La Sicurezza nelle Reti Wireless

LA SICUREZZA NELLE RETI WIRELESS

Garantire la sicurezza nelle reti wireless è di fondamentale importanza soprattutto perché i segnali si propagano attraverso un mezzo impossibile da isolare come l'aria. È quindi necessario che chi utilizza le reti wireless sia consapevole dei problemi e delle contromisure necessarie. In questa Lezione affronteremo i **rischi** a cui sono sottoposte le reti wireless e le tecniche per rafforzare la sicurezza mediante **crittografia** e **autenticazione**.

LA SICUREZZA NELLE RETI WIRELESS

Sniffing

Attività di intercettazione passiva dei dati che transitano in una rete. Usato per monitorare il traffico o intercettare in maniera fraudolenta i dati sensibili. I software per lo sniffing, oltre a memorizzare il traffico, offrono funzionalità di analisi del traffico stesso.

LA SICUREZZA NELLE RETI WIRELESS

Sniffing

Può essere usato per scopi **legittimi** (analisi ed individuazioni delle congestioni di rete o tentativi di intrusione), oppure per scopi **illeciti** (intercettazione di password, numeri di carte di credito, altre informazioni sensibili).

LA SICUREZZA NELLE RETI WIRELESS

Sniffing

Gli *sniffer* intercettano i singoli pacchetti, decodificano gli header dei vari livelli e ricostruiscono lo scambio di dati tra le applicazioni. Solo l'utilizzo di efficaci meccanismi di crittografia consente di mantenere la segretezza dei dati.

LA SICUREZZA NELLE RETI WIRELESS

Accesso non autorizzato

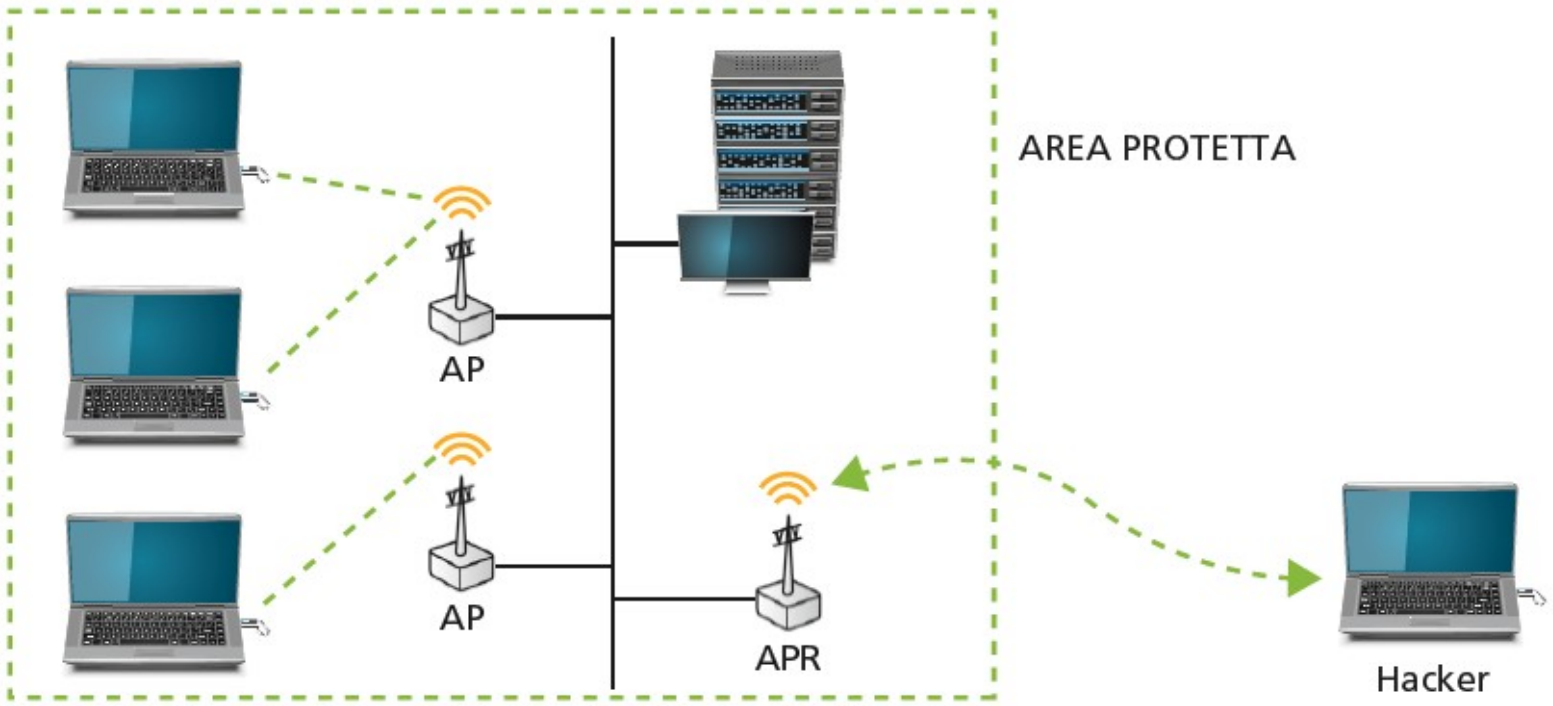
Accesso a una rete privata senza esplicita autorizzazione.

La tecnica più utilizzata è quella di servirsi di un **Access Point Rouge** (**APR**) cioè un AP non autorizzato.

Ad esempio un dipendente che acquista ed installa un AP non autorizzato, privo di adeguata crittografia, rende la rete aziendale vulnerabile rispetto ad accessi esterni.

LA SICUREZZA NELLE RETI WIRELESS

Accesso non autorizzato



LA SICUREZZA NELLE RETI WIRELESS

Accesso non autorizzato

Per ostacolare l'accesso non autorizzato, è necessaria l'autenticazione reciproca tra i WT e gli AP.

Inoltre gli AP devono eseguire l'autenticazione con gli switch, in modo da impedire la connessione di un APR.

LA SICUREZZA NELLE RETI WIRELESS

Accesso non autorizzato

I **wardriver** infrangono le scarse misure di sicurezza delle reti private, soprattutto domestiche, per navigare gratis ad alta velocità. Accedendo alla rete wireless diventa possibile esplorare le risorse di qualsiasi altro host collegato alla medesima rete.

