INFORME TÉCNICO

aruba
a Hewlett Packard Enterprise company

WPA3 Y ENHANCED OPEN: SEGURIDAD WI-FI DE PRÓXIMA GENERACIÓN

TABLA DE CONTENIDOS

PROBLEMAS DE SEGURIDAD DE WI-FI EN LA ACTUALIDAD

El trabajo sobre los protocolos que se convirtieron en WPA2 comenzó en 2001 por parte del grupo de trabajo IEEE 802.11i. En aquel momento no había "Wi-Fi", y 802.11 no era tan omnipresente como lo es hoy en día. Se trataba en gran medida de una tecnología de primer salto para oficinas, y las interfaces de Wi-Fi adoptaron la forma de tarjetas PCMCIA (es decir, tarjetas para PC) conectadas a computadoras portátiles. Además, los access points (AP) inalámbricos eran dispositivos independientes (todavía no existían las arquitecturas basadas en controladores) que tenían CPU pequeñas y limitadas que no podían realizar operaciones criptográficas complejas.

El estándar IEEE 802.11i fue ratificado finalmente en 2004 con dos modos de funcionamiento definidos: uno que utilizaba una clave precompartida (PSK) para autenticar un simple handshake; y 802.1X/EAP que descargaba el trabajo de autenticación a un servidor de un tercero.

Una vez finalizado el trabajo en IEEE 802.11i, la Wi-Fi Alliance certificó las implementaciones bajo el nombre de WPA2. Si una implementación lograba la certificación WPA2, casi se garantizaba que funcionaría con otros dispositivos con certificación WPA2. El modo PSK en IEEE 802.11i se conoció como WPA2-Personal (o a veces WPA2-PSK), y el modo 802.1X/EAP en IEEE 802.11i se conoció como WPA2-Enterprise.

Eso fue hace más de 15 años (toda una vida en años de Internet) y ahora IEEE 802.11i está empezando a mostrar signos de envejecimiento.

Problemas con el modo PSK

Tan pronto como se lanzó, se reconoció que el modo PSK era susceptible a los ataques. Para reducir al mínimo las operaciones criptográficas del AP, la clave secreta utilizada en el sencillo y ligero handshake de autenticación se basaba directamente en la clave precompartida. Esto abrió el modo a un ataque de diccionario fuera de línea donde un atacante ve el simple handshake ejecutarse en el aire, y luego toma copias de los mensajes de handshake y se desconecta, y prueba cada contraseña imaginable hasta que encuentra una que pueda validar los mensajes de handshake.

Esto no es tan oneroso como podría parecer porque la mayoría de las contraseñas que se usan hoy en día son típicamente una de varias miles, por lo que la cantidad de poder computacional necesaria para descubrir la contraseña estaba fácilmente al alcance de cualquier atacante moderado. Además, dado que se trata de un ataque fuera de línea, el trabajo podría ser transferido a otros. Así que incluso con contraseñas fuertes era solo cuestión de tiempo antes de que el atacante tuviera éxito.

De hecho, eso es exactamente lo que ha sucedido: se han utilizado matrices de FPGA programadas a fin de realizar este ataque específico para pasar por cientos de miles de PSK por segundo, lo que hace que incluso los PSK largos y algo complejos sean vulnerables al ataque.

El problema es que los AP no tenían el poder computacional necesario para implementar un protocolo fuerte y seguro en el momento en que se desarrolló el protocolo, por lo que la responsabilidad de la seguridad recaía en los usuarios. Para que el modo PSK de 802.11i se utilizara de forma segura, era necesario utilizar PSK largos, complejos y de caso mixto con números, letras y caracteres especiales. Pero cuanto más complejo es el PSK, más difícil es administrarlo y menor es la probabilidad de que se haya introducido correctamente.

El elemento humano en la administración de PSK pone un límite superior efectivo a la complejidad que es posible en una red administrada por PSK de 802.11i. Por lo tanto, es un límite superior en la seguridad que tendrá la red, lo que afectará a todos los usuarios y dispositivos.

Problemas con 802.1X/EAP

Para evitar que los AP tengan que hacer demasiado trabajo y aún permitan que se logre una autenticación criptográfica fuerte con IEEE 802.11i, se definió el modo de operación 802.1X/EAP. En general, utiliza un servidor independiente, separado del cliente y del AP, que tiene un lenguaje EAP (Protocolo de autenticación extensible) y se autentica a sí mismo ante el cliente, y opcionalmente autentica al cliente. Una vez que el intercambio de autenticación de EAP negocia un secreto compartido llamado Clave principal por pares (PMK), la clave se envía desde el servidor de EAP al AP que realiza el handshake ligero de autenticación.

