Radio e reti Wireless

Fondamenti di Cybersecurity 2022/2023

Davide Berardi <davide.berardi@unibo.it>

Le trasmissioni radio sono soggette a problemi di sicurezza informatica.
Molto integrate nei sistemi:

- Cancelli automatici
- Telecomandi automobili
- RFID (contactless)
- Wi-Fi (IEEE 802.11)
- Bluetooth / Zigbee / Domotica

Nella terminologia radio esistono:

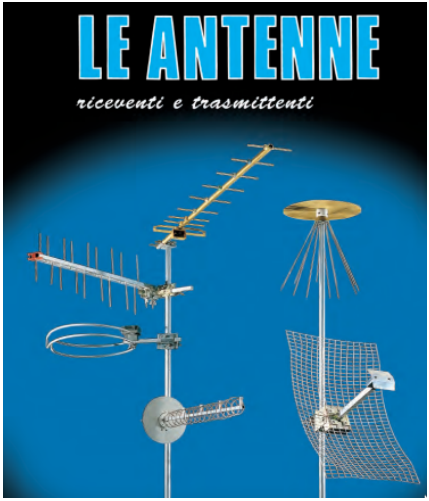
- Trasmettitore (TX): colui che invia informazioni.
- Ricevitore (RX): colui che riceve informazioni.

Un Transceiver è un dispositivo in grado di effettuare entrambe le operazioni.

Eccitando un antenna, il campo elettrico viene “spostato” nell’ambiente circostante. Sostanzialmente gli elettroni in cui è immersa l’antenna (l’etere) vengono spostati dall’energia a cui la sottoponiamo.

Figure: Fonte: Le antenne riceventi e trasmittenti

Ogni tipo di antenna ha la sua peculiarità e deve essere dimensionata correttamente per la trasmissione che vogliamo effettuare.



Un antenna grande non implica che ci sia grande potenza in trasmissione!

L'antenna riceve lo "spostamento" del campo elettrico e lo "invia" ai componenti elettronici a cui è collegata, i quali possono poi elaborare le informazioni ricevute.

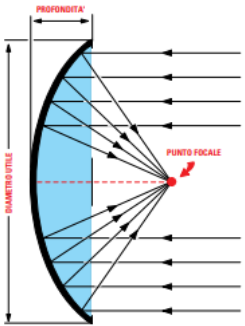


Figure: Fonte: Le antenne riceventi e trasmittenti

Per trasmettere l'antenna deve "vibrare". Questa vibrazione deve essere effettuata a una determinata frequenza (se pensiamo una corda di una chitarra, la seconda corda dall'alto vibra a 110Hz, A2).

Questa frequenza a cui si fa vibrare l'antenna prende il nome di "portante".

Per questo motivo le antenne in trasmissione devono essere dimensionate correttamente.

In ricezione (in linea di massima), un'antenna più grande risulterà in più informazioni ricevute (più frequenze catturate).

Avendo disponibili tutte le informazioni nello stesso momento, è necessario filtrarle in modo da ricevere solo quelle a cui siamo interessati. Questo processo si chiama sintonizzazione.

La sintonizzazione non è sicurezza!
Security by Obscurity

Deve essere quindi stipulato un protocollo di comunicazione (layer 1). Questo prevede come le informazioni (i bit) vengono codificate sull'antenna. Esistono tre principali classi:

- Modulazione in Ampiezza (AM)
- Modulazione in Frequenza (FM)
- Modulazione in Fase (PM)

Non vedremo le modulazioni. La più semplice che possiamo pensare è la modulazione OOK (on off keying), della classe AM.

In questa modulazione viene accesa (bit 1) o spenta (bit 0) la portante.

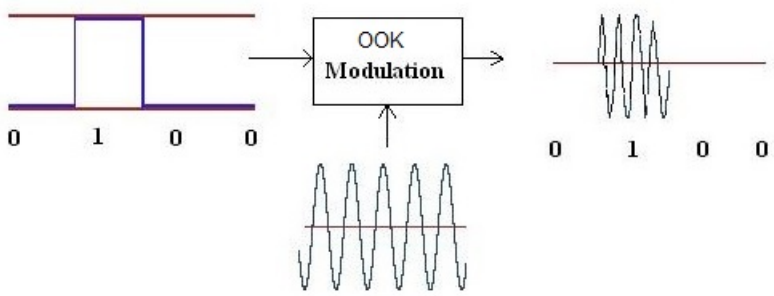


Figure: Fonte: rfwireless-world.com

È facile immaginare come accendendo sempre la portante non sia più possibile trasmettere o ricevere i dati.

