MFP(Management Frame Protection)에 대한 FAQ

목표

Wi-Fi는 모든 디바이스가 합법적인 디바이스 또는 비인가 디바이스로 엿보고 참여할 수 있도록 하는 브로드캐스트 매체입니다.인증, 인증 해제, 연결, 연결 해제, 신호 및 프로브와 같은 관리 프레임은 무선 클라이언트가 네트워크 서비스에 대한 세션을 시작 및 해제하기 위해 사용합니다.기밀성 수준을 제공하도록 암호화할 수 있는 데이터 트래픽과 달리 이러한 프레임은 모든 클라이언트에서 듣고 인식해야 하므로 개방형 또는 암호화되지 않은 상태로 전송되어야 합니다.이러한 프레임은 암호화할 수 없지만 무선 미디어를 공격으로부터 보호하려면 위조로부터 보호해야 합니다.예를 들어 공격자는 AP에서 관리 프레임을 스푸핑하여 AP와 연결된 클라이언트를 공격할 수 있습니다.

이 문서에서는 MFP(Management Frame Protection)에 대해 자주 묻는 질문에 대한 답변을 제공합니다.

자주 묻는 질문

목차

1.무엇을 이(가) MFP?

관리 프레임은 무선 클라이언트가 WAP(Wireless Access Point)와 협상할 수 있도록 IEEE 802.11에서 사용하는 브로드캐스트 프레임입니다.MFP는 암호화되지 않은 브로드캐스트 프레임 및 무선 디바이스 간에 전달되는 관리 메시지에 대한 보안을 제공합니다.

2. MFP 작동 방식

IEEE 802.11에서는 인증 해제, 연결 해제, 신호 및 프로브와 같은 관리 프레임이 항상 인증되지 않고 암호화되지 않습니다.WAP는 전송하는 각 관리 프레임에 MIC IE(Message Integrity Check Information Element)를 추가합니다.프레임을 복사, 변경 또는 재생하려는 모든 시도에서 MIC가 무효화됩니다.

3.MFP가 비활성화된 네트워크에서 공격자가 수행할 수 있는 몇 가지 작업은 무엇입니까?

- 관리 프레임에서 발견되는 취약성은 공격자가 WAP에서 관리 프레임을 스푸핑하여 연결된 클라이언트를 공격하도록 함으로써 네트워크에 큰 위협이 됩니다.공격자는 다음 작업을 수행할 수 있습니다.

— DoS(Denial of Service) 실행 — 공격자는 일반적인 볼륨 기반 공격 이외의 회피 기법을 사용하여 "낮음 및 느린" 공격 기술과 SSL 기반 공격을 비롯한 탐지 및 완화 작업을 회피하고 있습니다.이들은 네트워크 인프라 디바이스, 방화벽, 서버 및 애플리케이션을 포함하여 피해자의 인프라의 모든 계층을 대상으로 하는 다취약성 공격 캠페인을 구축하고 있습니다.
— 재연결 시 클라이언트에 대한 Man-in-the-Middle 공격 — 효율적인 메시지 무결성으로 인해 802.11 네트워크에서 효과적인 유도 키 파생 공격의 한 형태입니다.프레임을 전송하는 동안 프레임 수신자가 프레임이 변조되지 않았는지 확인할 수 없습니다.

- RF(Radio Frequency) Jammer — 사무실 외부에서 멀리 떨어진 고출력 지향성 안테나를 이용한 공격을 수행할 수 있습니다.침입자가 사용하는 공격 툴은 스푸핑된 802.11 관리 프레임, 스푸핑된 802.1x 인증 프레임 또는 무작위 대입 패킷 플러딩 방법과 같은 해킹 기술을 활용합니다.
- Evil Twin Router — 공격자가 합법적인 액세스 포인트로 이름을 지정하고 포즈를 취하는 피싱 유형입니다.이렇게 하면 사용자가 모바일 장치를 위조 액세스 포인트에 연결함으로써 사용자에게 더 큰 피해를 줄 수 있습니다.
- 오프라인 사전 공격 실행 — 사전 공격 중에 사용자 인증 자격 증명을 손상시키는 데 암호 변형이 사용됩니다.대부분의 비밀번호 기반 인증 알고리즘은 강력한 비밀번호 정책이 없는 경우 사전 공격에 취약합니다.

4.MFP의 유형은 무엇입니까?

