Reti Wireless

Le reti wireless utilizzano la tecnologia a radiofrequenza (RF) per trasmettere i dati tra i dispositivi. Ogni dispositivo su una rete wireless dispone di un adattatore wireless che converte i dati in segnali RF e li invia via etere.

Una volta connessi, i dispositivi possono comunicare tra loro e con Internet, consentendo agli utenti di accedere alle risorse online e scambiare dati.

Quando un dispositivo, come un laptop, desidera inviare dati sulla rete, comunica prima con il punto di accesso wireless (WAP) per richiedere l'autorizzazione alla trasmissione. Il WAP è un dispositivo centrale, come un router, che collega la rete wireless a una rete cablata e controlla l'accesso alla rete. Una volta che il WAP concede l'autorizzazione, il dispositivo di trasmissione invia i dati come segnali RF, che vengono ricevuti dagli adattatori wireless di altri dispositivi sulla rete. I dati vengono quindi riconvertiti in un formato utilizzabile e trasmessi all'applicazione o al sistema appropriato.

Il dispositivo deve inoltre essere configurato con le impostazioni di rete corrette, come il nome della rete/ Service Set Identifier (SSID) e password.

La richiesta al WAPè nota come connection request frame o association request e viene inviata utilizzando il protocollo IEEE 802.11

Il frame di richiesta di connessione contiene vari campi di informazioni, inclusi i seguenti ma non limitati a:

MAC address	Un identificatore univoco per l'adattatore wireless del dispositivo.
SSID	Il nome della rete, noto anche come nome Service Set Identifierdella rete Wi-Fi.
Supported data rates	Un elenco delle velocità dati che il dispositivo può comunicare.
Supported channels	Un elenco delle channels(frequenze) su cui il dispositivo può comunicare.
Supported security protocols	Un elenco dei protocolli di sicurezza che il dispositivo è in grado di utilizzare, ad esempi

1.1 Caratteristiche di sicurezza

Le reti WiFi hanno diverse funzioni di sicurezza per proteggere da accessi non autorizzati e garantire la privacy e l'integrità dei dati trasmessi sulla rete. Alcune delle principali funzionalità di sicurezza includono, a titolo esemplificativo ma non esaustivo:

- Crittografia
- Controllo di accesso
- Firewall

1.1.1 Crittografia

Possiamo utilizzare vari algoritmi di crittografia per proteggere la riservatezza dei dati trasmessi su reti wireless. Gli algoritmi di crittografia più comuni nelle reti WiFi sono Wired Equivalent Privacy (WEP), WiFi Protected Access 2 (WPA2) e WiFi Protected Access 3 (WPA3).

1.1.2 Controllo di accesso

Le reti WiFi sono configurate per impostazione predefinita per consentire ai dispositivi autorizzati di accedere alla rete utilizzando metodi di autenticazione specifici. Tuttavia, questi metodi possono essere modificati richiedendo una password o un identificatore univoco (come un indirizzo MAC) per identificare i dispositivi autorizzati.

1.1.3 Firewall

Un firewall è un sistema di sicurezza che controlla il traffico di rete in entrata e in uscita in base a regole di sicurezza predeterminate. Ad esempio, i router WiFi spesso dispongono di firewall integrati in grado di bloccare il traffico in entrata da Internet e proteggere da vari tipi di minacce informatiche.

1.2 Protocolli di crittografia

Wired Equivalent Privacy (WEP) e WiFi Protected Access (WPA) sono protocolli di crittografia che proteggono i dati trasmessi su una rete WiFi. WPA può utilizzare diversi algoritmi di crittografia, incluso Advanced Encryption Standard (AES).

1.2.1 WEP

WEP utilizza una chiave A 40-bit o a 104-bitper crittografare i dati, mentre WPA usando AES, ne utilizza una a 128-bit (più robusta e più resistenti agli attacchi).

Inoltre, WEP non è compatibile con i dispositivi e i sistemi operativi più recenti e generalmente non è più considerato sicuro. Infine, WEP utilizza l'RC4 cipher algoritmo di crittografia, che lo rende vulnerabile agli attacchi.

WEP utilizza a shared keyper l'autenticazione, il che significa che la stessa chiave viene utilizzata per la crittografia e l'autenticazione.

Esistono due versioni del protocollo WEP che garantiscono chiavi univoche:

- WEP-40/WEP-64 (chiave a 40 bit)
- WEP-104 (chiave a 104 bit)

1.2.2 WPA

WPA fornisce il massimo livello di sicurezza e non è suscettibile agli stessi tipi di attacchi di WEP. Inoltre, WPA utilizza metodi di autenticazione più sicuri, come una chiave precondivisa (PSK) o un server di autenticazione 802.1X, che forniscono una maggiore protezione contro l'accesso non autorizzato. Tutte le reti wireless, specialmente nelle infrastrutture critiche come gli uffici, dovrebbero generalmente implementare almeno a WPA2 o addirittura a WPA3 la crittografia.

1.3 Protocolli di crittografia

Lightweight Extensible Authentication Protocol (LEAP) e Protected Extensible Authentication Protocol (PEAP) sono protocolli di autenticazione utilizzati per proteggere le reti wireless e per fornire un metodo sicuro per l'autenticazione dei dispositivi su una rete wireless, sono spesso utilizzati insieme a WEP o WPA per fornire un ulteriore livello di sicurezza.

Una differenza fondamentale tra LEAP e PEAP è il modo in cui proteggono il processo di autenticazione.

LEAP utilizza a shared keyper l'autenticazione, il che significa che una stessa chiave viene utilizzata per crittografia e autenticazione (meno sicura) mentre PEAP utilizza un metodo di autenticazione più sicuro chiamato Transport Layer Security (TLS). Questo metodo stabilisce una connessione sicura tra il dispositivo e il WAP utilizzando un certificato digitale e un tunnel crittografato protegge il processo di

autenticazione. Ciò fornisce una protezione più solida contro l'accesso non autorizzato ed è più resistente agli attacchi.

1.3.1 TACACS+

TACACS+ è un protocollo utilizzato per autenticare e autorizzare gli utenti che accedono ai dispositivi di rete, come router e switch. Quando un WAP invia una richiesta di autenticazione a un TACACS+ server, la richiesta in genere include le credenziali dell'utente e altre informazioni sulla sessione.

Diversi metodi di crittografia possono essere utilizzati per crittografare la richiesta di autenticazione, ad esempio SSL/ TLSo IPSec. Il metodo di crittografia specifico utilizzato può dipendere dalla configurazione del TACACS+server e dalle capacità del WAP.