

## Redes Inalámbricas (WiFi) Conceptos Básicos de Seguridad y Best Practices

ACIS / Octubre 2006

Presentador: Ing. Eduardo Tabacman

Internacional/arroba/virusprot.com



© Copyright 2006 VIRUSPROT.COM Todos los derechos reservados



### Redes Inalámbricas (WIFI) - Seguridad

W000-1-03

#### Temario de Seguridad WiFi

- *Introducción*
- *Problemas de Seguridad/Puntos Débiles*
- *Soluciones de Seguridad Básicas*
- *Métodos de Autenticación: Estándares y Protocolos*
- *Puntos de Acceso Hostiles*
- *Políticas*
- *Capacitación*
- *Cómo actúan los hackers*
- *Conclusiones y Recomendaciones*

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

2



# Redes Inalámbricas (WIFI) - Seguridad

W001-1-04

Acerca de Virusprot.Com

- **Oficina Central:** Madrid (España)
- **Fundador:** Eduardo Tabacman, Director General ([internacional@aroba.virusprot.com](mailto:internacional@aroba.virusprot.com))
- **Establecida:** 1999
- **Equipo con más de 15 años de experiencia en el tema de la Seguridad Informática**
- **Actividades Principales:**
  - Portal de Seguridad Informática VIRUSPROT.COM [www.virusprot.com](http://www.virusprot.com)
  - 80.000 visitas mensuales
  - Servicios de asesoramiento y consultoría
  - Desarrollo de seminarios y conferencias
  - Business matching

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

3



# Redes Inalámbricas (WIFI) - Seguridad

W021

Portal de Seguridad Wi-Fi  
[www.virusprot.com/indexwf.html](http://www.virusprot.com/indexwf.html)



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

4

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

## Seguridad Informática

- Grandes cambios desde comienzo de siglo
- Van apareciendo nuevas tecnologías a gran velocidad
- Las organizaciones (y los particulares) **no ven los cambios hasta que son muy evidentes**
- **Inercia Mental:** Cuesta cambiar los parámetros de pensamiento y comportamiento
- Teléfono fijo/Teléfono celular
- Trabajo manual/computador

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 5

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*


## Instalación de Redes Wi-Fi

- Muy **Fáciles** de comprar
- Bastante **Difíciles** de Configurar
- Casi **Imposibles** de Proteger
- **Inseguridad Wireless** 

**Desde que aparece la primer computadora Wi-Fi en la empresa**

Según el NIST: Mantener una **red wireless segura** es un proceso **continuo** que requiere **esfuerzos mayores** que las otras redes y sistemas


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 6

 **Redes Inalámbricas (WIFI) - Seguridad**

**FALSO !!!**

- En la organización no hay redes Wi-Fi por lo tanto no tenemos que preocuparnos
- **El peligro lo representa la Tecnología Wi-Fi y no las redes.** Un solo computador con Wi-Fi es suficiente para crear puntos débiles en la seguridad de la información
- A veces la empresa no tiene ni un computador Wi-Fi, pero permite que se conecten dispositivos de empleados o visitantes

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **7**

 **Redes Inalámbricas (WIFI) - Seguridad**

**WIFI: El Asesino Silencioso !!!**

- Cables cortados con conexión a la oficina del vecino
- Con Wireless **no existen los cables y el vecino escucha las 24 horas**
- Micrófonos en la oficina del Presidente o del Director Financiero
- **Cualquiera trae un AP o un PDA WIFI y escucha todo y nadie se inmuta**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **8**

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Diferencias entre Red Cableada y Wireless

- Red Cableada envía la información a través de un medio exclusivo: **CABLE**
- **Ethernet** envía señales eléctricas a través del cable
- La información que viaja por el cable no puede ser vista por extraños
- Wireless envía la información a través de un medio compartido: **AIRE**
- **Wireless** envía energía de Radio Frecuencia
- La información que viaja por el aire puede ser vista por cualquiera dentro del rango

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **9**

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Modelo de Capas OSI – 802.11


Figure 1 - 802.11 and the OSI Model

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **10**

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

¿SOPA DE LETRAS O "TRABALUENGAS"?

- 802.11a, 802.11b, 802.11g, 802.11n, 802.11e, 802.11i, 802.11k, 802.1x
- TLS, TTLS, EAP, LEAP, FAST, WAPI, WPA, WPA2, MD-5, WEP, TKIP, AES, IP-Sec, PEAP
- MIMO, OFDM, DSS, CSMA/CA, RTS, CLS, EDF, EDCF, MAC, SSID, MAN, WWISE, RAND
- IEEE, IETF, WI-FI, WIMAX, CAPWAP, LWAPP, WiBRO, HIPERMAN



WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **11**

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad* W002

Tipos de Redes Inalámbricas

- IrDa (Infrarrojos)
- Bluetooth
- HomeRF (802.11)
- Wi-Fi (802.11)
- Wi-Max (802.16)

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **12**

W003

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Elementos de la Red Inalámbrica /WIFI (1)

- **Punto de Acceso (PA)**  
Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 13

W004

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Elementos de la Red Inalámbrica / WIFI (2)

- **Dispositivo Móvil (DM)**  
Ya sea Tarjeta PCMCIA, USB, PCI (Slot de un PC de sobremesa), Centrino\*, que sustituyen a las tarjetas de red  
Su función es la de recibir/enviar información desde la estación en que están instaladas (portátiles, PDAs, móviles, cámaras, impresoras,...)



\* Tecnología móvil Intel Centrino compuesta por un procesador Pentium M, chipset 855 y conectividad inalámbrica integrada

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 14

VIRUSPROT.COM **Redes Inalámbricas (WIFI) - Seguridad** W006

Topología de una Red Inalámbrica Empresarial Red Infrastructure

- 2 Elementos básicos:
  - Estaciones cliente (PCMCIA - adaptador USB)
  - Puntos de Acceso (PA)

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 15

VIRUSPROT.COM **Redes Inalámbricas (WIFI) - Seguridad** W007

Topología de una Red Inalámbrica Empresarial Red Ad-Hoc

- Similar a una red de grupos de trabajo
  - Todos los equipos conectados entre sí

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 16

W012-1-04

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## "Wi-Fi Certified"

- **The Wi-Fi Alliance**
  - **Finales de Mayo 2004**
  - *Logo más completo*
  - *Certificado Interoperatividad*
  - [www.wi-fi.org/certificate](http://www.wi-fi.org/certificate)
  - [www.wi-fi.org/certified\\_products](http://www.wi-fi.org/certified_products)
  - **Octubre 2004**
  - *Celulares Wi-Fi*




WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 17

W013-1-04

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Historia de las Redes Wireless Empresariales

Estándar	Velocidad	Banda Frecuencia
<b>802.11</b>	1 y 2 Mbps	2.4 Ghz
<b>802.11a</b>	54 Mbps	5.15 Ghz
<b>802.11b</b>	11 Mbps	2.4 Ghz
<b>802.11g</b>	54 Mbps	2.4 Ghz
<b>802.11n</b>	Para 2006	

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 18

W014

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

Estándar 802.11g

WWW.VIRUSPROT.COM Fuente: <http://www.virusprot.com/Nt200641.html>

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 19

W015

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

Pérdidas de Velocidad

**V=f(d,o,i)**

- ◆ **Obstáculos (o):** paredes/campos magnéticos...
- ◆ **Interferencias (i):** cantidad usuarios
- ◆ **Distancia (d):** entre usuario y PA

WWW.VIRUSPROT.COM © Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **20**



## Redes Inalámbricas (WIFI) - Seguridad

### Definiciones y Conceptos

- **MAC (Media Access Control) address:** Es un número de 48 bits asignado por el fabricante a los AP y estaciones. Aunque está grabado en el hard, se puede modificar por soft
- **SSID (Service Set Identifier):** Cada AP tiene uno de hasta 32 bytes. Sirve para identificar a la red.
- **IBSS (Independent Basic Service Set):** Identifica a las Redes Ad-Hoc (no hay AP)

