UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unIMC

Flipper Zero: Tecnologie di uso comune e relative Vulnerabilità

Francesco Berti

berti.francesco@proton.me

Martedì 19 Settembre 2023

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

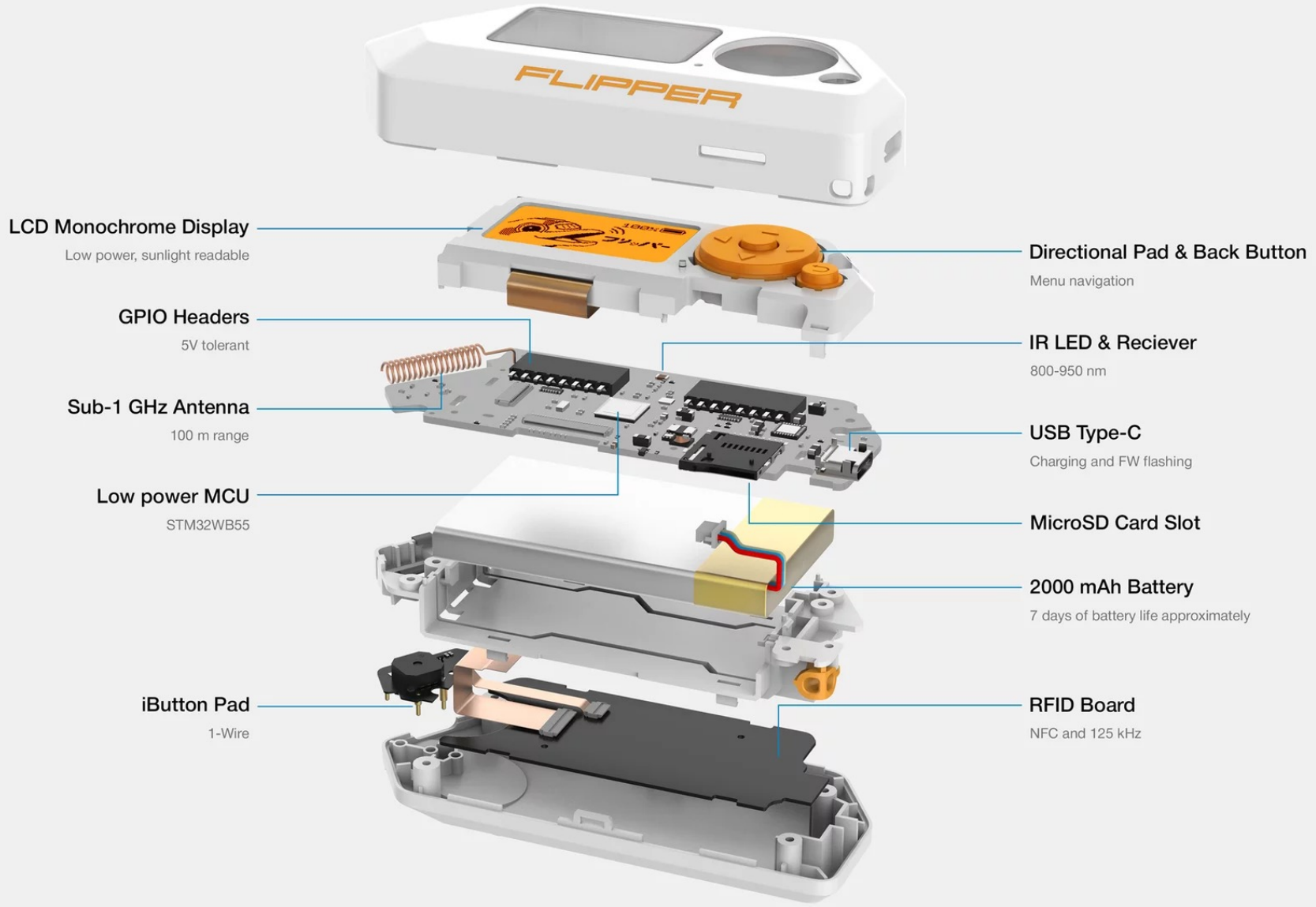
Flipper Zero

Flipper Zero: il Tamagotchi per Hacker

- Il **Flipper Zero** è un dispositivo **multi-tool** portatile per la **ricerca** e il **pentesting** di protocolli radio, RFID, sistemi di controllo degli accessi, Bluetooth, Wi-Fi, hardware ecc.