El primer método de EAP, LEAP, lamentablemente era inseguro y se determinó de inmediato que el protocolo de Seguridad de la capa de transporte (TLS) debería ser aprovechado en el EAP para facilitar una conexión más segura. Esto dio como resultado PEAPv0, PEAPv1 y TTLS, de los cuales todos los protocolos utilizan TLS para realizar la autenticación y el establecimiento de claves.

La autenticación es un proceso de dos pasos con estos métodos de EAP en el que el servidor se autentica ante el cliente utilizando TLS y, a continuación, a través del túnel TLS seguro, el cliente se autentica ante el servidor, por lo general, mediante un nombre de usuario y una contraseña.

La configuración de 802.1X/EAP es difícil y supone un conocimiento especial que el usuario medio de Wi-Fi no tiene. Por ejemplo, generalmente no pueden definir un "método de EAP interno" o una "identidad anónima", y mucho menos saber cuál debe ser el valor en esos campos. Por lo tanto, las implementaciones de 802.1X/EAP solo se realizan cuando un departamento de TI cualificado es capaz de aprovisionar a todos y cada uno de los clientes antes de conectarse a la red.

El gran problema con 802.1X/EAP se debe a sus numerosas opciones. Es posible conectarse con una configuración que parezca superficialmente segura —con hash de SHA256 o cifrada con AES y claves de 128 bits— pero en realidad termina siendo mucho menos segura debido a otros parámetros fuera del control del usuario final. Es posible negociar AES-CCM-128 en la asociación, pero se termina con un intercambio de claves que da como resultado una clave con aproximadamente 60 a 80 bits de seguridad.

Por ejemplo, la negociación de cualquiera de los siguientes conjuntos de cifrado de TLS dentro de EAP terminará produciendo una clave simétrica que no es adecuada para ningún cifrado no obsoleto en 802.11:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_DH_DSS_WITH_AES_256_CBC_SHA

Esto se debe al hecho de que SHA o MD5 es la función hash utilizada, o RC4 es el cifrado que se está utilizando. Además, el uso de un conjunto de cifrado TLS que realiza un intercambio de claves RSA con un certificado que tiene una clave RSA de 1024 bits dará como resultado una clave simétrica que no es adecuada para ningún cifrado no obsoleto en 802.11. El problema es que el cliente no tiene control programático sobre qué conjuntos de cifrado de TLS se negocian dentro de EAP.

Este problema se ve exacerbado por la necesidad de sentido común de garantizar que no haya problemas de conectividad debido a la negociación de conjuntos de cifrado incompatibles, al negociar hasta el denominador más común, que, como es lógico, no es el más seguro.

Problemas que abordan casos de uso populares

Como se mencionó anteriormente, IEEE 802.11i fue concebido antes de que el Wi-Fi se extendiera. Los cafés, hoteles y restaurantes no ofrecían Wi-Fi y si alguien se anticipaba a las implementaciones que vemos hoy en día, no participaba del desarrollo de IEEE 802.11i.

Cuando el Wi-Fi empezó a despegar, la tecnología de radio integrada sustituyó a los adaptadores PCMCIA en las computadoras portátiles. Poco después, se hizo necesario integrar radios Wi-Fi en todos los dispositivos móviles. La gente lo esperaba dondequiera que fuera y su presencia o ausencia influía en su decisión de entrar a un establecimiento o salir de él. Con el fin de atraer y retener clientes, los propietarios instalaban un AP y ofrecían un servicio gratuito de Internet en sus locales.

Pero estas personas no estaban en el negocio de proveer servicios de Internet. Estaban vendiendo café, bollos, cerveza o un filete grande y jugoso. No sabían mucho sobre seguridad de Wi-Fi y, francamente, no querían saberlo. Todo lo que sabían era que no iban a comprar, configurar y mantener un servidor de EAP y pedir a sus usuarios que intentaran configurar 802.1X/EAP.

