SICUREZZA NELLE RETI WIRELESS

GUADAGNO Alessio 5TI

Cosa sono le Wireless?

Per wireless si indica un insieme di tecnologie che consentono l’accesso via radio alla rete e alle risorse condivise.

Che protocolli utilizza la tecnologia Wireless?

Questa tecnologia è tuttora in continua evoluzione, per questo negli anni sono stati sviluppati vari protocolli.
L'associazione internazionale che sviluppa e brevetta questi protocolli è l'IEEE e tutti i protocolli sono denominati IEEE 802.11xx

Standard	Bit rate massimo	Throughput massimo	Frequenze e Banda	Anno di ratifica
802.11a	54 Mbit/s	25 Mbit/s	5 Ghz B= 20 Mhz	1999 (solo per aziende)
802.11b	11 Mbit/s	6 Mbit/s	2.4 Ghz B= 22 Mhz	1999
802.11g	54 Mbit/s	22 Mbit/s	2.4 Ghz B= 20 Mhz	2003
802.11n	300 Mbit/s	210 Mbit/s	2.4 Ghz/ 5 Ghz B= 20 / 40 Mhz	2009
802.11ac	1,3 Gbit/s	910 Mbit/s	5 Ghz B= 80 o 160 Mhz	2013

Che metodi esistono per mettere in sicurezza una rete Wireless

Per mettere in sicurezza una rete wireless esistono due procedure:

- Tramite autenticazione → Si basa sul riconoscimento del dispositivo;
- Tramite crittografia → Si basa su di una tecnica di cifratura della connessione.

Le tecniche impiegabili nelle WLAN per garantire sia l'autenticazione che la crittografia sono:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2

WEP (Wired Equivalent Privacy)

Caratteristiche:

- Utilizzato negli Open-System con il metodo Shared Key ossia è l'AP ad accettare il dispositivo e non viceversa
- Si occupa di cifrare il traffico tra dispositivo e Access Point
- Chiavi lunghe al massimo 64 bit →Chiavi statiche per tutti i soggetti connessi alla rete

Svantaggi:

- Chiavi non sufficientemente lunghe, con alte probabilità di decifrare il messaggio
- Non supporta le chiavi dinamiche obbligando l'amministratore a modificarle manualmente → Per questo utilizzato con il sistema MAC filtering
- Del pacchetto TCP/IP cripta solo la parte dei dati e non la parte dell'intestazione → ciò comporta una facilità di decriptazione del messaggio

WPA (Wi-Fi Protected Access)

Introdotto principalmente per ovviare ai problemi del WEP, il WPA vi si distingue prevalentemente per i seguenti motivi:

- le chiavi hanno una lunghezza di 128 bit;
- le chiavi sono dinamiche, cioè sono diverse per ogni utente, per ogni sessione e per ogni pacchetto inviato;
- le chiavi vengono distribuite in modo automatico, non richiedendo nessun intervento manuale da parte dell'amministratore di rete;
- prevede un meccanismo di autenticazione degli utenti.

Il WPA basa il proprio funzionamento su tre componenti fondamentali:

- TKIP (Temporal Key Integrity Protocol) come algoritmo di crittografia;
- 802.1X/EAP (Exstensible Authentication Protocol) come schema di autenticazione;
- MIC (Message Integrity Check) come strumento per garantire l'integrità dei messaggi scambiati.

WPA2 (Wi-Fi Protected Access 2)

Come funzionalità è identico alla versione originaria, l'unica differenza è che introduce un nuovo sistema di criptografia denominata AES (Adavanced Encryption Standard), che essendo più sicuro richiede un supporto hardware performante per essere utilizzato

MAC Filtering

→Il MAC filter costituisce un ulteriore livello di sicurezza;

→Sfruttando gli indirizzi MAC, univoci per ogni dispositivo, consente e nega l'accesso alla rete;

→Esistono due tipi di liste con funzioni diverse:

- Whitelist;
- Blacklist.

FINE

GUADAGNO Alessio

5TI