soluciones de seguridad en redes inalámbricas

María Victoria Figueroa Domínguez
Subdirectora General Adjunta del Ministerio de la Presidencia

Daniel Merino Mateo
Tecnocom

En este artículo se pretende exponer diferentes alternativas de seguridad en entornos inalámbricos adaptadas a un entorno de red de área local disponible en un entorno administrativo, de tal forma que se puedan conjugar las redes existentes hasta el momento con la instalación de nuevas redes inalámbricas. Se describen los elementos que participan en la solución así como los protocolos de red y funcionalidades necesarias para garantizar la seguridad de la red inalámbrica. Los diferentes factores que influyen en la conexión a través de redes inalámbricas como son principalmente la Autenticación y la encriptación.

Autenticación

Tener una buena solución de autenticación segura a la hora de conectarse a la red es esencial, tanto en entornos de redes de área local cableadas como en entorno de redes inalámbricas, máxime en estas últimas ya que la posibilidad de intrusismo es mayor que en las primeras. La solución elegida para nuestro supuesto para autenticación es la utilización de 802.1X, estándar de autenticación del IEEE para redes inalámbricas y cableadas.

El 802.1X es un estándar que permite el transporte de tramas EAP sobre redes cableadas e inalámbricas (*http://www.ieee802.org/1/pages/802.1X.html*). EAP es el protocolo que realiza la autenticación de los usuarios según un determinado mecanismo, en función de las distintas variantes que existen de este protocolo.

Utilizando 802.1X evitamos la asociación de usuarios no autorizados con cualesquiera de los puntos de acceso de la red. Antes de permitir que un usuario se asocie con un punto de acceso, éste debe proporcionar una identificación (usuario/contraseña, certificado, etc.) válida dentro de la base de datos de usuarios de la red. De esta forma evitamos el posible ataque a elementos de red por parte de cualquier usuario no autorizado.

En la **FIGURA 1** se presenta un diagrama del flujo de autenticación que se sigue antes de dar acceso a la red a un usuario autorizado:

Existen múltiples variantes de EAP, entre las cuales destacan:

* **EAP-LEAP:** protocolo de autenticación propietario de *Cisco Systems* que permite la autenticación de usuarios y servidor sin la necesidad de utilizar certificados digitales, únicamente utiliza autenticación mediante usuario/contraseña, la cual puede ser válida dentro de la base de datos de otro servidor (*Windows NT, Windows Active Directory*, ODBC).

* **EAP- TLS:** estándar de autenticación que utiliza certificados tanto en servidor como en cliente. Utiliza túneles TLS encriptados para el intercambio de claves públicas.
Definido según RFC 2176 (*http://www.ietf.org/rfc2176.txt*) .

Esta es una solución completa basada en certificados; siendo un estándar independiente de la tarjeta del cliente, sistema operativo o RADIUS utilizado.

* **EAP-TTLS:** actualmente en estado de borrador pretende ser una simplificación de EAP-TLS evitando la utilización de certificados en los clientes, utilizando por ejemplo la autenticación de usuario/contraseña del dominio de Windows para autorizar a los clientes. Propuesta de estándar realizada por Funk Software.

* **EAP-PEAP:** propuesta realizada por Cisco y Microsoft para, al igual que EAP-TTLS, simplificar los requisitos necesarios que inicialmente necesita EAP-TLS. Solución válida en entornos Cisco-Microsoft, pero todavía no está soportada por la mayoría de los fabricantes. Solución ajustada para entornos empresariales que aún no disponen de la posibilidad de tener un certificado digital en cada uno de los PCs de la red, realizando la autenticación de usuarios contra un servidor Windows (*Active Directory*, *Windows NT*), RADIUS o incluso contra los puntos de acceso de Cisco (solución limitada a 50 usuarios).

