KATHMANDU UNIVERSITY JOURNAL OF SCIENCE, ENGINEERING AND TECHNOLOGY
VOL. 5, No. II, SEPTEMBER, 2009, pp 17- 29.

ACCESS CONTROL SECURE TO RESTRICTED INFORMATION RESOURCES FOR IEEE 802.11 WIRELESS NETWORKS

J.L. Mejía-Nogales, S. Vidal-Beltrán, J. López-Bonilla

9ESIME-Zacatenco, Instituto Politécnico Nacional,
Anexo Edif. 3, Col. Lindavista, CP 07738 México DF
Corresponding author: jlopezb@ipn.mx, lopezbjl@mexico.com

Received 25 May, 2009; Revised 20 July, 2009

ABSTRACT

Information security has been one of the most sensible issues when designing communications systems; especially when this information is cataloged as confidential. The present document deals with a secure system that let you get access to privileged data, when the medium access is a wireless network based on IEEE 802.11 standards.

The system designed is conformed by three main functions, which capture the first http request and forward it to an authentication server; the server validates the user's identity in order to give access to the information resources. The control access entity determines which users are allowed or denied from the system. These functions are performed by a Captive Portal, an authentication Server and an Access Point.

Keywords: IEEE 802.11, Captive Portal, Authentication, Encryption, HTTP.

INTRODUCTION

In the last years, the Wireless Local Area Networks - WLAN have been one of the most increasing technologies, these networks usually provide to their users the access to a local computer network or an Internet connection without cables. Nevertheless, one of the great obstacles which the wireless networks progress has faced is the security[1]. The wireless networks are more difficult to protect than the wired networks, because they use radio waves as their carrier.

To guarantee the security in wireless networks the Institute of Electrical and Electronics Engineers - IEEE defines mechanisms of encryption and authentication into its standard 802.11, in the edition of 1999 [2]. Nevertheless, in 2001 were published a series of articles that exhibited the vulnerability of these encryption mechanism and the contradictions of the authentication method of the standard 802.11 [3]. To cover all the security needs on the wireless networks the IEEE published its standard 802.11i in 2004; this new standard incorporates a specific security layer [4].

The Wireless Local Area Networks incorporate usually encryption algorithms and authentication mechanism to protect themselves [5]; these alternatives verify the user's identity and verify that the known user has the authorization to use certain network services, besides the communication is encrypted if by chance someone intercepts it. One of the disadvantages to employ these alternatives mechanisms is the need to configure or install some specific software in the user's mobile computer.

The wireless networks security can be divided in two categories: the security when identity and permissions of the user are verified and the security when data is transferred between wireless devices using radio waves. The system designed in this document contains the first security category.

This secure access system allows that a mobile user gets access to the restricted information resources through a wireless access point connection; while the user is obtaining the access to the wireless network, the system never make public user's personal information. The goal to design a new alternative security system is develop access control mechanisms secure, open and flexible, but especially transparent for the users.

ANALYSIS OF THE SYSTEM

To fulfill the characteristics of an access control secure, open, and flexible, the proposed system was divided in three use cases or subsystems, as it is shown in the figure 1. The user will be related directly and independently with each use case. The goal of the first use case *Capture First Request* will be that the user pass by the authentication process before he access to the wireless network services [6], in this use case only HTTP requests will be accepted, and all petitions of not authenticated users will be forward to the presentation web page of the Authentication Server, where the user name and the password will be required.

The goal of the second use case *Authenticate User* will be verify user's identity. The Authentication Server will send to the user a challenge, then he will return to the server an answer to the trial, finally the server will determine if the user has passed the challenge. When the user is satisfactorily authenticated he will receive the address of the information resources where he has the authorized access, these directions are sent as links to their corresponding URLs. If the user doesn't pass the trial he will not has the authorized access to the local network services [7]. When the Authentication Server sends the links list to the user also sends temporary keys and its identifier, the Access Point to the information resources use this information to determine who authorized the access [8].