Il **wardriving** è un'attività che consiste nell'intercettare reti Wi-Fi, girando in automobile, in bicicletta o a piedi, con un laptop, solitamente abbinato a un ricevitore GPS per individuare l'esatta posizione della rete trovata ed eventualmente pubblicarne le coordinate geografiche su un sito web.
I wardriver operano in maniera lecita se si limitano a trovare un Access Point e a registrarne la posizione.

LA SICUREZZA NELLE RETI WIRELESS

Sostituzione del SID (Security IDentifier): spoofing

In una rete, ad ogni account viene assegnato un **identificativo SID univoco** a cui vengono associate, dall'amministratore della rete, autorizzazioni ben precise.

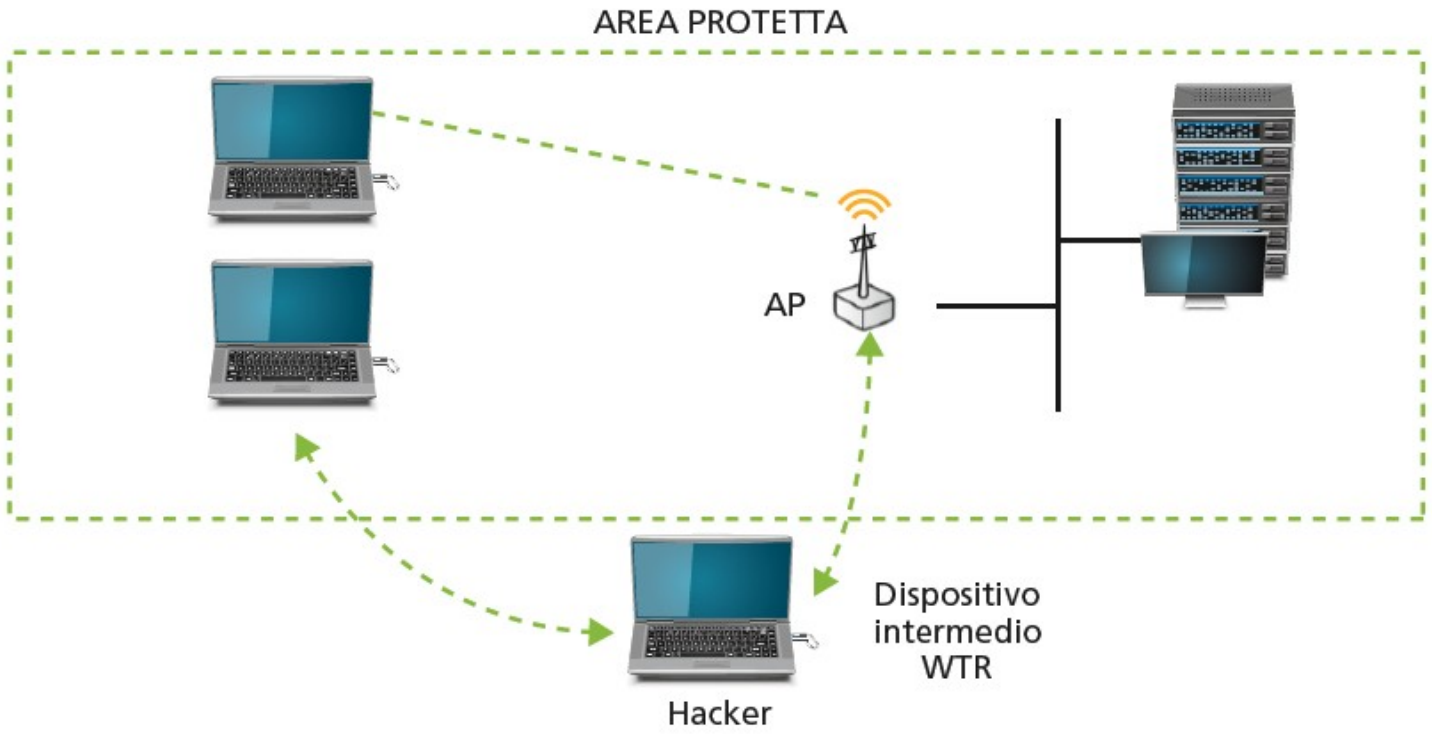
LA SICUREZZA NELLE RETI WIRELESS

Sostituzione del SID (Security IDentifier): spoofing

Sostituzione del SID avviene posizionando un **WTR** (Wireless Terminal Rouge) intermedio tra un utente della rete wireless ed un Access Point della stessa rete. Questo tipo di attacco può sfruttare il protocollo ARP mettendo in atto lo **spoofing ARP**.