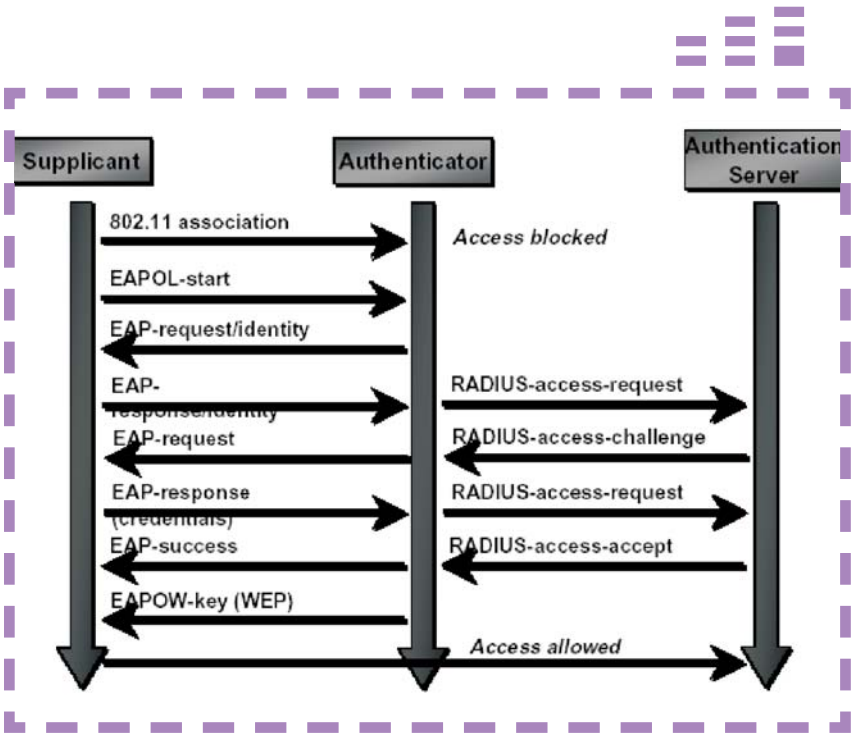

FIGURA 1. Autenticación 802.1X

En la **TABLA 1** se muestra una comparativa de las distintas opciones anteriormente presentadas:

Servidor RADIUS (*Remite Authentication Diel-In User Service*)

Existen multitud de servidores RADIUS en el mercado que se pueden utilizar para la autenticación de los usuarios, la verificación de certificados y la comunicación con las bases de datos de usuarios que les autentifican en la red local cableada existente (*Windows Active Directory*). Es conveniente utilizar un servidor RADIUS donde esté garantizada la completa compatibilidad con los puntos de acceso que se vayan a instalar. En el caso del supuesto que nos ocupa se ha optado por un servidor *Cisco Access Control Server* (ACS) ya que es completamente compatible con los puntos de acceso actualmente instalados puesto que ambos son del mismo fabricante (Cisco Systems), y del hecho de que uno de los protocolos de autenticación de usuarios (EAP-PEAP) está desarrollado también por Cisco Systems en colaboración con Microsoft.

Cifrado

Otro factor importante que influye en la seguridad de las redes inalámbricas es la necesidad de encriptar el contenido de la información que se trasfiere a través de la red inalámbrica. En la actualidad existen principalmente dos métodos de encriptación: WEP y WPA.

Tanto WEP como WPA aseguran que las tramas de los usuarios de la red inalámbrica que viajan están encriptadas según un determinado mecanismo y que en caso de ser capturadas por cualquier intruso, estas tramas son imposibles de descifrar (en la actualidad se han detectado ciertas vulnerabilidades que hacen que determinados mecanismos de encriptación basados en WEP sean vulnerables).

