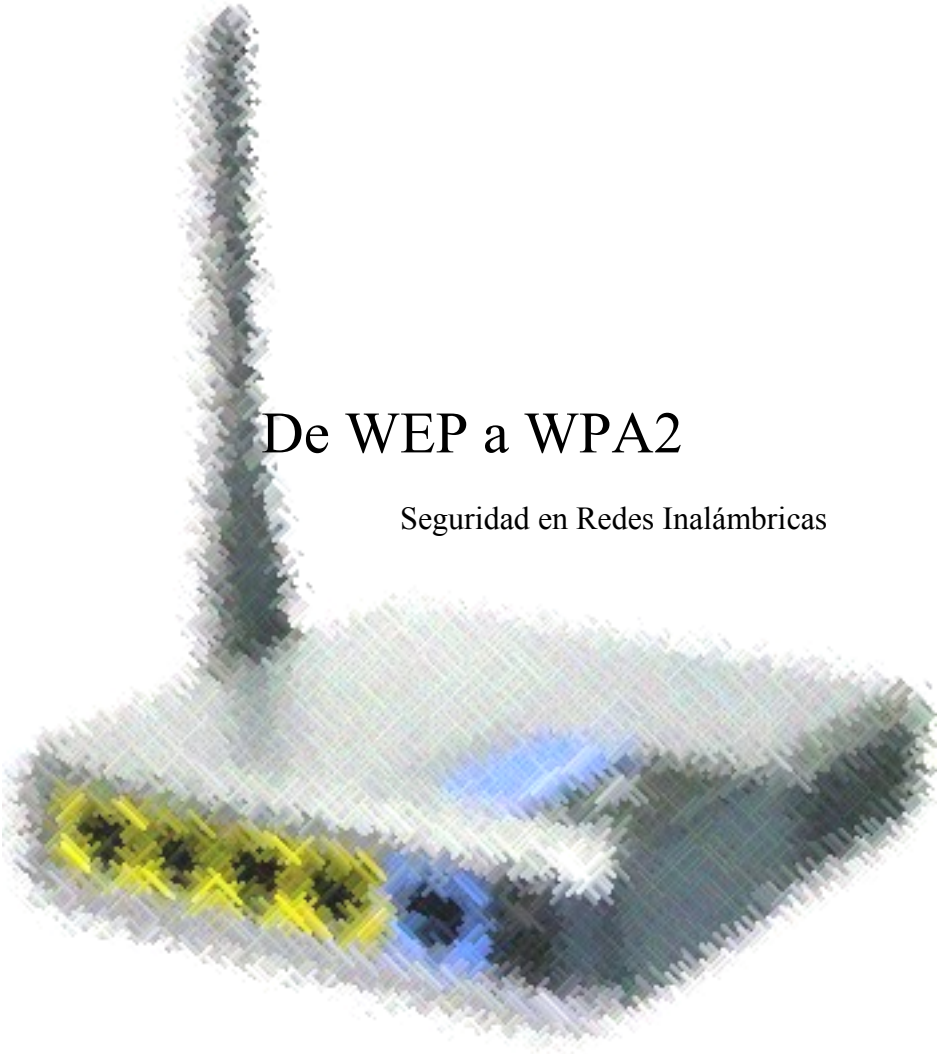
Universidad Técnica Federico Santa María
Departamento de Electrónica



De WEP a WPA2

Seguridad en Redes Inalámbricas

Profesor: Agustín González
Autor: Patricio Fernández
Fecha: 04 de agosto de 2008

Resumen

WEP significa Privacidad Equivalente a Cableado (Wired Equivalent Privacy). Fue publicada por la IEEE en la norma 802.11 en septiembre de 1999. Su objetivo es equiparar el nivel de seguridad de WLAN y LAN, sin embargo posee una serie de falencias que permiten ataques de diversos tipos como obtener accesos piratas a la red y escuchar lo que se transmite por la red inalámbrica, entro otros varios.

Los administradores de redes que usan WEP pueden realizar configuraciones de modo de fortalecer la seguridad.

Luego de varios años de desarrolla WPA y WPA2 que consiguen colocar una barrera mucho más alta a los atacantes, usando nuevos métodos de encriptación, claves más largas y métodos más robustos.

Introducción

En este trabajo se ha propuesto comprender el paso desde la tecnología WEP a la tecnología WPA.

Un aspecto inicial que se atiende es la deficiencia de seguridad que tiene la Wireless LAN (WLAN) con respecto de LAN.

Este trabajo presenta una definición de WEP, luego de la cual se explica la forma en que funciona y como opera y cual son los puntos en que su seguridad se sustenta. Finalmente se describe WEP desde el punto de vista de sus vulnerabilidades y la forma en que son aprovechadas por atacantes.

