Una arquitectura de control de acceso a redes de área local inalámbricas 802.11

Manuel Sánchez Cuenca[1] y Óscar Cánovas Reverte[1]

Resumen— **El auge de las redes inalámbricas de área local ha sacado a la luz toda una serie de deficiencias en lo que a mecanismos de seguridad se refiere. En este artículo se presenta el diseño de una arquitectura de control de acceso para redes inalámbricas basada en el estándar IEEE 802.1X. Dicho sistema hace uso de certificados digitales para proporcionar a los usuarios tanto servicios de autenticación como de autorización. Además, el sistema gestiona también la confidencialidad de la comunicación, integrando el protocolo WEP con el mecanismo de control de acceso.**

Palabras clave—**802.1X, 802.11, control de acceso, autenticación, autorización.**

I. Introducción

Hoy en día es común llegar a un lugar público, como un aeropuerto o un hotel, y encontrarse con una infraestructura de red inalámbrica de área local (WLAN) que ofrece servicio a los usuarios que así lo solicitan.

En relación con la tecnología de transmisión WLAN, en los últimos años han ido apareciendo una serie de estándares o especificaciones que tratan de cubrir las distintas áreas de esta tecnología. El más ampliamente extendido es el estándar IEEE 802.11 [12], aunque también existen otras propuestas alternativas, e incompatibles entre sí, como HiperLAN [7] o Bluetooth [11], este último más enfocado a las redes de área personal. Este tipo de tecnologías ofrecen a los usuarios mayor versatilidad a la hora de acceder a los servicios de red, proporcionando múltiples ventajas en lo que se refiere a mantenimiento de la red, implantación y movilidad de los usuarios. Sin embargo, el uso de un canal compartido y de elementos de acceso a la red cableada directamente accesibles por cualquier persona plantea también ciertos problemas de seguridad que deben ser resueltos, de entre los cuales el control de acceso de usuarios a la red será el eje principal de este artículo.

En general, el mecanismo más utilizado para realizar un control de conexiones ha sido el uso de bases de datos en las que se introducen manualmente los datos de los usuarios autorizados, ya sean sus identificadores de usuario o direcciones MAC. Sin embargo, esta solución presenta problemas de escalabilidad cuando las bases de datos crecen demasiado o los usuarios cambian frecuentemente.

Como se analizará más adelante, existen a día de hoy varias propuestas enfocadas a proporcionar servicios de control de acceso a redes WLAN. Dichas propuestas van desde la provisión de mecanismos de filtrado de direcciones de red o control de identificadores de sesión, hasta arquitecturas completas que proporcionan mayor versatilidad en cuanto a servicios. El trabajo aquí presentado está basado en la especificación IEEE 802.1X [13], un estándar que define claramente las entidades y protocolos necesarios para llevar a cabo procesos de control de acceso a cualquier servicio ofrecido por una red.

802.1X plantea un escenario con tres entidades básicas como son el cliente, el elemento que proporciona la conectividad a la red (punto de acceso) y el servidor de autenticación encargado de averiguar si un determinado cliente ha sido autorizado a hacer uso de dicha red. En lo que respecta a los protocolos que componen la especificación 802.1X, la propuesta es bastante flexible al no limitar los mecanismos de autenticación a ninguna solución concreta, sino que es posible hacer uso de cualquier tipo de especificación convenientemente adaptada al marco 802.1X. Esta flexibilidad nos va a permitir hacer uso de protocolos basados en certificados digitales [9] como elementos fundamentales a la hora de constatar la autenticidad de los participantes.

La importancia del uso de certificados digitales radica en su capacidad para aliviar los problemas de escalabilidad asociados a las soluciones fundamentadas en el uso de bases de datos. Estos elementos permiten que un usuario desconocido para el sistema pueda hacer uso de la red con solo proporcionarle el certificado adecuado. Además en este certificado pueden incluirse ciertos atributos acerca del usuario, como el tiempo máximo que puede utilizar la red, los servicios a los que puede acceder o los recursos que puede utilizar.

