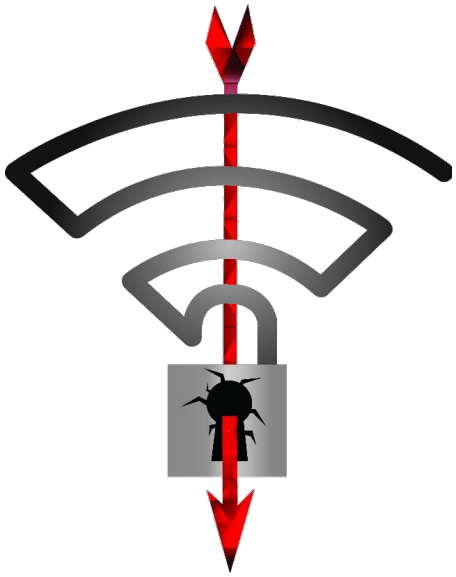
24/08/2018

KRACK:

Ataque de Reinstalación de Llaves en WPA2



Aquiles Viza

Pablo Ulloa

Clemente Jara

Resumen

Un ataque tipo KRACK, acrónimo de Key Reinstallation Attack, utiliza una vulnerabilidad en WPA2, específicamente en el protocolo Four-way handshake. Así, se logra restaurar las llaves de encriptación y tomar una posición denominada “Man In the Middle”, en donde los frames emitidos por un host determinado son captados y descifrados, permitiendo al atacante manipular los datos y eventualmente obtener información privada.

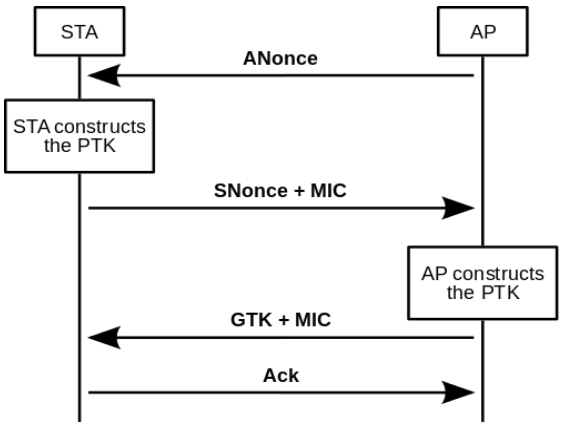
Introducción

La mayoría de nuestros dispositivos hoy en día tienen soporte para, y dependen de, múltiples tipos de conexiones inalámbricas. Estas se clasifican acorde a sus rangos de alcance y frecuencias. Una de las más utilizadas hoy en día son las redes WLAN, comúnmente conocidas como Wi-Fi. Wi-Fi es un término utilizado para referirse a las tecnologías basadas en el protocolo IEEE 802.11. Como esta es una red inalámbrica WLAN no es muy complicado que alguien entre a la red sin autorización y tenga acceso a los paquetes enviados y recibidos por usuarios dentro de la misma red. Es por eso que las redes Wi-Fi han implementado diversos protocolos de seguridad a lo largo de los años. El más usado actualmente el protocolo WPA2. Este fue aprobado el año 2004, y como indica su nombre, fue creado para corregir las deficiencias del protocolo más utilizado previamente, WPA.

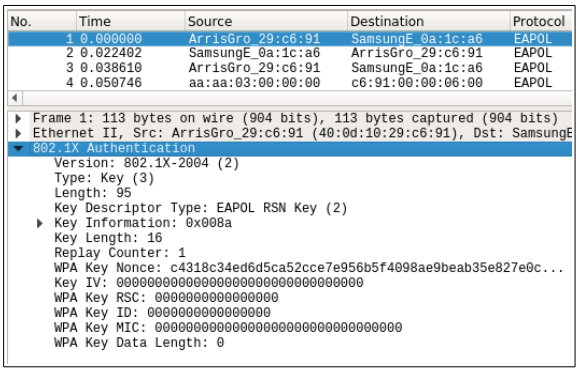
La gran característica de WPA2 sobre WPA es que utiliza el protocolo Four-way handshake, y el protocolo de Group key handshake, junto con un avance en el cifrado llamado AES. Cabe mencionar que el protocolo Four way-handshake es donde radica la vulnerabilidad que el ataque Krack aprovecha, por lo mismo es necesario entender a grandes rasgos cómo funciona este protocolo.

