UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Redes WPA/WPA2

SU VULNERABILIDAD

JAVIER RUZ MALUENDA
BASTIAN RIVEROS VASQUEZ
ANGEL VARAS ESCOBAR

Resumen

A través de las redes con seguridad WPA-WPA2 mediante su descripción y características principales mostraremos que a pesar de que son consideradas de una alta seguridad, que le brindan al usuario un servicio de alta confiabilidad estas pueden ser vulneradas debido a que ha aparecido información concreta y mal intencionada y además las herramientas necesarias con el software correspondiente para las distribuciones de Linux y Windows.

Estos mecanismos usados para vulnerar la seguridad de redes inalámbricas, para los usuarios que logran hacerlo, les demanda una alta cantidad de horas debido al gran número de contraseñas que tienen que ser analizadas por el programa especialista.

Introducción

En este informe queremos introducir a los protocolos de seguridad más seguros al día de hoy ver de forma sencilla como funcionan y experimentar a través de herramientas computacionales su seguridad.

Sabemos que las redes inalámbricas con sistema WEP, son altamente vulnerables y que su uso no está recomendado, ¿pero qué pasa con WPA y el estándar WPA2? Si bien estos protocolos son más recientes, ya están algo viejos, WPA2 es del año 2004. Han pasado varios años donde las vulnerabilidades pueden haber sido explotadas, es por esto que queremos explorar esas áreas ocultas de la informática.

Para el desarrollo de este trabajo utilizamos una distribución libre y herramientas de auditoria wireless. En la parte final dejamos como anexo nombre de herramientas y enlace a unos videos que grabamos durante el proceso.

WPA/WPA2 (WIRELESS PROTECTED ACCESS)

Su nombre proviene del acrónimo WPA, es decir, Wireless Protected Access (acceso inalámbrico protegido) y tiene su origen en los problemas detectados en el anterior sistema de seguridad creado para las redes inalámbricas. La idea era crear un sistema de seguridad que hiciera de puente entre WEP y el 802.11i (WPA2), el cual estaba por llegar.

Para el proceso de autentificación WPA y WPA2 usan una combinación de sistemas abiertos y 802.1x. El funcionamiento es igual al ya comentado en el apartado del 802.1x. Inicialmente el cliente se autentifica con el punto de acceso o AT, el cual le autoriza a enviarle paquetes. Acto seguido WPA realiza la autentificación a nivel de usuario haciendo uso de 801.1x. WPA sirve de interfaz para un servidor de autentificación como RADIUS o LDAP. En caso de que no se disponga de un servidor de autentificación se puede usar el modo con PSK. Una vez se ha verificado la autenticidad del usuario el servidor de autentificación crea una pareja de claves maestras (PMK) que se distribuyen entre el punto de acceso y el cliente y que se utilizarán durante la sesión del usuario. La distribución de las claves se realizará mediante los algoritmos de encriptación correspondientes TKIP o AES con las que se protegerá el tráfico entre el cliente y el punto de acceso.

WPA2 fue lazada en septiembre de 2004 por la Wi-Fi Alliance. WPA2 es la version certificada que cumple completamente el estándar 802.11i ratificado en junio de 2004. Análogamente a WPA presenta dos vertientes: la autentificación y la encriptación de datos. Para el primer elemento utiliza 802.1x / EAP o bien PSK. Para la encriptación se utiliza un algoritmo mejor que el TKIP, concretamente el AES.

En el modo Enterprise el sistema trabaja gestionada mente asignando a cada usuario una única clave de identificación, lo que proporciona un alto nivel de seguridad. Para la autentificación el sistema utiliza el ya comentado 802.1x y para la encriptación un algoritmo de cifrado mejor que el TKIP, el AES. Para el caso de funcionamiento en la versión personal, se utiliza una clave compartida (PSK) que es manualmente introducida por el usuario tanto en el punto de acceso como en las máquinas cliente,

utilizando para la encriptación o bien TKIP o AES. En este sentido las diferencias con WEP se basan en el algoritmo de cifrado de los datos.

Desgraciadamente WPA no está exento de problemas. Uno de los más importantes sigue siendo los DoS o ataques de denegación de servicio. Si alguien envía dos paquetes consecutivos en el mismo intervalo de tiempo usando una clave incorrecta el punto de acceso elimina todas las conexiones de los usuarios durante un minuto. Este mecanismo de defensa utilizado para evitar accesos no autorizados a la red puede ser un grave problema.

¿Que es wps?

