WPA+EAP-TLS+FreeRADIUS

Toni de la Fuente [blyx.com]

9 Julio'05

Jornadas Telemáticas

Vallekas - Madrid

WPA+EAP-TLS+FreeRADIUS

Contenido

- Introducción
- WPA
- EAP-TLS
- FreeRADIUS
- Instalación y configuración
- Clientes
- Vulnerabilidades

WPA+EAP-TLS+FreeRADIUS

Introducción

- Manual de instalación disponible en http://blyx.com
- Vamos a aprender a configurar una red wifi de forma segura usando los medios que nos ofrece la tecnología actual:
  - Infraestructura PKI
  - WPA
  - 802.1X (EAP-TLS)
  - RADIUS

WPA+EAP-TLS+FreeRADIUS

Conceptos: PKI

- Public Key Infraestructure
- Clave pública
- Clave privada
- Autoridad de Certificación
- OpenSSL power!!

WPA+EAP-TLS+FreeRADIUS

Conceptos: WPA

- Wireless Protected Access (WPA2 -> 802.11i)
- Mejoras de los protocolos de cifrado
- Soporte protocolo de control de acceso basado en puertos 802.1x

WPA+EAP-TLS+FreeRADIUS

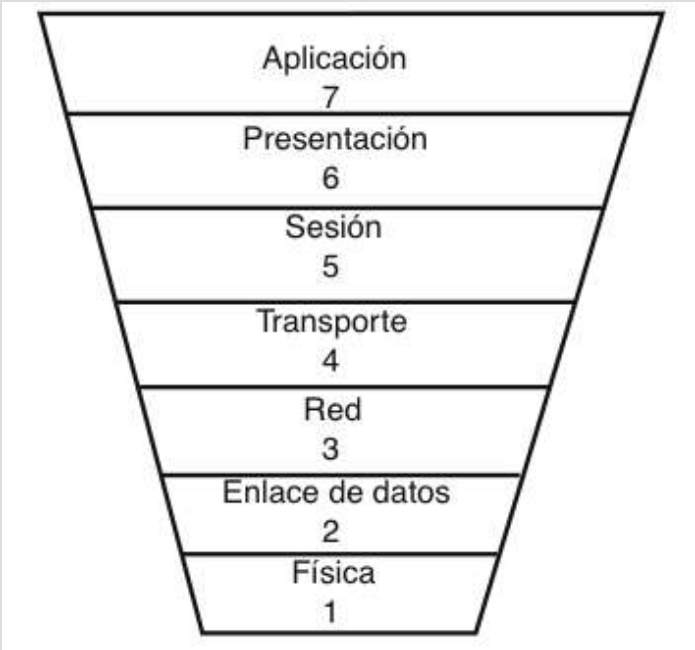
Conceptos: 802.1X

- Es un mecanismo estándar para autenticar centralmente estaciones y usuarios.
- Es un estándar abierto que soporta diferentes algoritmos de encriptación.
- Se apoya en el protocolo de autenticación EAP (Extensible Authentication Protocol), aunque en realidad es EAPoL (EAP over LAN) de forma que se puede usar en redes ethernet, 802.11, Token-Ring y FDDI.
- Requiere cliente (Xsupplicant en Linux), Punto de Acceso y servidor de autenticación.
- EAP es soportado por muchos Puntos de Acceso y por HostAP.
- Antes de la autenticación sólo se permite tráfico 802.1X (petición de autenticación).

