**FLIPPER ZERO**

**Introduction**

**Flipper Zero** is a multi-functional portable device designed for hardware hacking, research, and learning. It is particularly popular among cybersecurity professionals, enthusiasts, and hobbyists due to its versatility and user-friendly interface.



* **Using the Flipper Zero Desktop Application**

**1. Download the Desktop App:**

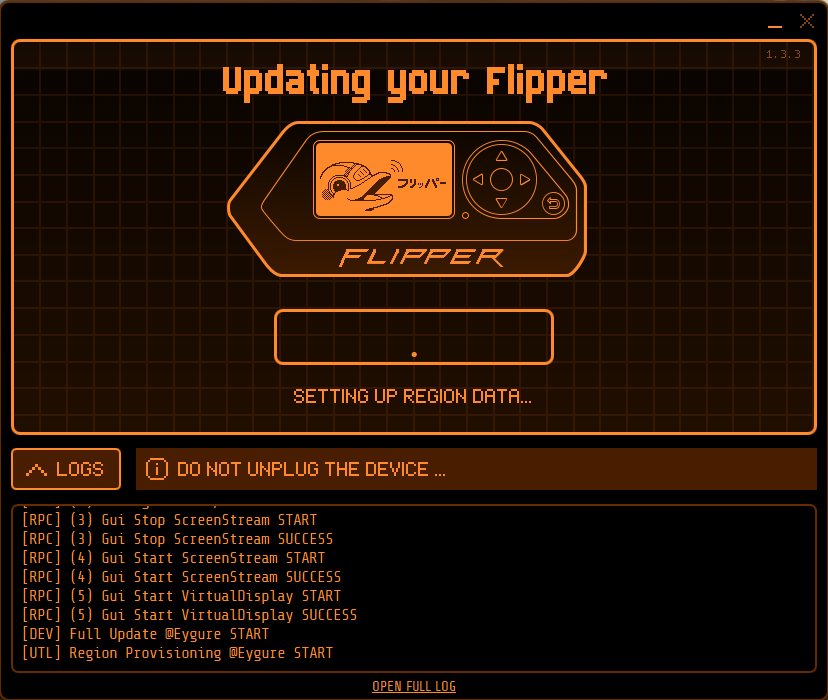
* Visit the [Flipper Zero website](https://flipperzero.one/).
* Download and install the desktop app for your OS.

**2.Connect and Update:**

* + Connect your Flipper Zero to your computer via USB.
* Open the desktop app.
* Follow prompts to check for and install firmware updates.

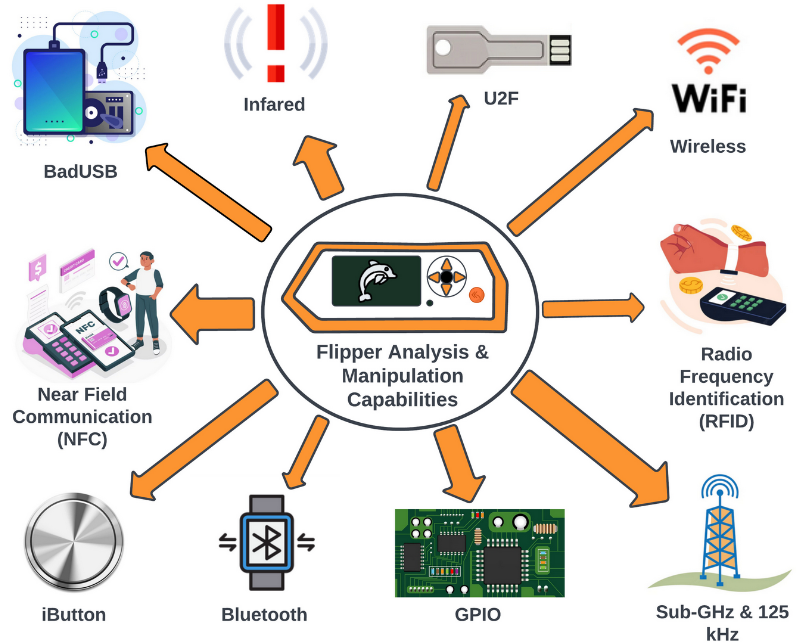
There are three firmware update channels:

* DEVELOPMENT (Dev)
* RELEASE-CANDIDATE (RC)
* RELEASE



**Functionalities**

* **Sub-1 GHz Transceiver:** Allows interaction with a variety of devices using frequencies in the sub-1 GHz range. This includes garage door openers, keyless entry systems, and other RF devices.
* **NFC and RFID:** Reads and emulates NFC and RFID cards, making it useful for tasks like duplicating access cards and experimenting with contactless payment systems.
* **Infrared:** Can transmit and receive infrared signals, enabling it to control TVs, air conditioners, and other IR-based devices.
* **GPIO:** General-purpose input/output pins for connecting to and controlling external hardware like sensors, LEDs, and other electronics.
* **Bluetooth:** Enables wireless communication with other devices, expanding its capabilities and allowing for remote control.



