Forums aux questions au sujet du Management Frame Protection (MFP)

Objectif

Le WiFi est un support de diffusion qui permet à n'importe quel périphérique d'écouter clandestinement et participer comme périphérique légitime ou escroc. Des trames de Gestion telles que l'authentification, la désauthentification, l'association, la dissociation, les balises, et les sondes sont utilisées par des clients sans fil pour initier et démolir des sessions pour des services réseau. À la différence du trafic de données, qui peut être chiffré pour fournir un niveau de confidentialité, ces trames doivent être entendues et compris par tous les clients et doit donc être transmis comme ouvert ou décrypté. Tandis que ces trames ne peuvent pas être chiffrées, elles doivent être protégées contre le contrefaçon pour protéger le support Sans fil contre des attaques. Par exemple, un attaquant pourrait charrier des trames de Gestion d'AP pour attaquer un client associé avec AP.

Ce document vise à apporter des réponses aux forums aux questions au sujet du Management Frame Protection (MFP).

Forum aux questions

Table des matières

1. Quel est MFP ?

Les trames de Gestion sont des trames d'émission utilisées par IEEE 802.11 pour permettre à un client sans fil pour être en pourparlers avec un point d'accès sans fil (WAP). MFP fournit la Sécurité pour les trames décryptées et les messages de gestion d'émission passés entre les périphériques sans fil.

2. Comment MFP fonctionne-t-il ?

Dans l'IEEE 802.11, les trames de Gestion telles que le deauthentication, la dissassociation, les balises, et les sondes sont toujours unauthenticated et décryptées. Le WAP ajoute

l'élément d'information de Message Integrity Check (IE MIC) à chaque trame de Gestion qu'il transmet. N'importe quelle tentative de copier, modifier, ou rejouer la trame infirme la MIC.

3. Queest-ce que certaines des choses sont un attaquant peuvent faire sur un réseau avec MFP ont désactivé ?

- La vulnérabilité fondent dans la pose de trames de Gestion une grande menace pour un réseau en permettant à un attaquant pour charrier une trame de Gestion d'un WAP pour attaquer un client qui est associé à lui. Un attaquant peut exécuter les actions suivantes :

— Exécutez un Déni de service (DOS) — des attaquants emploient des techniques d'évasion en dehors de des attaques basées sur volume typiques pour éviter la détection et la réduction, y compris des « basses et lentes » techniques d'attaque et des attaques basées sur SSL. Ils déploient les campagnes d'attaque de multivulnerability qui visent chaque couche de l'infrastructure de la victime, y compris les périphériques d'infrastructure réseau, les Pare-feu, les serveurs, et les applications.
— Attaque Homme-dans-le-moyenne sur le client une fois rebranché — c'est une forme d'une attaque inductive de dérivation de clé qui est efficace dans des réseaux de 802.11 en raison du manque d'intégrité des messages efficace. Le récepteur d'une trame ne peut pas vérifier que la trame n'a pas été trifouillée pendant sa transmission.

- Brouilleur de Radiofréquence (RF) — Des attaques avec une antenne directionnelle de haute puissance d'une distance peuvent être effectuées de l'extérieur de votre immeuble de bureau. Les outils d'attaque utilisés par des intrus accroissent entailler des techniques telles que les trames charriées de Gestion de 802.11, les trames charriées d'authentification de 802.1x, ou simplement suivre la méthode d'inondation de paquet de force brutale.
- Routeur jumeau mauvais — C'est une forme de phishing dans laquelle un attaquant nomme et pose comme Point d'accès légitime. Ceci dupe des utilisateurs dans connecter un périphérique mobile au faux Point d'accès, de ce fait pouvant entraîner plus de mal à l'utilisateur.
- Exécutez une attaque par dictionnaire hors ligne — Pendant une attaque par dictionnaire, des variations des mots de passe sont utilisées pour compromettre les qualifications d'authentification de l'utilisateur. La plupart des algorithmes basés sur mot de passe d'authentification sont vulnérables aux attaques par dictionnaire faute de stratégie de mot de passe fort.

