Vaak gestelde vragen over Management Frame Protection (MFP)

Doel

Wi-Fi is een uitzendmedium dat elk apparaat in staat stelt om te luisteren en te participeren als een legitiem of schurkenapparaat. Beheerframes zoals verificatie, desverificatie, associatie, dissociatie, bakens en sondes worden door draadloze klanten gebruikt om sessies voor netwerkservices te initiëren en af te breken. In tegenstelling tot gegevensverkeer, dat kan worden versleuteld om een niveau van vertrouwelijkheid te bieden, moeten deze frames worden gehoord en begrepen door alle klanten en moeten daarom worden verzonden als open of niet-gecodeerd. Terwijl deze frames niet kunnen worden versleuteld, moeten ze tegen vervalsing worden beschermd om het draadloze medium tegen aanvallen te beschermen. Bijvoorbeeld, zou een aanvaller beheerframes van een AP kunnen bespotten om een client aan te vallen verbonden met AP.

Dit document wil antwoorden op de veelgestelde vragen over Frame Relay Protection (MFP).

Veelgestelde vragen

Inhoud

1. Wat is MFP?
2. Hoe werkt MFP?
3. Hoe verschilt het van PMF?
4. Wat zijn de soorten MFP?
5. Wat zijn de componenten van client-MFP?
6. Hoe werkt Client MFP?
7. Hoe gebruik ik client-MFP?
8. Wat zijn de componenten van client-MFP?
9. Waarom kan mijn mobiele apparaat niet worden aangesloten op het MFP enabled infrastructuurapparaat?
10. Wat is bescherming van omroep Management Frame Relay?
11. Hoe moet u MFP op een draadloos access point (WAP) configureren?
12. Hoe moet u de Intel Wireless Network Card configureren om verbinding te maken met een MFP-enabled netwerk?

1. Wat is MFP?

Management-frames zijn broadcast-frames die door IEEE 802.11 worden gebruikt om een draadloze client mogelijk te maken om te onderhandelen met een draadloos access point (WAP). MFP biedt beveiliging voor niet-gecodeerde uitzendframes en beheerberichten die tussen draadloze apparaten worden doorgegeven.

2. Hoe werkt MFP?

In IEEE 802.11 worden beheerframes zoals verificatie, disassociatie, bakens en sondes altijd niet-echt gemaakt en niet gecodeerd. WAP voegt Message Integrity Control Information

element (MIC IE) toe aan elk beheerkader dat door haar wordt verzonden. Elke poging om het kader te kopiëren, wijzigen of opnieuw af te spelen maakt de MIC ongeldig.

3. Wat zijn enkele dingen die een aanvaller kan doen op een netwerk met MFP uitgeschakeld?

- De kwetsbaarheid die in beheerframes wordt gevonden vormt een grote bedreiging voor een netwerk door een aanvaller toe te staan om van een beheerkader van een WAP een client aan te vallen die eraan is gekoppeld. Een aanvaller kan de volgende handelingen uitvoeren:

— Start een Denial of Service (DoS) — Ataanvallen gebruiken ontwijkingstechnieken buiten de typische op volume gebaseerde aanvallen om detectie en beperking te voorkomen, inclusief "low-and-long" aanvalstechnieken en SSL-gebaseerde aanvallen. Ze zijn bezig met het opzetten van aanvallen op meerdere kwetsbaarheden die gericht zijn op elke laag van de infrastructuur van het slachtoffer, inclusief de netwerkinfrastructuren apparaten, firewalls, servers en toepassingen.
— Man-in-the-Middle aanval op de cliënt bij heraansluiting — Het is een vorm van een inductieve sleutelafleiding die effectief is in 802.11 netwerken vanwege het gebrek aan effectieve berichtintegriteit. De ontvanger van een frame kan niet controleren of het frame tijdens de transmissie niet met het frame is geknoeid.

