Científica Vol. 10 Núm. 4 pp.199-205
© 2006 ESIME-IPN. *ISSN 1665-0654*. Impreso en México

Sistema de acceso seguro a recursos de información para redes inalámbricas 802.11

José Luis Mejía-Nogales
Sergio Vidal-Beltrán
José Luis López-Bonilla

Sección de Estudios de Posgrado e Investigación (SEPI),
Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME),
Instituto Politécnico Nacional. U. P. "Adolfo López Mateos",
Ed. Z4, 3er piso, Col. Lindavista, México, DF.
MÉXICO.

email: mejianogales@yahoo.com
svidalb@ipn.mx
jlopezb@ipn.mx

Recibido el 25 de mayo de 2005; aceptado el 12 de noviembre de 2005.

1. Resumen

Este artículo presenta el diseño e implementación de un sistema de acceso seguro a recursos de información confidencial a través de redes inalámbricas del tipo IEEE 802.11. Para lograr esto, la seguridad del sistema se distribuye en tres procesos principales: un *portal cautivo*, un s*ervidor de autenticación* y un *punto de acceso*.

Palabras clave: IEEE 802.11, portal cautivo, autenticación, encriptación, HTTP.

2. Abstract (Secure Access System to Information Resources for IEEE 802.11 Wireless Networks)

This work 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*.

Key words: IEEE 802.11 standard, authentication mechanisms, captive portal.

3. Introducción

Una de las tecnologías que más ha evolucionado en los últimos años son las *redes inalámbricas de área local* (*Wireless Local Area Networks* - WLAN), que ofrecen a sus usuarios conexión a una red de computadoras local o a Internet sin la necesidad de enlazarse físicamente. No obstante, la seguridad [1] siempre ha sido uno de los factores más delicados en las redes de este tipo ya que los datos viajan a través del espacio libre; esto da origen a la necesidad de crear un sistema de seguridad específico para este tipo de tecnología.

Es necesario mencionar que, para garantizar la seguridad en las redes inalámbricas, el Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers - IEEE) define mecanismos de encriptación y autenticación dentro de su estándar 802.11, en la edición de 1999 [2]. Sin embargo, en 2001 se publicaron una serie de artículos que expusieron la vulnerabilidad de este mecanismo de encriptación y cuestionaron la forma de autenticar del estándar 802.11 [3]. Para cubrir las necesidades de seguridad sobre las redes inalámbricas el IEEE publicó su estándar 802.11i a mediados de 2004, este nuevo estándar incorpora una capa de seguridad específica [4].

Para proteger el acceso a redes inalámbricas, usualmente, se utilizan métodos de autenticación y encriptación [5], los cuales impiden el acceso a personas no autorizadas, y que algún intruso que intercepte una comunicación pueda descifrarla. Uno de los inconvenientes de la utilización de estos mecanismos es la necesidad de configurar o instalar algún software específico en el equipo móvil del usuario.

Podemos dividir la seguridad en las redes inalámbricas en dos categorías: la seguridad al momento de autenticar los usuarios e identificar sus correspondientes permisos, y la seguridad al momento de transmitir los datos entre dispositivos inalámbricos usando ondas de radio. El sistema propuesto en este trabajo abarcará únicamente la primera categoría de seguridad.

Este sistema de acceso seguro permite a un usuario móvil ingresar a contenidos de información confidencial a través de un punto de acceso de una red inalámbrica del tipo 802.11,

sin hacer pública su información personal. El propósito de desarrollar una nueva alternativa de seguridad mediante el diseño del sistema propuesto, es desarrollar mecanismos de control de acceso seguros, abiertos y flexibles, pero sobre todo, transparentes para los usuarios.

4. Desarrollo

4.1 Diseño del sistema de acceso seguro

Para dar una solución completa al sistema de acceso seguro se proponen implementar los siguientes componentes:

4.1.1 *Firewall*

Dispositivo encargado de filtrar la información no deseada antes que cualquier otro componente procese la información enviada a la red local a través de la red inalámbrica. Mediante la configuración de este elemento se logra que todos los paquetes desde y hacia el punto de acceso de la red inalámbrica sean administrados por el portal cautivo.

