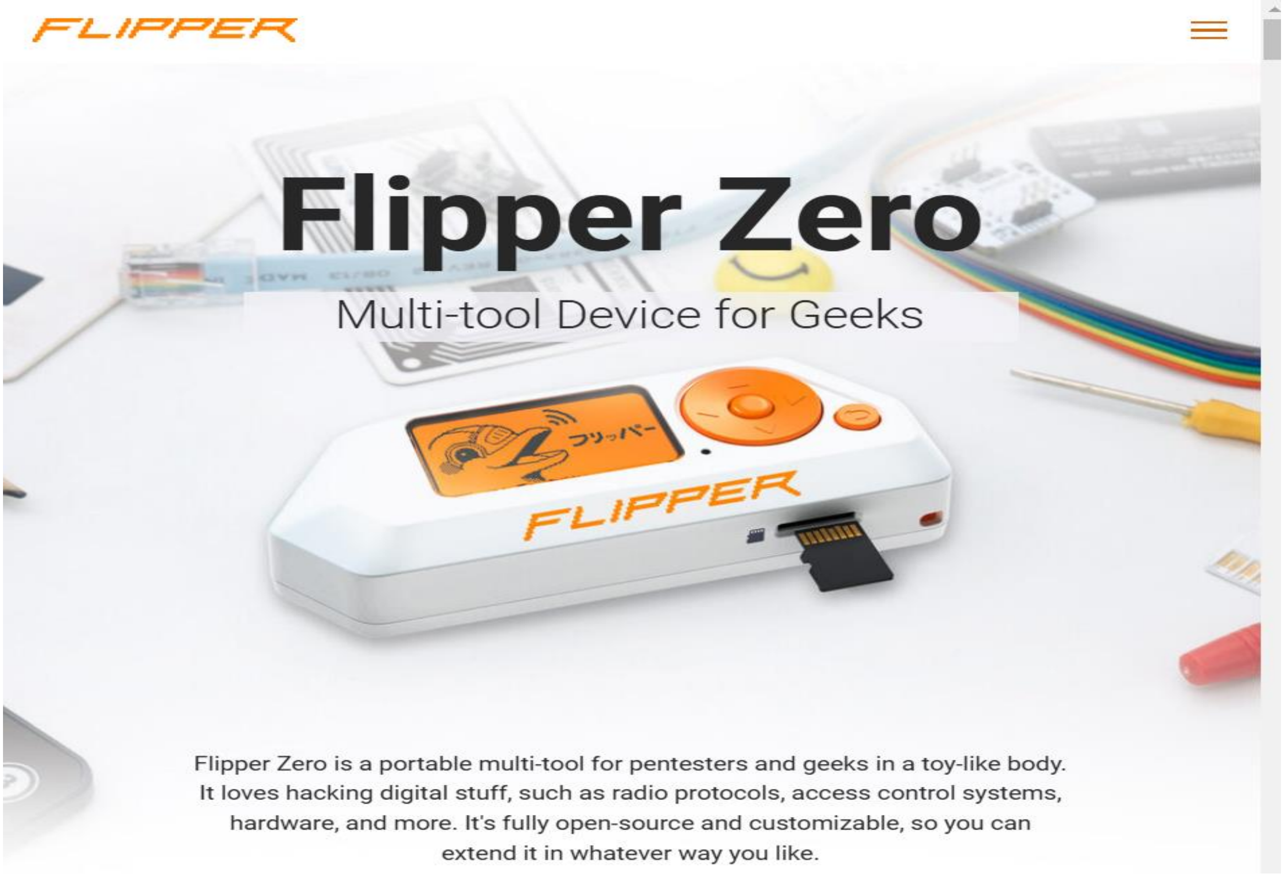
Cyber Security project: Flipper Zero Tool



