管理フレーム保護(MFP)に関するFAQ

目的

Wi-Fiは、任意のデバイスが傍受し、正当なデバイスまたは不正なデバイスとして参加できるようにするブロードキャストメディアです。認証、認証解除、関連付け解除、解離、ビーコン、プローブなどの管理フレームは、ワイヤレスクライアントがネットワークサービスのセッションを開始および切断するために使用します。データトラフィックは暗号化して機密性のレベルを提供できますが、これらのフレームはすべてのクライアントで受信および認識される必要があるため、オープンまたは非暗号化として送信される必要があります。これらのフレームは暗号化できませんが、攻撃からワイヤレスメディアを保護するために、偽造から保護する必要があります。たとえば、攻撃者がAPから管理フレームをスプーフィングして、APに関連付けられたクライアントを攻撃する可能性があります。

このドキュメントでは、Management Frame Protection（MFP；管理フレーム保護）に関するよくある質問(FAQ)に回答することを目的としています。

よく寄せられる質問（FAQ）

目次

1.このメッセージは何を is MFP?

管理フレームは、ワイヤレスクライアントがワイヤレスアクセスポイント(WAP)とネゴシエートできるようにIEEE 802.11で使用されるブロードキャストフレームです。MFPは、ワイヤレスデバイス間で渡される暗号化されていないブロードキャストフレームと管理メッセージに対するセキュリティを提供します。

2. MFPの仕組み

IEEE 802.11では、認証の解除、アソシエーション解除、ビーコン、プローブなどの管理フレームは、常に非認証および非暗号化です。WAPは、送信する各管理フレームにMessage Integrity Check Information Element(MIC IE)を追加します。フレームのコピー、変更、または再生を試みると、MIC が無効となります。

3.MFPが無効になっているネットワークで攻撃者が実行できるものは何ですか。

- 管理フレームに存在する脆弱性は、攻撃者がWAPから管理フレームをスプーフィングして、それに関連付けられているクライアントを攻撃できるようにすることで、ネットワークに大きな脅威をもたらします。攻撃者は次のアクションを実行できます。

– サービス拒否(DoS)の実行：攻撃者は、一般的なボリュームベースの攻撃以外の回避技術を使用して、「低および遅い」攻撃手法やSSLベースの攻撃などの検出と緩和を回避しています。ネットワークインフラストラクチャデバイス、ファイアウォール、サーバ、アプリケーションを含む、攻撃対象のインフラストラクチャのすべてのレイヤを対象とするマルチベンダーアラービリティ攻撃キャンペーンを展開しています。
– 再接続時のクライアントに対する中間者攻撃 – これは、効果的なメッセージ整合性の欠如のために802.11ネットワークで有効な誘導鍵導出攻撃の一種です。フレームのレシーバは、フレームが送信中に改ざんされていないことを確認できません。

- Radio Frequency（RF；無線周波数）妨害装置：距離からの高出力指向性アンテナを使用した攻撃は、オフィスビルの外部から実行できます。侵入者が使用する攻撃ツールは、スプーフィングされた802.11管理フレーム、スプーフィングされた802.1x認証フレーム、またはブルートフォースパケットフラッディング方式を使用したハッキング技術を活用します。
- Evil Twinルータ：攻撃者が正当なアクセスポイントとして名前を付け、ポーズを付けるフィッシングの一種です。これにより、ユーザは偽のアクセスポイントにモバイルデバイスを接続して、ユーザに害を及ぼすことができます。
- オフライン辞書攻撃の実行：辞書攻撃では、パスワードのバリエーションを使用して、ユーザの認証クレデンシャルを侵害します。ほとんどのパスワードベースの認証アルゴリズムは、強力なパスワードポリシーがない場合に辞書攻撃に対して脆弱です。

4.MFPのタイプは何ですか。

MFPには次の2つのタイプがあります。

- インフラストラクチャMFP：特に、インフラストラクチャMFPは、ネットワーク内の他のアクセスポイントによって検証されるクライアントから送信される管理フレームではなく、アクセスポイントから送信される管理フレームにMIC IEを追加することで、802.11セッション管理機能を保護します。インフラストラクチャMFPはパッシブです。侵入を検出して報告することはできますが、阻止する手段はありません。Denial of Service（DoS；サービス拒否攻撃）を実行している攻撃者を検出し、アソシエーションプローブを使用してネットワークをフラッディングし、不正なアクセスポイントとして干渉し、Quality of Service(QoS)および無線測定フレームを攻撃してネットワークパフォーマンスに影響します。
- クライアントMFP：認証されたクライアントをスプーフィングされたフレームから保護し、無線ローカルエリアネットワーク(LAN)に対する一般的な攻撃の多くが有効にならないようにします。認証解除攻撃など、ほとんどの攻撃は、有効なクライアントと競合することで、単にパフォーマンスを低下させるだけになります。

5.インフラストラクチャMFPのコンポーネントは何ですか。

インフラストラクチャMFPには3つのコンポーネントがあります。

- 管理フレーム保護：管理フレーム保護が有効な場合、WAPは送信する各管理フレームにMIC IEを追加します。フレームのコピー、変更、または再生を試みると、MIC が無効となります。
- 管理フレーム検証：管理フレーム検証が有効な場合、APはネットワーク内の他のWAPから受信したすべての管理フレームを検証します。これにより、MIC IE が存在していて（発信側がMFP フレームを送信するよう設定されている場合）、管理フレームの中身が一致しているこ