El sistema aquí presentado aborda las cuestiones relacionadas con la identificación de clientes que entran en el área de cobertura de un punto de acceso, la especificación del tipo de servicio que el cliente desea obtener de la red, la comprobación por parte del sistema de si dicho cliente ha sido autorizado a disfrutar de los privilegios que solicita, la generación de claves de cifrado de la comunicación entre cliente y punto de acceso (independientes para cada usuario), y el control de la movilidad del usuario. Para ello se han diseñado extensiones para los protocolos básicos del marco 802.1X.

[1] Departamento de Ingeniería y Tecnología de Computadores, Facultad de Informática, Universidad de Murcia. 30071 Murcia. Email:manuel.sanchez@ditec.um.es, ocanovas@ditec.um.es

El resto del artículo se encuentra estructurado de la siguiente forma. En el apartado II se realiza un análisis de las tecnologías implicadas en el desarrollo del sistema. El apartado III detallará el diseño de los protocolos introducidos como extensión al marco 802.1X. A continuación, en el apartado IV se muestran los detalles de la implementación de un prototipo del sistema. Posteriormente, el apartado V recogerá otros trabajos relacionados con nuestra propuesta. Finalmente, el artículo presenta las conclusiones alcanzadas a partir de esta experiencia.

II. ANÁLISIS

A. Objetivo

El objetivo de este estudio es analizar los diferentes componentes necesarios para desarrollar un sistema de control de acceso a redes WLAN basado en autenticación y autorización. Adicionalmente, se desea además contrastar las limitaciones de los sistemas actuales de cifrado de comunicación de cara a plantear también soluciones al respecto.

B. Redes inalámbricas de área local

Ya se ha comentado que en el campo de las redes inalámbricas han aparecido una serie de normas que intentan cubrir todos los ámbitos de su uso. De entre éstas, el estándar IEEE 802.11 [12] es el más extendido en la actualidad.

Este estándar describe una arquitectura basada en unidades elementales, o celdas, donde un conjunto de dispositivos intentan acceder al medio haciendo uso de una misma función de coordinación. Estas unidades pueden conectarse entre sí mediante una red o sistema de distribución. El elemento que sirve de puente entre la red inalámbrica y la red cableada es el punto de acceso, el cual jugará también un papel crucial en el proceso de control de conexiones.

Antes de que un equipo que se conecta a un punto de acceso pueda transmitir los datos, éste debe realizar una fase de asociación en la que da a conocer su identificador al punto de acceso para que éste informe al resto de la red de que dicho equipo se encuentra bajo su área de cobertura. Es tras esta fase cuando debe realizarse el proceso de control de acceso para ver si realmente el cliente tiene permiso para hacer uso de la red.

Uno de los mecanismos utilizados por las redes 802.11 para intentar proporcionar un cierto nivel de seguridad es el cifrado de los datos que se transmiten entre el cliente y el punto de acceso. Para ello se utiliza el protocolo WEP [12], el cual está basado en el uso de un secreto compartido, o clave WEP, entre los dos extremos de la comunicación. Debido a la naturaleza de este mecanismo, principalmente basado en el algoritmo de cifrado RC4 [19], en los últimos años se han descubierto varias vías de ataque [4] que permiten a un intruso descifrar la comunicación protegida mediante WEP. Con la finalidad de solucionar dicho problema, se recomienda el uso de claves de longitud no inferior a 128 bits así como su continua actualización con el fin de limitar la cantidad de información cifrada con la misma clave.

C. IEEE 802.1X

La especificación IEEE 802.1X [13] es un estándar de control de acceso desarrollado por el IEEE que permite utilizar diferentes mecanismos de autenticación. Su funcionamiento se basa en el concepto de puerto, visto éste como el punto a través del que se puede acceder a un servicio proporcionado por un dispositivo, que en este caso será el punto de acceso. En principio todos los puertos está desautorizados, excepto uno que el punto de acceso utiliza para comunicarse con el cliente. Cuando un nuevo cliente entra en su área de cobertura, le pasa al punto de acceso información de autenticación, dependiente del mecanismo utilizado, que éste reenvía al servidor de autenticación. Cuando éste le contesta, si la respuesta es que el cliente puede hacer uso de la red, autoriza un puerto para que lo utilice el cliente. La Figura 1 muestra la estructura general de un sistema IEEE 802.1X.

