有關管理幀保護(MFP)的常見問題

目標

Wi-Fi是一種廣播介質，允許任何裝置作為合法裝置或欺詐裝置竊聽和參與。無線客戶端使用管理幀（如身份驗證、取消身份驗證、關聯、分離、信標和探測）來啟動和中斷網路服務的會話。與可以加密以提供一定保密級別的資料流量不同，所有客戶端都必須聽到並理解這些幀，因此，必須以開啟或未加密方式傳輸這些幀。雖然這些幀無法加密，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)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接入點(WAP)協商。MFP為無線裝置之間傳輸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（例如取消驗證、解除關聯、信標和探測）始終未經驗證且未加密。WAP將消息完整性檢查資訊元素(MIC IE)新增到它傳送的每個管理幀。任何複製、更改或重播幀的嘗試都會使MIC失效。

3.在禁用MFP的網路上，攻擊者可以做哪些事情？

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

— 運行拒絕服務(DoS) — 攻擊者使用逃避技術，而不是典型的基於卷的攻擊，以避免檢測和緩解，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 — 這是一種歸納金鑰派生攻擊的形式，在802.11網路中因缺少有效的消息完整性而有效。幀的接收器無法驗證幀在傳輸期間是否未被篡改。

- 射頻(RF)干擾器 — 距離遠處使用大功率定向天線的攻擊可以在辦公大樓外進行。入侵者使用的攻擊工具利用駭客技術，例如偽裝的802.11管理幀、偽裝的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接入點。這誘使使用者將流動裝置連線到假接入點，從而能夠對使用者造成更大的傷害。
- 運行離線字典攻擊 — 在字典攻擊期間，密碼的變體用於危害使用者的身份驗證憑據。在沒有強密碼策略的情況下，大多數基於密碼的身份驗證演算法容易受到字典攻擊。

4.MFP是什麼型別？

以下為兩種MFP:

- 基礎架構MFP — 具體來說，基礎架構MFP通過將MIC IE新增到由接入點發出而不是由客戶端發出的、由網路中的其他接入點驗證的管理幀來保護802.11會話管理功能。基礎架構MFP是被動的。它可以檢測並報告入侵，但無法阻止入侵。它通過檢測正在呼叫拒絕服務攻擊、使用關聯探測器泛洪網路、作為惡意接入點進行插入，以及通過攻擊服務品質(QoS)和無線電測量幀來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偽裝幀，防止對無線區域網(LAN)的許多常見攻擊生效。大多數攻擊（如去驗證攻擊）會通過與有效客戶端競爭而恢復為僅降低效能。

5.基礎架構MFP有哪些元件？

基礎設施MFP有3個元件：

- 管理幀保護 — 當啟用管理幀保護時，WAP會將MIC IE新增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 — 啟用管理幀驗證後，AP將驗證從網路中的其他WAP收到的每個管理幀。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。如果它從屬於WAP（配置為傳輸MFP幀）的基本服務集識別符號(BSSID)接收到不包含有效MIC IE的任何幀，則會向網路管理系統報告差異。

  注意：為使時間戳正常運行，所有無線LAN控制器(WLC)都必須同步網路時間協定(NTP)。

- 事件報告 — 接入點檢測到異常時通知WLC。WLC聚合異常事件並通過SNMP陷阱將其報告給網路管理器。

6.客戶端MFP如何工作？

具體而言，客戶端MFP對接入點和Cisco Compatible Extension v5(CCXv5)客戶端之間傳送的管理幀進行加密，以便接入點和客戶端都可以通過丟棄偽裝的第3類管理幀（即，在接入點和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：解除關聯、解除驗證和QoS（無線多媒體擴展或WMM）操作。客戶端MFP可保護客戶端接入點會話免受最常見的拒絕服務攻擊。它通過使用與會話資料幀相同的加密方法來保護第3類管理幀。如果接入點或客戶端接收的幀解密失敗，則會丟棄該幀，並向控制器報告該事件。

7.如何使用客戶端MFP?

要使用客戶端MFP，客戶端必須支援CCXv5 MFP並且必須使用臨時金鑰完整性協定(TKIP)或高級加密標準密碼塊連結消息驗證代碼協定(AES-CCMP)協商Wi-Fi保護訪問版本2(WPA2)。可擴展身份驗證協定(EAP)或預共用金鑰(PSK)可用於獲取PMK。CCKM和控制器移動性管理用於在第2層和第3層快速漫遊的接入點之間分配會話金鑰。

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。

  — 取消身份驗證幀 — 請求客戶端或WAP斷開或取消關聯關係。

  - QoS WMM操作 — WMM引數新增到信標、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不會發出任何廣播類3管理幀。如果啟用了客戶端MFP，則處於工作組網橋模式、中繼器模式或非根網橋模式的AP會放棄廣播第3類管理幀。
- 錯誤報告 — MFP-1報告機制用於報告接入點檢測到的管理幀解封裝錯誤。即，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。

附註：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啟用了MFP的基礎設施裝置？

某些無線客戶端與支援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信標新增一組長資訊元素。某些無線客戶端（例如PDA、智慧手機、條形碼掃描器等）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，您完全看不到SSID，或者由於對SSID功能的誤解而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。 在即時部署之前，建議使用所有可用的客戶端型別在環境中測試啟用了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（欺詐遏製取消身份驗證或取消關聯幀除外）。支援CCXv5的客戶端站點必須丟棄廣播第3類管理幀。假設MFP會話位於正確保護的網路中（強身份驗證加上TKIP或CCMP），因此忽略惡意遏制廣播不會造成問題。

11. 如何在無線接入點(WAP)上配置MFP?

若要瞭解如何在WAP上配置MFP，請按一下此處。

12.如何配置英特爾無線網絡卡以連線到支援MFP的網路

要瞭解如何配置英特爾無線網絡卡，請按一下此處。