A SECURE WAP ENVIRONMENT FOR WIRELESS NETWORKS DEVELOPED WITH PHP & HTML

C. Polychronis, N. Sklavos, V.D. Triantafillou

I Telecom. Systems & Networks Dept., Techn. Educ. Inst. of Mesolonghi, Greece
II Electrical & Computer Engin. Dept, University of Patras, Greece

Abstract:
In our days, the rapidly growth of both tele-communications and networks has bring the wireless technology to the pole position in the world of unwired networks. Wireless Application Protocol is one of the most promising technologies in this area for the next decades. This work presents a secure WAP environment, offered through internet and mobile phones. The proposed system is built with PHP and HTML. It supports an efficient announcement mechanism, for users that needs news and informations, through their mobile and handheld devices.

I INTRODUCTION
Wireless Application Protocol is a latest developed concept. It is specified by an industry consortium, the WAP Forum [1]. This forum was founded in December 1997, by Ericsson, Motorola, Nokia, and Unwired Planet. WAP primary goal is to bring internet content and advanced data services to hand-held devices and other wireless terminals. At the same time the main attempt of the WAP Forum is to create a global wireless protocol specification that could be applied across all wireless existing or new technologies. A great number of applications and services are attended to be enabled in a wide range of wireless bearer networks and unwired devices. The WAP specifications have been developed in order the above described goals to be accomplished according to the specified principles of the WAP protocol [2].

Of course the types of both wireless devices and unwired communication networks set the limitations in the range and the kind of the provided services. Wireless networks have fundamental restrictions in the available spectrum, power consumption and mobility [3]. They also have less bandwidth and more latency compared with the wired world. The connection stability and the predictable availability are less, too. Furthermore, possible improvements in the bandwidth rate in the wireless communications have power consumption penalty in the limited battery life of the handheld devices. The low power dissipation of course is not the only limitation that the mobile phones tend to have [3-4].

In contractor with the personal computers, mobile phones have less powerful CPUs and less available memory of any kind. The small size of screens in addition with the different way of data input, voice input and smaller keypad, request a different user interface than the common used in personal computers [4-5].

Couple to the technology penetration to our everyday life, is the requirement for permanent and daily briefing as easily and fast as is this possible. The information is the vital component of technology and telecommunications. Man is served by the technology and requires always more information. One of the most exigent needs of person is the information. New systems are created daily and their aims are to serve the citizens in their daily needs. We try to provide information anywhere, anytime.

This work deals with a software development of WAP protocol. More analytically an announcement system is proposed for WAP subscribers. The users have access to this system through their mobile and handheld devices. It is efficient for a WAP subscriber can post, read and edit an announcement from this systems, with the supported services of the proposed system. The proposed systems has been developed by using PHP and HTML software description packages. It offers lightweight user interface, avoiding the allocation of the CPU resources. This is achieved with exploiting the advantages of PHP and HTLP development, compared with a possible conventional other system based on heavy software packages such as Oracle.

This paper is organized as follows: In Section II an overview of wireless networks and WAP protocol is presented. Section III is dedicated to the proposed system with detailed presentation and analysis. In the next section examples of the PHP used codes are presented. Section V refers to the privacy specifications of the Wireless transport Layer Security of WAP. Finally conclusions & outlook are discussed in the last part of this work.

II AN OVERVIEW: WIRELESS NETWORKS & WAP
WAP primary goal is to bring internet content and advanced data services to hand-held devices and other wireless terminals. At the same time the main attempt of WAP is to create a global wireless protocol, that could be applied across all wireless existing or new technologies. A great number of applications and services, are attended to be enabled in a wide range of wireless bearer networks and unwired devices. The WAP specifications have been developed in order the above described goals to be accomplished according to the specified principles of the WAP protocol [1].
Wireless networks have fundamental restrictions in the available spectrum, power consumption and mobility. They also have less bandwidth and more latency compared with the wired world. The connection stability and the predictable availability are less, too. Furthermore, possible improvements in the bandwidth rate in the wireless communications have power consumption penalty in the limited battery life of the handheld devices. The low power dissipation of course is not the only limitation that the mobile phones tend to have. In contractor with the personal computers, mobile phones have less powerful CPUs and less available memory of any kind. The small size of screens in addition with the different way of data input, voice input and smaller keypad, request a different user interface than the common used in personal computers.

