Domande frequenti sulla protezione MFP (Management Frame Protection)

Obiettivo

Wi-Fi è un mezzo di trasmissione che consente a qualsiasi dispositivo di origliare e partecipare come dispositivo legittimo o non autorizzato. I frame di gestione, ad esempio autenticazione, deautenticazione, associazione, dissociazione, beacon e probe, vengono utilizzati dai client wireless per avviare e interrompere sessioni per i servizi di rete. A differenza del traffico di dati, che può essere criptato per fornire un livello di riservatezza, questi frame devono essere ascoltati e compresi da tutti i client e quindi trasmessi come aperti o non crittografati. Anche se questi frame non possono essere crittografati, devono essere protetti dalla contraffazione per proteggere il supporto wireless dagli attacchi. Ad esempio, un utente malintenzionato potrebbe eseguire lo spoofing dei frame di gestione da un punto di accesso per attaccare un client associato a tale punto.

Lo scopo di questo documento è quello di fornire le risposte alle domande frequenti sulla protezione del frame di gestione.

Domande frequenti

Sommario

1. Cosa è MFP (Management Frame Protection)?

I frame di gestione sono frame di trasmissione utilizzati da IEEE 802.11 per consentire a un client wireless di negoziare con un punto di accesso wireless (WAP). MFP garantisce la protezione dei frame di trasmissione non crittografati e dei messaggi di gestione trasmessi tra dispositivi wireless.

2. Come funziona MFP?

In IEEE 802.11, i frame di gestione come la deautenticazione, la disassociazione, i beacon e le sonde sono sempre non autenticati e non crittografati. Il WAP aggiunge l'elemento MIC

(Message Integrity Check Information Element) a ogni frame di gestione trasmesso. Ogni tentativo di copiare, modificare o riprodurre il frame invalida il MIC.

3. Quali sono le operazioni che un utente non autorizzato può eseguire in una rete in cui è disattivato il protocollo MFP?

- La vulnerabilità rilevata nei frame di gestione rappresenta una grave minaccia per la rete, in quanto consente all'autore di un attacco di eseguire lo spoofing di un frame di gestione da un WAP per attaccare un client ad esso associato. Un utente non autorizzato può eseguire le azioni seguenti:

— Esecuzione di un DoS (Denial of Service) — Gli aggressori utilizzano tecniche di evasione al di fuori dei tipici attacchi basati su volumi per evitare il rilevamento e la mitigazione, incluse tecniche di attacco "lente e basse" e attacchi basati su SSL. Stanno implementando campagne di attacco multivulnerabilità che colpiscono ogni livello dell'infrastruttura della vittima, inclusi dispositivi dell'infrastruttura di rete, firewall, server e applicazioni.
— Attacco man-in-the-middle al client quando riconnesso — È una forma di attacco di derivazione della chiave induttiva che è efficace nelle reti 802.11 a causa della mancanza di effettiva integrità del messaggio. Il ricevitore di un frame non può verificare che il frame non sia stato manomesso durante la trasmissione.

- Jammer a radiofrequenza (RF) — Attacchi con un'antenna direzionale ad alta potenza da una certa distanza possono essere effettuati dall'esterno del vostro ufficio. Gli strumenti di attacco usati dagli intrusi sfruttano le tecniche di hacking, come i frame di gestione 802.11 falsificati, i frame di autenticazione 802.1x falsificati o semplicemente usando il metodo di flagellazione dei pacchetti di forza bruta.
- Evil Twin Router: è una forma di phishing in cui un utente malintenzionato assegna un nome e si pone come punto di accesso legittimo. Questo induce gli utenti a connettere un dispositivo mobile al falso punto di accesso, in modo da poter causare più danni all'utente.
- Esegui un attacco di dizionario non in linea - Durante un attacco di dizionario, le variazioni delle password vengono utilizzate per compromettere le credenziali di autenticazione dell'utente. La maggior parte degli algoritmi di autenticazione basati su password è vulnerabile agli attacchi dei dizionari in assenza di regole per le password complesse.

