UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

SISTEMI FLESSIBILI PER LA CATTURA DI TRAFFICO BLUETOOTH

CANDIDATO: Stefano Orioli

MATRICOLA: 72452

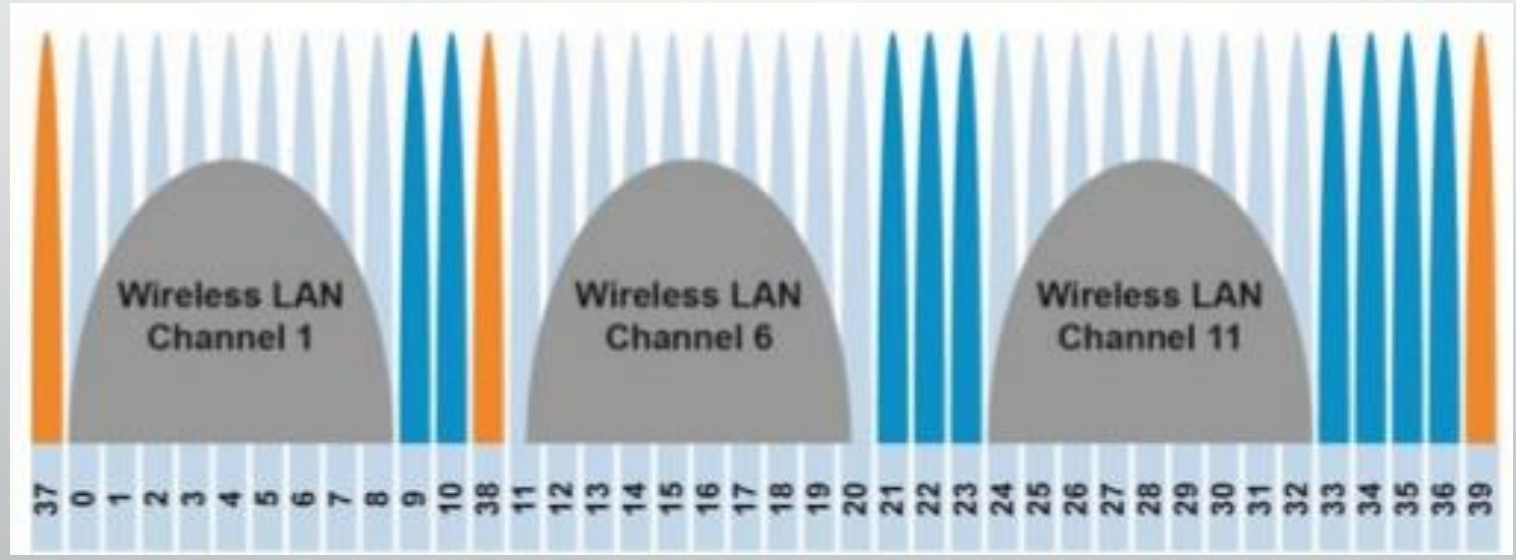
RELATORE: Francesco Gringoli

Sommario

- Bluetooth Low Energy
- Campi applicativi e sicurezza
- RedBear Nano2
- Progettazione Sniffer
- Pacchetti Catturati
- Conclusioni