WPA+EAP-TLS+FreeRADIUS

Conceptos: 802.1X

- Funciona en capa 2

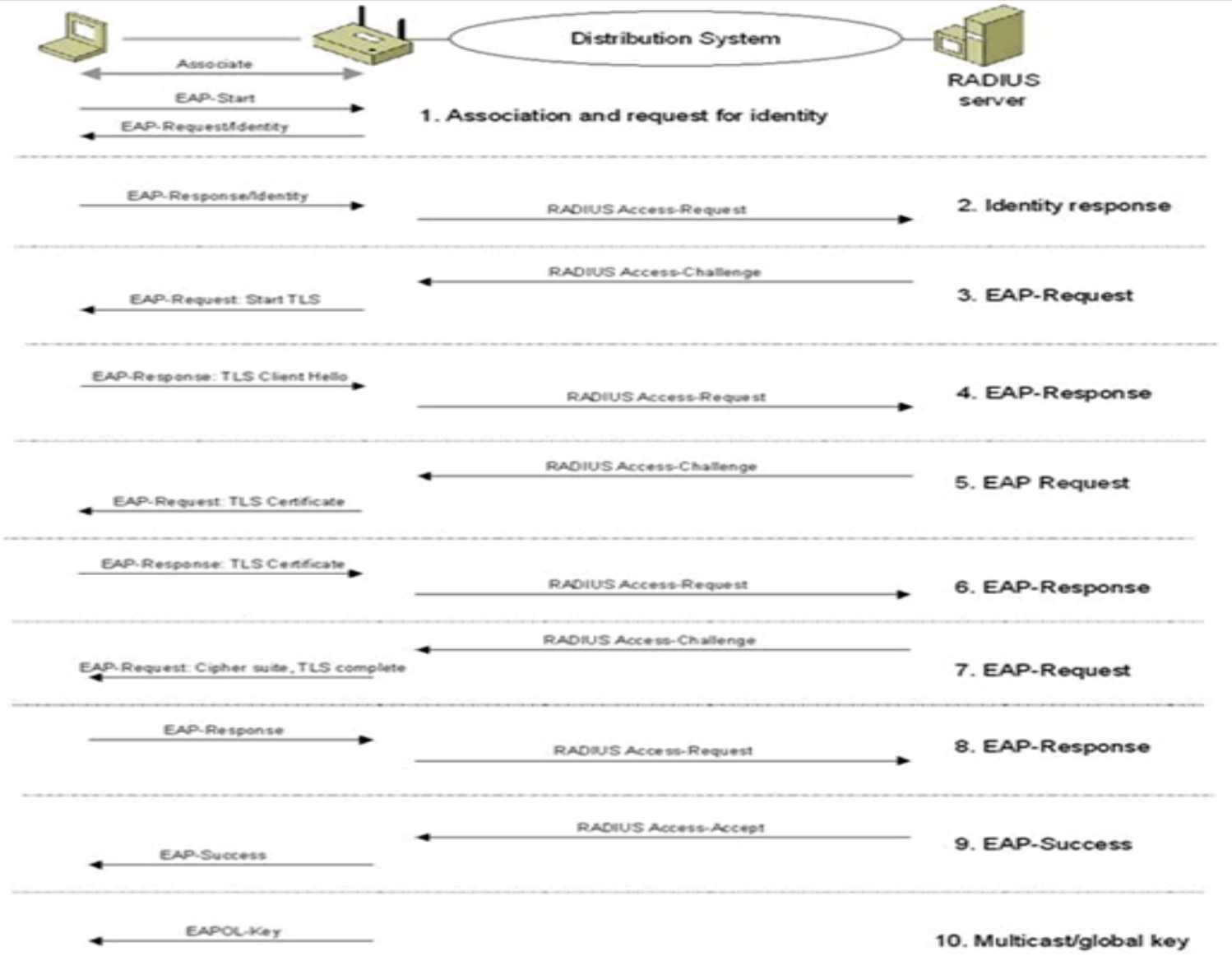


WPA+EAP-TLS+FreeRADIUS

Conceptos: EAP

- **EAP** (Extensible Authentication Protocol)
- **EAP-TLS** (EAP – Transport Level Security) Autenticación mutua, cifrada y depende de certificados de una CA. Soportado por hostapd.
- **EAP-TTLS** (EAP Tuneled TLS) No necesita ambos certificados, solo el de el servidor para crear un tunel.
- **EAP-MD5** El servidor envia un mensaje desafío al cliente y este contesta con otro mensaje MD5 o no autentica. Fácil de implementar pero menos fiable.
- **LEAP** (Lightweigth EAP) Implementacion de Cisco, autenticación mutua, permite el uso dinámico de WEP.
- **PEAP** (Protected EAP): desarrollado por M$, Cisco y RSA, similar a EAP-TTLS

WPA+EAP-TLS+FreeRADIUS



WPA+EAP-TLS+FreeRADIUS

RADIUS: AAA

- Es un servicio (servidor) para autenticación remota, estándar de facto.
- Compatible con SNMP.
- Se compone de un servidor y un cliente.
- Admite varios tipos de bases de datos de contraseñas, y usar varios tipos de esquemas de autenticación, por ejemplo PAP y CHAP (se integra prácticamente con cualquier BBDD y SO).
- Algunos incorporan protección contra "sniffing" y ataques activos.
- Permite administración centralizada.
- La Autorización viene definida en el RFC 2865.
- Los servicios de Accounting están disponibles en el RFC 2866.