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

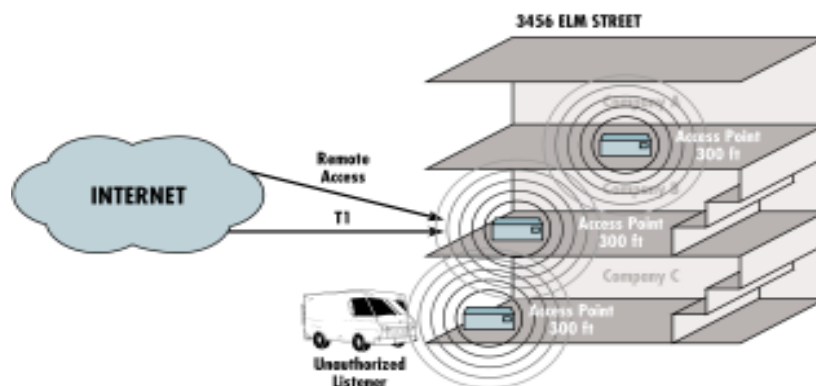
21



## Redes Inalámbricas (WIFI) - Seguridad

W018

### Puntos Débiles



WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

22

W019


**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

WarChalking

- Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico

Syntax V.0.9

Clave	Símbolo
	SSID X
	Ancho de Banda
	SSID O
	SSID Access Contact W
	Ancho de Banda



WWW.VIRUSPROT.COM Fuente: [www.warchalking.org](http://www.warchalking.org)

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

23

W020

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

WarDriving

- Técnica difundida donde individuos equipados con material apropiado tratan de localizar en coche puntos wireless

Estudio WarDriving New York

WEP Activado	25%
WEP Desactivado	75%

(Julio 2002)



Lugar: Barcelona  
Imagen: Miguel Puchol  
Puntos rojos protegidos  
Puntos verdes desprotegidos

WWW.VIRUSPROT.COM Foto: O'Reilly Network

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

24

W029-1-03

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Herramientas para el WarDriving



- **Portátil**, PDA u otro dispositivo móvil con **tarjeta inalámbrica** (PCMCIA) incorporada
- **Antena** comprada o casera tipo "lata de Pringles" o "tubo PVC"
- **Software** de rastreo tipo NetStumbler, Aircnort,...
- **Unidad GPS** para fijar las coordenadas exactas en el mapa de la WLAN

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 25

W645-1-04

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Resultados del WWWD (The WorldWide Wardrive)


CATEGORIA	2001 TOTAL / %	2002 TOTAL / %	2003 TOTAL / %	2004 TOTAL / %
<b>APs detectados</b>	9374 / <b>100</b>	24958 / <b>100</b>	88122 / <b>100</b>	250451 / <b>100</b>
<b>WEP Activado</b>	2825 / <b>30.13</b>	6970 / <b>27.92</b>	28427 / <b>32.26</b>	95317 / <b>38</b>
<b>WEP Desactivado</b>	6549 / <b>69.86</b>	17988 / <b>72.07</b>	59695 / <b>67.74</b>	155134 / <b>61.9</b>
<b>SSID Por Defecto</b>	2768 / <b>29.53</b>	8802 / <b>35.27</b>	24525 / <b>27.83</b>	79837 / <b>31.8</b>
<b>SSID Por Defecto+ WEP Desactivado</b>	2497 / <b>26.64</b>	7847 / <b>31.44</b>	21822 / <b>24.76</b>	70047 / <b>27.9</b>

\*Resaltado en verde los valores más altos  
\*Resaltado en azul los valores más bajos

WWW.VIRUSPROT.COM Fuente: <http://www.worldwidewardrive.org/>

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 26

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*




WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **27**

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

### Estudio de Panda Software y Kaspersky Labs

- 12 ciudades importantes: Estocolmo, Lisboa, Montevideo, Buenos Aires, Madrid, Bilbao
- Se detectaron 905 redes
- Sólo 41% tenían alguna protección
- El Rey de la Desprotección es España con menos del 20%, Uruguay 41%, Portugal 44% y Argentina 49%
- El más protegido Suecia con el 85%
- Kaspersky analizó el aire en CEBIT y encontró el 55% sin ninguna protección


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **28**

 **Redes Inalámbricas (WIFI) - Seguridad**

## Sólo Warchalking ?

- Wardriving
- Warflying
- Warspamming
- Warvirusing

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 29

 **Redes Inalámbricas (WIFI) - Seguridad**

## Informe de GAO sobre Seguridad de Redes Wireless – Octubre 2005

- GAO (Government Accountability Office)
- “Las Agencias Federales Necesitan Mejorar los Controles sobre las Redes Wireless”
- No han implementado controles claves como políticas y prácticas que permitan operar de manera segura una red wireless
- En 6 agencias federales se detectaron actividades no autorizadas y pérdidas de señal
- 9 Agencias no han establecido políticas
- 18 Agencias no proveen entrenamiento a sus empleados y visitantes
- En una Agencia se detectaron 90 laptops configuradas de manera impropia para la seguridad wireless

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 30

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

## Más del Informe de GAO

En 15 Manzanas De Washington se detectaron **MÁS DE MIL** Redes WLAN

Empresas Privadas Recibiendo Señales RF De Agencias Federales

“El control físico de los Dispositivos wireless adquiere una nueva importancia en el mantenimiento de la **seguridad de la información**”

Figure 3: Wireless Networks Detected in a Section of Downtown D.C.

Figure 4: Example of Signal Leakage from Federalized Private Facilities

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

31

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad* W201

## Desafíos en la Seguridad de las Redes Inalámbricas (1)

- Cualquiera dentro de un radio de 100 metros puede ser un intruso potencial

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

32

W202

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

Desafíos en la Seguridad de las Redes Inalámbricas (2)

- Las acreditaciones del usuario se deben poder intercambiar con seguridad
- Debe ser capaz de asegurar la conexión con la red de trabajo correcta



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 33

W203

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

Desafíos en la Seguridad de las Redes Inalámbricas (3)

- Los datos se deben poder transmitir con seguridad a través de la utilización apropiada de llaves de encriptación



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 34

W204

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Red Inalámbrica en una Empresa, Ataque Potencial 1

The diagram shows a central router connected to four wireless zones labeled 'Zona Inalámbrica'. Each zone contains several laptops. A red car is positioned outside the company's perimeter, with a laptop inside it. Red arrows indicate a signal being transmitted from the car's laptop to the central router. The text below the diagram reads: 'Hacker potencial con un PC y un adaptador inalámbrico en el Coche'.

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

35

W205

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Red Inalámbrica en una Empresa, Ataque Potencial 2

The diagram is identical to the one on slide 35, showing a wireless network in a company. However, the red car is now labeled 'Caballo de Troya W' (Trojan Horse W). Green arrows point from the car's laptop to the wireless zones, indicating that the car is acting as a malicious access point to lure users into connecting to it. The text below the diagram reads: 'Hacker potencial con un punto de acceso (A.P.) hostil en su coche engañando a usuarios para conectarse a su red'.

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

36

W206-1-04



### Redes Inalámbricas (WIFI) - Seguridad

**Peligros**


- Denegación de Servicios (DoS)
- Daño o Robo de Equipos
- Accesos no Autorizados
- Robo de Información
- Inserción de Códigos Dañinos
- Robo de Credenciales
- Uso de Internet
- Warspamming
- Warvirusing
- Puntos de Acceso Hostiles
- Redes Ad – Hoc
- Hot – Spots
- Phishing – Evil Twin

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

37

W209



### Redes Inalámbricas (WIFI) - Seguridad

**Filtrado de Direcciones MAC**

- MAC (*Media Access Control Address*)
  - Dirección del hardware originaria del fabricante
  - Sirve para identificar routers, tarjetas de red, etc...
- Crear en cada PA una base de datos de direcciones MAC
- **DESVENTAJAS**
  - Se debe repetir en todos los PAs existentes (puede ser mucho trabajo y originar errores)
  - Una vez capturadas por un hacker, pueden entrar a la red tranquilamente
  - Si algún usuario pierde o le roban su estación, queda comprometida la seguridad

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

38



### Redes Inalámbricas (WIFI) - Seguridad


W654-1-03

### Filtrado de direcciones MAC, ¿seguridad Wi-Fi?



WWW.VIRUSPROT.COMFuente: <http://www.virusprot.com/Charwif3.html>

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados39




### Redes Inalámbricas (WIFI) - Seguridad

## MAC Spoofing

- Las direcciones MAC son utilizadas en varios paquetes y **nunca van encriptadas**
- Es fácil capturar paquetes y sacar las direcciones MAC
- Luego hay que configurar el equipo con esas direcciones capturadas
- Hay un herramienta en Internet que realiza esta tarea: Spoof MAC (SMAC)
- Filtrado MAC sólo puede servir de algo para uso en casas o pequeñas oficinas.

