Comentario técnico: CTC-089
Componente: **WiFi Enterprise Authentication**
Autor: Sergio R. Caprile, Senior R&D Engineer

Revisiones	Fecha	Comentarios
0	14/04/20	

Las redes WiFi hogareñas son relativamente fáciles de administrar. Debido a la escalabilidad del manejo de las cuentas de usuario y los requerimientos de buenas prácticas en seguridad informática, las empresas suelen utilizar el esquema de autenticación empresarial que WiFi provee. Si nuestro desarrollo con soporte WiFi es un producto que puede o va a ser utilizado en un ambiente empresarial, deberíamos tener presente cómo funciona este esquema, qué opciones tenemos, y finalmente cómo configurar nuestro módulo para afrontar el desafío. Idealmente, también deberíamos ser capaces de probar el funcionamiento.

La autenticación en 802.11 WPA2 Enterprise se realiza mediante EAP (Extensible Authentication Protocol), un marco de autenticación que nos permite elegir entre una serie de mecanismos (métodos) de autenticación según lo especificado por IEEE 802.1X (EAPOL, EAP over LAN)[1]. Se realiza entonces, mediante EAP, entre el dispositivo que se conecta a la red, y un servidor RADIUS (Remote Authentication Dial-In User Service); el Access Point actúa sólo como proveedor de comunicación y no interviene en el proceso de autenticación[2].

Entre los protocolos que podemos utilizar, se encuentra MD5, el esquema se denomina EAP-MD5 y es el más simple de los disponibles. Este esquema no provee cifrado, y es bastante vulnerable para varios tipos de ataques, por lo que no se lo suele utilizar en esta forma sino como último eslabón de otro más complejo que describimos más adelante.

EAP comienza a operar una vez establecida la conexión al Access Point, y asume que es transportado en un medio con una cierta seguridad de acceso al mismo, lo cual no es cierto en WiFi; un sistema de radio en el que la autenticación sin claves pre-compartidas debe realizarse sobre un sistema abierto.

A fin de solucionar esto, se desarrolla EAP-TLS (EAP Transport Layer Security), que emplea TLS como transporte y certificados X.509 para autenticar mutuamente a ambos interlocutores y proceder de allí con claves derivadas a encriptar la comunicación. Dado que esto requiere la existencia de una CA (Certification Authority) para generar los certificados y probablemente una estructura de distribución para hacerlos llegar a sus destinatarios, se han desarrollado alternativas más simples que permitieran usar un sistema del tipo usuario/password dentro de una conexión segura y protegida como este mismo túnel TLS.

Así, EAP-TTLS (EAP Tunneled TLS) primero puede realizar un proceso de identificación elemental, luego pasa a una fase de autenticación TLS que no requiere certificado de parte de quien se conecta (pero puede utilizarlo)[3] y finalmente establece un túnel TLS. Dentro de este túnel se transporta un nuevo protocolo de autenticación que hará la identificación final del cliente mediante un esquema usuario/password. Dicho protocolo puede ser el mencionado EAP-MD5, aunque el más utilizado es MSCHAPv2.

De modo similar encontramos a PEAP (Protected EAP), que es EAP dentro de un túnel TLS. Un primer EAP, externo, permite establecer un túnel TLS sobre el cual se transporta un segundo EAP interno. Las credenciales del EAP externo son irrelevantes. El EAP interno a su vez transporta el protocolo de autenticación propiamente dicho; el más comúnmente utilizado es MSCHAPv2.

A modo de recapitulación, tenemos las siguientes opciones:

- **EAP-TLS** (considerado uno de los esquemas más seguros, y el más utilizado)

1 dado que fue originalmente desarrollado para operar en IEEE 802.3 Ethernet
2 Si bien un Access Point físico, producto, puede incorporar internamente un servidor RADIUS, nos referimos al concepto del punto de acceso, que en sí no requiere de poseer él mismo esta facilidad
3 es decir, autentica al punto de acceso (o a ambos si se agrega el certificado al cliente)

- **PEAP-MSCHAPv2** (el segundo más utilizado)
- **EAP-TTLS/MSCHAPV2**
- **EAP-TTLS/MD5**

Todas permiten autenticar al punto de acceso, y dependiendo de la implementación opcionalmente autentican también al usuario. En algunas implementaciones de EAP-TLS se requiere de forma obligatoria el certificado del usuario.

El proceso de autenticación, simplificado, se realiza mediante una operación basada en el certificado que para ser revertida es necesario conocer la clave privada. El servidor RADIUS envía al cliente su certificado. Este certificado es primero validado mediante la firma de la CA que contiene, de la cual se posee el certificado, y luego se procede a autenticar que quien lo envía es quien dice ser mediante un procedimiento como el mencionado. Todas las claves y certificados son generados por una CA cuya clave privada debe cuidarse y mantenerse a resguardo. El certificado de la CA se distribuye de modo que todos lo posean, a fin de poder confirmar la integridad del certificado que otro ente envía, pues ha sido firmado por la CA.

