redes inalámbricas

Control de acceso en

Ing. Alberto Arce Martínez, Dpto de Ingeniería y Gestión de Software
e Ing. Manuel Cheong Gómez, Dpto de Sistemas Digitales,
Universidad de las Ciencias Informáticas (UCI)
aarce@uci.cu, mcheong@uci.cu

1 Introducción

Actualmente, con el objetivo de ganar en movilidad cuando se trabaja desde cualquier lugar donde se encuentre un usuario, se está implementando con frecuencia redes inalámbricas.

En específico, la Universidad de las Ciencias Informáticas de Cuba (UCI), debido a la introducción de tecnología inalámbrica, paulatinamente, necesitará implementar este tipo de red a gran escala y, para lograrlo, el tema de la seguridad es de vital importancia dentro de este tipo de infraestructura.

En el presente trabajo se abordarán aspectos importantes a tener en cuenta para garantizar la seguridad en esta tipología de red, la integridad de los datos que se manejan y el control de acceso a la misma. Deben tomarse en consideración, por supuesto, las características propias de esta infraestructura tecnológica y las políticas de seguridad con las que se cuenta. Todo esto con un único propósito: garantizar que la seguridad en la red sea cada vez más robusta y el cumplimiento de los estándares internacionales que rigen esta actividad.

2 Aspectos para garantizar la seguridad en las redes inalámbricas

Para implantar una red inalámbrica deben estudiarse las tipologías existentes y las más adaptadas a nuestro medio. Hay dos topologías de red diferentes.

2.1 Topología

Red *ad-hoc —peer to peer—* es una red de área local independiente que no está conectada a una infraestructura cableada y donde todas las estaciones se encuentran conectadas directamente unas con otras —en una topología mallada—. La configuración de una Red Inalámbrica de Área Local —del inglés, *Wireless Local Area Network* (WLAN)— en modo *ad -hoc* , se utiliza para establecer una red donde no existe la infraestructura inalámbrica o donde no se requieran servicios avanzados de valor añadido. Estas redes, tales como Bluetooth, están diseñadas para conectar dinámicamente dispositivos remotos, por ejemplo, teléfonos celulares, *laptops* y PDAs —del inglés, *Personal Digital Assistant*—. Se identifican como *ad hoc* a causa de sus topologías de red cambiantes. Mientras que las WLAN utilizan una infraestructura de red fija, las redes *ad-hoc* mantienen configuraciones de red aleatorias, confiando en un sistema maestro-esclavo conectado por enlaces inalámbricos para que los dispositivos puedan comunicarse [1].

Red de infraestructura: en ella los clientes WLAN se conectan a una red corporativa a través de un punto de acceso inalámbrico. La mayoría de las redes de área local inalámbricas corporativas opera en modo de infraestructura. Las WLAN permiten mayor flexibilidad y portabilidad que las LAN —*Local Area Network* / Red de Área Local— cableadas tradicionales. A diferencia de estas, que requieren un cable para conectar la computadora de un usuario a la red, una WLAN conecta computadoras y otros componentes a la red utilizando un dispositivo como Punto de Acceso —del inglés, *Access Point* (AP)—. Un Punto de Acceso se comunica con dispositivos equipados con adaptadores de redes inalámbricas y, por otro lado, se conecta a una LAN Ethernet cableada a

través de un puerto RJ-45. Los dispositivos de Punto de Acceso típicamente tienen áreas que cubren hasta 300 pies —aproximadamente 100 metros—. Esta área de cubrimiento se llama celda (*cell*). Los usuarios se mueven libremente dentro de la celda con su *laptop* u otro dispositivo de red sin dejar de transmitir. Las celdas de los puntos de acceso se pueden unir para que los usuarios puedan hasta **vagar** o **andar** dentro de un edificio o entre edificios [1].