WWW.VIRUSPROT.COM© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados


40

 **Redes Inalámbricas (WIFI) - Seguridad** W210

WEP – Introducción

- Wired Equivalent Privacy
- Sistema de encriptación estándar 802.11
- Se implementa en la capa MAC
- Soportada por la mayoría de vendedores de soluciones inalámbricas
- Cifra los datos enviados a través de las ondas de radio
- Utiliza el algoritmo de encriptación RC4

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 41

 **Redes Inalámbricas (WIFI) - Seguridad** W211

WEP - Debilidades


- Longitud del vector IV (24 bits) insuficiente
- El IV se repetirá cada cierto tiempo de transmisión continua para paquetes distintos, pudiendo averiguar la llave compartida
- Utilización de llaves estáticas, el cambio de llave se debe realizar manualmente
- Hay herramientas para recalcular el ICV después de haber modificado el texto
- A pesar de todo, WEP ofrece un mínimo de seguridad

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 42

W212

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

AirSnort



WWW.VIRUSPROT.COM Fuente: <http://www.virusprot.com/Nt240821.html>

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 43

W213


**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

WEP - Carencias

- Interceptando aproximadamente 100 Mb  $\longrightarrow$  1 Gb
- Hay algunas tarjetas muy simples que el primer IV que generan es cero y lo van modificando de 1 en 1
- Algunas, al resetearse comienzan otra vez de 0
- 3.000 llaves cada semana son débiles
- 2.000 paquetes débiles son suficientes para adivinar un password
- 15 minutos (128 bits)

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 44



### Redes Inalámbricas (WIFI) - Seguridad

W214

#### Utilidades "Sniffers" para WLANs (1)

- **WEPCrack** (<http://sourceforge.net>)
  - 1ª herramienta de código abierto para romper llaves secretas 802.11 WEP
  - Implementación del ataque descrito por Fluhrer, Mantin, y Shamir en el ensayo "Weaknesses in the Key Scheduling Algorithm of RC4"
- **Airsnort** (<http://airsnort.shmoo.com>)
  - Desarrollada por Shmoo Group para sistemas Linux
  - Recupera las llaves de cifrado
  - Monitoriza de manera pasiva las transmisiones y computa la llave de cifrado cuando se han recopilado suficientes paquetes
- **Kismet** (<http://www.kismetwireless.net>)
  - Sistemas Linux
  - "Escucha" las señales de radio en el aire
  - Las unidades GPS, conectadas a notebooks a través de cables en serie, permiten localizar en mapas digitales la ubicación de estas redes

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 45



### Redes Inalámbricas (WIFI) - Seguridad

W215

#### Utilidades "Sniffers" para WLANs (2)

- **Ethereal** (<http://www.ethereal.com>)
  - Sistemas Linux
- **NetStumbler** (<http://www.netstumbler.com>)
  - Sistemas Windows
  - Detecta redes que revelan sus SSIDs (Service Set Identifier), que por lo general se transmiten con la configuración predefinida de los routers inalámbricos
- **Airopeek** (<http://www.wildpackets.com>)
  - Sistemas Windows
- **Airmagnet** (<http://www.airmagnet.com>)
  - Corre en Compaq iPaq
- **Wellenreiter** (<http://www.remote-exploit.org>)
  - Detecta PAs y muestra información sobre los mismos

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 46



## Más Recomendaciones WEP

- Algunos AP no requieren password de administrador para entrar a las configuraciones por defecto / El campo de la clave está en blanco
- Imprescindible cambiar las configuraciones por defecto
- Cambiar las claves de fábrica (11111)
- Configurar la encriptación en lo máximo que permite el AP (104?)
- Tratar de cambiar frecuentemente las claves WEP

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

47




## Soluciones más robustas

- Preocupación en la industria por falta de seguridad
- Muchos usuarios no se animan a adoptar este tipo de soluciones
- La IEEE busca nuevas opciones
- La WiFi Alliance aún no reacciona
- La IEEE adapta el estándar 802.1x para redes WiFi
- Este se basa en el control de acceso a puertos

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

48



### Redes Inalámbricas (WIFI) - Seguridad

W216


#### Qué es el Estándar 802.1x

- Estándar de la IEEE ratificado en 2001 para redes cableadas y adaptado en 2004 para Wireless
- Introduce cambios muy importantes en la seguridad de las redes WiFi
- Establece la necesidad de Autenticar a los usuarios antes de conectarse a una red WiFi
- Provee un método para la autenticación y autorización de conexiones a una RED INALÁMBRICA
- **Autenticación basada en el usuario**; puede usar credenciales tales como contraseñas o certificados
- Antes "sólo" se autenticaba al dispositivo
- Utiliza EAP (Extensible Authentication Protocol)
- Aprovechamiento de protocolos AAA tales como RADIUS para centralizar autenticación y autorizaciones

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

49



### Redes Inalámbricas (WIFI) - Seguridad


#### 802.1x – Esquema Básico

- **El puerto no se abre y no permite la conexión hasta que el usuario no está autenticado**
- El estándar define 3 elementos
- **Servidor de Autenticación:** Es el que verificará las credenciales de los usuarios. Generalmente es un servidor RADIUS
- **Autenticador:** Es el dispositivo que recibe la información del usuario y la traslada al servidor de autenticación
- **Suplicante:** Una aplicación "cliente" que provee la información de las credenciales al autenticador

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

50



**Redes Inalámbricas (WIFI) - Seguridad**

## Protocolos EAP

- Se basan en RFC 2284
- Originalmente desarrollado para PPP
- El estándar 802.1x los "aplica" a Redes WiFi
- Permiten añadir Autenticación sin que los AP tengan que "aprender" esta función
- Reduce el costo de los AP, al trasladar esta función al Servidor de Acceso (RADIUS)
- Compatible con el uso de OTP y otras autenticaciones robustas
- Existen variantes de EAP para redes cableadas
- Es necesario crear EAP específico para WLAN

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

51



**Redes Inalámbricas (WIFI) - Seguridad**

W217-1-04

## 802.1x trata sobre la seguridad en las Redes Inalámbricas

- **Por qué RADIUS**
  - La autenticación se basa en el usuario, en vez de basarse en el dispositivo
  - Elimina la necesidad de almacenar información de los usuarios en cada access point de la RED, por tanto es considerablemente más fácil de administrar y configurar
  - RADIUS ya ha sido ampliamente difundido para otros tipos de autenticación en la red de trabajo
- Se basa en RFC 2138 y RFC 2548 entre otros
- Generará las claves de encriptación de manera dinámica
- El administrador puede establecer los intervalos

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

52

W256-1-03

### Redes Inalámbricas (WIFI) - Seguridad

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

53

W218

### Redes Inalámbricas (WIFI) - Seguridad

Red Inalámbrica en una Empresa,  
la Solución según 802.1x

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

54

W219

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Proceso de Autenticación (1)

- El usuario Wireless LAN autenticará la red de trabajo
  - Para asegurar que el usuario se conectará a la red correcta

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

55

W220

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Proceso de Autenticación (2)

- El servidor RADIUS crea un túnel seguro entre el servidor y el cliente. El usuario es autenticado a través del túnel con la utilización del nombre de usuario y contraseña/token
- Esto asegura que un usuario autorizado se está conectando dentro de la red

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

56

W221

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

Proceso de Autenticación (3)

- El servidor de RADIUS generará llaves dinámicas WEP para encriptación de los datos
  - Ambas llaves se distribuyen al access point y al cliente

The diagram illustrates the third step of the authentication process. A central RADIUS server, labeled 'Servidor RADIUS', is connected to a central switch labeled 'Enterprise'. The switch is connected to three 'Zona inalámbrica' (wireless zones). Each zone contains wireless access points and clients. Red arrows show the RADIUS server distributing WEP keys to the access points in each zone. Green arrows show the RADIUS server distributing WEP keys to the clients in each zone. The RADIUS server is also connected to a database containing 'Windows', 'SQL/LDAP', and 'Tokens'. The wireless zones are also connected to a central switch labeled 'Enterprise'.

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

57

W222

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

Proceso de Autenticación (4)

- Tras la autenticación, el RADIUS autorizará al access point la apertura de un puerto virtual para el cliente de la RED INALÁMBRICA
  - El cliente obtiene su dirección IP (DHCP) y accede a la red

The diagram illustrates the fourth step of the authentication process. A central RADIUS server, labeled 'Servidor RADIUS', is connected to a central switch labeled 'Empresa'. The switch is connected to three 'Zona inalámbrica' (wireless zones). Each zone contains wireless access points and clients. Red arrows show the RADIUS server authorizing the access points in each zone to open virtual ports for the clients. Green arrows show the RADIUS server authorizing the clients in each zone to access the network. The RADIUS server is also connected to a database containing 'Windows', 'SQL/LDAP', and 'Tokens'. The wireless zones are also connected to a central switch labeled 'Empresa'.