Flipper Zero

Multi-tool Device for Geeks

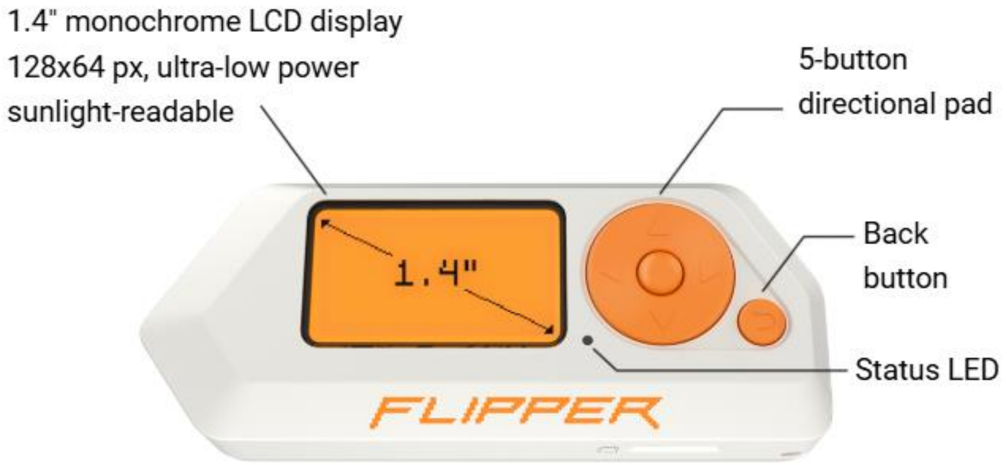
Flipper Zero is a portable multi-tool for pentesters and geeks in a toy-like body. It loves hacking digital stuff, such as radio protocols, access control systems, hardware, and more. It's fully open-source and customizable, so you can extend it in whatever way you like.

- NFC stands for Near Field Communication: It is a wireless communication technology that allows devices to exchange data over short distances, typically within 4 centimeters. It is commonly used for applications like contactless payments (e.g., Google Pay, Apple Pay), access control, data sharing, and pairing devices.

What is Flipper Zero?

Flipper Zero is a portable multi-tool device for hackers, security researchers, and tech enthusiasts. It is designed to interact with a variety of digital and radio protocols, enabling users to explore, debug, and experiment with devices, systems, and access control technologies.

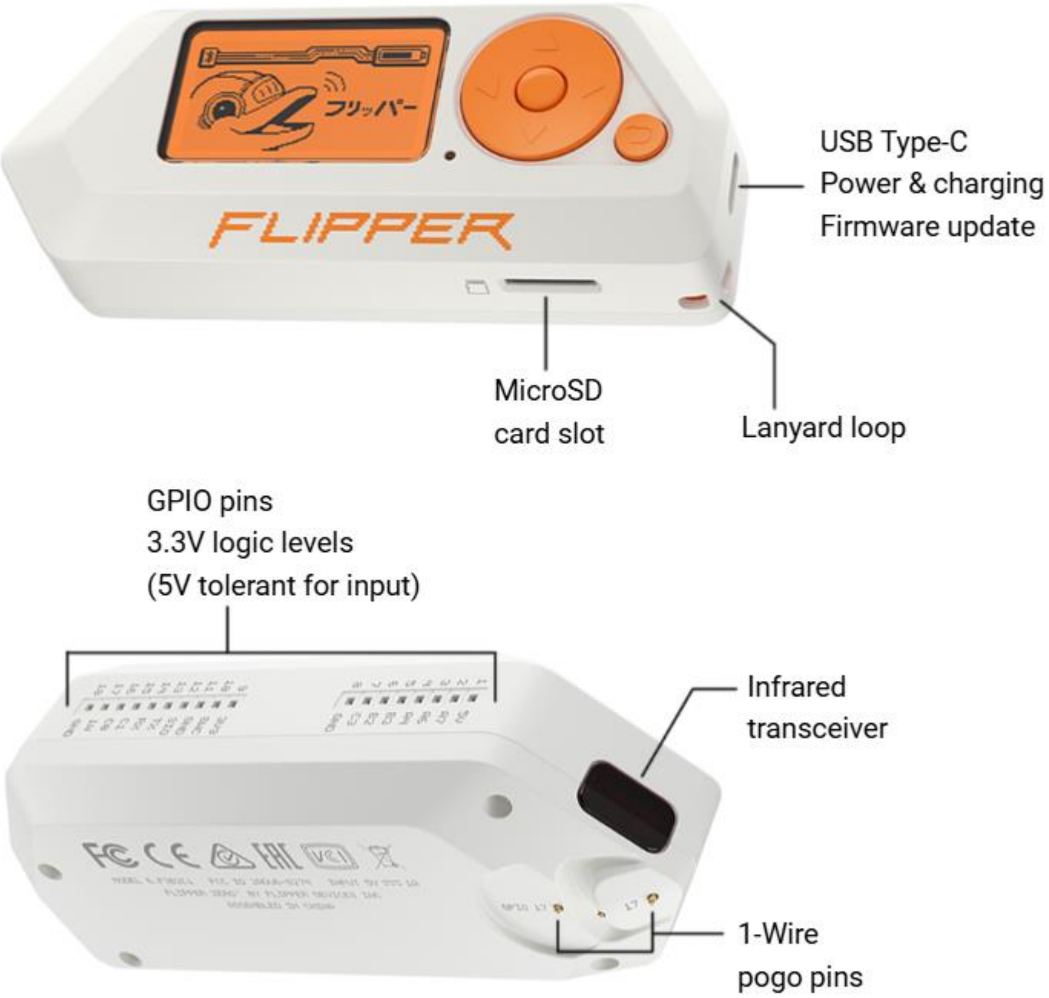
Flipper Zero is a small, smart device with a playful cyber-dolphin personality. It can interact with digital systems around you and improve as you use it. You can explore access control systems, RFID cards, radio signals, and even work with hardware using **GPIO** (General Purpose Input/Output) pins.