  – Il progetto è **open-source**
    - Annunciato nell'agosto 2020 e rilasciato dopo 18 mesi
    - La campagna **Kickstarter** ha avuto un grande successo raggiungendo i $4.882.784
    - Si prevedono vendite per $80.000.000 nel 2023

Flipper Zero: Componenti e Funzionalità



Flipper Zero: Scopo

- Il Flipper viene presentato come **Multi-tool Educational Device**: lo scopo principale è quindi quello di **esplorare**, **apprendere** e **migliorare** la **sicurezza** di alcune tecnologie

  – Il dispositivo è legale
    - Tutto ciò che fa può essere replicato con PC, smartphone e dispositivi esterni
    - L'hardware è in questo caso dedicato ai test di penetrazione
    - È completamente **open-source** e **personalizzabile**, per cui è possibile estenderlo in qualsiasi modo

Funzionalità e Tecnologie

Funzionalità e Tecnologie

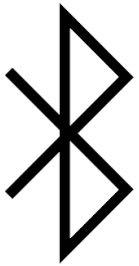
– **Sub-GHz**

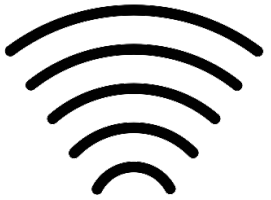
– **Infrared**

– **RFID**

– **NFC**

– **Bluetooth**

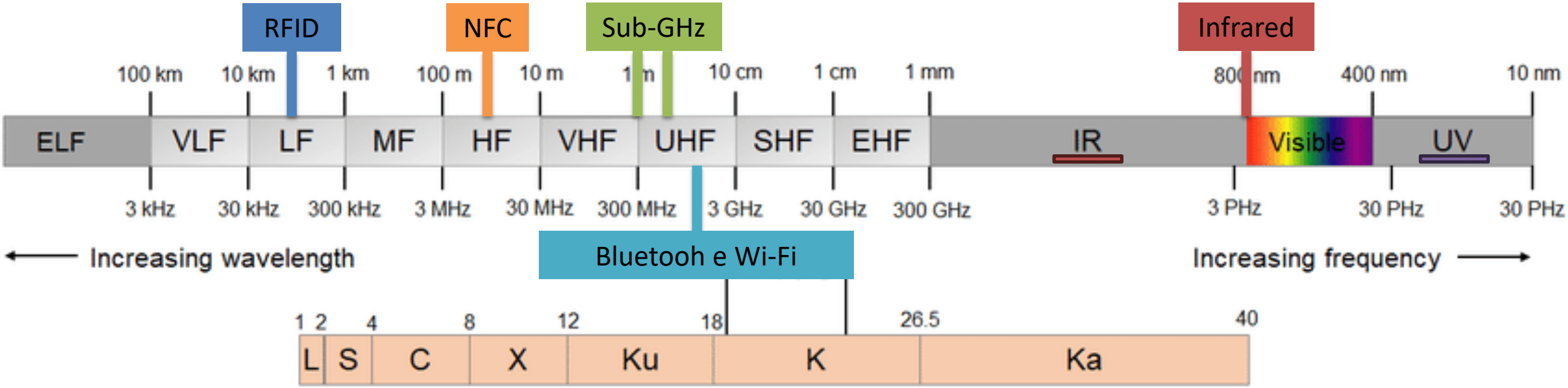




– **Wi-Fi**

Premessa: Spettro Elettromagnetico

- Spettro Elettromagnetico: tutte le possibili frequenze della **radiazione elettromagnetica**



Funzionalità e tecnologie: Sub-GHz

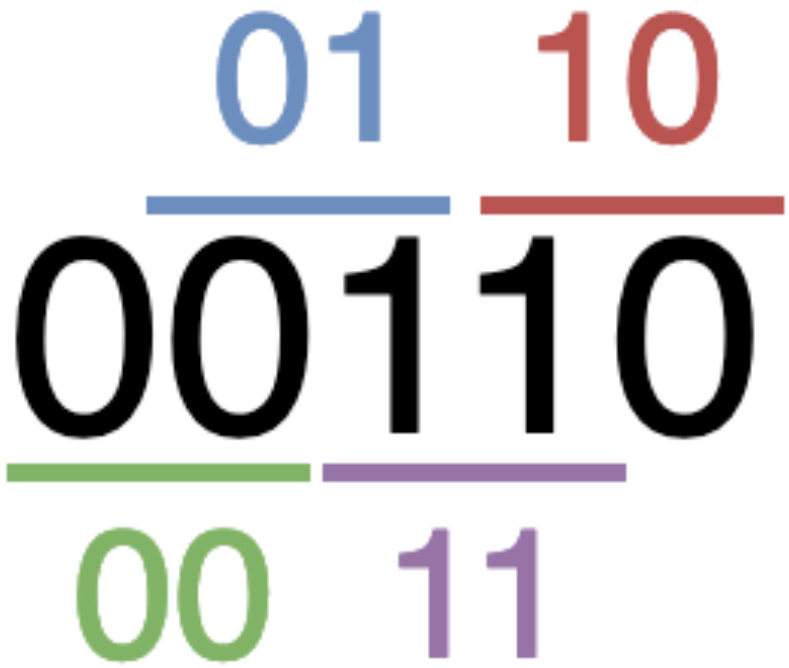
- Sono le frequenze sotto il Ghz e vengono utilizzate nei **telecomandi** di porte e cancelli. Un segnale è una particolare sequenza che rappresenta un codice di accesso specifico e può essere Fixed o Rolling