4.1.2. Portal cautivo

Se encargará de que ningún usuario tenga acceso a los servicios de la red inalámbrica sin antes pasar por un proceso de autenticación [6], en este subsistema sólo se aceptarán peticiones HTTP, y todas las peticiones de usuarios no autenticados serán redireccionadas hacia la URL de presentación del servidor de autenticación.

4.1.3. Servidor de autenticación

Se ocupa de identificar al usuario. El servidor de autenticación enviará al usuario un reto, el cual devolverá al servidor una respuesta a esta prueba, y si el servidor determina que el usuario ha pasado el reto, le enviará las direcciones de los contenidos de información a los que tiene permitido el acceso en forma de enlaces a sus correspondientes URL. Si el usuario no cumple con la prueba se le negará cualquier acceso a la red local [7]. Además de las URL, el servidor de autenticación envía al usuario una clave temporal con su identificador para que el punto de acceso a los contenidos de información sepa quién autorizó el acceso [8].

4.1.4. Servidor HTTP

Programa que implementa el protocolo HTTP. Este protocolo de transporte soporta la transferencia de archivos codificados con el lenguaje HTML. El servidor utilizará el protocolo SSL (Secure Sockets Layer) para proporcionar privacidad de la información entre el usuario y el servidor central mediante el uso de cifrado simétrico.

4.1.5. Servidor DHCP

Servidor encargado de enviar la configuración de red al cliente, incluida la dirección IP que utilizará el equipo móvil del usuario, la dirección del Gateway y las direcciones de los DNS.

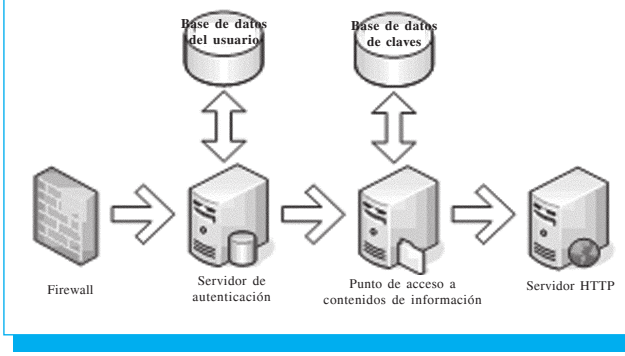

Fig. 1. Diagrama del sistema de acceso seguro.

4.1.6. Punto de acceso a contenidos de información

Programa que realiza el control de acceso efectivo para un conjunto de localizaciones web dentro del servidor HTTP. Este software utiliza las claves temporales codificadas como *cookies* para determinar a los usuarios con acceso autorizado [9].

4.1.7. Base de datos usuarios

Aquí residirán los datos confidenciales de los usuarios que incluyen el nombre de usuario y la contraseña. El servidor de autenticación utiliza estos datos para cumplir su función.

4.1.8. Base de datos de URL

En esta parte se almacenarán los datos de los diferentes contenidos de información confidencial, dentro de esta información se encuentra su localización dentro del servidor HTTP.

4.1.9. Base de datos de claves

Las claves temporales que crea el punto de acceso para cada usuario autenticado residen en esta parte del sistema. Cada registro de este repositorio está asociado a un contenido de información donde el usuario tiene autorizado el acceso [8].

En la siguiente sección se procede a detallar la forma en que interactúan los diversos componentes para lograr el objetivo del sistema.