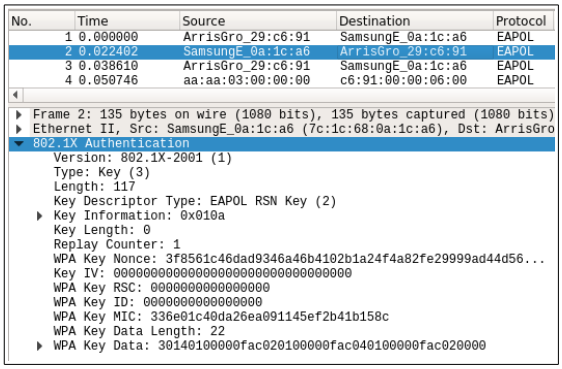
Four-way handshake

Four-Way handshake, como dice su nombre, se basa en una sucesión de 4 datagramas EAPOL que prueban que hay una conexión segura entre un Punto de acceso y un suplicante, alias de un host cliente, y establecen claves de encriptación entre ambos. Antes del comienzo del handshake, el PA y el suplicante poseen ambas direcciones MAC, y una clave común PMK generada a partir de una Master Key, o MK, la cual se obtiene de un proceso anterior de autenticación. Los pasos del Four-way handshake son los siguientes:



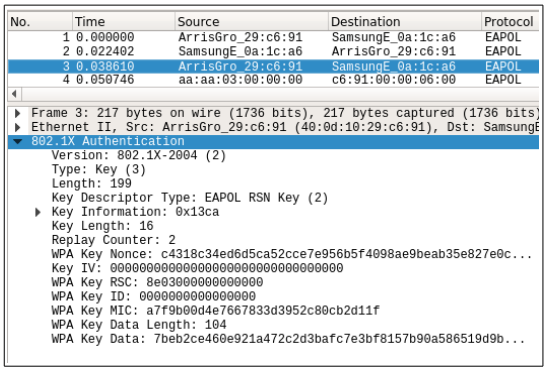
1. El AP genera y envía un nonce (number used once) al suplicante, denominado Anonce.
2. El suplicante genera su propio nonce denominado Snonce. Usando Anonce, Snonce, PMK y ambas direcciones MAC, el suplicante genera la PTK (Pairwise transient key). El Snonce se transmite al AP, junto con un código MIC que le permite verificar la integridad del mensaje luego de que se haya generado la PTK.

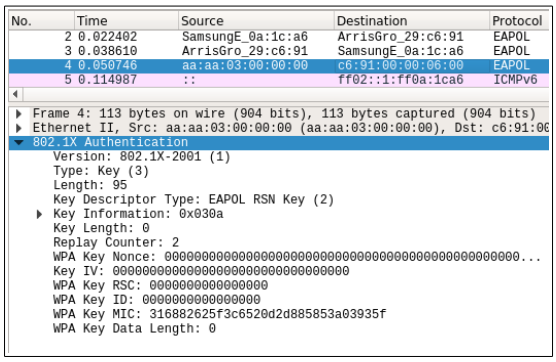




3. El AP ahora posee todo lo necesario para generar la PTK. Luego de verificar la integridad de esta usando el MIC, el AP envía la GTK (group temporal key) con su propio MIC al suplicante. En este paso, el AP todavía no ha instalado la PTK, y el suplicante la instala al recibir este paquete.

4. Luego de verificar la integridad de la GTK, el suplicante la instala junto con la PTK, y envía un paquete ACK al AP, el cual le indica que debe instalar la PTK.





De la manera en la que está planteado, genera un sistema que parece imposible de penetrar, pero en el año 2017, Mathy Vanhoef descubrió que en el tercer y cuarto paso de este protocolo poseen una vulnerabilidad, la cual en pocas palabras consiste en bloquear la llegada del ack, así el AP debe enviar repetidas veces el 3er paso, generando una oportunidad para que un atacante en una posición MITM(Man In The Middle) pueda manipular los paquetes enviados.

Key Reinstallation Attack

Mathy Vanhoef y Frank Piessens, ambos investigadores de posgrado de la universidad KU de Leuven, publicaron en 2017 un paper donde se describe una forma de explotar el protocolo WPA2, que llevaba desde su liberación el 2004 sin vulnerabilidades descubiertas

La vulnerabilidad ocurre en el Handshake, al bloquear el 4° mensaje del Four-way handshake, el AP envía al suplicante el mensaje 3 nuevamente, el cual incluye la orden de instalación de la llave PTK. Para lograr esto, el atacante establece una posición MITM, engañando al suplicante haciéndose pasar por el AP en otro canal wifi. Desde esta posición se interfiere con el 4° mensaje. Esto causa que se reinstale la PTK y se reinicie el nonce y el replay counter lo cual, deja una gran vulnerabilidad en la encriptación de paquetes entre el punto de acceso y el suplicante.

Ahora el atacante es capaz de encontrar un patrón en el contenido de los paquetes, ya que conoce el nonce utilizado para generar el keystream (secuencia pseudo-aleatoria de caracteres usada para encriptar los mensajes). Esto permite que el atacante pueda descifrar parcialmente paquetes, e inyectar contenido malicioso en estos.
Para garantizar la seguridad de una conexión, la instalación de una llave debe ser realizada una sola vez, pero con lo explicado anteriormente,se demuestra que WPA2

no puede garantizar esta necesidad.

Además del protocolo 4-way handshake, existe otro protocolo de handshake llamado “FAST BSS Transition Handshake”, el cual es utilizado con el fin de permitir una conexión continua al tener dispositivos en movimiento, permitiendo que el dispositivo mantenga su estabilidad incluso al cambiar de puntos de acceso dentro de la misma red. Lamentablemente KRACK también afecta a este protocolo, generando consecuencias iguales o peores que en 4-way handshake, principalmente por el hecho que da la posibilidad de retransmitir, desencriptar y crear paquetes de forma inversa.

