Telecomunicazioni 2024-2025 4IC

Approfondimento

BLUETOOTH E SICUREZZA

Simone Fusar Bassini, Gabriele Rosa, Tommaso Ingiardi, Alfredo Calabrese , Andrea Cornetti

Indice

Introduzione al Bluetooth

Il Bluetooth è una tecnologia che utilizziamo quotidianamente e che si trova praticamente in tutti i dispositivi elettronici che possediamo: computer, smartphone, auricolari, veicoli, tablet e molti altri. Essa consente comunicazioni wireless a corto raggio con un basso consumo di energia, senza la necessità di una connessione di rete. Esistono due modelli principali:

- BLUETOOTH LE
- BLUETOOTH CLASSIC (BR/EDR)

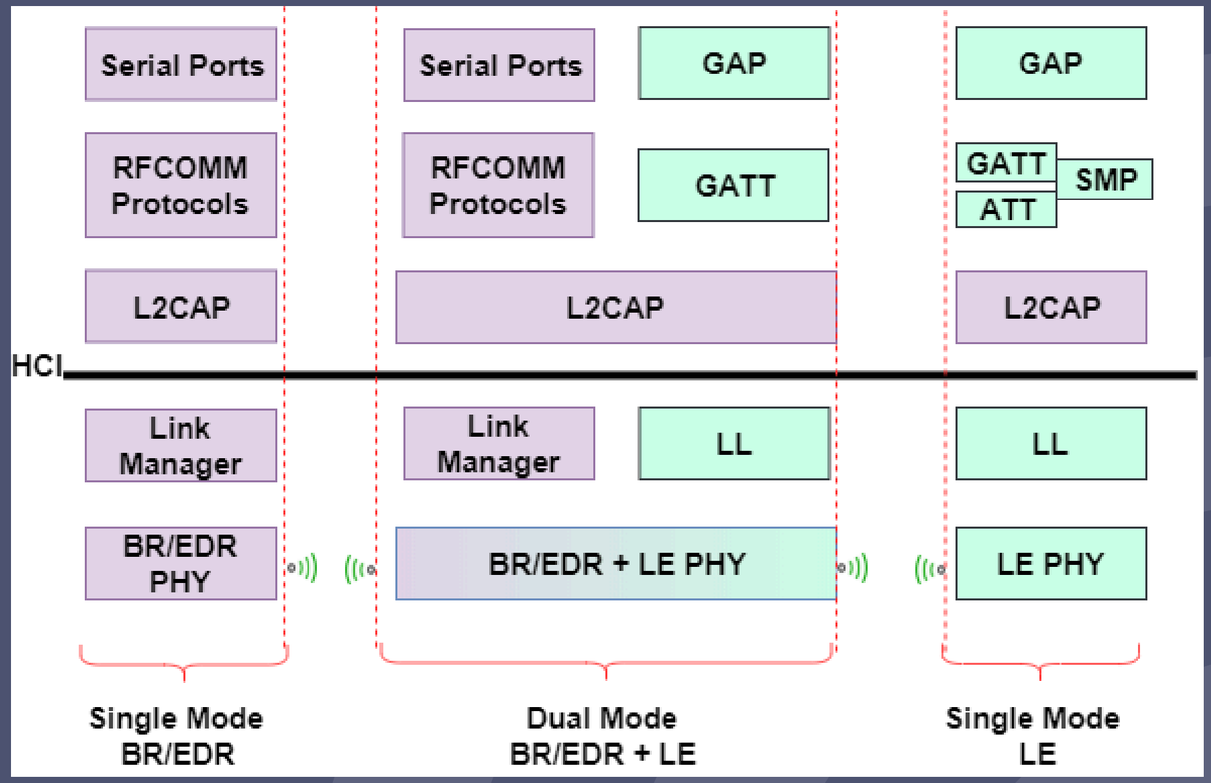
I tipi di dispositivi includono:

- Single mode BR/EDR
- Dual mode BR/EDR + LE
- Single mode LE

Stack Bluetooh

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

Nel Link Layer avviene:
-crittografia AES 128bit
-generazione indirizzi MAC randomici
-prevenzione attacchi replay