The goal of the last use case *Control the Access* is verify that only the authorized users accede to the restricted information resources. To control the access it will be used temporary keys for verify the identity of the authorized users any time, these keys will be sent to the user as part of the web page that it requested in his HTTP request [9].

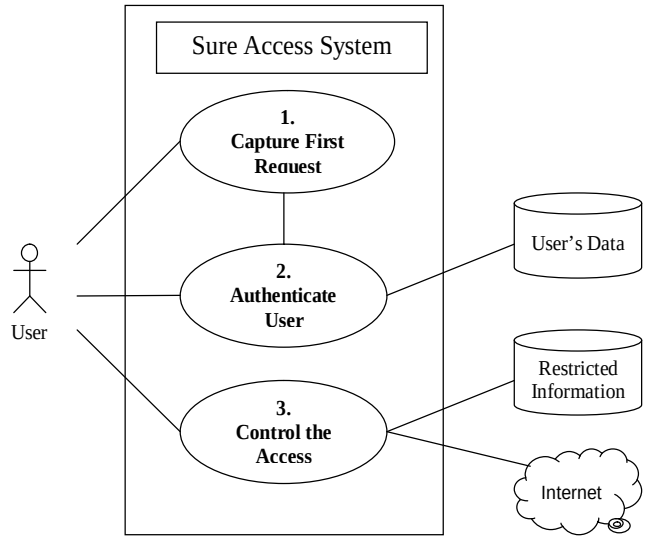

Fig.1. Use Cases of the System

DESIGN OF THE SYSTEM

A. Roles Definition

As soon as the use cases of the proposed system were identified, in the table 1 the roles or components are described:

TABLE 1
ROLES OF THE SYSTEM

Roles	Description
User	Person with a mobile computer who wants to use some of the wireless local network services.
Access Point of the wireless network	Hardware equipment that allows the communication between the local network and the wireless devices.
DHCP Server	Server that takes charge of sending the network configuration to the client, which includes: an IP address which will be used by the user's mobile computer, the Gateway address and the DNSs address.
Firewall	Logical device that controls the traffic between the access point of the wireless network and the local network. The Firewall is a packets filter which prevents some communications forbidden by the security policy of the local network.
Authentication Server	Server which provides an unique authentication point to the users. Also it allows that they obtain transparently the temporary keys, which will allow the access to the restricted information resources where the user has the authorized access [7].

User Database	Resources of restricted data of the users, which includes the user names and passwords. The Authentication Server uses this information to do its work.
URLs Database	Resources of the data of the different restricted information resources, inside this information are found its location into the HTTP Server.
Access Point	Program that realizes an effective access control to some web pages into the HTTP Server. This software uses temporary keys codified like cookies, which determine what user has the authorized access [9].
Key Database	Resources where is stored the body of the temporary keys created by the Access Point for every authenticated user. Every record of this database is associated with a restricted information resource where the user has the authorized access [8].
HTTP Server	Programs which implements the HTTP protocol. This protocol supports transfer of files codified by HTML language. These files are storage in dedicated web servers.

B. States Definition

To describe how the proposed system works, in the tables 2, 3 and 4 are defined the states for each use case:

TABLE 2
SYSTEM STATES
USE CASE 1: CAPTURE FIRST REQUEST

States	Description
1.1 Listening new user	The access point of the wireless network is working in open system without its own security method, this means that, any user inside the range of the wireless network can connect to the system [10].
1.2 Detecting user	Once the user's mobile computer has connection to the system through the access point of the wireless network, it must be configured as DHCP client so that does a request to the DHCP Server.
1.3 Assigning IP	When the user, in this case the client, is connected to the DHCP Server, this send the network configuration to the client which includes: an IP address, the Gateway address and the DNSs address. The user's mobile computer can access to the wireless network with the network configuration.
1.4 Waiting request	The local network has a Firewall which controls the accesses to the system all the time; it only allows the HTTP traffic and DNS request.
1.5 Redirecting request	When the system receives a new HTTP request, independently of the request destination address, it is forwarded to the Authentication Server.

