Reti Wireless

Le reti wireless, pur essendo comode e facili da implementare, sono vulnerabili a vari tipi di attacchi e sfide relative alla sicurezza. In questo contesto, esploreremo in dettaglio i canali di comunicazione, la sicurezza delle reti wireless, i principali attacchi e una spiegazione approfondita degli algoritmi di sicurezza (WEP, WPA, WPA2, WPA3) e di Mobile IP.

Canali di Comunicazione nelle Reti Wireless

Un canale di comunicazione in una rete wireless rappresenta la frequenza attraverso cui i dati vengono trasmessi tra i dispositivi. Questi canali sono fondamentali per garantire una comunicazione stabile, sicura e a bassa latenza. Le bande di frequenza comunemente utilizzate nelle reti wireless includono:

- La **banda a 2.4 GHz** (ISM Band), che è la più comune per dispositivi wireless come Wi-Fi, Bluetooth e Zigbee. Sebbene molto utilizzata, questa banda è anche molto congestionata e soggetta a interferenze da dispositivi come microonde e telefoni cordless.

- La **banda a 5 GHz**, che offre prestazioni migliori rispetto alla 2.4 GHz, con minori interferenze, ma una copertura inferiore. Viene utilizzata per Wi-Fi (802.11a/n/ac/ax).

- La **banda a 6 GHz** (Wi-Fi 6E), utilizzata per Wi-Fi 6E, che consente una maggiore capacità e supporta un numero maggiore di dispositivi con minore latenza.

Alcune tecnologie, come WiMAX e Wi-Fi (in modalità non licenziata), operano su bande di frequenza che non richiedono licenza (come la banda ISM), mentre altre come WiMAX possono operare su frequenze licenziate per garantire minori interferenze.

La latenza e la larghezza di banda di un canale sono cruciali per determinare la qualità della rete. La latenza rappresenta il ritardo con cui i pacchetti di dati arrivano a destinazione, ed è influenzata dalla distanza, dalla qualità del canale e dal tipo di interferenze. Una maggiore disponibilità di canali consente una gestione migliore del traffico ad alta velocità senza sovraccaricare la rete.

Attacchi alle Reti Wireless

Le reti wireless sono vulnerabili a numerosi tipi di attacchi, che spaziano dall’intercettazione passiva alla manipolazione attiva dei dati.

Attacchi di Intercettazione (Eavesdropping)

L'attacco di eavesdropping, o intercettazione passiva, avviene quando un attaccante si limita ad ascoltare il traffico di rete senza interferire direttamente con la comunicazione. Questo tipo di attacco è possibile nelle reti wireless, in quanto il segnale radio può essere captato a distanza. Gli attaccanti possono utilizzare strumenti come Wireshark e Aircrack-ng per intercettare e analizzare i pacchetti di rete, ottenendo informazioni sensibili come credenziali di accesso o dati non criptati. La crittografia avanzata, come quella offerta da WPA3, può proteggere i dati, rendendo difficoltoso per un attaccante decifrare le informazioni intercettate.

Attacco Man-in-the-Middle (MitM)

Un attacco Man-in-the-Middle si verifica quando un hacker si interpone tra due dispositivi legittimi, intercettando e alterando la comunicazione tra di essi. Questo tipo di attacco è particolarmente pericoloso poiché consente all'attaccante di leggere e modificare i dati o iniettare falsi messaggi. Per esempio, un hacker potrebbe intercettare una connessione Wi-Fi pubblica non protetta e farsi passare per il punto di accesso legittimo, inducendo i dispositivi a connettersi tramite lui, con il rischio di vedere e alterare tutto il traffico della rete. Per prevenire tali attacchi, è utile utilizzare una VPN (Virtual Private Network) e protocolli sicuri come HTTPS, che proteggono i dati tramite crittografia end-to-end.