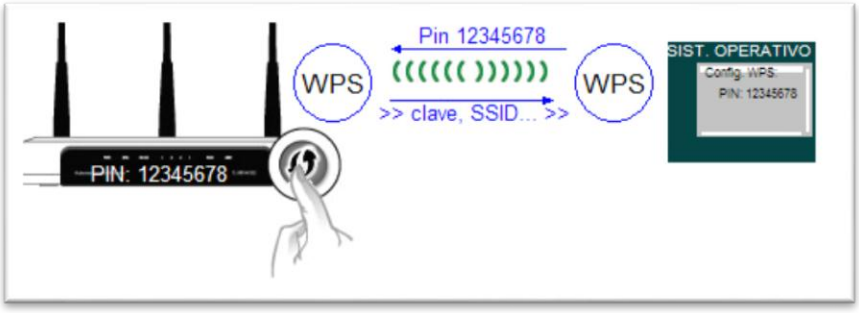
Wifi Protected Setup es un estándar que es promovido por la Wi-Fi Alliance, que permite la creación de redes Wlan seguras. En si WPS no es un sistema de seguridad, sino que un conjunto de mecanismos cuyo objetivo es facilitar la configuración de la red inalámbrica con seguridad WPA2 de usuarios domésticos y pequeñas oficinas. Lo que hace WPS es establecer mecanismos que permiten a diversos dispositivos obtener las credenciales necesarias para poder autenticarse en la red.

La arquitectura de WPS tiene tres elementos cada una con roles diferentes que permiten a este sistema funcionar:

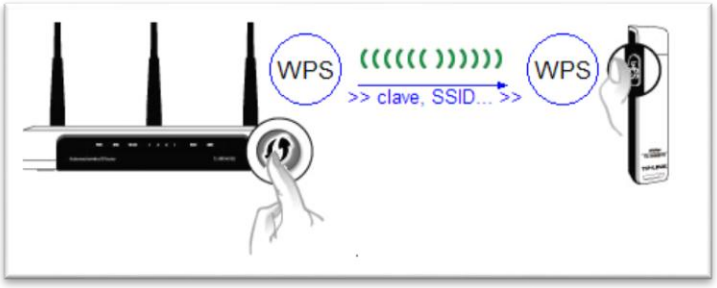
- Registrar: dispositivo que tiene la facultad de generar o quitar credenciales. Puede ser un AP u otra estación.p
- Enrollee: dispositivo que quiere participar de la red WLAN.
- Authenticator: AP que funciona como puente entre Registrar y Enrollee.

Existen diversas formas en que WPS permite la configuración y el intercambio de credenciales:

- PIN(Personal Identification Number): es un numero de 4 u 8 dígitos de longitud. Este debe ser de conocimiento de Registrar así como la contraparte que desea conectarse Enrollee.



- PBC(Push Botton Configuration): la configuración y el intercambio se hace de manera física, a través de un botón en el AP o en cualquier elemento Registrar; durante el lapso en que es presionado el botón, cualquier otro dispositivo próximo puede ganar acceso a la red.



- USB: a través de este método las configuraciones se transmiten de un dispositivo Registrar a uno Enrollee por medio de un dispositivo de almacenamiento.

Ventajas de sistema WPS

- La configuración mediante botín PBC es útil cuando por ejemplo no disponemos de un PC para configurar el punto de acceso, siempre y cuando todos nuestros dispositivos clientes Wi-Fi y el punto de acceso soporten el protocolo WPS.
- Cuando los usuarios no tiene mucha idea de cómo funciona o se configuran los equipos. Con esta funcionalidad y tan solo pulsando el botón WPS en ambos dispositivos, estos quedarían asociados y configurados en apenas un minuto con cifrado incluido.
- No se necesita conocer el nombre de la red ni la contraseña, ya que por defecto esta se genera aleatoriamente al usar el botín WPS por primera vez en caso de que no hubiera una escrita anteriormente.

Vulnerabilidades

La mayor vulnerabilidad de este sistema es que al ser un estándar impulsado por la misma Wi-Fi Alliance, para que un dispositivo tenga la certificación Wi-Fi debe poseer esta característica activada por defecto, por lo que hoy en día son más los dispositivos que presentan esta vulnerabilidad que hasta el día de hoy no tiene solución.

En diciembre de 2011 Stefan Viehböck y Craig Heffnet descubrieron una vulnerabilidad que afectaba a los Dispositivos WPS (en algunos dispositivos QSS), que permite a un atacante recuperar el PIN WPS y con esta recuperar la clave pre compartida WPA o WPA2 en cuestión de horas.

El poder que tiene el PIN WPS es muy grande ya que permite desde acceder a la red, hasta incluso reconfigurarla por completo.

Aprovechándose de las vulnerabilidades ¿Qué es reaver?

Reaver lleva a cabo un ataque de fuerza bruta contra el número pin de la configuración protegida del punto de acceso wifi. Una vez que el pin WPS es encontrado, la WPA PSK puede ser recuperada y alternativamente la configuración inalámbrica del AP puede ser reconfigurada.

Reaver tiene como objectivo la funcionalidad externa de "registrador" requerida por la especificación de configuración inalámbrica protegida. Los puntos de acceso proveerán "registradores" autenticados con su configuración inalámbrica actual (incluyendo la WPA PSK), y también aceptaran una nueva configuración del registro.

Con el fin de autenticarse como "registrador", el "registrador" debe probar su conocimiento del número pin de 8 dígitos del AP. Los "registradores" deberían autenticarse a sí mismos al AP sin importar cuando sin necesidad de la interacción del usuario.

A causa de que el protocolo WPS es conducido sobre EAP, el "registrador" sólo necesita estar asociado con el AP y ningún conocimiento previo del cifrado inalámbrico o de la configuración.

