Introducción

La aparición en el mercado de las redes inalámbricas ha introducido un nuevo lenguaje a la hora de hablar de redes de datos. Poder identificar correctamente la gran cantidad de nuevas siglas y acrónimos es una ventaja importante a la hora de discutir una propuesta concreta.

Debido a esto, hemos considerado útil presentar aquí los conceptos más importantes que se utilizan en este documento, así como un resumen del estado en que se encuentra esta tecnología en la actualidad.

Actualmente existen tres estándares de redes inalámbricas (en adelante wi-fi). Estos estándares determinan los detalles físicos de transmisión y recepción, como la velocidad de los datos, la banda radio donde operan y las potencias máximas de emisión:

- 802.11b: Hasta 11Mbps sobre banda 2,4Ghz
- 802.11g: Hasta 54Mbps sobre banda 2,4Ghz
- 802.11a: Hasta 54Mbps sobre banda 5Ghz

Estos estándares han sido aprobados para su uso en España, con el detalle de que para redes 802.11a los equipos que se instalen han de funcionar en modo 'workgroup' para interiores, y no han de sobrepasar la potencia de emisión de 1W.

Seguridad WEP

En redes wi-fi, el concepto de la seguridad se extiende más allá de lo que representaba en redes cableadas. El hecho de poder acceder a tráfico de red sensible sin ser necesaria una presencia física, obliga a extremar las medidas de seguridad en entornos corporativos.

Por ello, el primer estándar wi-fi (802.11b) incorpora desde su origen un sistema de seguridad denominado WEP (Wired Equivalent Privacy), basado en la encriptación de la información. De todas formas, la popularización de las redes wi-fi puso de manifiesto ya en sus inicios que WEP presentaba una serie de vulnerabilidades, debido principalmente al uso de claves estáticas de pocos bits y a un sistema de autenticación débil, que lo hacían poco útil para redes corporativas.

Para contrarrestar estos problemas aparecieron en el mercado soluciones basadas en dos enfoques complementarios:

- Autenticación 802.1x con claves dinámicas más largas.
- Redes privadas virtuales entre los clientes inalámbricos y la red local.

Seguridad WPA

Si bien la utilización de estas alternativas proporcionaban una primera solución al problema de la seguridad en redes inalámbricas, también presentaban una serie de desventajas que las hacían poco viables, como:

- Desarrollos propietarios.
- Nivel de seguridad limitado intrínsicamente por la debilidad de WEP.
- Poca escalabilidad.

Para dar una respuesta final a este problema, el IEEE comenzó en 2002 a desarrollar un nuevo estándar de seguridad para redes wi-fi, denominado 802.11i, con el objetivo de que cumpliera todos los requisitos de

seguridad necesarios para ser aplicable tanto en entornos corporativos como en entornos PYME y domésticos. Según el IEEE, está previsto que este estándar sea aprobado en el Q1 del 2004.

El hecho de que 802.11i no esté disponible hasta bien entrado el 2004, unido a la presión del mercado, hizo que la Wi-Fi Alliance se adelantara al IEEE promoviendo entre los principales fabricantes un estándar de-facto, el WPA (Wi-fi Protected Access), que quedó definido a principios de 2003. Este estándar cumple una serie de requisitos básicos:

- Compatible con el futuro 802.11i
- Seguridad fuerte para entornos corporativos y pequeños
- Disponible como actualización software en los equipos existentes

A continuación se presenta un esquema con la comparación entre los tres estándares de seguridad existentes:

	WEP	WPA	802.11i (RSN, WPA2)
Cipher Algorithm	RC4	RC4 (TKIP)	Rijndael (AES-CCMP)
Encryption Key	40-bit	128-bit (TKIP)	128-bit (CCMP)
Initialization Vector	24-bit	48-bit (TKIP)	48-bit (CCMP)
Authentication Key	None	64-bit (TKIP)	128-bit (CCMP)
Integrity Check	CRC-32	Michael (TKIP)	CCM
Key Distribution	Manual	802.1x (EAP)	802.1x (EAP)
Key unique to:	Network	Packet, session, user	Packet, session, user
Key hierarchy	No	Derived from 802.1x	Derived from 802.1x
Cipher Negotiation	No	Yes	Yes
Ad-hoc (P2P) security	No	No	Yes (IBSS)
Pre-authentication (wired LAN)	No	No	Using 802.1x (EAPOL)

Estándares de seguridad inalámbrica

Como se puede ver, WPA incorpora un nuevo sistema de encriptación (TKIP) y de autenticación y distribución de claves (802.1x). Desde Septiembre de 2003, la mayoría de nuevos equipos wi-fi ya soportan (o soportarán antes de 2004) este estándar.