WPA+EAP-TLS+FreeRADIUS

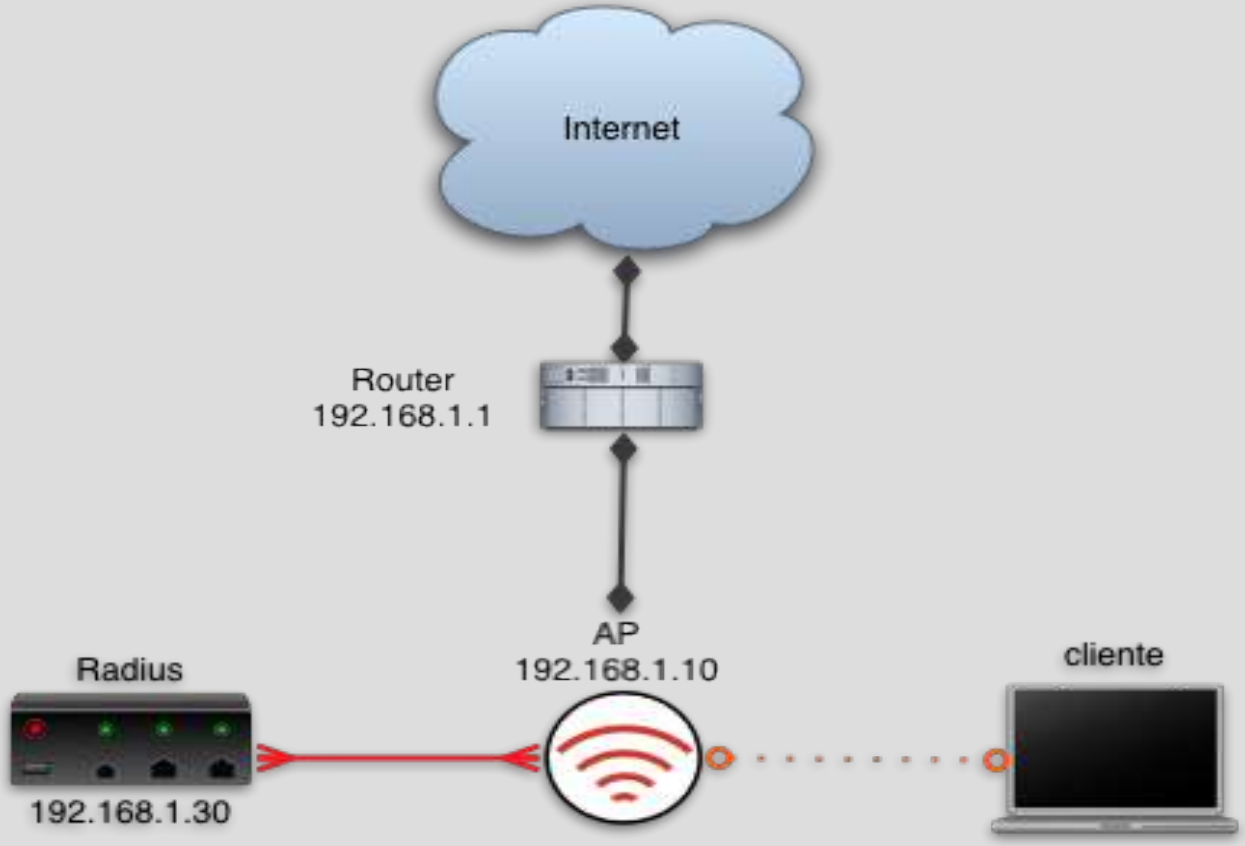
RADIUS: AAA

- **Autenticación:** Verificar que una entidad es quien dice ser. Suele incluir unas credenciales (usuario/contraseña, certificados, tokens, etc.).
- **Autorización:** Decidir si la entidad, una vez autenticada, tiene permiso para acceder al recurso.
- **Control de Acceso:** Conceder el permiso definitivo. ACL. Registro, monitorización, contabilidad e informes.