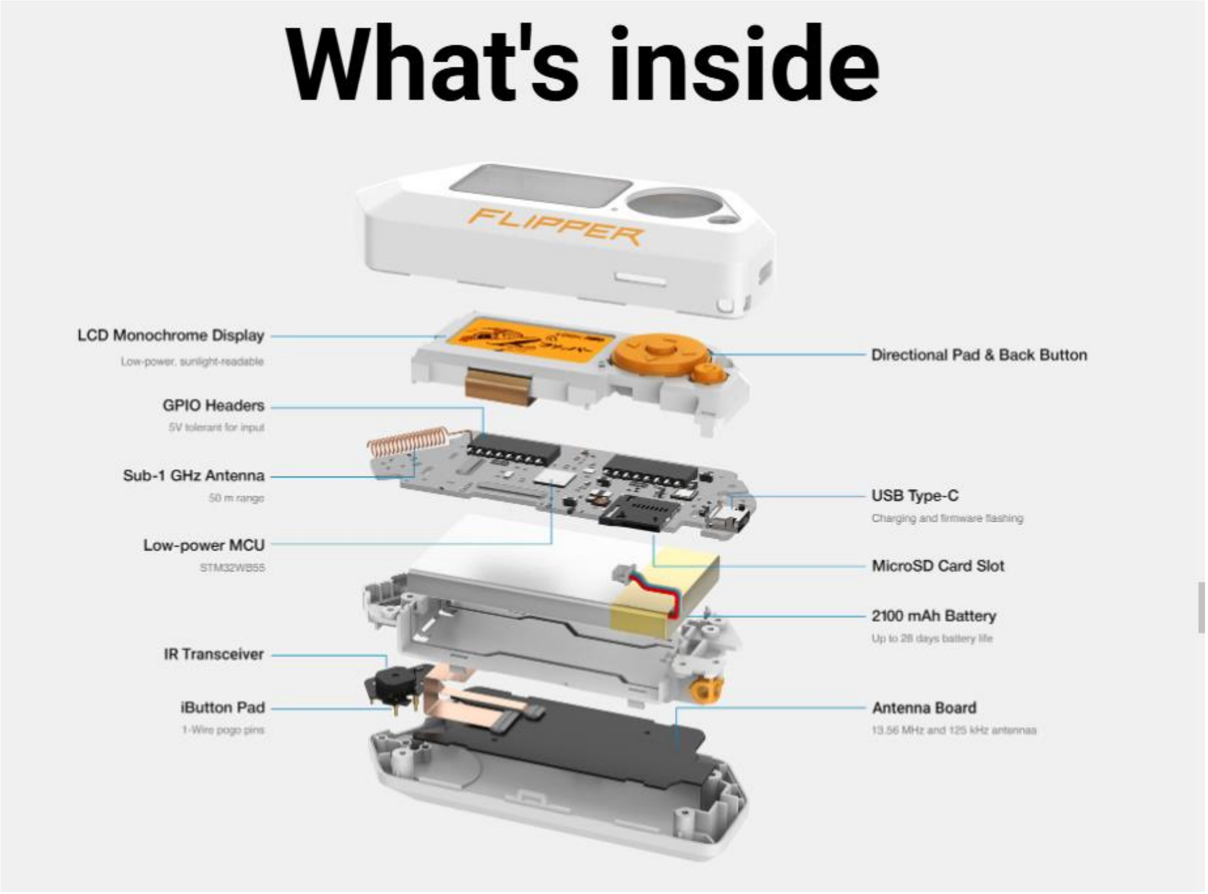


The Flipper Zero comes with a 1.4" monochrome LCD display, featuring a 128x64 pixel resolution, and is designed for ultra-low power consumption. The screen is sunlight-readable, making it easy to use in bright conditions. It includes a 5-button directional pad for navigation, along with a status LED and a back button.

Flipper Zero operates autonomously, meaning you can control it directly using the buttons, without needing a computer or smartphone. The main features are accessible through the Main Menu.

For additional control, you can connect to Flipper Zero via USB or Bluetooth. Instead of using a modern TFT, IPS, or OLED screen, Flipper Zero features a retro LCD display, giving it a unique, old-school vibe.





The important components of the Flipper Zero are:

1. Monochrome LCD Display

- **Purpose**: To display information, menus, and interactions with the device. The display is crucial for user interface navigation and feedback.

2.Button Directional Pad

- **Purpose**: Used for navigating through the menus and controlling the device. This allows you to operate the Flipper Zero without needing a computer or additional peripherals.

3. USB Type-C Port

- **Purpose**: Used for charging, data transfer, and connecting to a computer for firmware updates or interfacing with the device.

4. MicroSD Card Slot

- **Purpose**: Provides expandable storage for storing data such as logs, scripts, or configurations. It can hold extra payloads or information for your hacking projects.