4. Quels sont les types de MFP ?

Ce sont les deux types de MFPs :

- Infrastructure MFP — Spécifiquement, l'infrastructure MFP protège des fonctions de gestion de session de 802.11 en ajoutant l'IE MIC aux trames de Gestion émises par des Points d'accès et pas ceux émis par les clients, qui sont validés par d'autres Points d'accès dans le réseau. L'infrastructure MFP est passive. Il peut le détecter et des intrusions d'état mais il n'a aucun moyen de les arrêter. Il protège des trames de Gestion en détectant les adversaires qui appellent des attaques par déni de service, inondent le réseau avec des sondes d'association, exclament comme points d'accès non autorisé, et affectent des performances du réseau en attaquant le Qualité de service (QoS) et les trames par radio de mesure.
- Client MFP — Les boucliers ont authentifié des clients des trames charriées, empêchant plusieurs des attaques communes contre les réseaux locaux sans fil (réseaux locaux) de l'entrée en vigueur. La plupart des attaques, telles que des attaques de désauthentification,

retournent à la représentation dégradante simplement en faisant face aux clients valides.

5. Quels sont les composants de l'infrastructure MFP ?

L'infrastructure MFP a 3 composants :

- Protection de trame de Gestion — Quand la protection de trame de Gestion est activée, le WAP ajoute l'IE MIC à chaque trame de Gestion qu'il transmet. N'importe quelle tentative de copier, modifier, ou rejouer la trame infirme la MIC.
- Validation de trame de Gestion — Quand la validation de trame de Gestion est activée, AP valide chaque trame de Gestion qu'il reçoit d'autres WAP dans le réseau. Il s'assure que l'IE MIC est présent (quand le créateur est configuré pour transmettre des trames MFP) et apparie le contenu de la trame de Gestion. S'il reçoit n'importe quelle trame qui ne contient pas un IE MIC valide d'un identifiant d'ensemble des services de base (BSSID) qui appartient à un WAP, qui est configuré pour transmettre des trames MFP, il signale l'anomalie au système d'administration de réseaux.

  Remarque: Pour que les horodateurs fonctionnent correctement, tous les contrôleurs LAN Sans fil (WLC) doivent être Protocole NTP (Network Time Protocol) synchronisé.

- Enregistrement d'événement — Le Point d'accès informe le WLC quand il détecte une anomalie. WLC agrège les événements anormaux et les signale par des déroutements SNMP au gestionnaire de réseau.

6. Comment le client MFP travaille-t-il ?

Spécifiquement, le client MFP chiffre des trames de Gestion envoyées entre les clients de Points d'accès et de version 5 de Cisco Compatible Extension (CCXv5) de sorte que les Points d'accès et les clients puissent prendre une mesure préventive en relâchant les trames charriées de Gestion de la classe 3 (c'est-à-dire, trames de Gestion passées entre un Point d'accès et un client qui est authentifié et associé). Le client MFP accroît les mécanismes de sécurité définis par IEEE 802.11i pour protéger les types suivants de trames de Gestion d'unicast de la classe 3 : dissassociation, désauthentification, et action de QoS (multimédia Sans fil Extenions ou WMM). Le client MFP protège une session de point d'accès client contre le type le plus commun d'attaque par déni de service. Il protège des trames de Gestion de la classe 3 à l'aide de la même méthode de cryptage utilisée pour les trames de données de session. Si une trame reçue par le Point d'accès ou le client échoue déchiffrement, elle est lâchée, et l'événement est signalé au contrôleur.