– **Fixed Codes**
  - Il codice / segnale rimane **fisso**
  - Quando il telecomando invia il codice di accesso al ricevitore, se questo lo riconosce sblocca la porta o il cancello
  - Vulnerabile ad attacchi **Bruteforce** (si ottimizza con la sequenza de Bruijn)

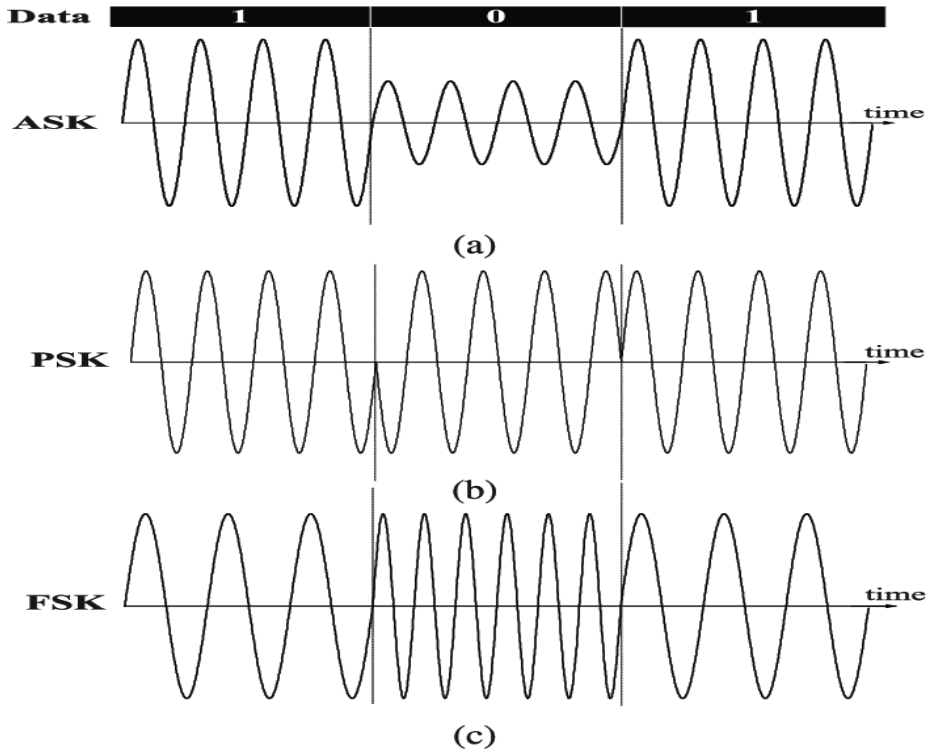
– **Rolling / Hopping Codes**
  - Il codice / segnale **cambia** a ogni utilizzo (in modo **ciclico**)
  - Chiave privata in comune tra trasmettitore e ricevitore da cui si generano le chiavi pubbliche
  - Una volta che un segnale è stato usato, non si può più riutilizzare

Funzionalità e tecnologie: Sub-GHz

- Sequenza **de Bruijn**
  - 5 bit al posto di 8 (00, 01, 10, 11)



- Modulazione
  - Come il segnale è **trasmesso**



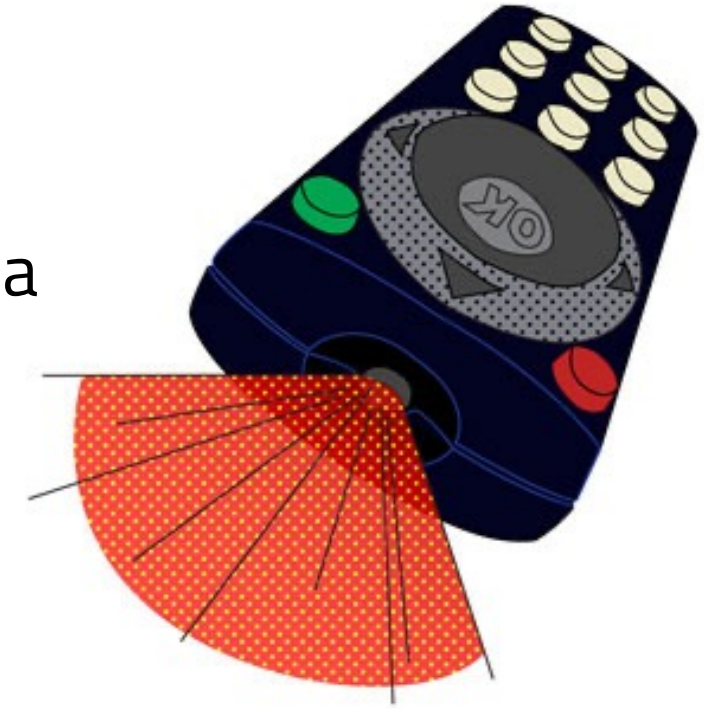
Funzionalità e tecnologie: Sub-GHz

- Il Flipper supporta, grazie al **chip radio** integrato CC1101, la trasmissione e la ricezione di segnali digitali nell'intervallo di frequenze **300-928 MHz** (sotto il GHz)