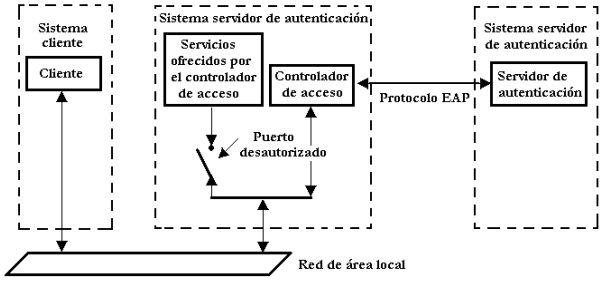


Figura 1. Arquitectura IEEE 802.1X

En esta arquitectura, la información de autenticación se encapsula en el protocolo EAP (Extensible Authentication Protocol) [3], un mecanismo genérico de transmisión de datos de autenticación que puede ser materializado en distintos subprotocolos entre los que, por ejemplo, se encuentra EAP-MD5 [22], que basa la autenticación del cliente en el uso de login y password, o EAP-TLS [1], que se basa en el uso del protocolo TLS [23] y permite autenticación mutua entre los dos extremos. El sistema aquí presentado hará uso de EAP-TLS principalmente por dos motivos: el primero es que que durante la fase de establecimiento de la conexión este protocolo hace uso de certificados X.509 [14] para identificar a las partes, lo cual constituye un mecanismo robusto de autenticación; el segundo es que dicha fase genera una clave compartida por los dos extremos que puede utilizarse para derivar claves para el cifrado de las transmisiones inalámbricas, lo cual es uno de los objetivos de nuestra arquitectura.

Finalmente, los paquetes EAP se transmiten mediante el protocolo EAPOL [12], el cual especifica cómo encapsular los paquetes EAP en una red de área local tanto Ethernet como 802.11.

D. Servidores de autenticación

Aunque en la especificación 802.1X se habla de los servidores de autenticación en términos genéricos, en la práctica se trata de elementos diseñados según los criterios del marco AAA (Authentication, Authorization and Accounting) [15]. Este marco define los elementos básicos necesarios para autenticar usuarios, manejar peticiones de autorización y realizar la contabilidad del sistema. Un servidor AAA debe ser capaz de recibir peticiones, examinar el contenido de dichas peticiones, determinar qué autorización se está pidiendo, recuperar las políticas que necesite de un repositorio, evaluar la petición y obtener la respuesta a la petición, o bien reenviar la petición a otro servidor AAA.

RADIUS [18] es un protocolo encuadrado dentro del marco AAA y utilizado principalmente en entornos donde los clientes son elementos de acceso a la red (como los puntos de acceso). Estos elementos mandan información al servidor cuando un nuevo cliente intenta conectarse, tras lo cual el servidor realiza el proceso de autenticación del usuario y devuelve al elemento de acceso la información de configuración necesaria para que éste trate al cliente de la manera adecuada. Toda la comunicación entre el elemento de acceso y RADIUS se encuentra cifrada mediante un secreto compartido que nunca se transmite por la red. Otro servidor de autenticación AAA es DIAMETER [5], el cual introduce algunas ventajas significativas respecto a RADIUS en materia de gestión de elementos de acceso complejos, si bien se encuentra aún en un estado menos avanzado de definición. La arquitectura presentada en este artículo se basa en el uso de servidores RADIUS dado que satisfacen completamente los requisitos del sistema al tener soporte para el protocolo EAP-TLS