Nel SMP(Security Manager Protocol) :
-viene definito chi inizializza e chi risponde
-gestione del pairing

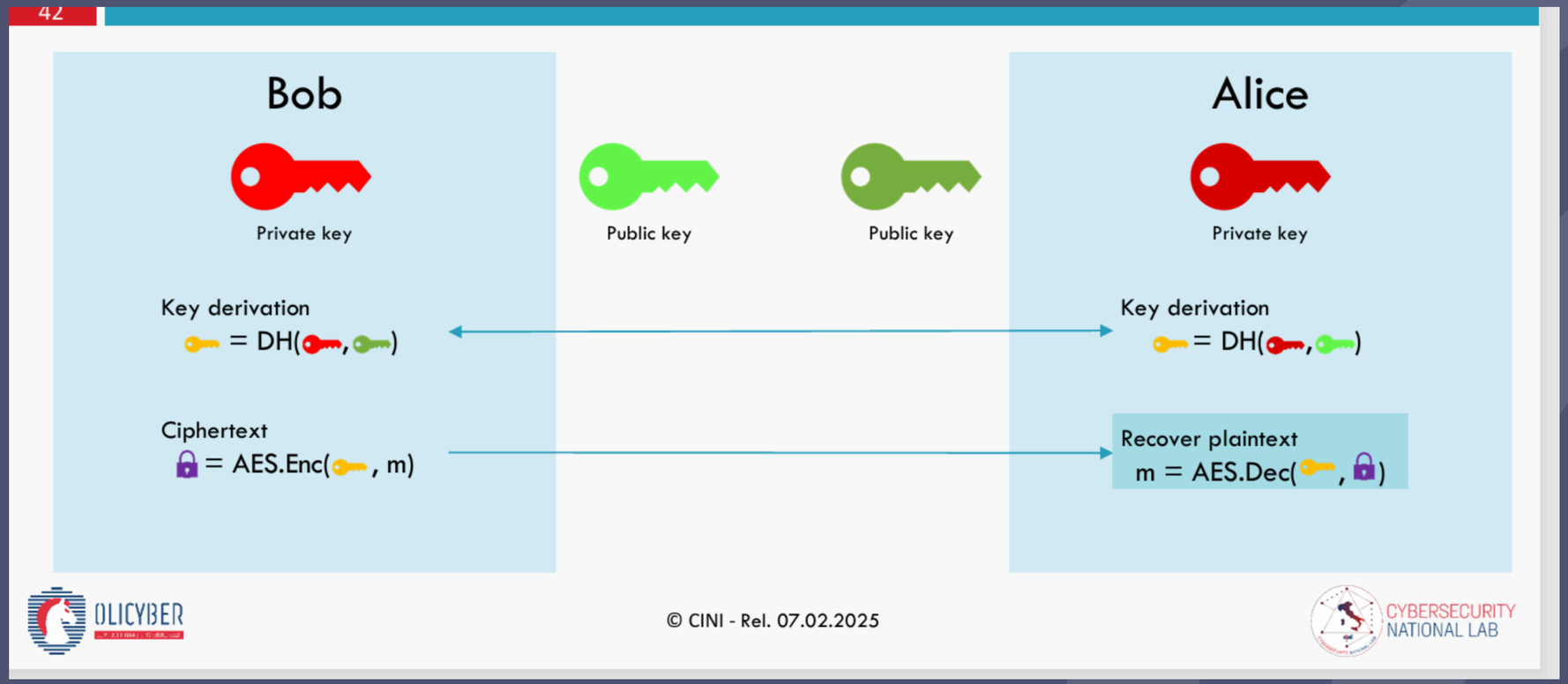
Ne esistono di diverse tipologie :JUST WORKS è senza AUTENTICAZIONE
PASSKEY ENTRY
NUMERIC COMPARISION

-distribuzione chiavi

Sicurezza nel Bluetooth LE

ATT fornisce autenticazione e autorizzazione per l'accesso ai dati.
GATT definisce servizi e caratteristiche, alcuni dei quali possono richiedere connessioni crittografate o autenticazione per l'accesso.