  – Dispositivi che usano Sub-GHz
    - Sistemi keyless remoti
    - Telecomandi
    - Dispositivi IoT (serrature, campanelli, luci)
    - Barriere e cancelli automatici
    - Porte di garage
    - Chiavi della macchina

Funzionalità e tecnologie: Infrared

- La tecnologia infrarossi viene utilizzata principalmente dai **telecomandi** (a partire dagli **anni 80**) per controllare i dispositivi, quindi come mezzo di trasmissione dati
  - Un LED infrarossi **lampeggia** a una particolare frequenza (modulazione) per evitare le interferenze
  - Il sensore «ascolterà» solo quella particolare frequenza
  - Vantaggi: tecnologia economica
  - Svantaggi: l'infrarosso può essere interrotto se qualcosa si interpone tra il trasmettitore e il ricevitore

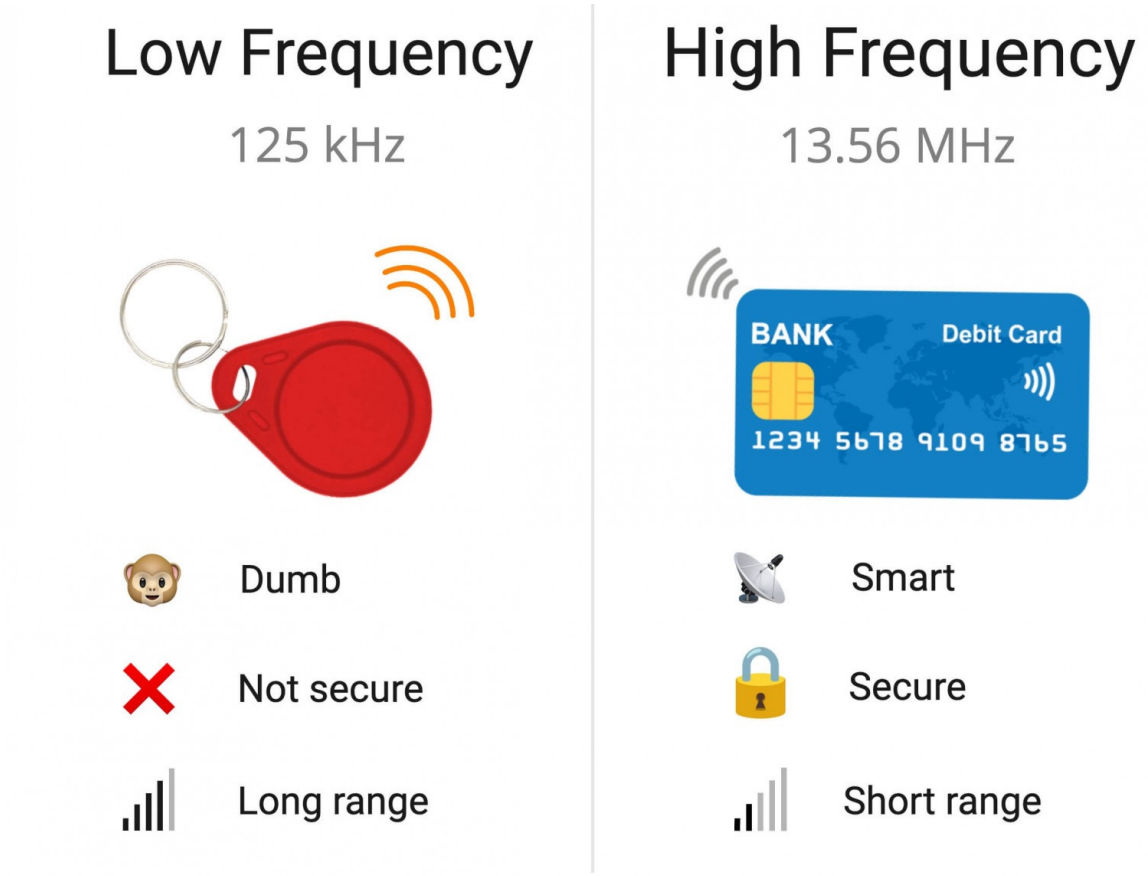


Funzionalità e tecnologie: Infrared

- Il Flipper integra un **LED** e un sensore a **infrarossi**. Il primo permette di inviare segnali mentre il secondo di rilevarli (velocità, trasmissione e frequenza)
  - Alcuni modelli di smartphone hanno la stessa funzionalità
  - I dispositivi che usano infrarossi
    - TV
    - Condizionatori d'aria
    - Impianti audio
    - Bluray

Funzionalità e tecnologie: RFID e NFC

- RFID ossia **Radio Frequency Identification** è una tecnologia (**anni 70**) che collega un'identità digitale a oggetti / animali / persone tramite radiofrequenze (**LF**, **HF**, **UHF**)
  - Sistema RFID è composto
    - **Chiave** passiva (tessere o tag) che contiene il chip con l'identificatore
    - **Lettore** attivo: trasmette costantemente energia intorno a sé
  - NFC o **Near Field Communication**
    - Comunicazione bidirezionale