7. Comment est-ce que j'utilise le client MFP ?

Pour utiliser le client MFP, les clients doivent prendre en charge CCXv5 MFP et doivent négocier la version 2 (WPA2) d'accès protégé par Wi-Fi utilisant le Protocole TKIP (Temporal Key Integrity Protocol) ou le code Protocol (AES-CCMP) d'authentification de message d'enchaînement de bloc de Standard-chiffrement de chiffrement avancé. Le Protocole EAP (Extensible Authentication Protocol) ou la clé pré-partagée (PSK) peut être utilisé pour obtenir le PMK. CCKM et gestion de la mobilité de contrôleur sont utilisés pour distribuer des clés de session entre les Points d'accès pour l'itinérance rapide de la couche 2 et de la couche 3.

8. Quels sont les composants du client MFP ?

Il y a 3 composants de client MFP :

- Génération de clés et distribution — Protocoles et mécanismes de Sécurité de leviers du client MFP définis par IEEE 802.11i pour protéger des trames de Gestion d'unicast de la classe 3 :

  – Trames de dissassociation — Une demande à un client ou à un WAP de déconnecter ou dissocier des relations d'authentification.

  – Trames de désauthentification — Une demande à un client ou à un WAP de déconnecter ou dissocier des relations d'association.

  – Action de QoS WMM — Le paramètre WMM est ajouté à la balise, à la réponse de sonde, et aux trames de réponse d'association.

- Protection et validation des trames de Gestion — Pour empêcher des attaques utilisant des trames d'émission, les aps qui prennent en charge CCXv5 n'émettent aucune trame de Gestion de la classe 3 d'émission. AP en mode de pont de groupe de travail, le mode répéteur, ou les écarts de mode de pont en non-racine annoncent des trames de Gestion de la classe 3 si le client MFP est activé.
- États d'erreur — Des mécanismes de l'enregistrement MFP-1 sont utilisés pour signaler des erreurs de De-encapsulation de trame de Gestion détectées par des Points d'accès. C'est-à-dire, le WLC collecte des statistiques sur les erreurs de validation MFP et des informations périodiquement en avant assemblées au WCS.

  Remarque: Des erreurs de violation MFP détectées par des stations client sont manipulées par l'itinérance CCXv5 et la caractéristique de diagnostics en temps réel.

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

Il y a certaines restrictions pour que quelques clients sans fil communiquent avec les périphériques d'infrastructure MFP-activés. MFP ajoute un long ensemble d'éléments d'information à chaque demande de sonde ou à balise SSID. Certains clients sans fil tels que des PDA, des smartphones, des scanners de code barre, et ainsi de suite ont limité la mémoire et l'unité centrale (CPU). Ainsi, vous ne pouvez pas traiter ces demandes ou balises. En conséquence, vous ne voyez pas le SSID entièrement, ou vous ne pouvez pas s'associer avec ces périphériques d'infrastructure, dus à un malentendu des capacités SSID. Cette question n'est pas spécifique à MFP. Ceci se produit également avec n'importe quel SSID qui a les plusieurs éléments d'information (IES). Il est toujours recommandé de tester le SSID MFP-activé sur l'environnement avec tous vos types disponibles de client avant que vous le déployiez en temps réel.

10. Quel est Management Frame Protection d'émission ?

Afin d'empêcher les attaques qui utilisent des trames d'émission, les aps qui les prennent en charge CCXv5 ne transmet aucune trame de Gestion de la classe 3 d'émission excepté la désauthentification escroc de retenue ou les trames de dissassociation. Les stations client CCXv5 capables doivent jeter des trames de Gestion de la classe 3 d'émission. On assume que des sessions MFP sont dans un réseau correctement sécurisé (authentification poussée plus le TKIP ou le CCMP) ainsi la négligence pour des émissions escrocs de retenue n'est pas une question.

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

Pour apprendre comment configurer MFP sur un WAP, a cliquez ici.

12. Comment configurer une carte réseau sans fil d'Intel pour se connecter à un réseau MFP-activé

Pour apprendre comment configurer la carte réseau sans fil d'Intel, a cliquez ici.