La única otra opción era el modo PSK. Intentar proporcionar a cada cliente un PSK único no era posible, por lo que el PSK debía compartirse entre todos los usuarios. Para facilitar el acceso a Internet y liberar al personal para que se ocupara del negocio en cuestión y no realizara tareas de TI, el PSK se hizo público. De hecho, la práctica popular de hoy en día es escribir el PSK en un pizarrón o menú para que todos lo vean: era la única opción disponible para satisfacer este caso de uso.

Lamentablemente, esta práctica es completamente insegura. Dado que el PSK está escrito en el pizarrón, un atacante no necesita realizar un ataque de diccionario. El PSK es conocido y puede capturar con facilidad el simple y ligero handshake que el cliente y el AP deben realizar. El PSK se utiliza para determinar las claves de cifrado que usan el cliente y el AP.

Cada marco se puede descifrar, modificar, repetir, y los marcos pueden falsificarse. Además, como el atacante conoce el PSK, es trivial crear un AP malicioso que atraiga a los clientes y sea capaz de interceptar todo el tráfico enviado desde y hacia un cliente. Los PSK compartidos y públicos ofrecen la misma seguridad que una red abierta.

Otro modelo de implementación popular que no recibió servicio por parte de los dos modos de WPA2 es el de un portal cautivo. Esto es para implementaciones en las que más que un enfoque de Proveedor de servicios de internet (ISP) se usa comúnmente. Los clientes se conectan al AP y luego los redirigen a un servidor que puede pedir que se acepten los términos y condiciones, requerir que el usuario vea un video o usar una tarjeta de crédito para obtener acceso a Internet. Una vez que el usuario haya cumplido con el flujo de trabajo del servidor de portal cautivo, el tráfico ya no se redirigirá y el usuario tendrá acceso a Internet.

Dado que estas implementaciones de portal cautivo utilizan un servidor de un tercero para gestionar la validación del usuario, y esta validación no requiere ningún aprovisionamiento previo de dispositivos de los clientes, la interacción entre el cliente y el AP se realiza de forma clara. El cliente hace asociación y autenticación de 802.11 "abierta", y los marcos enviados entre un cliente y un AP no son seguros.

La desventaja es que el portal cautivo normalmente realiza un intercambio criptográfico con el cliente antes de darle acceso a Internet, pero todo el estado criptográfico se descarta cuando el cliente termina la validación del portal cautivo. Cualquiera que se encuentre cerca del cliente y del AP también puede falsificar un marco de desautenticación, expulsar al usuario de la red y asumir la dirección MAC del cliente para robar el acceso a Internet.

Claramente, los anteriores son casos de uso que tienen un sistema deficiente por parte de WPA2.

WPA3 AL RESCATE

Cada uno de los problemas descritos anteriormente se descubrió a lo largo de los años y se hizo un esfuerzo para diseñar un protocolo adecuado que ayudara a abordar cada problema. Al final, se definió una familia de protocolos adecuados que se convirtieron en un nuevo programa de certificación de la Wi-Fi Alliance. Es decir, WPA3.

Abordaje del problema del PSK

La Ley de Moore establece que la cantidad de transistores en un circuito integrado se duplicará cada dos años. Esto ha llevado a algunos a inferir que o bien el tamaño de un transistor disminuye a la mitad o bien la potencia computacional se duplica. El efecto de la Ley de Moore sobre los AP significa que la potencia computacional de un AP utilizada para realizar importantes operaciones criptográficas se duplica cada dos años. Esto, junto con una criptografía de curva elíptica más eficiente, significa que los protocolos que realizan una autenticación criptográfica fuerte y los protocolos de intercambio de claves se pueden ejecutar en el AP. Finalmente, llegó el momento de abordar el problema del PSK.

El protocolo de Autenticación simultánea de iguales (SAE) se añadió a finales de la década de 2000 al estándar IEEE 802.11s (Red en malla). El IEEE 802.11s fue certificado en 2012. SAE es una instanciación del intercambio de claves dragonfly que realiza un intercambio de claves autenticadas por contraseña mediante el uso de una prueba de conocimiento cero: cada lado prueba que conoce la contraseña sin exponer la contraseña o cualquier dato derivado de ella.

Al utilizar una prueba de conocimiento cero, un atacante ya no es capaz de presenciar un solo intercambio y de desconectarse para descifrar el PSK. La única forma en que un atacante puede saber si una estimación de la contraseña es correcta o no es participar activamente en SAE —una estimación por ataque activo. Con SAE, todas esas matrices de FPGA y esas tablas rainbow dedicadas a descifrar contraseñas carecen de valor.