4.2. Funcionamiento del sistema de acceso seguro

Una vez que se han descrito los diferentes elementos que conformarán el sistema propuesto, se procede a describir el funcionamiento del mismo, el cual divide su operación en tres funciones principales:

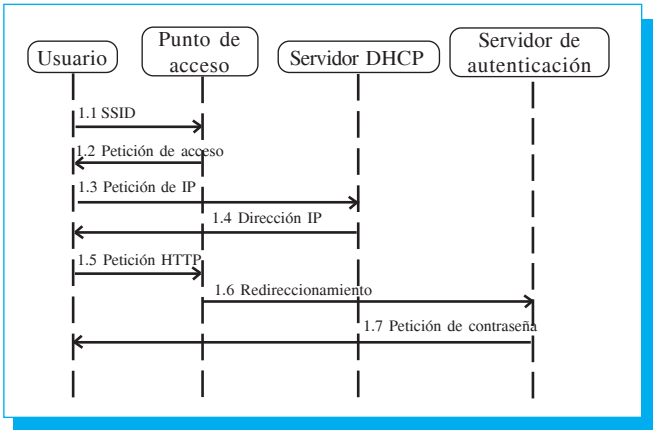

Fig. 2. Capturar el primer pedido.

- capturar el primer pedido
- autenticar al usuario
- controlar el acceso

4.2.1. Capturar el primer pedido

El propósito de esta etapa es que ningún usuario tenga acceso a los servicios de la red inalámbrica sin antes pasar por un proceso de autenticación; la figura 2 muestra los intercambios de información que realizan los distintos dispositivos involucrados. La tabla 1 describe en detalle cada uno de los estados cuando se captura el primer pedido.

Tabla 1. Capturar el primer pedido.

Flujo de datos	Descripción
1.1. SSID (estado 1.1)	El punto de acceso de la red inalámbrica transmite periódicamente su identificador de conjunto de servicio (*Service Set Identifier*-SSID).
1.2. Petición de acceso (estado 1.2)	El equipo móvil de usuario escucha el SSID del punto de acceso de la red inalámbrica y lo retransmite para lograr una asociación.
1.3. Petición de IP (estado 1.2)	El equipo móvil del usuario envía una petición DHCP al servidor.
1.4. Dirección IP (estado 1.3)	El servidor DHCP devuelve la configuración de red al usuario, que incluye una dirección IP, la dirección del Gateway y las direcciones de los servidores DNS.
1.5. Petición HTTP (estado 1.4)	El usuario hace una petición HTTP con una dirección URL específica.
1.6. Redireccionar (estado 1.5)	El *portal cautivo* de la red inalámbrica cambia la dirección URL de la petición HTTP recibida, por la dirección URL del servidor de autenticación y la reenvía.
1.7. Petición de contraseña (estado 1.6)	El *servidor de autenticación* envía su página web de presentación tras recibir la petición. HTTP.

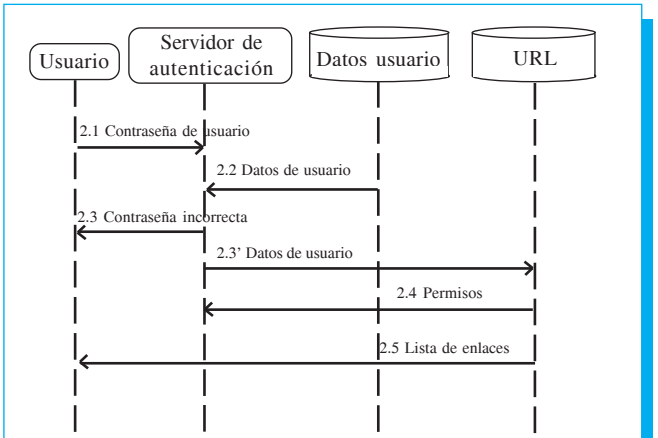

Fig. 3. Autenticar al usuario.

4.2.2. Autenticar al usuario

Una vez que se ha capturado la primera petición, se procede con la autenticación para verificar que el usuario puede tener acceso a la red inalámbrica, el intercambio de información entre los diferentes subsistemas se muestra en la figura 3. La

Tabla 2. Autenticar al usuario.

