Protocolos de seguridad en redes inalámbricas

Cristian Mello

Curso de Análisis y desarrollo de sistemas – Instituto Federal Sul Rio Grandense (IFSUL) – Campus Santana do Livramento

mellocristian45@gmail.com

WEP, WPA y WPA2 son los protocolos de seguridad inalámbrica utilizados, podríamos son básicamente algoritmos de seguridad. Dichos protocolos no sólo evitan que se realicen conexiones no deseadas a su red inalámbrica, sino que también cifran sus datos privados enviados a través de la red.

No importa lo protegida y cifrada que se encuentre nuestra red, las redes inalámbricas no cuentan con el mismo nivel de seguridad que las redes cableadas. Para enviar datos de A á B, las redes inalámbricas lo transmiten dentro de su alcance en todas las direcciones a cada dispositivo conectado que esté escuchando; lo que las hace estar más expuestas potencialmente.

WEP (Wired Equivalent Privacy) - Se trata del primer algoritmo de seguridad que se desarrolló, la misma utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso, todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. En la práctica general, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.'

Desventajas**:**

Hay un montón de problemas de seguridad bien conocidos en WEP, que también lo convierten en un protocolo fácil de romper y difícil de configurar.

Poca longitud de contraseñas: Lo primordial y lo más importante para enviar paquetes a internet es una buena contraseña. Lamentablemente para este tipo de protocolos de seguridad solo estaba disponible una contraseña que no podía tener más de 21 caracteres, además de que estos solo podían ser letras y números.

Cifrados fijos: Además de las claves, los cifrados de este tipo de protocolos de seguridad eran fijos, es decir, no tenían un cambio cada determinado tiempo. Esto se volvió algo inseguro para las empresas, ya que después de determinado tiempo se podía adivinar perfectamente y descifrar los procesos.

Facilidad: Lo que era una gran ventaja para los inexpertos, se convierte en una desventaja total, ya que la facilidad de uso y de configuración la vuelve demasiado vulnerable, por lo que no es una gran opción para empresas.

WPA (WiFI Protected Access) - Surgió como elemento de seguridad temporal para mejorar la seguridad del WEP, pero acabó sustituyendo ampliamente a su predecesor.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

Radius: Un radius es un servidor que controla los accesos de los usuarios a una red de datos. El radius verifica el nombre y la contraseña del usuario. Si el acceso se autoriza el Radius asigna una IP privada al dispositivo del usuario.

Desventajas:

No hay dispositivos compatibles: Es común ver que hay algunos productos móviles que todavía no pueden enviar paquetes a ese tipo de redes.

La seguridad WPA renueva contraseñas y cifrados, por lo que es un bunker de seguridad, pero esto provoca que las desconexiones sean bastante frecuentes, sobre todo si utilizas mucho tu red de internet.

WPA2 (Wi-Fi Protected Access versión 2) - La WPA2 surgió para solucionar las vulnerabilidades del WPA. Es un protocolo basado en el estándar de seguridad inalámbrica 802.11i.

WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS. Se trata de un algoritmo de cifrado de con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

Desventajas:

Probablemente la única desventaja de WPA2 es la potencia de procesamiento que necesita para proteger su red. Esto significa que se necesita un hardware más potente para evitar un menor rendimiento de la red.

WPA3 **(Wi-Fi Protected Access versión 3)** – WPA3 llega para reemplazar a WPA2, que ya no se puede considerar absolutamente segura. Las redes WPA3 podrán impedir que los dispositivos que solo soportan WPA2 se conecten, aunque en un principio lo más seguro es que prime el modo transicional, que permite la conexión de dispositivos tanto WPA2 como WPA3.

La primera gran diferencia es el cifrado, que pasa de usar una clave de 128 bits a otra de 192 bits. Cuanto mayor es la clave de cifrado, más difícil es romperlo, pues se requiere de ordenadores más potentes y de mayor tiempo para lograr descifrar los datos a la fuerza.

El protocolo WPA3 implementa características como la de deshabilitar protocolos anteriores, de manera que los dispositivos WPA2 no se podrán conectar a puntos de acceso exclusivos de WPA3 que no tengan habilitado un modo de transición especial. Además, ambos también requieren el PMF, que ayuda a prevenir las escuchas no deseadas.

También está preparado para proteger las conexiones con malas contraseñas. Para ello utiliza un nuevo protocolo de intercambio de claves que ayuda a proteger el ataque de diccionario, que es cuando se intenta averiguar una contraseña probando todas las palabras del diccionario. Los anteriores protocolos WPA eran vulnerables a este ataque, pero no el WPA3.

Otro de los beneficios prometidos por este nuevo protocolo es una mayor protección en el caso de que un atacante pueda averiguar la contraseña. Lo hace mediante un cifrado de datos individualizado que evita que al obtener acceso a tu conexión se pueda desencriptar el tráfico anterior que ha habido, ya que mantendrá cifrado todo el que hayas tenido hasta el momento de la intromisión.

Referencias

https://sistemas.tecnoderecho.com/desventajas-la-wep-la-seguridad-no-se-ha-utilizado/

http://director-it.com/index.php/es/ssoluciones/red-de-datos/240-radius.html

https://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml

https://es.xfinity.com/support/articles/wifi-protected-access

https://www.netspotapp.com/es/wifi-encryption-and-security.html

https://www.antelec.es/protocolos-seguridad-wep-wpa-wpa2/

https://tutorialesenlinea.es/40-protocolos-de-seguridad-en-redes-inalambricas.html

https://luisgyg.com/wpa3-red-inalambrica-segura/