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

58

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

## Seguridad VPN - IPSec

- IPSec crea un túnel entre los 2 puntos y transmite **todos** los paquetes. El usuario remoto tiene acceso a todos los recursos **sin importar donde está**
- Internet Protocol Security (IPSec) tiene 2 modos de encriptación
- TUNNEL: Cifra el encabezado y el contenido de cada paquete
- TRANSPORT: Cifra sólo el contenido
- IPSec encripta datos entre varios dispositivos:
  - ✓ Router – Router
  - ✓ Firewall – Router
  - ✓ Pc – Router
  - ✓ Pc - Server

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **59**

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

## Seguridad VPN + WEP

The diagram shows a VPN Device on the left and a Wireless client on the right. A thick grey cylinder representing a tunnel connects them, with a green arrow pointing to it labeled 'Túnel Desde Usuario a VPN'. Above the tunnel, a double-headed arrow labeled 'Internet Protocol Security (IPsec)' spans the distance between the VPN Device and the Wireless client. Above the wireless client, a double-headed arrow labeled 'WEP Security' spans the distance between the client and an Access Point (A).

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **60**

Fuente: NIST

W251-1-03

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Seguridad VPN 802.11

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

61

W252-1-03


**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Seguridad VPN (1)

- La red wireless es la red insegura
- Los PA se configuran con o sin WEP
- La encriptación es IPSec
- Acceso wireless es "aislado" de la red de la empresa por el servidor VPN
- Los PA se pueden interconectar creando una red virtual (VLAN)

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados


62

 **Redes Inalámbricas (WIFI) - Seguridad**

## Seguridad VPN (2)

- IPSec fue designado para conexiones punto-a-punto
- Las WLANs no son dial-up
- Las WLANs funcionan en un medio compartido, irradiado (broadcast)
- Están diseñadas para capa 3
- Para asegurar la capa 2 se necesita PKI y direcciones IP estáticas
- El cifrado se hace en capa 3 y después que el usuario se asocia al AP y está autenticado
- IPSec fuerza la re-autenticación en roaming si se pierden 3 paquetes secuenciales

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **63**

 **Redes Inalámbricas (WIFI) - Seguridad** W258-1-03

## Comparación RADIUS con VPN

- (1)
  - Con RADIUS toda la infraestructura wireless está dentro del firewall corporativo
  - Con VPN está fuera del firewall en la zona DMZ
  - A medida que crezca el parque de WLAN habrá más equipos fuera y se necesitarán más servidores VPN
- (2)
  - RADIUS protege en capa 2 cifrando el canal antes que el usuario sea autenticado y reciba la dirección IP
  - El cliente VPN necesita una dirección IP antes de ser autenticado. Está sujeto a ataques "man-in-the-middle"
- (3)
  - Al crecer la población wireless cada vez el manejo de VPNs se hace mas complejo y más costoso. Los túneles IPSec requieren mucho poder de computación y procesamientos criptográficos

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **64**

W223

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Unos se **quejan...**



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

65

W224

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

...Otros hacen algo...



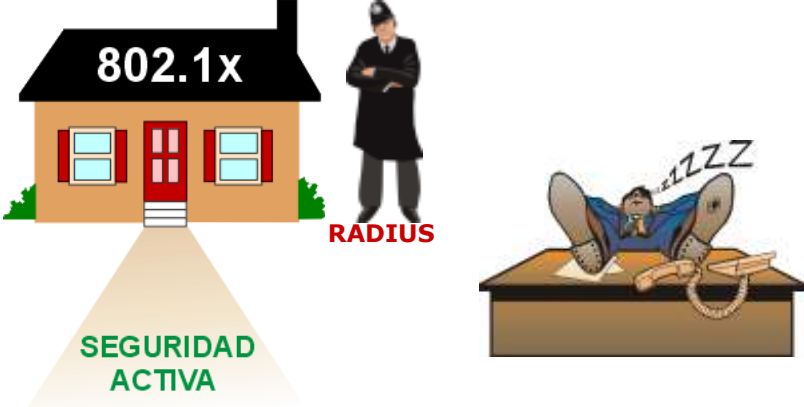
WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

66

W225

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

...y otros, DESCANSAN TRANQUILOS



**¡¡USTED DECIDE!!**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

67

W234


**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Wi-Fi Protected Access (WPA)-Estándar 802.11i

- Iniciativa de la WiFi Alliance
- Mejorar la seguridad del 802.11
- Se decidió buscar 2 soluciones
- Una urgente y temporal (intermedia)
- Otra definitiva que requiere más tiempo y nuevo hardware
- Nombre comercial WPA y WPA2
- Por defecto no vienen activados y deben ser configurados en la instalación

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados


68

 **Redes Inalámbricas (WIFI) - Seguridad** W234

Wi-Fi Protected Access (WPA)

- Disponible desde Abril de 2003
- Comienzan certificaciones
- Obligatorio desde Diciembre 2003
- Es más fuerte que WEP
- Se puede actualizar por medio de firmware o software tanto los PA como las tarjetas
- Se aprovecha el hardware existente
- Se basa en TKIP – un protocolo “temporal”
- Uso empresarial basado en 802.1x
- WPA HOME: Uso casero basado en PSK (Pre Shared Key). También se lo llama WPA-PERSONAL


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 69

 **Redes Inalámbricas (WIFI) - Seguridad**

WPA Empresarial

- Soporta 802.1x
- Autenticación mutua
- EAP
- Requiere hard cliente actualizado o WPA nativo
- Requiere un suplicante que soporte WPA
- AP WPA nativo o actualizado
- Servidor autenticación - RADIUS


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 70

 **Redes Inalámbricas (WIFI) - Seguridad**

## TKIP (Temporal Key Integrity Protocol)

- Se hizo como una "envoltura" alrededor de WEP
- Debía prevenir la alteración de datos
- Debía prevenir la fragilidad de encriptación
- Mejorar el tema de las claves estática
- Evitar el Robo de Paquetes
- Aprovechar los AP existentes
- Upgrade por firmware/software
- No degradar demasiado el rendimiento
- Procesador AP = I80386 a 25 MHz
- 90% de la capacidad ya ocupada con funciones básicas
- Debía "ahorrar" en instrucciones por limitaciones de hard


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **71**

 **Redes Inalámbricas (WIFI) - Seguridad** W233-1-04

## WPA2

- Implementación de 802.11i de la WI-FI Alliance
- Se requiere nuevos AP
- Los PDAs antiguos tampoco sirven
- Algunos clientes pueden servir
- Septiembre 2004 – Primeras Certificaciones
- WPA y WPA2 son compatibles
- Existe la opción de trabajar en modo mixto:WPA/WPA2
- Upgrade de WPA a WPA2:soft,hard
- WPA2 Personal ⇒ password
- WPA2 Enterprise ⇒ 802.1x y EAP
- WPA2 ⇒ FIPS 140-2


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **72**

 **Redes Inalámbricas (WIFI) - Seguridad**

### Nivel de Seguridad de WPA2

- AES reemplazó a 3DES
- Llevó 20 años crackear 3DES
- Si existiera una máquina capaz de crackear 3DES en 1 segundo
- Tardaría 149 trillones de años para crackear una clave 128-bit de AES
- Edad del universo  $\Rightarrow$  20 billones de años
- Se calcula que se necesitan 2 (120) operaciones para romper una clave de AES
- AES es computacionalmente eficiente  $\Rightarrow$  menor capacidad de computo

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **73**

 **Redes Inalámbricas (WIFI) - Seguridad**

### Suplicantes

- Hay diversos tipos y su elección también debe requerir un estudio previo
- En que S.O. funcionan: Linux, Windows XP, Windows 98, Windows 2000, Pocket PC, OS Palm, etc
- Que EAP soportan: LEAP, PEAP, TLS, etc
- Si soportan autenticación 802.1x
- Con que hardware funcionan: Solo Cisco?
- Otras funciones de gestión: Perfiles de Clientes, Distribución centralizada, Protección por password
- Facilidad de uso para los usuarios
- Transparencia?

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **74**

W235

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

**CASI ACABAMOS PERO...**

...¡¡Uf!!  
¡¡Qué lío!!