Flujo de datos	Descripción
2.1. Contraseña de usuario (estado 2.1)	El usuario envía una respuesta de autenticación con su nombre de usuario y contraseña.
2.2. Datos del usuario (estado 2.2)	El *servidor de autenticación* lee los nombres de usuario y contraseñas de su base de datos para comparar con los datos del usuario recibidos.
2.3. Contraseña incorrecta(estado 2.2)	El *servidor de autenticación* envía una página web al usuario, informándole que los datos recibidos no son válidos.
2.3'. Datos del usuario (estado 2.3)	El *servidor de autenticación* utiliza el nombre de usuario para consultar en la base de datos de las URLs, los permisos del usuario.
2.4. Permisos (estado 2.3)	El *servidor de autenticación* lee los datos de los contenidos de información donde el usuario tiene autorizado el acceso.
2.5. Lista de enlaces (estado 2.5)	El *servidor de autenticación* envía una página web de enlaces que incluye: las URL de los contenidos de información, los datos del usuario codificados y su identificador.

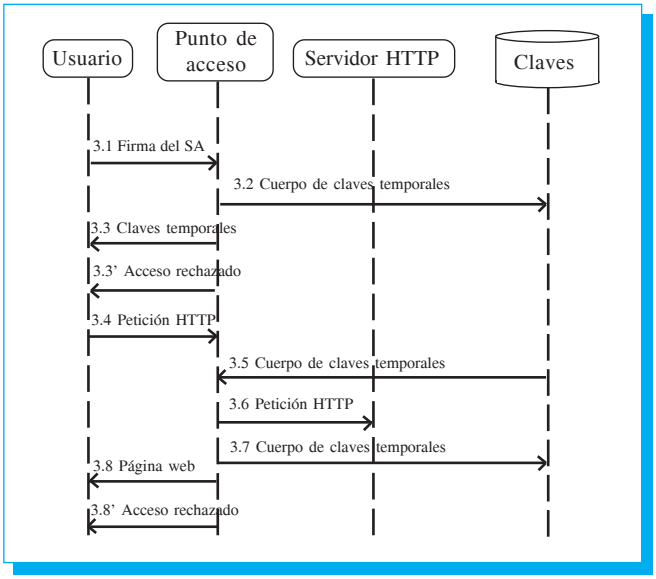

Fig. 4. Controlar el acceso.

tabla 2, define cada una de las actividades involucradas en la autenticación.

4.2.3. Controlar acceso

Finalmente, una vez que se ha capturado el primer pedido y que se ha validado la identidad del usuario, se procede a verificar a qué contenidos de información tiene derecho de acceder, la figura 4 muestra cómo se realiza este procedimiento. La tabla 3 define cada una de las etapas involucradas en el control de acceso.

De esta manera es como el sistema propuesto en este trabajo lleva a cabo su operación. En la siguiente sección se describe su puesta en marcha en un prototipo inicial.

4.3. Implementación y pruebas

El sistema propuesto se implementará como un intermediario entre la red inalámbrica y la red cableada, como se muestra en la figura 5. Un prototipo de este sistema se encuentra actualmente instalado en la Maestría en Ciencias en Ingeniería de Telecomunicaciones de la ESIME Zacatenco, donde proveerá acceso para aproximadamente 50 estudiantes de maestría y licenciatura, 15 investigadores y el personal administrativo asignado al departamento.

Una vez que el usuario intente conectarse al punto de acceso de la red inalámbrica, comienza el intercambio de información entre

Tabla 3. Control de acceso.