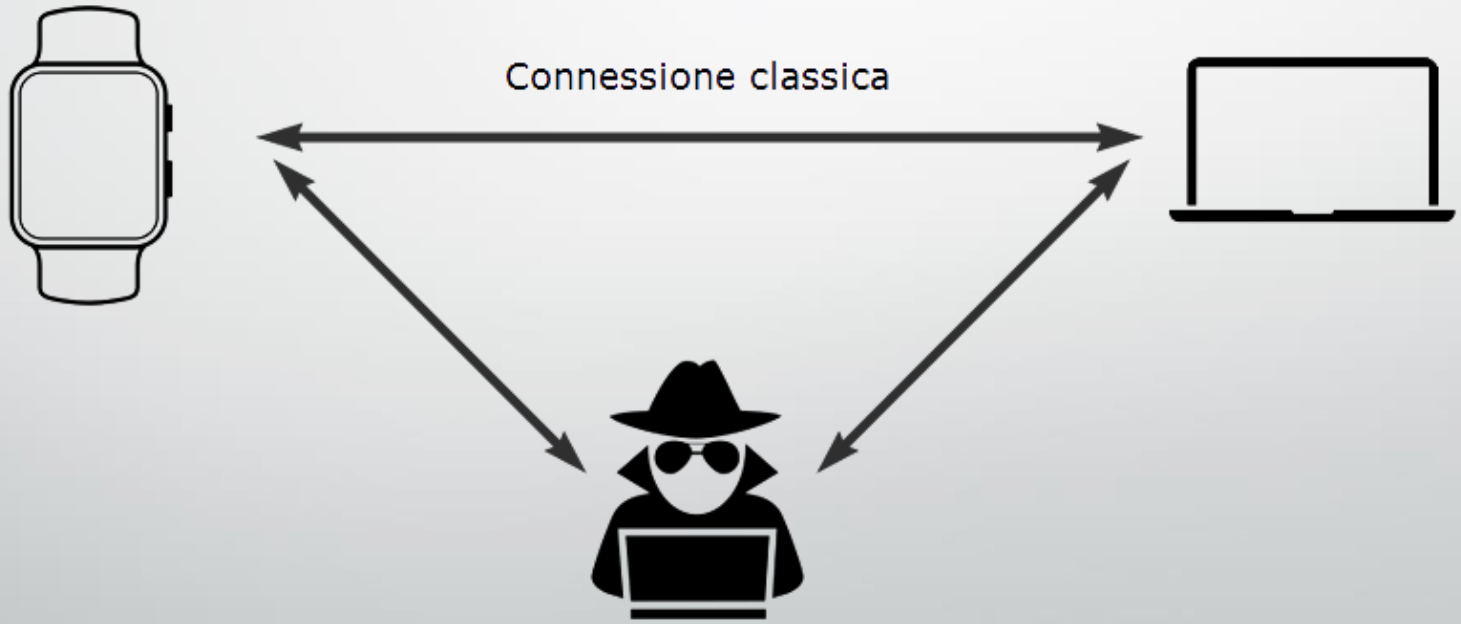
Bluetooth Low Energy

- Tecnologia Wireless a ridotto consumo energetico ideata per trasmissioni di dati di breve dimensione.
- Introdotta nello Standard 4.0 da SIG
- Banda di frequenze ISM, molte fonti di interferenza
- Divisione in 40 canali, 37 per dati e 3 Advertise, con Channel Hopping e Adaptive Channel Selection



Campi applicativi e sicurezza

- Utilizzata in larga scala, soprattutto dai dispositivi Smart.
- Con essa vengono scambiate anche informazioni personali.
- Utilizzato nell'IoT come dispositivo di identificazione personale.
- Robustezza ad attacchi Man in the Middle necessaria.



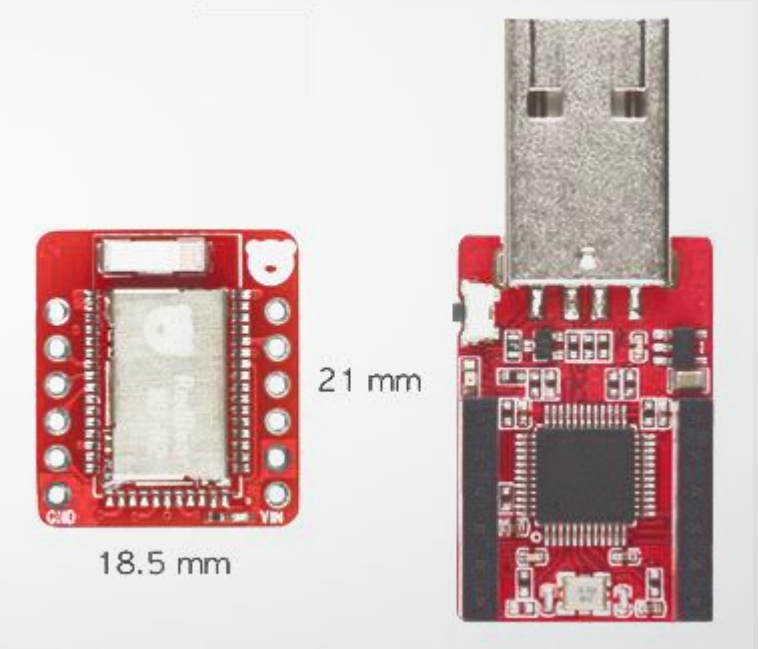
Alternative

- Seguire una connessione richiede di essere in ascolto in tutti i canali trasmissivi
- Compito oneroso, possibile con periferiche molto costose.
- Tramite due USRP B210 è possibile catturare tutte le trasmissioni nella Banda BLE