とが確認されます。MFPフレームを送信するように設定されたWAPに属するBasic Service Set Identifier(BSSID)から、有効なMIC IEを含まないフレームを受信すると、その不一致がネットワーク管理システムに報告されます。

> **注：タイムスタ**ンプが正しく動作するためには、すべてのワイヤレスLANコントローラ(WLC)がネットワークタイムプロトコル(NTP)同期されている必要があります。

- イベントレポート：アクセスポイントは、異常を検出するとWLCに通知します。WLC は異常イベントを集積して、SNMP トラップ経由でそれをネットワーク管理者に報告します。

6.クライアントMFPはどのように動作しますか。

具体的には、クライアントMFPはアクセスポイントとCisco Compatible Extension Version 5(CCXv5)クライアント間で送信される管理フレームを暗号化し、スプーフィングされたクラス3管理フレーム（認証および関連付けられたアクセスポイントとクライアント間で渡された管理フレーム）を廃棄します。 クライアントMFPは、IEEE 802.11iで定義されたセキュリティメカニズムを利用して、次のタイプのクラス3ユニキャスト管理フレームを保護します。関連付け解除、認証解除、およびQoS(Wireless Multimedia Extension(WMM)アクション)クライアントMFPは、最も一般的なタイプのサービス拒否攻撃からクライアントアクセスポイントセッションを保護します。セッションデータフレームに使用したのと同じ暗号化方式を使用して、クラス3管理フレームを保護します。アクセス ポイントやクライアントで受信されるフレームを復号化できない場合、フレームは廃棄され、このイベントがコントローラに報告されます。

7.クライアントMFPを使用するにはどうすればよいですか。

クライアントMFPを使用するには、クライアントがCCXv5 MFPをサポートし、Temporal Key Integrity Protocol(TKIP)またはAdvanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol(AES-CCMP)を使用してWi-Fi Protected Accessバージョン2(WPA2)をととのとのとのネゴシエーションをををします。 PMKの取得には、Extensible Authentication Protocol(EAP)または事前共有キー(PSK)を使用できます。CCKMとコントローラモビリティ管理は、レイヤ2とレイヤ3の高速ローミング用にアクセスポイント間でセッションキーを配布するために使用されます。

8.What aクライアントMFPのコンポーネントですか。

クライアントMFPには3つのコンポーネントがあります。

- キーの生成と配布：クライアントMFPは、IEEE 802.11iで定義されたセキュリティプロトコルとメカニズムを利用して、クラス3ユニキャスト管理フレームを保護します。

  – 関連付け解除フレーム：クライアントまたはWAPに対する、認証関係の切断または関連付け解除の要求。

  – 認証解除フレーム：クライアントまたはWAPに対する、アソシエーション関係の切断または関連付け解除の要求。

  - QoS WMMアクション：WMMパラメータが、ビーコン、プローブ応答、および関連付け応答フレームに追加されます。

- 管理フレームの保護と検証：ブロードキャストフレームを使用した攻撃を防止するために、CCXv5をサポートするAPはブロードキャストクラス3管理フレームを送信しません。ワークグループブリッジモード、リピータモード、または非ルートブリッジモードのAPは、クライアントMFPが有効な場合、ブロードキャストクラス3管理フレームを廃棄します。

- エラーレポート：MFP-1レポートメカニズムは、アクセスポイントによって検出された管理フレームのカプセル化解除エラーをレポートするために使用されます。つまり、WLC は MFP 検証エラー統計情報を収集し、定期的に照合情報を WCS に転送します。

  注：クライアントステーションで検出されたMFP違反エラーは、CCXv5ローミングおよびリアルタイム診断機能で処理されます。

9.モバイルデバイスがMFP対応インフラストラクチャデバイスに接続できないのはなぜですか。

一部のワイヤレス クライアントが MFP 対応インフラストラクチャ デバイスと通信する場合には、一部制限があります。MFP により、各プローブ要求または SSID ビーコンには、一連の長い情報要素が付加されます。PDA、スマートフォン、バーコードスキャナなどの一部のワイヤレスクライアントには、メモリと中央処理装置(CPU)が限られています。 したがって、これらの要求やビーコンを処理することはできません。その結果、SSID機能が正しく認識されないか、SSID機能が誤解されているため、これらのインフラストラクチャデバイスに関連付けることができません。この問題は MFP に特有なものではありません。これは、複数の Information Element (IE; 情報要素) を含むすべての SSID でも発生します。 リアルタイムで展開する前に、使用可能なすべてのクライアントタイプを使用して環境でMFP対応SSIDをテストすることをお勧めします。

10. ブロードキャスト管理フレーム保護とは何ですか。

ブロードキャストフレームを使用する攻撃を防ぐために、CCXv5をサポートするAPは、不正な抑止の認証解除フレームまたは関連付け解除フレームを除き、ブロードキャストクラス3管理フレームを送信しません。CCXv5 対応クライアント ステーションは、ブロードキャスト クラス 3 管理フレームを廃棄する必要があります。MFP セッションは適切にセキュリティ保護されたネットワーク (強力な認証と TKIP または CCMP) 内にあると想定されているため、不正 AP 抑止ブロードキャストを無視しても問題にはなりません。

11 . ワイヤレスアクセスポイント(WAP)でMFPを設定する方法

WAPでMFPを設定する方法については、ここをクリックしてください。

12. MFP対応ネットワークに接続するためのインテルワイヤレスネットワークカードの設定方法

インテル・ワイヤレス・ネットワーク・カードの設定方法については、ここをクリックしてください。