) illustrating the decks that compose the bank application. Any screen represents a card, and the arrows between each pair of screen represent the possible navigation path the user can take from one card to another. The block represents a deck.

When a deck sent containing multiple cards to a mobile phone, all the cards except one are being kept hidden by the browser. While this is useful for improving the system responsiveness, an obvious implication is that such hidden cards cannot contain information produced by the server as a response to the input user provide through a card in the same deck.

Let us start by looking at the first deck (main.asp) in the application. The deck contains four cards.

The first card (logo) is a splash screen that contains the name and the logo of the bank. The second card (services) , this contains the time and links to the rest of the system. The third card (currency) is the popular currency used and a link to other currency card. The last card (other) allows user from chose foreign currencies from a select menu.

The second deck (currency.asp) is the response to the foreign currency sends from the previous deck (main.asp) contains only one card (currency), which we need to extract new information from the server side Database.

The third deck (authentication.asp) received the ID number of the user who access the ElexBank site through the Gateway and prompt the user to enter his password until its authenticate, then personalization hallo appear, otherwise user try to enter password again.

The last deck (customer.asp) can be reachable if and only if matched user authenticated with the correct password, and display its present account, and a link to the HOME.

Chapter Six

Conclusion And Recommendations

6.Conclusion and Recommendations

6.1.Conclusion

WAP enables mobile phone to browse on the internet , The security architecture of WAP consists of three parts. The mobile phone ,the WAP gateway and the internet. We implemented WAP in our sensitive application (ElexBank) and this make secure sensitive information for bank customer by authorizing them before accessing to their account by password.

Also we make complete configuration of own gateway to guarantee accessing for specific users, it specifies them by storing their IPs and allowing them to access and others don't storing them denied from accessing. This achieves high level of security which will be important here.

The gateway kwon that the client is send request and this shown in one of it's options(Run as a service) then it forward this request to the server, the problem which we met is that the server don't return back with response to the client.

6.2. Recommendations

- The data which passes from the gateway to the server is not specified and the server does not understand this request so it rejects it and send error message to the client tell him that the request is a bad request. So, we recommend with using packet sniffer with the gateway .and this also defines the incompatible format between the gateway and the server.

- Make the system more wider.

References:

[1] Kwon, Eun-Kyeong, Yong-Gu Cho, and Ki-Joon Chae. "Integrated transport layer security: end-to-end security model between WTLS and TLS." Information Networking, 2001. Proceedings. 15th International Conference on. IEEE, 2001.

[2] Muruganandam, K., and CH Kalyan Chandra. "Implementation of WAP gateway technologies through wireless communication." Computer Science".

[3] Juul, Niels Christian, and Niels Jørgensen. "WAP may Stumble over the Gateway." network 11 (2001): 11.

[4] Singelée, Dave, and Bart Preneel. "The wireless application protocol (WAP)." Cosic Internet Report (2003).

[5] Kaur, Parminder. "Security of Wireless Application Protocol." Proceedings of 'I-Society 2012'atGKU .

[6] Hessel, Anders, and Paul Pettersson. "Model-based testing of a wap gateway: an industrial case-study." Formal Methods: Applications and Technology. Springer Berlin Heidelberg, 2007. 116-131.

[7] Muruganandam, K., and CH Kalyan Chandra. "Implementation of WAP gateway technologies through wireless communication." Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on. IEEE, 2009.

[8] Viehland, Dennis, and John Hughes. "The future of the wireless application protocol." AMCIS 2002 Proceedings (2002): 260.

[9] Professional WAP (Programmer to programmer) Paperback – July 27, 2000, by Charles Arehart (Author),Nirmal Chidambaram (Author), Shashikiran Guruprasad (Author), &10 more .

[10] Kumar, Vijay, Srinivas Parimi, and Dharma P. Agrawal. "WAP: present and future." Pervasive Computing, IEEE 2.1 (2003): 79-83.

[11] https://en.wikipedia.org/wiki/Internet_Information_Services. web site last visited 5/9/2015(7:30pm).

[12] Chien, Eric. "Potential Threats to WAP Enabled Devices." and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on. IEEE, 2009.

[13] Chikomo, Kelvin, et al. "Security of mobile banking." University of Cape Town, South Africa, Tech. Rep., Nov 1 (2006).

[14] Viehland, Dennis, and John Hughes. "The future of the wireless application protocol." AMCIS 2002 Proceedings (2002): 260.

Appendix A : The Code

We'll now turn to the code for our application. All the code is provided here, and also, with the CD shipped with this research.

A1.Conn.asp

```
<!--#include file ="conn.asp"-->

<%

Option explicit

Dim conn ‘connection to access database ‘

Set conn=server.creat object("ADODB .connection")

DSN-less connection to access

Conn.open=Microsoft.jet.OLEDB.4.0;Data
Souece="&-

Server.Mappath("elexbank.mdb")

<%
```