Problema presente anche in altri protocolli (e.g.I2C).

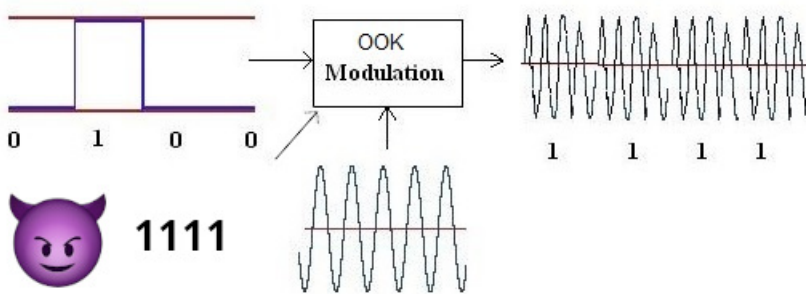


Figure: Fonte: rfwireless-world.com (modificata)

Questo attacco richiede tanta energia da parte del Jammer.

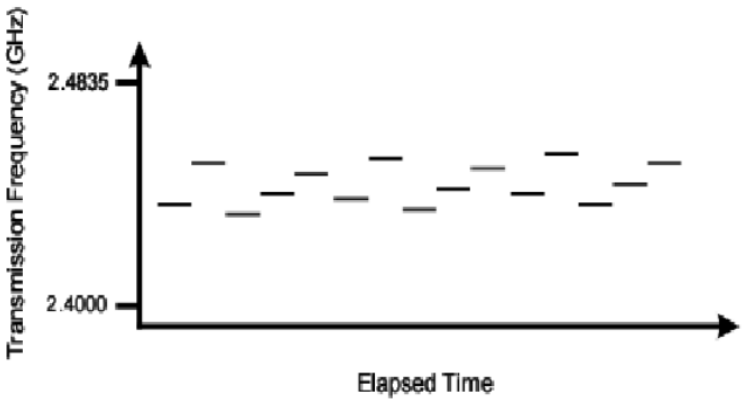
L'idea per renderlo meno efficace è quella di usare più frequenze portanti (banda larga). In questo modo sarebbe necessario per il Jammer usare molta più energia.

Figure: Fonte: jammerinthebox.com

Un meccanismo per utilizzare la banda larga è il cosiddetto Frequency Hopping Spread Spectrum (FHSS).

Con questo meccanismo si selezionano più portanti e si salta da una all'altra con una sequenza decisa a priori.

Nel caso ci sia una collisione o un Jamming su una singola portante ci sarà la perdita solo di quella parte di informazione.



FHSS with five frequency (Akin, 2003)

Eavesdropping e sniffing in ambito radio sono molto semplici da perpetrare (sapendo il seed del PRNG dell'eventuale FHSS). Sono necessari:

- Un ricevitore (più antenna) alla corretta distanza per ricevere il segnale;
- conoscere la modulazione utilizzata;
- il protocollo utilizzato.

Esistono attacchi perpetrabili senza informazioni come la modulazione utilizzata o il protocollo utilizzato (li rivedremo con altri protocolli).

È sufficiente catturare una porzione di frequenze (spettro) e ritrasmetterle così come ricevute.

Questo prende il nome di attacco di Replay.

Questo attacco NON è protetto da meccanismi di confidenzialità o integrità!!!

Cosa succede se reinoltro un messaggio cifrato e integro che so essere il messaggio per effettuare un'operazione?

Il messaggio viene considerato valido!

Questo meccanismo normalmente viene implementato nei cancelli automatici. Catturando il treno di impulsi OOK sulla portante corretta (normalmente 433Mhz) è possibile reinviare il messaggio al cancello automatico per farlo aprire.

Questa operazione non richiede la comprensione del contenuto del treno di impulsi.

