Perguntas frequentes sobre a proteção de quadro de gerenciamento (MFP)

Objetivo

Wi-Fi é um meio de transmissão que permite que qualquer dispositivo escute e participe como um dispositivo legítimo ou invasor. Quadros de gerenciamento como autenticação, desautenticação, associação, dissociação, beacons e sondas são usados por clientes sem fio para iniciar e desligar sessões para serviços de rede. Ao contrário do tráfego de dados, que pode ser criptografado para fornecer um nível de confidencialidade, esses quadros devem ser ouvidos e entendidos por todos os clientes e, portanto, devem ser transmitidos como abertos ou não criptografados. Embora esses quadros não possam ser criptografados, eles devem ser protegidos contra falsificação para proteger o meio sem fio contra ataques. Por exemplo, um invasor pode falsificar quadros de gerenciamento de um AP para atacar um cliente associado ao AP.

Este documento tem como objetivo fornecer respostas para as perguntas frequentes sobre a proteção de quadro de gerenciamento (MFP).

Perguntas mais freqüentes

Table Of Contents

1. O que é MFP?
2. Como funciona o MFP?
3. Qual é a diferença do PMF?
4. Quais são os tipos de MFP?
5. Quais são os componentes do Client MFP?
6. Como o MFP do cliente funciona?
7. Como uso o MFP do cliente?
8. Quais são os componentes do Client MFP?
9. Por que meu dispositivo móvel não pode se conectar ao dispositivo de infraestrutura habilitado para MFP?
10. O que é a proteção do quadro de gerenciamento de broadcast?
11. Como configurar o MFP em um ponto de acesso sem fio (WAP)?
12. Como configurar a Placa de rede sem fio Intel para conectar-se a uma rede habilitada para MFP?

1. O que é MFP?

Os quadros de gerenciamento são quadros de broadcast usados pelo IEEE 802.11 para permitir que um cliente sem fio negocie com um ponto de acesso sem fio (WAP). O MFP oferece segurança para quadros de broadcast não criptografados e mensagens de gerenciamento passadas entre dispositivos sem fio.

2. Como funciona o MFP?

No IEEE 802.11, os quadros de gerenciamento como desautenticação, desassociação, beacons e sondas são sempre não autenticados e não criptografados. O WAP adiciona o

MIC IE (Message Integrity Check Information Element) a cada quadro de gerenciamento que transmite. Qualquer tentativa de copiar, alterar ou reproduzir o quadro invalida o MIC.

3. Quais são algumas das coisas que um invasor pode fazer em uma rede com o MFP desabilitado?

- A vulnerabilidade encontrada nos quadros de gerenciamento representa uma grande ameaça para uma rede ao permitir que um invasor falsifique um quadro de gerenciamento de um WAP para atacar um cliente associado a ele. Um invasor pode executar as seguintes ações:

— Execute um DoS (Denial of Service, negação de serviço) — Os invasores estão usando técnicas de evasão fora dos ataques típicos baseados em volume para evitar a detecção e mitigação, incluindo técnicas de ataque "baixas e lentas" e ataques baseados em SSL. Eles estão implantando campanhas de ataque de multivulnerabilidade voltadas para cada camada da infraestrutura da vítima, incluindo dispositivos de infraestrutura de rede, firewalls, servidores e aplicativos.
— ataque do tipo "homem no meio" ao cliente quando reconectado — é uma forma de ataque indutivo de derivação de chave que é eficaz em redes 802.11 devido à falta de integridade efetiva da mensagem. O receptor de um quadro não pode verificar se o quadro não foi adulterado durante sua transmissão.

- Jammer de radiofreqüência (RF) — Os ataques com uma antena direcional de alta potência a uma distância podem ser realizados a partir da parte externa do prédio do seu escritório. As ferramentas de ataque usadas por invasores utilizam técnicas de hacking como quadros de gerenciamento 802.11 falsificados, quadros de autenticação 802.1x falsificados ou simplesmente usando o método de inundação de pacote de força bruta.
- Roteador Evil Twin — É uma forma de phishing na qual um invasor nomeia e se apresenta como um ponto de acesso legítimo. Isso faz com que os usuários conectem um dispositivo móvel ao ponto de acesso falso, podendo causar mais danos ao usuário.
- Executar um ataque de dicionário offline — Durante um ataque de dicionário, variações de senhas são usadas para comprometer as credenciais de autenticação do usuário. A maioria dos algoritmos de autenticação com base em senha está vulnerável a ataques de dicionário na ausência de uma política de senha forte.

