Häufig gestellte Fragen zum Management Frame Protection (MFP)

Ziel

Wi-Fi ist ein Übertragungsmedium, über das jedes Gerät als legitimes oder unberechtigtes Gerät abgehört und daran teilnimmt. Verwaltungs-Frames wie Authentifizierung, De-Authentifizierung, Zuordnung, Trennung, Beacons und Sonden werden von Wireless-Clients verwendet, um Sitzungen für Netzwerkservices zu initiieren und zu beenden. Im Gegensatz zum Datenverkehr, der verschlüsselt werden kann, um eine gewisse Vertraulichkeit zu gewährleisten, müssen diese Frames von allen Clients gehört und verstanden werden und müssen daher als offen oder unverschlüsselt übertragen werden. Diese Frames können zwar nicht verschlüsselt werden, müssen jedoch vor Fälschung geschützt werden, um das Wireless-Medium vor Angriffen zu schützen. Ein Angreifer könnte beispielsweise Verwaltungs-Frames von einem AP manipulieren, um einen Client anzugreifen, der dem AP zugeordnet ist.

Dieses Dokument soll Antworten auf häufig gestellte Fragen zum Management Frame Protection (MFP) liefern.

Häufig gestellte Fragen

Inhaltsverzeichnis

1. Was ist MFP?

Verwaltungs-Frames sind Broadcast-Frames, die von IEEE 802.11 verwendet werden, um einem Wireless-Client die Aushandlung mit einem Wireless Access Point (WAP) zu ermöglichen. MFP bietet Sicherheit für unverschlüsselte Broadcast-Frames und Managementnachrichten, die zwischen Wireless-Geräten übertragen werden.

2. Wie funktioniert MFP?

In IEEE 802.11 sind Management-Frames wie Dekodierung, Trennung, Beacons und

Sonden immer nicht authentifiziert und unverschlüsselt. Der WAP fügt jedem Management-Frame, den er überträgt, Message Integrity Check Information Element (MIC IE) hinzu. Bei jedem Versuch, den Frame zu kopieren, zu verändern oder erneut abzuspielen, wird die MIC ungültig.

1. Was kann ein Angreifer in einem Netzwerk mit deaktiviertem MFP tun?

- Die Schwachstelle in Management-Frames stellt eine große Bedrohung für ein Netzwerk dar, da ein Angreifer einen Management-Frame von einem WAP manipulieren kann, um einen Client anzugreifen, der diesem zugewiesen ist. Ein Angreifer kann folgende Aktionen durchführen:

- Denial of Service (DoS) ausführen - Angreifer verwenden Verschleierungstechniken außerhalb der typischen volumenbasierten Angriffe, um Erkennung und Eindämmung zu vermeiden, einschließlich "niedriger und langsamer" Angriffstechniken und SSL-basierten Angriffen. Sie implementieren Angriffskampagnen mit Multivability, die auf jede Ebene der Infrastruktur des Opfers abzielen, einschließlich Geräte, Firewalls, Server und Anwendungen in der Netzwerkinfrastruktur.
— Man-in-the-Middle-Angriff auf den Client bei erneuter Verbindung — Dies ist eine Form eines induktiven Key-Derivation-Angriffs, der in 802.11-Netzwerken wirksam ist, weil es an effektiver Nachrichtenintegrität mangelt. Der Empfänger eines Frames kann nicht überprüfen, ob der Frame während seiner Übertragung manipuliert wurde.

- Radiofrequenz-Hammer (RF) - Angriffe mit einer Hochleistungsantenne aus der Ferne können von außerhalb Ihres Bürogebäudes durchgeführt werden. Angriffstools, die von Eindringlingen verwendet werden, nutzen Hacking-Techniken wie gespoovierte 802.11-Management-Frames, gespoovierte 802.1x-Authentifizierungs-Frames oder einfach die Brute-Force-Methode zur Paketflutung.
- Evil Twin Router - Es ist eine Form des Phishing, bei der ein Angreifer einen legitimen Access Point benennt und darstellt. So werden Benutzer dazu veranlasst, ein Mobilgerät mit dem gefälschten Access Point zu verbinden, was dem Benutzer mehr Schaden zufügen kann.
- Ausführen eines Offline-Wörterbuchangriffs — Bei einem Wörterbuchangriff werden verschiedene Kennwörter verwendet, um die Authentifizierungsdaten des Benutzers zu kompromittieren. Die meisten kennwortbasierten Authentifizierungsalgorithmen sind anfällig für Wörterbuchangriffe, wenn keine strenge Kennwortrichtlinie vorliegt.