Figure: Fonte: faac.it

Le automobili e i cancelli automatici con più sicurezza rispetto a quelli elencati precedentemente utilizzano un meccanismo di protezione chiamato Rolling Code.

- Il trasmettitore seleziona un codice basandosi su un PRNG e lo invia.
- Il trasmettitore seleziona il codice successivo, basandosi sul PRNG.
- Il ricevitore controlla che il codice ricevuto sia consistente con il suo PRNG, nel caso effettua l'operazione e fa avanzare il PRNG.

Problema: Cosa succede se un codice viene trasmesso e non ricevuto?

Problema: Cosa succede se un codice viene trasmesso e non ricevuto?

Disallineamento del PRNG. Non viene più effettuata l'operazione.

Per questo motivo il ricevitore controlla una finestra (supponiamo 100) di codici successivi a quello abilitato, poi sposta la finestra di conseguenza.

Questa cosa risolve l'attacco di Replay?

Questa cosa risolve l'attacco di Replay?

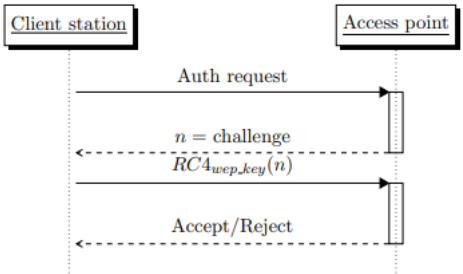
No! Ma lo rende meno efficiente. L'attaccante dovrà catturare vari codici, terminati quelli dovrà ricatturare i codici dal trasmettitore.

Il problema di questi metodi è la mancanza di un canale di ritorno. Questi cancelli o macchine non dialogano con il trasmettitore e si limitano a ricevere.

Tramite dei transceiver è possibile effettuare quello che viene chiamato Challenge and Response.

Presente anche in vari protocolli applicativi, funziona nel seguente modo:

- L'autenticando (trasmettitore nei casi precedenti) richiede di accedere al sistema tramite un messaggio.
- L'autenticatore (cancello o macchina) genera un numero random (nonce) e lo invia all'autenticando.
- L'autenticando cifra il nonce inviato e reinvia il valore cifrato all'autenticatore.
- L'autenticatore decifra il valore cifrato e valida o meno l'autenticazione.


Client station
Access point
Auth request
n = challenge
$RC4_{wep\_key}(n)$
Accept/Reject

Ovviamente la cifratura può essere applicata, oltre che ai meccanismi di autenticazione, per mantenere la confidenzialità e l'integrità dei dati in transito.

Nel mondo radio questa viene implementata tramite cifrari a blocco (e.g. AES) o a flusso (e.g. Kasumi per il mondo 4G).

Un altro sistema radio prende il nome di Radio Frequency Identification (RFID).

Questo è normalmente utilizzato per autenticare (quello che si ha) tramite badge, telefoni o portachiavi.

Figure: Fonte: amazon.com

Ad esempio, i badge Unibo utilizzano una tecnologia chiamata EM410X. Questa prevede un ID interno univoco per ogni badge, che viene assegnato dal database Unibo al vostro account.

In questo modo, i portali in cui si richiede l'autenticazione effettueranno una ricerca sul database per controllare se il vostro account è effettivamente autorizzato per passare un determinato varco (autorizzazione).

I badge EM410X vengono venduti senza la possibilità di modificare il loro ID univoco.

Come possiamo aggirare questa protezione?

I badge EM410X vengono venduti senza la possibilità di modificare il loro ID univoco.

Come possiamo aggirare questa protezione?

Comprando dei badge che hanno questa possibilità! (Rasoio di Occam, o percorso di minima resistenza)

Figure: Fonte: amazon.com

E se non fossero presenti badge “liberi” per una determinata tecnologia?

In assenza di meccanismi crittografici, anche in questo caso, è sempre possibile spacciarsi per un badge con un transceiver RFID.

Figure: Fonte: proxmark.com

Una delle comunicazioni radio più influenti nel mondo informatico / telecomunicazionistico è lo standard IEEE 802.11, comunemente chiamato Wi-Fi.

