Estudio de los riesgos relacionado con las redes Wi-Fi

A. Alejandro González Martínez

Índice

- Introducción
- Seguridad en redes Wi-Fi
- Cifrado WEP
- Cifrado WPA/WPA2
- WPA2-Enterprise
- Infraestructura
- Beneficios de la plataforma
- Consejos de seguridad
- Conclusiones

Introducción

Una red Wi-Fi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica, siguiendo unas normas establecidas.

La utilización de estas redes se ha disparado en los últimos años debido a:

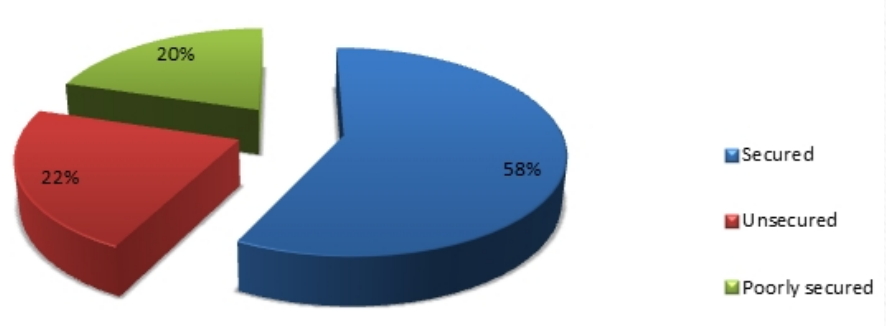
- Gran flexibilidad
- Alta movilidad
- Aumento exponencial de dispositivos inalámbricos

Introducción

Según el estudio desarrollado por Bitdefender entre el 22/11/2010 y el 03/10/2011 una de cada cuatro redes inalámbricas son altamente vulnerables a ataques hackers.

Del estudio se extraen los siguientes datos:

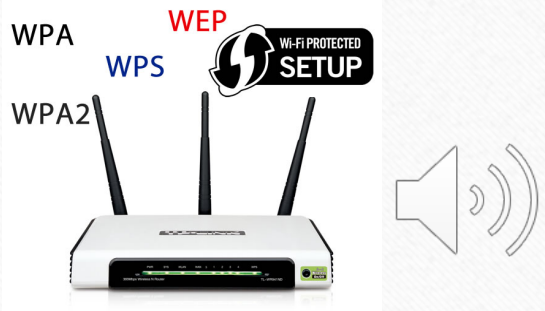
- El 21% de las empresas no utilizan cifrado
- El 15% usaba como tecnología de cifrado WEP
- El 62% utiliza un sistema WPA/WPA2



Datos basados en redes cuyo SSID coincidían con el nombre de la empresa

Seguridad en redes Wi-Fi

- Los actuales protocolos de encriptación son vulnerables.
- Actualmente las redes Wi-Fi tienen grandes problemas de seguridad y si no tomamos unas buenas medidas para solventarlos, cualquier usuario puede llegar a comprometer nuestra red.
- La seguridad de una red inalámbrica viene determinada por varios aspectos, los cuales podremos configurar desde los ajustes del router o el punto de acceso.

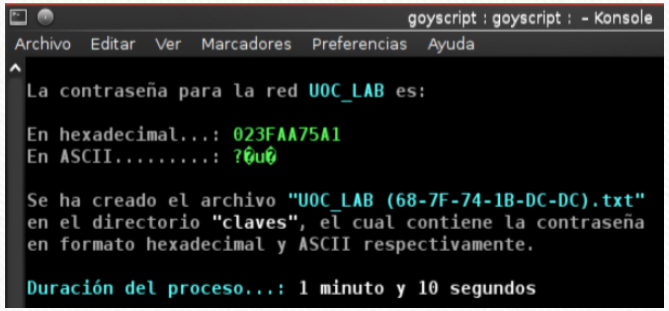


Cifrado WEP

La encriptación abierta y encriptación WEP son las menos seguras. Con la abierta cualquiera puede acceder a nuestra red y obtener una clave WEP es un proceso relativamente sencillo.