2.2 Problemas de seguridad en redes inalámbricas

La ausencia de cables para acceder a los recursos de red, es lo que ha marcado el gran impacto de las redes inalámbricas actualmente. No obstante, a la vez, constituye su problema más grande en cuanto a seguridad se refiere. Cualquier equipo que se encuentre a 100 metros o menos de un Punto de Acceso, podría tener acceso a la red inalámbrica. Como las ondas de radio pueden salir de los edificios, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a ella.

Según estudios realizados se plantea que lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de tener Puntos de Acceso Inalámbrico —del inglés, *Wireless Access Point* (WAP)— en la red de una institución. Es muy común encontrar redes en las que el acceso a Internet se protege adecuadamente con un *firewall* (corta-fuego) bien configurado; pero, en el interior de la red, existen WAP totalmente desprotegidos y que emiten una señal hacia el exterior. Cualquier persona que, desde el exterior, capte la señal del Punto de Acceso, podrá acceder a la red de la institución, y podrá emplear la red como punto de ataque hacia otras redes y, luego, desconectarse para no ser detectado, robar software o información, introducir virus o algún software maligno, etc. Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que hace vulnerable por completo la seguridad informática de una institución [2].

Estos problemas han traído consigo que se realicen ataques a este tipo de red.

2.3 Tipos de ataques

Existen diferentes tipos de ataques dentro de los que se destacan:

- Espionaje (*surveillance*)

Consiste simplemente en observar el entorno donde se encuentra instalada la red inalámbrica. No se necesita ningún tipo de hardware o software especial. Sirve para recopilar información y puede combinarse con otros tipos de ataques [3].

- Lenguaje de marcado (*war-chalking*)

Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que **pasen por allí**. Es decir, es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico. En este tipo de ataque los símbolos son pintados con tiza (*chalk*) aunque actualmente se utilizan otros medios, como la pintura normal, *spray* de color, etc. El significado de cada símbolo existente es el siguiente:

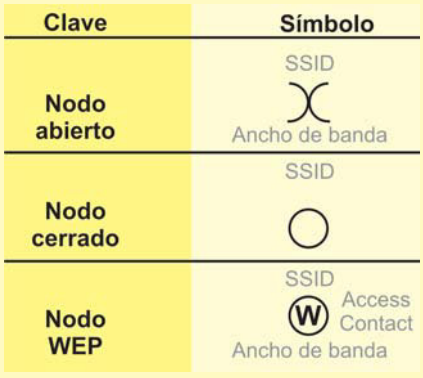

Figura 1 Lenguaje de símbolos [1].

- Método de detección de redes (*War-driving*)

Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como una *notebook* o un PDA. El método es realmente simple: el atacante pasea con el dispositivo móvil y, en el momento en que detecta la existencia de la red, se realiza un análisis de la misma. El dispositivo móvil puede estar equipado con un sistema GPS para marcar la posición exacta donde la señal es más fuerte o, incluso, una antena direccional para recibir el tráfico de la red desde una distancia considerable.

Si la red tiene DHCP —*Dynamic Host Configuration Protocol* / Protocolo de Configuración de Host Dinámico—, el dispositivo móvil se configura para preguntar continuamente por una IP dentro de un cierto rango, si la red no tiene DHCP activado se puede ver la IP que figure en algún paquete analizado.

Existen varias herramientas útiles para detectar redes inalámbricas, las más conocidas son el AirSnort o Kismet para Linux y el NetStumbler para sistemas Windows.

Para realizar el *War-driving* se necesitan pocos recursos. Los más usuales son una computadora portátil con una tarjeta inalámbrica, un dispositivo GPS —*Global Positioning System* / Sistema de Posicionamiento Global— para ubicar el AP en un mapa y el software apropiado —AirSnort para Linux, BSD- AriTools para BSD— [3].

