Foire aux questions sur Management Frame Protection (MFP)

Objectif

Le Wi-Fi est un support de diffusion qui permet à n'importe quel périphérique d'écouter et de participer en tant que périphérique légitime ou non autorisé. Les trames de gestion, telles que l'authentification, la désauthentification, l'association, la dissociation, les balises et les sondes, sont utilisées par les clients sans fil pour initier et arrêter des sessions pour les services réseau. Contrairement au trafic de données, qui peut être chiffré pour fournir un niveau de confidentialité, ces trames doivent être entendues et comprises par tous les clients et doivent donc être transmises en mode ouvert ou non chiffré. Bien que ces trames ne puissent pas être chiffrées, elles doivent être protégées contre la falsification pour protéger le support sans fil des attaques. Par exemple, un pirate peut usurper les trames de gestion d'un point d'accès pour attaquer un client associé au point d'accès.

Ce document vise à fournir des réponses aux questions fréquemment posées sur la protection des trames de gestion (MFP).

Forum aux questions

Table des matières

1. Qu'est-ce que MFP ?
2. Comment fonctionne le programme MFP ?
3. En quoi diffère-t-elle du CMR ?
4. Quels sont les types d'imprimantes multifonctions ?
5. Quels sont les composants de l'imprimante multifonction client ?
6. Comment fonctionne la fonction MFP du client ?
7. Comment utiliser la fonction MFP du client ?
8. Quels sont les composants de l'imprimante multifonction client ?
9. Pourquoi mon appareil mobile ne peut-il pas se connecter à l'appareil d'infrastructure compatible MFP ?
10. Qu'est-ce que Broadcast Management Frame Protection ?
11. Comment configurer MFP sur un point d'accès sans fil (WAP) ?
12. Comment configurer la carte réseau sans fil Intel pour la connexion à un réseau compatible MFP ?

1. Quoi ? est MFP ?

Les trames de gestion sont des trames de diffusion utilisées par la norme IEEE 802.11 pour permettre à un client sans fil de négocier avec un point d'accès sans fil (WAP). MFP assure la sécurité des trames de diffusion non cryptées et des messages de gestion transmis entre les périphériques sans fil.

2. Comment fonctionne le programme MFP ?

Dans IEEE 802.11, les trames de gestion telles que la désauthentification, la dissociation, les balises et les sondes sont toujours non authentifiées et non chiffrées. Le WAP ajoute l'élément d'information de contrôle d'intégrité de message (MIC IE) à chaque trame de gestion qu'il transmet. Toute tentative de copie, de modification ou de relecture de la trame invalide le MIC.

3. Quelles sont certaines des actions qu'un pirate peut effectuer sur un réseau dont la fonction MFP est désactivée ?

- La vulnérabilité trouvée dans les trames de gestion constitue une menace importante pour un réseau en permettant à un pirate d'usurper une trame de gestion à partir d'un WAP pour attaquer un client qui lui est associé. Un pirate peut effectuer les actions suivantes :

  — Exécuter un déni de service (DoS) — Les pirates utilisent des techniques d'évasion en dehors des attaques classiques basées sur le volume pour éviter la détection et l'atténuation, y compris les techniques d'attaque « lente et faible » et les attaques basées sur SSL. Ils déploient des campagnes d'attaque multivulnérabilités qui ciblent chaque couche de l'infrastructure de la victime, y compris les périphériques de l'infrastructure réseau, les pare-feu, les serveurs et les applications.
  — Attaque Man-in-the-Middle sur le client lors de la reconnexion — Il s'agit d'une forme d'attaque par dérivation de clé inductive qui est efficace dans les réseaux 802.11 en raison du manque d'intégrité effective des messages. Le récepteur d'une trame ne peut pas vérifier que la trame n'a pas été altérée lors de sa transmission.

