



Wireless Insecurity

Ing. Fabián Calvete

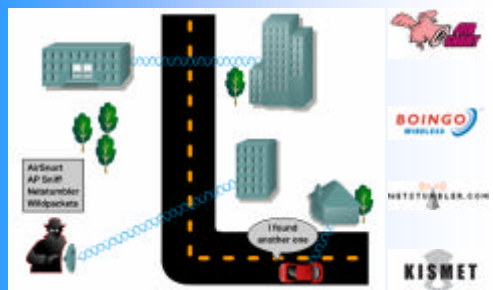
Vulnerabilidades

- Tecnología
 - TCP/IP
 - SSID y WEP
 - Proceso de asociación
 - Interferencia inalámbrica
- Configuración
 - Passwords predeterminadas
 - Servicios innecesarios
 - Pocos o ningún filtro
- Políticas
 - Política de Seguridad débil
 - Ninguna Política de Seguridad
 - Incumplimiento de las Políticas
 - Acceso físico
 - Supervisión pobre o no existente

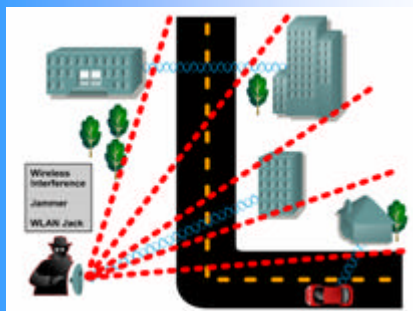
Amenazas

- Internas
- Externas
- Estructuradas
- No estructuradas

Ataques a la seguridad—Reconocimiento y Acceso



Ataques a la seguridad—Denegación de Servicio (DoS)



Consideraciones Sobre Seguridad WLAN

Autenticación: Sólo deberían estar permitidos usuarios y dispositivos autorizados.

Encriptación: El tráfico debería estar protegido de accesos no autorizados.

Seguridad de la Administración: Sólo usuarios autorizados deberían poder acceder y configurar las distintas interfaces del AP.

Seguridad básica en WLAN

Requerimientos de seguridad para las WLANs

Primera generación

- SSID
- Autenticación MAC
- WEP estático de 40 o 128 bits

Segunda generación

- Autenticación centralizada en servidores AAA (RADIUS)
- WEP dinámica de 128 bits
- VPN

Actualidad

- 802.1x
- TKIP
- MIC
- AES
- Detección de APs clandestinos

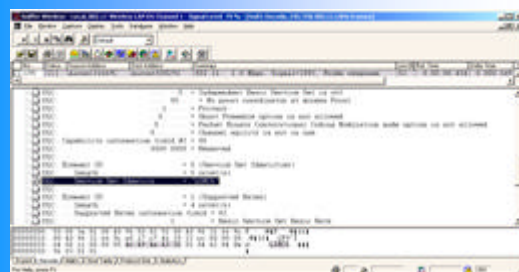


SSID (Service Set Identifier)

Permite conectarse a una red inalámbrica
Está compuesto por un máximo de 32 caracteres alfanuméricos
Es sensible a mayúsculas y minúsculas (Case Sensitive)
Podemos hallarlo en:

- ✓ Balizas (Beacon)
- ✓ Solicitudes de sonda
- ✓ Respuestas de sonda
- ✓ Solicitudes de asociación y reasociación

SSID para conexión



Autenticación MAC

Mecanismo de autenticación débil
Las direcciones MAC se envían sin encriptar
Las direcciones MAC pueden ser capturadas y enmascaradas

WEP



WEP usa claves.
WEP codifica las comunicaciones entre el AP y el cliente.
El AP y el cliente deben usar las mismas claves WEP.
Las claves WEP encriptan unicast y multicast.
Basado en el algoritmo simétrico RC4
WEP es atacado con facilidad

WEP — Encriptación

Opciones de encriptación

- Ninguna encriptación
- Encriptación de 40 bits
- Encriptación de 128 bits


WEP basado en software

- 20% performance hit (128 bits)

WEP basado en Hardware

- 3% performance hit (128 bits)

El WEP Estático requiere que alguien “configure” TODOS los clientes y APs



¿Qué es un IV?