Además de establecer una conexión segura, WPA2 debe asegurar la encriptación de los datos. Para ello existen los “Protocolos de confidencialidad de datos”, de ellos hay tres que son los más usados:
1.-TKIP(Temporal-key Integrity Protocol): Hoy en día está obsoleto debido a diversas fallas de seguridad.
2.-(AES)-CCMP:Actualmente el protocolo más usado.
3.-GCMP(Galios/Counter Mode Protocol):Protocolo habilitado para WPA2 desde el 2012, veremos a continuación que KRACK afecta de manera grave a este estándar.

WPA2 combina los protocolos de Handshake con uno de estos protocolos de cifrado, de esta manera mantiene la seguridad de los datos a través de la encriptación y comprueba que la conexión entre Host y AP sea segura. Es por ello que KRACK afecta de manera distinta a cada una de estas combinaciones, por ello, para expresar de manera simple y concisa, resumimos los diferentes casos en la siguiente tabla:

- KRACK da la capacidad de retransmitir, desencriptar, o forjar paquetes.
- La tabla expresa las capacidades de cada protocolo con sus diversas formas.
- Ejemplo: AP->Suplicante indica que se pueden retransmitir datos desde AP hacia el suplicante.

Impacto	Retransmitir	Desencriptar(A)	Forjar

4-Way Handshake:			
TKIP	AP -> Suplicante	Suplicante -> AP	Suplicante -> AP(B)
CCMP	AP -> Suplicante	Suplicante -> AP	
GCMP	AP -> Suplicante	Suplicante -> AP	Suplicante -> AP(B)
FT:			
TKIP	Suplicante -> AP	AP -> Suplicante	AP -> Suplicante
CCMP	Suplicante -> AP	AP -> Suplicante	
GCMP	Suplicante -> AP	AP -> Suplicante	AP -> Suplicante(B)

- (A): Permite inyección de datos en paquetes TCP.
- (B): Permite uso de AP para inyectar paquetes a cualquier dispositivo de la red.

A pesar de que los ataques Krack pueden afectar a cualquier dispositivo que no haya sido actualizado contra ellos, particular cuidado debe tomarse para sistemas Linux y Android, ya que estos poseen una vulnerabilidad extra que puede ser explotada en uno de estos ataques. Cuando el mensaje 3 del handshake es recibido por segunda vez en estos sistemas, el nonce se resetea a un dígito conocido de solo ceros. Sabiendo esto, el atacante sabe que el keystream generado por el suplicante será el mismo cada vez que se reinstalan las llaves. Usando algoritmos de fuerza bruta, el atacante puede desencriptar paquetes enviados por el suplicante, y obtener información privilegiada fácilmente.

Conclusión

Los ataques Krack son una vulneración muy reciente al protocolo WPA2, los cuales presentan un gran peligro para la privacidad y seguridad de sus usuarios. Debido a que la vulnerabilidad yace en una capa tan baja de la red, y depende no solo del software del equipo host sino también del software utilizado por el punto de acceso, es difícil

asegurarse de que uno se encuentra seguro al momento de acceder a una red pública. Por esto, tenemos varias recomendaciones para protegernos de un ataque Krack:

- Asegurarse de mantener sistemas operativos actualizados.
- Usar VPN al conectarse a redes desconocidas, así será más difícil rastrear los paquetes que enviamos.
- Revisar si las páginas a las que accedemos poseen HTTPS. De esta manera sabemos que los paquetes que enviamos están cifrados por este protocolo.
- Tener distintas contraseñas para nuestras diferentes cuentas. De esta manera evitamos una total exposición de nuestros datos.
- Evitar ingresar a cuentas de banco o de similar importancia en redes públicas (Ej: café), ya que en estos sectores es más probable que se pueda realizar un KRACK.
- Dentro de lo posible utilizar datos móviles.

Referencias:

- El sitio web creado por Vanhoef y su equipo, contiene su paper titulado “Key Reinstallation Attacks:Forcing Nonce Reuse in WPA2” y una sección de preguntas y respuestas que encontramos muy útil: https://www.krackattacks.com/
- Diagrama de Four-way hanshake obtenido de Wikipedia, creado por un usuario: https://en.wikipedia.org/wiki/File:4-way-handshake.svg
- Infografía de Ataque Krack usada en nuestra presentación fue obtenida de www.cysreport.com Lamentablemente este sitio se ha puesto a la venta y no se puede acceder. La presentación que contiene esta imagen se encuentra en: https://www.slideshare.net/dbakernc/cys-report-krack-attack-threat-briefing
- El canal computerphile tiene un video explicando a grandes rasgos cómo funcionan los ataques Krack, y entran en detalle sobre cómo se utilizan para desencriptar paquetes: https://youtu.be/mYtvjijATa4