È uno standard pensato per creare reti locali interoperabili con reti Ethernet.

Lo standard è diviso in vari sotto-standard (e.g. IEEE 802.11g per le reti 2.4GHz o IEEE 802.11ac per le reti operanti nella banda dei 5GHz).

A seconda dello standard di afferenza, si utilizzano diversi livelli fisici e modulazioni (per accesso al canale principalmente).

A livello fisico non vengono poste protezioni normalmente.

Essendo le onde radio propagate nello spazio, esistono soluzioni per isolare spazialmente gli ambienti (e.g. pitture in grado di attenuare molto le onde radio).

Le reti 802.11, essendo radio, sono sensibili alle collisioni (ricordiamo l'esempio del denial of service su OOK quando viene mantenuta la portante).

Per questo motivo c'è bisogno di un protocollo di accesso al canale tra i dispositivi, in modo da risolvere eventuali collisioni.

Inoltre, non è sempre possibile vedere tutti i nodi, il punto d'accesso ha normalmente visibilità dell'intera rete (se singolo) ma i singoli nodi no. Questo problema prende il nome di "Terminale Nascosto"

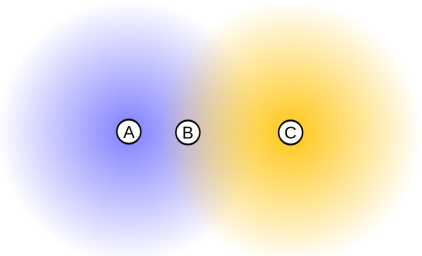


Figure: Fonte: wikipedia.org

Il problema della collisione viene “risolto” accorgendosi che si è presentata ed aspettando un tempo random prima di ritrasmettere il messaggio.

Il protocollo prevede quindi degli “spazi” di silezio per evitare la collisione, che devono essere rispettati.

La gestione di questi spazi è particolarmente complessa con diverse classificazioni (spazi che può aspettare solo l’access point, spazi dedicati ai client etc etc) e prendono il nome di IFS (inter frame space).

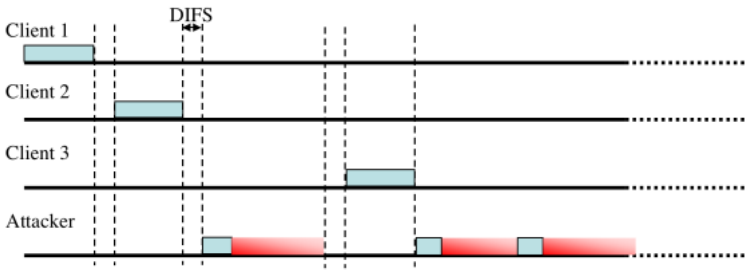


Figure: Fonte: John Bellardo and Stefan Savage.

Cosa succede se qualcuno non rispetta lo spazio di silenzio successivo a una collisione e non aspetta nessun IFS?

Cosa succede se qualcuno non rispetta lo spazio di silenzio successivo a una collisione e non aspetta nessun IFS?

Parla sempre e solo lui!

Cosa succede se due terminali non rispettano lo spazio di silenzio successivo a una collisione e non aspettano nessun IFS?

Cosa succede se due terminali non rispettano lo spazio di silenzio successivo a una collisione e non aspettano nessun IFS?

Nessuno può più parlare!

Un primo meccanismo di “sicurezza” è quello di nascondere la rete agli occhi di un attaccante. Per accedervi bisognerà conoscerne il nome...

Un primo meccanismo di “sicurezza” è quello di nascondere la rete agli occhi di un attaccante. Per accedervi bisognerà conoscerne il nome...

Nome che viene inviato in chiaro dagli host che richiedono l’accesso...

Un primo meccanismo di “sicurezza” è quello di nascondere la rete agli occhi di un attaccante. Per accedervi bisognerà conoscerne il nome...

Nome che viene inviato in chiaro dagli host che richiedono l’accesso...

Guess what?

Security by Obscurity

A livello 2, i terminali IEEE 802.11 utilizzano degli indirizzi Mac, esattamente come le schede di rete Ethernet.

Un meccanismo di sicurezza potrebbe essere quello di abilitare solo alcuni indirizzi Mac, in modo da vincolare la rete a quelli.