WEP (*Wired Equivalent Privacy*) ha sido hasta el momento el estándar utilizado en todas las redes inalámbricas para la encriptación de datos. WEP está disponibles en distintas variantes

	EAP-LEAP	EAP-TLS	EAP-TTLS	EAP-PEAP
Soporte de RADIUS	Cisco, FreeRadius (Linux), Funk, Interlink, Meetinghouse, Radiator	Cisco, FreeRadius (Linux), Funk, Interlink, Meetinghouse, Radiator, Microsoft	Funk, Interlink, Meetinghouse, Radiator	Cisco, Funk, Interlink, Meetinghouse, Microsoft, Radiator
Soporte en cliente	Cisco, Funk, Meetinghouse	Cisco, Funk, Meetinghouse, Microsoft, Open1X	Alfa-Ariss, Funk, Meetinghouse, Open1X	Funk, Meetinghouse, Microsoft
Sistema Operativos embebidos	-	Windows XP/2000/2003	-	Windows XP/2000/20003
Plataformas soportados con software de terceros	Win32	MacOS X, BSD, Linux, Win32	MacOS X, BSD, Linux, Win32	Win32
Autenticación de servidor	Password Hash	Clave pública (certificado)	Clave pública (certificado)	Clave pública (certificado)
Autenticación de cliente	Password Hash	Clave pública (certificado o tarjeta inteligente)	CHAP, PAP, MS-CHAP (v2), EAP	Cualquier EAP, como EAP-MS-CHAP (v2) o clave pública
Claves dinámicas	Sí	Sí	Sí	Sí

TABLA1. Comparativa de las distintas opciones de EAP

en función del grado de encriptación utilizado (64 bits, 128 bits)

En diversos foros de seguridad se han anunciado vulnerabilidades existentes en WEP que hace desaconsejable la utilización de este mecanismo para la encriptación de datos en aquellos entornos donde la seguridad es imperativa.

WEP fue diseñado para imponer tres metas de seguridad fundamentales:

* **Confidencialidad:** El objetivo fundamental de WEP es evitar escuchas fortuitas.

* **Control de acceso:** Un segundo objetivo del protocolo es proteger el acceso a la infraestructura de red inalámbrica. El estándar 802.11 incluye una característica opcional para desechar aquellos paquetes que no estén apropiadamente encriptados usando WEP, a la vez que los fabricantes promocionan la habilidad de WEP para proveer control de acceso.

* **Integridad de datos:** Un objetivo relacionado es prevenir la manipulación de los mensajes transmitidos; el campo *checksum* se incluye con este propósito.

En los tres casos, la afirmación de la seguridad del protocolo "reside en la dificultad de obtener la clave pública por medio de ataques por fuerza bruta".

Hoy día hay dos clases de implementación WEP: la clásica, tal cual viene estipulada en el estándar, y una versión extendida desarrollada por algunos fabricantes para proveer claves más largas. El estándar WEP especifica el uso de claves de 40 bits, así elegidas por las restricciones aplicadas por el gobierno norteamericano para la exportación de tecnología criptográfica vigentes cuando el protocolo fue definido. Esta longitud de clave es lo suficientemente corta como para realizar ataques prácticos de fuerza bruta a individuos y organizaciones, con recursos de cálculo bastante modestos. No obstante, es trivial extender el protocolo para usar claves más largas, y de hecho algunos fabricantes ofrecen en sus productos versiones de 128 bits. Esta extensión convierte en imposibles los ataques por fuerza bruta incluso para el adversario con los mayores recursos, dada la tecnología actual. A pesar de ello, hay atajos que permiten evitar el uso de ataques por fuerza bruta a la clave para descubrir la misma, lo que convierte en inseguras incluso a las implementaciones WEP de 128.

WPA (*Wi-Fi Protected Access*) viene a ser el sustituto de WEP ya que este último se ha demostrado muy vulnerable. La nueva especificación estará basada en el nuevo estándar IEEE 802.11i y en principio no requerirá un cambio de *hardware*.

En la nueva protección WPA la cadena ASCII que se introduce sirve de semilla para una clave en constante rotación, de forma que cada paquete de información lleva una clave completamente diferente a los anteriores. WPA necesita que todos los dispositivos de red sean compatibles con el nuevo sistema. Si uno de los adaptadores inalámbricos no está preparado, la red entera se encriptará utilizando el antiguo WEP.

WPA utiliza 802.1X y EAP como base de su mecanismo de autentificación, haciendo uso de un servidor RADIUS para la validación de los usuarios. Aún así, existe un modo de trabajo denominado WPA-PSK (*WPA Pre-Shared Key*) que únicamente requiere una password para acceder al punto de acceso. Este modo de trabajo está preparado para ser utilizado en entornos domésticos o pequeñas empresas.

