VÍDEO intypedia012es

LECCIÓN 12: SEGURIDAD EN REDES WI-FI

AUTOR: Raúl Siles

Fundador y Analista de Seguridad de Taddong

ALICIA

Hola, bienvenidos a intypedia. Hoy vamos a hablar del apasionante mundo de la seguridad de las redes inalámbricas o redes Wi-Fi. ¡Acompáñanos!

ESCENA 1. INTRODUCCIÓN A LA SEGURIDAD DE LAS REDES WI-FI

ALICIA

Bernardo, estoy muy interesada en profundizar en la seguridad de las redes inalámbricas, o por simplificar, redes Wi-Fi, basadas en las tecnologías 802.11, ya que son utilizadas por millones de personas en todo el mundo a diario dada la facilidad de conexión, flexibilidad y movilidad que ofrecen. He oído que las redes inalámbricas que usamos para conectarnos, por ejemplo, a la red de casa, de nuestra empresa o a Internet desde nuestros ordenadores portátiles o dispositivos móviles, como el teléfono o tableta, son inseguras. ¿Es eso cierto?

BERNARDO

La principal diferencia entre las redes inalámbricas y las redes cableadas, como Ethernet, está en el acceso físico a la red. En las redes cableadas tradicionales, para disponer de acceso a la red o a las comunicaciones que viajan por ella, es necesario conectarse a la misma a través de una toma de red o punto de conexión físico. Sin embargo, las redes Wi-Fi envían sus datos a través de señales de radiofrecuencia que viajan por el aire, como la TV o la radio, por lo que es más sencillo para cualquiera poder tener acceso a estas comunicaciones. Podríamos considerar

que una red Wi-Fi sería equivalente a tirar un cable de red por la ventana o la puerta del edificio hacia la calle, abriendo la posibilidad de que cualquiera que pase por allí pueda conectarse.

ALICIA

Pero entonces… sólo podría conectarse sin autorización alguien que esté cerca de la red Wi-Fi. Creo recordar que la distancia máxima de conexión habitual a redes Wi-Fi es de unos 100 metros, ¿no?

BERNARDO

Pese a que los estándares y especificaciones Wi-Fi normalmente referencian distancias teóricas de unos 100 metros, la distancia real que puede alcanzar la señal de las tecnologías inalámbricas depende del equipamiento empleado por la red y por el atacante. Influyen muchos factores en esa distancia, como la existencia de obstáculos, la densidad de los mismos, la potencia de transmisión, la sensibilidad de recepción y la utilización de antenas de alta ganancia.

Numerosos proyectos y demostraciones han logrado conexiones de cientos de metros empleando equipamiento estándar, por lo que se puede asumir que en un entorno real el atacante de una red Wi-Fi puede estar situado a cientos de metros, incluso varios kilómetros, de la red.

ALICIA

¡Y yo que pensaba que sólo me podían atacar mis vecinos! Entonces, si alguien decide acceder a mi red Wi-Fi de casa, a la de la cafetería a la que me conecto habitualmente, o a la de la empresa en la que trabajo, ¿qué tipo de ataques puede realizar?

BERNARDO

Los ataques sobre redes Wi-Fi son muy numerosos, pero podríamos clasificarlos en cuatro categorías generales.

Los ataques de negación de servicio (DoS, Denial of Service) son los más difícilmente evitables por cómo funcionan las tecnologías inalámbricas, ya que alguien puede generar suficiente "ruido" en la frecuencia empleada por la red Wi-Fi y hacer imposible ningún tipo de comunicación inalámbrica, afectando a la disponibilidad de la red. Este ataque es especialmente relevante en entornos críticos, como redes Wi-Fi de monitorización en hospitales o infraestructuras críticas.

Por otro lado, es trivial para un atacante interceptar las comunicaciones de la red Wi-Fi que viajan por el aire, y tener así acceso a los datos intercambiados si estos no están cifrados. Este ataque es indetectable y afecta a la confidencialidad de las comunicaciones.

Los dos últimos tipos de ataque son la inyección de tráfico y el acceso a la red. Un atacante sin acceso a la red podría inyectar tráfico y modificar su comportamiento, pero también podría

establecer una conexión no autorizada con la red Wi-Fi y disponer de acceso completo a la misma, afectando en ambos casos a la integridad de las comunicaciones.

ALICIA

¡Qué interesante! ¿Qué se puede hacer para proteger una red Wi-Fi de todos esos ataques?

BERNARDO

Alicia, antes de profundizar en los mecanismos de protección disponibles, es importante reseñar que es necesario proteger tanto las redes Wi-Fi, puntos de acceso y controladores, como los clientes que se conectan a esas redes Wi-Fi, como ordenadores de escritorio y portátiles, teléfonos móviles o smartphones, tabletas, y cualquier otro dispositivo móvil.