Funzionalità e tecnologie: RFID

- Sul fondo del corpo del Flipper è presente un'**antenna** a **125 kHz** che permette di leggere **carte** e **tag** RFID

  – I dispositivi che usano RFID a bassa frequenza (LF)
    - Impianti sottocute di animali (e talvolta persone)
    - Carte di accesso (alberghi, uffici)
    - Sistemi di controllo degli accessi
    - Portachiavi auto
    - Braccialetti

Funzionalità e tecnologie: NFC

- È dotato di un **modulo NFC** integrato (**13,56 MHz**). Insieme al modulo RFID da 125 kHz, il Flipper può operare sia a bassa frequenza (**LF**) sia ad alta frequenza (**HF**)

  – I dispositivi che usano NFC o RFID ad alta frequenza (HF)
    - Carte prepagate (criptate)
    - Contactless (criptato)
    - Biglietti
    - Abbonamenti
    - Carte d'identità
    - Passaporti

Funzionalità e tecnologie: Bluetooth e Wi-Fi

- Il **modulo** Bluetooth Low Energy (**BLE**) permette al Flipper di interagire come periferica, consentendo il collegamento con dispositivi di terze parti e smartphone

- Una **scheda esterna** Wi-Fi (ESP32-S2) può essere aggiunta alle **18 porte GPIO** (General Purpose Input / Output) del Flipper per aggiungere la funzionalità Wi-Fi

Vulnerabilità e possibili attacchi

Vulnerabilità e possibili attacchi

– Sub-GHz

- Copiare Fixed e Rolling Code (RAW)
- Bruteforcing (sequenza de Bruijn)
- Jamming, Rollback e Rolljam

– RFID

- Copiare tag e memorizzare tag
- Attacchi a dizionario o Bruteforce

– Bluetooth

- Bad Keyboard (Bad Bluetooth)
- Bluetooth Low Energy Spam

– Infrared

- Copiare telecomandi
- Telecomandi universali (Bruteforce)
- Controlling Traffic Lights

– NFC

- Copiare e memorizzare tag (limitato)
- Attacchi a dizionario o Bruteforce

– Wi-Fi

- Beacon Spam, Deauth e Probe
- Evil Portal

Sub-GHz: RollJam Attack

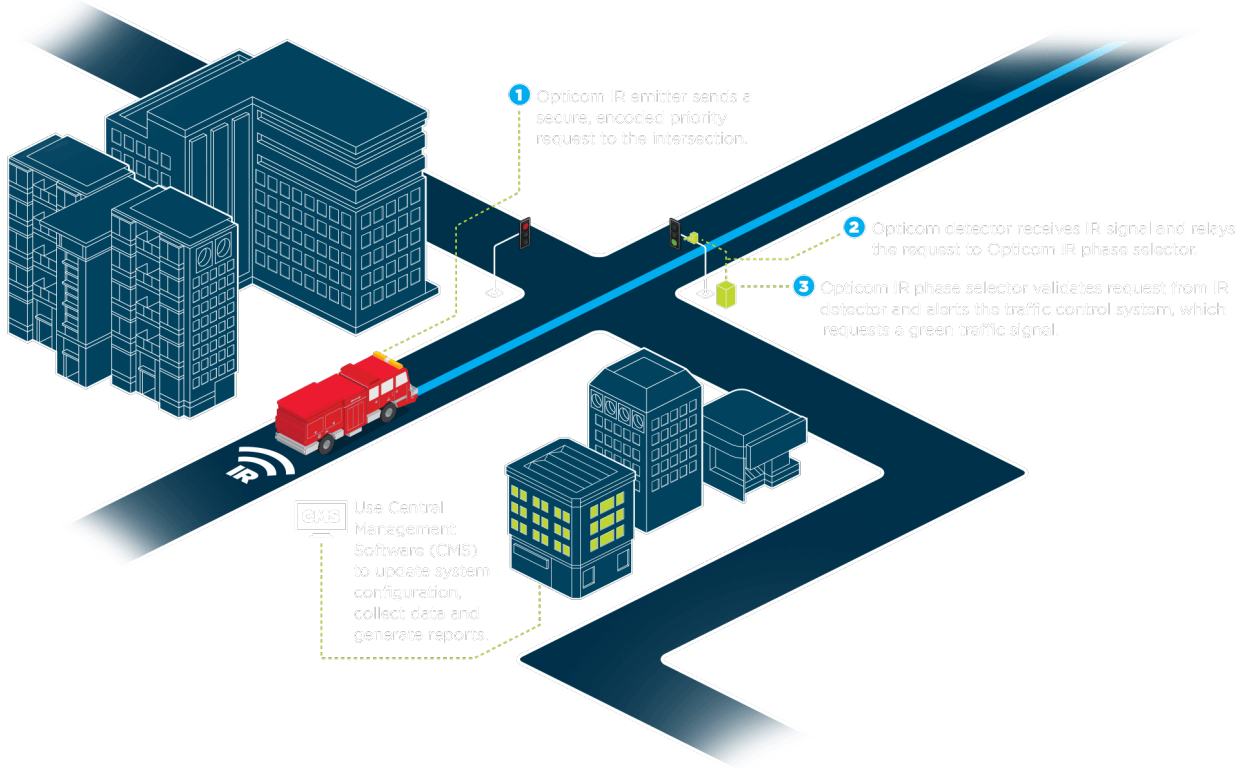
- Attacco che consente di utilizzare il Flipper per aprire le portiere di una vettura, all'insaputa del proprietario, registrando il segnale della chiave