1.6 Showing page for the authenticati on	When the new HTTP request is forwarded, the request original URL is changed by the URL corresponding to the presentation web page of the Authentication Server. Then, the user will be received the presentation web page, which consist in a welcome to the wireless network and a request so that the user enter his user name and password.

TABLE 3
SYSTEM STATES
USE CASE 2: AUTHENTICATE USER

States	Description
2.1 Waiting the password	The Authentication Server will be set in a wait state after sends its presentation web page, which is composed by a welcome to the wireless network and the request of user name and password
2.2 Authenticati ng User	When the Authentication Server receives a user name and password, it compares this information with its database to determine if the user is valid. For security reasons, the Authentication Server handles the passwords in encrypted form. If the information of the user doesn't coincide with the stored data in the server, an error message will be sent to the user.
2.3 Consulting user's permission	As soon as the authentication was made, it is proceeded to determine the user's valid permissions. Based on these permissions, the URLs of the information resources where the user has the authorized access are captured since the database of the Authentication Server.
2.4 Codifying data of the user	Afterwards the Authentication Server encrypts the user's information obtained in its database using its private key.
2.5 Showing URLs authorized	Finally, a web page is sent to the user with a links list; each link corresponds to an information resource where the user has the authorized access. To this information is added the user's encrypted data and the Authentication Server identifier.

TABLE 4
SYSTEM STATES
USE CASE 3: CONTROL THE ACCESS

States	Description
3.1 Verifying data of the user	When the user's web browser receives the list of URLs from the Authentication Server, it connects to the Access Point of the information resource, this process is transparently for the user. The Access Point uses the public key of the Authentication Server to verify the integrity of the user's encrypted information, which receives from the web browser. If everything is correct the temporary keys Hcook and Lcook are created, they are sent to the user's web browser

	codified like cookies and the keys body is stored in the database of the Access Point.
3.2 Waiting HTTP request	The Access Point protect the HTTP Server where the restricted information recourses are stored, only the authorized users will be able to access to this information. Nevertheless, the server will be active all the time, waiting some HTTP request.
3.3 Verifying temporary key	When the Access Point receives a HTTP request verifies if temporary keys Hcook and Lcook are found in the cookies received. In first instance, the key Lcook is decrypted and verified, if it is correct the request is responded, but if it is overdue the key Hcook is decrypt and verifies. If some flaw is found in the verification process the request is denied and an error message is sent to the user.
3.4 Creating new temporary key	After decrypt and verify satisfactorily the key Hcook, the new temporary keys Hcook and Lcook are created and the keys body is stored in the database of the Access Point.
3.5 Capturing web page	When the temporary keys have been verified, the Access Point captures the web page solicited in the HTTP request from the HTTP Server.
3.6 Sending web page	Finally, the Access Point sends to the user the web page requested with the new temporary keys Hcook and Lcook codified as cookies, if they were created.

C. Functions Description

The relation between the components of the proposed system is defined by the information exchange, as far as is necessary to describe what data are sent and received for every component in the different states of the system. In the tables 5, 6, 7 and figures 2, 3, 4 the information flows are described for the three use cases:

TABLE 5
DATA FLOW
USE CASE 1: CAPTURE FIRST REQUEST

Data Flow	Description
1.1. SSID (State 1.1)	The access point of the wireless network transmits periodically its Service Set Identifier – SSID.
1.2. Access Request (State 1.2)	The user's mobile computer listens the SSID from the access point and retransmits it for associating to the wireless network
1.3. IP Request (State 1.2)	The user's mobile computer sends a DHCP request to the server.
1.4. IP Address (State 1.3)	The DHCP Server sends the network configuration to the user, which includes an IP address, the Gateway address and the DNSs Servers address.