- Radio Frequency (RF) Jammer — Aanvallen met een hoogspanningsgerichte antenne vanaf een afstand kunnen worden uitgevoerd vanaf de buitenkant van uw kantoorgebouw. Attack tools die gebruikt worden door indringers hefboomtechnieken zoals gespoofde 802.11 beheerframes, gespoofde 802.1x authenticatieframes, of simpelweg gebruik makend van de brute force Packet overstromingsmethode.
- Het is een vorm van phishing waarin een aanvaller zich noemt en posteert als een legitiem toegangspunt. Dit trickt gebruikers om een mobiel apparaat aan te sluiten op het nep access point, waardoor ze meer schade kunnen toebrengen aan de gebruiker.
- Draai een offline woordenboekaanval — Tijdens een woordenboekaanval, worden de varianten van wachtwoorden gebruikt om de authenticiteitsreferenties van de gebruiker in gevaar te brengen. De meeste op wachtwoord gebaseerde authenticatiemethoden zijn kwetsbaar voor woordenboekaanvallen bij ontstentenis van een sterk wachtwoordbeleid.

4. Wat zijn de soorten MFP?

Dit zijn de twee soorten MFP's:

- Infrastructuur MFP — Met name, infrastructuur MFP beschermt 802.11 sessiebeheerfuncties door MIC IE toe te voegen aan de beheerframes die door toegangspunten worden uitgestoten en niet door klanten uitgestoten, die door andere toegangspunten in het netwerk worden gevalideerd. Infrastructuur MFP is passief. Het kan inbreuken opsporen en melden, maar het heeft geen middelen om ze tegen te houden. Het beschermt beheerframes door vijanden te detecteren die zich beroepen op denial-of-service aanvallen, het netwerk te overspoelen met associatiedondes, te onderwerpen als schurken access points en de netwerkprestaties te beïnvloeden door de QoS-kwaliteit (Quality of Service) en radiofrequentiesoframes aan te vallen.
- Cliënt MFP — Geautomatiseerde cliënten van gespoofde frames worden gescand, waardoor veel van de gemeenschappelijke aanvallen op draadloze LAN’s (Local Area Networks) niet effectief worden. De meeste aanvallen, zoals de-authenticatie aanvallen, keren terug naar het eenvoudigweg verslechteren van de prestaties door verbinding te maken met geldige klanten.

5. Wat zijn de onderdelen van MFP-infrastructuur?

Infrastructuur MFP bevat 3 onderdelen:

- Bedieningskader bescherming — Wanneer de bescherming van het beheerkader is ingeschakeld, voegt WAP MIC IE toe aan elk beheerkader dat zij doorgeeft. Elke poging om het kader te kopiëren, wijzigen of opnieuw af te spelen maakt de MIC ongeldig.
- geldigmaking van beheerframe — Wanneer de validatie van beheerframe is ingeschakeld, bevestigt AP elk beheerframe dat het ontvangt van andere WAP's in het netwerk. Dit waarborgt dat de MIC IE aanwezig is (wanneer de originator is ingesteld om MFP-frames door te geven) en de inhoud van het beheerkader aanpast. Als het een kader ontvangt dat geen geldig MIC IE bevat van een Basic Service Set Identifier (BSSID) die tot een WAP behoort, dat wordt geconfigureerd om MFP-frames door te geven, rapporteert het de discrepantie aan het netwerkbeheersysteem.

  N.B.: Om de tijdstempels goed te laten werken, moeten alle draadloze LAN-controllers (WLC) gesynchroniseerd zijn met Network Time Protocol (NTP).

- Rapportage van gebeurtenissen — Het toegangspunt meldt de WLC wanneer het een anomalie detecteert. WLC aggregeert de anomalische gebeurtenissen en rapporteert het door SNMP vallen aan de netwerkmanager.

6. Hoe werkt client MFP?

Met name client-MFP versleutelt beheerframes die tussen access points en Cisco Compatibele Extension versie 5 (CCXv5) worden verzonden, zodat zowel de access points als de clients preventieve actie kunnen uitvoeren door gespoofde klasse 3 beheerframes af te zetten (dat wil zeggen, beheerframes die tussen een access point en een client worden doorgegeven die authentiek en gekoppeld is). ClientMFP maakt gebruik van de beveiligingsmechanismen die door IEEE 802.11i zijn gedefinieerd om de volgende typen beheerframes van klasse 3 te beschermen: disassociatie, desverificatie en QoS (draadloze multimedia extensies of WMM)-actie. Client MFP beschermt een client-access point sessie tegen het meest gebruikelijke type 'denial-of-service'-aanval. Het beschermt class 3 beheerframes door gebruik te maken van dezelfde coderingsmethode die gebruikt wordt voor de sessiegegevensframes. Als een kader dat door het toegangspunt of de client wordt ontvangen, niet decryptie heeft, wordt het ingetrokken en wordt de gebeurtenis aan de controller gemeld.