Flujo de datos	Descripción
3.1. Firma del servidor de autenticación (estado 3.1)	El navegador del usuario envía al *punto de acceso* las URL de los contenidos de información, los datos del usuario codificados y el identificador del *servidor de autenticación*.
3.2. Cuerpo de claves temporales (estado 3.1)	El *punto de acceso* almacena el cuerpo de las nuevas claves temporales que se compone de: el nombre de usuario, URL donde las claves dan acceso, el tiempo de expiración de las claves, un bloque aleatorio y un registro de la última modificación.
3.3. Claves temporales (estado 3.1)	El *punto de acceso* envía a la página web de enlaces, las claves temporales codificadas como *cookies* y un objeto para informar al usuario a qué enlaces tiene autorizado el acceso. El objeto, generalmente, es una imagen característica que aparece al lado izquierdo de cada enlace.
3.3'. Acceso rechazado (estado 3.1)	El *punto de acceso* envía un objeto a la página web de enlaces para informar al usuario a qué enlaces no tiene autorizado el acceso. El objeto es una imagen característica que aparece al lado izquierdo del enlace.
3.4. Petición HTTP (estado 3.2)	El usuario envía una petición HTTP por medio del enlace de la página web que está cargada en su navegador. También se envían, de forma transparente al usuario, las claves temporales codificadas como cookies.
3.5. Cuerpo de claves temporales (estado 3.3)	El *punto de acceso* lee de su base de datos el cuerpo de las claves temporales, para verificar la validez de las claves temporales recibidas en la petición HTTP.
3.6. Petición HTTP (estado 3.5)	El *punto de acceso* reenvía la petición HTTP al servidor correspondiente.
3.7. Cuerpo de claves temporales (estado 3.4)	El *punto de acceso* almacena el cuerpo de las nuevas claves temporales que se compone de: el nombre de usuario, URL donde las claves dan acceso, el tiempo de expiración de las claves, un bloque aleatorio y un registro de la última modificación.
3.8. Página web (estado 3.6)	El *punto de acceso* envía al usuario la página web que solicitó, junto con las claves temporales codificadas como *cookies*.
3.8'. Acceso rechazado (estado 3.6)	El *punto de acceso* envía al usuario una página web informándole que no tiene autorizado el acceso al contenido de información que solicitó.

los componentes del sistema de acceso seguro a recursos de información para redes inalámbricas. El usuario no advierte en su totalidad este flujo de información, es decir, que no percibe el

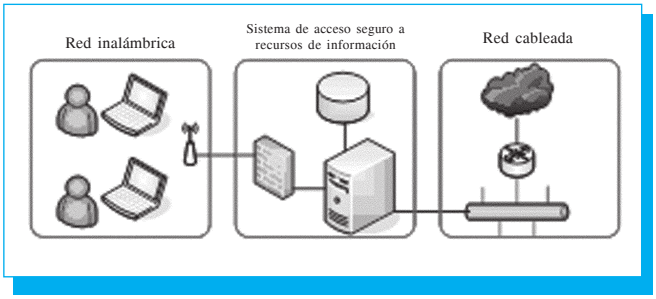

Fig. 5. Diagrama de red.

envío de datos codificados entre el sistema y su navegador HTTP de su equipo móvil. Cuando el usuario abra su navegador HTTP le aparecerá automáticamente la ventana de presentación del servidor de autenticación que se muestra en la figura 6.

El usuario tendrá que ingresar su nombre de usuario y su contraseña para poder acceder a la información de la red local. Si la autenticación es correcta, aparecerá la ventana que se muestra en la figura 7.

En la ventana de la figura 7 se informa al usuario que ha sido identificado correctamente por el *servidor de autenticación*, también se le muestran los enlaces a los que tiene autorizado el acceso, según la base de datos del *servidor de autenticación*. Además, el punto de acceso a los contenidos de información, avisa al usuario si los enlaces están habilitados, esto mediante una imagen característica que se muestra al lado izquierdo de cada enlace.

Después de ser autenticado el usuario podrá acceder a la red de Internet de forma normal y a los contenidos de información

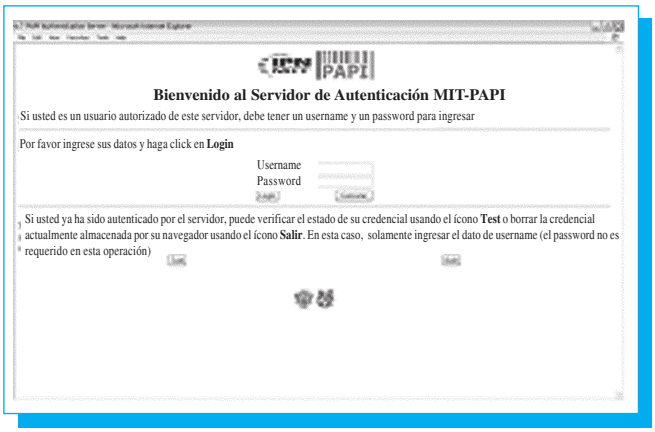

Fig. 6. Ventana de presentación.