1.5. HTTP Request (State 1.4)	The user sends a HTTP request with a specific URL location.
1.6. Readdressing (State 1.5)	The Captive Portal of the wireless network changes the original URL location of the HTTP request received, by the Authentication Server URL and forwards the request.
1.7. Password Request (State 1.6)	The Authentication Server after receiving the HTTP request sends its presentation web page.

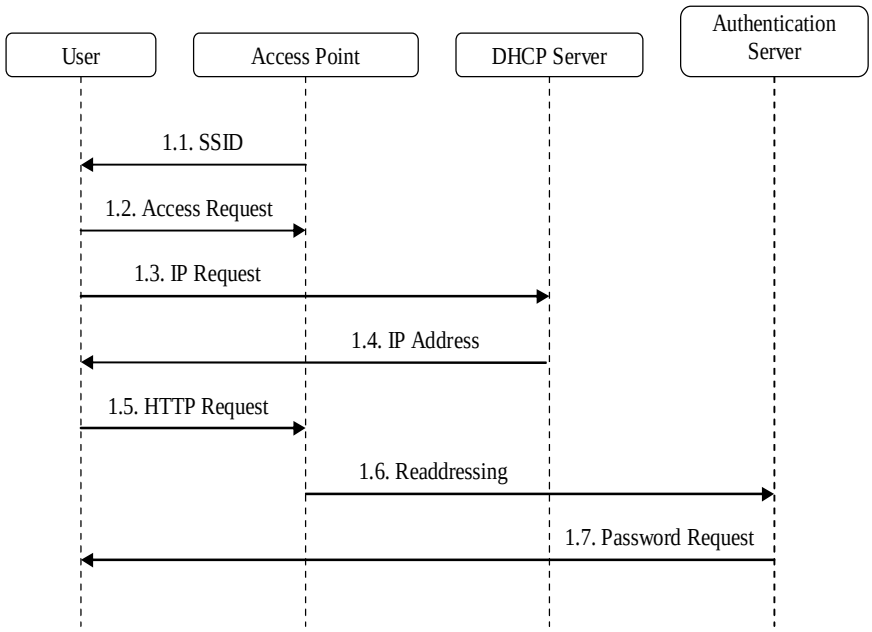

Fig.2. Sequences Diagram of Use Case 1: Capture First Request

TABLE 6
DATA FLOW
USE CASE 2: AUTHENTICATE USER

Data Flow	Description
2.1. User's Password (State 2.1)	The user sends his user name and password like response to authentication process.
2.2. Data of the User	The Authentication Server reads the user names and passwords from its database to compare with the user data received.

(State 2.2)	
2.3. Incorrect Password (State 2.2)	The Authentication Server sends a web page to the user, to report that the data received are invalid.
2.3'. Data of the User (State 2.3)	The Authentication Server uses the user name to consult in the URLs database the user's permission.
2.4. Permission (State 2.3)	The Authentication Server takes the data of the information resources where the user has the authorized access.
2.5. List of Links (State 2.5)	The Authentication Server sends a links web page, which includes: the URLs of the information resources, the encrypted user data and its identifier.

