Preguntas frecuentes sobre Management Frame Protection (MFP)

Objetivo

Wi-Fi es un medio de difusión que permite que cualquier dispositivo escuche y participe como dispositivo legítimo o no autorizado. Los clientes inalámbricos utilizan tramas de administración como autenticación, desautenticación, asociación, disociación, balizas y sondas para iniciar y eliminar sesiones para los servicios de red. A diferencia del tráfico de datos, que se puede cifrar para proporcionar un nivel de confidencialidad, todos los clientes deben oír y entender estas tramas y, por lo tanto, deben transmitirse como abiertas o sin cifrar. Si bien estas tramas no se pueden cifrar, se deben proteger de la falsificación para proteger el medio inalámbrico de los ataques. Por ejemplo, un atacante podría falsificar tramas de administración de un AP para atacar a un cliente asociado con el AP.

Este documento tiene como objetivo proporcionar respuestas a las preguntas frecuentes sobre la protección de tramas de administración (MFP).

Preguntas Frecuentes

Table Of Contents

1. Qué es MFP?

Las tramas de gestión son tramas de difusión utilizadas por IEEE 802.11 para permitir que un cliente inalámbrico negocie con un punto de acceso inalámbrico (WAP). MFP proporciona seguridad para las tramas de difusión sin cifrar y los mensajes de administración que se transmiten entre los dispositivos inalámbricos.

2. ¿Cómo funciona MFP?

En IEEE 802.11, las tramas de administración como la desautenticación, la desasociación, las balizas y las sondas siempre están sin autenticar y sin cifrar. WAP agrega Message Integrity Check Information Element (MIC IE) a cada trama de administración que transmite.

Cualquier intento de copiar, alterar o reproducir la trama invalida el MIC.

3. ¿Cuáles son algunas de las cosas que un atacante puede hacer en una red con MFP desactivado?

- La vulnerabilidad encontrada en las tramas de administración representa una gran amenaza para una red al permitir que un atacante falsifique una trama de administración de un WAP para atacar a un cliente asociado a ella. Un atacante puede realizar las siguientes acciones:

— Ejecutar una denegación de servicio (DoS): los atacantes utilizan técnicas de evasión fuera de los ataques habituales basados en volumen para evitar la detección y la mitigación, incluidas técnicas de ataque "bajas y lentas" y ataques basados en SSL. Están implementando campañas de ataque de multivulnerabilidad dirigidas a todos los niveles de la infraestructura de la víctima, incluidos los dispositivos de infraestructura de red, firewalls, servidores y aplicaciones.
— Ataque de intrusos contra el cliente cuando se vuelve a conectar — Es una forma de ataque de derivación de clave inductiva que es efectivo en redes 802.11 debido a la falta de integridad efectiva del mensaje. El receptor de una trama no puede verificar que la trama no se haya alterado durante su transmisión.

- Radio Frequency (RF) Jammer: los ataques con una antena direccional de alta potencia desde una distancia se pueden realizar desde el exterior del edificio de la oficina. Las herramientas de ataque utilizadas por los intrusos aprovechan técnicas de pirateo como tramas de administración 802.11 simuladas, tramas de autenticación 802.1x falsificadas o simplemente usan el método de inundación de paquetes de fuerza bruta.
- Router gemelo malvado: es una forma de suplantación de identidad en la que un atacante nombra y se presenta como un punto de acceso legítimo. Esto hace que los usuarios conecten un dispositivo móvil al punto de acceso falso, lo que puede causar más daño al usuario.
- Ejecutar un ataque de diccionario sin conexión: durante un ataque de diccionario, se utilizan variaciones de contraseñas para poner en peligro las credenciales de autenticación del usuario. La mayoría de los algoritmos de autenticación basados en contraseñas son vulnerables a ataques de diccionario en ausencia de una política de contraseña segura.

4. ¿Cuáles son los tipos de MFP?

Estos son los dos tipos de MFP:

- MFP de infraestructura: específicamente, MFP de infraestructura protege las funciones de administración de sesiones 802.11 mediante la adición de MIC IE a las tramas de administración emitidas por los puntos de acceso y no las emitidas por los clientes, que son validadas por otros puntos de acceso en la red. La MFP de infraestructura es pasiva. Puede detectar y notificar intrusiones, pero no tiene forma de detenerlas. Protege las tramas de gestión mediante la detección de adversarios que están invocando ataques de denegación de servicio, inundando la red con sondas de asociación, interjectando como puntos de acceso no autorizados y afectando al rendimiento de la red mediante el ataque a las tramas de medición de calidad de servicio (QoS) y radio.
- MFP de cliente: protege a los clientes autenticados de tramas simuladas, lo que evita que muchos de los ataques habituales contra las redes de área local (LAN) inalámbricas se hagan efectivos. La mayoría de los ataques, como los ataques de desautenticación, vuelven a degradar el rendimiento al competir con clientes válidos.

5. ¿Cuáles son los componentes de la MFP de infraestructura?

La MFP de infraestructura tiene 3 componentes:

- Protección de tramas de administración: cuando se habilita la protección de tramas de administración, el WAP agrega el IE MIC a cada trama de administración que transmite. Cualquier intento de copiar, alterar o reproducir la trama invalida el MIC.
- Validación de tramas de administración: cuando se habilita la validación de tramas de administración, el AP valida cada trama de administración que recibe de otros WAP en la red. Se asegura de que el IE MIC esté presente (cuando el originador está configurado para transmitir tramas MFP) y coincida con el contenido de la trama de administración. Si recibe cualquier trama que no contenga un IE de MIC válido de un Identificador de conjunto de servicios básicos (BSSID) que pertenece a un WAP, que está configurado para transmitir tramas MFP, informa la discrepancia al sistema de administración de red.

