Common Security Protocols for Wireless Networks: AComparative Analysis

Francisco Villanueva Quirós - 2021043887

Redes

Preguntas

1. Comente de acuerdo a la lectura las principales características de WEP, WAP y WAP2

- **WEP**: Primeramente, este protocolo fue desarrollado por Ron RIvest en 1987. Sin embargo, fue implementado en 1997 por la IEEE y fue etiquetado como el protocolo IEEE 802.11. Este se creo para dar cifrado de datos en la red. En la parte de la **autenticación**, este ofrece dos tipos: Open System y Shared Key. En Open system, el red no va a necesitar ningún mecanismo de seguridad para prevenir el acceso no autorizado, en otras palabras cualquiera puede unirse a la red sin restricciones. Shared Key, utilizada una clave de acceso previamente establecida. Esto se hace mediante un texto al dispositivo y si este lo cifra con la clave, se le concede acceso. En la parte del **cifrado (Encryption)**, se utiliza el protocolo RC4 y la ayuda de CRC-32. El protocolo RC4 es utilizado la alcanzar la confidencialidad en los paquetes de datos, mientras el CRC-32 usa para la integridad de los datos. Mediante estos algoritmos de encriptación los datos estan protegidos en la transmisión. **Las claves** en este protocolo, una solo clave es compartida en los dispositivos en al red, lo que se conoce como Root Key. La longitud de esta clave es de 40 bits, aunque existen versiones extendidas con 104 bits y en algunos casos 232 bits. Algunas **fortalezas**, el impacto que tuvo con la seguridad para transmitir datos a través de la red es muy impactante, lo hackers deben hacer un esfuerzo para romper el cifrado mencionado anteriormente. No obstante, existen **debilidades**, en un alto grado de la manipulación de los datos, se puede perder data en WEP y como la llave es común puede ser decodificada fácilmente y capturar la data, la integridad de los datos no esta asegurada. Otra desventaja es el manejo de las claves, no se mantiene una debida tabla de claves, lo que hace que se use una clase por un período extendido. Además, el tamaño de la llave es pequeña lo hace que no haya mucha seguridad en los paquetes. Entre los ataques más conocidos que explotan vulnerabilidades de WEP se encuentra el Chopchop Attack.
- **WAP**: WPA fue introducido en 2003 por la organización WiFi Alliance como una solución para resolver las debilidades de WEP, incorporando una capa de seguridad adicional basada en el protocolo 802.11i. En la parte de la **autenticación**, existen diferentes tipos dependiendo de la version del protocolo. En el WPA Personal, se utiliza el sistema de

claves PSK, mientras que en WPA Enterprise, se hace una autenticación EAP junto a servidores Radius. Los componentes de autenticación en este protocolo son: client, access point (AP) y network access server (NAS). El **cifrado (encryption)**, El algoritmo principal de cifrado en WPA es TKIP, actúa como una mejora sobre RC4. TKIP utiliza el sistema de clave de paquetes a través de un mecanismo de clave dinámica y proporciona más seguridad a la red. Puede integrarse con AES como opción de seguridad adicional, aunque esto no era estándar en la primera versión de WPA. TKIP mejoró la seguridad respecto a WEP. **Las claves**, en WAP son generadas en el servidor de autenticación, estas claves son validadas y certificadas. En el caso de WPA-PSK, se usa una clave de 128 bits que se considera robusta, TKIP permite generar hasta 280 trillones de combinaciones de claves por paquete. Algunas **fortalezas**, WAP incluye mecanismos como el Message Integrity Code (MIC), que detecta errores o manipulaciones en los paquetes de datos. Además, la introducción de un vector de inicialización (IV) nuevo por paquete y el cambio periódico de claves refuerzan la seguridad. No obstante, existen algunas **debilidades**, la implementación de Pairwise Master Key (PMK) es débil ya que hay una laguna en Passfrase Choice en WPAInterface. Además, este protocolo de seguridad está muy expuesto a ataques de fuerza bruta. La colocación de MIC se considera otro problema. Con la combinación de ataque de fuerza de abrasión, MIC se puede utilizar para validar la información del mensaje descifrado. Algunos de los ataques más relevantes contra WPA son el Beck y Tews Attack, que expone debilidades en TKIP para descifrar tráfico ARP y el Ohigashi-Morii Attack.

- **WAP2**: WAP2 fue implementado para 2004 con el estantar de la IEEE 802.11i, como solución a los problemas del protocolo WEP y complementar el protocolo WAP. El WAP2 es considerado el protocolo mas fiable para la seguridad de redes inalámbricas. En la parte de **autenticación**, WPA2 utiliza el mismo mecanismo de autenticación que se un WPA. Los tipos presentes son autenticación de servidor y las llaves pre-compartidas. Pre-Shared Key para redes domésticas o de pequeñas empresas y 802.1X/EAP para entornos empresariales con servidores de autenticación. En el caso de las redes grandes, el proceso de autenticación genera varias claves temporales de 128 bits. El protocolo 802.1x se utiliza para crear los PMK. El **cifrado (encryption)**, WAP2 utiliza Advanced Encryption Standard (AES) para la encriptación y la decodificación. AES se combina con el protocolo CCMP, que protege tanto el contenido como los encabezados de los paquetes, asegurando confidencialidad e integridad. Para la **claves**, se utiliza PTK para generar la claves, permitiendo claves de 128 bit a 256 bits. Solamente entidades autorizadas van a saber cuales son las claves generadas, eso permite seguridad para los paquetes de datos. Las **fortalezas**, una seguridad más robusta gracias a su cifrado fuerte con AES y CCMP. La longitud del vector de inicialización se incrementa a 48 bits, reduciendo el riesgo de colisiones. También permite una transición rápida entre puntos de acceso, gracias al PMK caching y re-autenticación que permiten al usuario moverse sin reingresar credenciales. No obstante, de igual forma hay **debilidades**. Sin embargo, a día de hot no se han descubierto

debilidades significativas, se presentan debilidades menores. Una de ellas es la dependencia de la fuerza de la clave PSK. Debido a que esta es la fortaleza, si esta es débil, el protocolo puede ser vulnerable a ataques de diccionario o fuerza bruta. WPA2 no protege contra ataques de denegación de servicio (DoS), como el RF jamming o la inundación de paquetes, ya que estos ocurren en la capa física.