有关管理帧保护(MFP)的常见问题

目标

Wi-Fi是一种广播介质，允许任何设备窃听并作为合法或非法设备参与。无线客户端使用管理帧（例如身份验证、解除身份验证、关联、分离、信标和探测）来启动和中断网络服务会话。数据流量可以加密以提供一定程度的机密性，与此不同的是，所有客户端都必须听到并理解这些帧，因此必须将其作为开放或未加密的数据流传输。虽然这些帧无法加密，但必须防止伪造，以保护无线介质免受攻击。例如，攻击者可以伪装来自AP的管理帧，以攻击与AP关联的客户端。

本文档旨在提供有关管理帧保护(MFP)常见问题的解答。

常见问题解答

目录

1. 什么是MFP？
2. MFP如何工作？
3. 它与PMF有何不同？
4. MFP是什么类型？
5. 客户端MFP包含哪些组件？
6. 客户端MFP如何工作？
7. 如何使用客户端MFP？
8. 客户端MFP包含哪些组件？
9. 为什么我的移动设备无法连接到启用了MFP的基础设施设备？
10. 什么是广播管理帧保护？
11. 如何在无线接入点(WAP)上配置MFP？
12. 如何配置Intel无线网卡以连接到启用MFP的网络？

1.什么 is MFP？

管理帧是IEEE 802.11用来允许无线客户端与无线接入点(WAP)进行协商的广播帧。MFP为无线设备之间传送的未加密广播帧和管理消息提供安全性。

2. MFP如何工作？

在IEEE 802.11中，管理帧（如解除身份验证、解除关联、信标和探测）始终未经验证和加密。WAP将消息完整性检查信息元素(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。

3.在禁用MFP的网络上，攻击者可以做哪些事情？

- 管理帧中发现的漏洞对网络造成巨大威胁，因为攻击者可以伪装来自WAP的管理帧，攻击与之关联的客户端。攻击者可能会执行以下操作：

  — 运行拒绝服务(DoS) -攻击者使用基于流量的典型攻击之外的规避技术来避免检测和缓解，包括“低和慢”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每一层（包括网络基础设施设备、防火墙、服务器和应用）的多漏洞攻击活动。
  — 重新连接时客户端上的中间人攻击—这是一种归纳密钥派生攻击，在802.11网络中由于缺乏有效的消息完整性而有效。帧的接收方无法验证帧在传输期间是否未被篡改。

- 射频(RF)干扰器-距离较远的大功率定向天线攻击可在办公大楼外部进行。入侵者使用的攻击工具利用黑客攻击技术，例如伪装的802.11管理帧、伪装的802.1x身份验证帧，或仅使用暴力数据包泛洪方法。
- Evil Twin Router -这是一种网络钓鱼形式，攻击者以此命名并冒充合法接入点。这会诱使用户将移动设备连接到虚假接入点，从而对用户造成更多伤害。
- 运行离线字典攻击-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。在没有强密码策略的情况下，大多数基于密码的身份验证算法容易遭受字典攻击。

4.MFP是什么类型？

以下是MFP的两种类型：

- 基础架构MFP -具体而言，基础架构MFP通过将MIC IE添加到由接入点而不是客户端发出的管理帧（由网络中的其他接入点验证）来保护802.11会话管理功能。基础设施MFP是被动的。它可以检测并报告入侵，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、作为恶意接入点插入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 -防止经过身份验证的客户端受到伪装帧攻击，防止许多针对无线局域网(LAN)的常见攻击生效。大多数攻击（如解除身份验证攻击）会恢复到仅通过与有效客户端竞争而降低性能的状态。

5.基础设施MFP包含哪些组件？

基础设施MFP包含3个组件：

- 管理帧保护-当启用管理帧保护时，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—当启用管理帧验证时，AP验证其从网络中其他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)（配置为传输MFP帧）收到不包含有效MIC IE的任何帧，它会将差异报告给网络管理系统。

注意：为了让时间戳正常运行，所有无线局域网控制器(WLC)都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加密在接入点和Cisco Compatible Extension v5 (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伪造的第3类管理帧（即，在接入点与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。它通过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(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和控制器移动管理用于分配接入点之间的会话密钥，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：

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

  - 取消关联帧—请求客户端或WAP断开或取消关联身份验证关系。

  - 取消身份验证帧—请求客户端或WAP断开或取消关联关系。

  - 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-为了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，则处于工作组桥模式、中继器模式或非根桥模式的AP将丢弃广播第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：客户端站点检测到的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了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（例如PDA、智能手机、条码扫描仪等）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，由于对SSID功能的误解，您可能无法完全看到SSID，或者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。在您实时部署之前，始终建议使用所有可用的客户端类型测试环境中启用MFP的SSID。

10. 什么是广播管理帧保护？

为了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（非法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？

若要了解如何在WAP上配置MFP，请单击此处。

12. 如何配置Intel无线网卡以连接到启用MFP的网络

若要了解如何配置Intel无线网卡，请单击此处。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。