  – Servono due dispositivi (o due moduli radio)
    - Il primo disturba la ricezione del segnale in arrivo verso la vettura (**Jamming**)
    - Il secondo cattura i segnali trasmessi e ne registra le informazioni inviate (cattura un **Rolling Code** valido)
  – Il proprietario si accorge di non essere riuscito ad aprire la vettura
    - Effettua un secondo tentativo. Si registra il secondo segnale e si invia il primo per aprire la vettura, evitando così eventuali sospetti
    - In questo modo si registra un codice (il secondo) valido per una futura apertura

Infrared: Controlling Traffic Lights

- Sfrutta un LED a **infrarossi esterno** (più potente di quello integrato) per inviare un segnale al sistema Opticom, che negli Stati Uniti permette a polizia, vigili del fuoco e ambulanze di ottenere «un'onda verde»

  - Il sistema Opticom utilizza 3 frequenze
    - **14 Hz (alta priorità)**
    - 12 Hz (media priorità)
    - 10 Hz (bassa priorità)



Bluetooth: BLE Spam

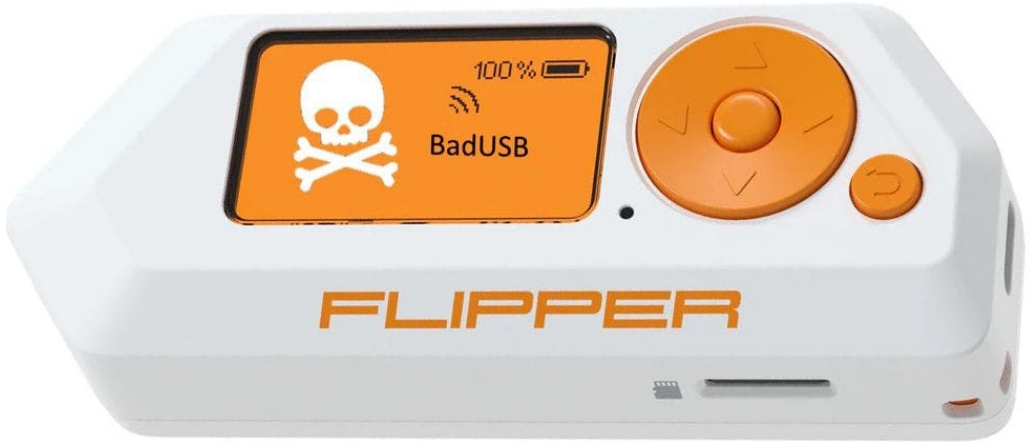
- Il Flipper potrebbe rendere i dispositivi di Apple inutilizzabili, imitando dei dispositivi accoppiabili in realtà inesistenti

  – Si sfrutta il protocollo Bluetooth Low Energy
    - Apple utilizza i pacchetti pubblicitari (**ADV**) per consentire ad altri dispositivi Apple di mostrarsi nell'elenco di quelli pronti a ricevere
    - Il Flipper può effettuare lo **Spoofing** di questi pacchetti e trasmetterli
    - I dispositivi Apple potrebbero essere quindi inondati (**Spam**) da queste notifiche pop-up false

Bluetooth e USB: Bad Keyboard

- Il Flipper può essere collegato via USB (Bad USB) o tramite Bluetooth (Bad Bluetooth) a un computer per effettuare un attacco chiamato **Keystroke Injection**