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 75

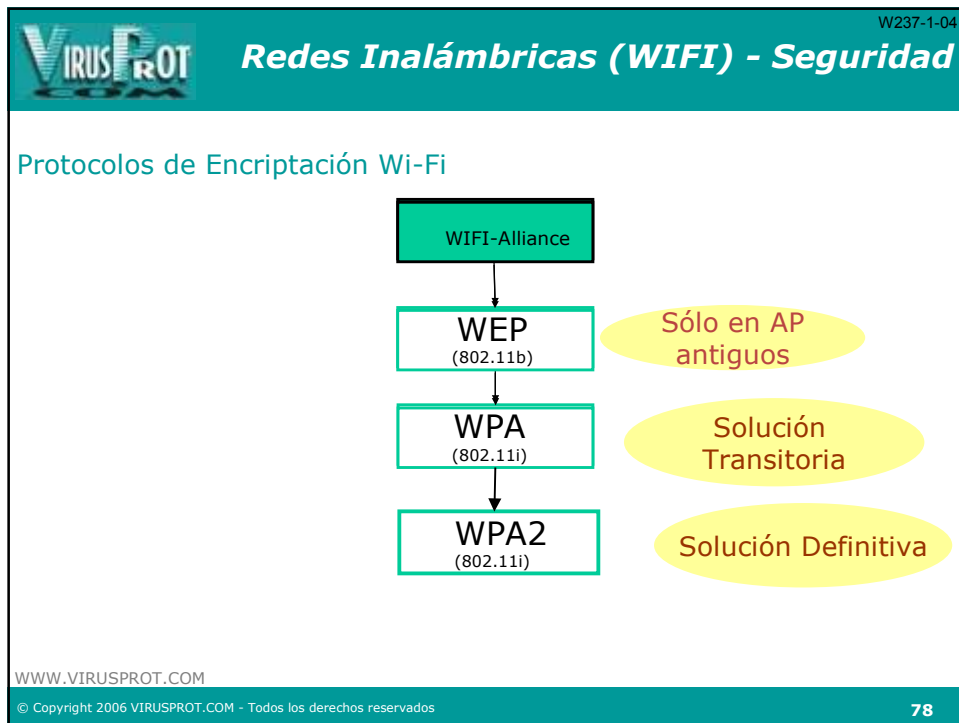
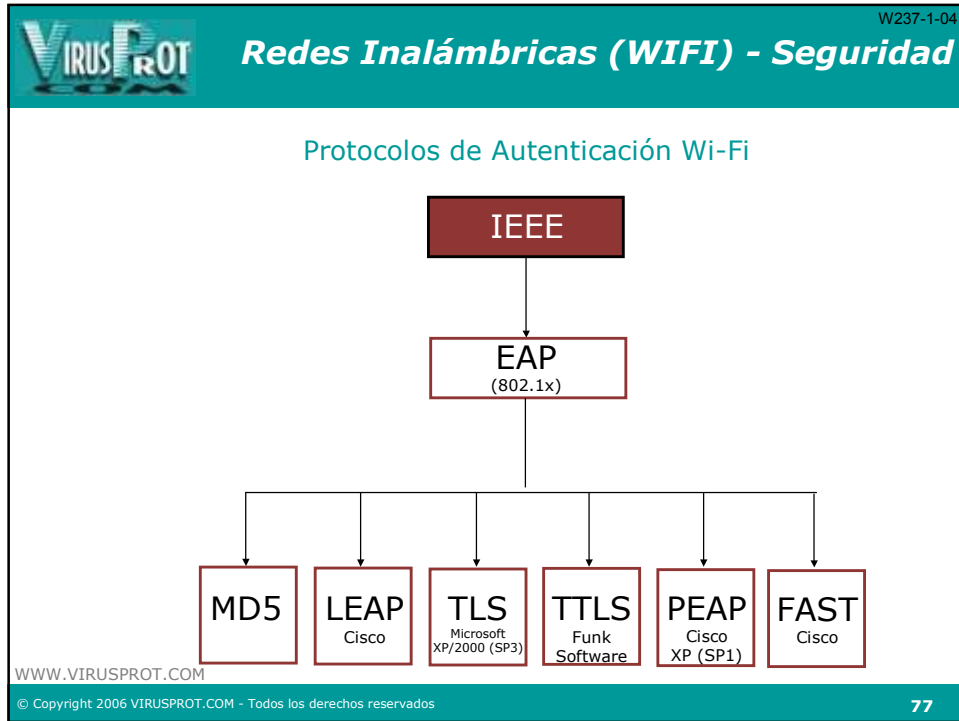
W236

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*


Evolución de Protocolos de Encriptación WIFI

Período	1999-2002	2003-2004	2005-
Función	WEP	WPA	WPA2
Algoritmo de Encriptación	RC4	RC4	AES
Encriptación	Débil	Soluciona debilidades	Fuerte
Claves	40 bits	128 bits	128 bits
Generación de Claves	Estáticas	Dinámicas	Dinámicas
Claves	Distribución manual	Automática	Automática
IV	24 bits	48 bits	48 bits
Autenticación	Débil	Fuerte, según 802.1x y EAP	Fuerte, según 802.1x y EAP

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 76



W240-1-04




## Redes Inalámbricas (WIFI) - Seguridad

### Comparativa de Protocolos EAP

Tema	MD5	LEAP (Cisco)	TLS (MS)	TTLS (Funk)	PEAP (Varios)	FAST (Cisco)
<b>Solución Seguridad</b>	Estándar	Patente	Estándar	Estándar	Estándar	Estándar
<b>Certificado-Cliente</b>	No	N/A	Sí	No (opcional)	No (opcional)	No
<b>Certificado-Servidor</b>	No	N/A	Sí	Sí	Sí	No/Sí
<b>Credenciales de Seguridad</b>	Ninguna	Deficiente	Buena	Buena	Buena	Depende
<b>Soporta Autenticación de Base de Datos</b>	Requiere Borrar la Base de Datos	Active Directory, NT Domains	Active Directory	Act. Dir., NT Domains, Token Systems, SQL, LDAP	Act. Dir. NT Domains LDAP Novell NDS Token	Act. Dir. NT Domains LDAP
<b>Intercambio de llaves dinámicas</b>	No	Sí	Sí	Sí	Sí	No
<b>Autenticación Mútua</b>	No	Sí	Sí	Sí	Sí	Sí

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 79




## Redes Inalámbricas (WIFI) - Seguridad

### Métodos de Encriptación

	Ventajas	Desventajas	Activación
<b>IPSec VPN</b>	Aprovechar herramienta existente	<ul style="list-style-type: none"> <li>No protege capa2</li> <li>Software cliente</li> <li>Difícil escalar</li> </ul>	Apropiada para FIPS
<b>WEP Estático</b>		<ul style="list-style-type: none"> <li>IV débil</li> <li>Integridad mensajes</li> </ul>	Hay que evitarlo
<b>WEP Dinámico</b>	Disminuye debilidad IV	Integridad mensajes	Implementación sencilla
<b>WPA /TKIP</b>	<ul style="list-style-type: none"> <li>Elimina debilidad IV</li> <li>Integridad mensajes</li> </ul>	Vulnerable DoS	Upgrade
<b>WPA2/AES</b>	Encriptación fuerte		<ul style="list-style-type: none"> <li>Upgrade</li> <li>Hardware</li> </ul>

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 80


Redes Inalámbricas (WIFI) - Seguridad

## Generaciones de Access Points

Aparición	Estándar	Nombre	Upgrade	Algoritmo	Autenticación
I	802.11b	WEP	Gratuito a WPA	RC4	No soporta
II	802.1x	WEP-Dinámico	Gratuito a WPA	RC4	Si soporta
III	802.11i Provisorio	WPA	A WPA2 por soft o hard	TKIP	Si soporta
IV	802.11i Definitivo	WPA2		CCMP/AES	Si soporta

WWW.VIRUSPROT.COM
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados
81


Redes Inalámbricas (WIFI) - Seguridad

## Para los más frecuentes




WWW.VIRUSPROT.COM
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados
82

 **Redes Inalámbricas (WIFI) - Seguridad**

**Comunicaciones  
Incontrolables**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **83**

 **Redes Inalámbricas (WIFI) - Seguridad**

**Comunicaciones Incontrolables**

- ¿O...Descontroladas?
- Es uno de los problemas de seguridad más graves de WiFi
- Es muy difícil o casi imposible de solucionar
- Hay muchísimos casos en que se establecen conexiones "a espaldas" del que gestiona o gobierna los sistemas corporativos
- Vimos hasta ahora diferentes maneras de proteger la red o el perímetro

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **84**



## Protección de Comunicaciones WIFI

- 802.1x es efectivo para proteger el acceso a la red. Sólo pueden entrar los autorizados después de autenticarse
- WPA/WPA2 son efectivos para proteger la comunicación entre las estaciones y el PA o entre estaciones en una red ad-hoc
- EAP es efectivo para autenticar usuarios con el RADIUS antes de acceder a la red cableada
- VPN protegen las comunicaciones entre un usuario remoto y la red corporativa

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

85




## Conexiones Descontroladas

- Las que se hacen **voluntariamente** en los aeropuertos, hoteles, etc
- Las que se consuman **involuntariamente** en los aeropuertos, hoteles, aviones, etc.
- Las que se establecen **voluntariamente** con vecinos de la organización
- Las que se establecen **involuntariamente** con los vecinos de la organización
- Ataques inalámbricos de todo tipo