5. GPIO Pins (General Purpose Input/Output)

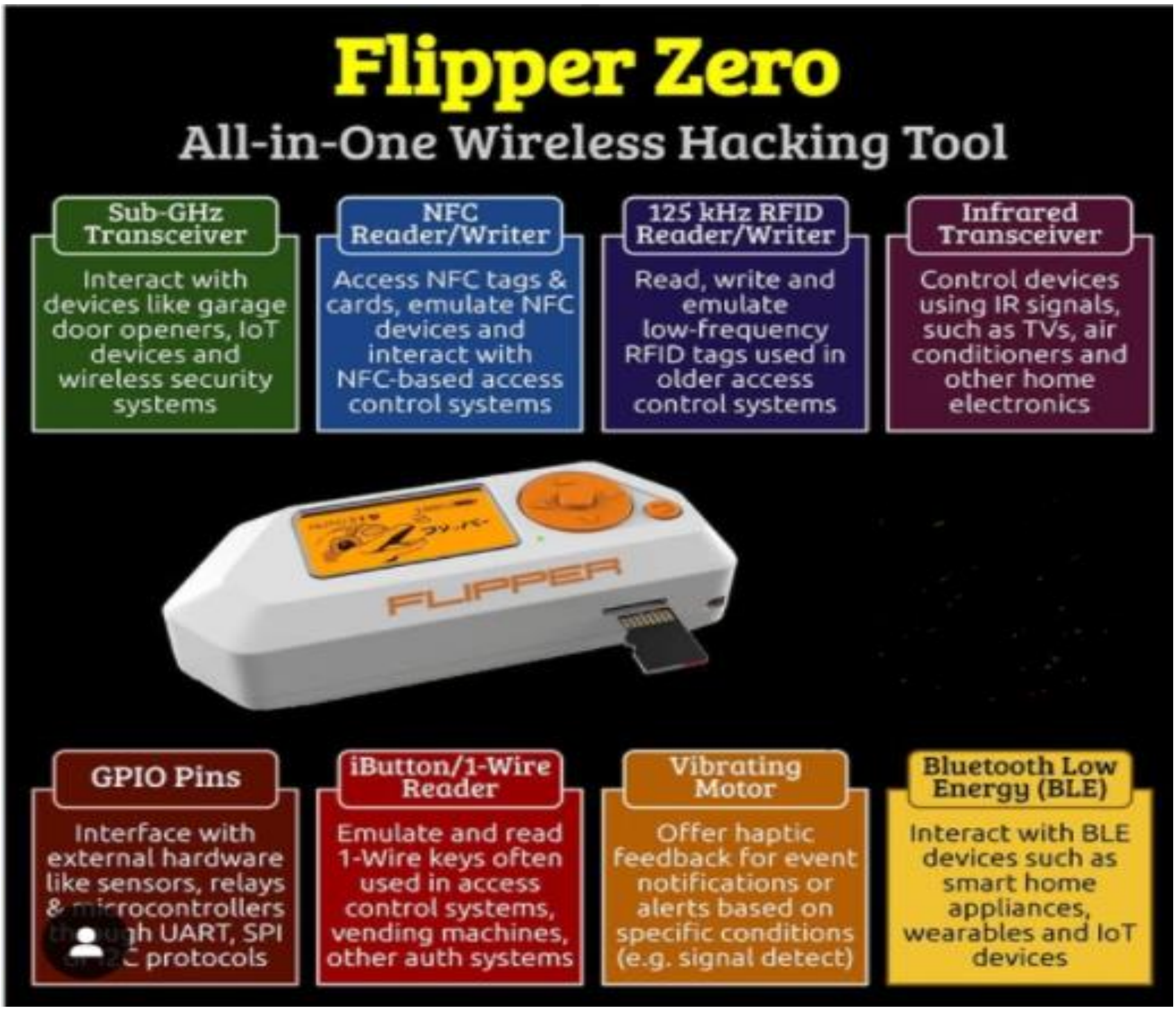
- **Purpose**: These pins allow you to connect external hardware components, such as sensors or other devices. They are critical for experiments and hardware interactions.

6. Infrared Transceiver

- **Purpose**: Allows Flipper Zero to send and receive infrared signals, enabling it to interact with IR-based devices, such as remote controls for TVs, air conditioners, and other appliances.

7. Wire Pogo Pins

- **Purpose**: These pins are used for temporary contact with external devices for debugging or testing, particularly those that use the 1-Wire protocol.



Flipper Zero

All-in-One Wireless Hacking Tool

Sub-GHz Transceiver
Interact with devices like garage door openers, IoT devices and wireless security systems

NFC Reader/Writer
Access NFC tags & cards, emulate NFC devices and interact with NFC-based access control systems

125 kHz RFID Reader/Writer
Read, write and emulate low-frequency RFID tags used in older access control systems

Infrared Transceiver
Control devices using IR signals, such as TVs, air conditioners and other home electronics

GPIO Pins
Interface with external hardware like sensors, relays & microcontrollers through UART, SPI or I2C protocols

iButton/1-Wire Reader
Emulate and read 1-Wire keys often used in access control systems, vending machines, other auth systems

Vibrating Motor
Offer haptic feedback for event notifications or alerts based on specific conditions (e.g. signal detect)

Bluetooth Low Energy (BLE)
Interact with BLE devices such as smart home appliances, wearables and IoT devices

How Does Flipper Zero Work?

- Flipper Zero is a versatile multi-tool designed to interact with digital systems by capturing, storing, and emulating wireless signals. It is widely used for exploring wireless communication protocols, debugging systems, and testing hardware security. Below is a detailed explanation of how it works:
- **Wireless Communication Capabilities**
- Flipper Zero contains various built-in antennas that allow it to interact with multiple wireless signal types:

❖ **Near Field Communication (NFC):**
Flipper Zero can read NFC signals from devices like bank cards, building access cards, and tags. It allows users to save and emulate NFC signals for testing purposes. However, for security reasons, it cannot save or emulate NFC bank cards.

❖ **125kHz RFID:**
RFID signals, commonly used in older access control systems and animal microchips, can be captured and emulated using Flipper Zero. This enables users to analyse and test RFID systems.