La sección dedicada a WAP hace un poco de análisis histórico para situar esta tecnología en un marco correcto, para concluir explicando sus virtudes y buscando la forma en que su seguridad puede ser vulnerada.

WLAN

Wireless LAN surge para permitir la conexión a la red corporativa a estaciones móviles de trabajo como los Notebooks y para evitarse el cableado que significa LAN. De esta forma se instala un Punto de Acceso (AP) que normalmente no es otra cosa que un router inalámbrico, de modo que los equipos que están al alcance de la señal del Punto de Acceso pueden integrarse a la red. Pero entregar el servicio de esta forma resulta en serios inconvenientes de seguridad.

Los problemas que presenta WLAN provienen precisamente del hecho de ser inalámbrico, pues se elimina de esta forma una importante barrera de seguridad como lo es el cable, puesto que cualquier persona que constase con los medios podría "escuchar" las conversaciones que sostiene el Punto de Acceso con los integrantes de la red inalámbrica. Además el problema no se queda ahí, sino que además de este ataque pasivo en que sólo se escucha, se puede realizar un ataque activo a la red desde cualquier lugar cercano. Un ataque activo puede ser desde obtener simplemente acceso a Internet, hasta perjudicar malintencionadamente la red.

Es por ello que la IEEE desplegó en la norma 802.11 un mecanismo de seguridad para las redes inalámbricas llamado WEP de modo de resolver las vulnerabilidades antes presentadas, entregándoles a los administradores de las redes esta herramienta opcional.

WEP

Definición

WEP significa Privacidad Equivalente a Cableado (Wired Equivalent Privacy). Esta herramienta de seguridad fue publicada por la IEEE en la norma 802.11 en septiembre de 1999 y permaneció intacta por varias revisiones de esta norma. Tal como lo indica su nombre, su objetivo es equiparar el nivel de seguridad de WLAN y LAN.

Funciones

WEP realiza dos funciones una es cifrado y la otra es autentificación.
Es un hecho conocido el que las transmisiones inalámbricas pueden ser captadas por terceros de forma pasiva. WEP hace que estas transmisiones no tengan sentido para otro que no sea el destinatario, puesto que los mensajes quedan escritos en clave, es decir cifrados.
El problema de que una máquina no deseada forme parte de la red, corresponde al problema de la autentificación. WEP da la opción de liberar el acceso a la red o de si lo restringe mediante el uso de una contraseña.

Operación: Cifrado

El procedimiento de cifrado es el siguiente:
1. El texto plano recibe una suma de chequeo llamada CRC-32 para garantizar la integridad del texto transmitido. CRC-32 se usa por ser simple y muy poderoso detectando errores en canales de alto ruido.
2. Se forma una cadena de 64 bits, utilizando 24 bits del llamado vector de iniciación y 40 bits correspondientes a la clave de autentificación de la red. El vector de iniciación es un vector binario generado unilateralmente por el punto de acceso.
3. Utilizando un método llamado RC4 se genera una cadena de unos y ceros a partir de la cadena de 64 bits.
4. La cadena del RC4 y el texto plano son pasados por un proceso de XOR, dando por resultado el texto cifrado. Vale decir que para recuperar el mensaje en el otro extremo se debe saber el valor de la cadena RC4, que como ya dijimos es el vector de iniciación junto a la clave.
5. Finalmente se envía un paquete que tiene por encabezado lo establecido en la norma 802.11, luego lleva el vector de iniciación, luego el mensaje cifrado y finalmente el valor de la suma de chequeo CRC-32.

El hecho de que se transmita el vector de iniciación explícitamente en el paquete será relevante en una mirada posterior a las vulnerabilidades de WEP.

Operación: Autentificación

En este caso se usa el "four-way challenge-response handshake". Este término hace referencia a un procedimiento en el que el usuario que desea conectarse a la red debe superar un desafía impuesto por el punto de acceso, en el que se transmiten 4 mensajes entre ambos.

1. El primer mensaje corresponde al usuario pidiendo conexión al punto de acceso.
2. El segundo es la respuesta del punto de acceso, en la que se envía un texto generado aleatoriamente por él y que corresponde a un desafío dirigido al solicitante.
3. El solicitante utiliza su clave para responder al desafío del punto de acceso y envía un mensaje cifrado.
4. El punto de acceso finalmente descifra el mensaje y lo compara con el original. Si son iguales el solicitante pasa a ser parte de la red.

Vulnerabilidades

Cifrado

Las vulnerabilidades de WEP son variadas y se combinan de distintas formas permitiendo que la seguridad del punto de acceso sea burlada. La debilidad fundamental viene dada por el aprovechamiento del XOR usado en el cifrado. Esta debilidad se traduce en que capturando dos cifrados C1 y C2 y conociendo alguno de los textos planos P1, se puede obtener el texto plano P2 con una simple operación binaria. El texto de algunos mensajes puede ser predicho debido a que en la red hay muchos paquetes circulando que son redundantes. Además se necesita que los 64 bits (vector y clave) usados para el cifrado sean los mismos.