La implicación de una prueba de conocimiento cero significa que SAE puede utilizarse con contraseñas que tradicionalmente se han denominado débiles. WPA2-PSK es un protocolo débil y lo compensa al poner la carga de la seguridad en el único lugar al que no debería pertenecer: los usuarios. Se exigía que las contraseñas fueran de dos dígitos de longitud, en mayúsculas y minúsculas, incluyendo números y caracteres especiales, etc.

Esto creó una situación en la que la contraseña era difícil de recordar y al querer introducirla correctamente se podían cometer errores. Por supuesto, esto dio como resultado que las contraseñas se escribieran en algún lugar, lo que derrotó por completo su propósito. Con SAE, el único requisito para las contraseñas es que sean difíciles de adivinar, por ejemplo, elegir un número entre 1 y 10 000 000. Si esta contraseña se usara con WPA2-PSK, se necesitarían unos segundos de un diccionario fuera de línea para determinar la contraseña. Pero si se utiliza la misma contraseña con SAE, se necesitarían aproximadamente 5 000 000 de ataques activos antes de que la probabilidad se convirtiera en 0,5. Los ataques activos son fáciles de detectar y mitigar.

Consistencia de 802.1X

WPA3 introduce una nueva opción de configuración para 802.1X/EAP llamada CNSA (Algoritmos de seguridad nacional comercial). CNSA fue definido por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) para proteger los datos secretos y de máximo resguardo en las redes gubernamentales y militares. Debido al hecho de que CNSA ofrece una seguridad consistente sin la posibilidad de errores de configuración, está siendo adoptado por empresas que tienen fuertes requisitos de seguridad, como las instituciones financieras.

CNSA establece un conjunto de algoritmos criptográficos que proporcionan aproximadamente el mismo nivel de protección: SHA384 para el hash, la curva elíptica p384 del NIST para el establecimiento de claves y firmas digitales, y AES-GCM-256 para el cifrado y autenticación de datos. Con CNSA, el método de EAP debe ser EAP-TLS y el conjunto de cifrado de TLS negociado debe utilizar exclusivamente algoritmos criptográficos del conjunto CNSA.

Esto significa que la implementación de CNSA asegura que no se produzcan errores de configuración en 802.1X/EAP. No es posible combinar y conciliar algoritmos de forma insegura y no hay posibilidades de incompatibilidad o de reducción de cifrado, lo que simplifica enormemente la implementación de la red.

Enhanced Open: Protección de redes abiertas

Los cafés y otros lugares públicos quieren una forma sencilla de proporcionar a los clientes una apariencia de seguridad. Las redes abiertas presentan problemas bien conocidos, por lo que no tuvieron más remedio que utilizar WPA2-PSK con un PSK compartido y público. Ahora hay una nueva solución que proporciona más seguridad que un PSK compartido y público: Wi-Fi CERTIFIED Enhanced Open™ con cifrado inalámbrico oportunista (OWE).

OWE es una alternativa a las redes abiertas. Tiene el mismo flujo de trabajo y las mismas necesidades de los usuarios. Básicamente, haga clic en la red disponible y conéctese. Para el usuario, una red de OWE se parece a una red abierta (sin símbolo de candado), pero la ventaja es que está cifrada. OWE realiza un Diffie-Hellman no autenticado cuando el cliente se asocia al AP. El resultado de ese intercambio es una clave conocida solo por dos entidades en todo el mundo: el cliente y el AP. Esta clave se puede utilizar para derivar claves a fin de cifrar todo el tráfico de datos y de administración enviado y recibido por el cliente y el AP.

Aunque un Diffie-Hellman no autenticado es técnicamente inseguro, en realidad, proporciona un mayor nivel de seguridad que un PSK compartido y público con WPA2-PSK —básicamente el enfoque de "contraseña en el pizarrón" para el acceso a la red. Debido a que el PSK es público, todo el mundo al alcance de la mano del AP puede averiguarlo, y debido a que es compartido, todo el mundo utiliza el mismo PSK.

Las implicaciones son que cualquier usuario puede hacerse pasar por el AP (el cliente no puede autenticar el AP) y el AP no tiene idea de quién se está conectando (el AP no puede autenticar al cliente); básicamente el modo PSK compartido y público no está autenticado, como en OWE. Pero con OWE, el intercambio Diffie-Hellman dará una clave verdaderamente única y por pares para el cliente y el AP, lo que significa que nadie más puede escuchar la conexión. No es posible que un atacante descifre, falsifique, modifique o reproduzca cualquier marco enviado entre el cliente y el AP.