다음은 두 가지 유형의 MFP입니다.

- 인프라 MFP — 특히 인프라 MFP는 액세스 포인트에서 방출되는 관리 프레임에 MIC IE를 추가하여 네트워크의 다른 액세스 포인트에서 검증하는 방식으로 802.11 세션 관리 기능을 보호합니다.인프라 MFP는 패시브입니다.침입을 탐지하고 보고할 수 있지만 막을 방법이 없습니다.QoS(Quality of Service) 및 무선 측정 프레임을 공격함으로써 서비스 거부 공격을 호출하고, 연결 프로브로 네트워크를 플러딩하고, 비인가 액세스 포인트로 상호 연결하며, 네트워크 성능에 영향을 미치는 공격자를 탐지하여 관리 프레임을 보호합니다.
- 클라이언트 MFP — 인증된 클라이언트를 스푸핑된 프레임으로부터 보호하여 무선 LAN(Local Area Network)에 대한 다수의 일반적인 공격이 효과적으로 수행되지 않도록 합니다.중복 인증 공격과 같은 대부분의 공격은 유효한 클라이언트와 연결하여 단순히 성능을 저하시키는 것으로 돌아갑니다.

5.인프라 MFP의 구성 요소는 무엇입니까?

인프라 MFP에는 3가지 구성 요소가 있습니다.

- 관리 프레임 보호 — 관리 프레임 보호가 활성화되면 WAP는 전송하는 각 관리 프레임에 MIC IE를 추가합니다.프레임을 복사, 변경 또는 재생하려는 모든 시도에서 MIC가 무효화됩니다.
- 관리 프레임 검증 — 관리 프레임 검증이 활성화되면 AP는 네트워크의 다른 WAP에서 수신하는 모든 관리 프레임을 검증합니다.MIC IE가 있는지 확인하고(발신자가 MFP 프레임을 전송하도록 구성된 경우) 관리 프레임의 내용과 일치시킵니다.MFP 프레임을 전송하도록 구성된 WAP에 속하는 BSSID(Basic Service Set Identifier)에서 유효한 MIC IE를 포함하지 않는 프레임을 수신하면 네트워크 관리 시스템에 불일치를 보고합니다.

> **참고:** 타임스탬프가 제대로 작동하려면 모든 WLC(Wireless LAN Controller)가 NTP(Network Time Protocol)와 동기화되어야 합니다.

- 이벤트 보고 — 액세스 포인트는 WLC가 이상 징후를 탐지하면 이를 알립니다.WLC는 비정상적인 이벤트를 집계하여 SNMP 트랩을 통해 네트워크 관리자에게 보고합니다.

6.클라이언트 MFP는 어떻게 작동합니까?

특히, 클라이언트 MFP는 액세스 포인트와 CCXv5(Cisco Compatible Extension version 5) 클라이언트 간에 전송되는 관리 프레임을 암호화하여 액세스 포인트와 클라이언트 모두 스푸핑된 클래스 3 관리 프레임(즉, 액세스 포인트와 인증 및 연결된 클라이언트 간에 전달되는 관리 프레임)을 삭제하여 예방적인 조치를 취할 수 있도록 합니다. 클라이언트 MFP는 IEEE 802.11i에서 정의한 보안 메커니즘을 활용하여 다음과 같은 유형의 클래스 3 유니캐스트 관리 프레임을 보호합니다.연결 해제, 인증 해제 및 QoS(무선 멀티미디어 확장 또는 WMM) 작업클라이언트 MFP는 가장 일반적인 유형의 서비스 거부 공격으로부터 클라이언트 액세스 포인트 세션을 보호합니다.세션 데이터 프레임에 사용되는 것과 동일한 암호화 방법을 사용하여 클래스 3 관리 프레임을 보호합니다.액세스 포인트 또는 클라이언트에서 받은 프레임이 암호 해독에 실패하면 해당 프레임이 삭제되고 이벤트가 컨트롤러에 보고됩니다.

7.클라이언트 MFP는 어떻게 사용합니까?