La forma en que WEP se protege de la forma de ataque mencionada es cambiando constantemente el vector de iniciación. Normalmente la forma en que cambia este vector es simplemente sumándole 1 cada vez que un nuevo paquete es transmitido. En si este no es

un defecto muy grande, sino que el problema está en que luego de 2^24 el vector inevitablemente se va a repetir, dándose la condición que se desea para el ataque.
La forma común en que se consiguen estos textos conocidos es inyectando tráfico al punto de acceso, de manera que éste responda y se pueda conseguir la información necesaria para conseguir la clave y así descifrar los mensajes transmitidos en la red.

Clave de Acceso

La mayor velocidad a la que se trabaja actualmente, permite que la información sea tanta que tlizando técnica probabilisticas se consiga adivinar la clave de la red y poder acceder a la red de manera pirata. Esto se usa frecuentemente en la actualidad para utilizar internet Wi-Fi ajeno.

Autentificación de los Mensajes

Otra debilidad que tiene WEP tiene que ver con que se pueden introducir mensajes con errores basándose en la linealidad de XOR y en conocimientos previos de los mensajes que se transmiten, incluso sin conocer la clave de red.

Contramedidas

Para tratar de hacer más segura una red que usa WEP se pueden tomar algunas medidas por parte de la administración. Una medida es colocar los accesos inalámbricos fuera del firewall institucional de modo que los accesos inalámbricos sean considerados como potencialmente riesgosos. Además se puede utilizar VPN (Virtual Private Network) que permite acceso a la red sólo a los clientes autorizados por el administrador y hace que la información transmitida por el aire posea doble encriptación (encriptación WEP y VPN) lo que hace que sea mucho menos exitoso un ataque pasivo y además impide que se pierda ancho de banda valioso por tener intrusos robando recursos de la red.
Otras medidas saludables tienen que ver con metodología para cambiar con frecuencia de uno o algunos pocos días, de modo que crackear la nueva clave diariamente resulte tedioso y desalentador.

WPA

WPA fue la respuesta que el año 2003 se dio a toda una gama de falencias que tiene WEP. Las virtudes de WPA son las siguientes:

- Compatibilidad con hardware que trabaja con WEP.
- Uso de cambio de claves dinámicas y vector de iniciación más grandes.
- Nuevo y más robusto método de integridad en los mensajes.
- Sistema para evitar ataques de repetición.
- Detección de ataques.

WPA2 es una versión mejorada de WPA pero que no es compatible con las tarjetas de red más antiguas. Se destaca principalmente por el uso de AES (Advanced Encryption System).

Los ataques contra WPA son posibles pero son muchísimo más lentos, mientras que se desconocen ataques fructíferos contra WPA2. Hasta el momento la única opción que queda para intentar acceder a estos sistemas es a través de métodos de "fuerza bruta" que consisten en, a través de un software, ingresar un diccionario completo de posibles keywords esperando acertar a la corecta, pero estos ataques son inútiles cuando la clave establecida es robusta, es decir, cuando el administrador evita usar palabras y contiene tanto números como letras. Además existe una variante en que si se captura el four way handshake de cuando un usuario legítimamente se conecta a la red, el atacante puede intentar un ataque de diccionario offline.

Conclusiones

Dado que las redes inalámbricas son cada vez más abundantes y las familias utilizan sus recursos en ello, es importante que estas puedan preservar su ancho de banda y, al igual que las empresas, poder confiar en que pueden realizar sus operaciones de forma segura. Es por esto que se vuelve necesario que se aprenda a utilizar los recursos que poseen los puntos de acceso inalámbrico de modo de conseguir estos objetivos. Muchos de los productos presentan a los administradores distintas opciones de seguridad como lo son WEP, WPA y WPA2. Como ya hemos visto es necesario abandonar el uso de WEP por ser muy vulnerable y con formas de atacar muy difundidas.

Con este trabajo queda demostrado como en el área de las redes de computadores nunca está dicha la última palabra y siempre se presentan nuevos desafíos y caminos para mejorar.

Fuentes

Trabajo pionero en vulnerabilidades de WEP

www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

Normas de la IEEE

http://www.ieee802.org/11/

Generalidades sobre WEP y WPA

http://en.wikipedia.org/

Tipos de Ataque a WEP

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Sobre VPN

http://www.informit.com/guides/content.aspx?g=security&seqNum=70

Sobre ataques a WPA y WPA2

http://www.wve.org/entries/show/WVE-2006-0041