Rogue Access Point (AP Malevolo)

Un rogue access point è un dispositivo che simula un punto di accesso legittimo, utilizzando lo stesso SSID della rete wireless. Gli utenti ignari possono connettersi a questo AP malintenzionato, permettendo all'attaccante di raccogliere informazioni sensibili o di lanciare attacchi più complessi. L'uso di sistemi di rilevamento delle intrusioni wireless, come i WIDS (Wireless Intrusion Detection System), può aiutare a monitorare la rete alla ricerca di AP sconosciuti o malevoli.

Attacco di Denial of Service (DoS)

Un attacco DoS in una rete wireless può essere effettuato inviando segnali interferenti per sovraccaricare i canali wireless o distruggere la connessione tra dispositivi e access point. Gli attaccanti possono anche inondare la rete di pacchetti di dati inutili, riducendo così la qualità del servizio. Per prevenire tali attacchi, è possibile implementare sistemi di monitoraggio per rilevare traffico anomalo e utilizzare meccanismi di difesa, come il rate limiting.

Algoritmi di Sicurezza nelle Reti Wireless

WEP (Wired Equivalent Privacy)

WEP è uno dei primi protocolli di crittografia usati per proteggere le reti Wi-Fi, ma nel tempo è stato ampiamente compromesso. Utilizza una chiave di crittografia statica di 64 o 128 bit combinata con un vector di inizializzazione (IV) per produrre una chiave di sessione che cifra i dati. Tuttavia, l'algoritmo WEP è vulnerabile a vari tipi di

attacchi, come il cracking della chiave e l'intercettazione dell'IV, che possono essere facilmente sfruttati tramite strumenti come Aircrack-ng.

- **WPA (Wi-Fi Protected Access)**
  WPA è stato introdotto per migliorare la sicurezza delle reti Wi-Fi e sostituire WEP. Utilizza il TKIP (Temporal Key Integrity Protocol), che cambia la chiave di crittografia per ogni pacchetto, risolvendo parzialmente le vulnerabilità di WEP. Tuttavia, WPA è ancora suscettibile a vari attacchi, come quelli di packet injection e attacchi di dictionary, dovuti alla debolezza intrinseca del protocollo TKIP.

- **WPA2 (Wi-Fi Protected Access 2)**
  WPA2 migliora WPA, sostituendo TKIP con il più sicuro AES (Advanced Encryption Standard) in modalità CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). AES-CCMP offre una crittografia di livello superiore, ma, sebbene sicuro, WPA2 è vulnerabile a attacchi come il KRACK (Key Reinstallation Attack), che sfrutta un difetto nel processo di handshake.

- **WPA3 (Wi-Fi Protected Access 3)**
  WPA3 è l'ultima evoluzione dei protocolli di sicurezza Wi-Fi, con diversi miglioramenti significativi, come la protezione contro gli attacchi brute-force tramite Simultaneous Authentication of Equals (SAE). Inoltre, supporta la crittografia individuale per ogni dispositivo connesso, migliorando la sicurezza generale della rete.

Mobile IP

Mobile IP è un protocollo che consente ai dispositivi mobili di mantenere una connessione attiva mentre si spostano tra diverse reti IP, come tra una rete Wi-Fi e una rete cellulare. Questo protocollo è fondamentale per garantire che i dispositivi mobili non perdano la connessione a Internet mentre si spostano. Il funzionamento di Mobile IP coinvolge il **Home Agent (HA)**, un server che memorizza l'indirizzo IP del dispositivo mobile nella sua rete principale; il **Foreign Agent (FA)**, un server nella rete esterna che aiuta a instradare i pacchetti destinati al dispositivo mobile; e la **Care-of Address (CoA)**, un indirizzo IP temporaneo assegnato al dispositivo quando si trova in una rete diversa dalla sua home network. Grazie al processo di handover, il traffico viene instradato tramite il Home Agent al dispositivo mobile, garantendo una connessione continua senza interruzioni.