클라이언트 MFP를 사용하려면 클라이언트가 CCXv5 MFP를 지원해야 하며 TKIP(Temporal Key Integrity Protocol) 또는 AES-CCMP(Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol)를 사용하여 WPA2(Wi-Fi Protected Access 버전 2)를 협상해야 합니다. EAP(Extensible Authentication Protocol) 또는 PSK(Pre-Shared Key)를 사용하여 PMK를 얻을 수 있습니다.CCKM 및 컨트롤러 모빌리티 관리는 레이어 2와 레이어 3 빠른 로밍의 액세스 포인트 간에 세션 키를 배포하는 데 사용됩니다.

8.정말클라이언트 MFP의 구성 요소입니까?

클라이언트 MFP에는 3가지 구성 요소가 있습니다.

- 키 생성 및 배포 — 클라이언트 MFP는 IEEE 802.11i에서 정의한 보안 프로토콜 및 메커니즘을 활용하여 클래스 3 유니캐스트 관리 프레임을 보호합니다.

  - 프레임 연결 해제 — 인증 관계의 연결 해제 또는 연결을 해제하기 위한 클라이언트 또는 WAP에 대한 요청입니다.

  - 인증 해제 프레임 — 연결 관계를 연결 해제하거나 연결 해제하기 위한 클라이언트 또는 WAP에 대한 요청입니다.

  - QoS WMM 작업 — WMM 매개변수가 신호, 프로브 응답 및 연결 응답 프레임에 추가됩니다.

- 관리 프레임 보호 및 검증 — 브로드캐스트 프레임을 사용하는 공격을 방지하기 위해 CCXv5를 지원하는 AP는 어떤 브로드캐스트 클래스 3 관리 프레임도 내보내지 않습니다.워크그룹 브리지 모드, 리피터 모드 또는 비루트 브리지 모드의 AP는 클라이언트 MFP가 활성화된 경우 브로드캐스트 클래스 3 관리 프레임을 무시합니다.
- 오류 보고서 — MFP-1 보고 메커니즘은 액세스 포인트에서 탐지된 관리 프레임 캡슐화 해제 오류를 보고하는 데 사용됩니다.즉, WLC는 MFP 검증 오류 통계를 수집하고 정기적으로 수집된 정보를 WCS에 전달합니다.

  참고:클라이언트 스테이션에서 탐지된 MFP 위반 오류는 CCXv5 로밍 및 실시간 진단 기능을 통해 처리됩니다.

9. 모바일 장치가 MFP 지원 인프라 장치에 연결할 수 없는 이유는 무엇입니까?

일부 무선 클라이언트가 MFP 지원 인프라 디바이스와 통신하는 데 특정한 제한이 있습니다

.MFP는 각 프로브 요청 또는 SSID 신호에 긴 정보 요소 집합을 추가합니다.PDA, 스마트폰, 바코드 스캐너 등과 같은 일부 무선 클라이언트는 메모리 및 CPU(Central Processing Unit)가 제한적입니다. 따라서 이러한 요청이나 신호를 처리할 수 없습니다.따라서 SSID를 완전히 볼 수 없거나 SSID 기능에 대한 오해로 인해 이러한 인프라 디바이스와 연결할 수 없습니다.이 문제는 MFP에만 국한되지 않습니다.이는 IE(정보 요소)가 여러 개인 SSID에서도 발생합니다. 실시간으로 배포하기 전에 사용 가능한 모든 클라이언트 유형으로 환경에서 MFP 지원 SSID를 테스트하는 것이 좋습니다.

10. Broadcast Management Frame Protection이란 무엇입니까?

브로드캐스트 프레임을 사용하는 공격을 방지하기 위해 CCXv5를 지원하는 AP는 비인가 억제 제거 인증 또는 연결 해제 프레임을 제외하고 브로드캐스트 클래스 3 관리 프레임을 전송하지 않습니다.CCXv5 지원 클라이언트 스테이션은 브로드캐스트 클래스 3 관리 프레임을 폐기해야 합니다.MFP 세션은 적절한 보안 네트워크(강력한 인증 + TKIP 또는 CCMP)에 있는 것으로 간주되므로 비인가 억제 브로드캐스트를 무시해도 문제가 되지 않습니다.

11 . WAP(Wireless Access Point)에서 MFP를 구성하는 방법

WAP에서 MFP를 구성하는 방법을 알아보려면 여기를 클릭하십시오.

12. MFP 지원 네트워크에 연결하도록 인텔 무선 네트워크 카드를 구성하는 방법

인텔 무선 네트워크 카드를 구성하는 방법을 알아보려면 여기를 클릭하십시오.