- Interceptar una señal

El atacante intenta identificar el origen y el destino que posee la información. Es decir, la toma de posesión y el uso del ancho de banda de las WLAN privadas y de los *hotspots* públicos —lugares donde se brinda acceso inalámbrico—, mediante un *kit* —grupo de herramientas— básico del *wardriver* —atacante de este tipo de método—: programas *sniffer* —herramienta para monitorear el tráfico en la red— descargables de la red, antenas direccionales hechas de las formas más inverosímiles —incluso con paquetes de papas fritas Pringles— e instrucciones colgadas en los sitios de Net-activismo más visitados. Tras haber interceptado la señal, el ata-

cante intentará recopilar información sensible del sistema.

Para llevar a cabo este método, puede que el *wardriver* tenga que exponerse peligrosamente, teniendo que acercarse a la red para capturar la señal. Esto puede provocar una probable tendencia a una mayor prudencia [3].

2.3.1 Técnicas de intrusión

- *Spoofing* (burla)

Esta técnica de ataque se engloba dentro de los ataques activos donde un intruso pretende ser la fuente real u original.

- *Sniffing* y *eavesdropping* (escuchas-intercepción)

El programa monitoriza los datos y determina hacia dónde van, de dónde vienen y qué son, siempre que haya una tarjeta de red que actúa en **modo promiscuo**. El modo promiscuo es un modo de operación en el que una computadora conectada a una red compartida captura todos los paquetes, incluidos los paquetes destinados a otras computadoras. Es muy útil para supervisar la red, sin embargo, presenta un riesgo de seguridad dentro de una red de producción [3].

- *Hijacking* (secuestro)

El atacante falsifica información, un identificador de usuario o una contraseña permitidos por el sistema atacado. Esto lo hace redefiniendo la dirección física o MAC —*Media Access Control / Control de Acceso al Medio* — de la tarjeta inalámbrica por una válida (*hijacking*). De esta manera, asocia una dirección IP válida del sistema atacado. La idea es secuestrar la comunicación entre dos sistemas suplantando a uno de ellos, para lo que es necesario estar situado en la ruta de comunicación [3].

- Denegación de Servicio —del inglés, *Denial of Service* (DoS)— o ataques por inundación (*flooding attacks*)

La Denegación de Servicio sucede cuando un atacante intenta ocupar la mayoría de los recursos disponibles de una red inalámbrica. Impide a sus usuarios legítimos disponer de dichos servicios o recursos. Puede producirse a través de:

- Ataques por sincronización (SYN *Flooding*).
- Ataque *smurf*.
- Sobrecarga del sistema.
- Falsedad de Nombres de Dominio (DNS *Spoofing*) [3].

2.4 Soluciones de seguridad en redes inalámbricas

Inicialmente para resolver los problemas de seguridad que aparecen con el uso de las redes inalámbricas, muchos fabricantes han fomentado la creación de dispositivos que soporten protocolos de cifrado. Se desarrolla el protocolo WEP —*Wireless Encryption Protocol* / Protocolo de Cifrado Inalámbrico— el cual utiliza una clave secreta estática —no hay renovación de la clave de manera automática y frecuente— que es compartida por el Punto de Acceso y todos los clientes que accedan a través de este a la red, y con la cual se realiza la autenticación y la protección de los datos. Pero WEP comienza a presentar debilidades de seguridad debido al manejo estático de su llave y al uso de un vector de inicialización que se puede identificar en los paquetes transmitidos periódicamente. En la actualidad, esto puede realizarse de forma automática con herramientas que facilitan la captura de los datos [4].

La IEEE consciente de estas fallas desarrolló el estándar de seguridad 802.11i para redes inalámbricas, que también se conoce como Red de Seguridad Sólida —del inglés, *Robust Security Network* (RSN)—. Por otro lado, el consorcio de proveedores de tecnología inalámbrica Wi-Fi generó el estándar WPA —*Wi-Fi Protected Access* / Acceso Protegido Wi-Fi— para la protección de los datos y el control del acceso inalámbrico a las redes, el cual se basa en el estándar 802.11 y puede implementarse en las tecnologías inalámbricas de tipo Wi-Fi. Este estándar incluye los mecanismos más adecuados para realizar el control de acceso y protección de datos en ambientes inalámbricos porque integra mecanismos fuertes de autenticación, control de acceso, integridad y confidencialidad. WPA utiliza 802.1x como mecanismo de control de acceso y autenticación a la red y para generar y entregar las llaves de sesión WPA a los usuarios autenticados [4].