LA SICUREZZA NELLE RETI WIRELESS

Sostituzione del SID (Security IDentifier): spoofing

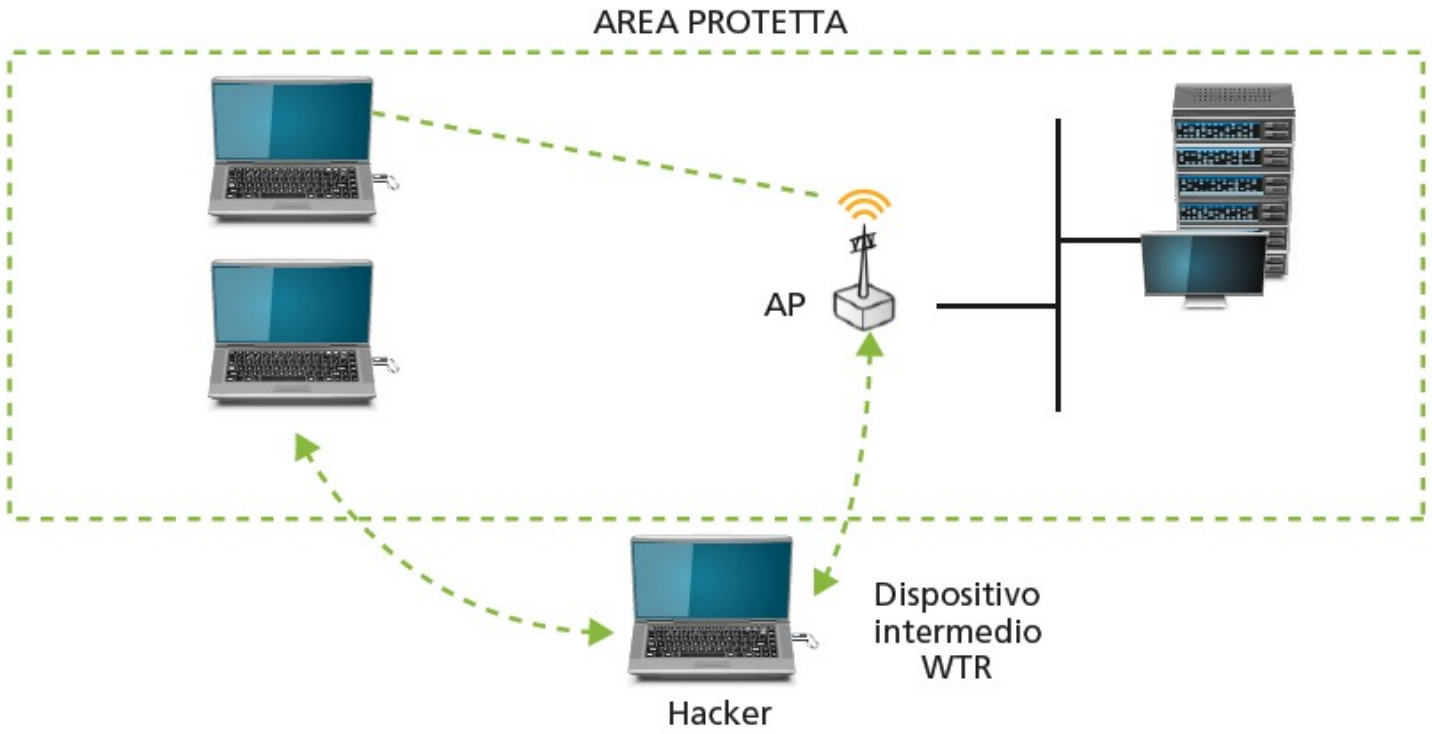


Lo **spoofing** è un tipo di attacco informatico in cui si realizza la falsificazione dell'identità.

Lo spoofing può avvenire in qualsiasi livello della pila ISO/OSI

LA SICUREZZA NELLE RETI WIRELESS

Sostituzione del SID (Security IDentifier): spoofing



Per effettuare lo spoofing ARP, è sufficiente che un dispositivo esterno invii all'AP della rete un pacchetto contenente il proprio indirizzo MAC e l'indirizzo IP del WT a cui vuole sostituirsi.

LA SICUREZZA NELLE RETI WIRELESS

Sostituzione del SID (Security IDentifier): spoofing

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 posto all'estremità del tunnel, di ignorare ogni risposta non associata al client posto esattamente all'altra estremità.

LA SICUREZZA NELLE RETI WIRELESS

Attacco DoS (Denial of Service)

Tipo di attacco capace di paralizzare o disattivare una rete wireless, rendendola indisponibile per un periodo di tempo indeterminato.

In generale il DoS è un attacco di tipo *brute force* (forza bruta) in cui un numero elevatissimo di pacchetti viene inviato, per esempio, a un server web, o FTP o di posta elettronica con lo scopo di impedire agli utenti l'accesso e l'utilizzo di quei servizi.
Per rendere più efficace l'attacco, vengono utilizzati molti computer inconsapevoli, detti zombie, sui quali precedentemente è stato caricato un programma appositamente creato e che si attiva a un comando del cracker creatore.

LA SICUREZZA NELLE RETI WIRELESS

Attacco DoS (Denial of Service)

Usa attacchi **brute force**, oppure attacchi che utilizzano **forti segnali radio** che si sovrappongono ai segnali della rete rendendo inutilizzabili gli AP e i wireless terminal.

I protocolli IEEE 802.11 permettono al segnale dell'attacco Dos di accedere al supporto senza limiti di tempo.

LA SICUREZZA NELLE RETI WIRELESS

Attacco DoS (Denial of Service)

Per contro, un simile tipo di attacco è piuttosto rischioso per chi lo mette in atto poiché la fonte è di facile identificazione, utilizzando gli strumenti di rilevazione forniti con gli analizzatori di rete.

In generale è possibile proteggere una LAN wireless dagli attacchi DoS proteggendo l'edificio dai segnali radio esterni mediante una serie di accorgimenti:

- verificare che le travi metalliche nelle pareti interne siano state messe a terra;
- montare finestre con isolamento termico basato su film in rame o metallici;
- utilizzare vetri oscurati al posto di veneziane o tende;
- utilizzare vernici a base metallica per le pareti interne ed esterne;
- indirizzare le antenne direzionali degli AP verso l'interno;
- regolare la potenza dei trasmettitori allo scopo di limitare la dispersione.

LA SICUREZZA NELLE RETI WIRELESS

Attacco DoS (Denial of Service)

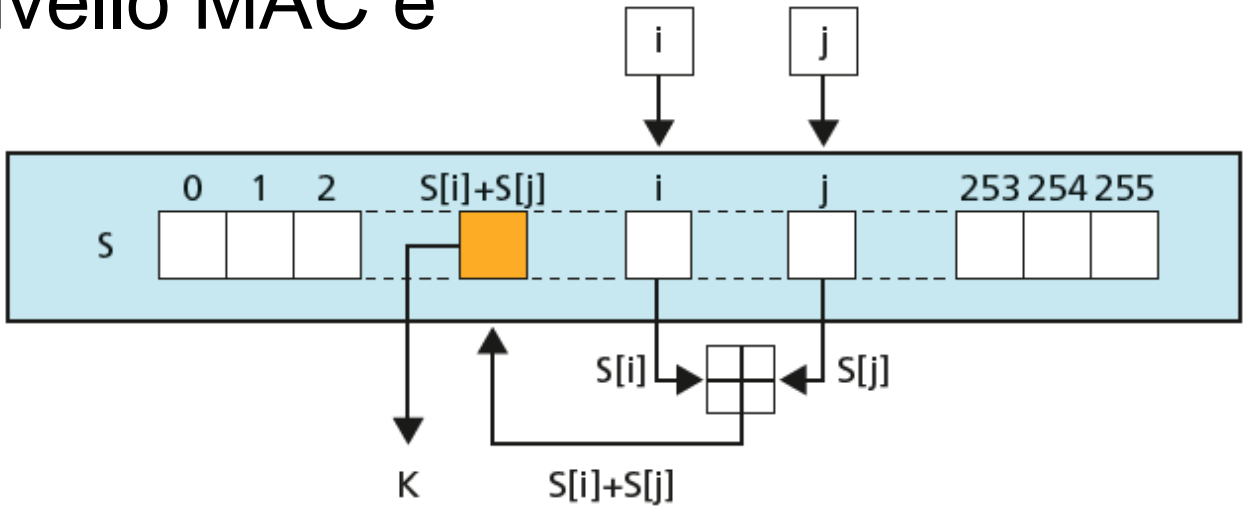
Un attacco DoS può, in certi casi, essere **non intenzionale**. Per esempio, una rete wireless con standard 802.11g, funzionando in uno spettro radio piuttosto affollato (cellulari, microonde e Bluetooth), può essere soggetta a interferenze tanto forti da impedire il funzionamento della rete stessa.

