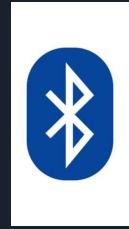


Introduzione al Bluetooth



Il Bluetooth è una tecnologia che usiamo tutti i giorni e troviamo in praticamente tutti i dispositivi elettronici che usiamo : computer, smartphone, auricolari, veicoli, tablet...

E' una tecnologia di comunicazione wireless a corto raggio, per la comunicazione a bassa potenza .

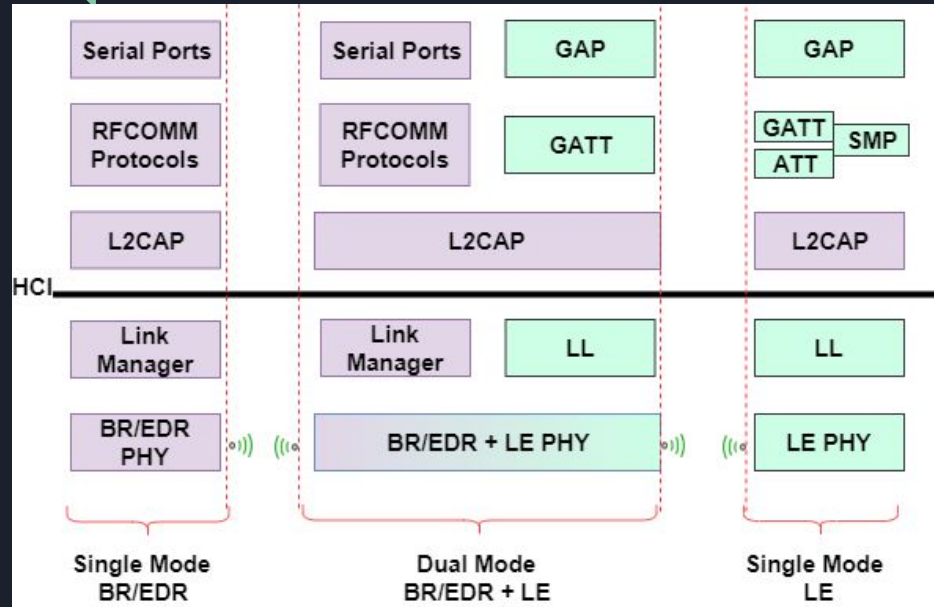
Non vi è bisogno di connessione

Due modelli :

-BLUETOOTH LE

-BLUETOOTH CLASSIC (BR/EDR)

Stack Bluetooth



Per quanto riguarda il Bluetooth LE, la sicurezza è gestita su più livelli dello stack di protocollo, ognuno con ruoli specifici, in particolare intervengono : LL,SMP,ATT,GATT

Per quanto riguarda invece il Bluetooth Classic , Il livello LMP è quello che si occupa anche di operazioni di sicurezza e anche il Baseband Layer.




Sicurezza nel Bluetooth LE : Link Layer

- crittografia AES a 128 bit
- genera indirizzi MAC randomici
- previene attacchi replay

Sicurezza nel Bluetooth LE : SMP

- definisce chi inizializza e chi risponde
- gestisce il pairing → diverse tipologie :
ATTENZIONE a JUST WORKS → senza autenticazione
- distribuisce chiavi



Sicurezza nel Bluetooth LE : ATT e GATT, Secure Connections

ATT : fornisce autenticazione e autorizzazione accesso ai dati

GATT definisce servizi e caratteristiche

Dalle versioni 4.2 di Bluetooth è stato introdotto ECDH → logaritmo discreto per scambio di chiavi



Sicurezza nel Bluetooth Classic

- LMP gestisce il pairing, l'autenticazione e lo scambio delle chiavi. (livello collegamento)
- Baseband Layer implementa la crittografia e la protezione dai replay(a livello fisico)

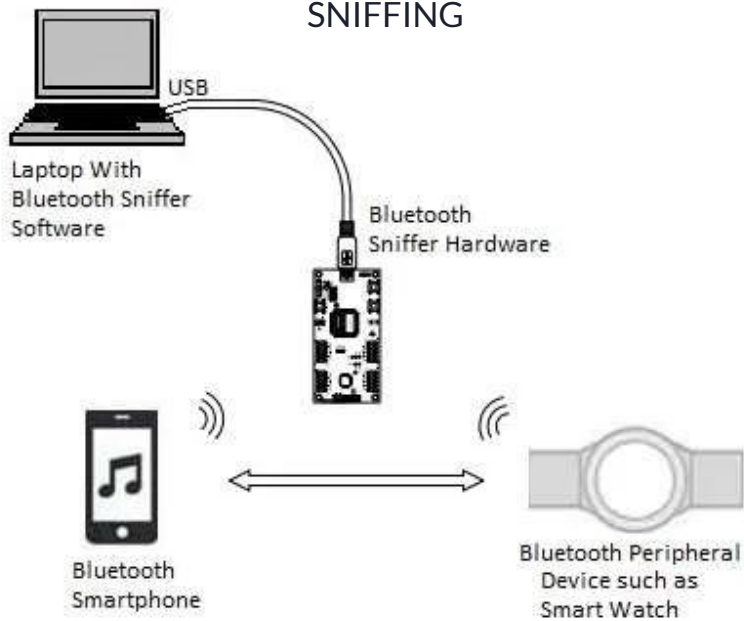


Vulnerabilità

- debole autenticazione
- protezione chiavi
- versioni non aggiornate

Attacchi principali

SNIFFING



MAN IN THE MIDDLE





Altri attacchi

- DoS: vengono inviati pacchetti di disturbo per interrompere la connessione Bluetooth di dispositivi
- Bluesnarfing: dati vengono rubati, grazie a tecniche viste in precedenza
- Bluebugging: un attaccante riesce a inviare attraverso il Bluetooth comandi che permettono di prendere il controllo del dispositivo che sta subendo l'attacco.
- Bruteforce: su Pin per accoppiamento via Bluetooth

Come difendersi ?



Sebbene le ultime versioni di Bluetooth siano più sicure , è bene prestare alcune attenzioni quando utilizziamo il Bluetooth su ogni nostro dispositivo.



Conclusione

Riferimenti

<https://github.com/simofb21/Sicurezza-Bluetooth> – repository github che contiene quanto detto

-le informazioni dette :

<https://www.cybersecurity360.it/nuove-minacce/hacking-bluetooth-attacchi-piu-comuni-e-consigli-per-la-sicurezza-delle-comunicazioni/>

<https://gitlab.com/4i3785803/Telecomunicazioni/>

-google

Immagini :

<https://dnewpydm90vfx.cloudfront.net/wp-content/uploads/2021/05/Bluetooth-vulnerabilita.jpg>

<https://prep-wizard.com/wp-content/uploads/Untitled-1024x449.pngv>

https://www.mathworks.com/help/bluetooth/ug/ble_bredr.png

<https://static.vecteezy.com/ti/vettori-gratis/t1/35560743-avvertimento-icone-impostato-triangolo-esclamazione-marchio-simboli-attenzione-vettore-grafica-vettoriale.jpg>

https://www.malwarebytes.com/wp-content/uploads/sites/2/2018/07/shutterstock_758712814.jpg

<https://www.sergentelorusso.it/wp-content/uploads/2021/11/Progetto-senza-titolo-3.png>