Flipper Zero: Innovación y Casos de Uso
Profesión y Sociedad - PyS 22/23

G14: Jhon Steeven Cabanilla Alvarado, Ángel Manuel Casado Rodríguez, Miguel Chaveinte García, Javier Pericacho Ávila.

Resumen

Flipper Zero es una herramienta innovadora para la seguridad informática y el hacking ético. Permite interactuar con sistemas digitales en tiempo real y hackearlos, lo que posibilita a pentesters (auditor de seguridad informática que simula ataques cibernéticos reales para evaluar la seguridad de un sistema), hackers y aficionados al hardware influir en el comportamiento de estos sistemas.

Inspirado en proyectos de código abierto como Proxmark y HydraNFC, Flipper Zero es una herramienta versátil que ofrece una gran cantidad de funcionalidades en un dispositivo compacto y fácil de usar. Además, es independiente y no requiere de hardware externo para funcionar, aunque es posible conectarlo a un ordenador y ampliarlo, modificarlo e incluso actualizarlo en función de sus necesidades.

Qué pasaría si tuvieras una cerradura electrónica y alguien pudiera abrir tu puerta con simplemente un dispositivo de 170 €, o que te abrieran los puertos de carga de tu coche Tesla [1]; ¿te sentirías seguro? Esto y más cosas se pueden llevar a cabo con Flipper Zero. En este paper vamos a intentar hablar sobre su funcionalidad, casos de uso y demás temas que han convertido al Flipper Zero en innovación, y que esté en boca de todos.

Lanzamiento

Flipper Zero fue anunciado por primera vez en agosto de 2020 en una campaña de recaudación de fondos en Kickstarter, en la que se llegó a recaudar 4.8 millones de dólares [2]. Sin embargo, su lanzamiento al mercado no se llevó a cabo hasta 18 meses después de esta campaña, con una fecha de registro de la patente el 25 de enero de 2022 [3].

Funcionalidad

Algunos usos del Flipper Zero incluyen la manipulación de puertas de garaje y barreras, la creación de imágenes de tarjetas RFID (Identificación por Radiofrecuencia) para emularlas, lector de NFC y el control de dispositivos electrónicos a través de la emulación de dispositivos HID (Dispositivo de Interfaz Humana) mediante infrarrojos.También se puede utilizar como un puente USB para depurar y hacer "fuzzing" de dispositivos, es decir, encontrar y corregir errores o "bugs" en su código[4].

El Flipper Zero puede ser utilizado de manera independiente, sin necesidad de un ordenador u otro hardware externo. Cuenta con un botón de navegación de 5 direcciones y una pantalla LCD que permiten controlar el dispositivo y acceder a sus diferentes funciones. Sin embargo, también se puede conectar a un ordenador o a aplicaciones móviles, lo que permite ampliar, modificar, actualizar y mejorar sus funciones de manera sencilla.

Construcción

En cuanto a su construcción, el Flipper Zero está compuesto por cuatro placas de circuito impreso (PCB) que se producen y testean por separado. Estas placas son la Main PCB, la iButton PCB, la NFC_RFID PCB y la Antenna PCB (Fig:1). Cada una de estas placas cuenta con un conjunto de componentes específico y se somete a un proceso de producción y testeo detallado para garantizar su calidad y confiabilidad (Fig:2)[5].

La Main PCB es la placa principal del Flipper Zero y en ella se encuentran el microcontrolador, la pantalla, la antena de radio y los botones. La iButton PCB tiene pines especiales iButton pogo-pins (conectores eléctricos fiables y resistentes a la conexión y desconexión repetidas), el zumbador y el transceptor infrarrojo. La NFC_RFID PCB tiene los componentes RFID y NFC. Finalmente, la Antenna PCB contiene una antena Wifi dual que se encuentra debajo de la NFC_RFID PCB (Fig:3, Fig:4).