Per proteggersi dai rischi per la sicurezza, occorre mettere in campo tecniche crittografiche e di autenticazione.

LA SICUREZZA NELLE RETI WIRELESS

Crittografia WEP (**Wired Equivalent Privacy**)

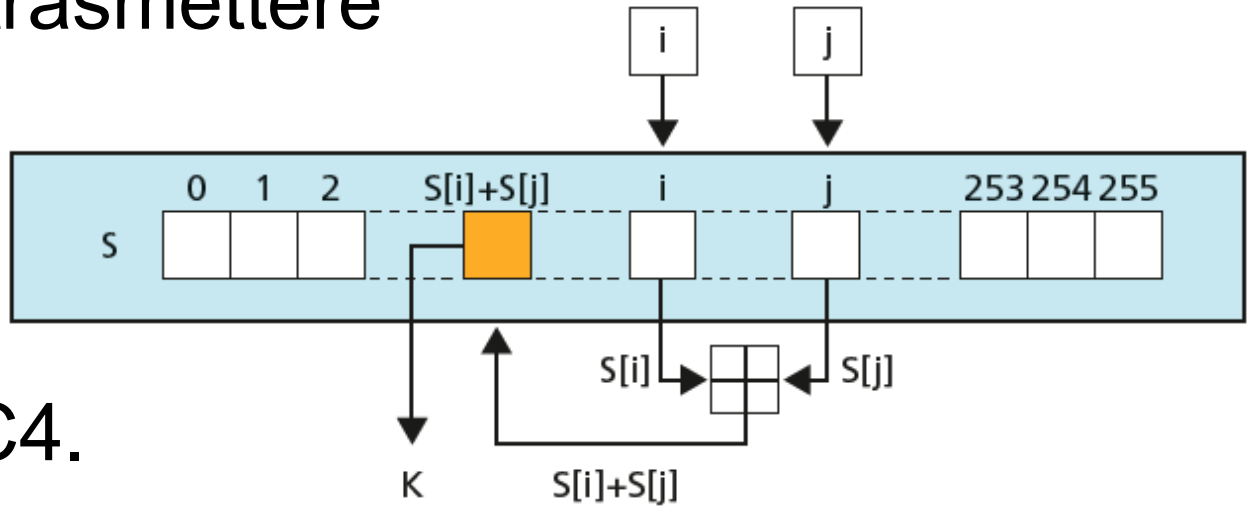
WEP è una tecnica di crittografia a chiave **simmetrica** a flusso, implementata a livello MAC e supportata dalla maggior parte dei dispositivi mobili e AP



LA SICUREZZA NELLE RETI WIRELESS

Crittografia WEP (**Wired Equivalent Privacy**)

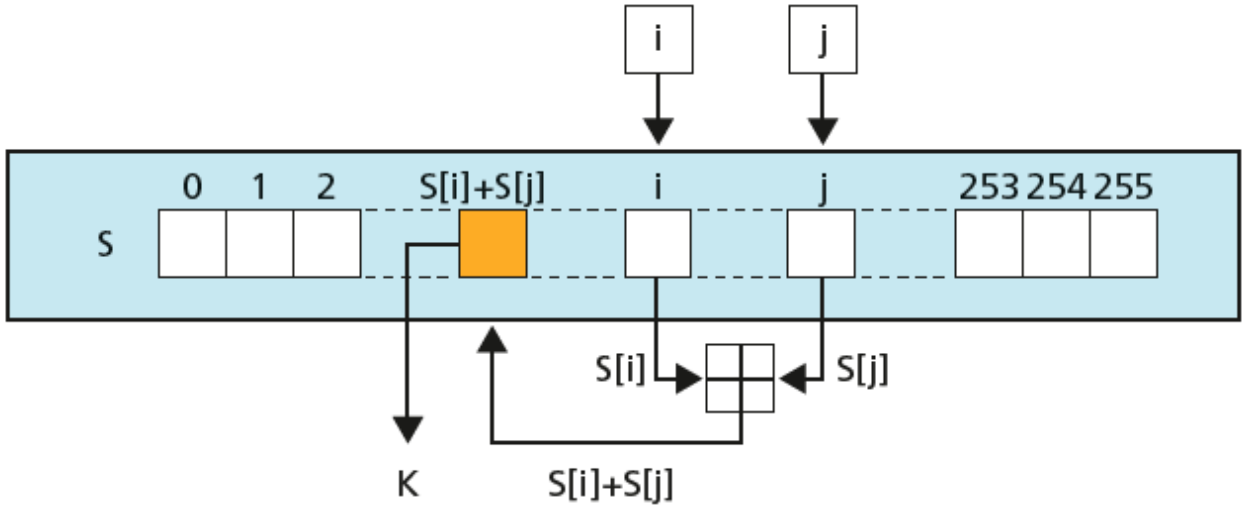
Quando è attivata WEP, viene crittografato il payload del frame da trasmettere utilizzando l'algoritmo di cifratura a flusso, a chiave simmetrica, RC4.



LA SICUREZZA NELLE RETI WIRELESS

Crittografia WEP (Wired Equivalent Privacy)

RC4 genera un flusso di bit pseudo casuali (*key-stream*) mediante una S-box di 256 byte e due indici da 8 bit, generalmente identificati con le lettere *i* e *j* (figura 3).
La chiave di cifratura è generalmente lunga da 40 a 256 bit ed è utilizzata per inizializzare l'S-box mediante una funzione di *scheduling* della chiave.
Il Wireless Terminal ricevente o l'Access Point, eseguono la decrittografia all'arrivo del frame, di conseguenza il segnale viaggia crittografato solo tra due nodi wireless 802.11.