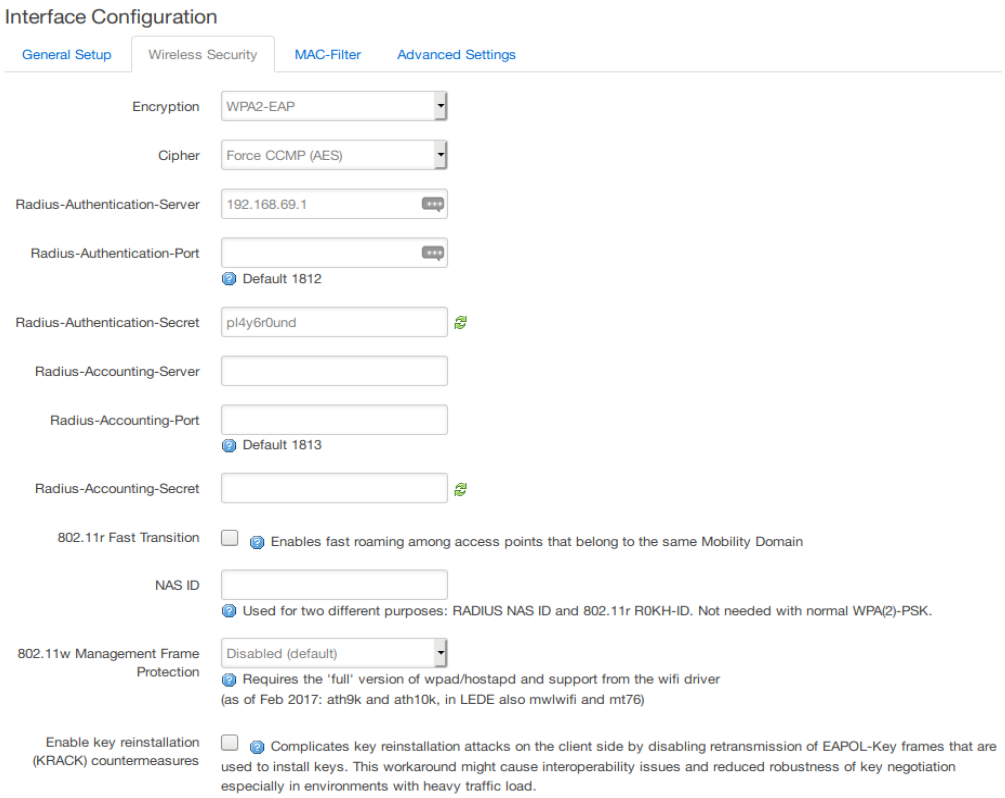
Para verificar el funcionamiento de un dispositivo, si no disponemos de ayuda de parte del área de Sistemas de nuestro cliente o de nuestra empresa, vamos a necesitar:

- un servidor RADIUS (idealmente *freeradius*, o en su defecto *hostapd*)
- una aplicación para verificar el funcionamiento de la configuración del servidor RADIUS (*eapol_test*[4])
- certificados X.509 (OpenSSL[5] o easy-rsa2[6], que viene con algunas distribuciones de OpenVPN)[7]
- un Access Point con capacidad de Enterprise Authentication (idealmente hardware soportado por *LEDE*)

A continuación:

1. En el servidor RADIUS guardaremos la clave privada (radius.key) y el certificado (radius.crt), junto con el certificado de la CA (CA.crt).
2. En los dispositivos guardaremos el certificado de la CA (CA.crt), la clave privada del usuario (nombredelusuario.key) y su certificado (nombredelusuario.crt)
3. Configuramos el servidor RADIUS[8]
    1. *clients.conf*, configuramos usuario, password, y dirección IP del Access Point. En el esquema provisto, deberemos modificar al menos la dirección IP y tomar nota de la clave para cargarla en el Access Point
    2. *users* (*mods-config/files/authorize*), configuramos el nombre de usuario y su password. En este esquema hemos configurado al usuario “bob” con clave "hello"
    3. *mods-available/eap*, configuramos las diversas formas de autenticación, las que hemos comentado y muchas más. No debería ser necesario modificar este archivo excepto para algunas pruebas específicas.
4. Comprobamos su correcta configuración corriendo los scripts de *eapol_test* (usando los certificados y claves)
5. El Access Point se configura con su correspondiente nombre de usuario y clave, configurados también en el servidor RADIUS, para derivar a éste el tráfico de autenticación.

4 http://deployingradius.com/scripts/eapol_test/
5 Algunas distribuciones de freeradius incorporan un script que permite generar certificados utilizando OpenSSL, al iniciar por primera vez.
6 https://openvpn.net/community-resources/how-to/#setting-up-your-own-certificate-authority-ca-and-generating-certificates-and-keys-for-an-openvpn-server-and-multiple-clients
7 La generación de certificados excede las posibilidades de este comentario. Hemos incluido un conjunto mínimo elemental de éstos.
8 La configuración de un servidor RADIUS excede ampliamente las posibilidades de este comentario y los conocimientos del autor. Hemos incluido un esquema elemental preconfigurado para ambiente GNU/Linux. https://freeradius.org/



6. Configuramos el dispositivo de acuerdo al método a probar. La configuración de cada dispositivo (cliente, usuario) y la operatoria detallada dependen de cada uno en particular.