Autenticación de clientes de red

Como hemos comentado, la autenticación en entornos WPA corporativos se basa en 802.1x. Este estándar no define qué autenticación se utilizará, sino cómo se realizará la negociación concreta de una autenticación determinada. Es el protocolo EAP (Extensible Authentication Protocol), incluido en el estándar 802.1x, el que define el procedimiento para realizar esta negociación.

Esto permite que la autenticación en entornos WPA soporte varios métodos diferentes, cada uno con sus propias ventajas e inconvenientes. La clave al implantar WPA en una red wi-fi consiste en decidir el tipo de autenticación que se utilizará, ya que esto determinará los componentes necesarios para ponerla en marcha.

Existen multitud de métodos EAP especificados (alrededor de 40), siendo los más comunes en la actualidad los siguientes:

- EAP-TLS
- EAP-TTLS
- PEAP

En la siguiente figura se observan las principales diferencias entre los tres:

	EAP-TLS (RFC 2716)	TTLS	PEAP
Software			
Client implementations	Cisco, Funk, Meetinghouse, Microsoft, Open1x (open source)	Funk, Meetinghouse	Microsoft
Supported client platforms	Linux, Mac OS X,Windows 95/98/ME, Windows NT/2000/XP	Linux, Mac OS X, Windows 95/98/ME, Windows NT/2000/XP	Windows XP
Authentication server implementations by	Cisco, Funk, HP, FreeRADIUS (open source), Meetinghouse,	Funk, Meetinghouse	Cisco
Authentication methods	Client certificates	Any[1]	Any EAP method[2]
Protocol Operations			
Basic protocol structure	Establish TLS session and validate certificates on both client and server	Two phases: (1) Establish TLS between client and TTLS server (2) Exchange attribute-value pairs between client and server	Two parts: (1) Establish TLS between client and PEAP server (2) Run EAP exchange over TLS tunnel
Fast session reconnect	No	Yes	Yes
WEP Integration	Server can supply WEP key with external protocol (e.g. RADIUS extension)		
PKI and Certificate Processing			
Server Certificate	Required	Required	Required
Client Certificate	Required	Optional	Optional
Cert Verification	Through certificate chain or OCSP TLS extension (current Internet draft)		
Effect of private key compromise	Re-issue all server and client certificates	Re-issue certificates for servers (and clients if using client certificates in first TLS exchange)	
Client and User Authentication			
Authentication direction	Mutual: Uses digital certificates both ways	Mutual: Certificate for server authentication, and tunneled method for client	Mutual: Certificate for server, and protected EAP method for client
Protection of user identity exchange	No	Yes; protected by TLS	Yes; protected by TLS

[1] Currently, CHAP, PAP, MS-CHAP, and MS-CHAPv2 are implemented in addition to EAP.
[2] Only the "generic token card" method is implemented in current shipping products.

Esquemas de autenticación más comunes

El hecho de que el soporte PEAP esté soportado (como un patch descargable) en Windows XP e integrado con el servicio Wireless Zero Configuration y el servidor Radius (IAS) de Windows 2003, hace que, a priori, parezca la solución más interesante a la hora de desplegar redes nuevas en entornos Microsoft que no dispongan ya de una infraestructura PKI consolidada. De todas maneras, esto no es generalizable, y se debe contemplar en cada caso la mejor solución.

Para redes pequeñas y/o domésticas, el estándar WPA también contempla un modo de funcionamiento especial (WPA-PSK) que permite evitar la utilización de un servidor RADIUS y el protocolo 802.1x-EAP correspondiente. Este modo utiliza claves preasignadas (pre-shared keys) localmente en los puntos de acceso y en los clientes de red para realizar la autenticación. Una vez realizada ésta, la encriptación y el cambio dinámico de claves se efectúan de la misma manera que ya se ha comentado (vía TKIP), lo que permite un nivel de seguridad muy superior al conseguido vía WEP a la vez que la dificultad en la implantación resulta mínima.

Esteban Navarro
enavarro@atonsystems.com
Director Técnico
aTon Systems