LA SICUREZZA NELLE RETI WIRELESS

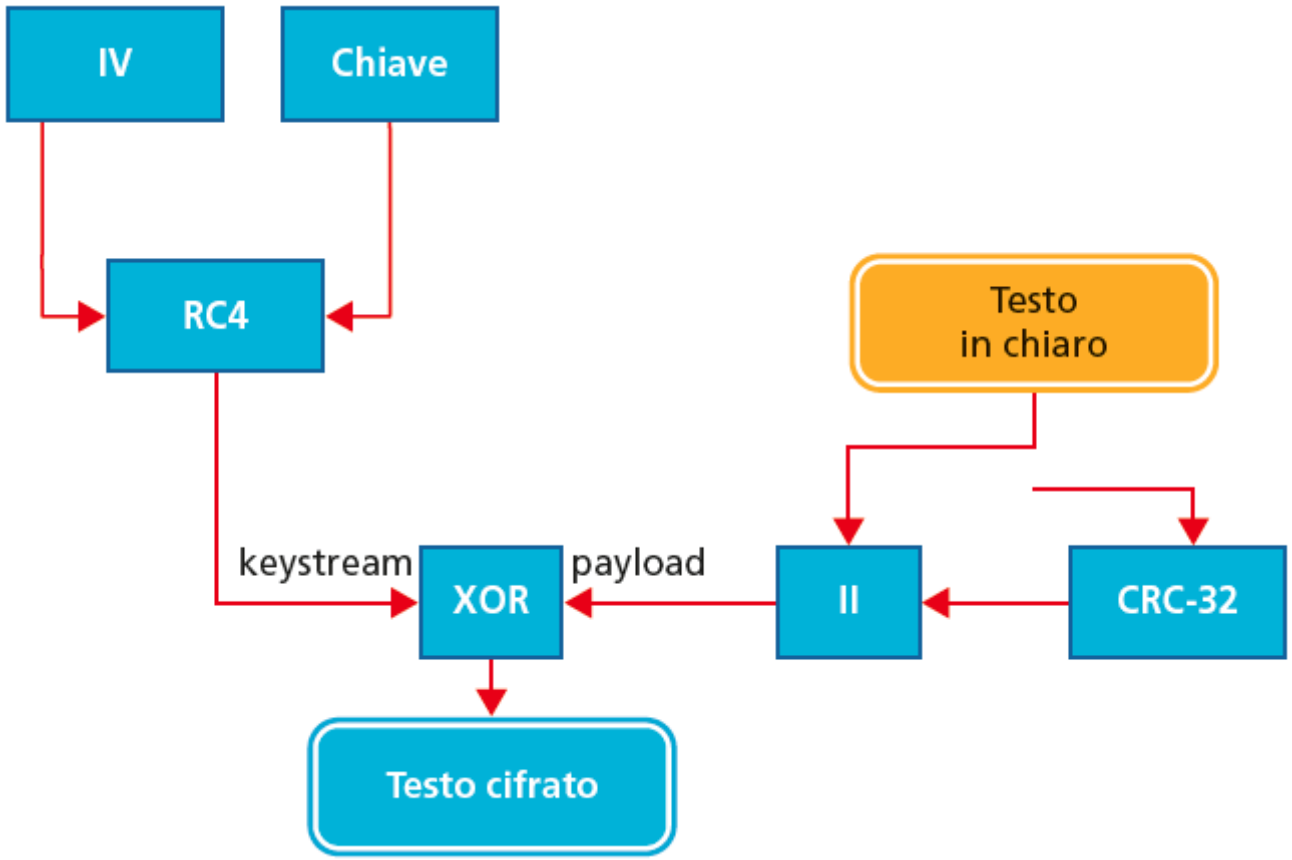
Crittografia WEP (Wired Equivalent Privacy)

Quando entra nella parte cablata della rete, WEP non si applica più.
WEP si basa su una chiave di crittografia assegnata a ogni utente per collegarsi all'Access Point con dati crittografati. Le chiavi sono da 10 cifre esadecimali (40 bit) o da 26 esadecimali (104 bit) corrispondenti alla crittografia rispettivamente a 64 o 128 bit per via dell'aggiunta, in entrambi i casi, di un vettore d'inizializzazione (IV, *Initialization Vector*) a 24 bit.
WEP, essendo a **chiave simmetrica**, utilizza la **stessa chiave** per crittografare e decrittografare, e di conseguenza ogni WT e ogni AP deve essere configurato con la stessa chiave.

LA SICUREZZA NELLE RETI WIRELESS

La tecnica WEP con RC4 agisce in 5 passi

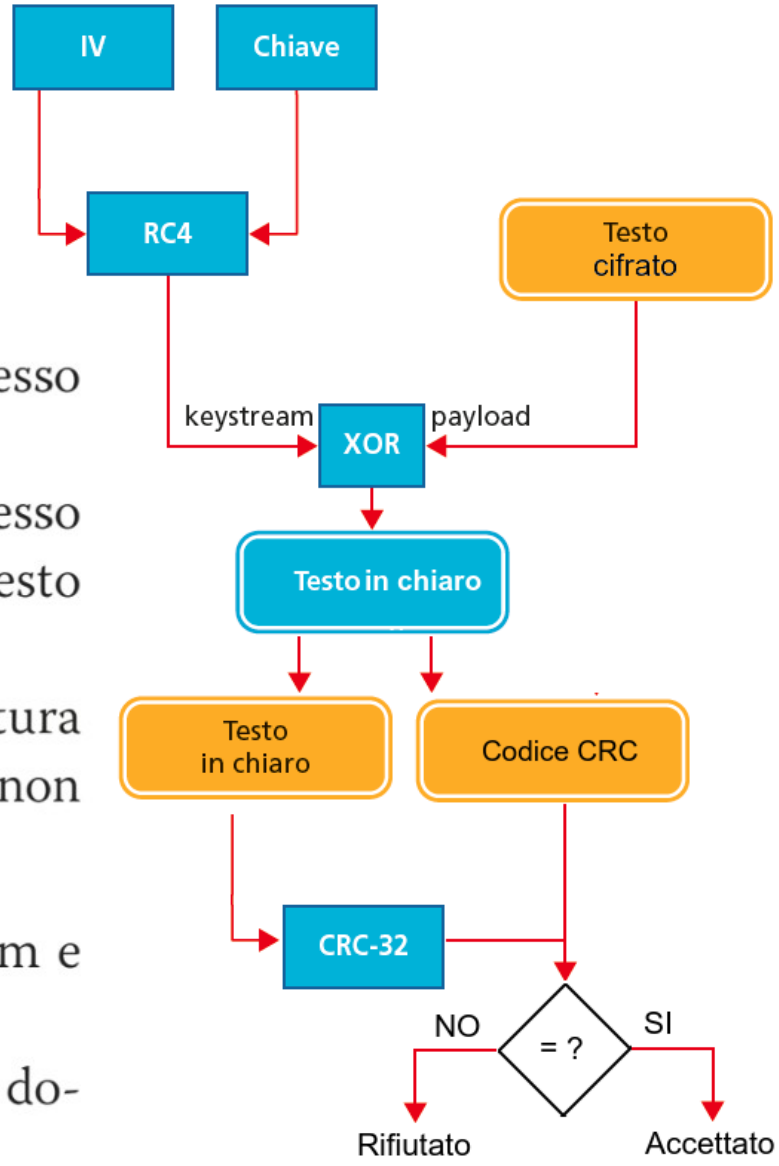
1. L'IV a 24 bit, generato in modo casuale, verrà trasmesso in chiaro (non crittografato) nei primi byte del frame.
2. L'IV viene combinato con la chiave di cifratura segreta dell'utente creando una sequenza di chiavi.
3. Mediante tale sequenza, RC4 crea un flusso di bit pseudocasuali della stessa lunghezza del payload.
4. Il payload viene composto con il testo in chiaro e l'aggiunta dei bit di check calcolati con CRC-32 (Cyclic Redundancy Code a 32 bit).
5. Viene eseguita un'operazione di XOR tra keystream e payload ottenendo il frame crittografato da inviare.