**Activity 1**

**RFID/NFC Analysis:**

Typically, information from RFID and NFC is processed using Flipper Zero. Attempt using fake RFID cards or tags or attempting to duplicate the cards or tags in other ways to find out the weaknesses that are present.

**Attacks on NFC Systems:**

**1. Signal Capture:**

Try using Flipper Zero to clone the RFID/NFC signals of the college ID card you have.

**2. Signal Replay:**

Use recorded RFID/NFC signals to mimic the physical card to achieve the objective of the program.

**3. Data Cloning:**

Swipe your college identification card and input the data on that card like the identification number, or access code etc, and print the same details on another card or gadget.

**Defence on NFC Systems:**

**1. Signal Capture:**

Incorporate shield or encrypt the signal that being transmitted by the RFID or NFC.

**2. Signal Replay:**

Thus, rolling codes, or challenge-response, are to be used for security reasons and to prevent replay attacks.

**3. Data Cloning:**

Ensure that all the data stored on the issuing card is encrypted/securely stored to prevent the above unauthorized cloning.

**Activity - 2**

**2. Infrared Control:**

Using Flipper Zero to control your projector via infrared (IR) is a good way to understand both the functionality and potential security implications of IR-controlled devices. Here's how you can explore attacks and defenses for your IR-controlled projector:

**Attacks on IR-Controlled Projector:**

* 1. **Signal Capture and Replay:**
* **Attack:** Capture the IR signals from your projector's remote using Flipper Zero. Replay the signals to turn the projector on and off.
* **Process:**

Use Flipper Zero to record the IR signals when you press buttons on the projector’s remote.

* Save the recorded signals.
* Replay the signals to control the projector.

**Defense:** Implement rolling codes or unique session identifiers in the IR signal to prevent unauthorized replay.

* 1. **Signal Injection:**

**Attack:** Generate and transmit new IR signals using Flipper Zero to control the projector without needing the original remote.

**Process:** Navigate to Infrared > Universal Remotes > Projects on the Flipper Zero.

Experiment with different IR codes to see which ones control the projector.

**Défense:** Use IR signals with complex, encrypted protocols that are harder to replicate or guess.

**3.Denial of Service (DoS):**

**Attack:** Flood the projector with IR signals using Flipper Zero, causing it to become unresponsive.

**Process:** Continuously transmit IR signals towards the projector.

**Défense:** Implement rate limiting and signal validation mechanisms to filter out excessive or malformed IR signals.

**Defences for Your IR-Controlled Projector:**

1. Encryption
2. Rolling Codes
3. Signal Validation

**Practical Steps to Test and Defend:**

**1.Capture IR Signals:**

* Point your projector’s remote at Flipper Zero.
* Use Flipper Zero to record the IR signals for various functions like power on/off.

**2. Replay IR Signals:**

* Use the recorded signals to control the projector via Flipper Zero.
* Test the effectiveness of signal replay and see if the projector responds correctly.

3. **Experiment with Universal Codes:**

* Navigate to Infrared > Universal Remotes > Projects on Flipper Zero.
* Test different universal remote codes to see which ones can control the projector.

1. **Implement Physical Defences:**

* Cover the projector’s IR receiver when not in use.
* Place the projector in a secure location to prevent unauthorized access.
* By understanding how these attacks are performed and implementing the necessary defences, you can better secure your IR-controlled projector and other similar devices.

**Activity – 3**

**Emulate NFC Cards With Flipper Zero to Store any number of Cards in its Memory.**

**Using Flipper Zero with NTAG 15 NFC Tags**

1. **Reading nTAG Tags:**

* Open NFC on Flipper Zero.
* Place the nTAG 15 tag near the NFC reader.
* Flipper Zero will read and display the tag’s data.

1. **Emulating nTAG Tags:**

* Save the read nTAG 15 data on Flipper Zero.
* Select the saved profile from the NFC menu.
* Choose the Emulate option to use Flipper Zero as the nTAG 15 tag.

1. **Storing Multiple Tags:**
   * Save multiple NFC tag profiles in Flipper Zero.
   * Switch between stored profiles as needed.

**Applications**

* + **Access Control:** Use for secure access to buildings.
  + **Event Management:** Check-ins and ticketing.
  + **Product Authentication:** Verify product authenticity.
  + **Data Sharing:** Store and share information like URLs and contact details.