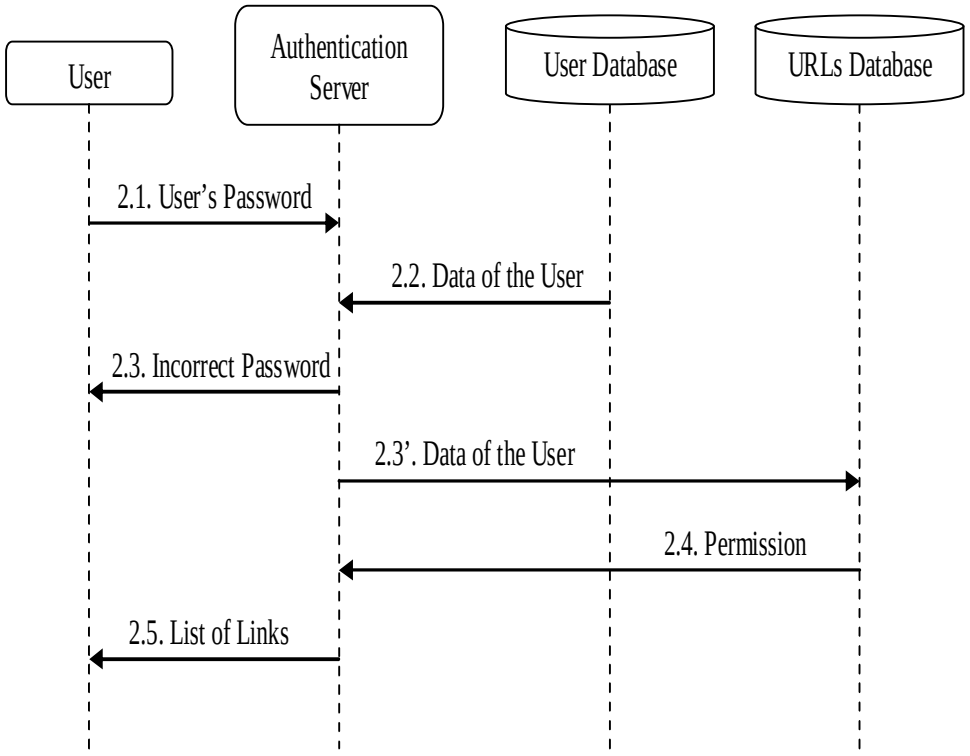

Fig.3. Sequences Diagram of Use Case 2: Authenticate User

TABLE 7
DATA FLOW
USE CASE 3: CONTROL THE ACCESS

Data Flow	Description
3.1. Authentication Server Firm (State 3.1)	The user's web browser sends to the Access Point the URLs of the information resources, the encrypted user data and the Authentication Server identifier.
3.2. Body of Temporary Keys (State 3.1)	The Access Point stores the new temporary keys body, which includes: the user name, the URL where the keys gives access, the keys expiration time, a random block and a record of the last modification.
3.3. Temporary Keys (State 3.1)	The Access Point sends to the links web page, the temporary keys codified like cookies and an object to report the user to what links he has the access authorized. The object usually is a characteristic image that appears in the left side of each link.
3.3'. Access Rejected (State 3.1)	The Access Point sends an object to the links web page to report the user to what links he has the unauthorized access. The object usually is a characteristic image that appears in the left side of each link.
3.4. HTTP Request (State 3.2)	The user sends a HTTP request through a link of the web page that is loaded in his browser. Also, the temporary keys codified like cookies are sent transparently for the user.
3.5. Body of Temporary Keys (State 3.3)	The Access Point takes from its database the temporary keys body, to verify the validity of the temporary keys received in the HTTP request.
3.6. HTTP Request (State 3.5)	The Access Point forwards the HTTP request to the corresponding server.
3.7. Body of Temporary Keys (State 3.4)	The Access Point stores the new temporary keys body, which includes: the user name, the URL where the keys gives access, the keys expiration time, a random block and a record of the last modification.
3.8. Web Page (State 3.6)	The Access Point sends to the user the web page that he requested, together with the temporary keys codified like cookies.
3.8'. Access Rejected (State 3.6)	The Access Point sends to the user a web page for report that he has the unauthorized access to the information resource requested.