❖ **Infrared Signals:**
Infrared communication, typically used in remote controls for devices like TVs and air conditioners, can be read and emulated. Flipper Zero can act as a universal remote by replaying these signals.

❖ **Sub-1 GHz Radio Signals:**
Flipper Zero interacts with devices like garage door openers and car key fobs that use Sub-1 GHz frequencies. It can capture these signals and replay them for testing or educational purposes.

❖ **Steps to Capture and Emulate Signals**

❖ **Select Signal Type:**
The user selects the program that matches the type of signal (e.g., NFC, RFID, Infrared, or Sub-1 GHz).

❖ **Capture the Signal:**
The user holds Flipper Zero close to the source (e.g., an RFID tag or remote) and selects the “Read” function to capture the signal.

❖ **Store the Signal:**
Captured signals are saved in Flipper Zero's internal memory or an SD card for later use.

❖ **Emulate the Signal:**
The stored signal can be accessed and replayed, allowing Flipper Zero to emulate the original device's behavior.

❖ **Hardware Features**

- Flipper Zero's hardware supports additional functionalities:
- **18 GPIO Connectors:**
  These connectors allow it to interface with other electronic devices, sensors, and circuits for testing and debugging purposes.
- **USB-C Port:**
  The USB 2.0 Type-C port connects Flipper Zero to computers for data transfer, programming, and charging.
- **iButton 1-Wire Support:**
  Flipper Zero supports iButton devices, which are commonly used for asset control and tracking.
- **Removable Storage:**
  An SD card slot expands its storage capabilities for signals, logs, and firmware.

- **LCD Screen and Five-Button Control Pad:**
  The display screen provides a simple interface for navigating menus, while the control pad allows users to manage operations.

- **Operating System used for the flipper zero is:**
  Flipper Zero runs on **FreeRTOS**, a lightweight real-time embedded operating system for microcontrollers. This ensures efficient management of tasks, signal processing, and user interactions.

Built-in Hardware Modules:

The Flipper Zero comes with multiple built-in modules to communicate with various technologies:

- **RFID/NFC**: Reads, emulates, and writes RFID/NFC cards (e.g., key cards or payment cards).
- **Sub-GHz Radio**: Transmits and receives radio signals in the sub-GHz spectrum (e.g., garage door openers, remote controls).
- **Infrared (IR)**: Sends and receives IR signals to interact with devices like TVs or air conditioners.
- **GPIO Pins**: Controls or reads signals from external hardware (e.g., sensors or relays).
- **Bluetooth**: Communicates with Bluetooth-enabled devices (requires an external module).

Each module has specific software functionality pre-installed in the Flipper Zero.

For Example: To unlock a car door, you can use the Flipper Zero to read and record the frequency from the car's unlock button. The device saves this frequency, allowing you to replay it later to unlock the car.

However, most modern vehicles use a security feature called **Rolling Code**, which prevents this type of attack from working. Older model cars, however, do not have this feature.

An alternative to the Flipper Zero is using **ESP32 boards** to interact with and "hack" digital devices. ESP32 boards are versatile, affordable, and can be programmed to perform tasks like reading signals, emulating devices, or controlling hardware, making them a popular choice for DIY hacking and experimentation projects.

Real-World Use Cases:

- **real-world scenarios where Flipper Zero has been used, such as:**
  - **<u>Testing RFID/NFC-based access control systems:</u>**
  - RFID (Radio Frequency Identification) and NFC (Near Field Communication) are used in many access control systems, such as:
    - Office keycards
    - Building entry systems
    - Public transport passes
    - Contactless payment cards
  - These systems typically involve a reader and a card/tag. The card contains data (like an identifier) that the reader verifies to grant or deny access.
  - **2. Tools and Equipment**
  - To test these systems, you can use:
  - **Flipper Zero:** Reads, emulates, and writes RFID/NFC cards.