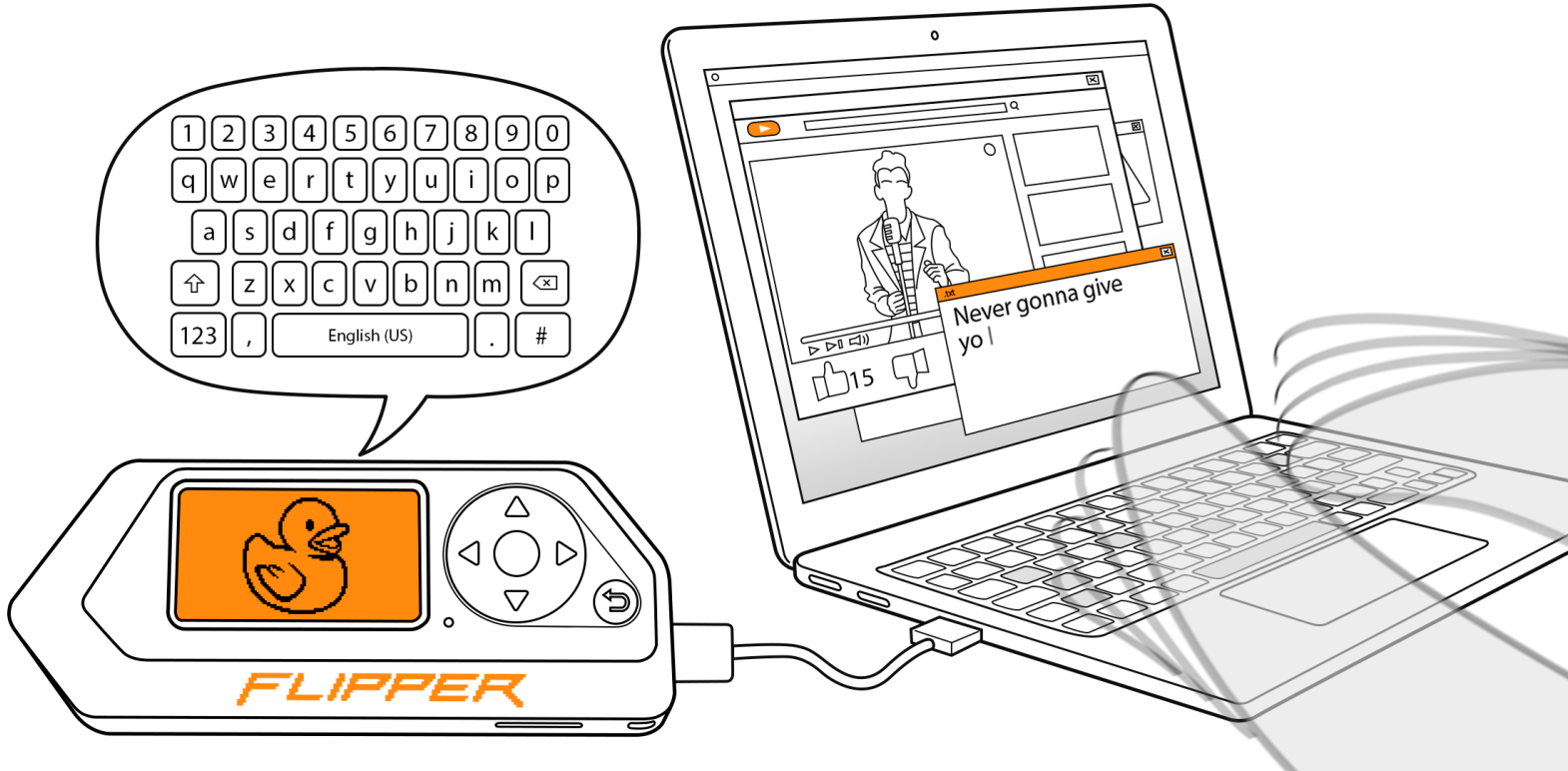
  – Il Flipper si identifica come **tastiera** (HID) simulandone il comportamento
    - Le sequenze di tasti (**payload**) inviate sono programmate e molto rapide
    - Il linguaggio utilizzato è chiamato Rubber Ducky



Bluetooth e USB: Bad Keyboard

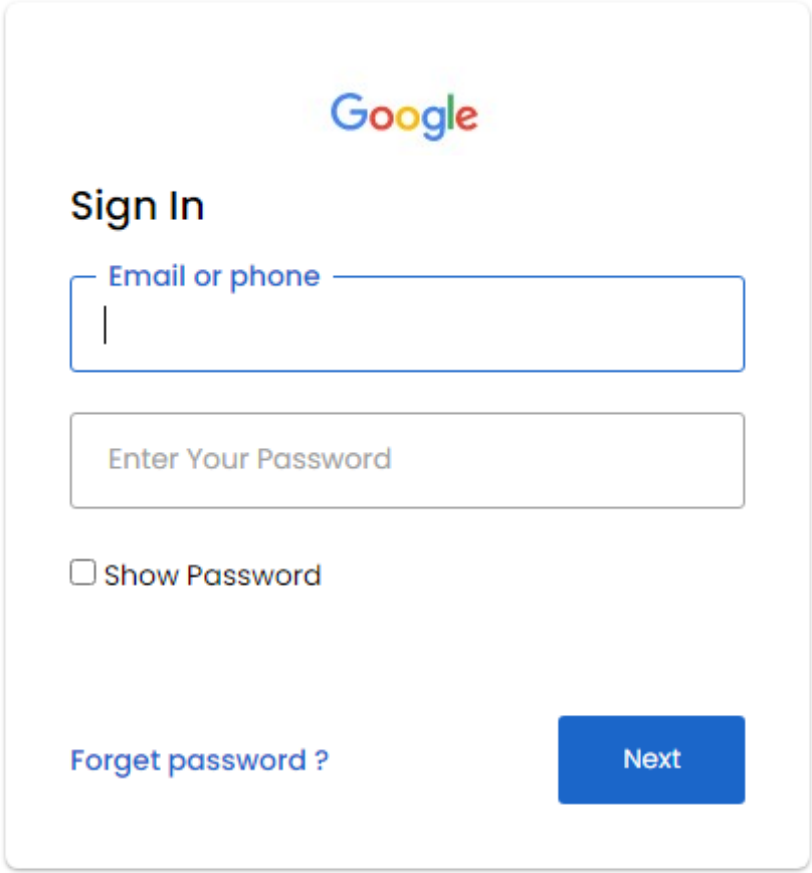
- Un attacco Bad Keyboard richiede l'**accesso fisico** (USB) o l'accoppiamento (Bluetooth) con il dispositivo vittima, il quale deve essere **sbloccato**