Para corregir las principales debilidades de WEP, WPA utiliza el protocolo TKIP —*Temporary Key Integrity Protocol* / Protocolo integral de clave temporal— el cual aumenta el tamaño de las claves, refresca dichas claves periódicamente, utiliza un contador de secuencia para el vector de inicialización y realiza una función de mezcla de este mismo vector por paquete. De este modo, previene los ataques de clave de WEP. Adicionalmente, WPA utiliza una función llamada MIC —*Message Integrity Code*— que verifica la integridad de los mensajes transmitidos y previene que atacantes capturen paquetes, los modifiquen y los reenvíen [4].

WPA fue una solución intermedia hasta la llegada del estándar 802.11i aprobado por el IEEE y aceptado por Wi-Fi *Alliance* en septiembre del 2004. Este estándar se basa en el algoritmo de cifrado TKIP; no obstante, también admite el AES —*Advanced Encryption Standard* / Estándar de Cifrado Avanzado— que es mucho más seguro. Wi-Fi *Alliance* creó una nueva certificación, denominada WPA2, para dispositivos que admiten el estándar 802.11i [5].

A diferencia del WPA, el WPA2 puede asegurar tanto redes inalámbricas en modo de infraestructura como también redes en modo *ad hoc*.

El estándar IEEE 802.11i define dos modos operativos:

- **WPA-Personal**: este modo permite la implementación de una infraestructura segura basada en WPA sin tener que utilizar un servidor de autenticación. WPA Personal se fundamenta en el uso de una clave compartida, llamada **PSK** —*Pre Shared Key*— que significa Clave Precompartida, que se almacena en el

Punto de Acceso y en los dispositivos cliente. A diferencia de WEP no se necesita ingresar una clave de longitud predefinida. El WPA le permite al usuario ingresar una contraseña. Después, un algoritmo condensador la convierte en PSK [6].

◆ **WPA-Enterprise**: este modo requiere de una infraestructura de autenticación 802.1x con un servidor de autenticación, generalmente un servidor RADIUS o FreeRadius, un controlador de red —Punto de Acceso— y un cliente [6].

No todos los organismos e instituciones disponen de los recursos necesarios para implantar el estándar 802.11i debido a que se necesita invertir en hardware —que por lo general son costosos— para soportar este estándar. Por lo tanto, las entidades que no tengan instaladas estas tecnologías con soluciones WPA o WPA2, utilizan alternativas que integran el uso del mecanismo de control de acceso y autenticación a la red 802.1x con el uso de cifrado WEP con manejo dinámico de claves —WEP dinámico—. Y, de esta forma, se garantiza el control del acceso a los recursos de la red y se eliminan las brechas de seguridad creadas al tener un punto de acceso inalámbrico desprotegido.

2.5 Estándar 802.1x para el control de acceso a la red

El uso de 802.1x se encuentra dentro del grupo de mejores prácticas para garantizar la seguridad en redes inalámbricas**.** Se plantea que el estándar 802.1x es el pilar fundamental de la seguridad Wi-Fi o Seguridad inalámbrica. Antes de la adaptación de este estándar para redes inalámbricas Wi-Fi, no existía ningún control sobre los accesos a este tipo red.

Para pequeñas y medianas empresas el estándar 802.1x no es muy fácil de aplicar, sin embargo, en las organizaciones medianas o grandes, es imprescindible su uso para lograr un mínimo de seguridad en sus redes inalámbricas. En ninguna organización se puede hablar de una seguridad inalámbrica robusta, si no se aplica el estándar 802.1x.