WPA+EAP-TLS+FreeRADIUS

Instalación y configuración:

- Esquema de red:



WPA+EAP-TLS+FreeRADIUS

RADIUS: Configuración

- **radiusd.conf** - Archivo general de configuración de FreeRADIUS.
- **eap.conf**– Archivo de configuración de las directivas EAP a utilizar. Es un *include* de radiusd.conf
- **clients.conf**– Descripción y credenciales de los diferentes dispositivos que consultan al RADIUS.
- **users** – Archivo donde se especifican las credenciales de los usuarios de la red. Se usa este archivo si no existe otro backend para el almacenamiento de los usuarios.
- **secret** - es usada para cifrar la comunicación entre el cliente RADIUS (AP) y el servidor RADIUS

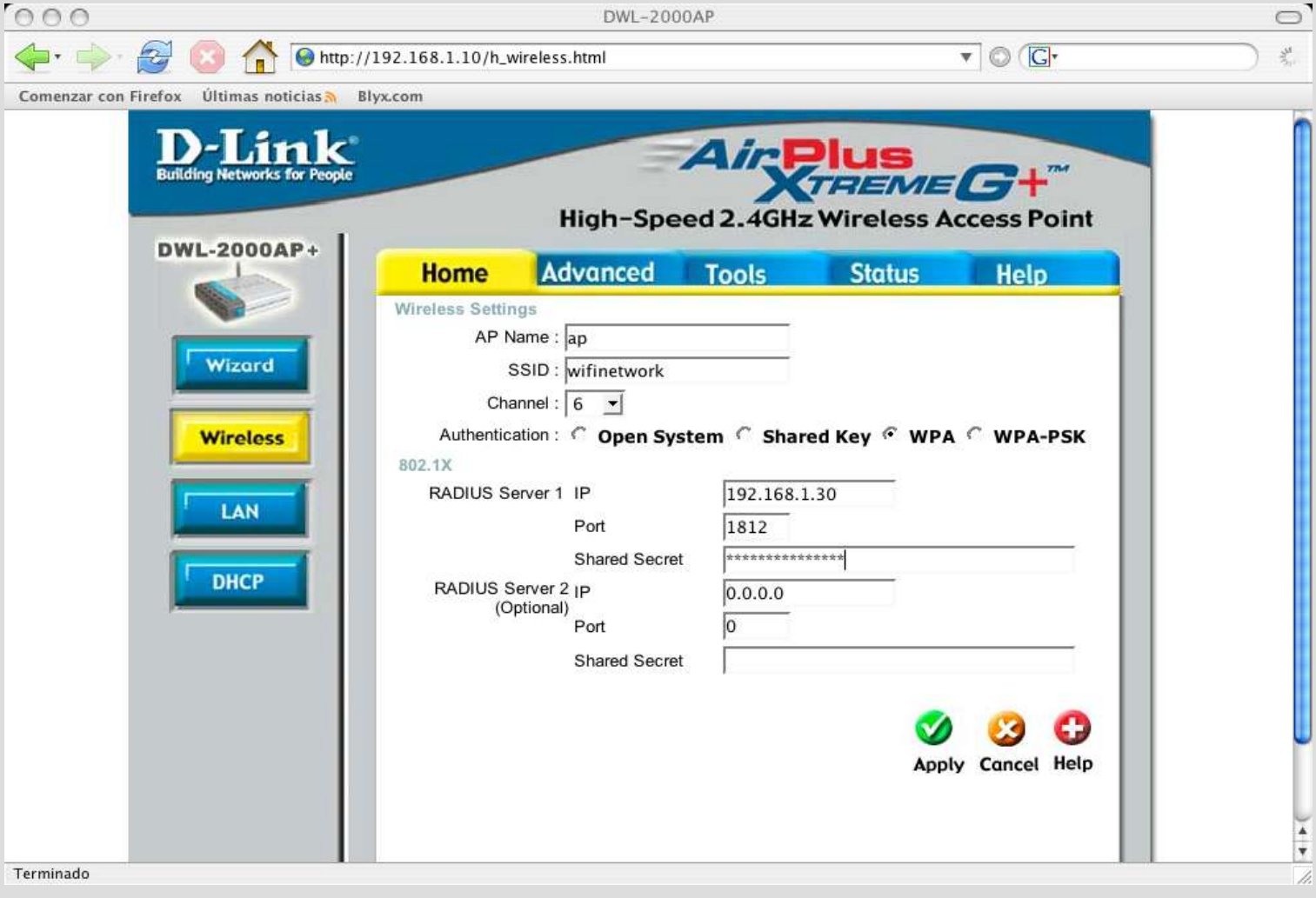
WPA+EAP-TLS+FreeRADIUS

RADIUS: Certificados

- **CA.root** – Creación de la CA.
- **CA.server**– Creación de certificados para el servidor (fqdn).
- **CA.client**– Creación de certificados para cada usuario. No confundir con clients.conf de RADIUS.