ESCENA 2. SEGURIDAD DE LAS REDES WI-FI

ALICIA

Bernardo me han quedado claros los diferentes tipos de ataque que existen sobre las redes Wi-Fi. Sin embargo, a la hora de configurar una red Wi-Fi adecuadamente he visto que hay muchas tecnologías y opciones diferentes, como WEP, WPA y WPA2, 802.1x, etc. No tengo claro cuál es la más segura…

BERNARDO

A la hora de configurar una red Wi-Fi hay dos elementos de seguridad a tener en cuenta, el cifrado de las comunicaciones y la autentificación o control de acceso a la red. Por un lado, para evitar que nadie pueda capturar las comunicaciones y acceder a su contenido, es necesario cifrarlas. Las tecnologías que mencionas permiten cifrar las comunicaciones, pero algunas son inseguras. Por otro lado, para evitar que alguien pueda acceder a la red de forma no autorizada, es necesario disponer de mecanismos de autentificación robustos que permitan identificar quién puede conectarse a la red.

ALICIA

El problema es que cuando compras un punto de acceso Wi-Fi está configurado por defecto como abierto, es decir, sin ningún tipo de cifrado ni de autentificación, por lo que es necesario configurarlo de forma segura. ¿Qué opción es la más recomendada?

BERNARDO

Efectivamente, es muy habitual que los puntos de acceso Wi-Fi estén configurados por defecto como abiertos, pudiendo cualquiera capturar el tráfico de la red o conectarse a la misma. También es habitual recibir el punto de acceso o router Wi-Fi del proveedor de servicios de Internet configurado con WEP (Wired Equivalent Privacy), un mecanismo de cifrado antiguo e inseguro, aunque requiera utilizar una contraseña. La utilización de la contraseña crea una falsa

sensación de seguridad. Pese a que WEP emplea el algoritmo de cifrado RC4, al igual que otros protocolos en los que confiamos en la actualidad, como HTTPS, se empleó de forma incorrecta e insegura en su diseño, siendo posible actualmente para un atacante obtener la contraseña WEP de una red Wi-Fi en menos de un minuto.

Las redes Wi-Fi personales deberían ser configuradas con WPA2 (Wireless Protected Access 2), en su variante Personal o PSK (Pre-Shared Key), una opción segura si se emplean contraseñas suficientemente largas (más de 20 caracteres) y difícilmente adivinables, que deben configurarse tanto en los clientes como en la red Wi-Fi. WPA2 ofrece mecanismos de cifrado y de autentificación.

ALICIA

Sí, pero a la hora de seleccionar WPA2 Personal, creo recordar que aparecen dos opciones: TKIP (Temporal Key Integrity Protocol) y AES (Advanced Encryption Standard). ¿Cuál es la más segura?

BERNARDO

La opción recomendada es AES, al estar basada en el conjunto de algoritmos criptográficos de referencia en la actualidad. TKIP es una evolución de los mecanismos de cifrado de WEP, también basada en RC4 pero con mejoras, que se diseñó para ser utilizada con WPA y los dispositivos Wi-Fi que ya soportaban WEP hace años. WPA es más inseguro que WPA2 y es una alternativa que se diseñó para ser usada sólo temporalmente.

ALICIA

¡Está muy claro, WPA2, AES y una contraseña robusta! En el caso de empresas y otras organizaciones, ¿qué opción es la más recomendada para configurar su red Wi-Fi de forma segura, también WPA2 Personal?

BERNARDO

También podrían usar WPA2 Personal, pero es más recomendable que las redes Wi-Fi corporativas sean configuradas con WPA2, en su variante corporativa o Enterprise, ya que es una opción aún más segura al emplear un servidor RADIUS (Remote Authentication Dial In User Service) para generar y distribuir contraseñas aleatorias y robustas, junto a los protocolos 802.1X y EAP (Extensible Authentication Protocol) para la autentificación. Existen múltiples tipos de protocolos EAP, cada uno utiliza diferentes credenciales, como usuario y contraseña, certificados digitales, tarjetas inteligentes (smartcards), etc., por lo que debe realizarse un estudio detallado de la infraestructura Wi-Fi para elegir el protocolo EAP más adecuado. Los mecanismos de cifrado son similares tanto en WPA2 Personal como en Enterprise.

Adicionalmente, es recomendable que las empresas dispongan de un sistema de detección de intrusos inalámbrico (WIDS, Wireless Intrusion Detection System) para saber qué está ocurriendo en su red Wi-Fi y poder reaccionar ante posibles ataques.

ALICIA

Por último, existen numerosas opciones adicionales de seguridad disponibles en los puntos de acceso Wi-Fi, como reducir la intensidad y alcance de la señal, el filtrado por dirección MAC o la ocultación del nombre de la red Wi-Fi en las tramas de anuncio (o beacon). ¿Merece la pena configurarlas también?