4. Quais são os tipos de MFP?

Estes são os dois tipos de MFPs:

- MFP de infraestrutura — Especificamente, o MFP de infraestrutura protege as funções de gerenciamento de sessão 802.11 adicionando o MIC IE aos quadros de gerenciamento emitidos pelos pontos de acesso e não os emitidos pelos clientes, que são validados por outros pontos de acesso na rede. O MFP de infraestrutura é passivo. Ele pode detectar e relatar intrusões, mas não tem como detê-las. Ele protege quadros de gerenciamento detectando criminosos que estão invocando ataques de negação de serviço, inundando a rede com testadores de associação, interagindo como pontos de acesso não autorizados e afetando o desempenho da rede atacando os quadros de medição de qualidade de serviço (QoS) e de rádio.
- MFP do cliente — Protege os clientes autenticados contra quadros falsificados, impedindo que muitos dos ataques comuns contra as LANs (Local Area Networks, redes locais) sem fio se tornem efetivos. A maioria dos ataques, como os ataques de desautenticação, reverte simplesmente a degradar o desempenho disputando com clientes válidos.

5. Quais são os componentes do MFP de infraestrutura?

O MFP de infraestrutura tem três componentes:

- Proteção do quadro de gerenciamento — Quando a proteção do quadro de gerenciamento está habilitada, o WAP adiciona o MIC IE a cada quadro de gerenciamento que transmite. Qualquer tentativa de copiar, alterar ou reproduzir o quadro invalida o MIC.
- Validação do quadro de gerenciamento — Quando a validação do quadro de gerenciamento está habilitada, o AP valida cada quadro de gerenciamento recebido de outros WAPs na rede. Garante que o MIC IE esteja presente (quando o originador estiver configurado para transmitir quadros MFP) e corresponda ao conteúdo do quadro de gerenciamento. Se receber qualquer quadro que não contenha um IE MIC válido de um BSSID (Basic Service Set Identifier) pertencente a um WAP, que está configurado para transmitir quadros MFP, ele reportará a discrepância para o sistema de gerenciamento de rede.

  Observação: para que os timestamps funcionem corretamente, todos os Wireless LAN Controllers (WLC) devem estar sincronizados com o Network Time Protocol (NTP).

- Relatório de eventos — O ponto de acesso notifica a WLC quando detecta uma anomalia. A WLC agrega os eventos anômalos e os relata através de armadilhas SNMP ao gerenciador de rede.

6. Como o MFP do cliente funciona?

Especificamente, o MFP do cliente criptografa quadros de gerenciamento enviados entre os pontos de acesso e os clientes do Cisco Compatible Extension 5 (CCXv5) para que tanto os pontos de acesso quanto os clientes possam tomar medidas preventivas ao descartar quadros de gerenciamento de classe 3 falsificados (ou seja, quadros de gerenciamento passados entre um ponto de acesso e um cliente autenticado e associado). O MFP do cliente aproveita os mecanismos de segurança definidos pelo IEEE 802.11i para proteger os seguintes tipos de quadros de gerenciamento unicast classe 3: ação de desassociação, desautenticação e QoS (Wireless Multimedia Extensions ou WMM). O MFP do cliente protege uma sessão de ponto de acesso do cliente do tipo mais comum de ataque de negação de serviço. Ele protege quadros de gerenciamento de classe 3 usando o mesmo método de criptografia usado para os quadros de dados da sessão. Se um quadro recebido pelo ponto de acesso ou cliente falha na descriptografia, ele é descartado e o evento é relatado ao controlador.