Dalle versioni 4.2 di Bluetooth è stato introdotto l'algoritmo DH



Sicurezza nel Bluetooth Classic

Baseband Layer e Link Control: implementa la crittografia e la protezione dai replay

- livello fisico
- forma una PICONET
- temporizzazione e controllo dell’accesso al canale
- crittografia
- connessione sincrona o asincrona

LMP gestisce il pairing, l'autenticazione e lo scambio delle chiavi. (livello collegamento):

- livello collegamento
- configura il collegamento e pone sistemi di autenticazione e crittografia
- pairing più vecchio con PIN, pairing da Bluetooth 2.1+ ha introdotto SSP

Vulnerabilità

Bluetooth , soprattutto Bluetooth LE presenta alcune vulnerabilità :

-versioni non aggiornate

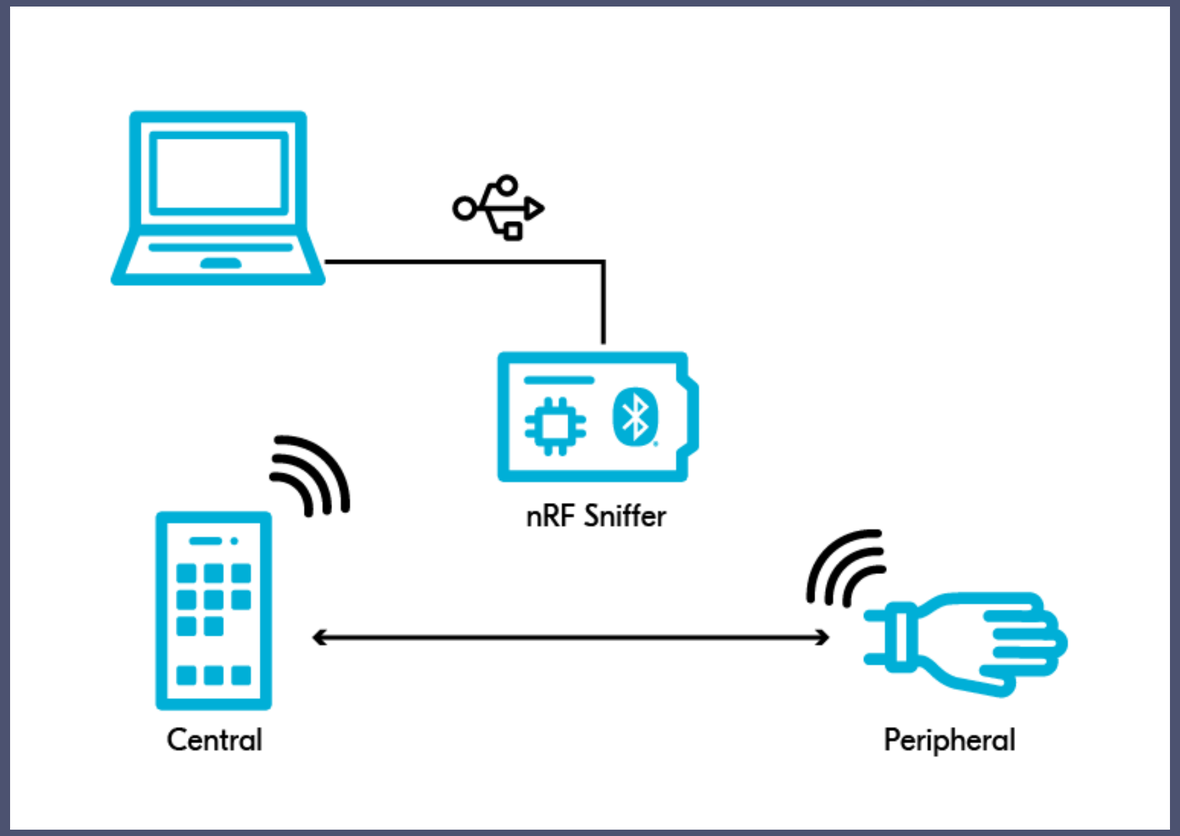
-debole autenticazione: possibilità di venire intercettati