Caso de uso: Imitando un AirTag

Uno de los usos más interesantes de Flipper Zero es la posibilidad de hacerse pasar por un AirTag, el dispositivo de rastreo de Apple. Esto se logra mediante la emulación de la señal Bluetooth del AirTag y la creación de una falsa dirección MAC (dirección física de la tarjeta de red) para engañar a otros dispositivos que intenten detectar el AirTag. Para ello, es necesario utilizar una aplicación llamada "spoof-hci" disponible en la documentación de Flipper Zero.

Una vez configurada la aplicación, Flipper Zero puede transmitir la señal Bluetooth del AirTag y la falsa dirección MAC de forma continua, lo que permite hacerse pasar por un AirTag real. De esta manera, se puede rastrear a una persona o un objeto

sin que ellos sepan que están siendo seguidos.Además, Flipper Zero también puede utilizarse para evitar ser rastreado por un AirTag, creando una señal falsa que impida que el dispositivo detecte la señal real del AirTag(Enlace Hilo-Twitter 1 Enlace Twitter 2).

Caso de uso: Imitando una huella dactilar

Otra aplicación interesante de Flipper Zero es la posibilidad de imitar la huella dactilar de una persona. Aunque Flipper Zero no tiene la capacidad de replicar o falsificar una huella dactilar, puede guardar identificadores en su memoria interna y luego simularlos para suplantar una identificación biométrica, como una huella dactilar. Para ello, es necesario utilizar un escáner de huellas dactilares o una cámara de alta resolución para leer la huella y crear una imagen de la misma. Luego, se puede utilizar la aplicación "fingerjam" de Flipper Zero para enviar la imagen de la huella a un dispositivo que utilice la huella dactilar como medida de seguridad, lo que permite desbloquear el dispositivo como si se estuviera utilizando la huella dactilar original [6].

Sin embargo, es importante tener en cuenta que esto solo funcionaría en sistemas de identificación que no tengan medidas adicionales de seguridad, como una contraseña o autenticación de dos factores. Además, el usuario necesitaría conocer el identificador específico para poder guardarlo en Flipper Zero y utilizarlo para suplantar la identificación biométrica. En general, la utilización de Flipper Zero para imitar una huella dactilar dependerá del nivel de seguridad de la tecnología de identificación biométrica utilizada en el dispositivo.

Foros, proyectos y documentación

Cuenta con un foro oficial[7] y una comunidad en Reddit [8] donde los usuarios pueden compartir sus proyectos y experiencias con el dispositivo. También hay una amplia documentación disponible en su página web que incluye instrucciones detalladas sobre cómo configurar y utilizar el dispositivo, así como diagramas y esquemas que ilustran su funcionamiento interno. Además, hay una serie de proyectos en GitHub [9] relacionados con Flipper Zero, como aplicaciones y módulos de hardware para ampliar sus funcionalidades.

Legalidad

El uso de Flipper Zero puede generar dudas sobre su legalidad debido a la naturaleza de su funcionalidad, que incluye la manipulación de señales de RFID y la emulación de dispositivos HID. Sin embargo, es importante tener en cuenta que el firmware oficial de Flipper Zero no incluye ningún tipo de características potencialmente ilegales, como el bloqueo de señales o la fuerza bruta. Además, el firmware es de código abierto, lo que permite a los usuarios modificarlo o utilizar firmware de terceros si así lo desean. En este caso, toda la responsabilidad recae en el usuario[10].

Para ayudar a los usuarios a utilizar Flipper Zero de forma legal, Lab401, el distribuidor exclusivo de Flipper Zero en Europa, está trabajando en una guía de uso ético que incluirá información sobre cómo utilizar el dispositivo de manera legal para fines de pentesting y otras actividades legítimas. En general, Flipper Zero es un dispositivo legal siempre y cuando se utilice de forma responsable y en conformidad con la ley.

