Universidad Técnica Federico Santa María
Departamento de Electrónica
ELO323 – Redes de Computadores 2
2do Semestre 2017

Proyecto

Ataque a vulnerabilidad WPA2

Juan Pablo Rothkegel Ide 201221075-5
Johannes Rothkegel Sielfeld 201221031-3

22 de diciembre de 2017

Índice

1. Introducción

Como se ha visto muchas veces en este ramo, la seguridad es un tema fundamental al momento de la transferencia de datos. Es un problema no menor especialmente para una institución (como una empresa o una universidad) que sus datos se mantengan seguros durante el camino de un punto a otro fuera o dentro de la empresa.

Para poder garantizar seguridad de las redes tanto cableadas como inalámbricas, existen múltiples protocolos de encriptación, para así poder garantizar autenticación, confidencialidad e integridad de los datos.

El 17 de octubre del presente año, se desabrió una vulnerabilidad en lo que hasta ahora venia siendo el protocolo de seguridad inalámbrica mas sofisticado, Wireless Protected Access II (mas conocido como WPA2), dejando totalmente vulnerables los datos transmitidos por el aire, ya que, ahora estos pueden ser robados y desencriptados por cualquiera que este conectado a la red inalambrica protegida con WPA2.

Por consecuencia de aquello, se considera fundamental hacer una breve introducción a lo que es el protocolo WPA2, mostrar sus vulnerabilidades y como es posible defenderse de ellas.

2. Wireless Protected Access II

2.1. ¿Que es el Wireless Protected Access II?

Wireless Protected Access II o mejor conocido como WPA2 es un protocolo de seguridad comunmente utilizado en redes inalambricas (Wi-Fi), creado para corregir las deficiendias de las versiones anteriores, llegando a reemplazar versiones mas antiguas y menos seguras como WEP (Wired Equivalent Privacy) y funcionar como mejora del protocolo original WPA(Wi-Fi Protected Access).

EL protocolo WPA2 usa el estándar de cifrado avanzado (AES) para el cifrado de sus datos. AES trabaja con la encriptacion por bloques fijos de 128 bits y tamaños de claves de 128, 192 o 256 bits. Gracias a esto el gobierno de los Estados Unidos lo considero lo suficientemente robusto para ser implementado en sistemas de seguridad nacional o ultra secretos.

2.2. 4 Way-Handshake

Este handshake está diseñado para que tanto el AP como el cliente puedan demostrar de manera independiente, que cada uno sabe la PSK/PMK, sin siquiera revelar la clave. En vez de revelar la clave, el AP con el cliente encriptan los mensajes usando PMK, y si la desencriptación es correcta, se prueba que ambos conocen la clave.

La clave PMK está diseñada para durar la sesión completa y debería minimizarse su exposición, por lo que, se necesitan claves derivadas para encriptar el tráfico.

El handshake se usa para establecer una nueva clave derivada llamada "Pairwise Transient Key"(PTK). Esta es generada concatenando los siguientes atributos:

- PMK
- AP nonce
- STA nonce
- Dirección MAC del AP
- Dirección MAC del cliente

Este producto se pasa por una función pseudo aleatoria. El handshake igual produce la GTK (Group Temporal Key), usada para desencriptar tráfico multi- y broadcast.

Como se ve en la figura 1 en el 4 Way Handshake se trabajan 4 mensajes:

- El AP envía un valor nonce al cliente. Con esto el cliente obtiene todo lo necesario para construir PTK.
- El cliente envía su propio valor nonce al AP junto a un MIC (Message Integrity Code).
- El AP construye y envía el GTK junto a un número de secuencia y otro MIC. Este número de secuencia será usado para el próximo frame multicast o broadcast, para que el cliente pueda realizar detección de repetición.

