SICUREZZA E VULNERABILITA NELLE RETI WIRELESS

Loriggiola Manuel

COSA E’ UNA RETE WIRELESS

Una rete wireless è un tipo di rete che consente la comunicazione tra dispositivi senza l'uso di cavi fisici.

L'elemento centrale di una rete wireless è l'Access Point (AP).

I dispositivi wireless comunicano inviando e ricevendo segnali radio dall’ Access Point, che li collega alla rete cablata o a internet.

Le reti wireless operano principalmente su 2.4 GHz e 5 GHz

VULNERABILITA NELLE RETI WIRELESS

Le reti wireless sono vulnerabili a causa della trasmissione dei dati via aria.
Una delle principali debolezze è WEP (Wired Equivalent Privacy), un protocollo di sicurezza obsoleto e facilmente violabile. Gli attaccanti possono decifrare il traffico protetto da WEP in pochi minuti usando strumenti disponibili pubblicamente, compromettendo così l'intera rete.

VULNERABILITA AL LIVELLO 2

Oltre alle debolezze nei protocolli, le reti wireless sono vulnerabili agli attacchi che sfruttano la connessione tra i dispositivi.

Un esempio è l’attacco MITM (Man-in-the-Middle), in cui un intruso si inserisce nella comunicazione tra due dispositivi, potendo così intercettare, leggere o alterare i dati.

Un altro attacco comune è l'Evil Twin, dove un malintenzionato crea una rete Wi-Fi falsa che imita una rete legittima, ingannando gli utenti e rubando informazioni personali.

ATTACCO MITM ESEMPIO CONCRETO

Attacco Man-in-the-Middle (MITM) su una rete Wi-Fi pubblica

Un esempio classico di vulnerabilità in una rete Wi-Fi pubblica è l'attacco Man-in-the-Middle (MITM). In questo tipo di attacco, un hacker può facilmente "inserirsi" tra un utente e la rete.

Ad esempio, se un utente si connette a una rete Wi-Fi pubblica non protetta, un attaccante potrebbe rubare dati sensibili, come credenziali bancarie o password. Questo dimostra quanto sia importante proteggere le proprie informazioni e utilizzare VPN e crittografia per evitare intercettazioni su reti non sicure.

VULNERABILITA A LIVELLO 3

Le reti sono vulnerabili anche a livello di traffico e instradamento dei dati.

Un attacco DDoS (Distributed Denial of Service) mira a sovraccaricare una rete o un server con traffico in eccesso, impedendo l'accesso ai legittimi utenti.

Inoltre, un attacco al routing può deviare i dati verso percorsi controllati dagli attaccanti, permettendo loro di rubare informazioni sensibili o compromettere la sicurezza della rete.

SOLUZIONI TECNICHE: WPA

WEP, il primo protocollo di sicurezza, è vulnerabile a attacchi di forza bruta ed è ormai obsoleto.

WPA ha migliorato la sicurezza introducendo TKIP, ma rimane suscettibile a cracking delle chiavi, quindi non è sufficientemente sicuro.

SOLUZIONI TECNICHE: WPA2

WPA2, con AES per crittografia avanzata, ha migliorato notevolmente la sicurezza. Tuttavia, è ancora vulnerabile a attacchi che possono compromettere la rete.

SOLUZIONI TECNICHE: WPA3

WPA3 migliora ulteriormente con SAE, proteggendo meglio contro attacchi MITM e il cracking delle password. Tuttavia, richiede hardware compatibile, limitando la sua adozione.

ALGORITMI DI CIFRATURA E CONTROLLO

Gli algoritmi di controllo e cifratura sono essenziali per la protezione delle reti wireless.

Algoritmi di Cifratura:

- AES (Advanced Encryption Standard): Algoritmo di cifratura avanzato che rende i dati illeggibili a chi non possiede la chiave corretta.

Algoritmi di Controllo:

- TKIP (Temporal Key Integrity Protocol): Algoritmo utilizzato nelle versioni più vecchie di WPA per garantire l'integrità dei dati trasmessi.
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol): Algoritmo di controllo utilizzato per garantire una protezione robusta nei sistemi WPA2 e WPA3.

PRIVACY NELLE RETI PUBBLICHE E RESPONSABILITA NELLE CONDIVISIONI DI RETI WIRELESS

- Le reti Wi-Fi pubbliche sono vulnerabili e mettono a rischio la privacy degli utenti, poiché i dati trasmessi possono essere facilmente intercettati.
- Gli utenti devono essere consapevoli di questi rischi e adottare misure di sicurezza come l'uso di VPN o crittografia.
- Chi condivide una rete wireless ha la responsabilità di proteggerla, configurando adeguatamente password e firewall per evitare che dati sensibili possano essere accessibili da altri utenti.

DIGITAL DIVIDE E ACCESSO ALLE RETI PUBBLICHE

Il digital divide è la disuguaglianza che fa sì che alcune persone non possiedano accesso a Internet o ai dispositivi necessari per usarlo. Le reti Wi-Fi pubbliche possono ridurre questa disuguaglianza, ma spesso non sono sicure o facili da usare per tutti.

È importante che tutti possano accedervi in modo sicuro.

SOSTENIBILITA RETI MESH COMUNITARIE

Le reti mesh comunitarie sono reti wireless decentralizzate, dove ogni nodo (utente) aiuta a trasmettere il segnale.

Queste reti possono ridurre i costi di accesso a Internet e migliorare la connettività nelle aree meno servite.

Sono anche più sostenibili, perché usano meno energia e hardware rispetto alle reti tradizionali.

CRITICHE PERSONALI

Anche con tecnologie come WPA e AES, molte persone non si rendono conto dei rischi delle reti pubbliche. Inoltre, non tutti hanno accesso a Internet sicuro, e questo crea una disparità digitale. Penso che dovremmo essere più consapevoli e responsabili quando usiamo queste tecnologie.

CONCLUSIONE

Le reti wireless sono utili, ma senza sicurezza diventano pericolose. Credo che dobbiamo lavorare per garantire che tutti possano avere una connessione sicura e che la gente impari a proteggere i propri dati.