WAP standard defines an application environment and an application protocol. The actual application protocol architecture provides a scalable and extensible application development environment for mobile communications devices. This is achieved through a layered architecture of the protocol stack. WAP is designed as a layered type protocol in order to be extensible, flexible, and scalable. Based on the Open System Interconnection model (OSI) the WAP stack basically is divided into five essential layers. Each layer of WAP provides a set of functions and services to other applications through of well defined interfaces. The protocol stack isolates the applications from the bearer so that one application can be executed or run regardless of the actual transport service being used. Fig.1 shows the WAP protocol stack and how it relates to the protocols on the internet.

![WAP Stack Architecture](image.png)

**Figure 1. WAP Stack Architecture.**

The differences between WAP and the common used internet protocol stack are proved the most important part of enabling wireless access for mobile devices. WAP stack does not map directly onto other stacks but a comparison between them could be take place. As it is illustrated in Fig. 1, the kind of functionality that is provided by HTML and Java in the internet is incorporated in the Wireless Application Protocol (WAE) layer of WAP and the Wireless Session Layer (WSP). At the same time WSP and Wireless Transactions Protocol (WTP) layers include the functionality that is provided by HTTP. The transport layer in the wired communications is usually either TCP or User Datagram Protocol (UDP), while in the wireless world it is UDP over IP where it is possible. The Wireless Datagram Protocol (WDP) is provided for networks that cannot support IP at the network layer.

### III WAP SECURE PROPOSED SYSTEM

The design philosophy behind the proposed system is based on three different levels of processing. These have been developed by using PHP and HTML software packages [6]. The first level is the admin panel. It is made with HTML and PHP and is accessible by Internet & GPRS. It contains a password box which certifies the identity of user. Aim of application is to support also in an efficient way both functionalism and safety. Although, more secured environment (for example https), could be used alternatively.

In the first level, two different account types, for users, have access: administrator and simple admin. This is determined from the password that is used. If the user types a wrong password then there are recorded his elements as well as the text that it used for password and return at the central menu where it can retry. The password system is analyzed in detail, in the next paragraph.

Password is determined by the following scheme:

- **one standard word or phrase of determined length**
- **plus the 3 initial letters of the current day**
- **plus the sum of the digits of the time multiplied on 2**

It is obvious, that with this mechanism they can become inexperienced combinations. This way was preferred (instead of putting a static word), because we can avoid brute force attack for finding the password using a simple brute force program. The dynamic importation is strengthened to make it difficult for those who want illegally to enter the system.

![Password Box](image.png)

**Figure 2. Announcement Service Login Interface.**

Also for avoiding the theft of password with network sniffers, the following system of encoding/decoding has been used: Before the password is sent to the server for confirmation, it passes from an encoding process. This mechanism encrypts the password data. After that, when the server receives the encoded password it follows the reverse processes to decrypt (decoding) the password and finally to verify it. This mechanism that has been previously described is illustrated in the following Fig. 3.

![Encrypted Password Mechanism](image.png)

**Figure 3. Encrypted Password Mechanism.**

There exists a cookies support system, so we can avoid the problem of continuous logins. Super-user can post announcements that will be appeared through the system of registration posts. Administrators have more choices based
on system safety. These operations are shown alternately in the next graph.

Figure 4. Account Types Operations.

The system of registration posts, works as follows: When the user writes his post into the textbox, he clicks the button and the text is stored temporarily. Then the script creates two files. One HTML file with pure HTML code (headers title and text formatting) that can be read from any browser, that supports HTML-type files. The second file is built with WML, in order to efficient the file to be viewed under WAP environment. The text of the announcement is appended as a part of the code and is stored temporally.

In each post is recorded the hour that the announcement posted, the date, also a log file with the ip, the host, the code and the browser that the user uses.

The interface that the user has access to via HTML corresponding to WML is the following:

Figure 5. User Access Interface.

The proposed system has been programmed on PHP scripts that could be runned on every functional system supports HTML and PHP. PHP description language supports the flexibility of the small size of the developed code. Scripts occupy very small size as a result of the benefits of PHP that has been written, apart from the 2 files where the size is determined by the quantity of text that they contain.

The attribution of system is rapid because of technology that PHP also uses. It has been avoided the use of SQL database, reason of high use of CPU resources. With this way, scripts could be runned at more systems. On the other hand SQL databases require 3 more factors: more memory, more CPU resources but also the existence of an SQL database to the system which the program will be installed. According to our experimental measurements for a typical computer with Windows XP, 2.4Ghz and 256mb of RAM running an apache server with PHP, the allocated resources measured in CPU power is at about 4%.