Herramientas como GOYscriptWEP permiten obtener la contraseña de forma muy simple y en un periodo de tiempo muy corto.

GOYscriptWEP aprovecha la mala implementación del vector de inicialización en el algoritmo de cifrado WEP.



Cifrado WPA/WPA2

La encriptación más recomendada es WPA/WPA2, ya que solo es posible obtenerla la contraseña realizando un ataque de diccionario o de fuerza bruta.

Este ataque se realiza generando un diccionario con varias claves para intentar que coincida alguna con la del router y obtener así el acceso, cuanto mayor es el diccionario, mayores son la probabilidades de acceder.

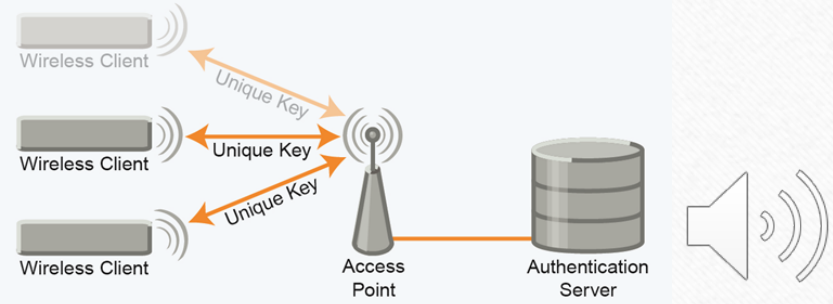
Al igual que ocurría con el cifrado WEP, existen herramientas que permiten obtener la contraseña.

WPA2-Enterprise

¿Cómo se puede mejorar la seguridad en entornos empresariales?

La encriptación WPA2-Enterprise es el método más seguro pero menos extendido en el ámbito domestico. Éste método consiste en la autenticación mediante usuario y contraseña guardadas en un servidor RADIUS.

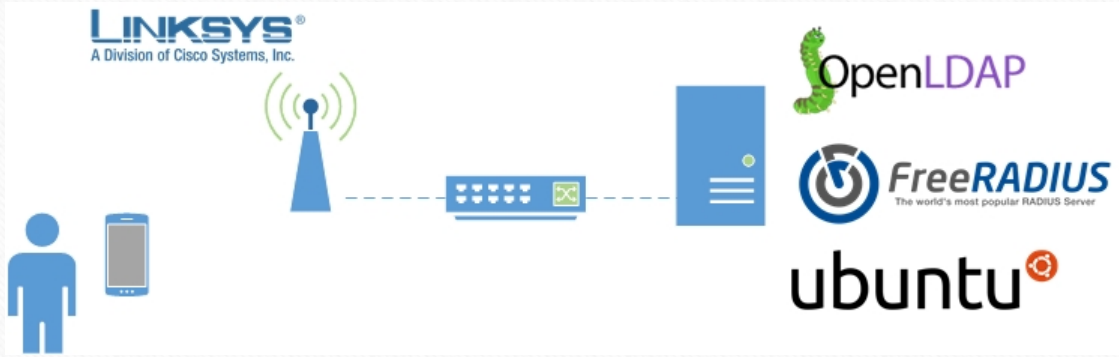
Este método de autenticación es difícil de configurar, ya que tendremos que crear un servidor y configurar el servicio.



Infraestructura

En el proyecto fin de grado se ha planteado una plataforma WPA2-Enterprise EAP-TTLS 100% open source

- Sistema Operativo: Ubuntu Server
- Servicio RADIUS: FreeRADIUS
- Servicio LDAP: OpenLDAP
- Configuración: EAP-TTLS PAP



RADIUS

- Las empresas demandan redes Wi-Fi seguras. Las debilidades en los sistemas de cifrado presentes en Wi-Fi se puede evitar mediante el uso de la autenticación EAP con un servidor RADIUS.
- Radius (Remote Authentication Dial-In User Server), es un protocolo de autenticación para aplicaciones de acceso a la red o movilidad IP.
- Podemos decir que más que un protocolo de autenticación, es un protocolo AAA (Authentication, Authorization, Administration).