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados


86

 **Redes Inalámbricas (WIFI) - Seguridad**

## Conexiones Descontroladas-Volatilidad

- Por su naturaleza son temporales
- A veces sólo unos pocos minutos
- Hay que detectarlas "en caliente". Cuando están ocurriendo
- Si no es así es imposible su detección
- Muchas se realizan lejos de los "ojos" de la organización
- Con o sin el consentimiento del usuario

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 87

 **Redes Inalámbricas (WIFI) - Seguridad**

## Conexiones Descontroladas - Riesgos

- Pueden causar daños inmensos a la empresa
- Muchas veces irreversibles
- Rompen la Seguridad Perimetral
- Son uno de los puntos más débiles en los esquemas de seguridad modernos
- Son la puerta de entrada de Virus, Spyware, Troyanos y Keyloggers
- Constituyen un punto de acceso fácil para hackers aún con escasos conocimientos

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 88

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

### Nuevas posibilidades de Acceso

Arranque Protegido Por Clave O Token

Acceso desde Internet Protegido por Defensas Perimetrales

Comunicación Infra Rojo  
Comunicación Bluetooth  
Comunicación Wifi  
Comunicación SMS

Arranque Protegido Por Clave O Token

Acceso desde Internet Protegido por Defensas Perimetrales

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 89

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

### Desafíos que Presenta Wireless

- Estos desafíos **son únicos** de esta tecnología
- Protegerse contra los ataques que explotan las transmisiones Wi-Fi
- Establecer **control físico** de los dispositivos wireless
- Prevenir instalaciones **no autorizadas.**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 90

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Guia del NIST para Wireless

- NIST (National Institute of Standards and Technology)
- Antes de comprar tecnología wireless hay que:
  - estudiar los riesgos
  - desarrollar políticas de seguridad
  - Comprar en función de los requerimientos de seguridad

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **91**

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad* W027-1-03

P. A. Hostil Conectado por Cable

Red Cableada

Access Point No Autorizado

Lurker

Company AP


Employee

Wired Network

WWW.VIRUSPROT.COM Fuente: Air Magnet  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **92**

VIRUSPROT.COM **Redes Inalámbricas (WIFI) - Seguridad** W027-1-03

P. A. Hostil Fuera del Edificio



WWW.VIRUSPROT.COM Fuente: Air Magnet

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 93


VIRUSPROT.COM **Redes Inalámbricas (WIFI) - Seguridad**

### Puntos de Acceso Hostiles

- Se define como tal, a todo AP que no haya sido instalado y autorizado por la organización
- Hay 3 fuentes
- **Insiders** – Empleados de nuestra organización. Lo más probable es que sean AP baratos y mal configurados. Seguro que no siguen la política de la empresa
- **Hackers** – Generalmente mal intencionados. Pueden estar configurados con el mismo ESSID de la organización. Pueden lanzar un ataque "Man-in-the-middle"
- **Vecinos** – Esta población está aumentando vertiginosamente y no lo podemos evitar. Windows XP se conecta automáticamente a la mejor conexión del vecindario

WWW.VIRUSPROT.COM


© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 94

 **Redes Inalámbricas (WIFI) - Seguridad**

## Otros Dispositivos Hostiles

- Dispositivos Cliente (PDAs, Laptops) controlados por atacantes y creando "puentes" con equipos conectados a la red cableada
- Dispositivos Cliente, involucrados en Redes Ad-Hoc. En este caso no se aplica 802.1x ni las claves dinámicas.
- Teléfonos GSM/WIFI creando conexiones a dispositivos WIFI


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **95**

 **Redes Inalámbricas (WIFI) - Seguridad** W206-1-04

### P. A. Hostiles - Estrategia

- Prevención
- Detección
- Bloqueo
- Localización
- Eliminación


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **96**

Redes Inalámbricas (WIFI) - SeguridadW244-1-03

### Detección desde la Red Cableada con Herramientas Tradicionales

- **Pros**
  - Es más sencillo detectar desde la oficina
  - Se puede monitorear sitios remotos
- **Contras**
  - El software existente aún no está muy preparado para detectar PA
  - Crea falsas alarmas en IDS y firewalls personales
  - Sólo es eficaz en casos muy particulares

WWW.VIRUSPROT.COM© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados97


Redes Inalámbricas (WIFI) - SeguridadW242-1-03

### Pros y Contras de los Analizadores

- **Pros**
  - Efectivos cuando el PA emite el SSID
- **Contras**
  - El analizador no los "ve" cuando hay interferencias
  - Muchos no "ven" PA que no transmiten el SSID
  - El analizador debe estar dentro del rango del PA
  - El administrador debería recorrer las instalaciones con un sniffer
  - El ataque o la conexión deben estar realizándose cuando uno pasa con el Analizador

WWW.VIRUSPROT.COM© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados98

W279-1-03

 **Redes Inalámbricas (WIFI) - Seguridad**


Analizadores (1)

- Móviles
  - PDA
  - Portátiles
- Función
  - Monitoreo de PAs
  - Monitoreo ambiental
  - Site Survey

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 99

W280-1-03

 **Redes Inalámbricas (WIFI) - Seguridad**

Analizadores (2)

- Detección de PAs hostiles
- Detección Interferencias
- Problemas de mantenimiento
- Detección de intrusos
- Ubicación óptima de cada PA
- Árbol de SSID
- Jerarquía de conexiones
- Estadísticas

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 100

VIRUSPROT.COM *Redes Inalámbricas (WIFI) - Seguridad* W663-1-04

## AR – Access Controllers



Appliances

# Switches WLAN


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 101

VIRUSPROT.COM *Redes Inalámbricas (WIFI) - Seguridad* W279-1-03

## Monitoreo – Recolección de Datos

- Por medio de laptops de usuarios
  - No es un medio dedicado y sólo funciona cuando no trabajan
  - Esto mejora con computadores dedicados
- Por medio de Puntos de Acceso
  - Alcance limitado
  - Limitaciones 11a/b/g
  - Limitaciones de canales
  - DoS
- Por medio de Sensores
  - Costos
  - Tiempo de Instalación

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 102

 **Redes Inalámbricas (WIFI) - Seguridad** W281-1-04

WLAN Switches (1)

- Administradores reportan problemas:
  - localizar clientes
  - contabilizar clientes
  - optimizar anchos de banda
  - upgrade de PA numerosos
  - PAs fuera de servicio
  - controlar la potencia de RF
- Solución: ¡Unas buenas zapatillas y ropa del gimnasio!


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 103

 **Redes Inalámbricas (WIFI) - Seguridad** W282-1-03

WLAN Switches (2)

- Cajas Negras
- Hard y Soft
- Cada uno su propio estándar
- 5 start-ups
- Solucionan Problemática del IEEE 802.11k y del 802.11e (QoS)
- Key players

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 104

 **Redes Inalámbricas (WIFI) - Seguridad** W665-1-04

WLAN Switches (3)  
*Nuevas Funciones*

- Comprobar la salud de cada PA
- Cuánta gente conectada
- Quién está conectado
- Qué servicios utilizan
- Generan estadísticas
- Monitorean el espectro de RF
- Ayudan a calibrar el PA
- Monitorean para detectar clientes con inconvenientes
- Detección de interferencias
- Previenen ataques DoS contra PAs y clientes
- Balanceo de cargas

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 105

 **Redes Inalámbricas (WIFI) - Seguridad** W665-1-04

WLAN Switches (4)  
*INFORMACIÓN - Herramientas*

- Señal/Ruido
- Ancho de Banda
- Exportar Información
- Utilización de los canales
- AP desconfigurados
- Velocidades de transmisión
- Estándar utilizado para conexión
- Red Ad-hoc
- Encriptación por hardware (FIPS 140-2)
- Paquetes perdidos
- Interferencias entre PAs

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 106

W666-1-03

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Políticas de Seguridad

- Físicas
  - Paredes
  - Vigilancia
- Laboral
  - PAs hostiles
  - Dispositivos móviles privados
- Viajeros frecuentes
  - Chequeos
  - Cuarentena

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

107

W666-1-03

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Políticas de Seguridad (2)

- Visitantes
  - Pueden usar su máquina?
  - A qué servicios tienen acceso?
  - Claves?
- Observación Física
  - PAs hostiles
  - Signos de warchalking

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

108

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

Políticas y Controles según GAO

- Desarrollar políticas que gobiernen la **implementación y el uso** de wireless
- Establecer programas de monitoreo que ayuden a confirmar que las redes wireless están **operando con seguridad**
- Entrenar a empleados y contratistas en las políticas de wireless de la agencia
- Definir requisitos de configuración para las instalaciones
- **Reconocer que el desarrollo de políticas es esencial para reducir de una manera económica el riesgo a la información debido a la tecnología**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 109

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

¿Quiénes son tus usuarios?

