有關管理幀保護(MFP)的常見問題

目標

Wi-Fi是一種廣播媒體，可讓任何裝置以合法或欺詐裝置的身份進行竊聽和參與。無線客戶端使用管理幀（例如身份驗證、解除身份驗證、關聯、分離、信標和探測）來啟動和斷開網路服務的會話。與可以加密以提供一定保密級別的資料流量不同，這些幀必須被所有客戶端偵聽和理解，因此必須以打開或未加密的形式傳輸。雖然這些幀不能加密，但必須防止偽造，以保護無線介質免受攻擊。例如，攻擊者可以偽裝來自AP的管理幀，以攻擊與AP關聯的客戶端。

本文檔旨在提供有關管理幀保護(MFP)的常見問題的解答。

常見問題

目錄

1.什麼 是 MFP？

管理幀是IEEE 802.11使用的廣播幀，用於允許無線客戶端與無線存取點(WAP)協商。MFP為無線裝置之間傳遞的未加密廣播幀和管理消息提供安全性。

2. MFP如何工作？

在IEEE 802.11中，管理幀（如解除身份驗證、解除關聯、信標和探測）始終未經驗證和加密

。WAP將消息完整性檢查資訊元素(MIC IE)增加到其傳輸的每個管理幀。任何複製、更改或重播幀的嘗試都會使MIC失效。

3.在停用MFP的網路中，攻擊者可以做哪些事情？

- 在管理幀中發現的漏洞對網路構成巨大威脅，因為攻擊者能夠欺騙來自WAP的管理幀，攻擊與其相關聯的客戶端。攻擊者可以執行以下操作：

  — 運行拒絕服務(DoS) -攻擊者使用規避技術（在典型的基於卷的攻擊之外）來避免檢測和緩解，包括「低和慢」攻擊技術和基於SSL的攻擊。他們正在部署多漏洞攻擊活動，針對受害者基礎設施的每一層，包括網路基礎設施裝置、防火牆、伺服器和應用。
  — 重新連線時客戶端上的中間人攻擊—這是一種誘導式金鑰派生攻擊，在802.11網路中因缺乏有效的消息完整性而有效。幀的接收方無法驗證幀在傳輸過程中是否被篡改。

- 射頻(RF)干擾器-從遠處使用高功率定向天線的攻擊可從商辦大樓外部進行。入侵者使用的攻擊工具利用駭客技術，例如假冒的802.11管理幀、假冒的802.1x身份驗證幀，或者僅使用暴力資料包泛洪方法。
- Evil Twin Router —這是一種網路釣魚形式，攻擊者將其命名並偽裝成合法存取點。這誘使使用者將流動裝置連線到假存取點，從而能夠對使用者造成更多傷害。
- 執行離線詞典攻擊—在詞典攻擊期間，會使用各種密碼來危害使用者的認證認證。大多數基於密碼的身份驗證演算法都容易受到詞典攻擊，因為缺少強密碼策略。

4.MFP有哪些型別？

MFP有兩種型別：

- 基礎架構MFP -具體來說，基礎架構MFP可保護802.11會話管理功能，方法是將MIC IE增加到由存取點而不是客戶端發出的管理幀（這些幀由網路中的其他存取點驗證）。基礎架構MFP是被動的。它可以檢測到並報告入侵，但無法阻止入侵。它透過檢測正在呼叫拒絕服務攻擊、使用關聯探測泛洪網路、作為惡意存取點插入以及透過攻擊服務品質(QoS)和無線電測量幀影響網路效能的攻擊者來保護管理幀。
- 客戶端MFP -保護經過身份驗證的客戶端免受欺騙幀，從而防止許多針對無線區域網(LAN)的常見攻擊生效。大多數攻擊（如去身份驗證攻擊）會透過與有效客戶端競爭而恢復為僅降低效能。

5.基礎設施MFP有哪些元件？

基礎架構MFP包含3個元件：

- 管理幀保護-當啟用管理幀保護時，WAP會將MIC IE增加到其傳輸的每個管理幀。任何複製、更改或重播幀的嘗試都會使MIC失效。
- 管理幀驗證-當啟用管理幀驗證時，AP驗證其從網路中其他WAP接收的每個管理幀。它確保MIC IE存在（當發起方被配置為傳輸MFP幀時），並且匹配管理幀的內容。如果從