E. Autorización en WLAN

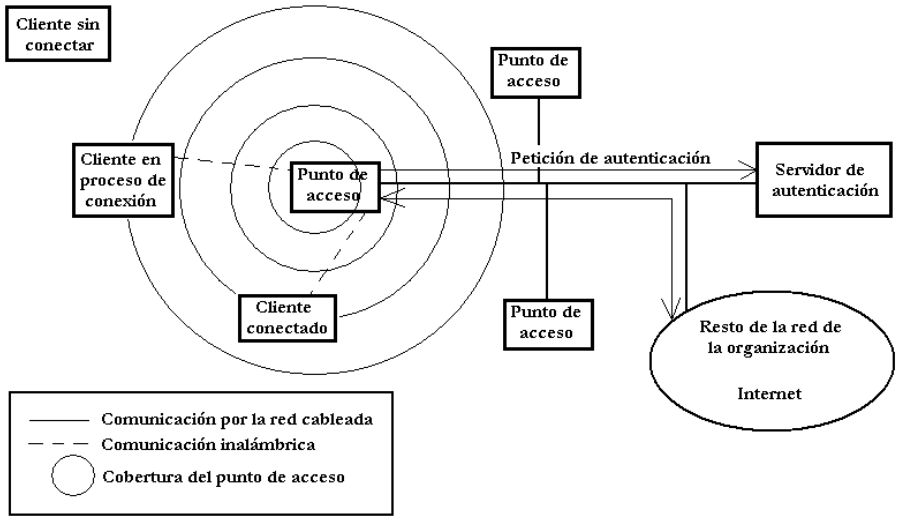
Una de las alternativas para implementar mecanismos de autorización, si no se quiere mantener una base de datos con los permisos de cada usuario, es la utilización de certificados digitales. Un certificado es una estructura que contiene información del usuario en cuanto a identidad o permisos, y que va firmado digitalmente por una entidad de confianza.

Dado que los certificados de clave pública X.509 [14] (los más ampliamente extendidos) se utilizan exclusivamente para propósitos de identidad, se decidió incorporar a nuestra arquitectura el uso de certificados SPKI (Simple Public Key Infrastructure) [6], una especificación que permite plasmar de forma sencilla los privilegios asociados a un usuario individual o a un grupo de usuarios en conjunto. Este tipo de certificados pueden ser utilizados también para representar la pertenencia de un usuario a distintos grupos de privilegios (o roles). La especificación SPKI además define un algoritmo para obtener decisiones de autorización en base a un conjunto de certificados presentados como pruebas, una solicitud de acceso y una política de seguridad del sistema.

III. DISEÑO

Una vez analizado un subconjunto los componentes que formarán parte de la arquitectura, es necesario ilustrar cuál ha sido el diseño de la arquitectura de control de acceso desarrollada.

La Figura 2 muestra un entorno típico de aplicación de la arquitectura. En ella se pueden ver varios puntos de acceso y un servidor de autenticación conectados mediante un sistema de distribución, y un conjunto de clientes que cuando entran por primera vez en el área de cobertura de un punto de acceso inician el proceso de conexión. Este proceso consta básicamente de tres fases:



autenticación, autorización y distribución de la clave de cifrado WEP. Una vez conectado el cliente, el sistema realizará periódicamente un proceso de renegociación de la clave WEP. Del mismo modo, también gestionará la posibilidad de que el usuario se desplace hacia el área de cobertura de otro punto de acceso, todo ello con el fin de reaprovechar la asociación para que el proceso de conexión a través del nuevo punto de acceso se realice de forma eficiente.

La Figura 3 presenta un esquema de las fases del protocolo, las cuales se detallan en los siguientes subapartados.

A. Fase de autenticación

La primera fase funciona siguiendo el estándar IEEE 802.1X, es decir, cuando el cliente entra en el área de cobertura del punto de acceso, este le pide su identidad, y el cliente se la proporciona.

