

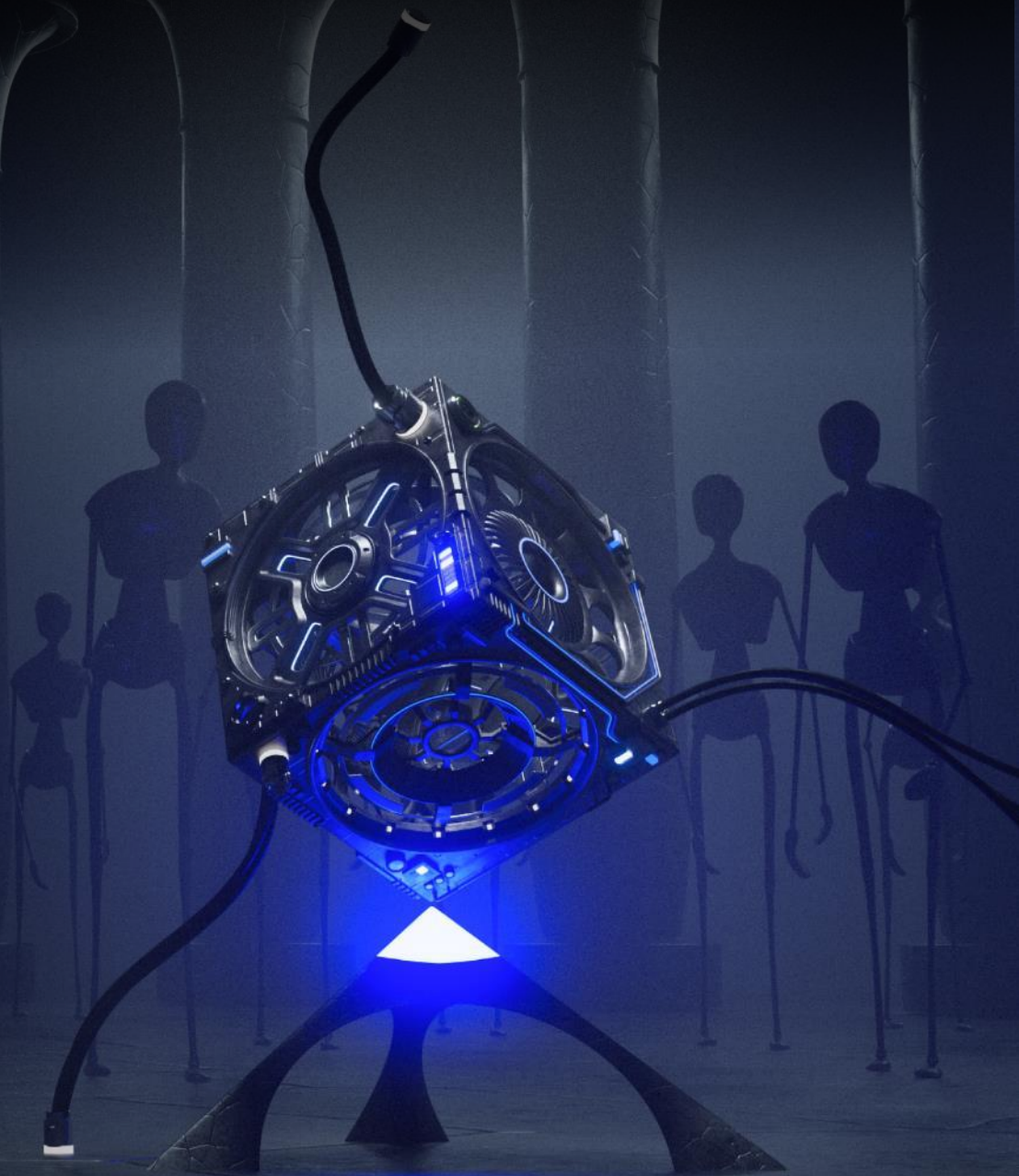


Flipper Zero usage in RedTeam projects

Kumurzhi Georgii

Chief Engineer of the Cybersecurity Department,
PJSC Sberbank

 @gmkmurzhi



Flipper zero itself



Front side



Back side

LCD Monochrome Display

Low power, sunlight readable

GPIO Headers

5V tolerant

Sub-1 GHz Antenna

100 m range

Low power MCU

STM32WB55

Directional Pad & Back Button

Menu navigation

IR LED & Reciever

800-950 nm

USB Type-C

Charging and FW flashing

MicroSD Card Slot

2000 mAh Battery

7 days of battery life approximately

iButton Pad

1-Wire

RFID Board

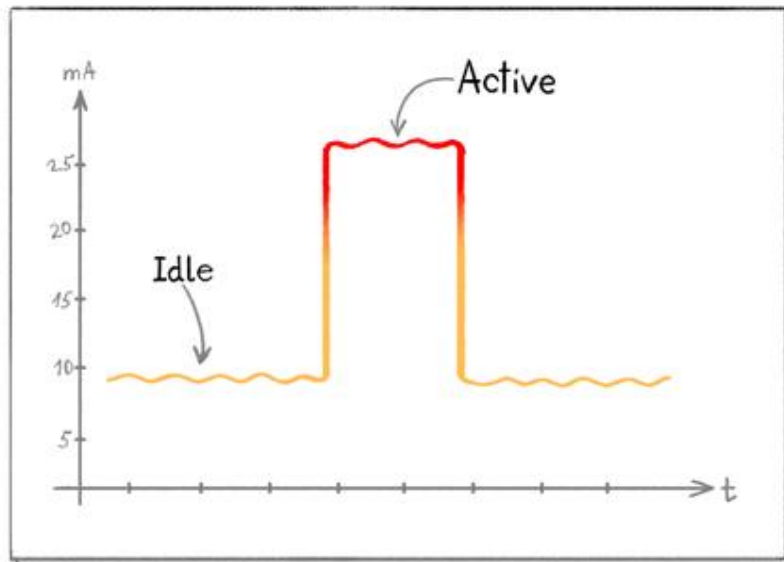
NFC and 125 kHz



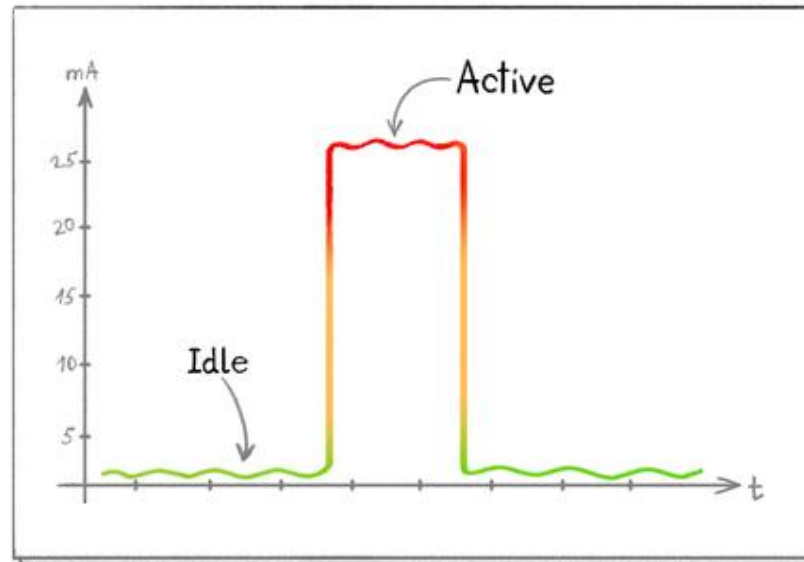
1 Month Battery Life with Firmware Update



Before
Firmware 0.81



After ✨
Firmware 0.82



The new firmware results in power consumption of approximately 1.5 mA in the new deep sleep mode, compared to about 9 mA in the old sleep mode