Il problema di questo approccio, sempre di security by obscurity, è che l'indirizzo Mac è inviato in chiaro nella comunicazione IEEE 802.11. È possibile effettuare facilmente "spoofing" (successivamente a una fase di sniffing, ad esempio con Wireshark).

```
[root@snark ~]# macchanger -m 11:22:33:44:55:66 virbr0
Current MAC:   52:54:00:b7:9a:84 (unknown)
Permanent MAC: 00:00:00:00:00:00 (XEROX CORPORATION)
```

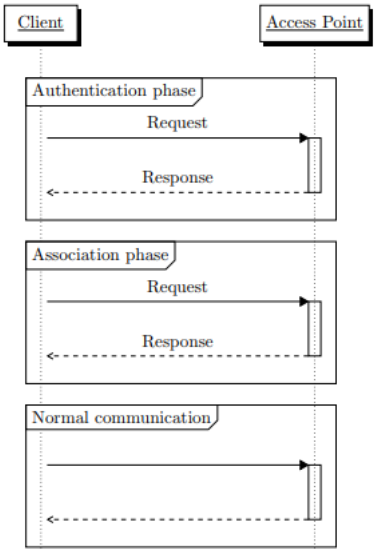
L'autenticazione alla rete e la confidenzialità sono cruciali in reti di questo tipo, in quanto per fare eavesdropping non è richiesto il man in the middle.

In una rete open le informazioni vengono inviate nell'etere in chiaro, tutti le possono leggere anche senza essere associati alla rete.

Per questo motivo esistono diversi meccanismi di protezione basati su meccanismi crittografici (cifrari).

Nonostante i meccanismi di cifratura e accesso alla rete, IEEE 802.11 prevede messaggi che vengono inviati in chiaro, senza nessun meccanismo di autenticazione o confidenzialità o anti replay.

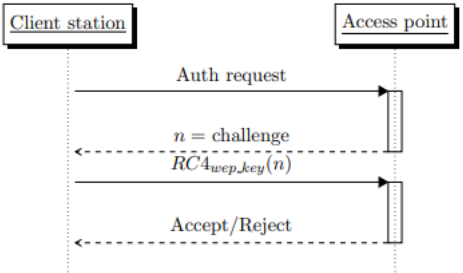
Ad esempio esiste un messaggio di “disassociazione” a una rete. Con questo messaggio è possibile far sì che un terminale tolga l’associazione con un determinato access point.


Client
Access Point
Authentication phase
Request
Response
Association phase
Request
Response
Normal communication

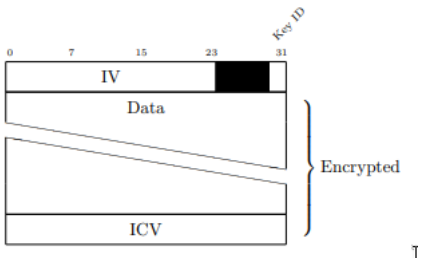
La prima forma di autenticazione e confidenzialità delle parti è un meccanismo che prende il nome di Wired Equivalent Privacy.

Non è sicuro!!! Presenta due modalità di funzionamento:

- Shared Key
- Open System



Viene dimostrata la possessione della chiave da parte del client utilizzando un meccanismo di challenge and response.
Dannoso!!! Si può attaccare con attacchi KPA (known plaintext) e ricavare la chiave da tutte le autenticazioni.



Il richiedente della connessione è già a conoscenza del segreto comune, ovvero la chiave condivisa, altrimenti non sarebbe in grado di decifrare i pacchetti cifrati provenienti dall'access point.

$$m = m_0||m_1||m_2...m_n$$

$$RC4\_seed(IV||k)$$

$$c_0 = RC4() \oplus m_0$$

$$...$$

$$c_i = RC4() \oplus m_i$$

$$...$$

$$c_n = RC4() \oplus m_n$$

Dopo 30000 pacchetti trasmessi dalla rete le probabilit'a di collisione sono praticamente impossibili da evitare!

$$collisionP \approx 1 - e^{\frac{-30000^2}{2*2^{24}}} = 0.99999999999774...$$

Catturando pacchetti con lo stesso IV è possibile fare attacchi statistici.