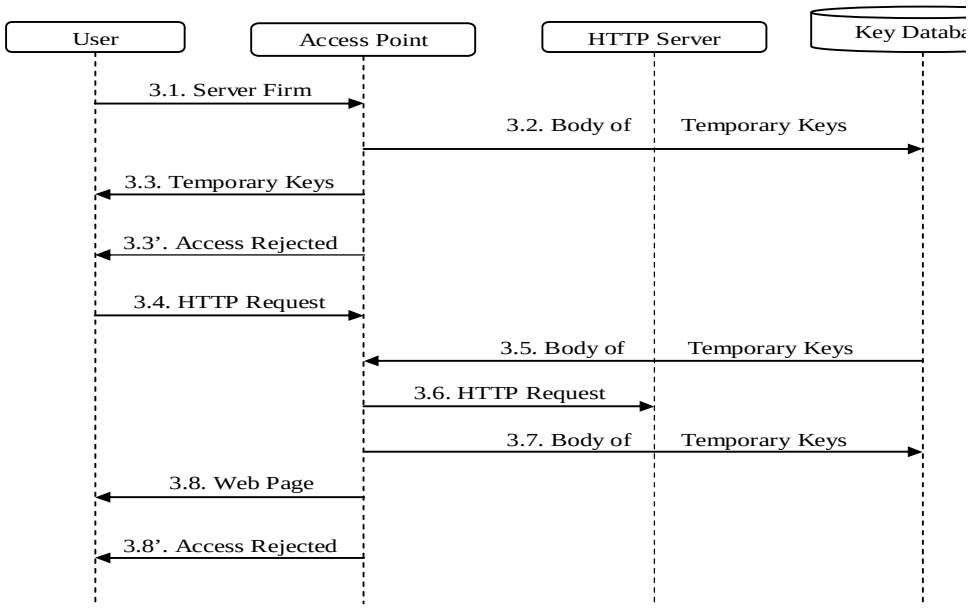

Fig.4. Sequences Diagram of Use Case 3: Control the Access

D. Network Structure

The proposed system will be implemented as an intermediary between the wireless network and the local network, as it is shown in the figure 5. After that the mobile user is connected to the access point of the wireless network, he will follow transparently the information flow of the proposed system, this means that, he only will enter his valid user name and password when these be requested, then he will choose to what information he wants to access, and if he has the authorized access this information will be loaded his web browser. The user never will perceive the encrypted data exchange between different roles of the proposed system and the HTTP browser of his mobile computer.

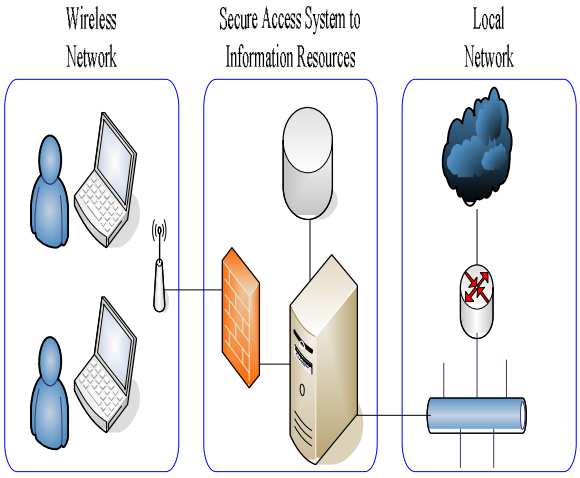

Fig.5. Network Diagram

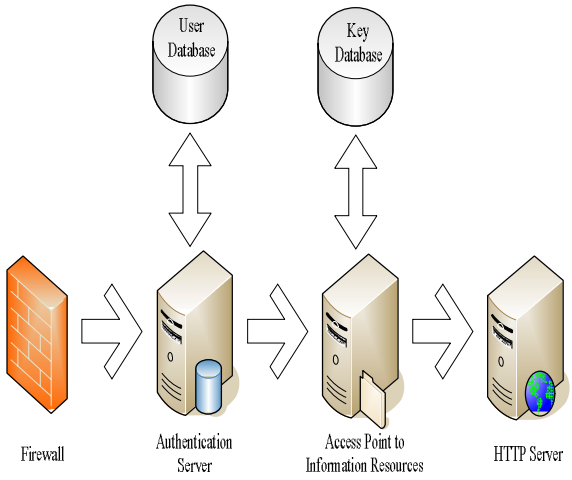

Fig.6. Components of the Central Server

CONCLUSIONS

In this work a secure access system to information resources for wireless networks 802.11 was designed, which allows to a mobile user to enter to restricted information resources through an access point, the system never make public user's personal information. A prototype of the proposed system was implemented to evaluate its design using only free software.