WPA utiliza TKIP y MIC para distribuir claves dinámicas temporales a los clientes y comprobar la integridad de las tramas recibidas (evita que se modifique tramas capturadas y se reenvíen).

En la actualidad la asociación Wi-Fi Alliance ha propuesto una segunda versión de WPA denominada WPA-2 (basada en el estándar de seguridad ya ratificado 802.11i) que pretende mejorar la seguridad proporcionada por WPA. Si bien la definición está preparada, aún son pocos los fabricantes que incluyen esta segunda versión.

Utilización de IPsec

Otra posible forma de autenticar a los usuarios y de cifrar las comunicaciones está basada en la utilización de *IPsec*. Si bien ésta puede ser una solución válida y totalmente segura. A continuación se enumeran las principales razones por las que se considera como una segunda alternativa la utilización de IPsec como método de acceso a la red corporativa para los usuarios inalámbricos:

1. Implica la utilización de un software específico para establecer la conexión, por lo tanto se complica el modelo de acceso de los clientes a la red pues se les obliga a tener conocimiento de este software de acceso.

2. Determinados protocolos no viajan por túneles IPsec. Estos túneles sólo transportan tráfico IP y no otros protocolos que pueden estar corriendo en la actualidad sobre la red ya existente.

3. El hecho de disponer de un terminador de túneles IPsec actualmente podría simplificar y abaratar la solución final, pero se debería garantizar la conexión directa de los usuarios inalámbricos hacia la red pública definida en el terminador ya existente y con un rango de direcciones enrutable desde ese interfaz (probablemente direccionamiento público). En caso de no poder disponer del actual terminador de túneles o de verificarse inviable su utilización, obligaría a la compra de otro terminador exclusivamente dedicado para los usuarios inalámbricos de la red.

4. En cualquier caso sería necesario asignar direcciones mediante un servidor DHCP (en caso de utilizar direccionamiento dinámico) y se realizaría NAT (traducción de direcciones IP) en el terminador de túneles. Esto supone que determinadas aplicaciones no funcionen correctamente, lo cual supone una degradación del servicio ofrecido a los clientes inalámbricos

En la actualidad la asociación Wi-Fi Alliance ha propuesto una segunda versión de WPA denominada WPA-2 que pretende mejorar la seguridad proporcionada por WPA