Reaver lleva a cabo un ataque de fuerza bruta contra el AP, probando cada posible combinación para adivinar el número pin de 8 dígitos del AP. Dado que los números pin son enteramente numéricos, hay 10^8 (100.000.000) posibles valores para cualquier número pin. Sin embargo, el último dígito del pin es un valor checksum (de comprobación) que puede ser calculado en base a los 7 dígitos previos, la posibles claves son reducidas a 10^7 (10,000,000) valores posibles.

Las posibles llaves son reducidas incluso más debido al hecho de que el protocolo de autentificación WPS corta el pin por la mitad y valida cada mitad individualmente. Eso significa que hay 10^4 (10.000) posibles valores para la primera mitad del pin y 10^3

(1.000) posibles valores para la segunda mitad del pin, contando el último dígito de comprobación del pin.

Reaver hace fuerza bruta a la primera mitad del pin y luego a la segunda mitad, provocando que todos los posibles valores del número pin del WPS puedan ser puedan ser agotados en 11.000 intentos. La velocidad a la que Reaver puede probar los números pin está totalmente limitada por la velocidad a la que el AP puede procesar peticiones WPS. Algunos APs son suficientemente rápidos para que se pueda probar un pin cada segundo; otros son más lentos y solo permiten un pin cada 10 segundos. Estadísticamente, sólo llevara la mitad del tiempo adivinar el número pin correcto.

Otras debilidades de WPA/WPA2

A pesar de la fortaleza de estos protocolos, aún tienen falencias mínimas en su funcionamiento, con un poco de conocimiento al respecto se puede explotar.

Una de las vulnerabilidades más conocidas es el ataque a la clave PSK, ya que toda la información da la red va en formato texto y se transmite cuando un usuario se autentifica en el conocido 4-handshake. Esta vulnerabilidad se puede explotar con ataques por diccionarios o por fuerza bruta, donde el procedimiento es básicamente el mismo, se va comparando múltiples claves con la suma de chequeo del handshake, una vez que la coincidencia se logra, la red está al descubierto.

El éxito o fracaso de este ataque dependerá ciento por ciento de la fortaleza de la clave y de otras pequeñas opciones de seguridad como el filtrado MAC (aunque no será un reto para un hacker con conocimientos, si lo será para un atacante casual) que pueden hacer una red robusta.

Y definitivamente en cuanto a la fuerza bruta, una clave que combine letras y al menos un número incrementa de manera descomunal las combinaciones a probar lo que hace que demore mucho tiempo, incluirle un carácter especial, hace que sea prácticamente imposible.

Y en cuanto a esta nueva tecnología WPS, si bien es una característica que pretende agilizar y reducir el tiempo de configuración de una red, es una puerta trasera a

posibles ataques, ya que aún no hay solución a la vista lo mejor que puede hacerse es desactivar esta característica, si es que es posible.

Conclusión

La seguridad en las redes inalámbricas es un tema verdaderamente apasionante, en un mundo totalmente globalizado donde desde los pc de escritorio hasta los Smartphone poseen conexiones inalámbricas, fue interesante sumergirse en lo que es la seguridad de una red Wi-Fi, conocer las ventajas de los protocolos de seguridad, sus fortalezas y sus debilidades y lo más importante saber cómo protegerse de ataques, ya sea una gran empresa o no querer que un tercero robe mi internet.

El principio para desarrollar esta investigación fue la práctica, atacar a nuestras mismas redes a fin de ponerlas a prueba, y ponernos a prueba a nosotros mismo a ver si podíamos manejar estas tecnologías, y si, tan solo basta un poco de curiosidad.

La seguridad de las redes es algo que aún queda mucho camino por recorrer, porque en el estado actual no hay seguridad absoluta, cualquier persona con un poco de manejo de distribuciones libres, manejo de sistema, compilar, etc. Puede vulnerar mucho más que una red Wi-Fi con seguridad WEP.

Es sorprendente darse cuenta de que nuevas tecnologías destinadas a hacer más cómoda y rápida la interacción entre máquinas y humanos, puede ser una desventaja a la hora de la seguridad, o bien el ingenio, para ocupar las mismas características del protocolo wpa2 que impiden los ataques, para realizar uno.

Bibliografía

Alliance, W.-F. (26 de 07 de 2012). *wi-fi.org*. Obtenido de http://www.wi-fi.org/media/press-releases/wi-fi-alliance-introduces-next-generation-wi-fi-security

Viehböck, S. (25 de 07 de 2012). *reaver-wps*. Obtenido de http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

Wi-Fi Alliance. (25 de 07 de 2012). *wi-fi.org*. Obtenido de http://www.wi-fi.org/knowledge-center/articles/wi-fi-protected-setup%E2%84%A2

Anexo

Herramientas utilizadas

Ubuntu 12.04	:	http://www.ubuntu.com/
Aircrack-ng	:	http://www.aircrack-ng.org/
John the Ripper	:	http://www.openwall.com/john/
Reaver	:	http://code.google.com/p/reaver-wps/