LA SICUREZZA NELLE RETI WIRELESS

Essendo XOR simmetrico e l'IV in chiaro, il destinatario potrà procedere nello stesso modo per l'operazione di decrittografia.
La modifica dell'IV può essere impostata per essere effettuata a ogni frame trasmesso (operazione non richiesta dallo standard 802.11, ma fortemente consigliata) e questo rende più difficile la decrittografia non autorizzata.
La chiave di crittografia resta invece uguale per lunghi periodi (a volte addirittura anni) salvo interventi da parte dell'amministratore di rete. Il protocollo di per sé non ne prevede la modifica.

La dimensione relativamente piccola dell'IV, la forte correlazione tra keystream e chiave e le chiavi statiche rendono WEP particolarmente vulnerabile.
In definitiva, WEP rappresenta il livello minimo di sicurezza, adeguato per reti domestiche o piccoli uffici.



LA SICUREZZA NELLE RETI WIRELESS

Crittografia TKIP (**Temporal Key Integrity Protocol**)

Evoluzione del WEP, utilizza ancora 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. Tale chiave viene rigenerata a ogni pacchetto o a ogni burst (raffica) di pacchetti inviati. Si ha quindi una **distribuzione dinamica delle chiavi**.

LA SICUREZZA NELLE RETI WIRELESS

Crittografia TKIP (**Temporal Key Integrity Protocol**)

TKIP è più robusto di WEP, cioè più difficile da violare, sia per la temporalità della chiave, sia per la maggior lunghezza dell'IV. È possibile passare da WEP a TKIP attraverso semplici patch del firmware dei WT e degli AP. I dispositivi WEP possono comunque dialogare con dispositivi TKIP.

LA SICUREZZA NELLE RETI WIRELESS

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, capacità che non tutti gli AP in commercio possono supportare.

LA SICUREZZA NELLE RETI WIRELESS

Crittografia WPA (Wi-Fi Protected Access)

Lo standard WPA distribuito dalla Wi-Fi Alliance è un aggiornamento WEP dotato di distribuzione dinamica delle chiavi e autenticazione reciproca.
La distribuzione dinamica è realizzata includendo TKIP in WPA e prende il nome di *WPA 1.0*. Wi-Fi Alliance ha poi introdotto i termini *WPA 2.0-Personal* e *WPA 2.0-Enterprise* per differenziare le due classi di sicurezza fornite dai prodotti wireless. I WPA 2.0-Personal utilizzano una PSK (*passphrase*) di autenticazione condivisa mentre i WPA 2.0-Enterprise utilizzano un server di autenticazione.

LA SICUREZZA NELLE RETI WIRELESS

Nel 2018 la Wi-Fi Alliance ha introdotto un programma di certificazione per il **WPA3**, con l'obietivo di fornire miglioramenti e nuove funzionalità di sicurezza tra cui il blocco degli attacchi basati su **KRACK** (Key Reinstallation Attacks) a cui il protocollo WPA2 è risultato vulnerabile.

KRACK: chi effettua questo attacco, si intromette, con una tecnica *man in the middle* (cioè si interpone nello scambio di messaggi), forzando a generare una chiave composta di soli 0. Questo rende facile decrittare i dati in arrivo e in partenza. E non importa come siano crittografati i dati una volta che viaggiano in rete, perché l'attacco li prende di mira prima che partano (nel caso il dispositivo mobile li trasmetta) o dopo il loro arrivo (nel caso il dispositivo mobile li riceva).

LA SICUREZZA NELLE RETI WIRELESS

La Wi-Fi Alliance ha previsto due versioni anche di WPA3.

1. **WPA3-Personal** è ottimizzato per reti piccole (tipo reti domestiche) garantendo la sicurezza tramite il protocollo **SAE** (**Simultaneous Authentication of Equals**) che prevede una tecnica di scambio della password peer-to-peer (quindi diretta tra i dispositivi e non delegata a una certification authority) in grado di garantire una sicurezza equivalente a quella di una crittografia tramite certificato. Questo nuovo sistema di sicurezza sarà inoltre immune da attacchi brute force che tentano tutte le combinazioni di parole note. WPA3-Personal è quindi sicuro anche se la password dell'utente risultasse essere troppo debole.

LA SICUREZZA NELLE RETI WIRELESS

2. **WPA3-Enterprise** è invece pensato per grandi installazioni Wi-Fi e permette la cifratura a 192 bit, allineata alla suite CNSA (Commercial National Security Algorithm), che soddisferà le esigenze di tutela delle reti in ambito governativo, industriale e nel settore della difesa.

Il nuovo standard, pensato per durare anni, è chiaramente rivolto anche al futuro e al mondo dei dispositivi della Internet of Things (IoT). Per questo motivo è stato introdotto **Wi-Fi Easy Connect**, un nuovo protocollo di connessione per reti WPA2 e WPA3, che semplifica la connessione dei dispositivi molto essenziali, in particolar modo quelli senza display. Easy Connect utilizza un dispositivo terzo dotato di un'interfaccia più completa (come potrebbe essere uno smartphone o un tablet) per scannerizzare un codice di sicurezza **QR**.