7. Como uso o MFP do cliente?

Para usar o MFP do cliente, os clientes devem suportar o CCXv5 MFP e devem negociar o WPA2 (Wi-Fi Protected Access versão 2) usando o TKIP (Temporal Key Integrity Protocol) ou o AES-CCMP (Advanced Encryption Standard-Cipher Block Message Authentication Protocol). O Extensible Authentication Protocol (EAP) ou Pre-Shared Key (PSK) pode ser usado para obter o PMK. O CCKM e o gerenciamento de mobilidade do controlador são usados para distribuir chaves de sessão entre pontos de acesso para o roaming rápido de Camada 2 e Camada 3.

8. O quesão os componentes do cliente MFP?

Há 3 componentes do MFP do cliente:

- Geração e distribuição de chaves — O MFP do cliente aproveita os protocolos e mecanismos

de segurança definidos pelo IEEE 802.11i para proteger quadros de gerenciamento unicast de classe 3:

- Quadros de desassociação — Uma solicitação a um cliente ou WAP para desconectar ou desassociar uma relação de autenticação.

- Quadros de desautenticação — Uma solicitação a um cliente ou WAP para desconectar ou desassociar uma relação de associação.

Ação WMM de QoS — O parâmetro WMM é adicionado aos quadros beacon, resposta de sondagem e resposta de associação.

- Proteção e validação de quadros de gerenciamento — Para evitar ataques usando quadros de broadcast, os APs que suportam CCXv5 não emitem nenhum quadro de gerenciamento de classe 3 de broadcast. Um AP no modo de bridge de grupo de trabalho, no modo de repetidor ou no modo de bridge não raiz descarta os quadros de gerenciamento de classe 3 de broadcast se o MFP do cliente estiver ativado.
- Relatórios de erros — Os mecanismos de relatório MFP-1 são usados para relatar erros de desencapsulamento de quadros de gerenciamento detectados por pontos de acesso. Ou seja, a WLC coleta estatísticas de erro de validação de MFP e encaminha periodicamente informações coladas para o WCS.

Note: Os erros de violação de MFP detectados por estações clientes são tratados pelo recurso CCXv5 Roaming e Real Time Diagnostics.

9. Por que meu dispositivo móvel não pode se conectar ao dispositivo de infraestrutura habilitado para MFP?

Há certas restrições para alguns clientes sem fio se comunicarem com dispositivos de infraestrutura habilitados para MFP. O MFP adiciona um longo conjunto de elementos de informação a cada solicitação de sondagem ou beacon SSID. Alguns clientes sem fio, como PDAs, smartphones, scanners de código de barras e assim por diante, têm memória limitada e unidade central de processamento (CPU). Portanto, você não pode processar essas solicitações ou beacons. Como resultado, você não consegue ver o SSID completamente ou não consegue se associar a esses dispositivos de infraestrutura, devido a um mal-entendido sobre os recursos do SSID. Esse problema não é específico do MFP. Isso também ocorre com qualquer SSID que tenha vários elementos de informação (IEs). É sempre aconselhável testar os SSIDs habilitados para MFP no ambiente com todos os tipos de clientes disponíveis antes de implantá-los em tempo real.

10. O que é a proteção do quadro de gerenciamento de broadcast?

Para evitar ataques que usam quadros de broadcast, os APs que suportam CCXv5 não transmitem nenhum quadro de gerenciamento de classe 3 de broadcast, exceto para quadros de desautenticação ou desassociação de contenção de invasão. As estações cliente com capacidade para CCXv5 devem descartar quadros de gerenciamento de classe 3 de broadcast. Supõe-se que as sessões de MFP estejam em uma rede adequadamente segura (autenticação forte mais TKIP ou CCMP), de modo que o desrespeito por broadcasts de contenção não autorizados não seja um problema.

11. Como configurar o MFP em um ponto de acesso sem fio (WAP)?

Para saber como configurar o MFP em um WAP, clique aqui.

12. Como configurar uma Placa de Rede Sem Fio Intel para se conectar a uma Rede

habilitada para MFP

Para saber como configurar a Placa de rede sem fio Intel, clique aqui.