NOFF ONE
2023



Agenda

- Cloning of RFID/NFC tags used in ACS
- Preparing Flipper Zero for operation
- Variants of behavior when performing an operation
- Masking Flipper Zero
- Existing problems and ways to solve them
- Today's out of scope, but worthy of mention





Cloning of RFID/NFC tags used in ACS

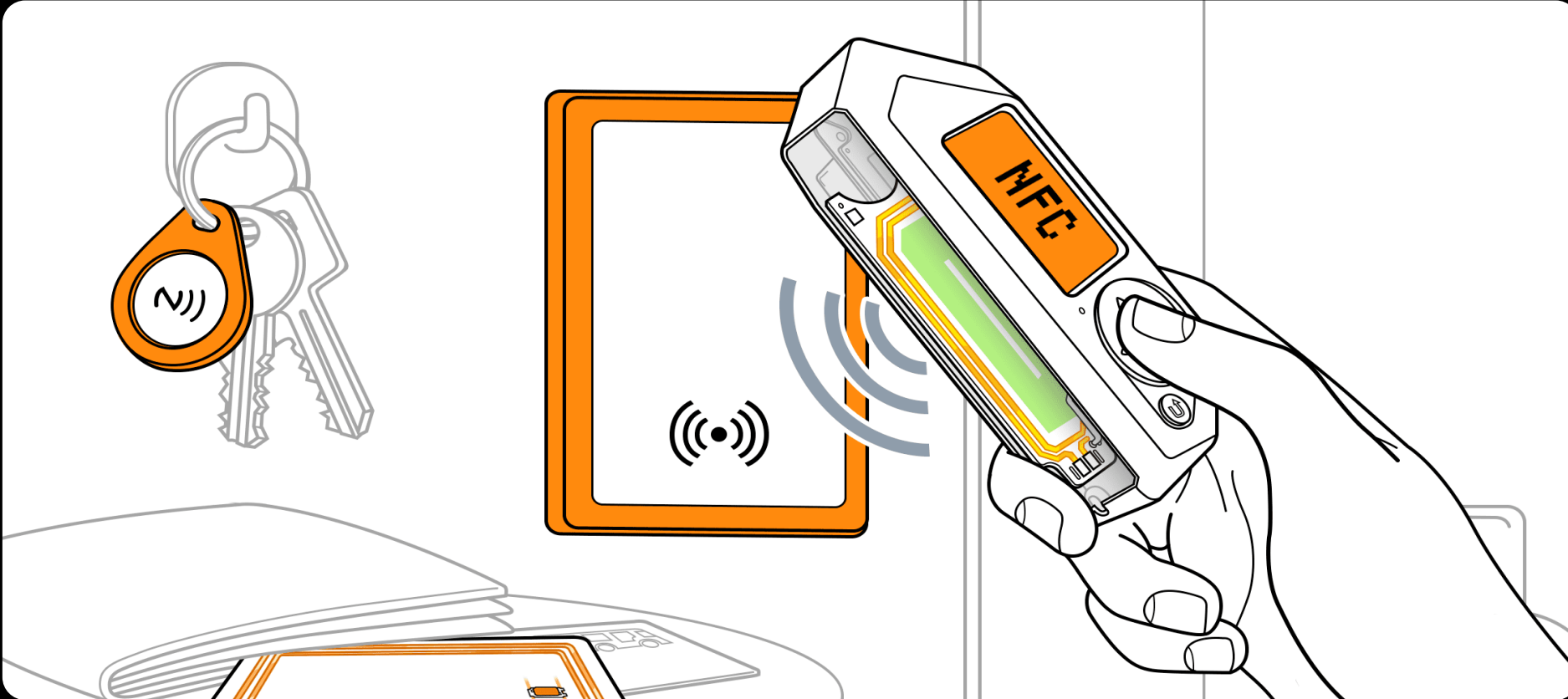


125 kHz RFID



Flipper Zero supports low-frequency (LF) radio frequency identification (RFID) technology that is implemented in access control systems, animal chips, and supply chain tracking systems. Unlike NFC cards, LF RFID cards usually do not provide high levels of security. This technology comes in many form-factors, such as plastic cards, key fobs, tags, wristbands, and animal microchips. Flipper Zero has a low-frequency RFID module capable of reading, saving, emulating, and writing LF RFID cards.