LA SICUREZZA NELLE RETI WIRELESS

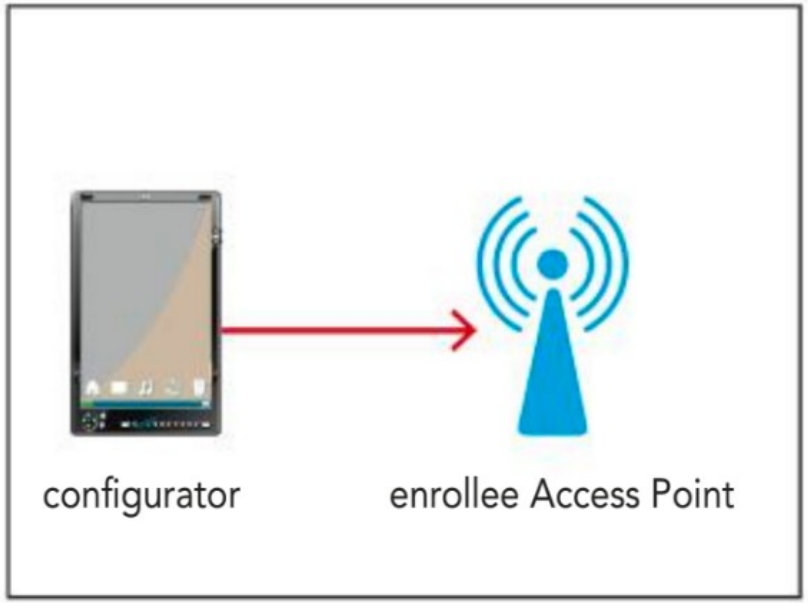
Provisioning: processo mediante il quale un amministratore di sistema assegna risorse e privilegi agli utenti di una rete.

La **FIGURA 15** mostra la sequenza di passi per collegare al Wi-Fi svariati dispositivi mediante uno smartphone che funge da **configuratore**:

1. il configuratore effettua la registrazione alla rete Wi-Fi mediante la scannerizzazione del QR code dell'access point;
2. il configuratore effettua la registrazione e il **#provisioning** dei dispositivi client mediante la scannerizzazione del QR code di ciascuno;
3. i dispositivi si connettono senza difficoltà alla rete.

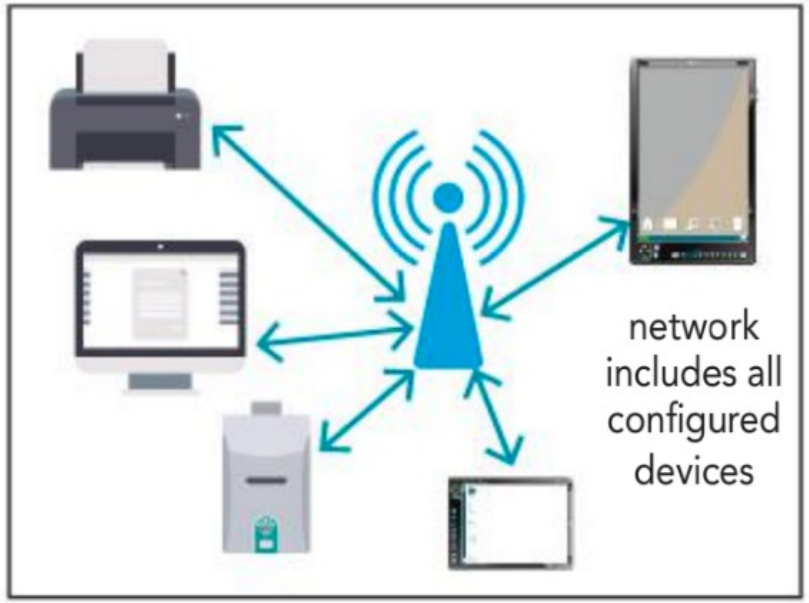
LA SICUREZZA NELLE RETI WIRELESS

1 Scan Access Point QR code to establish the network



2 Scan client device QR code to provision and enroll devices

3 Devices seamlessly connect to the network



LA SICUREZZA NELLE RETI WIRELESS

Autenticazione

L'autenticazione reciproca, tipica delle reti wireless, può risolvere parecchi problemi legati alla sicurezza, come per esempio gli attacchi DoS. È importante che l'autenticazione sia reciproca e non unilaterale per rendere più difficili le operazioni di intrusione.

> Ciò che si richiede per l'**autenticazione reciproca** è che il client riconosca la rete wireless come quella di appartenenza e che la rete riconosca il client come parte della rete stessa.