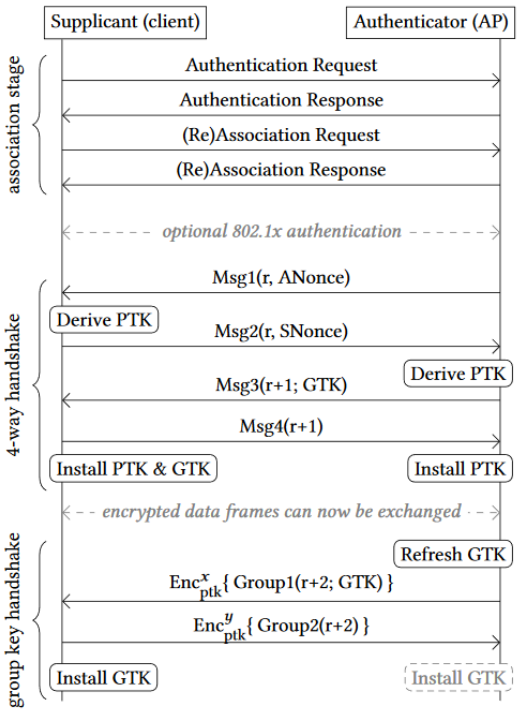

Figura 1: 4 Way Handshake

- El cliente envía confirmación al AP.

La PTK está dividida en 5 claves distintas:

- 16 bytes de clave de confirmación EAPOL (KCK): Usada para computar el MIC en el mensaje de la clave WPA EAPOL.
- 16 bytes clave de encriptación EAPOL (KEK): El AP usa esta llave para encriptar datos adicionales para el cliente.
- 16 bytes de una clave temporal (TK): Usada para encriptar o desencriptar paquetes de datos unicast.
- 8 bytes de clave de autenticación de transmisión MIC: Usado para computar paquete de datos MIC enviados por el AP.
- 8 bytes de clave de autenticación de recepción MIC: Usado para computar paquete de datos MIC enviados por el cliente.

2.3. Vulnerabilidad

Cada vez que el AP no recibe una respuesta apropiada del cliente después de enviar el mensaje 3, este se encarga de reenviarlo. Cada vez que ese mensaje se reenvía se reinician los contadores de paquetes enviados y recibidos. Luego cuando el mensaje 3 llega y se envia el 4 mensaje se instala la clave.

Los atacantes usan este proceso para usar una técnica llamada KRACK (Key Reinstallation Key). Esta técnica consiste en:

- Engañar a la víctima para poder reinstalar una clave que ya está en uso.
- Cuando se reinstala la clave, los parámetros asociados al incremento de número de paquete (nonce) y el número de paquete recibido, son reseteados a su valor inicial.
- La instalación se lleva a cabo después de recibir el 3 mensaje.
- En el caso de que mensajes sean botados o perdidos, el AP retransmitirá el mensaje 3, si es que no recibe una respuesta apropiada. Como resultado el cliente puede recibir el mensaje 3 varias veces.
- Cada vez que recibe el mensaje, reinstalará la clave de encriptación y resetear los controladores.

2.4. Resultados

El resultado de un ataque se puede ver en el siguiente link.
También están disponibles los scripts para probar si un cliente o AP es vulnerable a un posible ataque KRACK.

3. Conclusiones

La seguridad de las redes inalámbricas es un tema muy importante, ya que, por ellas pasan datos sensibles, como claves y usuarios de mails, bancos, empresas, entre otros.

Por consecuencia de esto es fundamental trabajar en un entorno seguro, en el que los datos enviados sean confidenciales , integros y se asegure una autenticación de extremo a extremo entre emisor y receptor.

En este proyecto se mostraron las vulnerabilidades del protocolo WPA2, lo que solía ser el protocolo de seguridad de redes inalámbricas mas robusto hasta el momento.

A partir de esto se llega a la conclusión, de que con el tiempo, hasta los sistemas mas seguros y mejor encriptados pueden ser vulnerados. El problema de man-in-the-middle es un problema que existe en múltiples protocolos y que ha sido muy difícil evitarlo.
Finalmente para evitar las vulnerabilidades de WPA2, las empresas tienen que parchar a los sistemas de seguridad para que esta vulnerabilidad quede obsoleta.

4. Contacto

- Juan Pablo Rothkegel Ide - Juan.rothkegel.12@sansano.usm.cl
- Johannes Rothkegel Sielfeld - Johannes.rothkegel.12@sansano.usm.cl

5. Bibliografía

Referencias

[1] Mathy Vanhoef and Frank Piesens. *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. Mathy Vanhoef, 2017.

[2] Wikipedia: Wi-Fi Protected Access, `https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access`