-protezione chiavi: chiavi AES devono essere protette

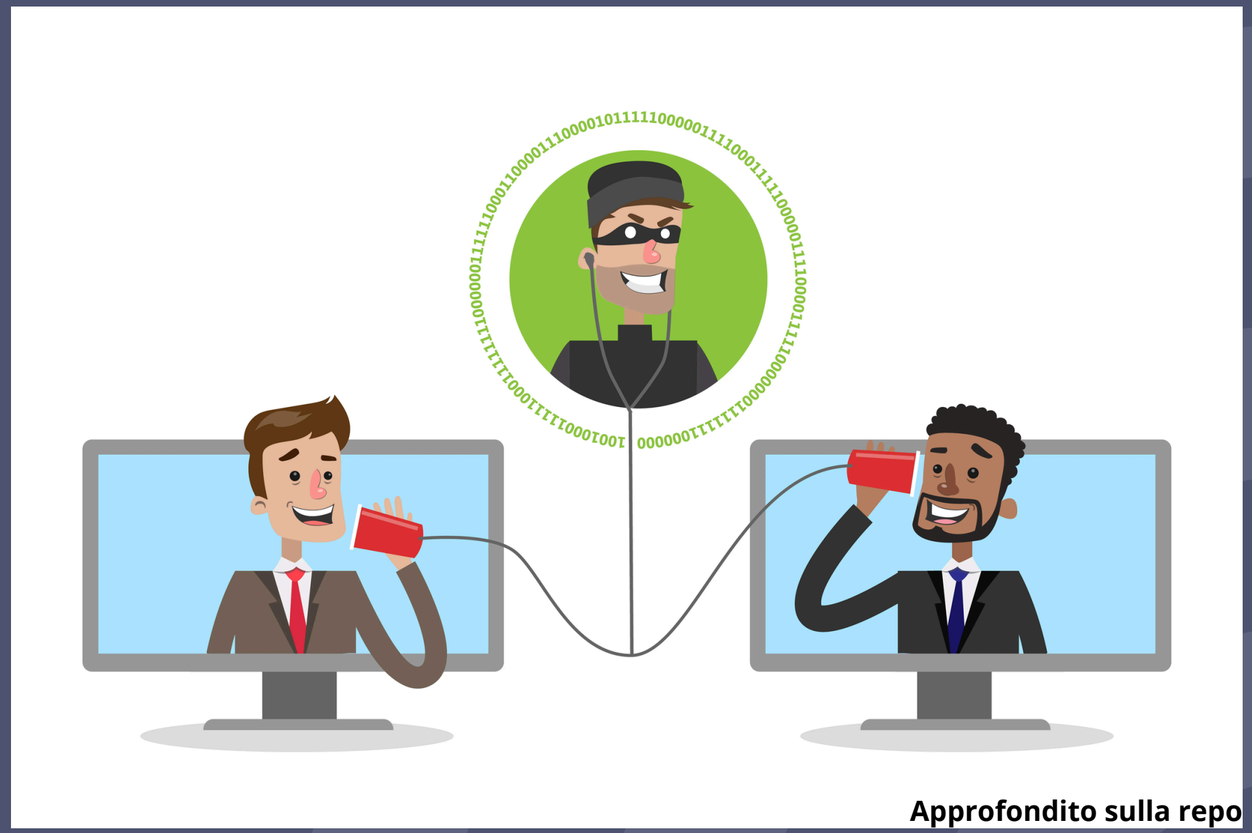
-indirizzi MAC non abbastanza randomici

Attacchi principali

SNIFFING



MITM



Approfondito sulla repo

Esistono però anche altri attacchii ....

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 proteggersi

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

CONCLUSIONE

Abbiamo quindi visto cos'è il Bluetooth, quali livelli dello Stack Bluetooth si occupano di sicurezza e quali sono alcune problematiche che riguardano la sicurezza., ma anche come stanno venendo risolti questi problemi.

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/

https://training.olicyber.it/training/crypto/