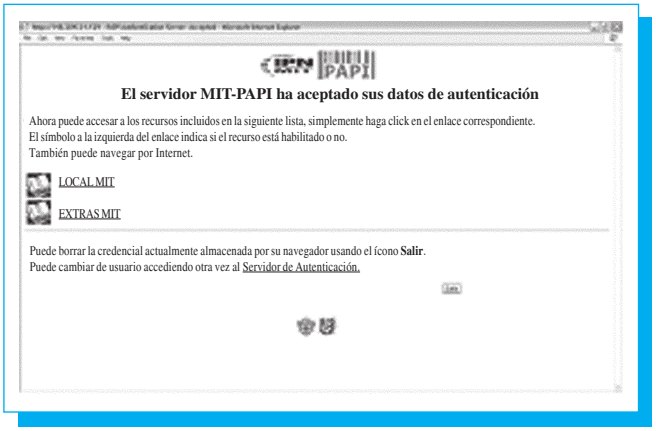

Fig. 7. Ventana con enlaces autorizados.

confidencial habilitados haciendo uso de su enlace correspondiente. Si la autenticación falla, el usuario recibirá la ventana que se muestra en la figura 8.

En la ventana de presentación (figura 6) aparecen dos opciones auxiliares: *test* y *salir*, la primera de ellas evalúa las *cookies* almacenadas por el navegador web y envía una nueva ventana con la lista de enlaces a los que el usuario tiene permitido el acceso, y si estos enlaces están habilitados, esta ventana se muestra en la figura 9.

Al elegir la opción salir, se borran todas las *cookies* almacenadas por el navegador del usuario.

Es importante reiterar que el usuario solamente utiliza su navegador web para ingresar a la información confidencial,

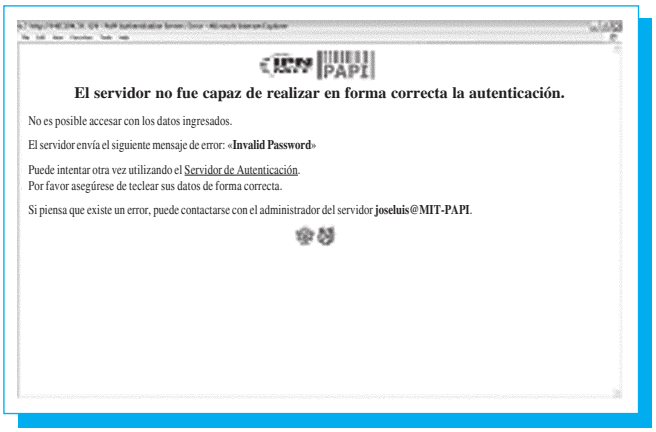

Fig. 8. Ventana con autenticación rechazada.

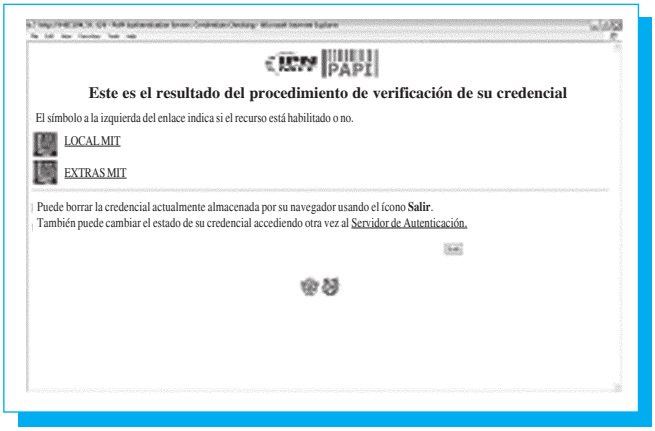

Fig. 9. Respuesta a la opción test.