802.1x es un estándar del IEEE para realizar el control de acceso a una red mediante un proceso de autenticación que habilita o impide el acceso de los dispositivos que se conectan a un puerto de red LAN. Este estándar puede implementarse en redes cableadas al igual que en redes inalámbricas. Además, este tipo de implementación puede utilizarse para administrar las claves empleadas con el propósito de proteger la información que trasmiten los dispositivos autenticados. En la implementación 802.1x se requieren, mínimo, los siguientes componentes:

◆ Usuario que intenta acceder a la red o **suplicante**.

◆ Punto de Acceso que habilita o impide el ingreso del suplicante, también llamado **autenticador**.

◆ Servidor de autenticación que negocia y valida la identidad del suplicante; y le informa el éxito o fracaso de este proceso al **autenticador** para que ejecute la acción indicada.

Este estándar hace referencia al uso del Protocolo de Autenticación Extensible —del inglés, *Extensible Authentication Protocol* (EAP)— ante el **suplicante** —usuarios de acceso inalámbrico—, el **autenticador** —Puntos de Acceso Inalámbrico— y los servidores de autenticación —como el RADIUS o FreeRadius solución libre— [7].

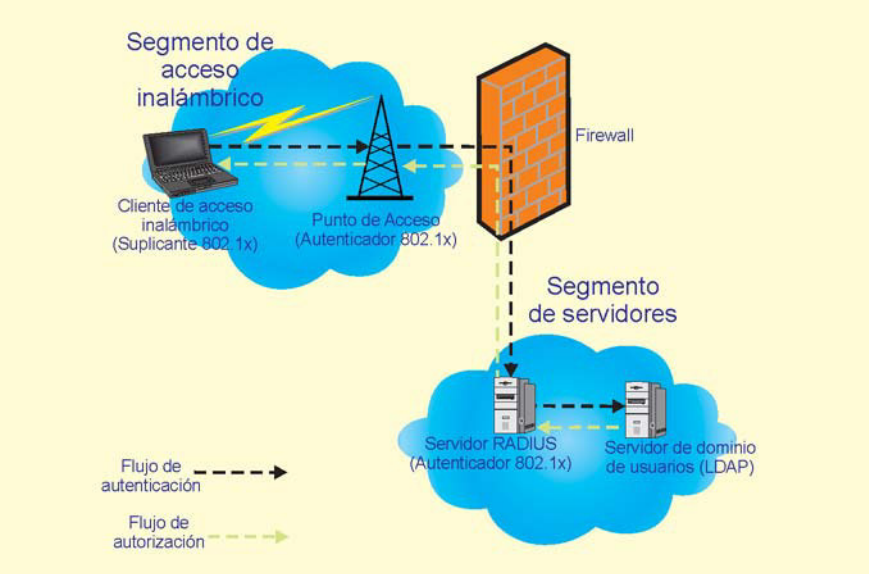

Figura 2 Esquema de autenticación basada en 802.1x [7].

2.5.1 Protocolos de autenticación

Con el objetivo de resolver y minimizar los daños producidos por los ataques y técnicas de intrusión analizados, es necesario aplicar mecanismos que garanticen la seguridad de la red. Se requiere conocer, de este modo, los diferentes protocolos que han surgido para evitar los problemas que puedan ocasionar estos ataques. Algunos de estos protocolos que garantizan la autenticación en el proceso de controlar el acceso a la red se describen a continuación:

PAP —*Password Authentication Protocol* / Protocolo de Autenticación de Clave de Acceso—: este protocolo realiza la validación cuando se

establece la conexión entre el cliente y el servidor. Utiliza el nombre de usuario y contraseña como credenciales, las cuales son enviadas en texto plano sobre el enlace, por lo que se considera un método poco seguro [7].

