有关管理帧保护(MFP)的常见问题

目标

Wi-Fi是一种广播介质，它使任何设备都能够作为合法或欺诈设备窃听和参与。无线客户端使用诸如身份验证、解除身份验证、关联、解离、信标和探测等管理帧来发起和断开网络服务的会话。与可加密以提供一定机密性的数据流量不同，所有客户端都必须听到和理解这些帧，因此必须以开放或未加密的形式传输。虽然这些帧无法加密，但必须保护它们不被伪造，以保护无线介质免受攻击。例如，攻击者可能欺骗来自AP的管理帧，以攻击与AP关联的客户端。

本文档旨在解答有关管理帧保护(MFP)的常见问题。

常见问题

目录

1。什么 is MFP?

管理帧是IEEE 802.11使用的广播帧，用于允许无线客户端与无线接入点(WAP)协商。MFP为未加密的广播帧和无线设备之间传递的管理消息提供安全性。

2. MFP如何工作？

在IEEE 802.11中，取消身份验证、取消关联、信标和探测等管理帧始终未经身份验证且未加密。WAP会将消息完整性检查信息元素(MIC IE)添加到它传输的每个管理帧。任何试图复制、修改或者重播帧的操作均使 MIC 无效。

3。在禁用MFP的网络中，攻击者可以执行哪些操作？

- 在管理帧中发现的漏洞会使攻击者欺骗来自WAP的管理帧，攻击与其关联的客户端，从而对网络构成巨大威胁。攻击者可能会执行以下操作：

— 运行拒绝服务(DoS) — 攻击者在典型的基于卷的攻击之外使用规避技术来避免检测和缓解，包括“低速”攻击技术和基于SSL的攻击。他们正在部署针对受害者基础设施的每一层的多漏洞攻击活动，包括网络基础设施设备、防火墙、服务器和应用。

— 重新连接时对客户端的中间人攻击 — 这是一种感应密钥派生攻击的形式，由于缺少有效的消息完整性，在802.11网络中有效。帧的接收方无法验证帧在传输过程中是否未被篡改。

- 射频(RF)干扰器 — 使用距离较远的大功率定向天线可以从办公楼外部发起攻击。入侵者使用的攻击工具利用欺骗性802.11管理帧、欺骗性802.1x身份验证帧等黑客技术，或仅使用暴力数据包泛洪方法。
- 恶性双路由器 — 这是一种网络钓鱼形式，攻击者在其中命名并伪装成合法接入点。这诱使用户将移动设备连接到假接入点，从而能够对用户造成更大的伤害。
- 运行脱机字典攻击 — 在字典攻击期间，密码的变体用于危害用户的身份验证凭证。大多数基于密码的身份验证算法在缺乏强密码策略的情况下容易受到字典攻击。

4。MFP的类型是什么？

以下是两种MFP:

- 基础设施MFP — 具体而言，基础设施MFP通过将MIC IE添加到接入点发出的管理帧而不是客户端发出的管理帧中来保护802.11会话管理功能，客户端发出的管理帧由网络中的其他接入点验证。基础设施MFP是被动的。它可以检测和报告入侵，但无法阻止入侵。它通过检测调用拒绝服务攻击、使用关联探测功能泛洪网络、作为欺诈接入点进行干扰以及通过攻击服务质量(QoS)和无线电测量帧影响网络性能的攻击者来保护管理帧。
- 客户端MFP — 屏蔽经过身份验证的客户端与欺骗的帧，防止针对无线局域网(LAN)的许多常见攻击变得有效。大多数攻击（例如取消身份验证攻击）都会通过与有效客户端竞争而恢复为仅仅降低性能。

5。基础设施MFP有哪些组件？

基础设施MFP有3个组件：

- 管理帧保护 — 启用管理帧保护后，WAP会将MIC IE添加到其传输的每个管理帧。任何试图复制、修改或者重播帧的操作均使 MIC 无效。
- 管理帧验证 — 启用管理帧验证后，AP会验证从网络中的其他WAP接收的每个管理帧。这确保 MIC IE 存在（当配置发送方来传输 MFP 帧时）并与管理帧的内容匹配。如果它从属于WAP的基本服务集标识符(BSSID)接收到任何不包含有效MIC IE的帧，并配置为传输MFP帧，它会向网络管理系统报告差异。