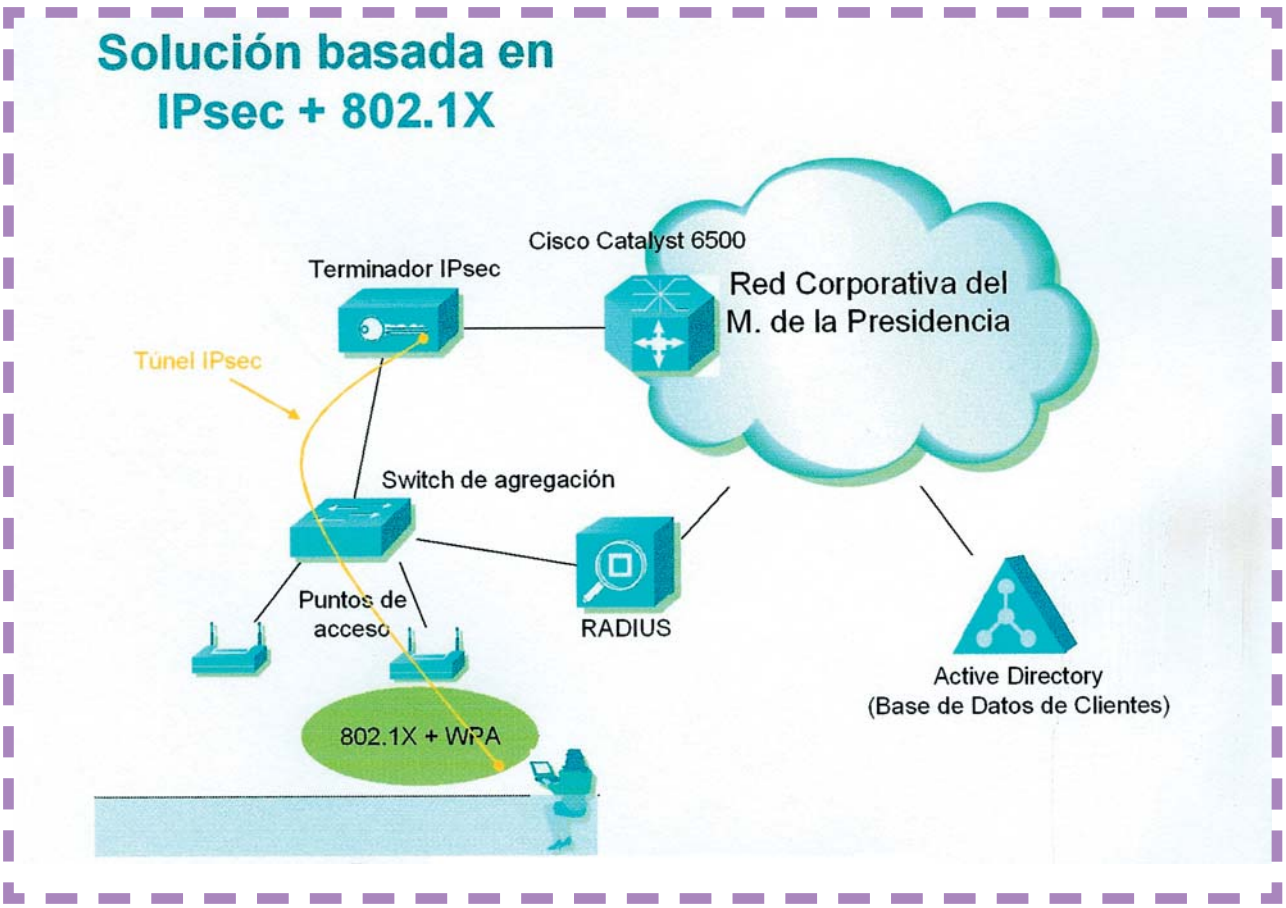

FIGURA 2. Solución basada en IPsec + 802.1X

frente a los cableados.

En caso de utilizar esta solución, existen dos posibles alternativas:

* No securización en el entorno inalámbrico

* Securización en el entorno inalámbrico

Si no se securiza el entorno inalámbrico la solución resulta más sencilla de implementar y de mantener dado que evitamos la necesidad de gestionar y operar dos redes seguras sobre la misma infraestructura, por un lado la seguridad de la red inalámbrica, propiamente dicha (802.1X y WPA), y por otro la securización con IPsec.

La utilización de ambos entornos seguros (802.1X y WPA junto a IPsec) nos garantiza una total confidencialidad de los datos de los usuarios y nos permiten autenticar de forma completamente segura a los usuarios que acceden a la red corporativa, a costa de aumentar la sobrecarga de información de los paquetes enviados y recibidos y de modificar el método de acceso de los usuarios a la red.

En la **FIGURA 2** presentamos un esquema de la arquitectura de red necesaria para implementar la solución basada en la securización del entorno inalámbrico combinada con IPsec.

Las fases por las que debe pasar un usuario utilizando esta alternativa serán las siguientes:

1. Autenticación del usuario utilizando 802.1X contra el servidor RADIUS (base de datos de usuarios alojada en el Active Directory o bien utilizando certificados digitales, en una segunda fase).

2. Encriptación de la comunicaciones inalámbricas mediante WPA.

3. Obtención de una dirección IP mediante DHCP o bien utilización de direccionamiento estático en los PCs de los clientes.

4. Lanzar un túnel IPsec contra el terminador de túneles.

5. Autenticación del usuario contra el *Active Directory* (o bien utilizando certificados digitales, en una segunda fase)

6. Asignación de una dirección IP al cliente para el tráfico que viaje dentro del túnel *IPsec*.