RETI WIRELESS

Le reti wireless possono utilizzare onde radio o segnali infrarossi per comunicare e vengono classificate in base alla loro estensione (come le reti wired)

- **WPAN** (Wireless Personal Area Network)
- **WLAN** (Wireless Local Area Network)
- **WMAN** (Wireless Metropolitan Area Network)
- **WWAN** (Wireless Wide Area Network)

WPAN

- Coprono il campo d'azione di una persona (fino a 10-15 metri)
- La maggior parte usa le onde radio
  - **Bluetooth** (frequenza libera ISM a 2,4 GHz), 2 Mb/s
- Altre usano gli infrarossi (fino a 3 metri, dispositivi **Line of Sight (LoS)**)
  - **IrDA** (Infrared Device Applcation), 4 Mb/s

WLAN

- Sono simili alle LAN cablate
- Lo standard più diffuso è IEEE 802.11
- Sono composte da:
  - **Wireless Terminal (WT)** → dispositivi mobile (pc, tablet, smartphone)
  - **Access Point (AP)** → agisce da bridge (wired-wireless) e da gateway

- AP + WT = **BSS (Basic Service Set)** → costituisce una **cella**
- È possibile collegare + più AP alla rete → **Wireless Distribution System**
- 2 o più BSS collegati da un WDS → **ESS (Extended Service Set)**

All'interno di un ESS **i diversi BSS possono essere collocati:**

- **BSS parzialmente sovrapposti** → copertura continua
- **BSS fisicamente disgiunti**
- **BSS co-locati** → diversi BSS nella stessa area (ridondanza / + prestazioni)

Lo standard 802.11 gestisce la mobilità delle stazioni distinguendo **3 tipi di transizioni:**

- **Transizione statica:** immobile o si sposta nell'area di 1 singolo BSS
- **Transizione tra BSS:** la stazione si sposta tra 2 BSS parzialmente sovrapposti
- **Transizioni tra ESS:** la stazione si sposta tra BSS appartenenti a 2 ESS diversi

La **configurazione di un AP:**

- **SSID (Service Set Identifier)**: nome assegnato alla WLAN, inviato con il beacon
- **Potenza**: **l'EIRP (Effective Isotropic Radiated Power)**, potenza dell'antenna
- **Canale:** (1-13), bisogna applicare la regola del 5 per non farli sovrapporre
- **Crittografia:** standard **WEP (Wireless Equivalent Privacy)**
- **Incapsulamento:** se l'AP è anche router
- **NAT e DHCP**

Oltre le WLAN aziendali e domestiche ci sono le **MANET (Mobile Ad hoc NETwork)**, usate dove non è possibile installare un AP (es. WI-FI Direct)

WMAN

- Distribuire dati tramite un'antenna
- Connessione di tipo:
  - Point-to-point (brighe → 2 antenna collegate alla rete cablata)
  - Point-to-multipoint (1 antenna omnidirezionale + N antenne unidirezionali)

WWAN

- Coprono uno spazio molto ampio come uno stato o un continente
- Queste tecnologie sono offerte da **WISP (Wireless Internet Service Provider)**

Attacchi nelle reti wireless

Sniffing: intercettazione passiva dei dati che transitano in rete. Usato per monitorare il traffico o intercettare in maniera fraudolenta i dati sensibili. Gli sniffer intercettano i singoli pacchetti, decodificano gli header dei vari livelli e ricostruiscono lo scambio di dati tra le applicazioni.

- **Scopi legittimi:** individuazione delle congestioni di rete o tentativi di intrusione
- **Scopi illeciti:** intercettazione di password, numeri di carte di credito, …

Accesso non autorizzato: a una rete privata senza autorizzazione. La tecnica più utilizzata è quella di servirsi di un **Access Point Rouge (APR)** cioè un AP non autorizzato. Per ostacolarlo è necessaria l'autenticazione reciproca tra i WT e gli AP. Inoltre, gli AP devono eseguire l'autenticazione con gli SW, impedendo la connessione di un APR.

I **wardriver** infrangono le scarse misure di sicurezza delle reti private per navigare gratis

Sostituzione del SID (Security IDentifier) (spoofing): Ad ogni account viene assegnato un identificativo SID a cui vengono associate autorizzazioni precise. La sostituzione del SID avviene posizionando un WTR intermedio tra un utente e AP. Questo tipo di attacco può sfruttare il protocollo ARP.

Lo **spoofing** è un tipo di attacco informatico in cui si realizza la falsificazione dell'identità. Questo attacco può avvenire in qualsiasi livello della pila ISO/OSI.

Per evitare lo spoofing, si può usare il protocollo **SARP (Secure ARP)**, che fornisce un tunnel protetto tra client e AP o router. Questo protocollo permette all'AP di ignorare ogni risposta non associata al client posto esattamente all'altra estremità.

Attacco DoS (Denial of Service): capace di paralizzare o disattivare una rete wireless, rendendola indisponibile per un periodo di tempo indeterminato. Usa attacchi **brute force**, oppure attacchi che utilizzano forti segnali radio che si sovrappongono ai segnali della rete rendendo inutilizzabili AP e WT

Crittografia WEP (Wired Equivalent Privacy):
WEP viene implementata a livello MAC ed è supportata dalla maggior parte dei dispositivi mobili e AP. Viene crittografato il payload del frame da trasmettere utilizzando l'algoritmo di cifratura a flusso (a chiave simmetrica) **RC4**.

Crittografia TKIP (Temporal Key Integrity Protocol):
Evoluzione del WEP, mantiene l'RC4, ma parte con una chiave temporale a 128 bit condivisa tra WT e AP (simmetrica). Alla chiave temporale combinata con l'indirizzo MAC del WT, si aggiunge un IV di altri 128 bit per creare la chiave di crittografia dei dati. Questa chiave viene rigenerata a ogni pacchetto o a ogni burst (raffica) di pacchetti inviati. **(distribuzione dinamica delle chiavi).**

TKIP > WEP → temporalità della chiave e > lunghezza dell'IV

Crittografia AES (Advanced Encryption Standard):
Alternativa a TKIP che garantisce una crittografia più sicura. AES è ritenuto indecifrabile **(uncrackable)** grazie all'utilizzo dell'algoritmo di **crittografia a blocchi Rijndael** al posto dell'RC4. Lo svantaggio di AES è che richiede una grande capacità di elaborazione (non tutti gli AP in commercio possono supportare).

WPA:

Nel 2018 la Wi-Fi Alliance ha introdotto un programma di certificazione per il WPA3, con l'obbiettivo di fornire miglioramenti e nuove funzionalità di sicurezza, tra cui il blocco degli attacchi basati su KRAC (riusciti su WPA2).