Questions fréquentes sur la protection des trames de gestion (MFP)

Objectif

Le Wi-Fi est un support de diffusion qui permet à tout 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 lancer et démonter 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 comme ouvertes ou non chiffrées. Bien que ces trames ne puissent pas être chiffrées, elles doivent être protégées contre les faux 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 cadres de gestion (MFP).

Forum aux questions

Table des matières

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 MFP ?

Dans IEEE 802.11, les trames de gestion telles que la déauthentification, la dissociation, les balises et les sondes ne sont toujours pas authentifiées et non chiffrées. Le WAP ajoute

l'élément MIC IE (Message Integrity Check Information Element) à chaque trame de gestion qu'il transmet. Toute tentative de copie, de modification ou de relecture de la trame invalide la MIC.

3. Que peut faire un pirate sur un réseau avec MFP désactivé ?

- La vulnérabilité trouvée dans les trames de gestion représente une grande menace pour un réseau en permettant à un pirate de pirater une trame de gestion 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 basées sur les volumes classiques pour éviter la détection et l'atténuation, notamment des techniques d'attaque « lente et faible » et des attaques basées sur SSL. Ils déploient des campagnes d'attaque multivulnérabilité ciblant chaque couche de l'infrastructure de la victime, notamment les périphériques d'infrastructure réseau, les pare-feu, les serveurs et les applications.
— Attaque de l'homme du milieu sur le client lors de sa reconnexion — Il s'agit d'une forme d'attaque de dérivation de clé inductive qui est efficace dans les réseaux 802.11 en raison du manque d'intégrité des messages. Le récepteur d'une trame ne peut pas vérifier que la trame n'a pas été falsifiée lors de sa transmission.

- Jammer de radiofréquence (RF) : les attaques avec une antenne directionnelle haute puissance à distance peuvent être effectuées depuis l'extérieur de votre bureau. Les outils d'attaque utilisés par les intrus exploitent des techniques de piratage telles que les trames de gestion 802.11 usurpées, les trames d'authentification 802.1x usurpées, ou simplement en utilisant la méthode d'inondation de paquets force brute.
- Routeur jumeau malveillant - Il s'agit d'une forme d'hameçonnage dans laquelle un pirate nomme et pose comme point d'accès légitime. Cela incite les utilisateurs à connecter un appareil mobile au faux point d'accès, ce qui leur permet de causer plus de dommages.
- Exécuter une attaque de dictionnaire hors connexion : lors d'une attaque de dictionnaire, des variantes de mots de passe sont utilisées pour compromettre les informations d'authentification de l'utilisateur. La plupart des algorithmes d'authentification basés sur un mot de passe sont vulnérables aux attaques de dictionnaire en l'absence d'une stratégie de mot de passe forte.

4. Quels sont les types de MFP ?

Voici les deux types de MFP :

- MFP d'infrastructure - Plus précisément, la MFP d'infrastructure protège les fonctions de gestion de session 802.11 en ajoutant MIC IE aux trames de gestion émises par les points d'accès et non par les clients, qui sont validées par d'autres points d'accès du réseau. Le MFP d'infrastructure est passif. Il peut détecter et signaler les intrusions, mais il n'a aucun moyen de les arrêter. Elle protège les trames de gestion en détectant les hackers qui invoquent des attaques par déni de service, en inondant le réseau de sondes d'association, en les interjetant en tant que points d'accès non autorisés et en affectant 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 sans fil de devenir efficaces. La plupart des attaques, telles que les attaques de déauthentification, reviennent simplement à dégrader les performances en affrontant des clients valides.

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

Le module MFP d'infrastructure comporte 3 composants :

- Protection des trames de gestion : lorsque la protection des trames de gestion est activée, le WAP ajoute MIC IE à chaque trame de gestion qu'il transmet. Toute tentative de copie, de modification ou de relecture de la trame invalide la MIC.
- Validation des trames de gestion : lorsque la validation des trames de gestion est activée, le point d'accès valide toutes les trames de gestion qu'il reçoit des autres points d'accès sans fil du réseau. Il garantit que l'IE MIC est présente (lorsque l'émetteur est configuré pour transmettre des trames MFP) et correspond au contenu de la trame de gestion. S'il reçoit une trame qui ne contient pas d'IE MIC valide d'un BSSID (Basic Service Set Identifier) appartenant à un WAP, 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 de réseau local sans fil (WLC) doivent être synchronisés avec le protocole NTP (Network Time Protocol).

- Rapports d'événements : le point d'accès avertit le WLC lorsqu'il détecte une anomalie. Le WLC agrège les événements anormaux et les signale via des interruptions SNMP au gestionnaire de réseau.

6. Comment fonctionne la MFP client ?

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

7. Comment utiliser la MFP client ?

Pour utiliser la MFP du client, les clients doivent prendre en charge la MFP CCXv5 et négocier le protocole 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-Chipher Block Chaining Message Authentication Code Protocol). Le protocole EAP (Extensible Authentication Protocol) ou la clé prépartagée (PSK) peut être utilisé pour obtenir la clé PMK. CCKM et la gestion de la mobilité des contrôleurs sont utilisés pour distribuer les clés de session entre les points d'accès pour l'itinérance rapide de couche 2 et de couche 3.

8. QuelleLes composants du client MFP sont-ils ?

Il existe trois composants de la MFP client :

- Génération et distribution de clés - La MFP client exploite les 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 de déconnecter ou de dissocier une relation d'authentification.

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

    - Action QoS WMM : 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 prenant en charge CCXv5 n'émettent aucune trame de gestion de classe de diffusion 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 classe de diffusion 3 si la 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. Autrement dit, le WLC collecte des statistiques d'erreur de validation MFP et transmet périodiquement les informations collectées au WCS.

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

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

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

10. Qu'est-ce que la protection de trame de gestion de diffusion ?

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

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