- Una valida alternativa è il Frontline BPA Low Energy, con cui si riescono a catturare tutti i pacchetti di una connessione

RedBear Nano v.2

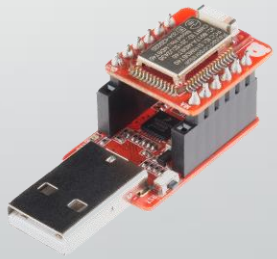
- Dispositivo usato per la creazione dello Sniffer.
- Economico ma versatile, integra SoC Nordic nRF52832 con processore ARM Cortex-M4F.
- Programmabile e collegabile a PC tramite DAPLink.
- Funziona autonomamente con batteria a bottone.
- Dotato di porte UART e SPI per la comunicazione.



Progettazione Sniffer

- Sviluppato in ambiente Linux con IDE Eclipse Mars in linguaggio C.
- Necessita compilatore ARM Cortex.
- Dialoga con PC tramite UART e virtualizzazione interfaccia seriale su USB.

Scambio dati



Pacchetti catturati

- La prima fase dello sviluppo si è concentrata sulla cattura dei pacchetti di Advertise.
- Canali di ascolto 37, 38 o 39.

42	0C	00	5A	33	A8	F9	F2	47	05	FF	0F	0F	01	23

- 42 : ADV_NONCONN_IND, Advertise di non connessione ad indirizzo privato.
- 0C : lunghezza del payload, pari a 12 Byte.
- 5A 33 A8 F9 F2 47: Indirizzo dell'Advertiser.
- 05 : lunghezza del campo dati, pari a 5 Byte.
- FF : Advertising Data Type.
- 0F 0F 01 23: Dati specifici del pacchetto.

CONNECT_REQ

- Per seguire una connessione è fondamentale ottenere la CONNECT_REQ.

Type	Len		InitA						AdvA					
C5	22	00	CE	45	D7	73	B8	6F	AC	F4	BF	9F	E6	F9

AA				CRCInit			WS	Woffset		Interval		Latency		TimeOut		Channel Map					Hop
F4	B0	6F	94	E6	7A	F5	02	05	00	27	00	00	00	D0	07	FF	FF	FF	FF	1F	A7

- Fondamentale ottenere l'AA e il CRCInit per poter catturare i pacchetti della connessione.
- Necessario anche HopCount e ConnInterval per conoscere tempistiche e canali su cui saranno trasmessi i dati.

Connessione

CH: 37 Time: 20 CONNECT_REQ

E5	22		8F F9 35 2C 36 C6	48 6F 6F 4C 0F 77	1D ED E6 12	54 CC 83	05	00 00	D0 02	00 00	90 01	FF FF FF FF	1F	EE

CH: 14 Time: 921

1E	0A		06 00 05 00 13 02 02 00 00 00

CH: 14 Time: 994

02	12		0E 00 04 00 11 06 01 00 09 00 00 18 0A 00 FF FF 01 18

CH: 28 Time: 1825

01	00

CH: 28 Time: 1894

05	00

CH: 5 Time: 2721

0D	00

CH: 5 Time: 2772

09	00

CH: 19 Time: 3627

01	00

CH: 19 Time: 3695

05	00

CH: 33 Time: 4529

01	00

CH: 33 Time: 4597

05	00

Sessione di cattura di una connessione partendo dalla CONNECT_REQ

Conclusioni

Risultati raggiunti:

- Creazione di uno Sniffer economico e multicanale.
- Invio dati catturati a sistemi di elaborazione.
- Cattura di pacchetti di connessione.
- Salto temporizzato tra canali per seguire una connessione.
- Cattura di tutti i pacchetti di una connessione.

Implementazioni future:

- Utilizzo di Sniffer e Raspberry per implementare un attacco Man in the Middle a dispositivi Bluetooth Low Energy

GRAZIE PER L'ATTENZIONE