BERNARDO

Todos los mecanismos de seguridad adicionales que mencionas permiten incrementar ligeramente la seguridad de la red Wi-Fi; sin embargo, presentan debilidades y no evitarán que un atacante con los conocimientos necesarios pueda evitarlos. En algunos casos, además, su implantación es compleja, como por ejemplo la gestión de la dirección MAC de todos los clientes Wi-Fi de una empresa que dispone de miles de dispositivos cliente. En otros, su utilización puede ser incluso reducir el nivel de seguridad del entorno Wi-Fi, como la ocultación del nombre de la red Wi-Fi, al tener implicaciones en los clientes.

ALICIA

La verdad es que no es tan complicado una vez te lo explican.

ESCENA 3. SEGURIDAD DE LOS CLIENTES WI-FI

ALICIA

Bernardo, has comentado que hay que tener en cuenta también la seguridad de los clientes Wi-Fi. ¿Quieres decir que alguien podría atacar mis dispositivos móviles, con capacidades Wi-Fi, cuando estoy por ahí dando un paseo?

BERNARDO

¡Efectivamente! Dado que las redes Wi-Fi pueden ser configuradas en la actualidad de forma mucho más segura que en el pasado, los atacantes han centrado sus actividades también en los clientes Wi-Fi, el eslabón más débil de la cadena. Sólo por el hecho de tener un interfaz Wi-Fi activo en un dispositivo móvil alguien podría comunicarse con él y atacarlo.

El objetivo de un ataque cuando ni siquiera el dispositivo está conectado en una red Wi-Fi es el controlador de la tarjeta Wi-Fi y el sistema operativo. Por este motivo se recomienda siempre tener tanto el sistema operativo como, específicamente, los controladores Wi-Fi de todos los dispositivos actualizados en todo momento.

ALICIA

Sí, yo siempre intento tener ambos actualizados y al día. Incluso en ese caso, ¿todavía podría alguien atacar mis dispositivos móviles a través de Wi-Fi?

BERNARDO

Todos los clientes Wi-Fi almacenan una lista de las redes a las que se han conectado previamente, o redes preferidas (PNL, Preferred Network List), e intentan conectarse a éstas cuando el interfaz Wi-Fi está activo.

Uno de los ataques más comunes sobre clientes Wi-Fi es el de punto de acceso falso (evil twin), donde el atacante suplanta una de estas redes Wi-Fi preferidas y anunciadas por tu dispositivo, con el objetivo de que el cliente se conecte a la red del atacante pensando que es la red Wi-Fi preferida, por ejemplo la de tu empresa, aunque estés a kilómetros de distancia de ésta. Una vez conectado a la red falsa, el atacante intentará lograr acceso completo a tu dispositivo y a sus comunicaciones.

ALICIA

Pero, para que ese ataque funcione mi dispositivo tiene que anunciar al menos una de las redes incluidas en su lista de redes preferidas. Entiendo que actualmente, y para evitar este ataque, los dispositivos Wi-Fi no desvelan su lista de redes preferidas, ¿no?

BERNARDO

Exacto, el ataque sólo es posible si el dispositivo Wi-Fi desvela al menos una red preferida. Hoy en día, muchos dispositivos Wi-Fi evitan anunciar estas redes, aunque aún existen otros, como algunos dispositivos móviles, que son vulnerables y sí lo hacen.

Sin embargo, hay un escenario común que afecta a todos los dispositivos Wi-Fi. Alicia, ¿recuerdas cuando antes comentamos la ocultación del nombre de la red Wi-Fi en las tramas de anuncio (o beacon) como mecanismo de protección? Cuando un cliente Wi-Fi se quiere conectar a una red, pregunta qué redes hay disponibles en su ubicación actual, recorre su lista de redes preferidas, y si alguna coincide, intenta conectarse a ella.

Si una red está configurada como oculta, no será visible en el conjunto de redes actualmente disponibles, por lo que el cliente no podrá conectarse a ella. Para que esta conexión sea posible, el dispositivo tiene que preguntar específicamente por la existencia de la red oculta, desvelando el nombre de esa red. Por tanto, el ataque de punto de acceso falso es posible si el dispositivo contiene redes ocultas en su lista de redes preferidas. Por este motivo se desaconseja configurar las redes Wi-Fi como ocultas, ya que esta supuesta medida de protección disminuye la seguridad de los clientes Wi-Fi.

ALICIA

En cuanto acabemos eliminaré todas las redes ocultas de mi lista de redes preferidas, y de paso, aquellas otras redes Wi-Fi a las que me he conectado alguna vez y a las que es poco probable que lo vuelva a hacer.