- Brouilleur de radiofréquences (RF) : les attaques à distance à l'aide d'une antenne directionnelle haute puissance peuvent être effectuées depuis l'extérieur de votre immeuble de bureaux. Les outils d'attaque utilisés par les intrus utilisent des techniques de piratage telles que les trames de gestion 802.11 usurpées, les trames d'authentification 802.1x usurpées ou simplement la méthode de diffusion de paquets en force.
- Evil Twin Router : il s'agit d'une forme d'hameçonnage dans laquelle un pirate se fait passer pour un point d'accès légitime. Cela incite les utilisateurs à connecter un appareil mobile au faux point d'accès, ce qui peut causer plus de mal à l'utilisateur.
- Exécuter une attaque par dictionnaire hors connexion : lors d'une attaque par

dictionnaire, des variations de mots de passe sont utilisées pour compromettre les informations d'authentification de l'utilisateur. La plupart des algorithmes d'authentification par mot de passe sont vulnérables aux attaques par dictionnaire en l'absence d'une stratégie de mot de passe forte.

4. Quels sont les types d'imprimantes multifonctions ?

Voici les deux types d'imprimantes multifonctions :

- Infrastructure MFP : plus précisément, l'infrastructure MFP protège les fonctions de gestion de session 802.11 en ajoutant l'IE MIC aux trames de gestion émises par les points d'accès et non pas à celles émises par les clients, qui sont validées par d'autres points d'accès du réseau. La fonction MFP d'infrastructure est passive. Il peut détecter et signaler les intrusions, mais il n'a aucun moyen de les arrêter. Il protège les trames de gestion en détectant les hackers qui lancent des attaques par déni de service, inondent le réseau avec des sondes d'association, s'interjettent en tant que points d'accès non autorisés et affectent les performances du réseau en attaquant les trames de mesure de la qualité de service (QoS) et de la radio.
- Client MFP : protège les clients authentifiés contre les trames usurpées, empêchant ainsi de nombreuses attaques courantes contre les réseaux locaux (LAN) sans fil de devenir efficaces. La plupart des attaques, telles que les attaques de désauthentification, se contentent de dégrader les performances en entrant en conflit avec des clients valides.

5. Quels sont les composants du module MFP d'infrastructure ?

La fonction MFP d'infrastructure comporte 3 composants :

- Protection de la trame de gestion : lorsque la protection de la trame de gestion est activée, le WAP ajoute l'IE MIC à chaque trame de gestion qu'il transmet. Toute tentative de copie, de modification ou de relecture de la trame invalide le MIC.
- Validation de la trame de gestion — Lorsque la validation de la trame de gestion est activée, le point d'accès valide chaque trame de gestion qu'il reçoit des autres points d'accès sans fil du réseau. Il s'assure que l'IE MIC est présent (lorsque l'émetteur est configuré pour transmettre des trames MFP) et qu'il correspond au contenu de la trame de gestion. S'il reçoit une trame qui ne contient pas un IE MIC valide d'un BSSID (Basic Service Set Identifier) qui appartient à un WAP, qui est configuré pour transmettre des trames MFP, il signale la différence au système de gestion du réseau.

  Remarque : pour que les horodatages fonctionnent correctement, tous les contrôleurs LAN sans fil (WLC) doivent être synchronisés avec le protocole NTP (Network Time Protocol).

- Event reporting : le point d'accès avertit le WLC lorsqu'il détecte une anomalie. WLC agrège les événements anormaux et les rapporte via des déroutements SNMP au gestionnaire de réseau.

6. Comment fonctionne le programme MFP client ?

Plus précisément, le client MFP chiffre les trames de gestion envoyées entre les points d'accès et les clients CCXv5 (Cisco Compatible Extension version 5) de sorte que les points d'accès et les clients puissent prendre des mesures préventives en abandonnant les trames de gestion usurpées de classe 3 (c'est-à-dire les trames de gestion passées entre un point d'accès et un client authentifié et associé). Le protocole MFP client exploite les mécanismes de sécurité définis par la norme IEEE 802.11i pour protéger les types suivants de trames de gestion de monodiffusion de classe 3 : désassociation, désauthentification et action QoS (Wireless Multimedia Extensions ou WMM). Le protocole MFP client protège une session de point d'accès client contre le type d'attaque par déni de service le plus courant. Il protège les trames de gestion de classe 3 en utilisant la même méthode de cryptage que celle utilisée pour les trames de données de session. Si une trame reçue par le point d'accès ou le client ne parvient pas à être déchiffrée, elle est abandonnée et l'événement est signalé au contrôleur.