NFC



Flipper Zero supports NFC technology, which is implemented in public transport smart cards, access cards or tags, and digital business cards. These cards have complex protocols and support encryption, authentication, and full-fledged two-way data transfer. Flipper Zero has a built-in 13.56 MHz NFC module capable of reading, saving, and emulating NFC cards.

Evolution of turnstiles



Compact Tripod Turnstile



Full Height Turnstile



Turnstile with Face Recognition Modules

Consequences of the evolution of turnstiles



Something is fashionable



Something has gone out of fashion



??? / This is the end?

Consequences of the evolution of turnstiles



Something is fashionable



Something has gone out of fashion



Something lasts forever...

Consequences of the evolution of turnstiles



Cowboys are in business too!



Preparing Flipper Zero for operation



Preparing Flipper Zero for operation

1.

Go to "**Settings**"->"**LCD and Notifications**" and set the value of the **Volume** parameter to "**0%**", and the value of the **Vibro** parameter to "**ON**"



2.

If you want, in the same menu, you can set the value of the "**LED Brightness**" parameter to "**0%**" so that the LED does not light up at all while using Flipper Zero

3.

If you want to control your Flipper Zero remotely*, be sure to set the "**Bluetooth**" parameter to "**ON**" in the "**Settings**"->"**Bluetooth**" menu



* You can read more about the official mobile application "Flipper" here: <https://docs.flipper.net/mobile-app>

NO
FF
ONE
2023

Are we ready yet?



1. The Way of the Berserker



2. A smarter way



Can you see the gopher? No? Neither can I. But he's here!



Masking Flipper Zero



Disguise option #1: hide in the glasses case

1.

Launch a relevant
RFID/NFC scanner



3.

Close the case and
practice reading data
from RFID/NFC tags, if
you encounter the
"Faraday cage" effect,
then change the case



2.

Then put the Flipper
Zero in the glasses
case and remember
which side of the
case the device is
leaning against with
its lower part



Disguise option #2: hide in an umbrella (1 of 3)

1.

Find a suitable umbrella, in which you can slightly bend the spokes to place the Flipper Zero there



Disguise option #2: hide in an umbrella (2 of 3)

2.

Launch the relevant RFID/NFC scanner and place the Flipper Zero between the bent spokes of your umbrella



Disguise option #2: hide in an umbrella (3 of 3)

3.

Practice reading RFID/NFC tags, it's not that hard ;)



Disguise option #3 (joke):
pretend you're holding a vape



Vape
for sure

Why would it work?



Because on average, **10 cm distance from the Flipper Zero reader to the RFID/NFC tag** will be enough for successful information reading.



There is still one
problem...



The problem is...

When the flipper attempts to read information from NFC/RFID tags, **the vibration response will be the same**, both **in case of successful reading** and **in case of an error during reading**. How do we understand what happened — we will have to waste time moving some distance away from the target to look at the Flipper screen.



The idea of solving this problem:

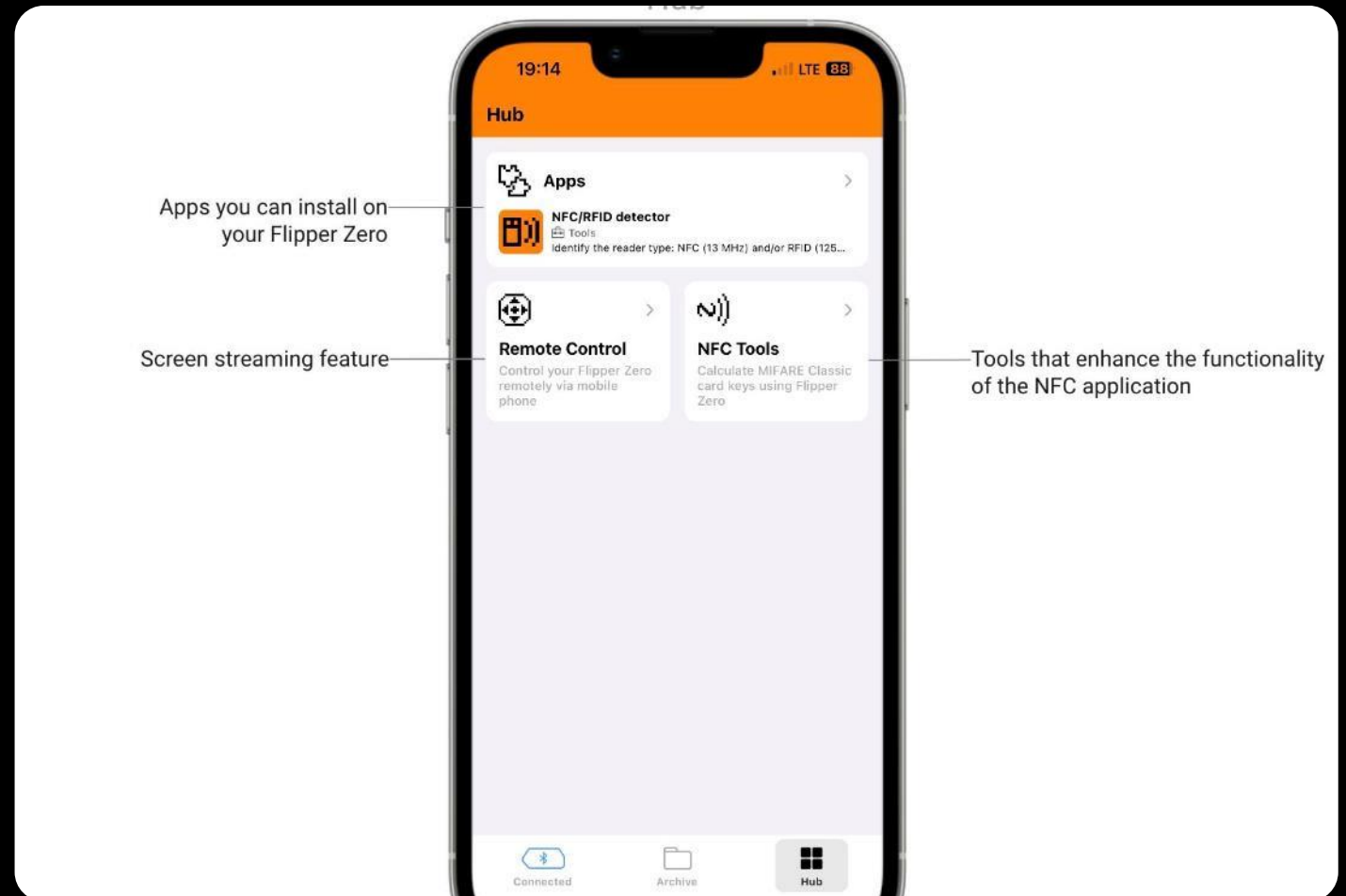
It is possible to patch the source code of the program of the relevant scanner by making the following changes:

1. If an error occurs when reading information, restart the scanner
2. If the reading is successful, save the result in automatic mode and also restart the scanner



The solution that exists today

- With the **Flipper Mobile App**, you **can remotely control** and **update your Flipper Zero**, share saved keys, manage and edit data, and more.
- In the **Hub** tab, you can find apps for your Flipper Zero, remote control feature, and NFC application tools.
- The **Apps** store is completely free and is regularly updated by developers. The best practices used in custom flipper firmware are added.



The solution that exists today

- **"Remote control"** is an absolute **killer-feature** of the **official Flipper Zero firmware**.
- From now on, **all control of the device will take place from the phone**, which you can not let go of your hands.
- No need to waste time getting your well-hidden Flipper in front of everyone and putting it back away.
- Did you see on your phone that the RFID/NFC tag scanner gave an error message? Immediately give the command to restart the scanner and continue to collect the catch!

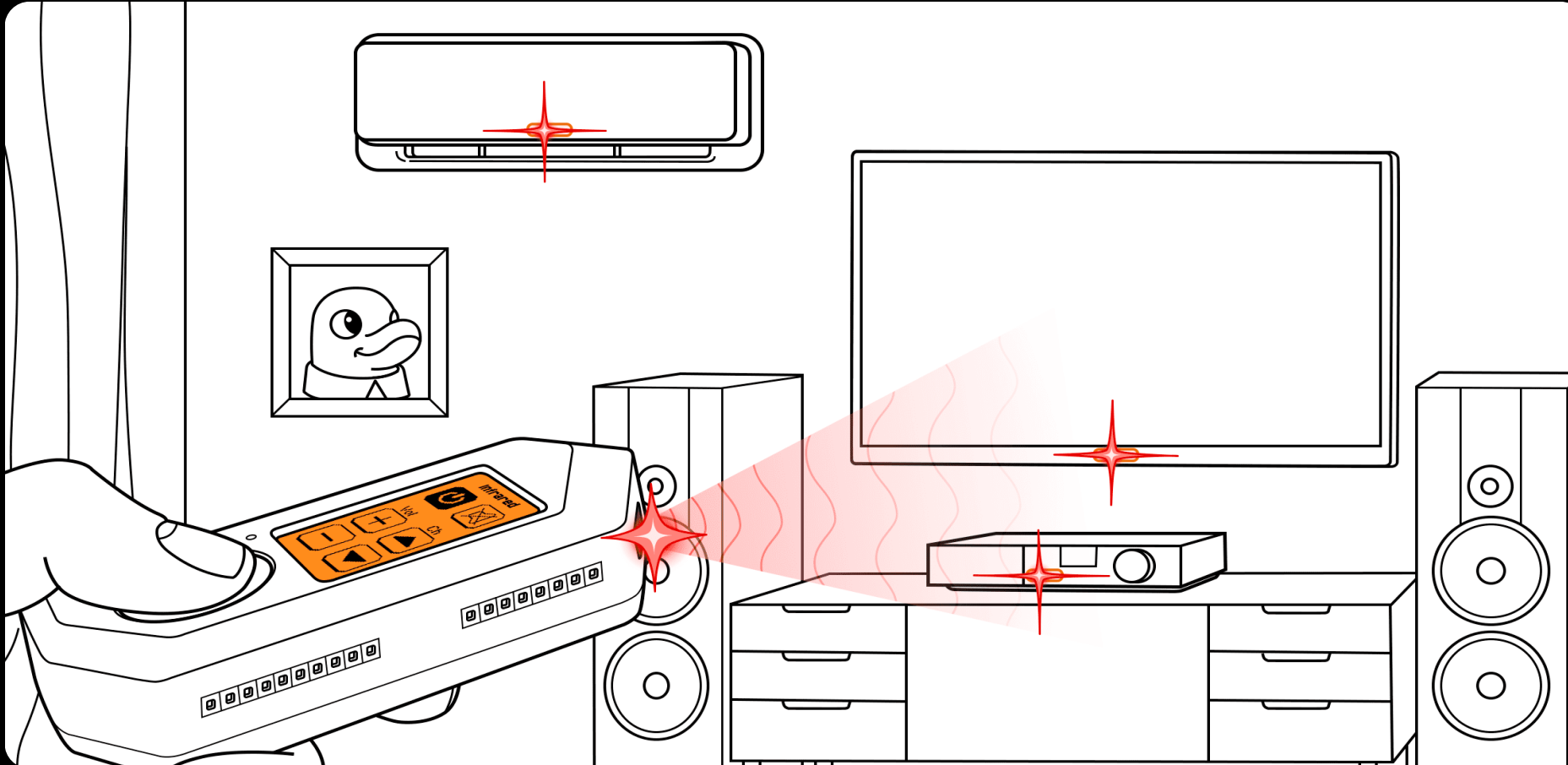




Today's out of scope,
but worthy of mention

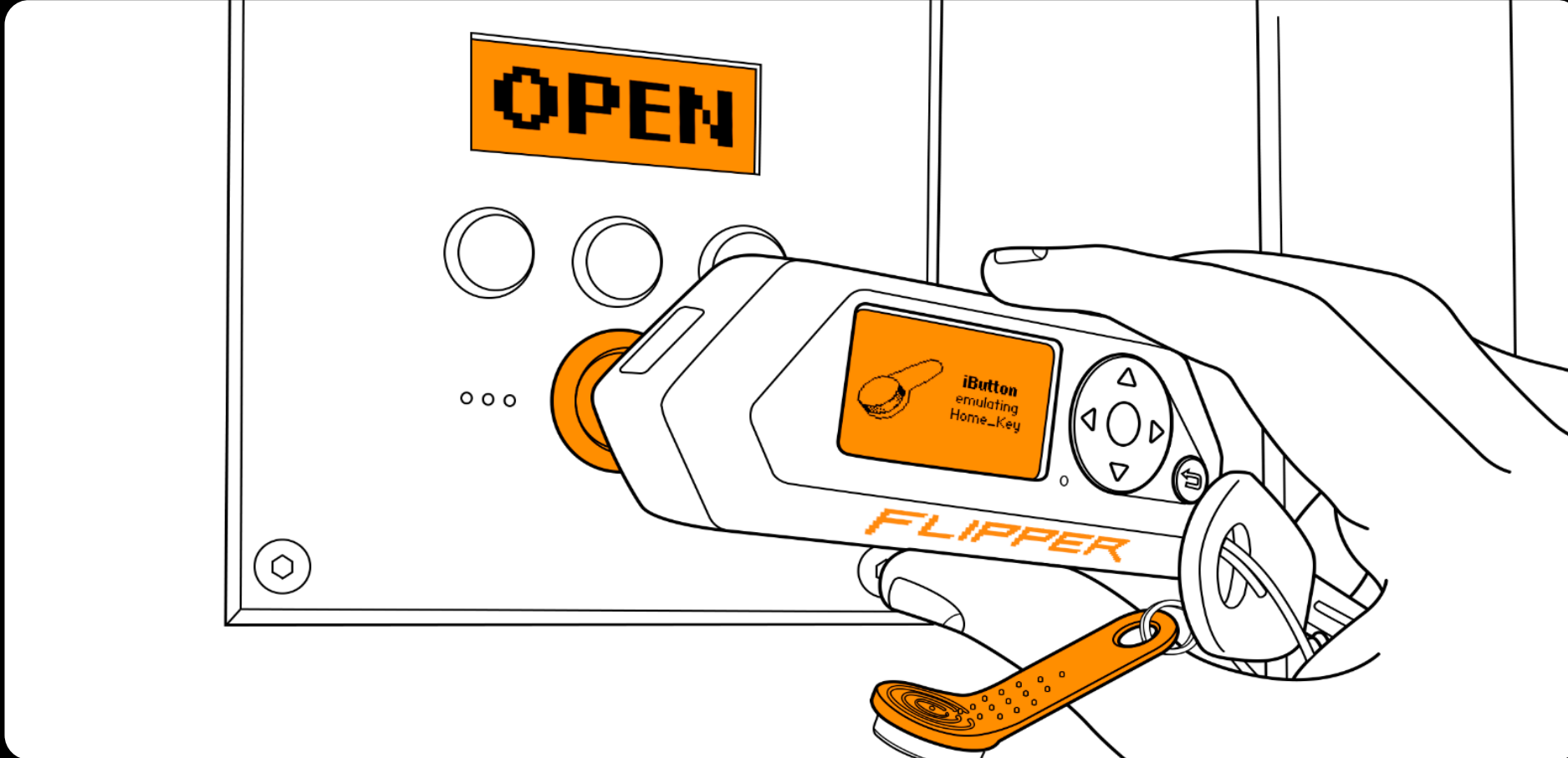


Infrared Transceiver



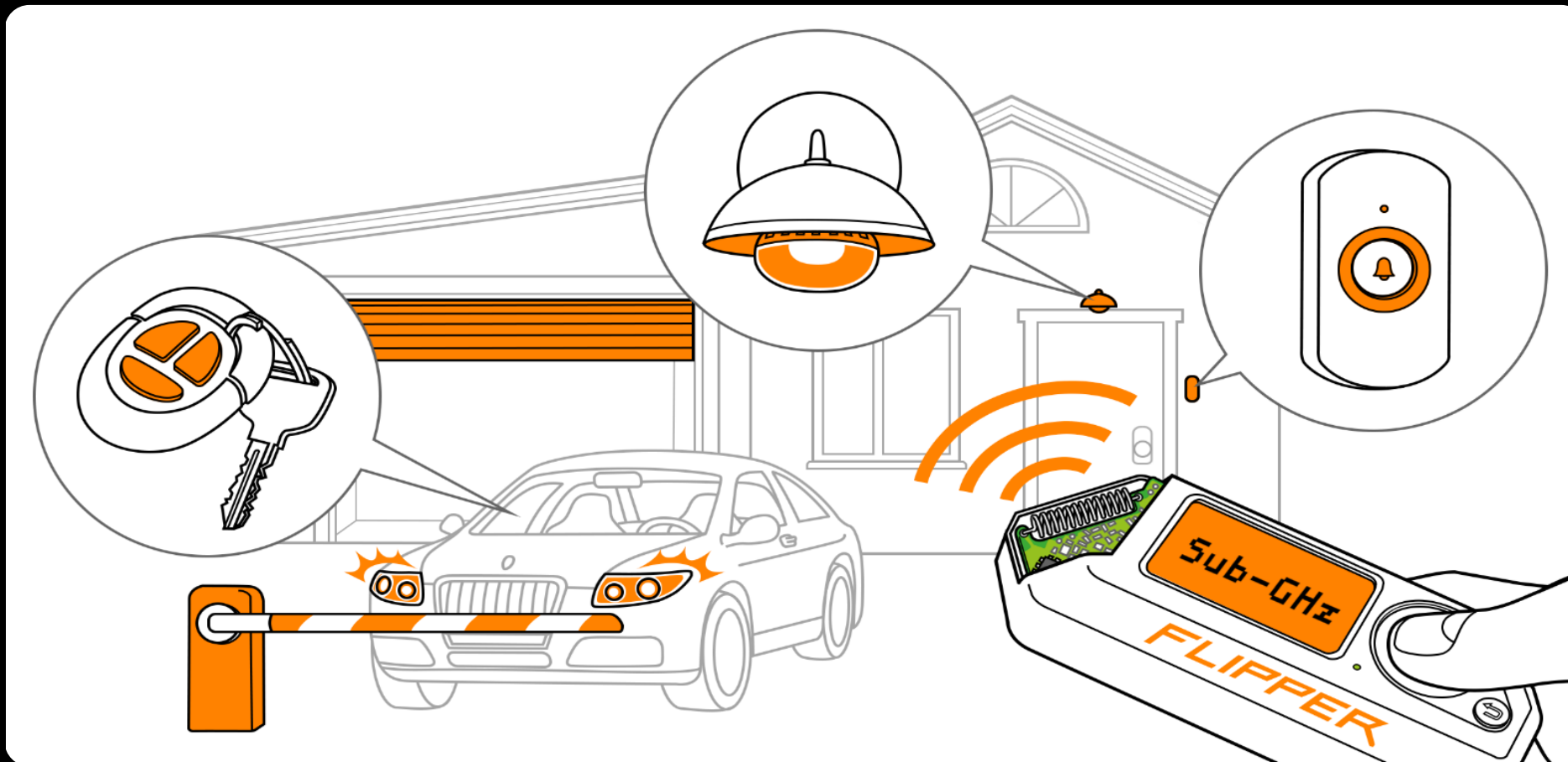
Flipper Zero can interact with devices that use infrared (IR) light for sending commands, such as TVs, air conditioners, multimedia systems, etc. With its built-in infrared module, Flipper Zero can learn and save infrared remotes and use its own universal remotes to control other devices.

iButton. 1-Wire keys (Touch Memory)