- ¿Tus amigos?
- ¿Tus enemigos?
- ¿Te preocupan?
- ¿Te colaboran?
- ¿Cumplen con la política establecida?



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 110

VIRUSPROT.COM **Redes Inalámbricas (WIFI) - Seguridad** V038-1-04

## Usuarios... ¡Como siempre!

Categoría	Porcentaje
En gran parte	47%
Cuando les conviene	31%
Por casualidad	12%
Al pie de la letra	7%
Nunca	3%

Fuente: Watchguard  
[www.watchguard.com](http://www.watchguard.com)

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **111**

VIRUSPROT.COM **Redes Inalámbricas (WIFI) - Seguridad**

## ¿Qué factores contribuyeron más, a los ataques a sus sistemas?

Factor	2005	2004	2003
Lack of central knowledge of network strategies	20%	20%	20%
Lack of control associated with shared access to your network by third parties	8%	11%	7%
Inadequate levels of security on home and other computers used by clients, customers and staff	20%	20%	20%
Remote accessibility and/or connectivity of your servers to the Internet	33%	24%	19%
Poor security culture in organisation	40%	38%	30%
Inadequate security technologies or controls	0%	0%	0%
Lack of security technologies	10%	14%	18%
Inadequate human resources for system handling and other security practices and procedures	24%	33%	48%
Inadequate staff training and education in security practices and procedures	47%	42%	40%
Exploitation of insider knowledge or access	10%	11%	11%
Exploitation of unpatched or unprotected software vulnerabilities	43%	20%	16%
Exploitation of default (out of the box) operating system configurations	21%	21%	21%
Exploitation of misconfigured operating systems, applications or network devices	21%	24%	24%
None of the above	10%	10%	10%
Other	8%	8%	8%

Fuente: 2005 Australian Computer Crime & Security Survey

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados **112**

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Principales Causas de Riesgo Para la Información

What do you feel are the major causes of corporate data risk, now and in the future?

Causa de Riesgo	now (%)	Future (%)	not a major issue (%)
Human incompetence, threat from disgruntled employees	~85	~10	~5
Computer, network or software failure	~45	~45	~10
Increasingly clever methods of attack, e.g. more complex viruses, spyware	~45	~45	~10
Theft of corporate equipment	~35	~45	~20
Extension of corporate network through remote working, wireless access	~45	~45	~10
Hacking or competitor espionage	~45	~45	~10
Terrorist Threat, natural disaster, fire	~25	~45	~30

From IT Security – Bridging the Gap – Summer 2004

Fuente: Quocirca

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

113

**VIRUSPROT.COM** *Redes Inalámbricas (WIFI) - Seguridad*

## Usuarios - Desconocimiento

- Redes Ad-Hoc / aviones, aeropuertos
- Phishing Hot-Spots
- Peligro visitar otras redes
- Warchalking – Wardriving
- Encriptar comunicación
- Puntos de acceso hostiles

**Imprescindible capacitar a todos los usuarios de Wireless, que dentro poco serán la mayoría**

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

114

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

## CAPACITACIÓN

- Conferencias (1-2 horas) - Información sobre peligros: phishing, spam, hacking, PA hostiles, equipos móviles.
- Charlas en pequeños grupos - La gente se ve más comprometida y acata más las políticas
- Seminarios (4 - 8 horas) - Grupos especializados: IT, Seg. Informática, Depto. Ing., Depto. Programación, Arquitectos, Dibujantes, usuarios de Lap-Tops/PDAs/Celulares, etc.
- Control y Seguimiento **externo** - **Factor Clave del Éxito!!!**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

115

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

## ¿Qué pretendemos del usuario?



- Es **Imprescindible** para **reducir** la **inseguridad** de ese cliente o satélite
- ¿Cómo lograrlo?



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

116

VIRUSPROT.COM W602-1-04

## Redes Inalámbricas (WIFI) - Seguridad

SEGURIDAD SATELITAL  
(PAPA-MÓVIL)

20%/30%  
Perimetro Red Cableada

Punto Móvil

Red WIFI

Punto Móvil

Punto Móvil

Punto Móvil

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

117

VIRUSPROT.COM

## Redes Inalámbricas (WIFI) - Seguridad

Nuevos escenarios – Nuevos Peligros

- Por dónde se rompe la cadena de seguridad?
- **Por los puntos más débiles**

**NUEVOS PUNTOS DÉBILES**

Computadores móviles sin protecciones  
Usuarios móviles desinformados  
Usuarios móviles despreocupados  
Falta de controles en tránsito de equipo  
Huecos de Wi-fi  
Huecos de Bluetooth

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

118

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

El mundo evoluciona

<p><b><u>Pasado</u></b></p> <ul style="list-style-type: none"><li>• Entorno: Redes cableadas</li><li>• Un equipo por usuario en lugar fijo</li><li>• Control grande sobre las actividades del usuario</li><li>• Información confidencial en servidores – equipos sin disco</li><li>• Puntos débiles ⇒ <b>Comunicaciones</b></li><li>• Robo equipos ⇒ <b>Cero</b></li></ul>	<p><b><u>Actualidad</u></b></p> <ul style="list-style-type: none"><li>• Entorno: Cables/Movilidad/ Wi-Fi</li><li>• Equipos múltiples – lugares múltiples</li><li>• Pérdida progresiva de control sobre actividades del usuario</li><li>• Información confidencial en Laptops, PDAs y teléfonos móviles</li><li>• Puntos débiles ⇒ <b>Movilidad, WiFi, cada uno de los equipos</b></li><li>• Robo equipos ⇒ <b>Considerable</b></li></ul>
--	--

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 119

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad* W267-1-03

**EUREKA!!**



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 120

VIRUSPROT.COM *Redes Inalámbricas (WIFI) - Seguridad* W273-1-03

**Un momento...**




**nos falta algo...**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 121

VIRUSPROT.COM *Redes Inalámbricas (WIFI) - Seguridad*

¿Hay cosas que... saben los hackers y Ud. no ?!



WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 122

VIRUSPROT.COM **Redes Inalámbricas (WIFI) - Seguridad** W537-1-04

## Ataques DoS

- Torrente de Autorizaciones ⇒ **Saturar PA**
- Ruido RF ⇒ **Saturar el ambiente**
- Spoofed Deauthentication ⇒ Air-Jack (Linux)
- Broadcast Deauthentication ⇒ Hunter-Killer
- FakeAP – Torrente de Beacons (contra wardrivers) ⇒ **HotSpots**
- EAP-Handshake ⇒ **Autenticaciones** –EAPOL
- WPA – Modificar paquetes – MIC: Más de 2 en 1 min. ⇒ TKIP impide conexiones ⇒ **favorece DoS**
- Power Save – Reemplazar a la estación mientras esta “descansa” y robarle los paquetes

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 123

VIRUSPROT.COM **Redes Inalámbricas (WIFI) - Seguridad** W537-1-04

## Imitación/Falsificación

- **Mac address spoofing** ⇒ **Air-Jack**
- **Imitación de PA** ⇒ Usa SSID válido
- **Session Hijacking**: El atacante desactiva a un cliente autenticado mediante DoS y se conecta al servidor en lugar del legítimo. Luego lo deja volver a conectarse. Este ataque suele durar un par de segundos
- **Man-In-The-Middle**: El mismo paquete Air-Jack trae una aplicación denominada “Monkey\_Jack” que automatiza el ataque
  - Una estación (W) está autenticada con PA1
  - El atacante tiene un laptop con 2 tarjetas wifi. Una emula un AP (PA2). También se puede con un AP y un computador
  - El atacante envía paquetes de Desautenticación a W
  - W queda desautenticada y busca un AP para volver a conectarse
  - Encontrará a PA2 y si se conecta **hará de puente entre W y PA1**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 124


 **Redes Inalámbricas (WIFI) - Seguridad** W537-1-04

## Intrusión en Redes y Clientes

- "Honeypot" PA ⇒ Emite SSID empresa
- Roaming a PA inválido
- Pas mal configurados
- Puntos Acceso Hostiles (3 categorías)
- Redes Ad-Hoc ⇒ **PELIGRO !!!**
- ASLEAP ⇒ **CISCO**
- VPN – Comunicaciones con Printers y dispositivos no encriptadas
- Aprovechamiento de Vulnerabilidades