- **xpextensions** – OID para EAP-TLS.
- Copiar archivos root.der (certificado de CA) y <usuario>.p12 (clave privada y certificado del cliente)

WPA+EAP-TLS+FreeRADIUS

AP: Configuración



WPA+EAP-TLS+FreeRADIUS

Cliente: Configuración

- Linux:
  - Xsupplicant: http://www.open1x.org/
  - AEGIS Client http://www.mtghouse.com
  - wpa_supplicant http://hostap.epitest.fi/wpa_supplicant
- Mac OS X:
  - Soporte nativo del sistema.
  - AEGIS Client http://www.mtghouse.com
- FreeBSD:
  - PANA: http://www.opendiameter.org/

WPA+EAP-TLS+FreeRADIUS

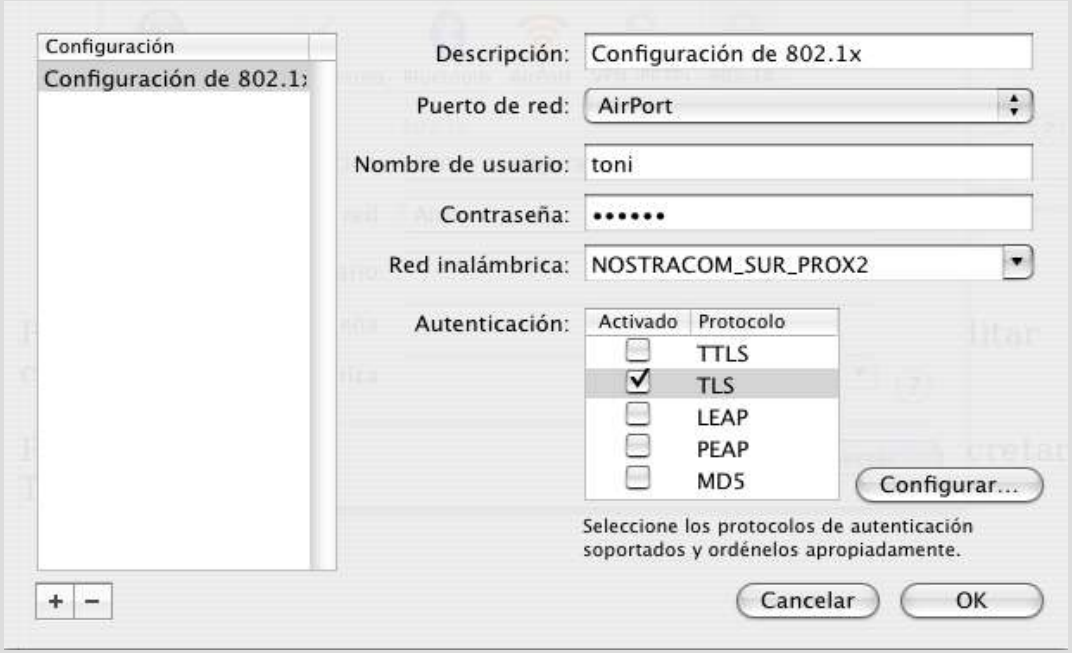
Cliente: Configuración

- Windows:
  - Soporte nativo del sistema Windows XP SP2.
  - WIRE1x: http://wire.cs.nthu.edu.tw/wire1x/
  - AEGIS Client (98/CE/Me/2K/NT4) http://www.mtghouse.com
- Solaris:
  - AEGIS Client http://www.mtghouse.com

WPA+EAP-TLS+FreeRADIUS

Cliente: Configuración

- Mac OS X (Tiger):
  - Instalar los certificados de CA y Cliente.
  - Configuración 802.1x (EAP-TLS):