LDAP

- Protocolo de Acceso Ligero a Directorios es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.
- Un directorio de información LDAP es un tipo de base de datos, pero no es una base de datos relacional.
- El protocolo LDAP es utilizable por distintas plataformas y está basado en estándares, por lo que puede ser utilizado de forma conjunta con un RADIUS.

EAP-TTL

Los motivos de elegir EAP-TTLS son los siguientes:

- Actualmente no es vulnerable a ataques de fuerza bruta ni Man-in-the-middle.
- Es un método de autenticación tunelado.
- Solo se requiere de un certificado en el servidor.
- Todo el tráfico circula totalmente cifrado.
- Soporta una amplia variedad de métodos de autenticación interna.

	Clear-text	NTLM (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash
PAP	✓	✓	✓	✓	✓	✓
CHAP	✓	x	x	x	x	x
MSCHAP	✓	✓	x	x	x	x
MSCHAPv2	✓	✓	x	x	x	x

PAP

- PAP viaja en texto plano por lo que no es recomendable usarlo independiente, pero no hay ningún problema al utilizarlo de forma conjunta con EAP-TTLS ya que éste cifra toda la comunicación cliente-servidor.
- Como se hace uso de LDAP solo podemos usar PAP ya que es compatible con sus algoritmos de cifrado.

	PAM	LDAP "bind as user"	ntlm_auth
PAP	√	√	√
CHAP	x	x	x
Digest	x	x	x
MS-CHAP	x	x	√
PEAP	x	x	√
EAP-MSCHAPv2	x	x	√
Cisco LEAP	x	x	x
EAP-GTC	x	x	x
EAP-MD5	x	x	x
EAP-SIM	x	x	x

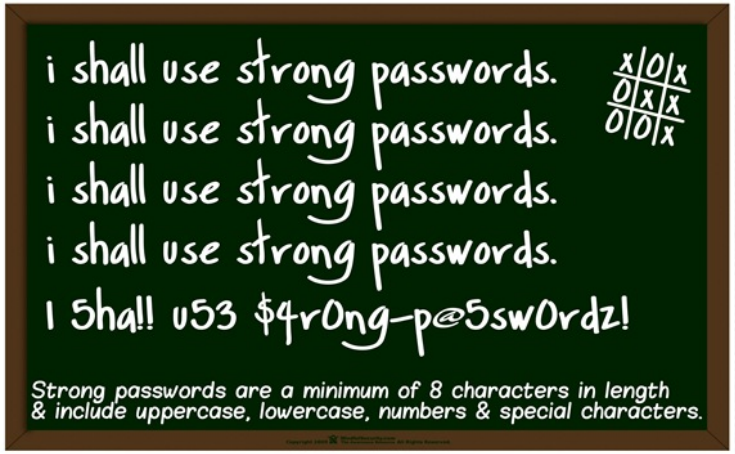
Beneficios de la plataforma

Esta plataforma EAP-TTLS / PAP presenta un escenario robusto y complejo que disuade a atacantes poco experimentados y pone a prueba a un experto.

Consejos de seguridad

Si no es posible implementar una solución RADIUS es conveniente tener en cuenta los siguientes consejos:

- Ocultar el SSID y cambiar el que se establece por defecto.
- Establecer cifrado WPA/WPA2 - PSK.
- Desactivar WPS.
- Evitar el uso del cifrado WEP.
- Usar una contraseña compleja.



Conclusiones

- El mayor problema que presentan las redes Wi-Fi reside en que todos sus protocolos presentan debilidades.
- Una persona con pocos conocimientos puede acceder a una red Wi-Fi sin autorización.
- 802.1x a día de hoy es la forma más fiable de securizar una red Wi-Fi.
- La configuración del servicio FreeRADIUS y OpenLDAP no es trivial.

Fin