4. Welche MFP-Typen gibt es?

Dies sind die beiden MFP-Typen:

- Infrastruktur-MFP - Insbesondere Infrastruktur-MFP schützt 802.11-Sitzungsmanagement-Funktionen durch Hinzufügen von MIC IE zu den Management-Frames, die von Access Points ausgegeben werden, und nicht von Clients, die von anderen Access Points im Netzwerk validiert werden. Infrastruktur-MFP ist passiv. Sie kann Eindringlinge erkennen und melden, aber sie kann sie nicht aufhalten. Sie schützt Management-Frames durch die Erkennung von Angreifern, die Denial-of-Service-Angriffe auslösen, das Netzwerk mit Zuordnungsproben überfluten, als nicht autorisierte Access Points eingreifen und die Netzwerkleistung durch Angriffe auf QoS- und Funkmessrahmen beeinträchtigen.
- Client MFP - Schirmt authentifizierte Clients vor gefälschten Frames und verhindert so, dass viele häufige Angriffe auf die Wireless Local Area Networks (LANs) wirksam werden. Die meisten Angriffe, wie z. B. Deauthentifizierungs-Angriffe, kehren zu einer schlicht

herabgesetzten Leistung zurück, indem sie mit gültigen Clients konkurrieren.

5. Welche Komponenten umfasst das Infrastruktur-MFP?

Das Infrastruktur-MFP besteht aus drei Komponenten:

- Management Frame Protection - Wenn der Management Frame Protection aktiviert ist, fügt der WAP jedem Management-Frame, den er überträgt, MIC IE hinzu. Bei jedem Versuch, den Frame zu kopieren, zu verändern oder erneut abzuspielen, wird die MIC ungültig.
- Management Frame Validation - Wenn die Management Frame-Validierung aktiviert ist, validiert der AP jeden Management-Frame, den er von anderen WAPs im Netzwerk empfängt. Es stellt sicher, dass der MIC IE vorhanden ist (wenn der Ausgangspunkt für die Übertragung von MFP-Frames konfiguriert ist) und den Inhalt des Management-Frames abstimmt. Wenn ein Frame, der keinen gültigen MIC IE enthält, von einem Basic Service Set Identifier (BSSID) empfangen wird, der zu einem WAP gehört, der für die Übertragung von MFP-Frames konfiguriert ist, meldet er die Diskrepanz an das Netzwerkmanagementsystem.

  Hinweis: Damit die Zeitstempel ordnungsgemäß funktionieren, müssen alle Wireless LAN Controller (WLC) mit dem Network Time Protocol (NTP) synchronisiert werden.

- Ereignisberichte - Der Access Point benachrichtigt den WLC, wenn er eine Anomalie erkennt. WLC aggregiert die ungewöhnlichen Ereignisse und meldet diese über SNMP-Traps an den Netzwerkmanager.

6. Wie funktioniert Client MFP?

Client-MFP verschlüsselt Verwaltungs-Frames, die zwischen Access Points und Cisco Compatible Extension Version 5 (CCXv5)-Clients gesendet werden, sodass sowohl Access Points als auch Clients vorbeugende Maßnahmen ergreifen können, indem sie gefälschte Management-Frames der Klasse 3 (d. h. Management-Frames, die zwischen einem Access Point und einem authentifizierten und zugeordneten Client übergeben werden) verwerfen. Client MFP nutzt die von IEEE 802.11i definierten Sicherheitsmechanismen, um die folgenden Typen von Unicast-Management-Frames der Klasse 3 zu schützen: Trennung, Entauthentifizierung und QoS (Wireless Multimedia Extensions oder WMM)-Aktion. Client MFP schützt eine Client-Access Point-Sitzung vor den häufigsten Denial-of-Service-Angriffen. Sie schützt Management-Frames der Klasse 3, indem sie dieselbe Verschlüsselungsmethode verwendet, die auch für die Sitzungsdaten-Frames verwendet wird. Wenn ein vom Access Point oder Client empfangener Frame nicht entschlüsselt werden kann, wird er verworfen, und das Ereignis wird an den Controller gemeldet.