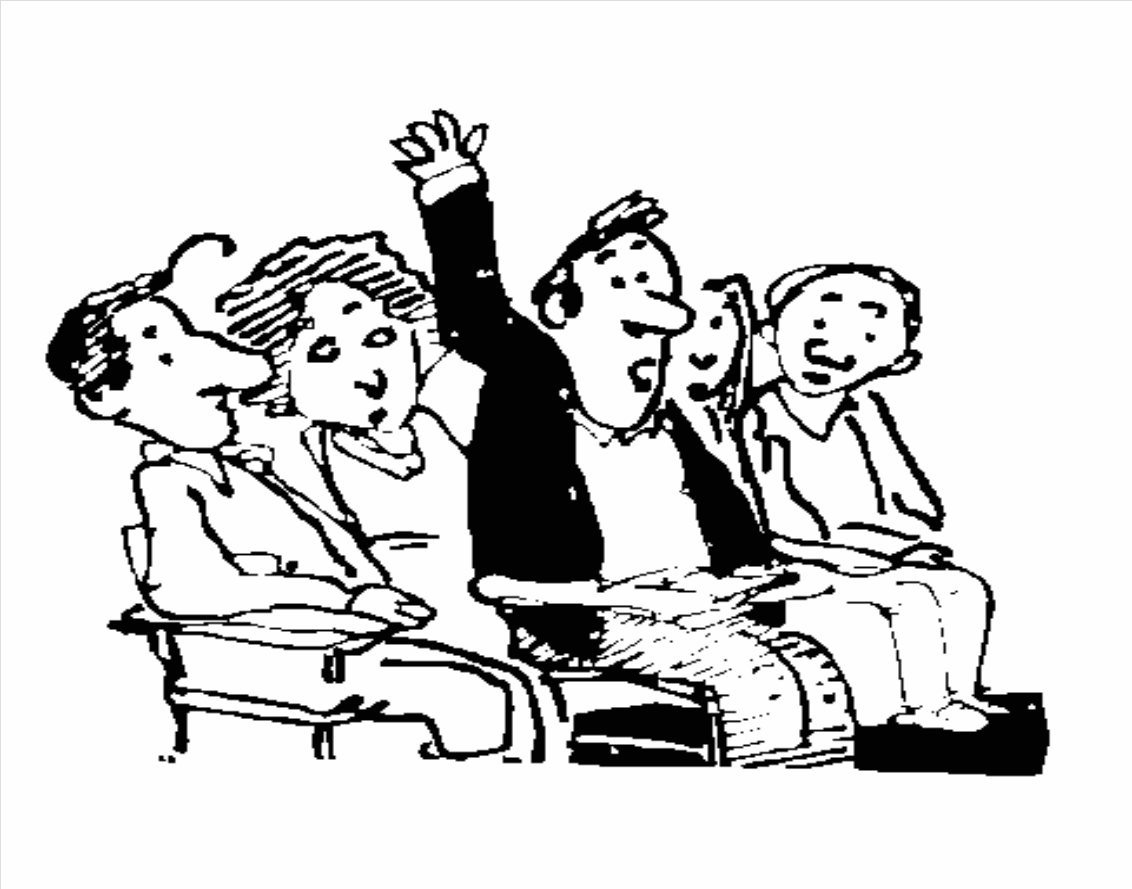
WPA+EAP-TLS+FreeRADIUS

Vulnerabilidades:

- Denegación de servicio (EAPOL-Start bombing, etc)
- Ingeniería social para conseguir certificados
- Desde la zona cableada atacar al servidor de certificados

WPA+EAP-TLS+FreeRADIUS

Preguntas¿?



WPA+EAP-TLS+FreeRADIUS

Referencias

- Wi-Foo: The secrets of wireless hacking. Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky. http://www.wi-foo.com
- http://www.freeradius.org/doc/EAPTLS.pdf
- http://www.missl.cs.umd.edu/wireless/eaptls/?tag=missl-802-1
- http://www.alphacore.net/contrib/nantes-wireless/eap-tls-HOWTO.
- http://www.fi.infn.it/system/WiFi/802.1X/macosx/
- http://www.dartmouth.edu/~pkilab/greenpass/gp-web-images/inter
- http://www.alphacore.net/spipen/article.php3?id_article=1
- http://oriol.joor.net/blog-dev/?itemid=1574

WPA+EAP-TLS+FreeRADIUS

Gracias
;P