7. Comment utiliser le module MFP client ?

Pour utiliser la fonction MFP du client, les clients doivent prendre en charge la fonction MFP CCXv5 et négocier la version 2 de la norme WPA2 (Wi-Fi Protected Access version 2) à l'aide du protocole TKIP (Temporal Key Integrity Protocol) ou du protocole AES-CCMP (Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol). Le protocole EAP (Extensible Authentication Protocol) ou la clé prépartagée (PSK) peuvent être utilisés pour obtenir la clé PMK. CCKM et la gestion de la mobilité du contrôleur sont utilisés pour distribuer des clés de session entre les points d'accès pour l'itinérance rapide des couches 2 et 3.

8. Quel estLes composants de l'imprimante multifonction client sont-ils

Il existe 3 composants de l'imprimante multifonction client :

- Génération et distribution de clés — Client MFP tire parti des protocoles et mécanismes de sécurité définis par la norme IEEE 802.11i pour protéger les trames de gestion de monodiffusion de classe 3 :

  - Trames de dissociation : demande adressée à un client ou à un WAP pour déconnecter ou dissocier une relation d'authentification.

- Trames de désauthentification : demande à un client ou à un WAP de déconnecter ou de dissocier une relation d'association.

- Action WMM QoS : le paramètre WMM est ajouté aux trames de réponse de balise, de sonde et d'association.

- Protection et validation des trames de gestion : pour empêcher les attaques utilisant des trames de diffusion, les points d'accès qui prennent en charge CCXv5 n'émettent aucune trame de gestion de diffusion de classe 3. Un point d'accès en mode pont de groupe de travail, en mode répéteur ou en mode pont non racine rejette les trames de gestion de diffusion de classe 3 si l'interface MFP du client est activée.
- Rapports d'erreurs — Les mécanismes de rapport MFP-1 sont utilisés pour signaler les erreurs de désencapsulation de trame de gestion détectées par les points d'accès. En d'autres termes, le WLC collecte des statistiques d'erreur de validation MFP et transmet périodiquement les informations collectées au WCS.

  Remarque : les erreurs de violation MFP détectées par les stations clientes sont gérées par la fonctionnalité CCXv5 Roaming and Real Time Diagnostics.

9. Pourquoi mon appareil mobile ne peut-il pas se connecter à l'appareil d'infrastructure compatible MFP ?

Certaines restrictions s'appliquent à certains clients sans fil pour communiquer avec des périphériques d'infrastructure compatibles MFP. MFP ajoute un ensemble d'éléments d'information à chaque demande de sonde ou balise SSID. Certains clients sans fil, tels que les assistants numériques personnels, les smartphones, les scanners de codes à barres, etc., disposent d'une mémoire limitée et d'une unité centrale (UC). Par conséquent, vous ne pouvez pas traiter ces demandes ou balises. Par conséquent, vous ne voyez pas le SSID entièrement, ou vous ne pouvez pas vous associer à ces périphériques d'infrastructure, en raison d'une mauvaise compréhension des capacités du SSID. Ce problème n'est pas spécifique à l'imprimante multifonction. Cela se produit également avec n'importe quel SSID qui a plusieurs éléments d'information (IE). Il est toujours conseillé de tester les SSID compatibles MFP sur l'environnement avec tous les types de clients disponibles avant de les déployer en temps réel.

10. Qu'est-ce que Broadcast Management Frame Protection ?

Afin d'empêcher les attaques qui utilisent des trames de diffusion, les AP qui prennent en charge CCXv5 ne transmettent aucune trame de gestion de classe 3 de diffusion, à l'exception des trames de désauthentification ou de désassociation de confinement non autorisées. Les stations clientes compatibles CCXv5 doivent ignorer les trames de gestion de diffusion de classe 3. Les sessions MFP sont supposées se trouver dans un réseau correctement sécurisé (authentification forte plus TKIP ou CCMP), de sorte que le non-respect des diffusions de confinement non autorisé ne pose pas de problème.

11. Comment configurer MFP sur un point d'accès sans fil (WAP) ?

Pour savoir comment configurer MFP sur un WAP, cliquez ici.

12. Configuration d'une carte réseau sans fil Intel pour la connexion à un réseau compatible MFP

Pour savoir comment configurer la carte réseau sans fil Intel, cliquez ici.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.