  > **Nota:** Para que las marcas de tiempo funcionen correctamente, todos los controladores de LAN inalámbrica (WLC) deben estar sincronizados con el protocolo de tiempo de red (NTP).

- Informes de eventos: el punto de acceso notifica al WLC cuando detecta una anomalía. El WLC agrega los eventos anómalos y los informa a través de las trampas SNMP al administrador de red.

6. ¿Cómo funciona la MFP del cliente?

Específicamente, la MFP del cliente cifra las tramas de administración enviadas entre los puntos de acceso y los clientes de Cisco Compatible Extension versión 5 (CCXv5) de modo que tanto los puntos de acceso como los clientes puedan tomar medidas preventivas al eliminar tramas de administración de clase 3 simuladas (es decir, las tramas de administración pasadas entre un punto de acceso y un cliente que se autentica y asocia). La MFP del cliente aprovecha los mecanismos de seguridad definidos por IEEE 802.11i para proteger los siguientes tipos de tramas de administración unicast de clase 3: acción de desasociación, desautenticación y QoS (extensiones multimedia inalámbricas o WMM). La MFP del cliente protege una sesión de punto de acceso del cliente del tipo de ataque de denegación de servicio más común. Protege las tramas de administración de clase 3 utilizando el mismo método de cifrado utilizado para las tramas de datos de sesión. Si una trama recibida por el punto de acceso o el cliente falla en el descifrado, se descarta y el evento se informa al controlador.

7. ¿Cómo utilizo MFP de cliente?

Para utilizar la MFP del cliente, los clientes deben admitir la MFP CCXv5 y negociar la versión 2 de acceso Wi-Fi protegido (WPA2) mediante el protocolo de integridad de clave temporal (TKIP) o el protocolo de código de autenticación de mensajes de encadenamiento de cifrado estándar de cifrado avanzado (AES-CCMP). Se puede utilizar el protocolo de autenticación extensible (EAP) o la clave precompartida (PSK) para obtener la PMK. CCKM y la gestión de movilidad del controlador se utilizan para distribuir las claves de sesión entre los puntos de acceso para la itinerancia rápida de capa 2 y capa 3.

8. Qué¿son los componentes de MFP del cliente?

Hay 3 componentes de MFP de cliente:

- Generación y distribución de claves: la MFP del cliente aprovecha los protocolos y mecanismos de seguridad definidos por IEEE 802.11i para proteger las tramas de administración de unidifusión de clase 3:

- Tramas de desasociación: una solicitud a un cliente o WAP para desconectar o desasociar una relación de autenticación.

- Tramas de desautenticación: una solicitud a un cliente o WAP para desconectar o desasociar una relación de asociación.

- Acción WMM de QoS: el parámetro WMM se agrega a las tramas de respuesta de baliza, sonda y asociación.

- Protección y validación de tramas de administración: para evitar ataques usando tramas de broadcast, los AP que soportan CCXv5 no emiten ninguna trama de administración de clase de broadcast 3. Un AP en el modo de puente de grupo de trabajo, el modo repetidor o el modo de puente no raíz descarta las tramas de administración de clase de broadcast 3 si el cliente MFP está habilitado.
- Informes de errores: los mecanismos de informes MFP-1 se utilizan para informar de errores de desencapsulación de tramas de administración detectados por los puntos de acceso. Es decir, el WLC recopila estadísticas de error de validación de MFP y reenvía periódicamente información recopilada al WCS.

  Nota: Los errores de violación de MFP detectados por las estaciones cliente son manejados por la función CCXv5 Roaming and Real Time Diagnostics.

9. ¿Por qué mi dispositivo móvil no se puede conectar al dispositivo de infraestructura habilitado para MFP?

Hay ciertas restricciones para que algunos clientes inalámbricos se comuniquen con dispositivos de infraestructura habilitados para MFP. MFP agrega un largo conjunto de elementos de información a cada solicitud de sonda o baliza SSID. Algunos clientes inalámbricos, como los PDA, los smartphones, los escáneres de código de barras, etc., tienen memoria limitada y unidad de procesamiento central (CPU). Por lo tanto, no puede procesar estas solicitudes o balizas. Como resultado, no puede ver el SSID en su totalidad o no puede asociarse a estos dispositivos de infraestructura debido a un malentendido en las capacidades de SSID. Este problema no es específico de MFP. Esto también ocurre con cualquier SSID que tenga varios elementos de información (IE). Siempre es recomendable probar los SSID habilitados para MFP en el entorno con todos los tipos de cliente disponibles antes de implementarlos en tiempo real.

10. ¿Qué es la protección de tramas de administración de difusión?

Para evitar ataques que utilizan tramas de broadcast, los AP que soportan CCXv5 no transmiten ninguna trama de administración de clase de broadcast 3 excepto para tramas de desautenticación o desasociación de contención no autorizada. Las estaciones cliente compatibles con CCXv5 deben descartar las tramas de administración de clase de broadcast 3. Se supone que las sesiones MFP se encuentran en una red protegida correctamente (autenticación fuerte más TKIP o CCMP), por lo que el desprecio por las transmisiones de contención no autorizada no es un problema.

11. ¿Cómo se configura MFP en un punto de acceso inalámbrico (WAP)?

Para aprender a configurar MFP en un WAP, haga clic aquí.

12. Cómo configurar una tarjeta de red inalámbrica Intel para conectarse a una red habilitada para MFP

Para saber cómo configurar la tarjeta de red inalámbrica Intel, haga clic aquí.