CHAP —*Challenge Handshake Protocol*—: provee un mejor nivel de seguridad, porque realiza una validación de tres vías entre cliente y servidor, donde este último envía un parámetro de control a quien se autentica, este lo encripta con su contraseña y lo reenvía al servidor, donde se realiza el mismo procedimiento con la contraseña almacenada y se verifica si se obtiene el mismo resultado.

EAP: es un protocolo que permite elevar aún más el nivel de seguridad de la autenticación, admite diversos métodos y tipos de credenciales a utilizar —incluyendo la capacidad de manejar certificados digitales—. De acuerdo con esto, distintos tipos de EAP pueden implementarse conforme a las características y condiciones propias de cada infraestructura donde se requiera. Los principales tipos de EAP se resumen a continuación [7].

Método	Características
EAP-TLS	•*Transport Layer Security* •Autenticación muy segura •Reemplaza simples claves por certificados para el cliente y el servidor.
EAP-TTLS	•*Tunneled Transport Layer Security*. Extensión de TLS. •Desarrollada para sobreponerse a la desventaja en cuanto a la necesidad de poseer un certificado por cliente.
EAP-PEAP	•*Protected Extensible Authentication Protocol* •Soporta métodos EAP a través del túnel, pero a diferencia de TTLS, no soporta otros métodos para la negociación de la autenticación del cliente.
EAP-LEAP	•*Light Extensible Authentication Protocol* •Autenticación mutua, distribución de clave de sesión segura y dinámica para cada usuario. •Vulnerable ante ataques de diccionario.

Figura 3 Métodos EAP [7].

Es importante tener en cuenta que el control de acceso es un factor imprescindible para implementar cualquier tipo de red porque se convierte en un método que permite tener claro quién o quiénes interactúan en la red y, de esta forma, garantizar la integridad, disponibilidad y confidencialidad de los datos que circulan en la misma.

2.6 FreeRadius

FreeRadius es la implementación libre más conocida y usada del protocolo RADIUS —*Remote Authentication Dial-In User Service*—. Se inició en el año 1999 como un proyecto de servidor RADIUS para cubrir las necesidades que otros servidores RADIUS no podían realizar. Actualmente, incluye soporte para LDAP —*Lightweight Directory Access Protocol* / Protocolo Ligero de Acceso a Directorios—, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Además de ofrecer soporte para todos los protocolos comunes de autenticación y bases de datos [8].

Los servidores de autenticación remota de usuarios por *dial-in* permiten la autenticación de usuarios cuando estos intentan acceder al servidor. RADIUS es el protocolo de autenticación, autorización y manejo de cuentas de usuario originalmente desarrollado por Livingston Enterprises y publicado en 1997. Es utilizado para administrar el acceso remoto y la movilidad IP, como ocurre en servicios de acceso por módem, DSL, servicios inalámbricos 802.11 o servicios de VoIP —*Voice over Internet Protocol* / Voz sobre el Protocolo de Internet—. Este protocolo trabaja a través del puerto 1812 por UDP —*User Datagram Protocoln* / Protocolo de Datagrama de Usuarios— [9].

La autenticación gestionada por este protocolo se realiza a través del ingreso de un nombre de usuario y una clave de acceso. Esta información es procesada por un dispositivo NAS —*Network Access Server* / *Servidor de Acceso a la Red*— a través de PPP —*Point-to-Point Protocol* / Protocolo Punto a Punto—. Posteriormente, es validada por un servidor RADIUS a través del protocolo correspondiente a partir del empleo de diversos esquemas de autenticación, por ejemplo, PAP o EAP y permite el acceso al sistema [10].

FreeRadius es, sin duda, una opción real para las instituciones que necesiten implementar el control de acceso utilizando el estándar 802.1x, sin coste alguno para la misma.

3 Aplicación

La Universidad de las Ciencias Informáticas (UCI) ha apostado por la inserción de esta tecnología dentro sus áreas docentes y productivas. Por este motivo se necesita considerar todos los aspectos respecto a la seguridad, principalmente, aquellos que distinguen a dicha tecnología.