IV PHP and Script Code

As it has been stated in the previous paragraphs, the script was manufactured with PHP, mostly of the attributes that this particular description language has. PHP from itself uses at crown html and with precisely this way, the menu and pages were made. Here are some examples of codes of the proposed system, that were developed:

```php
$addr = $_SERVER['REMOTE_ADDR'];
$host = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$port = $_SERVER['REMOTE_PORT'];
$bro = $_SERVER['HTTP_USER_AGENT'];

if (file_exists("failedlog.html")) {
    echo "<a href="failedlog.html">Open failed logins</a>
    echo "<a href="delfailedlogs.php">Delete failed logins</a>
}
else {
    echo "<a href="postlog.html">Open successfull announcements</a>
    echo "<a href="delnonfailed.php">Delete successfull announcements</a>
}
```

Concrete function presents the choices of administrator with the following process: It presents the header, and it creates 2 links to the two pages that the users see. It examines the existence of the files “postlog.html” and “failedlog.html” and if they exist it proceeds creating a link for their reading, but also creating a link to another link to a php script that erases each file. Also clicking on the link “Delete announcements” it opens a php script that lists all the announcements and allows the admin to delete one entry.

Figure 6. Failed-to-Log Case.
V WTLS: A SECURE ENVIRONMENT FOR WAP

Wireless Application protocol uses Wireless Transport Layer Security (WTLS), a variant of the previous developed SSL/TLS protocol, specified for wireless communications, to secure the communication between the mobile devices and the other parts of the communication handshake [1], [4], [7].

In the WTLS three different encryption operations have been defined: privacy, authentications and data integrity [4], [7]. These operations are full supported by the WTLS layer with the availability of selection between different encryption algorithms in each kind of security process. With the rule privacy an applied transfer method that ensures a private end-to-end transfer, is defined. The sender and the recipient have to use a common know cryptographic algorithm to encrypt and decrypt the transmitted data. They also have to know the used key, in which is based the operation of the encryption algorithm. It is obvious that the used algorithm should be resistant to all known cryptanalysis attacks. The encryption algorithms that are proposed to be used in the WTLS are IDEA, DES and RC5 [4], [7].

Authentication is described as the security unit that ensures if the identity of every communication part is the one that it has been claimed. The two contacting parties have to present verifications to prove their identities. This is achieved by using digital signatures or electronic certificates. After the authentication, the service provider is sure that the supported service is available to the user who requests to use it. On the other hand, the user can be confident about the service provider with the same way of authentication. The RSA, Diffie-Hellman and Elliptic Curve algorithms serve authentication in WAP [1], [4], [7].

Integrity is used in order to verify that the transmitted data have not been modified in all the travel through the network. In different words integrity secures the reliability of the information. Hash functions are the most common method for integrity. In the WTLS the SHA and the MD5 hash functions are introduced by the specifications [1], [4], [7]. The internal architecture of WTLS is shown in the next Figure 7.

![Figure 7. WTLS Internal Architecture.](image)

The alert messages that are shared between the client and the server contain the level of severity of the error, as well as a description of the alert. There is a 4-byte checksum used in most alerts. This checksum is calculated from the last record received. The Record Protocol is a layered protocol where data to be received is decrypted, decompressed, verified and transmitted to the higher levels. The data to be transmitted is compressed, the Message Authentication Code (MAC) is applied, and finally the data is encrypted. There is no fragmentation performed in the WTLS layer.

The Record Payload Protection changes the WTLS Compressed structure into a WTLS Cipher structure using the encryption and MAC functions. The Change Cipher Spec Protocol was developed to allow either the client or the server signal the other that the Cipher specification for upcoming records will be changing. This Change Cipher message consists of a one-byte record that is sent during the handshake between the client and the server.

VI CONCLUSIONS & OUTLOOK

Wireless networks are available anywhere, anytime and the user’s acceptance is high. Wireless Application Protocol is one of the most promising communication protocols in the wireless world. Of course the sensitivity of the transmitted information has increased the needs for communications privacy. This work is dedicated to a secure WAP environment through internet and mobile phones. The proposed system supports an announcement mechanism. It has been developed with PHP and HTML. It offers a flexible and efficient solution to WAP subscribers, for posting, reading and editing announcements, through their handheld wireless devices.

REFERENCES