This prototype was developed into a central server, in this server was installed the operating system Linux Red Hat 9 with kernel 2.4, also were used the programs Apache 1.3 as the HTTP Server, PAPI 1.4 as access control, and Perl 5.8 as programming language. During the implementation of the prototype the following components were built:

- Firewall
- Authentication Server
- User Database
- URLs Database
- Access Point to Information Resources
- Key Database
- HTTP Server

In the figure 6 is shown the components of the central server, which is connected to the local network and the access point of the wireless network. The DHCP Server is found configured inside the hardware of the access point of the wireless network. Based on prototype implementation determined that the proposed system provides the following advantages:

- *Standardization*. The recommendations of the standard IEEE 802.11i and the observations of the articles that showed the vulnerability in the wireless networks security were considered in the analysis and design of the proposed system.

- *Independence between subsystems*. The architecture of the system is designed to guarantee the independence between the three subsystems. This helps to modifications and updates to each subsystem without affecting the structure of the others.
- *Transparent procedures*. The proposed system uses completely transparent procedures for the users when implements its secure access, this means that, the user don't need an additional training for use the system.
- *Flexibility*. The wireless network manager who implements the proposed system will have the option to employ his own authentication methods, based on his security policies.
- *Compatibility*. The proposed system offers compatibility with any additional security procedure, that is, the system can work in parallel form with others access control systems.
- *Use Free Software*. This advantage provides to the wireless network managers the possibility to do changes according to the security policies or network needs. But he should have knowledge about programming and functioning of the proposed system for realize changes in the code source of the used software.
- *Easy implementation*. The necessary requirements to implement the secure access system to information resources for wireless networks are smallest, only is needed the hardware to build the wireless network and obtain the Free Software.

After authenticating to a user the proposed system consult its database for determine the user's permissions. Each user have an unique profile, this means that, he will be able to accede to certain restricted information resources inside the local network, or to accede Internet or both, according to his user's profile.

The mobile user only must be authenticated by the secure access system to information resources; the unique tool that he will use in this process is his preferred web browser. The user doesn't need to install a specific program, does complicated configurations or report the identity of his mobile computer by means of his IP address or the MAC of his wireless card.

REFERENCES

1. Matthew Gast "802.11 Wireless Networks: The Definitive Guide", Ed. O'Reilly & Associates, 2001. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

2. ANSI/IEEE Std 802.11, 1999 Edition, The Institute of Electrical and Electronics Engineers, 20 August 1999, Available: http://standards.ieee.org/getieee802/download/802.11-1999.pdf

3. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks**,** Wi-Fi Alliance, April 2003, Available: http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf
4. Jon Edney and William A. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Ed. Addison-Wesley, August 2003.

5. Bruce Potter and Bob Fleck "802.11 Security", Ed. O'Reilly & Associates, December 2002.

6. Enterprise Solutions for Wireless LAN Security, Wi-Fi Alliance, February 2003, Available: http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Enterprise2-6-03.pdf

7. IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control**,** IEEE Std 802.1X-2001, The Institute of Electrical and Electronics Engineers, Approved 14 June

2001 IEEE-SA Standards Board and Approved 25 October 2001American National Standards Institute**,** Available: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

8. The PAPI Development Team, "A Detailed Description of the PAPI Protocol", RedIRIS, Available: http://papi.rediris.es/doc/PAPI_Protocol_Detailed.pdf

9. Diego R. López and Rodrigo Castro Rojo, "Acceso Ubicuo a Recursos de Información en Internet: El Sistema PAPI", RedIRIS, Available: http://papi.rediris.es/dist/pod/PAPI-gb.html

10. Stewart S. Miller, "Seguridad en WiFi", Ed. McGraw-Hill, 2004.