  – Si può usare per
    - Installare **malware**
    - Esfiltrare **dati** privati
    - Modificare impostazioni
    - Aprire **backdoor**
    - Avviare shell
    - Recuperare dati



Wi-Fi: Evil Portal

- Trasforma la scheda esterna Wi-Fi in un Access Point aperto. Quando gli utenti si connettono a questo AP, viene visualizzata una schermata di **login fittizia**.
  - Ad esempio, la schermata di login dell'account Google
  - Le credenziali dell'utente inserite vengono inviate al Flipper e salvate in un **file di log**



Considerazioni etiche e legali

Considerazioni etiche e legali

Considerazioni etiche e legali

- L’agenzia delle telecomunicazioni brasiliana (ANATEL) ha sequestrato dei dispositivi Flipper Zero. È giusto o meno?

– Secondo William Budington (Senior Staff Technologist | **EFF**)

- Esistono già **leggi** che criminalizzano gli **atti di pirateria**
- Vietare gli strumenti di hacking non farà altro che rendere i sistemi di sicurezza **più vulnerabili**, limitando l’accesso di coloro che lavorano per proteggere tali sistemi
- I difetti di sicurezza possono essere **corretti** solo una volta **scoperti**, è per questo che serve la ricerca sulla sicurezza

ELECTRONIC FRONTIER FOUNDATION

Considerazioni etiche e legali

- L’agenzia delle telecomunicazioni brasiliana (ANATEL) ha sequestrato dei dispositivi Flipper Zero. È giusto o meno?

– Secondo Marc Rivero (Security Researcher | **Kaspersky**)
  - Vietare i dispositivi non è la soluzione migliore
  - Si dovrebbero stabilire **norme chiare** ed **educare** gli utenti a utilizzare questi strumenti in modo etico e responsabile

kaspersky

Considerazioni etiche e legali

- L’agenzia delle telecomunicazioni brasiliana (ANATEL) ha sequestrato dei dispositivi Flipper Zero. È giusto o meno?

– Secondo Candid Wüest (Vice President of Cyber Protection Research | **Acronis**)
  - Lo strumento in sé non è il problema principale
  - Il **problema** è che esistono ancora **sistemi deboli**
  - Sarebbe come vietare un tool di Bruteforce per proteggere persone che usano **123456** come password

Acronis

Considerazioni etiche e legali

- Il Flipper Zero non sta portando nuova tecnologia, ma sta solo «riconfezionando» cose già **esistenti da tempo**. Un PC può sferrare attacchi della stessa portata o di una portata maggiore (ad esempio una distro **Kali Linux** installata su un PC con una buona scheda Wi-Fi)
- La «colpa» di Flipper Zero, forse, è quella di essere diventato **popolare**

Considerazioni etiche e legali

Tratto da un articolo di **Panorama** («Il boom di Flipper Zero», 25 agosto 2020)

« […] Ancora nel secolo scorso esistevano software utilizzati per controllare il corretto funzionamento delle reti, ma per farlo intercettavano il traffico e consentivano, per esempio, di carpire password in chiaro. Negli stessi anni il Governo degli Stati Uniti intentò una causa contro Phil Zimmermann creatore del celebre software open source PGP per la cifratura dei messaggi. L'autore fu accusato di avere violato la legge sull'esportazione degli armamenti perché dal punto di vista del governo un **sistema crittografico** era paragonabile a delle **munizioni**. Sappiamo bene che rispetto a potenziali "armi" appellarsi al buon senso delle persone non si è mai storicamente rivelato utile. Un intervento normativo, se non fosse su scala globale avrebbe poco senso. Forse una certa **responsabilizzazione** di chi crea, produce e distribuisce oggetti del genere potrebbe essere utile, anche se spesso si tratta di armi improprie, cioè **non concepite per nuocere, ma utilizzabili allo scopo**. Un po' come i coltelli da cucina: qualcuno li usa per affettare il pane, altri le persone. »

Alessandro Curioni (Consulente tecnico-scientifico **Leonardo** Cyber & Security Academy)

Grazie a tutti per l’attenzione

Companies should be using secure technologies. Not security through obscurity.