7. Hoe gebruik ik cliënt MFP?

Om MFP van een client te gebruiken, moeten klanten CCXv5 MFP ondersteunen en moeten zij met Wi-Fi Protected Access versie 2 (WAP2) onderhandelen met TKIP (Temporal Key Integrity Protocol) of Advanced Encryption Standard-Cipher Block Chaining Message Authentication Protocol (AES-CCMP). Extensible Authentication Protocol (EAP) of Pre-Shared Key (PSK) kan worden gebruikt om de PMK te verkrijgen. CCKM en het mobiliteitsbeheer van controllers worden gebruikt om de sessies tussen de toegangspunten voor Layer 2 en Layer 3 snelle roaming te verdelen.

8. Wat eenzijn de componenten van client-MFP?

Er zijn 3 componenten van client-MFP:

- Belangrijkste generatie en distributie — ClientMFP maakt gebruik van beveiligingsprotocollen en -mechanismen die door IEEE 802.11i zijn gedefinieerd ter bescherming van de

beheersframes van klasse 3:

- Scheidingsframes — Een verzoek aan een client of WAP om een authenticatierelatie los te koppelen of te ontkoppelen.

- De-authenticatie frames — Een verzoek aan een cliënt of WAP om een associatie-relatie los te koppelen of te ontkoppelen.

- QoS WMM-actie — WMM-parameter wordt toegevoegd aan de beacon, de sonde-respons en de associatie-responsframes.

- Bescherming en validatie van beheerframes — Om aanvallen met uitzendframes te voorkomen, zenden AP's die CCXv5 ondersteunen geen beheerframes uit van omroepklasse 3. AP in de modus van de werkgroepbridge, van de repeatermodus, of van de niet-worteloverbruggingsmodus gooit uit klasse 3 beheerframes weg als client MFP is ingeschakeld.
- Foutenrapporten — MFP-1 rapportagemechanismen worden gebruikt om fouten van beheerframe-de-insluitingsfouten te melden die door toegangspunten worden gedetecteerd. Dat wil zeggen, de WLC verzamelt MFI - valideringsfoutstatistieken en stuurt periodiek verzamelde informatie naar de WCS door.

Opmerking: MFP-overschrijdingsfouten die door clientstations zijn gedetecteerd, worden verwerkt door de optie CCXv5-roaming en realtime-diagnostiek.

9. Waarom kan mijn mobiele apparaat geen verbinding maken met het MFP-enabled-infrastructuurapparaat?

Er zijn bepaalde beperkingen voor sommige draadloze klanten om met MFP-enabled-infrastructuuraanpassingen te communiceren. MFP voegt een lange reeks informatie elementen toe aan elk sonde verzoek of SSID baken. Sommige draadloze klanten zoals PDA's, smartphones, barcodes scanners, enzovoort hebben een beperkt geheugen en een centrale verwerkingseenheid (CPU). Je kunt deze verzoeken of bakens dus niet verwerken. Als resultaat hiervan, ziet u SSID niet volledig, of kunt u niet met deze infrastructuuracties associëren, wegens een misverstand van de mogelijkheden van SSID. Deze kwestie is niet specifiek voor MFP. Dit gebeurt ook met elke SSID die meerdere informatie-elementen (IE's) heeft. Het is altijd raadzaam om met MFP-enabled SSID's op de omgeving te testen met al uw beschikbare clienttypen voordat u deze in real time implementeert.

10. Wat is bescherming van omroep Management Frame Relay?

Om aanvallen te voorkomen die uitzendframes gebruiken, zenden APs die CCXv5 ondersteunen geen broadcast-klasse 3 beheerframes uit, behalve rotatielampjes die de-verificatie of disassociatieformulieren bevatten. CCXv5-kabelstations moeten kabelstations van omroepklasse 3-beheerframes afwijzen. MFP-sessies worden verondersteld in een goed beveiligd netwerk te zijn (sterke authenticatie plus TKIP of CCMP), zodat het niet in acht nemen van aanvallen op uitzendingen van rotatiebeheersing geen probleem is.

11. Hoe moet u MFP op een draadloos access point (WAP) configureren?

Klik hier om te leren hoe u MFP op een WAP moet configureren.

12. Een Intel draadloze netwerkkaart configureren voor aansluiting op een MFP-enabled-netwerk

Klik hier voor informatie over de configuratie van de Intel Wireless Network Card.