A2. Unconn.asp

```
<%

Conn.close

Set conn = Nothing

%>
```

A3. Main.asp

```
<!--#include file=”conn.asp”- - >

<%

‘send the right MIME type

Response.contentType= “text/vnd.wap.wml”

Dim SQLquery, uniqueid1,uniqueid2,
currvalue1,currvalue2, currname1,currname2

   Dim rsUser



  uniqueid1 = 1

  uniqueid2 = 2



  SQLquery = "SELECT * FROM currancy WHERE
id = " & uniqueid1

   Set rsUser = conn.Execute(SQLquery)

      currvalue1 = rsUser("value")

      currname1 = rsuser("curr")



  SQLquery = "SELECT * FROM currancy WHERE
id = " & uniqueid2

   Set rsUser = conn.Execute(SQLquery)

      currvalue2 = rsUser("value")

      currname2 = rsuser("curr")
```

```
<?xml version="1.0"?>

<!DOCTYPE    wml   PUBLIC    /"WAPFORUM"//DTD
wml    1.1//EN "

"http ://www.wapforum .org/DTD/wml_1.1.xml">

<wml>

<card id="logo"title="ElexBank"ontimer="#index">

<timer value="40"/>

<do type="prev"lable="skip">

<go href="#index"/>

</do>

<p>

Welcome to <br/>

<img src="elex.wbmp"alt="The Electronic Bank"/>

</p>

</card>

</card>

<card id="index"title="services">

<do type ="prev"lable="prev">

<prev/>

</do>

<p>

Times is now<br/><%=NOW()%>

<a href ="#currancy">

Currency value

</a><br/>
```

```
<a href ="authentication.asp">

Customer credit

<card id="currency" title="Currency Value">

</a><br/>

</p>

</card>

<card id="currency"title="Currency Value">

<do type ="prev"label="prev">

<prev/>

</do>

<p>

<do type= "accept" label="skip">

<go href  " #index"  />

</do>

Against Sudanese Bound <br/>

<%=currname1%>=<%currvalue1%> sd<br/>

<%=currname2%>=<%=currvalue2%> sd

<a href= "#other" >
```

```
</p>

</card>

<card id= "other" title="other currency" >

<do type ="accept" label="  skip" >

<go href = "#index" />

</do>

<p>

<select iname=" R" title= "currancy">

<option>Dollar</option>

<option>British Pound</option>

<option>Frank</option>

<option>JPY</option>

<option>CNY</option>

<option>Euro</option>

<option>Riyal</option>

<option>Dinar</option>

</select>

<br/>

<anchor>convert..

<go href= "currancy" value=" $(R)" />

</go>

</anchor>

</p>

</card>
```

```
<go href= "currancy" value=" $(R)" />

</go>

</anchor>

</p>

</card>

</wml>

<!--#include file="unconn.asp" -->
```

A4.Currency.asp

```
<!--#include file="conn.asp" -- >

<%

‘send the right MIME type

Response.contentType= " text/vnd.wap.wml"

Dim currency

Currency= Request.QureyString( "currancy")

Dim SQLquery, curvalue, currname

Dim reUser

SQLquery="SELECT*FROM currency  WHERE id
= "  &currency

Set reUser =connExecute(SQLquery)

Currvalue = rsUser("value" )

Currname = rsUser("curr " )
```

```
rsUSer .Close

Set rsUser = Nothing

%>

<?xml version="1.0" ?>

<!DOCTYPE wml PUBLIC"    -//WAPFORUM//DTD
WML     1.1//EN    "
http://www.wapfourm.org/DTD/wml_1.1.xml >

<wml>

<card id = "  currancy"  title = "currency Value" >

<do type = " prev"  label = "prev" >

<prev/>

</do>

<p>

<do type="accept"  label="skip"  >

< go href =   "#index"/>

</do>

<br/> against Sudanese Bound <br/> <br/>

<%=curname%>=<%=curvalue%> sd

</p>

</card>

</wml>

<!--#include file= "unconn.asp"-->
```

A5. Authentication.asp

```
<!--#include file ="conn.asp"- - >
<%
'send the right MIME type
Response.ContentType="text/vnd.wap.wml'
Dim  init
Init=""
Init =Reguest  QueryString("Passwd")
Dim  SQLquery, uniqueid, username, password, temp
temp=False
Dim rsUser
'uniqueid  = Request.Cookies("User-Identity-
Forward-msisdn")
'for testing when not going through the gateway,use
this:
Uniqueid=1
SQLquery= "SELECT*FROM customer WHERE id
= "& uniqueid
Set rsUser= conn Execute (SQL guery)
Username=rsUser("name")
If init = password then
Temp = True
End  If
rsUSer Close
set  rsUser =  Nothing
```

```
%>
<?xml version="1.0"?>
<wml>
<card id = "login" title = "login">
<p>
Hello<% = username%> <br/>
Enter your password: <input type="password"
name="passwd" value = "" maxlength ="8"/>
<%if temp then%>
<a href="customer.asp">
Verify Go…
</a><br/>
<%Else%>
<anchor>login..
<go href="authentication.asp">
<postfield name="passwd" value="$(passwd)"/>
</go>
</anchor>  <br/>
<%End if %>
</p>
</card>
</wml>
<!--#include file="unconn.asp"-->
```

A6. Customer.asp

```
<!--#include file="conn.asp"-- >

<%

'send the right MIME type

Response.contentType= "text/vnd.wap.wml"

Dim SQLquery, uniqueid, account

Dim rsUser

'uniqueid = Request.Cookies("user-Identity-forward-msisdn")

'for testing when not going through the gateway , use this:

Uniqueid = 12917772

SQLquery = "SELECT*FROM account WHERE id = "& uniqueid

Set rsUser=conn.Execute(SQLquery)

Account = rsuser("account")

rsUser.close

Set rsUser = Nothing

%>

<?xml  version="1.0"?>

<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD wml 1.1//EN"
```

```
<wml>

<card id ="currency"  title="currency value">

<do type="prev" label="prev">

<prev/>

</do>

<p>

Your Account Now 1s:<br/>

<%=account%>

<a href="main.asp">

HOME..

</a>

</p>

</card>

</wml>

<!--#include file="unconn.asp"-- >
```