4. Quali sono i tipi di stampanti multifunzione?

Di seguito sono riportati i due tipi di piani multifunzione:

- MFP infrastruttura: in particolare, MFP infrastruttura protegge le funzioni di gestione delle sessioni 802.11 aggiungendo MIC IE ai frame di gestione emessi dai punti di accesso e non quelli emessi dai client, che sono convalidati da altri punti di accesso nella rete. MFP infrastruttura passivo. Può rilevare e segnalare le intrusioni, ma non ha i mezzi per fermarle. Protegge i frame di gestione rilevando gli avversari che richiamano attacchi di negazione del servizio, inondando la rete con sonde di associazione, interrompendo come punti di accesso non autorizzati e compromettendo le prestazioni della rete attaccando i frame QoS (Quality of Service) e di misurazione radio.
- MFP client: protegge i client autenticati da frame falsificati, impedendo l'efficacia di molti attacchi comuni alle reti LAN (Wireless Local Area Network). La maggior parte degli attacchi, ad esempio quelli di deautenticazione, si risolve in una semplice riduzione delle prestazioni in quanto si scontra con client validi.

5. Quali sono i componenti di Infrastructure MFP?

Il programma di manutenzione dell'infrastruttura è costituito da 3 componenti:

- Protezione frame di gestione: quando la protezione frame di gestione è abilitata, WAP aggiunge MIC IE a ciascun frame di gestione che trasmette. Ogni tentativo di copiare, modificare o riprodurre il frame invalida il MIC.
- Convalida frame di gestione: quando la convalida frame di gestione è abilitata, l'access point convalida ogni frame di gestione ricevuto da altri WAP nella rete. Assicura che MIC IE sia presente (quando il creatore è configurato per trasmettere i frame MFP) e corrisponde al contenuto del frame di gestione. Se riceve un frame che non contiene un MIC IE valido da un Basic Service Set Identifier (BSSID) che appartiene a un WAP, configurato per trasmettere i frame MFP, segnala la discrepanza al sistema di gestione di rete.

  Nota: per il corretto funzionamento dei timestamp, tutti i controller WLC (Wireless LAN Controller) devono essere sincronizzati con il protocollo NTP (Network Time Protocol).

- Segnalazione eventi: il punto di accesso notifica il WLC quando rileva un'anomalia. WLC aggrega gli eventi anomali e li segnala al gestore della rete tramite trap SNMP.

6. Come funziona la funzione MFP del client?

In particolare, la funzione MFP client cripta i frame di gestione inviati tra i punti di accesso e i client Cisco Compatible Extension versione 5 (CCXv5) in modo che sia i punti di accesso che i client possano adottare misure preventive eliminando i frame di gestione di classe 3 contraffatti (ovvero, i frame di gestione passati tra un punto di accesso e un client autenticato e associato). La funzione MFP client sfrutta i meccanismi di sicurezza definiti da IEEE 802.11i per proteggere i seguenti tipi di frame di gestione unicast di classe 3: disassociazione, deautenticazione e azione QoS (Wireless Multimedia Extenions o WMM). La funzione MFP client protegge una sessione del punto di accesso client dal tipo più comune di attacco di tipo Denial of Service. Protegge i frame di gestione di classe 3 utilizzando lo stesso metodo di crittografia utilizzato per i frame dati della sessione. Se un frame ricevuto dal punto di accesso o dal client non viene decrittografato, viene eliminato e l'evento viene segnalato al controller.

7. Come si utilizza la funzionalità MFP client?

Per utilizzare la funzione MFP client, i client devono supportare la funzione MFP CCXv5 e negoziare l'accesso protetto Wi-Fi versione 2 (WPA2) utilizzando il protocollo TKIP (Temporal Key Integrity Protocol) o il protocollo AES-CCMP (Advanced Encryption Standard-Cipher Block Chaining Message Code Protocol). Per ottenere la chiave PMK è possibile utilizzare il protocollo EAP (Extensible Authentication Protocol) o la chiave precondivisa (PSK). La funzionalità CCKM e la gestione della mobilità dei controller vengono utilizzate per distribuire le chiavi di sessione tra i punti di accesso per il roaming veloce di layer 2 e layer 3.