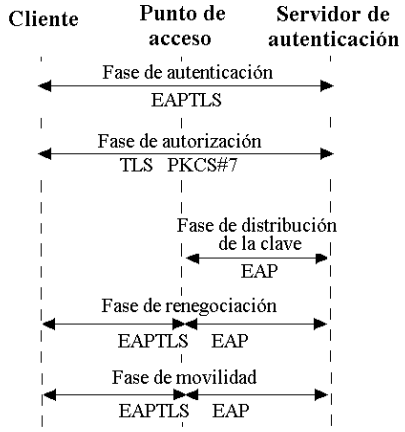


Figura 3. Esquema del protocolo

Tras esta fase inicial se realiza el proceso de establecimiento de conexión TLS entre los extremos, donde según el estándar tanto el cliente como el servidor de autenticación se autentican mutuamente mediante certificados X.509 y negocian los parámetros de configuración necesarios para establecer el canal de comunicación seguro. En nuestra arquitectura hemos relajado el criterio de la autenticación mutua hasta el punto de poder configurar si el cliente debe también desvelar su identidad, proporcionando por tanto también soporte para escenarios en los que el anonimato sea un requisito.

Una vez terminada la negociación, se establece un canal TLS entre el cliente y el servidor de autenticación basado en la posesión por ambas partes de un secreto compartido (Master Secret) que posteriormente se utilizará para derivar la clave WEP.

B. Fase de autorización

En esta fase, tal y como muestra la figura 4, el cliente indica al servidor de autenticación cual es el tipo de conexión que desea en cuanto al ancho de banda requerido y el tiempo que va a estar conectado, junto con los certificados SPKI que demuestran que dicho usuario está autorizado a realizar el uso de la red que pide. Entonces el servidor evalúa los certificados y comprueba si todo es correcto y si el nivel de privilegios del cliente es el necesario, continuando con el protocolo si todo va bien y desautorizando al cliente a acceder a la red si hay algún problema. De esta forma no es necesario acceder a ninguna base de datos de usuarios para comprobar los permisos de los mismos, sino que sólo se necesita confiar en las entidades emisoras de dichos certificados de autorización.

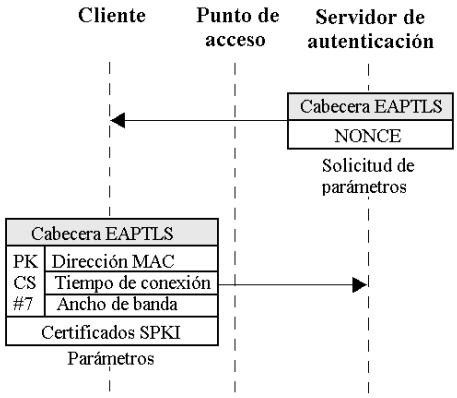


Figura 4. Fase de Autorización

Los parámetros del cliente se mandan en una estructura firmada PKCS#7 [21], de manera que el servidor de autenticación pueda estar seguro de que nadie ha modificado estos parámetros. Además, toda la información relativa a la autorización del cliente, parámetros y certificados, se manda a través del canal TLS establecido anteriormente, de manera que solo pueden haber sido enviados por parte del cliente con el que se ha iniciado el proceso de conexión. Dicha estructura PKCS#7 contiene el certificado del cliente con el que se ha realizado la firma para que el servidor pueda verificar que la firma es correcta. En el mensaje mediante el cual el servidor le pide al cliente sus parámetros de conexión, se incluye un identificador de 4 octetos aleatorio, que posteriormente se utilizará para derivar la clave WEP junto con la dirección MAC del punto de acceso y la clave maestra de la conexión TLS anteriormente establecida.

C. Fase de distribución de clave

En esta fase del protocolo, representada en la figura 5, únicamente participan el punto de acceso y el servidor de autenticación, y consiste en que éste último le pase al primero un descriptor de la clave WEP que debe utilizar con el cliente, así como el tipo de servicio que el cliente espera que se le ofrezca. Esta clave WEP la habrá generado el servidor como resultado de una función de resumen digital MD5 [20] aplicada sobre la concatenación de la clave maestra generada por EAP-TLS, la dirección MAC del punto de acceso, y la carga *nonce* comentada anteriormente.