Estoy pensando que… aunque yo tenga el interfaz Wi-Fi apagado la mayoría del tiempo, ya que consume más batería, ¿qué ocurre cuando me conecto a otras redes Wi-Fi, como las redes Wi-Fi públicas (hotspots) de la cafetería del trabajo, la biblioteca de mi barrio, un restaurante, hotel o aeropuerto?

BERNARDO

Las redes Wi-Fi públicas, que ofrecen acceso a Internet gratuito o de pago, son un entorno perfecto para los atacantes. Normalmente son redes abiertas que no utilizan mecanismos de cifrado, en todas ellas compartes la red Wi-Fi con otros usuarios, incluido el atacante, e incluso aunque utilicen cifrado, tu tráfico puede ser interceptado ya que la contraseña es conocida por todos los usuarios, salvo que hagan uso de WPA/WPA2 Enterprise, muy poco habitual en estos entornos.

El atacante puede realizar todo tipo de ataques contra tu dispositivo, como capturar tu tráfico cifrado enviado por la red Wi-Fi y acceder a sus contenidos, o intentar explotar vulnerabilidades de seguridad del sistema operativo u otro software cliente, por ejemplo, tu navegador Web o sus extensiones (plugins).

ALICIA

Para evitar ese tipo de ataques, lo habitual es hacer uso de las VPNs (Virtual Private Networks) basadas en SSL o IPSec para proteger todo el tráfico enviado a través de una red insegura, como la red Wi-Fi pública. ¿En ese caso no tengo que preocuparme, verdad?

BERNARDO

El uso de VPNs sobre redes Wi-Fi inseguras es una práctica muy común, y aunque se trata de una medida de seguridad recomendada, debe tenerse en cuenta que presenta vulnerabilidades. Por un lado, las tecnologías VPN protegen el tráfico en capas de comunicaciones superiores (nivel 3 en el caso de IPSec y nivel 5 en el de SSL), por lo que un atacante podría realizar ataques sobre las capas inferiores (nivel 2), como por ejemplo ataques de envenenamiento de la caché ARP.

Por otro, el usuario debe conectarse a la red Wi-Fi insegura para posteriormente establecer un canal de comunicación seguro a través de la VPN, pero ¿qué pasa si este canal seguro no llega a establecerse nunca, o se retrasa? Mientras, los ataques sobre el dispositivo y el tráfico del usuario son posibles. Un ejemplo muy común se presenta en las redes Wi-Fi que requieren autentificación del usuario a través de un portal web o portal cautivo, donde es necesario realizar múltiples conexiones a través de la red Wi-Fi insegura antes de disponer de acceso a Internet para poder establecer la VPN.

En resumen, es preferible por tanto emplear redes Wi-Fi seguras, junto a tecnologías VPNs y conexiones cifradas extremo a extremo, como las basadas en SSL/TLS.

ESCENA 4. RECOMENDACIONES DE SEGURIDAD

BERNARDO

Alicia, ¿te parece si hacemos un resumen rápido de las recomendaciones de seguridad para redes Wi-Fi? ¿Cuáles son las recomendaciones principales para proteger una red Wi-Fi?

ALICIA

Para proteger una red Wi-Fi es recomendable reducir el alcance de la señal, no configurar la red Wi-Fi como oculta y emplear tecnologías de seguridad como WPA2-AES, en su versión Personal (o PSK) con contraseñas suficientemente largas y difícilmente adivinables, o en su versión Enterprise junto al método EAP más adecuado según las características del entorno Wi-Fi corporativo. Adicionalmente es recomendable disponer de mecanismos de detección para poder identificar ataques en la red Wi-Fi.

BERNARDO

¡Muy bien! Y… ¿cuáles son las recomendaciones principales para proteger los clientes Wi-Fi?

ALICIA

Para proteger a los clientes Wi-Fi es recomendable mantener actualizado tanto el sistema operativo como los controladores Wi-Fi, deshabilitar el interfaz Wi-Fi cuando no se está utilizando, evitar conectarse a redes Wi-Fi inseguras, como por ejemplo redes públicas abiertas o con mecanismos de seguridad débiles como WEP, y mantener actualizada la lista de redes preferidas, eliminando redes ocultas o aquellas a las que no nos vayamos a volver a conectar.

BERNARDO

Alicia, es hora de aplicar estas recomendaciones y aumentar la seguridad de las redes y clientes Wi-Fi a los que tenemos acceso. En la página Web de intypedia encontrarás documentación adicional a esta lección. ¡Adiós!

ALICIA

¡Hasta la próxima lección!

Guión adaptado al formato intypedia a partir del documento entregado por D. Raúl Siles.

Madrid, España, enero de 2012

http://www.intypedia.com

http://twitter.com/intypedia

creative commons
Attribution
Noncommercial
No derivative works