屬於配置為傳輸MFP幀的WAP的基本服務集識別符號(BSSID)收到任何不包含有效MIC IE的幀，它會將差異報告給網路管理系統。

注意：為了讓時間戳能夠正常運行，所有無線LAN控制器(WLC)都必須與網路時間協定(NTP)同步。

- 事件報告-當檢測到異常情況時，存取點通知WLC。WLC會聚總異常事件，並透過SNMP設陷向網路管理員報告。

6.客戶端MFP如何工作？

具體而言，客戶端MFP對存取點和Cisco Compatible Extension版本5 (CCXv5)客戶端之間傳送的管理幀進行加密，以便存取點和客戶端都可以透過丟棄欺騙的第3類管理幀（即，在存取點與經過身份驗證和關聯的客戶端之間傳遞的管理幀）採取預防措施。客戶端MFP利用IEEE 802.11i定義的安全機制保護以下型別的3類單播管理幀：取消關聯、取消身份驗證和QoS（無線多媒體擴展或WMM）操作。客戶端MFP可保護客戶端-存取點會話免受最常見的拒絕服務攻擊。它透過使用用於會話資料幀的相同加密方法來保護第3類管理幀。如果存取點或客戶端收到的幀解密失敗，則會丟棄該幀，並向控制器報告事件。

7.如何使用客戶端MFP？

若要使用使用者端MFP，使用者端必須支援CCXv5 MFP，且必須使用暫時金鑰整合通訊協定(TKIP)或進階加密標準密碼區塊鏈結訊息驗證碼通訊協定(AES-CCMP)交涉Wi-Fi保護存取第2版(WPA2)。可延伸驗證通訊協定(EAP)或預先共用金鑰(PSK)可用於取得PMK。CCKM和控制器移動性管理用於在存取點之間分配會話金鑰，以實現第2層和第3層快速漫遊。

8.什麼是客戶端MFP的元件嗎？

客戶端MFP有3個元件：

- 金鑰生成和分發-客戶端MFP利用IEEE 802.11i定義的安全協定和機制來保護第3類單播管理幀：

  - 取消關聯幀—請求客戶端或WAP斷開或取消關聯身份驗證關係。

  - 取消驗證幀—請求客戶端或WAP斷開或取消關聯關係。

  - QoS WMM操作- WMM引數增加到信標、探測響應和關聯響應幀。

- 管理幀的保護和驗證-為了防止使用廣播幀的攻擊，支援CCXv5的AP不會發出任何廣播

第3類管理幀。如果啟用了客戶端MFP，處於工作組橋模式、中繼器模式或非根橋模式的AP將丟棄廣播第3類管理幀。

- 錯誤報告— MFP-1報告機制用於報告存取點檢測到的管理幀解封裝錯誤。也就是說，WLC收集MFP驗證錯誤統計資訊，並定期將整理的資訊轉發到WCS。

註：客戶端站點檢測到的MFP違規錯誤由CCXv5漫遊和即時診斷功能處理。

9. 為什麼我的流動裝置無法連線到支援MFP的基礎設施裝置？

某些無線客戶端與啟用了MFP的基礎設施裝置通訊存在某些限制。MFP向每個探測請求或SSID信標增加了一組長資訊元素。某些無線客戶端（例如PDA、智慧型手機、條形碼掃描器等）的記憶體和中央處理器(CPU)有限。因此，您無法處理這些請求或信標。因此，由於對SSID功能的誤解，您無法完全看到SSID，或者無法與這些基礎設施裝置關聯。此問題並非特定於MFP。具有多個資訊元素(IE)的任何SSID也會出現這種情況。在您即時部署之前，始終建議使用所有可用的客戶端型別測試環境中啟用MFP的SSID。

10. 什麼是廣播管理幀保護？

為了防止使用廣播幀的攻擊，支援CCXv5的AP不會傳輸任何廣播第3類管理幀，但欺詐遏製取消身份驗證或取消關聯幀除外。支援CCXv5的使用者端站台必須捨棄廣播第3類管理訊框。假設MFP會話位於適當安全的網路中（強身份驗證加上TKIP或CCMP），因此忽略惡意遏制廣播不是問題。

11. 如何在無線存取點(WAP)上配置MFP？

要瞭解如何在WAP上配置MFP，請點選這裡。

12. 如何設定Intel無線網路卡以連線到啟用MFP的網路

要瞭解如何配置Intel無線網絡卡，請點選這裡。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。