8. Chel componenti sono di Client MFP?

Sono disponibili 3 componenti di Client MFP:

- Generazione e distribuzione di chiavi: la funzionalità Client MFP utilizza i protocolli e i meccanismi di sicurezza definiti da IEEE 802.11i per proteggere i frame di gestione unicast di classe 3:

  - Frame di disassociazione - Richiesta a un client o a un punto di accesso Windows di

disconnettere o dissociare una relazione di autenticazione.

- Frame di deautenticazione: richiesta a un client o a un punto di accesso Windows di disconnettere o dissociare una relazione di associazione.

- Azione WMM QoS - Il parametro WMM viene aggiunto ai frame di beacon, risposta probe e risposta associazione.

- Protezione e convalida dei frame di gestione: per evitare attacchi tramite frame di trasmissione, i punti di accesso che supportano CCXv5 non emettono frame di gestione di classe 3. Un punto di accesso in modalità bridge di gruppo di lavoro, ripetitore o non root bridge elimina i frame di gestione della classe 3 broadcast se l'opzione MFP client è abilitata.
- Segnalazioni errori: i meccanismi di segnalazione MFP-1 vengono utilizzati per segnalare gli errori di decapsulamento del frame di gestione rilevati dai punti di accesso. In altri termini, il WLC raccoglie le statistiche sugli errori di convalida dei dispositivi multifunzione e inoltra periodicamente le informazioni raccolte al WCS.

Nota: Gli errori di violazione MFP rilevati dalle stazioni client vengono gestiti dalla funzionalità Roaming e diagnostica in tempo reale di CCXv5.

9. Perché il dispositivo mobile non è in grado di connettersi al dispositivo di infrastruttura abilitato per MFP?

Esistono alcune restrizioni per la comunicazione tra alcuni client wireless e dispositivi di infrastruttura abilitati per MFP. La funzione MFP aggiunge un lungo set di elementi di informazione a ciascuna richiesta di sonda o beacon SSID. Alcuni client wireless, ad esempio PDA, smartphone, scanner di codici a barre e così via, dispongono di una quantità limitata di memoria e di CPU (Central Processing Unit). Non è quindi possibile elaborare tali richieste o beacon. Di conseguenza, non è possibile visualizzare completamente l'SSID o associarlo a questi dispositivi di infrastruttura a causa di un'errata comprensione delle funzionalità SSID. Questo problema non riguarda solo le stampanti multifunzione. Ciò si verifica anche con qualsiasi SSID che dispone di più elementi di informazione (IE). È sempre consigliabile testare gli SSID abilitati per MFP nell'ambiente con tutti i tipi di client disponibili prima di distribuirli in tempo reale.

10. Cos'è la protezione del frame di gestione della trasmissione?

Per prevenire attacchi che utilizzano frame di trasmissione, gli access point che supportano CCXv5 non trasmettono alcun frame di gestione di classe 3 ad eccezione dei frame di disassociazione o deautenticazione con contenimento anomalo. Le stazioni client compatibili con CCXv5 devono eliminare i frame di gestione broadcast di classe 3. Si presume che le sessioni MFP si trovino in una rete adeguatamente protetta (autenticazione avanzata più TKIP o CCMP), quindi non è un problema ignorare le trasmissioni di contenimento non autorizzate.

11. Come configurare una stampante multifunzione su un punto di accesso wireless (WAP)?

per informazioni su come configurare la stampante multifunzione su un server WAP, fare clic qui.

12. Come configurare una scheda di rete wireless Intel per la connessione a una rete abilitata per MFP

per informazioni su come configurare la scheda di rete wireless Intel, fare clic qui.