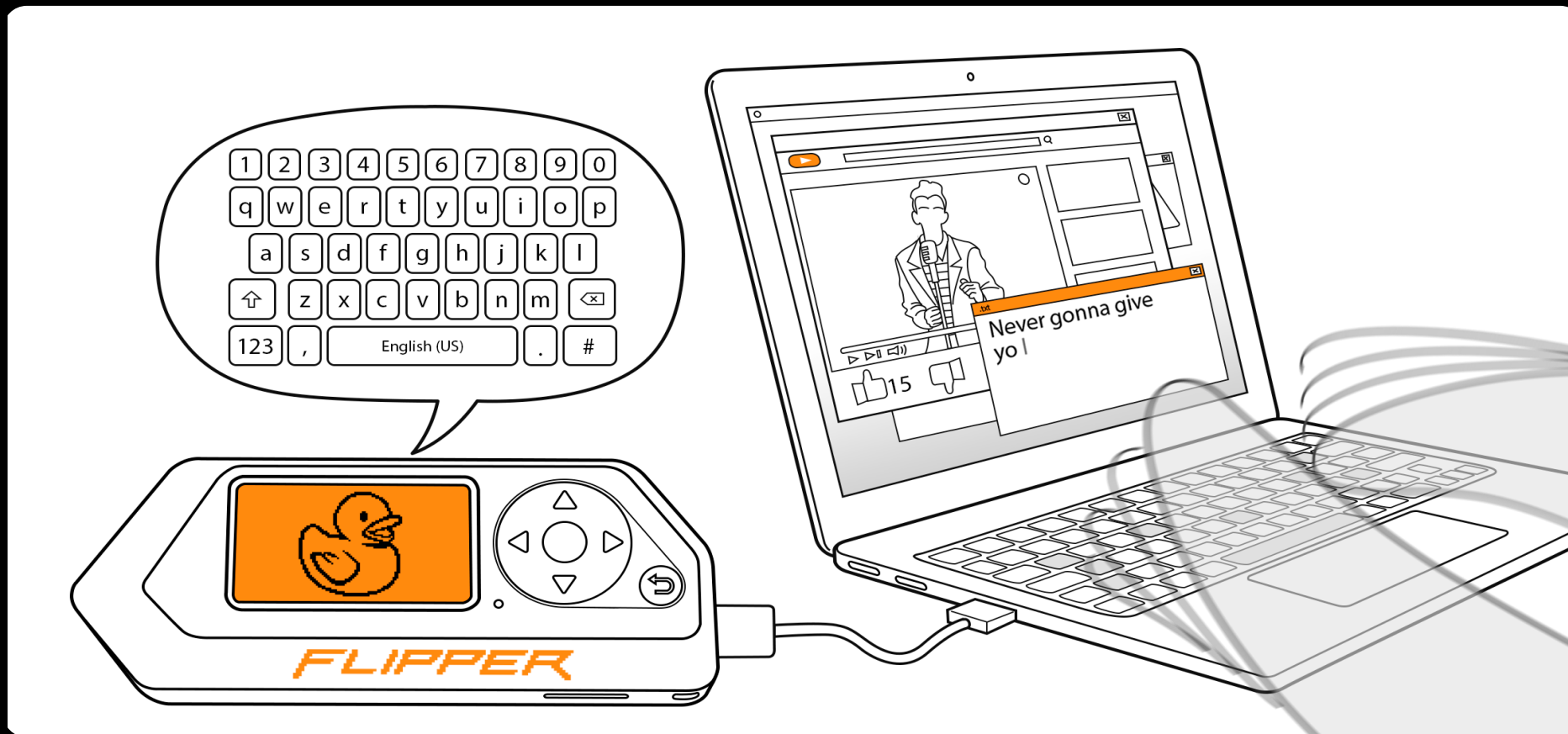
Flipper Zero supports a 1-Wire device communication protocol, which is implemented in small electronic keys known as iButton keys. These keys are used for access control, temperature measurements, humidity measurements, storing cryptographic keys, etc.

Sub-1 GHz Transceiver



Flipper Zero can receive and transmit radio frequencies in the range of 300-928 MHz with its built-in module, which can read, save, and emulate remote controls. These controls are used for interaction with gates, barriers, radio locks, remote control switches, wireless doorbells, smart lights, and more. Flipper Zero can help you to learn if your security is compromised.

