UNIVERSITÀ DI FIRENZE

Flipper Zero sending updated to Iphon into a never-ending Dos loop

Student:

Gennai Gian Maria

ANNO ACCADEMICO 2023/2024

All'interno di questo report troveremo una spiegazione approfondita per quanto riguarda un tipo di attacco che è stato fatto all'incirca intorno a Novembre del 2023. L'attacco in questione, che potete trovare qui, è banale ma porta l'utente a bloccare le attività che stava svolgendo con il suo dispositivo o comunque ad avere continue distrazioni. Infatti parliamo di un attacco che, tramite un piccolo dispositivo e un segnale bluetooth, riesce a rendere inutilizzabili gli Iphon/Ipad nel suo raggio di azione facendo continuamente aprire dei popups.

1 Flipper Zero

L'oggetto con cui è stato fatto l'attacco è un semplice dispositivo che chiunque può acquistare ed è molto simile ad una chiavetta USB, si chiama Flipper Zero.
Questo oggetto può sembrare innocuo ma, al contrario di alcuni anni fa che per fare attacchi come ad esempio a cancelli elettronici, tv o comunque molti dispositivi a radiofrequenza dovevi avere un minimo di conoscenza su quello che andavi a toccare, adesso basta uno di questi dispositivi acquistabili da chiunque per fare un attacco del genere ad un prezzo accessibile.
L'idea di Flipper Zero è quella di combinare tutti gli strumenti hardware necessari per l'esplorazione e lo sviluppo in movimento, quindi è molto pratico da utilizzare anche quando si è fuori casa ed esplora qualsiasi tipo di sistema di controllo degli accessi, RFID, protocolli radio e puoi eseguire il debug dell'hardware utilizzando i pin GPIO.
E' composto da un semplice sistema per interagirci tramite uno schermo LCD e dei pulsanti, poi ha vari ingressi per i collegamenti esterni.
Il Flipper Zero è progettato per essere uno strumento versatile utilizzato in ambito sicurezza, adatto a professionisti del settore, appassionati di hardware e penetration tester. Alcuni tipi di attacchi o compiti che il Flipper Zero può facilitare includono:

1. **Attacchi RFID/NFC:** Il Flipper Zero può emulare carte RFID e NFC, consentendo agli utenti di testare e potenzialmente sfruttare vulnerabilità nei sistemi che si basano su queste tecnologie per il controllo degli accessi.

2. **Attacchi Infrarossi:** Dispone di funzionalità per controllare dispositivi infrarossi, il che potrebbe essere utilizzato per simulare attacchi a dispositivi che utilizzano la comunicazione infrarossa.

3. **Trasmissione di Segnali Radio:** Il Flipper Zero può interagire con vari segnali radio, utile per analizzare e testare sistemi di comunicazione wireless.

4. **Hacking Hardware:** Il dispositivo può assistere nelle attività di hacking hardware, come la verifica e l'interazione con componenti elettronici per test di sicurezza.

5. **Test di Controllo degli Accessi:** Grazie alla sua capacità di emulare RFID, il Flipper Zero può essere utilizzato per testare la sicurezza dei sistemi di controllo degli accessi.

Possiamo vedere le varie connessioni e l'hardware del dispositivo nelle figure 1 e 2.

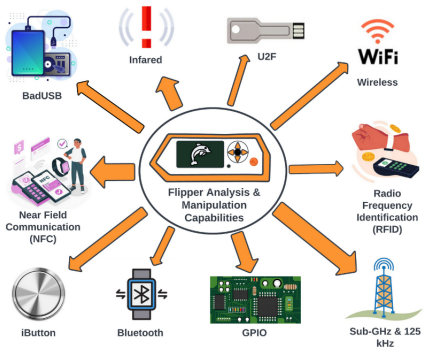

Figura 1: Flipper Zero con varie connessioni a dispositivi esterni

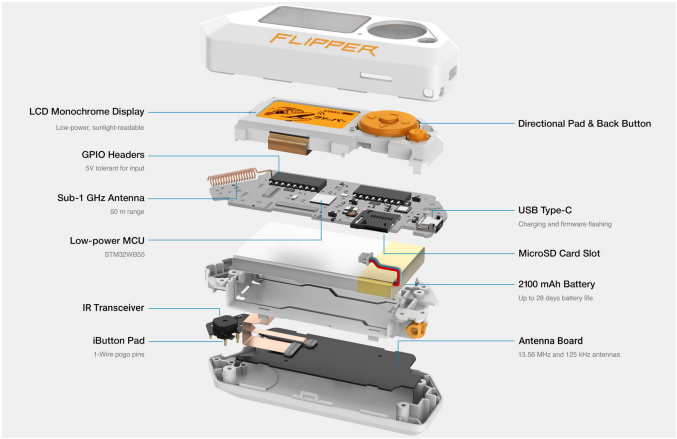

Figura 2: Hardware Flipper Zero

2 Flipper Zero Attack

Durante un viaggio in treno in Olanda il *security researcher Jeroen van der Ham* ha subito un attacco DoS verso il suo smartphone, ad un certo punto il suo Iphone ha iniziato ad aprire una serie di pop-up che rendevano impossibile l'utilizzo del dispositivo. Avendo poi subito lo stesso problema nello stesso giorno, anche sul treno di ritorno dal viaggio che stava facendo e notando che non era l'unico con quel problema ma anche agli altri passeggeri stava succedendo la medesima cosa, ha cercato di trovare una spiegazione e notando uno stesso soggetto che era presente anche la mattina è riuscito a smascherare il colpevole.
Il ragazzo connettendosi tramite il Flipper Zero ai dispositivi IOS con bluetooth