Con un PSK compartido y público, un atacante conoce el PSK (¡todo el mundo lo conoce!) y, por lo tanto, puede determinar las claves de cifrado usadas por el cliente y el AP simplemente mediante la observación pasiva del handshake de 4 vías. OWE proporciona un nivel de seguridad superior al que WPA2 puede ofrecer a las implementaciones en lugares públicos.

Para implementaciones de portales cautivos, OWE ofrece seguridad donde antes no existía. En estos entornos, el cliente y el AP realizan un intercambio de OWE antes de que el portal cautivo entre en funcionamiento. Todos los marcos, incluyendo los que estén siendo redirigidos al portal cautivo, estarán protegidos por las claves únicas y de pares derivadas del intercambio de OWE. El portal cautivo puede hacer su negocio de autorización, al obligar al usuario a hacer clic en los términos y condiciones, hacer que el usuario vea un video u obtener información de la tarjeta de crédito para el acceso a Internet, con la tranquilidad de saber que el aire está cifrado.

Una vez que el portal cautivo autorizó al cliente, el AP puede permitir el tráfico del cliente en Internet y retener las claves establecidas por OWE en el momento de la asociación. El portal cautivo ha autorizado a un usuario identificado por una dirección MAC y las claves OWE establecidas son identificadas por la misma dirección MAC. Dado que OWE incluye protección de marcos de administración, no es posible que un atacante falsifique marcos de desautenticación para expulsar a un usuario válido de la red y robar su dirección MAC.

RESUMEN

WPA3 y Enhanced Open representan una evolución largamente esperada para la seguridad de Wi-Fi. Internet y su uso han cambiado considerablemente desde que se lanzó WPA2, y los problemas y cuestiones asociados con él han pasado a primer plano. WPA3 aborda las deficiencias de WPA2 y también los casos de uso que la WPA2 no pudo resolver.

Una parte importante de WPA3 es que la seguridad aumenta mientras que la complejidad no. Por lo general, el aumento de la seguridad va acompañado de un aumento de la complejidad, lo que dificulta la obtención e implementación de la seguridad. La ventaja de usar WPA3 es que no hay cambios en los flujos de trabajo ni en el uso, no hay nuevos pasos que seguir ni advertencias que recordar. OWE se parece a las redes abiertas a las que todos estamos acostumbrados: haga clic y conéctese. Además, WPA3-SAE se parece a WPA2-PSK, donde se introduce una contraseña y uno se conecta. Por último, CNSA elimina la posibilidad de que se produzcan errores de configuración y deja solo el flujo de trabajo de 802.1X/EAP.

REFERENCIAS

- Harkins, D. y W. Kumari, "Cifrado inalámbrico oportunista", RFC 8110, marzo de 2017
- IEEE 802.11-2016, https://standards.ieee.org/standard/802_11-2016.html, diciembre de 2016
- Harkins, D., “El intercambio de claves dragonfly”, RFC 7664, noviembre de 2015
- Agencia de Seguridad Nacional de los Estados Unidos, “Criptografía del conjunto B de NSA”, enero de 2009
- Wi-Fi Alliance, “Especificación técnica del protocolo de aprovisionamiento de dispositivo” v0.2.8, diciembre de 2017
- Harkins, D. “El intercambio de claves públicas”, draft-harkins-pkex-05, enero de 2018
- Stejano, F, y A. Ross, “El patito resucitado”, Lecture Notes in Computer Science, vol. 1796. Springer, Berlín, Heidelberg, 1999
- IEEE 802.11ai-2016, “Enmienda 1: Configuración inicial rápida del enlace”, 2016

aruba
a Hewlett Packard Enterprise company

© Copyright 2018 Hewlett Packard Enterprise Development LP. La información aquí contenida está sujeta a cambios sin previo aviso. Las únicas garantías para los productos y servicios de Hewlett Packard Enterprise se establecen en las declaraciones de garantía expresas que acompañan a estos productos y servicios. Nada de lo aquí expuesto debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se hace responsable de los errores técnicos o editoriales o de las omisiones aquí contenidas.

WP_WPA3EnhancedOpen_110118 a00059003enw