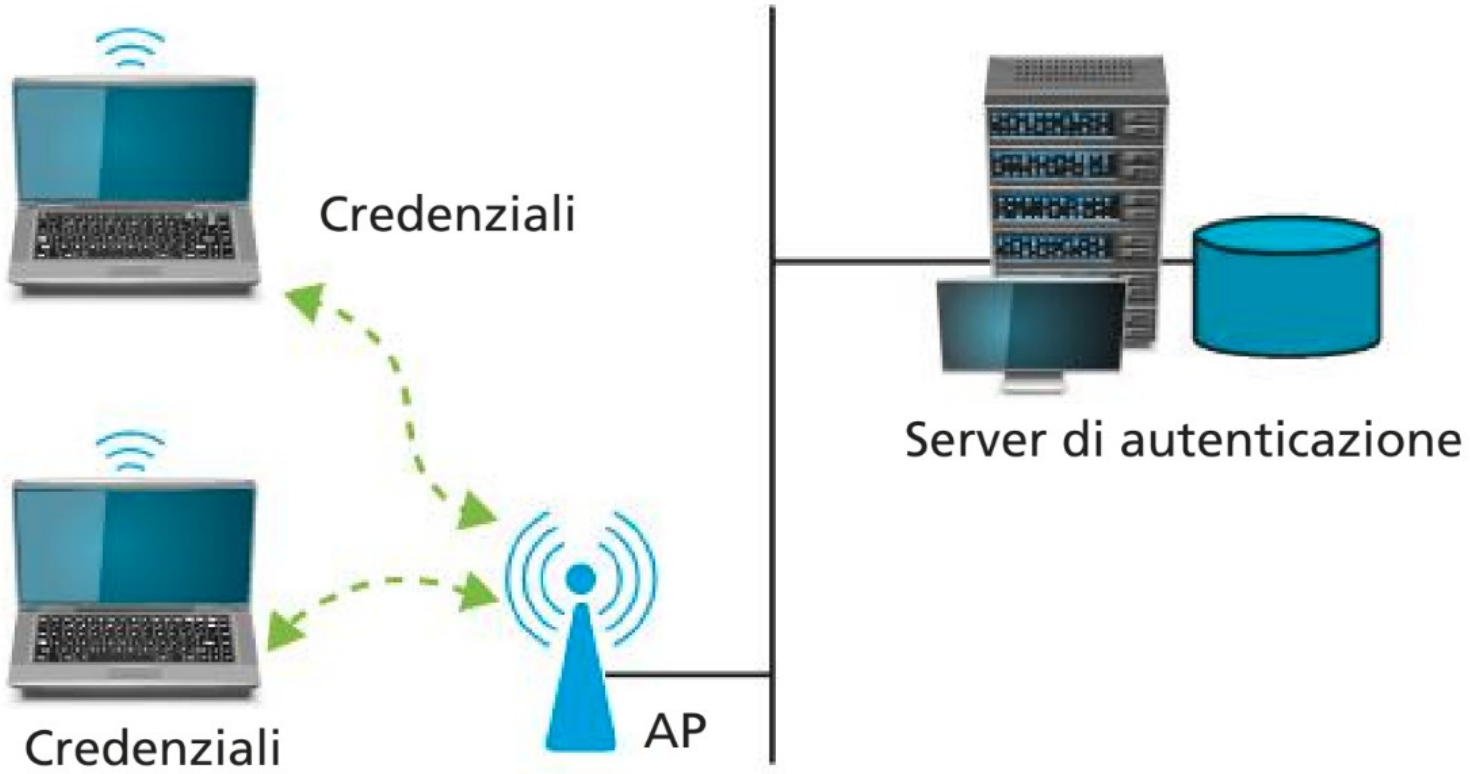
LA SICUREZZA NELLE RETI WIRELESS

Autenticazione

La miglior forma di autenticazione possibile è ottenuta utilizzando lo standard **IEEE 802.1x**, il quale definisce uno schema architetturale nel quale possono essere usate varie metodologie; per questo una delle sue caratteristiche fondamentali è la **versatilità**. La metodologia più diffusa è quella che implementa il protocollo **EAP** (Extensible Authentication Protocol) su entrambi i supporti di rete: parte wireless e parte cablata. Con l'EAP, al wireless terminal che cerca di utilizzare la rete viene consentito solo il passaggio dei pacchetti **EAP**. Tale processo si avvale di un server di autenticazione, posizionato nella parte cablata della rete (FIGURA 16) come, per esempio, il **RADIUS** (Remote Authentication Dial-In User), per eseguire l'autenticazione.

LA SICUREZZA NELLE RETI WIRELESS

Autenticazione



LA SICUREZZA NELLE RETI WIRELESS

Autenticazione

Ad autenticazione avvenuta, viene consentito il passaggio del traffico di rete.
Il server di autenticazione utilizza un algoritmo di autenticazione specifico per verificare l'identità del client.

Tale algoritmo non è espressamente definito dallo standard 802.1x. Occorre scegliere un tipo di EAP, come per esempio:

- EAP-TSL (Transport Layer Security)
- EAP-TTSL (Tunneled Transport Layer Security)
- LEAP (LigtweightEAP della Cisco)

Il software che supporta il tipo di EAP specifico si trova sul server di autenticazione e nel sistema operativo o in apposito software sui dispositivi client.

LA SICUREZZA NELLE RETI WIRELESS

Autenticazione

Un'altra forma di autenticazione prevede che l'amministratore della rete autorizzi l'accesso alla rete a un elenco di indirizzi MAC. Gli AP rifiuteranno i frame con un indirizzo MAC non in elenco. Il problema di questa tecnica è che la crittografia WEP non crittografa il campo del frame dedicato all'indirizzo MAC. Questo consente a uno sniffer che analizzi il traffico di individuare gli indirizzi MAC validi e di sostituirsi a un client quando questi non è collegato.

Riassumendo….

1. Scenari di reti senza fili

Le reti wireless, attraverso onde radio o segnali infrarossi, fanno comunicare dispositivi computerizzati, come notebook, tablet, smartphone, personal computer, router e stampanti.
La maggior parte dei produttori integra nei dispositivi schede di rete wireless e antenne.
Le reti wireless, come le reti cablate, sono classificate in base all'area fisica che possono coprire:

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

2. La normativa sul wireless

Attualmente, qualunque esercizio pubblico o privato che non sia principalmente un Internet provider/point non deve richiedere autorizzazione per fornire una rete e non è tenuto in alcun modo a identificare i clienti.
Tuttavia identificazione e monitoraggio tutelano l'esercente dai reati commessi utilizzando la sua linea Internet.
Chi fornisce il servizio deve comunque essere in grado di garantire l'inviolabilità della rete e preservare l'integrità dei dati personali dei clienti.

3. La sicurezza nelle reti wireless

Garantire la sicurezza nelle reti wireless è fondamentale soprattutto perché i segnali si propagano attraverso un mezzo impossibile da isolare e sono a disposizione di tutti.
È quindi necessario che gli utenti siano consapevoli dei problemi e delle relative contromisure per proteggere le proprie comunicazioni.
I principali rischi per la sicurezza sono:

- sniffing;
- accesso non autorizzato;
- sostituzione del SID (*Security IDentifier*);
- attacco DoS (*Denial of Service*).

Le tecniche per rafforzare la sicurezza sono la crittografia e l'autenticazione.

4. Configurazione di una rete wireless domestica

Se si desidera progettare e realizzare una rete domestica, la soluzione wireless è decisamente conveniente poiché consente di evitare modifiche strutturali, passaggi di canaline elettriche, posa dei cavi e installazioni delle prese a muro.
Lo standard consigliato è l'802.11g/n/ac poiché offre ottime prestazioni ed è compatibile con la maggior parte dei dispositivi attualmente sul mercato.
Per realizzare la rete occorrerà innanzitutto avere una connessione Internet (per esempio l'ADSL) e un router wireless dotato inoltre di porte LAN Ethernet con funzione di switch.

MAPPA CONCETTUALE