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 125


 **Redes Inalámbricas (WIFI) - Seguridad**

## Hotspots - Problemática

- Son PA públicos instalados con diversas finalidades
- Aeropuertos, hoteles, Universidades, Centros Comerciales, etc.
- Gratuitos: La finalidad es atraer a los usuarios y/o fidelizarlos. Aumentar los consumos
- De Pago: La finalidad es vender servicios de acceso a Internet y vender publicidad
- La seguridad cuesta plata
- La seguridad se divide en dos
- El tramo desde el Access Point hasta la red del ISP
- El tramo inalámbrico entre el dispositivo móvil y el Access Point
- A veces el AP tiene doble función

WWW.VIRUSPROT.COM


© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 126

 **Redes Inalámbricas (WIFI) - Seguridad**

## Wi-Phishing / Evil Twins (1)

- Consiste en un AP "ofreciendo" conexión wireless a Internet en lugares públicos
- Tienen la misma apariencia que cualquier servicio público legítimo
- Cómo es lógico, solicitan claves, número de tarjetas de crédito, etc
- Cualquiera lo puede hacer con un laptop configurado como Access Point (Soft Access Point)
- El "Access Point" enviará Beacons y SSID para que otros computadores sepan que está disponible
- El hacker puede inclusive utilizar nombres de empresas reconocidas para dar más credibilidad a su propuesta


WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 127

 **Redes Inalámbricas (WIFI) - Seguridad**

## Wi-Phishing / Evil Twin (2)

- Generalmente usan un SSID por defecto. Se encontrarán con muchísimos usuarios que no han modificado la configuración de fábrica
- Si la señal del AP falso es más fuerte que la del ISP legítimo, los dispositivos tenderán a conectarse al AP falso
- Hay alguna diferencia entre el Wi-Phishing y el ataque Evil Twin aunque utilizan métodos similares
- El Wi-Phishing "sólo" busca sacar alguna información del usuario conectado, como contraseñas y tarjetas de crédito

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 128

 **Redes Inalámbricas (WIFI) - Seguridad**

## Hotspot – Consejos (1)

- **No los use si no está convencido que es seguro:** Les deben dar una clave, cómo mínimo WEP. Mejor si es WPA/WPA2
- **Trate de usar "sólo" correos de tipo Web:** Hotmail, Yahoo! o Gmail y seleccione la opción más segura. Si sus correos van encriptados, mejor.
- **No use Mensajería Instantánea:** MSN Messenger y Yahoo! Envían todo en claro. Existen programas para encriptar las conversaciones con IM
- **Verifique que su tarjeta Wi-Fi está configurada de modo seguro:**
  - No está configurada para que se conecte automáticamente a cualquier red
  - Desabilite el modo ad-hoc
  - Desabilite la opción de Wi-Fi si no está conectado o quite la tarjeta, si es posible

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

129

 **Redes Inalámbricas (WIFI) - Seguridad**

## Hotspot – Consejos (2)

- **No se conecte a la red de la empresa,** a menos que esté protegido por VPN
- **Verifique que el firewall de Windows XP está activado,** a menos que esté utilizando otro firewall personal
- **Desactive "File Sharing"**
- **Mantenga el S.O actualizado.** No postergue la aplicación de parches
- **Trate de utilizar Hotspots conocidos:** A veces se puede contratar servicios que ofrecen garantías, como certificado digital
- **Preste mucha atención a los mensajes que aparecen en pantalla:** No diga automáticamente "YES" a todo

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

130

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

## Conferencia RSA – Febrero 2005



The screenshot shows a web browser window displaying an article on the VirusProt website. The article title is "Intentos de Phishing y Puntos de Accesos Hostiles en la Conferencia de RSA". The text discusses security incidents at the RSA conference, mentioning "Soluciones a medida" and "Herramientas GRATUITAS". The article is dated 30/02/05. The browser's address bar shows "http://www.virusprot.com".

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 131

**VIRUSPROT** *Redes Inalámbricas (WIFI) - Seguridad*

## Problemas de Seguridad Conferencia RSA

- 71 Redes Ad-hoc
- 48 ataques de phishing
- 116 intentos de spoofing de direcciones MAC
- 15 dispositivos ejecutando NetStumbler
- 45 ataques DoS contra AP
- 35 ataques DoS contra estaciones de trabajo
- 28 Puntos de Acceso no autorizados
- Estos monopolizaron 78% del tráfico de conexión a Internet

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados 132

 **Redes Inalámbricas (WIFI) - Seguridad**


## Best Practices – Recopilación de Medidas de Seguridad Para WiFi

**Políticas de Gestión y Administración**

- Establecer políticas y procedimientos de seguridad para la utilización de la tecnología WiFi
- Verificar que los usuarios de esta tecnología están entrenados y conocen los riesgos asociados con su utilización
- Realizar un estudio de riesgos
- Realizar con periodicidad auditorías de seguridad para verificar la seguridad de la red y detectar los cambios en el entorno
- Mantener actualizado un inventario de AP y dispositivos Wireless que pertenecen a la organización
- Asegurar que ningún dispositivo WiFi es utilizado hasta que no cumpla con las políticas de seguridad

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

133

 **Redes Inalámbricas (WIFI) - Seguridad**

## Best Practices -2

**Políticas Tecnológicas**

- Testear el alcance exacto de la cobertura de RF de cada AP, sobre todo hacia el exterior
- Verificar periódicamente que los AP no han sido reseteados sin autorización
- Cambiar el SSID por defecto
- Desactivar el broadcast del SSID
- Verificar que el SSID no incluya datos sobre la organización, la división, la calle, etc
- Verificar que el AP esté sintonizado en canales diferentes a los vecinos
- Verificar que se han modificado los parámetros de fábrica
- Activar el protocolo de encriptación más potente disponible
- Verificar que las claves tengan una longitud adecuada y cumplan con los preceptos de seguridad establecidos

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

134



## Best Practices -3

- Cambiar periódicamente las contraseñas
- Limitar la potencia de transmisión de los AP en todo lo posible
- Instalar un firewall personal en los clientes wifi
- Instalar un Antivirus en los clientes wifi
- Instalar herramientas de protección wifi
- Instalar software de "end-point security"
- Desactivar los archivos compartidos cuando sea posible
- Desactivar el modo Ad-Hoc siempre que sea posible
- Implementar filtrado MAC
- Utilizar VPN en los casos que sea posible o necesario
- Instalar todos los parches necesarios en S.O, AP, suplicantes, RADIUS, VPN, firewalls, etc

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

135



## Best Practices -4

- Revise los logs frecuentemente
- Desactive DHCP
- Utilizar 802.1x /EAP y RADIUS y Autenticación Mutua
- Configure los suplicantes adecuadamente
- Proteja la configuración del suplicante
- Implemente herramientas de monitoreo del espacio RF
- Si puede utilizar un switch WLAN, mejor
- Establezca una rutina de verificación de AP hostiles
- Mantenga un inventario de los AP que existen en la vecindad y que pueden interferir con sus usuarios
- Mantenga un inventario de los sitios "ruidosos" o con interferencias de su vecindad

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

136

VIRUSPROT.COM *Redes Inalámbricas (WIFI) - Seguridad* V001-1-04

Antes de que sea demasiado **TARDE...**



**¡PROTÉJELO!**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

137

VIRUSPROT.COM *Redes Inalámbricas (WIFI) - Seguridad*

**¡Le agradecemos su atención!**

¿Alguna Pregunta ?

**Ing. Eduardo Tabacman –  
[internacional/Arroba/virusprot.com](mailto:internacional@aroba.virusprot.com)**

WWW.VIRUSPROT.COM  
© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

138



## Enlaces de Interés

- Diseño de una Red Inalámbrica Segura – Business Case U. De Cataluña : [www.virusprot.com/art43.html](http://www.virusprot.com/art43.html)
- Índice de Noticias de Seguridad WiFi y Redes Inalámbricas: [www.virusprot.com/wfactualidad.html](http://www.virusprot.com/wfactualidad.html)
- Panorama de la Seguridad Wifi: [www.virusprot.com/indexwf.html](http://www.virusprot.com/indexwf.html)
- White Paper sobre Seguridad Wifi: [www.virusprot.com/whitepap1.html](http://www.virusprot.com/whitepap1.html)
- Guía para Seleccionar adecuadamente Access Points: [www.virusprot.com/whitepap4.html](http://www.virusprot.com/whitepap4.html)
- Artículos sobre Redes Inalámbricas: [www.virusprot.com/charlaswifi.html](http://www.virusprot.com/charlaswifi.html)

WWW.VIRUSPROT.COM

© Copyright 2006 VIRUSPROT.COM - Todos los derechos reservados

139