Conclusión

En conclusión, Flipper Zero es un dispositivo interesante y divertido que permite a los usuarios realizar diferentes tipos de hackeo de hardware. Sus ventajas incluyen la capacidad de utilizar diferentes herramientas como NFC, RFID, Sub-Ghz (frecuencias de radiofrecuencia por debajo de 1 GHz) e infrarrojo en un formato compacto. Sin embargo, una desventaja es que el firmware oficial solo permite hacer ciertas cosas, como ataques de reproducción en Sub-Ghz, copiar y emular la identificación única (UID) de NFC, entre otros. Pero el firmware se está actualizando regularmente con más capacidades y la comunidad también está contribuyendo con muchos proyectos divertidos, por lo que Flipper Zero todavía se encuentra en sus primeros estados de desarrollo y solo mejorará con el tiempo.

En general, Flipper Zero puede ser una herramienta útil para aquellos interesados en el aprendizaje y la experimentación con el hackeo de hardware, sobre todo en formato compacto; pero para usos más serios y profesionales, es posible que se necesiten dispositivos más especializados y con una mayor capacidad.

Referencias

[1] R.Stumpf(2022, July 18).Nerds Are Trolling Tesla Owners by Wirelessly Opening Charging Ports.[Online]. Available:Enlace.Last access: 01-12-2022.

[2] T. Nardi (2020, September 2). Flipper Zero blasts past funding goal and into our hearts. [Online]. Available: Enlace.Last access: 29-11-2022.

[3] Apartado de Complience y Patentes de la página oficial de Flipper Zero.[Online]. Available: Enlace.Last access: 27-11-2022.

[4] Lab401, distribuidor en Europa.[Online]. Available:Enlace.Last access: 30-11-2022.

[5] P. Zhovner (2021, June 30). Flipper's Electronics: How it's Made and Tested. [Online]. Available: Enlace.Last access: 29-11-2022.

[6] G. Martí (2022, October 12). La seguridad no está en tu huella dactilar. [Online]. Available: Enlace.Last access: 29-11-2022.

[7] Flipper Zero Official Forum. [Online]. Available: Enlace.Last access: 29-11-2022.

[8] Foro Reddit.Enlace.Last access: 30-11-2022.

[9] Github's Proyectos Flipper Zero: Github Oficial. Github Comunidad.Last access: 03-11-2022.

[10] P. Zhovner (2020, August 3). Under the pressure of unexpected fame. Answering your questions. [Online]. Available: Enlace.Last access: 29-11-2022.

Anexo: Imágenes

Figura 1: Flipper Zero PCBs layout

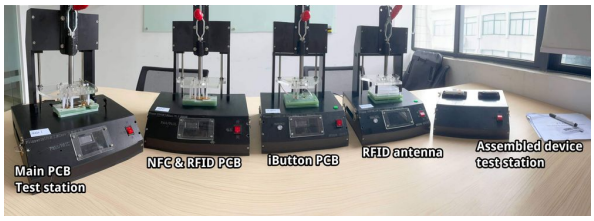

Figura 2: Plantillas de prueba para las 4 placas de circuito impreso de Flipper Zero (Main, NFC_RFID, iButton, Antenna) y del dispositivo ensamblado

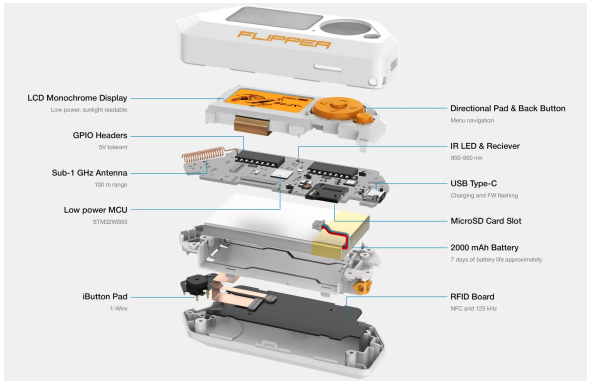

Figura 3: Construcción componentes internos Flipper Zero

Figura 4: Exterior Flipper Zero