Inoltre, catturando pacchetti con un IV noto è possibile far ricircolare pacchetti vecchi aumentando il traffico!!!

Per ovviare a questi (e altri) problemi di WEP, è stato sviluppato Wi-Fi Protected Access (WPA). Questo standard (arrivato alla versione 3), pone diversi modi di utilizzo per il canale:

- PSK, per reti domestica, chiave segreta su ogni dispositivo.
- Enterprise, per reti con molti utenti (e.g. ALMAWIFI)
- WPS, sistema di autenticazione facilitato

e diversi metodi di cifratura

- TKIP, compatibile WEP, deprecato
- CCMP, basato su AES

Il primo metodo di autenticazione è WPA-PSK TKIP. Per retrocompatibilità è basato su RC4 (come wep) e gestisce le chiavi in modo da complicare gli attacchi a WEP. Soffre degli stessi problemi ed è deprecato.

WPA-PSK CCMP invece, utilizza un cifrario forte (AES) e gestioni delle chiavi complesse. Risulta essere uno dei metodi più resistenti per WPA al momento.

Ovviamente le reti PSK soffrono degli stessi problemi legati al meccanismo di autenticazione, non alla crittografia, ad esempio è possibile perpetrare attacchi bruteforce o a dizionario come per le password.

WPS è una semplificazione del metodo d'accesso alla rete wifi, senza necessità di password (una sorta di quello che si ha, l'accesso fisico al dispositivo).

Abilita diverse metodologie d'accesso:

- Tasto fisico
- PIN

Figure: Fonte: sony.com

Il settaggio del nome della rete non è crittografato (SSID), solo l'accesso ad essa.

Questo rende possibile attacchi di tipo Rogue Access Point, in grado di effettuare spoofing del nome della rete e invitando ad accedere i client, che si troveranno impossibilitati utilizzando una password diversa da quella configurata.

Il tasto fisico può essere facilmente aggirato tramite un rogue access point posto in una posizione tattica.

Il meccanismo di login tramite pin invece comporta un problema molto più preoccupante.

Il pin è normalmente implementato tramite un numero di 7 cifre (10000000 tentativi brute force).

Per qualche scelta implementativa (sbagliata?) il pin viene controllato dal sistema di autenticazione prima per le prime 4 cifre del numero, poi per le altre 3.

Visto che le successive 3 cifre vengono controllate solo se le prime 4 sono corrette, questo porta i tentativi di brute force a 10000 + 1000, 11000 tentativi, circa 20 ore.

Inoltre, l'implementazione di WPS su molti dispositivi embedded utilizzava un generatore di numeri random (nonce) predicibile. Portando questo brute force a un paio di minuti catturando e analizzando la comunicazione.

Le reti enterprise invece prevedono l'utilizzo di un server di login determinato Radius.

Questo server mantiene il login degli utenti (un po' come un database per un'applicazione web).

Qual è il problema in questo caso?

Il primo passaggio della rete non è cifrato con nessuna chiave (in realtà esiste un meccanismo che utilizza i certificati), aprendo la possibilità di creazione di Rogue Access Point.

Normalmente la comunicazione viene effettuata con uno scambio Challenge e Response. È possibile quindi per il Rogue Access Point effettuare un crack della password brute force o a dizionario!

Esiste un protocollo d'accesso basato su WPA-Enterprise simile a WPS per WPA-PSK. Questo viene chiamato GTC (generic token card e può essere richiesto come preferenziale dall'access point.

Abilitato di default su tutti i dispositivi mobili, il protocollo disabilita l'uso di challenge e response inviando la password **in chiaro**.

Chiedetevi a questo punto cos'è una backdoor.

Attacco di Replay per reti WPA2. Nella fase di autenticazione della rete viene utilizzato un nonce che può essere riusato identico per velocizzare le autenticazioni successive.

Questo comporta il poter reinstallare chiavi vecchie (un po' come funziona in WEP), in modo da poter analizzare facilmente la comunicazione e risalire alla chiave di cifratura.

Grazie a questo attacco lo standard è stato ulteriormente modificato, generando WPA3.

Domande?