- **Proxmark3:** Advanced RFID tool for deeper testing.
- **NFC-compatible smartphone:** Basic NFC reading/writing apps.
- **Test cards or blank tags:** Used for cloning or emulation.
- **3. Testing Process**
- **Step 1: Scanning the RFID/NFC Tag**
- Place the RFID/NFC tag near the Flipper Zero or compatible tool.
- Use the tool to read the tag's details, such as:
  - Tag type (e.g., MIFARE Classic, ISO 14443A)
  - UID (Unique Identifier)
  - Data stored in sectors/blocks
- **Step 2: Analyzing the Data**
- Check if the tag is encrypted. Many modern systems use encryption to protect stored data.
- If it's an older system (e.g., MIFARE Classic), weak encryption (e.g., CRYPTO-1) may be present, making it vulnerable to cloning or cracking.
- **Step 3: Cloning the Card (For Testing Purposes Only)**
- Use the tool to copy the data from the original tag to a blank tag.
- **Step 4: Emulating the Card**
- Instead of writing to a new tag, emulate the original tag using your tool.

- **Step 5: Testing the Reader**
- Present the cloned/emulated tag to the access control system's reader.
- If the system grants access, it indicates that the system relies solely on the UID and lacks additional security measures.
- **Step 6: Vulnerability Assessment**
- Evaluate:
- Whether the system encrypts communication between the reader and card.
- If encryption keys are weak or easy to extract.
- If the system uses secure practices like rolling codes or two-factor authentication.

4. Attacks and Countermeasures

Potential Attacks:

- **Card Cloning:**
  - Copying data from a legitimate tag to create a duplicate.
  - Countermeasure: Use tags with unique cryptographic keys.
- **Replay Attacks:**
  - Capturing and replaying signals between the card and reader.

    - Countermeasure: Implement rolling codes or session-specific authentication.

- **Eavesdropping:**
    - Intercepting communication between the card and reader.
    - Countermeasure: Encrypt communication (e.g., AES).
- **Brute Force/Cracking:**
    - Breaking weak encryption like MIFARE Classic's CRYPTO-1.
    - Countermeasure: Use secure protocols like DESFire EV1 or EV2.

Preventing Attacks Exploiting Devices Like Flipper Zero:

Flipper Zero and similar tools, while intended for legitimate testing and educational purposes, can be misused for malicious activities. Below is a structured approach to enhancing security across systems, highlighting critical measures.

1. Protecting NFC Systems

- Use Secure Protocols: Implement encrypted NFC communication (e.g., AES encryption) and cryptographic authentication.

- Restrict Access: Use NFC shields or blockers to prevent unauthorized scanning.
- Regular Key Updates: Periodically update NFC encryption keys to prevent cloning.

2. Securing RFID Systems

- Upgrade Legacy Systems: Replace outdated 125kHz RFID systems with modern, secure options like 13.56MHz with AES encryption.
- Use RFID Blockers: Employ RFID-blocking wallets or sleeves for protection.
- Implement Multi-Factor Authentication (MFA): Add layers like PINs or biometrics for critical access.

3. Protecting Against Infrared (IR) Exploits

- Limit Exposure: Keep infrared-dependent devices inaccessible to outsiders.
- Disable Unused Features: Turn off infrared receivers when not needed.
- Use Encrypted Controls: opt for devices with encrypted IR communication protocols.

4. Securing Sub-1 GHz Systems

- Use Rolling or Hopping Code Protocols: Prevent replay attacks with dynamic codes for car fobs and garage doors.
- Limit Signal Strength: Reduce the range of radio signals to prevent long-distance interception.

- Regular Code Updates: Frequently reset and update codes to enhance security.

5. Protecting GPIO and Hardware Systems

- Secure Hardware Ports: Restrict access to GPIO pins and exposed interfaces.
- Use Tamper Detection Systems: Set up alerts for unauthorized access to GPIO-connected devices.

6. General Best Practices for All Systems

- Enable Logging and Monitoring: Track access and log anomalies in communication systems.
- Educate Employees and Users: Train users to recognize suspicious activities like unauthorized scanning attempts.
- Apply Firmware Updates: Regularly update firmware to patch vulnerabilities.
- Encrypt Sensitive Communication: Ensure all wireless communication is encrypted when feasible.

- **Conclusion**
- Preventing attacks requires a multi-layered approach, combining system upgrades, encryption, physical security, and user awareness. By enforcing strong policies and technical safeguards, organizations can significantly reduce the risk of exploitation by tools like Flipper Zero.