Stream Cifrada — con IV

12345

TextoClaro SIC → WEP → TextoCifrado XXYYZZ

Sin un IV, el TextoClaro siempre producirá el mismo TextoCifrado; un atacante podrá “ver” los patrones y predecir el TextoClaro

Stream Cifrada — con IV

AC5+12345

TextoClaro SIC → WEP → TextoCifrado ZZYYAA

Con el IV, el TextoCifrado cambiará cuando el IV cambie, por lo tanto será más difícil que un atacante “vea” los patrones y pueda predecir el TextoClaro

El mismo paquete de textoclaro no debería generar el mismo paquete de textocifrado
IV es aleatorio, y cambia por paquete

WEP/IV en la seguridad inalámbrica del 802.11

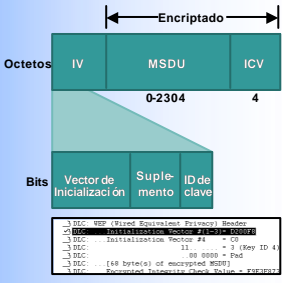
Los IVs de 802.11 son valores enteros de 24 bits

Aumenta las claves de 40 bits a 64 bits

Aumenta las claves de 104 bits a 128 bits

Se envía en texto claro

La recuperación de la clave es posible debido al análisis estadístico del texto claro y una serie de IV “débiles”



Seguridad avanzada en WLAN

WPA - 801.11i – WPA2

Seguridad de WLAN : Autenticación 802.1X

Autenticación Mutua

EAP- TLS

- EAP-Seguridad de Capa de Transporte
- Implementación de la Autenticación Mutua
- Utiliza certificados digitales

LEAP

- EAP “Liviano”
- Usa One Time Passwords (OTP)
- Soportado por casi todos los principales SO: WinXP/2K/NT/ME/98/95/CE, Linux, Mac

PEAP

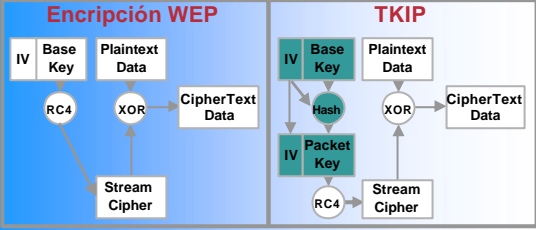
- EAP “Protegido”
- Utiliza certificados o One Time Passwords (OTP)
- Soportado por Cisco, Microsoft y RSA



Implementación TKIP

WEP usa un IV y una clave base; esto permite IVs débiles los cuales pueden ser comprometidos

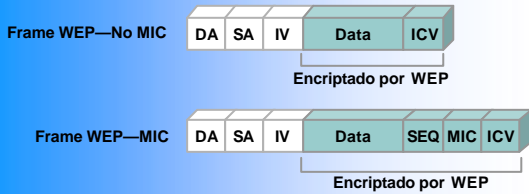
TKIP usa el IV y la clave base para producir un hash que será la nueva clave. En consecuencia habrá una nueva clave por cada paquete, lo que soluciona el problema de claves débiles



Message Integrity Check (MIC)

MIC se basa en un valor aleatorio, las direcciones MAC de destino y de origen, y en el payload

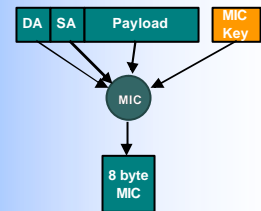
MIC usa una función de Hash para producir un valor único que se envía en el frame



Michael MIC[®] protege MSDUs

MIC está basado en:

- Valor aleatorio
- MAC destino
- MAC origen
- Payload



Evolución

- ✓ TKIP / WPA
 - Sucesor de WEP
 - TKIP es parte de Wi-Fi Protected Access (WPA)
- ✓ AES
 - Es el "Gold Standard" de la encriptación
 - AES es parte del estándar 802.11i (AES se incluye en WPA2)

Incrementar la seguridad mediante el uso de filtros (ACL)

Considerar a las VPNs como alternativa o complemento

Conclusiones



Algunas herramientas

Wardriving:

- NetStumbler (www.netstumbler.org)
- Kismet (www.kismetwireless.net)

Sniffers:

- AiropEEK (www.wildpackets.com/products/airopEEK)
- Ethereal (www.ethereal.com)
- Sniffer Wireless (www.sniffers.com/products/sniffer-wireless)

WEP Crack:

- Aircrack (www.softonic.com/ie/36121/Aircrack)
- Wepcrack (wepcrack.sourceforge.net)
- Aircsnort (airsnort.shmoo.com)
- WepLab (wepcrack.sourceforge.net)



Fin

Ing. Fabián Calvete

Colaboración: Hernán Serdá

fcalvete@sicinformatica.com.ar
www.sicinformatica.com.ar