Por su parte, el punto de acceso debe comprobar que en su situación actual puede soportar las necesidades del nuevo cliente, es decir debe comprobar que la suma total del ancho de banda necesitado por todos los usuarios que actualmente hay conectados, junto con el requerido por el nuevo cliente, no sobrepase su capacidad; y que vaya a estar disponible el tiempo que el cliente requiere; informando al servidor de autenticación sobre la decisión que tome.

Tras estas fases, el proceso de conexión ha terminado, y si todo se ha realizado correctamente, el servidor de autenticación notifica al punto de acceso la autorización por su parte a que el cliente haga uso de la red. El punto de acceso traslada entonces al cliente esta decisión para

que inicie la comunicación. El cliente, que habrá generado la misma clave WEP que obtuvo el punto de acceso, puede comenzar a hacer uso de la red, con la garantía de que sus mensajes son sólo descifrables por el punto de acceso, dado que la clave WEP generada es distinta para cada usuario.

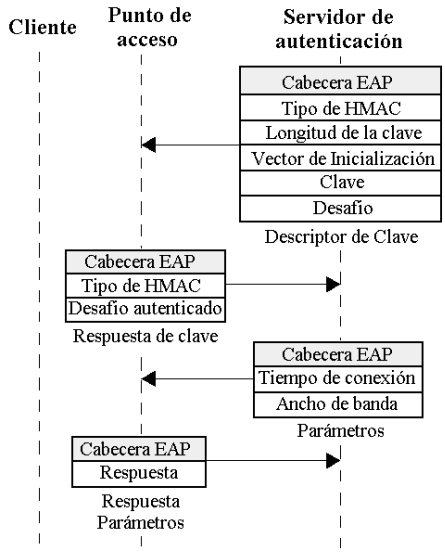


Figura 5. Fase de distribución de claves y parámetros

En este punto del diseño hay que dejar una puerta abierta a una probable modificación futura, ya que es posible que al aumentar la potencia de los ordenadores, una clave WEP de hasta 16 octetos (tamaño del resumen MD5) no proporcione suficiente seguridad, por lo que el protocolo dejaría de ser seguro. Por ello, en el caso de necesitar una clave WEP de mayor tamaño, podría utilizarse el método de extensión de longitud de claves mostrado en la Figura 6.

$$WEP_0=MD5(clave, MAC, nonce)$$
$$WEP_n=WEP_{n-1} \,||\, MD5(clave, MAC, nonce, WEP_{n-1})$$

Figura 6. Obtención de la clave WEP

D. Fase de renegociación

Periódicamente, y dependiendo esta periodicidad del nivel de seguridad que quiera el usuario, es posible renegociar la clave WEP que se está utilizando para cifrar la comunicación entre el cliente y el punto de acceso. Para ello, el cliente inicia un proceso de renegociación de conexión TLS. En esta ocasión, no será necesario que el cliente mande sus parámetros, a no ser que quiera cambiarlos, sino que únicamente se realiza esta fase para indicar al cliente cual es la nueva cadena aleatoria para generar la clave WEP.

De esta manera al terminar el nuevo proceso de conexión, tanto el punto de acceso como el cliente tendrán la nueva clave WEP a utilizar para cifrar sus comunicaciones.

E. Fase de movilidad

Esta fase se apoya en la anterior, ya que cuando un cliente detecta que está en el área de cobertura de un nuevo punto de acceso, en lugar de iniciar el proceso de conexión descrito desde el principio, inicia un proceso de renegociación de conexión TLS. Al basarse la nueva conexión en la anterior, la generación del secreto compartido se puede realizar de forma más ligera, y además se evita que el servidor de autenticación tenga que validar de nuevo al usuario. Una consecuencia directa es también que de forma automática se inicia la fase de renegociación de clave WEP, lo cual implica un cambio de la misma para trabajar con el nuevo punto de acceso.