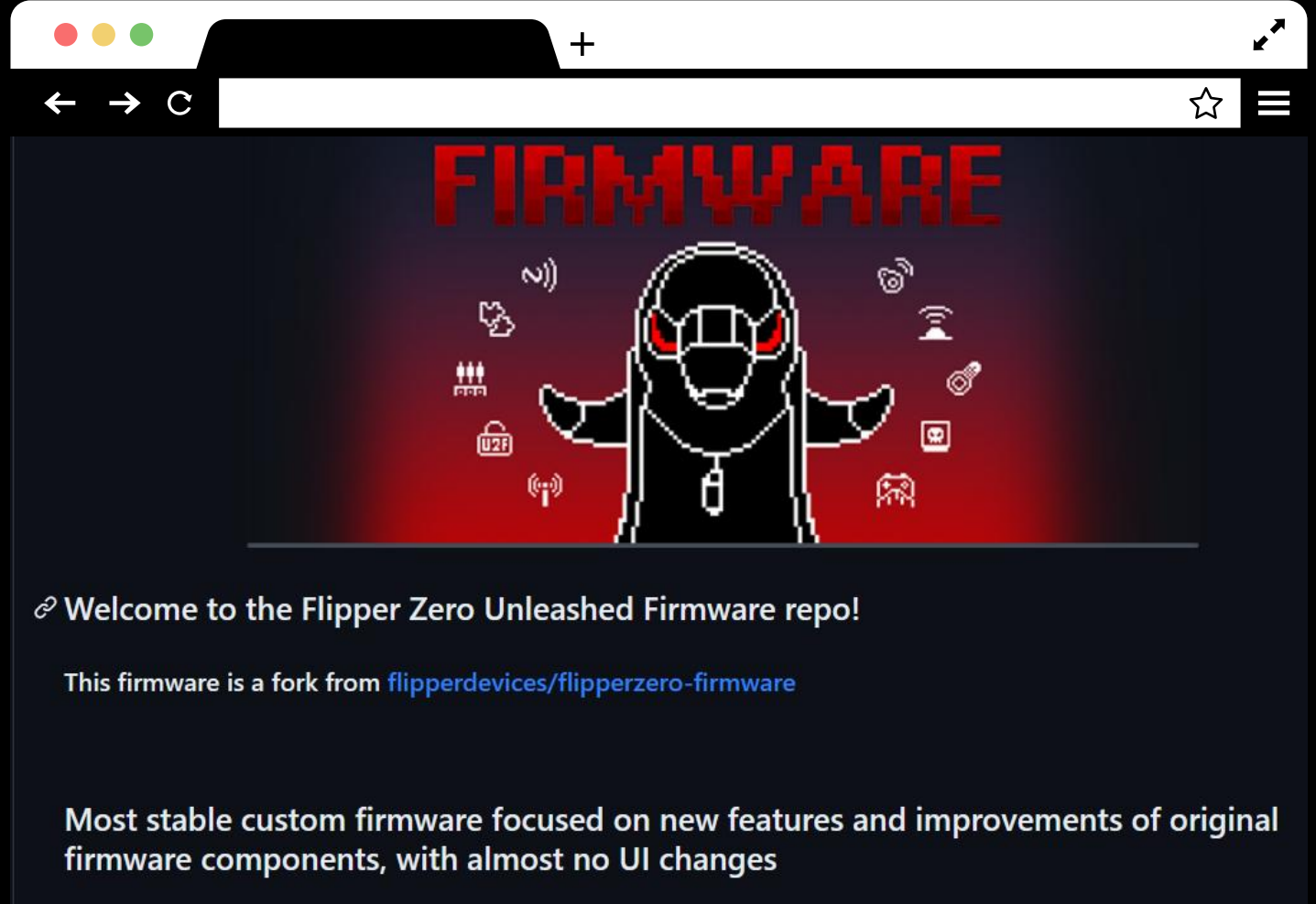
Bad USB



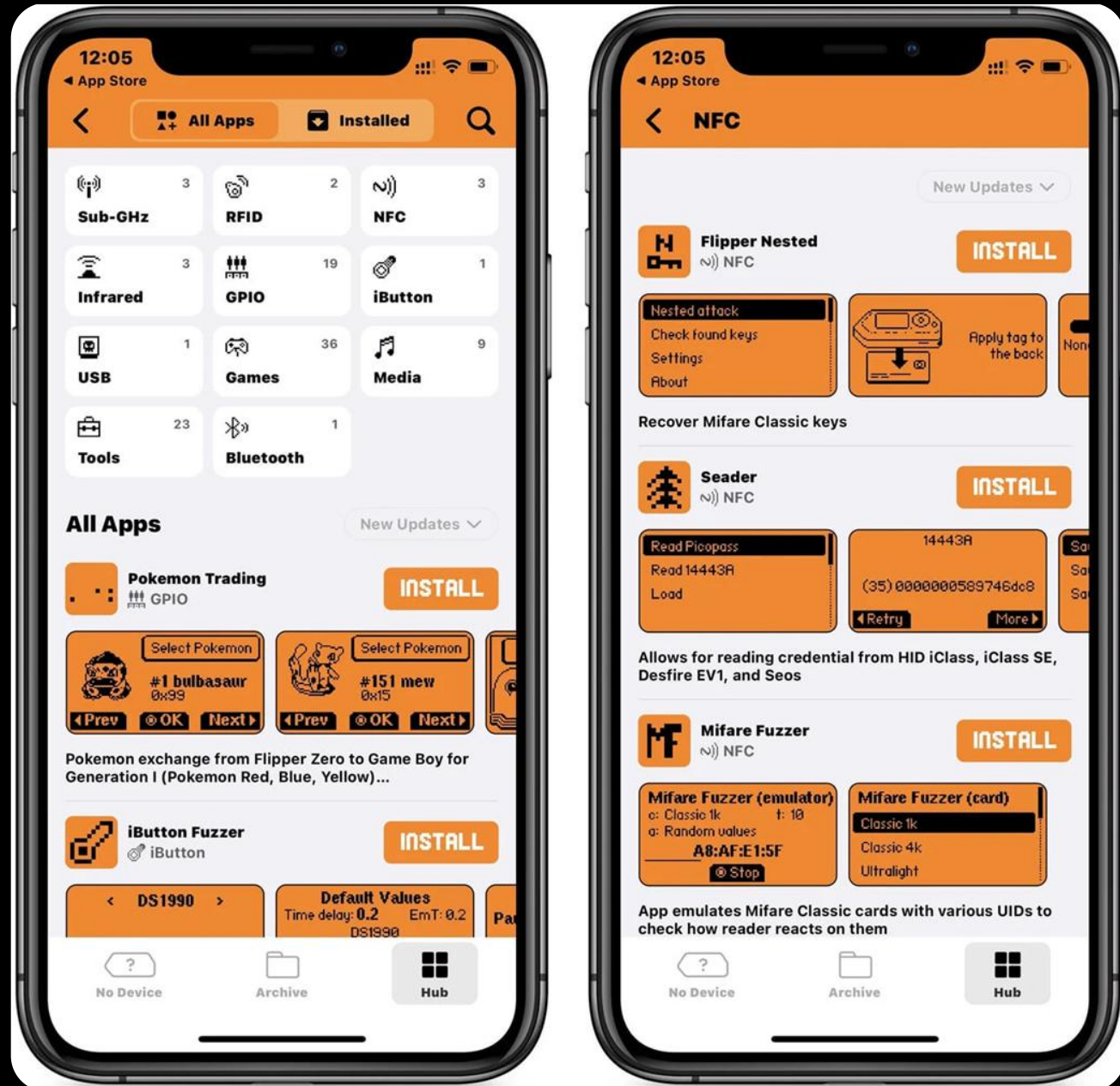
Flipper Zero can act as a BadUSB device, recognized by computers as a Human Interface Device (HID), such as a keyboard. A BadUSB device can change system settings, open backdoors, retrieve data, initiate reverse shells, or do anything that can be achieved with physical access. It is done by executing a set of commands written in the Rubber Ducky Scripting Language, also known as DuckyScript. This set of commands is also called a payload.

Custom firmware Flipper Zero/Additional resources

- <https://github.com/DarkFlippers/unleashed-firmware> — **Unleashed** is the first fork of the official firmware that **allows** you to **remove regional restrictions** from Flipper Zero, as well as **add new tools**. In the repository, it is presented in two forms: basic and advanced, which has a huge number of pre-installed applications.
- <https://github.com/djsim1/awesome-flipperzero> — A collection of Awesome resources for the Flipper Zero device: Databases & Dumps; Applications & Plugins; Firmwares & Tweaks; Graphics & Animations and much more.



Flipper Apps



Thank you!



- Join the community
<https://t.me/flipperzero/>
- Contact me via telegram:
<https://t.me/gmkumurzhi>

- Read the documentation on the topics you are interested in here: <https://docs.flipper.net/>
- Experiment! Have fun!