7. Wie verwende ich Client MFP?

Zur Verwendung von Client-MFP müssen Clients CCXv5 MFP unterstützen und entweder über das Temporal Key Integrity Protocol (TKIP) oder das Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) die Wi-Fi Protected Access Version 2 (WPA2) aushandeln. Der PMK kann über Extensible Authentication Protocol (EAP) oder Pre-Shared Key (PSK) bezogen werden. Das CCKM- und das Controller-Mobilitätsmanagement dienen zur Verteilung von Sitzungsschlüsseln zwischen Access Points für schnelles Layer-2- und Layer-3-Roaming.

8. Wassind die Komponenten von Client MFP?

Es gibt drei Komponenten von Client MFP:

- Schlüsselgenerierung und -verteilung - Client MFP nutzt Sicherheitsprotokolle und -mechanismen, die durch IEEE 802.11i definiert sind, um Unicast-Management-Frames der Klasse 3 zu schützen:

    - Trennrahmen - Eine Anforderung an einen Client oder WAP, eine Authentifizierungsbeziehung zu trennen oder zu trennen.

    - De-Authentication-Frames - Eine Anforderung an einen Client oder WAP, eine Beziehung zu trennen oder zu trennen.

    - QoS-WMM-Aktion - Der WMM-Parameter wird dem Beacon-, Sonde-Antwort- und Assoziations-Response-Frames hinzugefügt.

- Schutz und Validierung von Management-Frames: Um Angriffe mit Broadcast-Frames zu verhindern, geben APs, die CCXv5 unterstützen, keine Broadcast Class 3-Management-Frames aus. Ein AP im Arbeitsgruppen-Bridge-Modus, Repeater-Modus oder Nicht-Root-Bridge-Modus verwirft Management-Frames der Broadcast-Klasse 3, wenn Client MFP aktiviert ist.
- Fehlerberichte - MFP-1-Reporting-Mechanismen werden verwendet, um von Access Points erkannte Fehler bei der Entkapselung von Verwaltungsrahmen zu melden. Das heißt, der WLC sammelt Statistiken zu Fehlern bei der MFP-Validierung und leitet die erfassten Informationen regelmäßig an das WCS weiter.

    Hinweis: Von Client-Stationen erkannte MFP-Fehler werden von der CCXv5-Funktion für Roaming und Echtzeit-Diagnose behandelt.

9. Warum kann mein Mobilgerät nicht mit dem MFP-fähigen Infrastrukturgerät verbunden werden?

Einige Wireless-Clients können nur mit MFP-fähigen Infrastrukturgeräten kommunizieren. MFP fügt jeder Anfrage oder jedem SSID-Beacon eine Reihe von Informationselementen hinzu. Einige Wireless-Clients wie PDAs, Smartphones, Barcode-Scanner usw. verfügen über eingeschränkten Arbeitsspeicher und eine Central Processing Unit (CPU). Sie können diese Anfragen oder Beacons also nicht verarbeiten. Infolgedessen wird die SSID nicht vollständig angezeigt, oder Sie können aufgrund eines Missverständnisses der SSID-Funktionen keine Verbindung zu diesen Infrastrukturgeräten herstellen. Dieses Problem betrifft nicht nur den MFP. Dies gilt auch für alle SSIDs mit mehreren Informationselementen (IEs). Es ist immer ratsam, MFP-fähige SSIDs in der Umgebung mit allen verfügbaren Clienttypen zu testen, bevor Sie sie in Echtzeit bereitstellen.

10. Was ist Broadcast Management Frame Protection?

Um Angriffe zu verhindern, die Broadcast-Frames verwenden, senden Access Points, die CCXv5 unterstützen, keine Broadcast Class 3-Management-Frames außer bei der Deauthentifizierung von nicht autorisierten Containment-Elementen oder der Trennung von Frames. CCXv5-fähige Client-Stationen müssen Management-Frames der Broadcast-Klasse 3 verwerfen. MFP-Sitzungen werden als in einem ordnungsgemäß gesicherten Netzwerk (starke Authentifizierung plus TKIP oder CCMP) angesehen, sodass die Nichtbeachtung von nicht autorisierten Containment-Broadcasts kein Problem darstellt.

11. Wie wird MFP auf einem Wireless Access Point (WAP) konfiguriert?

Um zu erfahren, wie MFP auf einem WAP konfiguriert wird, klicken Sie hier.

12. Konfigurieren einer Intel Wireless-Netzwerkkarte für die Verbindung mit einem MFP-fähigen Netzwerk

Um zu erfahren, wie Sie die Intel Wireless-Netzwerkkarte konfigurieren, klicken Sie hier.