IV. Implementación

La implementación del prototipo de este protocolo se ha basado en una serie de aplicaciones y librerías ya existentes a las que se le ha añadido el soporte para las nuevas fases.

A. HostAP

HostAP[2] es un driver para Linux que permite que un ordenador con una tarjeta inalámbrica funcione como punto de acceso, además de incluir una implementación del estándar IEEE 802.1X.

En cuanto a las modificaciones realizadas sobre este software, se han centrado en añadirle soporte para la fase de generación de claves WEP. Durante el resto del protocolo, este dispositivo únicamente funciona como elemento puente, es decir reenvía todo lo que le llega desde el cliente al servidor de autenticación y viceversa.

B. XSupplicant

XSupplicant [17] es una aplicación que pertenece al proyecto Open1X, un intento de obtener una implementación completa y abierta del estándar IEEE 802.1X para Unix, pero que actualmente solo tiene disponible el cliente.

Las modificaciones realizadas sobre XSupplicant se centran básicamente en la fase de autorización, la fase de renegociación de clave y la de movilidad. Una vez que todo el proceso de conexión ha terminado y XSupplicant recibe la autorización de hacer uso de la red, es necesario establecer la clave WEP de la forma ya descrita.

C. FreeRADIUS

FreeRADIUS[3] es una implementación abierta para UNIX de RADIUS, que tiene la ventaja de que se ha comprobado su interoperabilidad con XSupplicant.

La mayor parte de los cambios realizados se han producido en FreeRADIUS debido a que, ya sea con el cliente o con el punto de acceso, el servidor de autenticación siempre está implicado en alguna fase del protocolo.

D. OpenSSL

OpenSSL[4] es una implementación de SSL de código abierto. Esta librería es necesaria para poder instalar

[2] http://hostap.epitest.fi
[3] http://freeradius.org

tanto FreeRADIUS como XSupplicant, ya que al usar EAP-TLS necesitan de una implementación de TLS que aquí se proporciona. Además, también se ha empleado como librería criptográfica con soporte para PKCS#7 y resúmenes digitales.

V. Trabajo relacionado

El control de acceso a redes WLAN es un campo de investigación bastante abierto. Encuadrados dentro del marco 802.1X han surgido varios protocolos EAP, además de los comentados EAP-MD5 y EAP-TLS, que ofrecen distintos niveles de seguridad. Por ejemplo, el protocolo LEAP (Lightweight EAP) [2], al igual que nuestra arquitectura, también incluye mecanismos para generar claves únicas de cifrado, si bien tiene grandes limitaciones al estar basado en el modelo EAP-MD5. Otra propuestas son EAP-TTLS [10] y PEAP [2], las cuales son capaces de trabajar con varios tipos distintos de datos de autenticación, si bien no tienen soporte para autorización, renegociación o movilidad.

En lo que respecta a arquitecturas completas de control de acceso, y no sólo a protocolos de autenticación EAP, existen otras propuestas como el sistema NoCatAuth [8], basado en el uso del Web como medio de autenticación frente al punto de acceso, o como la propuesta de Nikander [16], basada en 802.1X aunque demasiado limitada al filtrado de direcciones MAC como principal medio de control. La principal diferencia de la arquitectura que aquí se presenta respecto a estas otras propuestas está en el uso de la certificación digital y en el tratamiento global a todas las fases involucradas en el proceso de control de conexiones, no sólo la autenticación sino también la gestión de claves de cifrado, la especificación de la calidad de servicio deseada y la gestión de la movilidad.

VI. Conclusiones

Este artículo ha presentado una arquitectura de control de acceso a redes 802.11 basada principalmente el marco 802.1X. Partiendo de elementos básicos ya existentes, el sistema incorpora el uso de certificados digitales para especificar de forma robusta el tipo de servicio que puede obtener cada usuario de la red. Este esquema distribuido de gestión de autorizaciones permite aliviar los problemas derivados de la gestión centralizada de datos de usuarios, ya que basta con establecer relaciones de confianza entre las entidades emisoras de estos certificados y los servidores de autenticación del sistema. Además, la arquitectura presenta también servicios orientados a la gestión de claves de cifrado, únicas para cada usuario, al igual que trata de forma eficiente la posible movilidad de los usuarios o la necesidad de renegociar periódicamente las claves WEP.