todos los procesos que realiza el sistema de acceso seguro a recursos de información para redes inalámbricas son transparentes para él. Desde el ingreso de su contraseña hasta que le aparece la información deseada, el usuario no se percata de la codificación y verificación de claves o de la generación e intercambio de *cookies*.

Por último, se menciona que el prototipo fue implementado en un servidor central Hewlett Packard NetServer E800 con sistema operativo Linux Red Hat 9 y kernel 2.4, además se utilizaron los programas Apache 1.3 como *servidor HTTP*, PAPI 1.4 como control de acceso, y se trabajó con el lenguaje de programación Perl 5.8.

5. Conclusiones

En este trabajo se muestra el diseño e implementación de un sistema de acceso seguro a recursos de información para redes inalámbricas 802.11, y con base en las pruebas realizadas se puede concluir que el sistema posee las siguientes ventajas:

- Diseño estándar. En el análisis y el diseño del sistema se consideraron las recomendaciones del estándar IEEE 802.11i y los artículos que pusieron en evidencia la vulnerabilidad de sus predecesores.

- Independencia entre subsistemas. La arquitectura del sistema está diseñada para garantizar la independencia entre los tres subsistemas. Este aspecto ayuda a realizar modificaciones y actualizaciones a cada subsistema sin afectar el funcionamiento de los demás.

- Procedimientos transparentes. Para proporcionar accesos seguros, el sistema propuesto utiliza procedimientos completamente transparentes a los usuarios, de manera que no se requiere de una capacitación adicional para la utilización del sistema.

- Flexibilidad. El administrador de una red inalámbrica que implemente el sistema propuesto tendrá la opción de emplear esquemas de autenticación propios, según sus políticas de seguridad.

- Compatibilidad. El sistema propuesto ofrece compatibilidad con cualquier otro procedimiento adicional de seguridad, es decir, que puede trabajar en forma paralela con otros sistemas de control de acceso.

- Utilización de software libre. Esta ventaja ofrece a los administradores de la red inalámbrica la posibilidad de realizar cambios según las políticas de seguridad o los requerimientos de la red. Se deberán tener conocimientos de programación y del funcionamiento del sistema para realizar cambios en el código fuente del software utilizado.

- Fácil implementación. Los requisitos necesarios para implementar el sistema de acceso seguro a recursos de información para redes inalámbricas únicamente son: un servidor y un *access point* para redes IEEE802.11; además de instalar los componentes que se proponen en este trabajo.

- Robusto. Basado en las pruebas realizadas, el sistema resiste ataques informáticos activos tal como *Spoofing* o *Hijacking*; esto debido a que el sistema no usa direcciones MAC o IP como mecanismos de autenticación. Para el caso de los ataques pasivos, el sistema es robusto ya que no basa su funcionamiento en el algoritmo WEP.

- Información encriptada. La información crítica que es transmitida por la red inalámbrica es encriptada mediante el uso de el algoritmo AES (*Advanced Encryption Standard*), adicionalmente se usan claves temporales de tal manera que si un intruso llega a descrifar la clave, ésta ya será obsoleta debido a que expiran frecuentemente y deben ser renovadas.

- Protección de direcciones IP. Para prevenir que un intruso pueda hacer uso de una dirección IP, el servidor DHCP solo proporciona direcciones privadas [11], las cuales no son útiles si se quieren usar en la red cableada.

Finalmente, se puede mencionar que el sistema fue implementado en un ambiente académico; pero puede ser fácilmente integrado en cualquier institución que requiera proteger el acceso a su red y a los recursos de información confidencial que en ella se alberguen.