attivo, riusciva a far arrivare popups casuali rendendo l'utilizzo del dispositivo molto difficile e fastidioso. Tutto questo è stato possibile grazie ai radio software che permettono a chiunque di fare attacchi di questo tipo in modo semplice.
Questo ovviamente è un attacco DoS(Denial-of-Service) perché non ti permette di utilizzare il dispositivo che è stato attaccato andando a neutralizzare i servizi che offre solitamente finché non viene scoperta la fonte del problema.
Il ragazzo che stava provocando l'attacco era tranquillamente seduto sul treno con l'Iphon collegato al MacBook in modo da poter continuare a lavorare e senza dare troppa attenzione a quello che gli stava capitando attorno.
Questo attacco ha funzionato particolarmente bene con i dispositivi Iphone e Ipad della Apple perché il funzionamento del loro bluetooth è particolarmente suscettibile a questo attacco con questa strumentazione, probabilmente perché il firmware su cui si basa tutto questo è stato adattato più specificatamente verso questi tipi di dispositivi. Non ho trovato spiegazioni più chiare su come mai il bluetooth Apple dovrebbe essere più suscettibile rispetto a quello di un altro dispositivo, tenendo conto anche che le comunicazioni verso dispositivi che non sono nella sua '*lista dei preferiti*'(ovvero altri dispositivi Apple) li snobba.
Questo attacco è poi stato ricreato proprio da Van der Ham in un ambiente controllato per scopi informativi e ha utilizzato un firmware specializzato che si chiama Xtreme, il quale viene caricato sul dispositivo e fornisce varie funzionalità una tra cui una proprio per attaccare i dispositivi IOS 17.
In un articolo del 25/10/2023 (indicato nella sezione **link**), ho letto che adesso il dispositivo riesce a fare il medesimo attacco anche su dispositivi Android e Windows perché è stata aggiunta questa nuova funzionalità sul firmware Xtreme.

3 Rischi dell'attcco

Per quanto riguarda i rischi che ci troviamo a dover affrontare a discapito di quando è stato appena riportato e quindi dell'attacco tramite Flipper Zero dobbiamo fare due considerazioni differenti.
Per quando riguarda l'attacco di cui abbiamo parlato nella sezione precedente non c'è un rischio vero e proprio perché riesce solo a privarti dell'utilizzo delle funzionalità del dispositivo a corta distanza senza poter andare a rubare dati o andarli a modificare quindi una volta allontanato dal raggio di azione del bluetooth il dispositivo riprende il suo normale funzionamento. Quindi i rischi non sono troppo elevati per l'utente, a parte il fatto di ammattire per capire cosa sta succedendo e il non poter svolgere il proprio lavoro.
Per fare una piccola deviazione invece se consideriamo le possibilità di attacco tramite il dispositivo Flipper Zero, possiamo sfociare in problemi molto più seri. Leggendo tra commenti e informazioni in generale ho notato che possono essere clonate porte delle stanze di Hotel(non tutti i tipi), utilizzare il dispositivo per aprire cancelli elettronici, andare a copiare tessere per accedere ad uffici e molto altro(fortunatamente per le carte di credito è un po' più complicato che per le tessere degli uffici), quindi di-

ciamo che in mano a persone male intenzionate può portare ad avere molti problemi.

4 Come si contrasta?

Adesso che sappiamo di cosa si tratta, qual'è la strumentazione utilizzata e quali sono le conseguenze del nostro attacco, possiamo andare ad analizzare le soluzioni a questo problema.

4.1 Chi viene attaccato

Come prima cosa da fare, anche se può sembrare banale, basta disattivare il bluetooth del dispositivo attaccato in modo da renderlo irraggiungibile almeno da quel punto di vista, oppure comunque allontanarsi abbastanza da non essere catturato all'interno del raggio di azione del dispositivo e dato che parliamo di tecnologia bluetooth basteranno 10-15m.
Come abbiamo visto alla fine della sezione 2, adesso lo stesso attacco può essere fatto anche su dispositivi Windows e Android ma in questi dispositivi posso andare, oltre che a disattivare il bluetooth, anche a disattivare le notifiche oppure anche la funzione *Fast Pair* che rende il dispositivo invisibile anche con il bluetooth attivo.

4.2 Chi produce i dispositivi soggetti a questo attacco

A fronte di questo attacco la Apple ha fatto uscire un aggiornamento *IOS 17.2* nel quale viene risolto parzialmente il problema. Da quello che ho appreso leggendo l'articolo che troviamo nella sezione 5, prima di questo aggiornamento l'attacco riusciva a mandare in crash il dispositivo e adesso invece riesce a fare controlli più selettivi facendo aprire solo alcuni popups.

4.3 Dispositivi (ancora) non attaccabili

Ci sono dei dispositivi che, anche se viaggiano su radiofrequenze, non possono essere attaccati tramite il Flipper Zero e un esempio di quello che ho appena detto sono le automobili oppure anche determinate tessere degli hotel. Questi elementi che non possono essere attaccati perché o viaggiano su frequenze al quale il dispositivo di attacco non può accedere o proprio perché ha delle parti di hardware mancanti per riuscire a compiere quell'attacco.

5 Link di riferimento

Qui possiamo trovare i link relativi alle informazioni prese per fare questo elaborato:

- Flipper Zero
- Attacco con Flipper Zero
- Aggiornamento IOS per contrastare l'attacco Flipper Zero
- Attacco Flipper Zero verso dispositivi Android e Windows
- Xtreme