VII. Referencias

[1] B. Aboba, D. Simon, *PPP EAP TLS Authentication Protocol*, RFC 2716, Octubre 1999

[2] H. Anderson, S. Josefson, G. Zorn, D. Simon y A. Palekar. *Protected EAP Protocol (PEAP),* IETF draft, 2002

[3] L. Blunk, J. Vollbrecht, *Extensible Authentication Protocol (EAP)*, IETF RFC 2284, Marzo 1998

[4] Nikita Borisov, Ian Goldberg, and David Wagner. *Intercepting mobile communications: The insecurity of 802.11*. In Proceedings of MOBICOM 2001, 2001.

[5] P. R. Calhoun, J. Arkko, E. Guttman, G. Zorn, J. Loughney, *Diameter Base Protocol*, IETF draft, Diciembre 2002

[6] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, *SPKI Certificate Theory*, IETF RFC 2693: , Septiembre 1999

[7] ETSI TS 101 475 V1.1.1, *Broadband Radio Access Networks (BRAN); HIPERLAN Type 2*; April 2000.

[8] Rob Flickenger, *NoCatAuth: Authentication for Wireless Network,* White Paper, http://nocat.net/nocatrfc.txt

[9] W. Ford, M. S. Baum, *Secure Electronic Commerce. 2nd Edition*, Ed. Prentice Hall, 2001.

[10] P. Funk y S. Blake-Wilson. *EAP Tunneled TLS Authentication Protocol (EAP-TTLS)*, IETF draft, 2002.

[11] J. Haartsen, M. Naghshineh, J. Inouye, O. Joeressen, y W. Allen, W. Bluetooth: Vision, goals, and architecture. *Mobile Computing and Communications Review* 2, 38-45. Octubre 1998.

[12] LAN MAN Standards Committee of the IEEE Computer Society, *Wireless LAN medium access control (MAC) and physical layer (PHY) specification*, IEEE, New York, NY, USA, IEEE Std 802.11-1997 edition, 1997.

[13] IEEE Draft *P802.1X/D11: Standard for Port based Network Access Control*, LAN MAN Standards Committee of the IEEE Computer Society, March 27, 2001.

[14] ITU-T. ISO/IEC 9594-8, *The Directory: Authentication Framework*, 2001. Recommendation X.509

[15] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, *Generic AAA Architecture*, IETF RFC 2903, Agosto 2000

[16] P. Nikander, Authorization and charging in public WLANs using FreeBSD and 802.1x, *in Proceedings of the Freenix track: 2002 USENIX Annual Technical Conference*, Monterey, CA, June 10-15, 2002.

[17] N. Petroni, B. D. Payne, B. Arbaugh, and A. Mishra, *Open1x project home page*, University of Maryland, February 2002, http://www.open1x.org,

[18] C. Rigney, S. Willens, A. Rubens, W. Simpson, *Remote Authentication Dial In User Service (RADIUS),* IETF RFC 2865, Junio 2000

[19] R. L. Rivest. *The RC4 Encryption Algorithm*. RSA Data Security, Inc., Marzo 12, 1992. (Propietario).

[20] R. Rivest, *The MD5 Message-Digest Algorithm*, IETF RFC 1321, Abril 1992.

[21] RSA Security, *PKCS#7: Cryptographic Message Syntax, Version 15*, Noviembre 1993

[22] W. Simpson, *PPP Challenge Handshake Authentication Protocol (CHAP)*, IETF RFC 1994, Agosto 1996.

[23] S. Thomas, *SSL and TLS Essentials. Securing the Web*, Ed. Wiley, 2000

[4] http://www.openssl.org