Agradecimientos

Este trabajo fue desarrollado bajo el proyecto CGPI No. 20061080.

6. Referencias

[1] Matthew Gast «802.11 Wireless Networks: The Definitive Guide», Ed. O'Reilly & Associates, 2001.

[2] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) SpecificationsANSI/IEEE Std 802.11, 1999 Edition, The Institute of Electrical and Electronics Engineers, 20 August 1999, 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, 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, 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, http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[8] The PAPI Development Team, «A Detailed Description of the PAPI Protocol», RedIRIS, 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, http://papi.rediris.es/dist/pod/PAPI-gb.html

[10] Stewart S. Miller, «Seguridad en WiFi», Ed. McGraw-Hill, 2004.

[11] RFC 1918 - Address Allocation for Private Internets, February 1996, disponible en: http://www.ietf.org/rfc/rfc1918.txt?number=1918

Information for Authors Submitting Papers to Científica Journal

The manuscript must be prepared in following a Camera Ready format with all its section numbered starting with the abstract, as shown below:

1. **Abstract**
2. **Resumen (Spanish abstract if it is possible).**
3. **Body of the manuscript**
4. **Reference list**
5. **Acknowledgements if any**
6. **Reference list**
7. **Appendix if any**

Title

Must be concise and no longer than 3 lines using capital and lower case letters.

Authors Name and Affiliations

The authors name must be written below the title using a one column format staring with the given name followed by one or two family names, if two family names applies. Below the authors names must be written the affiliation including the address quality, fax, telephone number or email.

Abstract

The abstract with about 200 words must give a brief description about the research including some comments about the experimental or simulation results and conclusion.

Resumen (Spanish abstract)

It is desirable that, if it is possible, a Spanish abstract be provided.

Body of the Manuscript

The body of the manuscript must include an introduction in which the relevance of the research must be explained. A review of related research works by either, the same or another authors must be included.

The body of the manuscript also must include the theoretical aspects of the research, as well as experimental or simulation results is any, together with a Conclusions Section.

Format

All manuscripts must be written in letter size paper, only by one side, with the following requirements. *a*) It is recommended that, if possible, the text be written using a word processor. *b*) The text must be written in two columns with a separation between them of 0.77cm, using a 10 points Times font or similar, with lower, upper and right margins equal to 2.5 cm and left margin equal to 3.0 cm. *c*) All the equations must be numbered and written using an equations editor. *d*) All symbols or abbreviations must be defined the first time that they be used in the text. *e*) All figures must inserted in the manuscript. *f*) All figures must be numbered and its captions must be inserted below them. It is strongly recommended to use, when it be possible, words instead of symbols in the graphic axis. The table captions must be inserted above the corresponding table. *g*) All pictures and scanned figures must be high quality pictures for proper reproduction.

References

References must appear in the format given below. For multiple authors all family names and given names initials must be given. Titles of the journals must be all in lower case except the fist letter of each word. All references must be cited by number in brackets, in the order that they appear in the text.

Instituto Politécnico Nacional
Escuela Superior de Ingeniería Mecánica y Eléctrica
Científica: La Revista Mexicana de Ingeniería Electromecánica
Unidad Profesional Adolfo López Mateos
Edificio 1, Planta baja, Dirección, Col. Lindavista, CP. 07738, Tel. 5729 600 ext. 54518, Fax 55860758
email: revistacientifipn@yahoo.com.mx

El Instituto Politécnico Nacional

y la Escuela Superior de Ingeniería Mecánica y Eléctrica

publican

Científica

La Revista Mexicana de Ingeniería Electromecánica

Publicación incluida en el Índice de Revistas Mexicanas de Investigación Científica y Tecnológica del CONACyT

Suscripciones y venta de ejemplares:

Edificio 1, primer piso, Dirección, ESIME Zacatenco, Unidad Profesional Adolfo López Mateos, Col. Lindavista, CP 07738, México, DF.

Tel. 5729 6000 exts. 54518/54555

email:
revistacientifipn@ yahoo.com.mx