  > **注：为**了使时间戳正常运行，所有无线局域网控制器(WLC)必须同步网络时间协议(NTP)。

- 事件报告 — 当检测到异常情况时，接入点通知 WLC。WLC 聚集了异常事件并通过 SNMP 陷阱向网络管理器报告。

6。客户端MFP如何工作？

具体而言，客户端MFP会加密接入点和思科兼容扩展版本5(CCXv5)客户端之间发送的管理帧，以便接入点和客户端都可以通过丢弃虚假的第3类管理帧（即，在接入点和经过身份验证和关联的客户端之间传递的管理帧）采取预防措施。 客户端MFP利用IEEE 802.11i定义的安全机制来保护以下类型的3类单播管理帧：取消关联、取消身份验证和QoS（无线多媒体扩展或WMM）操作。客户端MFP可保护客户端接入点会话免受最常见的拒绝服务攻击。它使用与会话数据帧相同的加密方法来保护第3类管理帧。如果接入点或客户端接收的帧解密失败，则将其丢失，并将事件报告给控制器。

7。如何使用客户端MFP?

要使用客户端MFP，客户端必须支持CCXv5 MFP，并且必须使用临时密钥完整性协议(TKIP)或高级加密标准密码块链消息身份验证代码协议(AES-CCMP)协商Wi-Fi保护访问版本

2(WPA2)。 可扩展身份验证协议(EAP)或预共享密钥(PSK)可用于获取PMK。CCKM和控制器移动性管理用于在接入点之间分配会话密钥，以实现第2层和第3层快速漫游。

8。什么是客户端MFP的组件吗？

客户端MFP有3个组件：

- 密钥生成和分发 — 客户端MFP利用IEEE 802.11i定义的安全协议和机制来保护第3类单播管理帧：

  — 取消关联帧 — 向客户端或WAP发出的断开或取消关联身份验证关系的请求。

  — 取消身份验证帧 — 向客户端或WAP发出断开或取消关联关系的请求。

  - QoS WMM操作 — WMM参数添加到信标、探测响应和关联响应帧。

- 管理帧的保护和验证 — 为防止使用广播帧的攻击，支持CCXv5的AP不会发出任何广播第3类管理帧。如果启用了客户端MFP，处于工作组网桥模式、中继器模式或非根网桥模式的AP将丢弃广播3类管理帧。
- 错误报告 — MFP-1报告机制用于报告接入点检测到的管理帧解封错误。即，WLC 收集 MFP 验证错误统计信息，并定期将整理的信息转发至 WCS。

注意：客户端工作站检测到的MFP违规错误由CCXv5漫游和实时诊断功能处理。

9.为什么我的移动设备无法连接到启用MFP的基础设施设备？

与启用 MFP 的基础架构设备进行通信时，一些无线客户端具有特定的限制。MFP 将一组冗长的信息元素添加到每个探测请求或 SSID 信标。某些无线客户端（如PDA、智能手机、条形码扫描仪等）的内存和中央处理器(CPU)有限。 因此，您无法处理这些请求或信标。因此，您无法完全看到SSID，或者由于对SSID功能的误解而无法与这些基础设施设备关联。此问题不是 MFP 特有的问题。这还出现在具有多信息元素 (IE) 的任何 SSID 上。 在实时部署之前，始终建议在环境中使用所有可用客户端类型测试启用MFP的SSID。

10. 什么是广播管理帧保护？

为防止使用广播帧的攻击，支持CCXv5的AP不传输任何广播第3类管理帧，但欺诈遏制取消身份验证或取消关联帧除外。支持 CCXv5 的客户端站点必须丢弃广播第 3 类管理帧。假设 MFP 会话在一个适当保护的网络（强认证加上 TKIP 或 CCMP）中，因此对恶意遏制广播的忽略并不是问题。

11. 如何在无线接入点(WAP)上配置MFP?

要了解如何在WAP上配置MFP，请单击此处。

12.如何配置英特尔无线网卡以连接到支持MFP的网络

要了解如何配置英特尔无线网卡，请单击此处。