Teniendo en cuenta las características de la UCI, en cuanto a nú-

mero de usuarios y área que abarca, se requiere una herramienta que automatice los procesos necesarios para garantizar el servicio de acceso a la red universitaria lo más seguro posible. Para este fin, existe un grupo de investigación que profundiza en el tema y, además, trabaja en el desarrollo de esta herramienta que, en un principio, provee las siguientes características:

- Gestión de usuarios desde una base de autenticación definida por el administrador del sistema —MySQL, PostgreSQL, Oracle, MS SQL Server, OpenLDAP, Active Directory—.
- Gestión de los equipos NAS que darán el servicio de acceso a los usuarios.
- Incluir una Infraestructura de Clave Pública para la generación de certificados utilizados por los usuarios.
- Administración del servicio lo más amigablemente posible para el administrador del sistema.

De esta manera, se provee a los administradores de red una aplicación que facilite la gestión de este tipo de servicio e incorpore, de antemano, elementos básicos respecto a su seguridad.

4 Conclusiones

Garantizar la máxima seguridad en las redes, es hoy de vital importancia en las instituciones y organismos que manejan información esencial. Por lo tanto, en los centros donde se implementen soluciones inalámbricas se debe prestar mucha atención a los estándares internacionales que rigen y garantizan la seguridad en este tipo de red. Siempre teniendo en cuenta la infraestructura tecnológica, organizacional y políticas de seguridad propias de cada institución.

Independientemente del estándar que se implemente —WEP, WPA, 802.11i o WPA2—, debe asumirse que el control de acceso es un factor muy importante. En consecuencia, implementar el estándar 802.1x en entornos inalámbricos, constituye una de las mejores recomendaciones de seguridad, no sólo porque aumenta el nivel de seguridad sino que permite a las organizaciones adoptar estándares de seguridad para la tecnología inalámbrica. Es, además, con la integración de soluciones libres como FreeRadius, una solución que se adapta sin impactos económicos o funcionales al crecimiento o cambio de tecnología en las organizaciones.

5 Referencias bibliográficas

[1] Tortosa, Carlos Cervera. "Seguridad en redes inalámbricas". (2005). http://www.uv.es/~montanan/redes/trabajos/SeguridadWLANs.pdf. (acceso septiembre 10, 2008).

[2] *Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas*. (junio de 2008). . http://www.inteco.es/file/10001147196. (acceso julio 11, 2008).

[3] Cors, Israel y Pernich, Patricia. "Seguridad en redes Wireless". (2004). http://www.criptored.upm.es/guiateoria/gt_m148s.htm. (acceso julio 14, 2008).

[4] Beaver, Kevin and Davis, Peter T. *Hacking Wireless Networks for Dummies*, 2005. USA: John Wiley & Sons Inc., pág. 362.

[5] Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise. http://www.wi-fi.org/knowledge_center/wpa2. (acceso septiembre 25, 2008).

[6] "WiFi - 802.11i / WPA2". http://es.kioskea.net/wifi/wifi-802.1x.php3. (acceso octubre 6, 2008).

[7] Espinoza, María P. y Loayza, Carlos C. "Seguridad para la red inalámbrica de un campus universitario". (2008). http://www.criptored.upm.es/guiateoria/gt_m538c.htm. (acceso octubre 6, 2008).

[8] Díaz, Toni de la Fuente. "Administración de FreeRADIUS vía Web". (2006). http://flossic.loba.es/Contenidos/actas/phpradmin.pdf. (acceso octubre 14, 2008).

[9] "Project The FreeRADIUS Server". (2008). http://freeradius.org. (acceso octubre 14, 2008).

[10] Valdés Jimenez, Alejandro. "FreeRADIUS + WPA + EAP + TLS". http://deb.utalca.cl/public/imagenes/radius.pdf. (acceso octubre 14, 2008).