Flipper Zero

HACKER OR DEFENDER? CHOOSE YOUR SIDE

Elizaveta Ragozina

CERN IT Lightning Talks #25

https://indico.cern.ch/event/1436466/

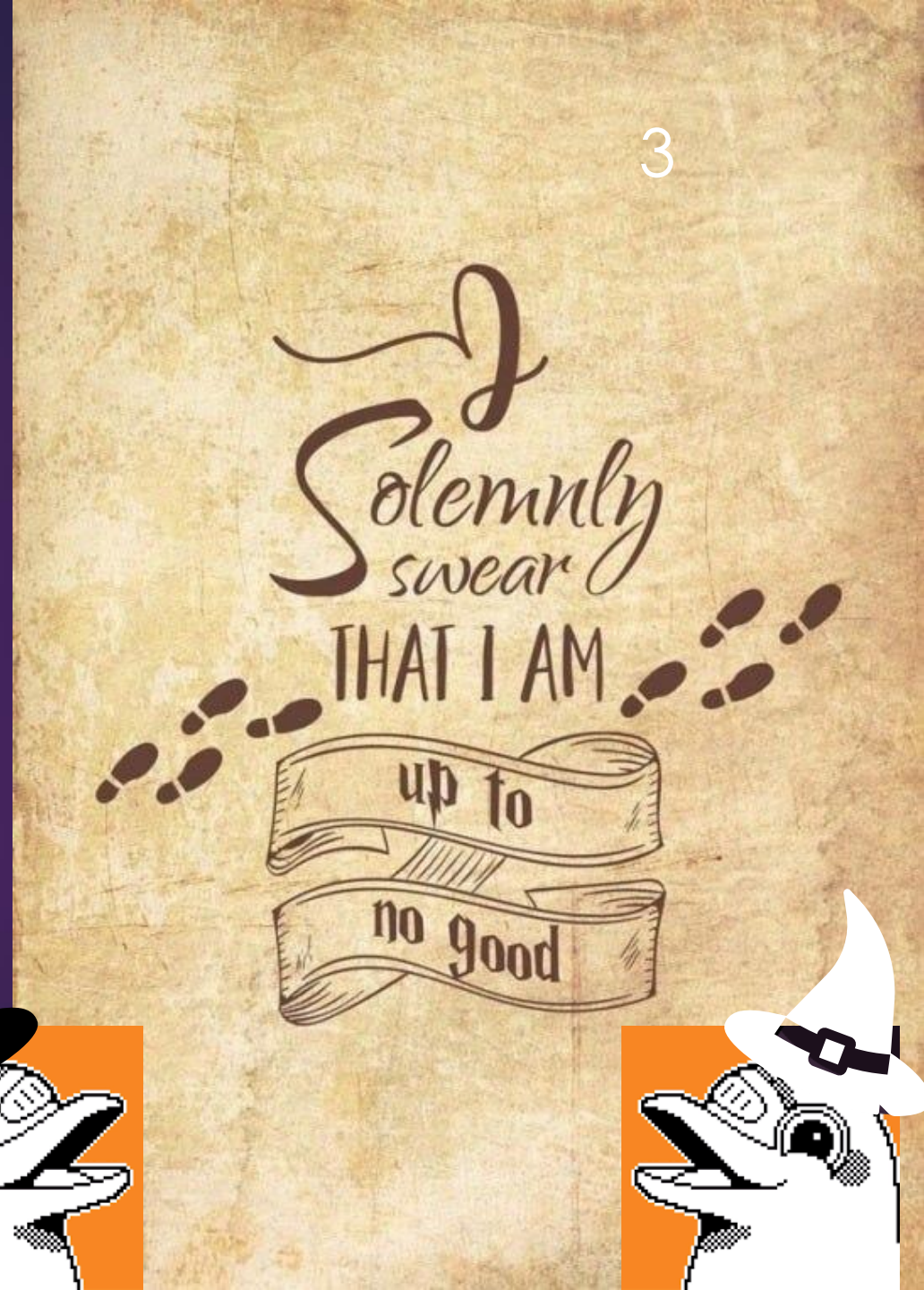
What it can

- Be compact and cute with gamified UI
- Read, copy, emulate different signal standards

.= CHF 153

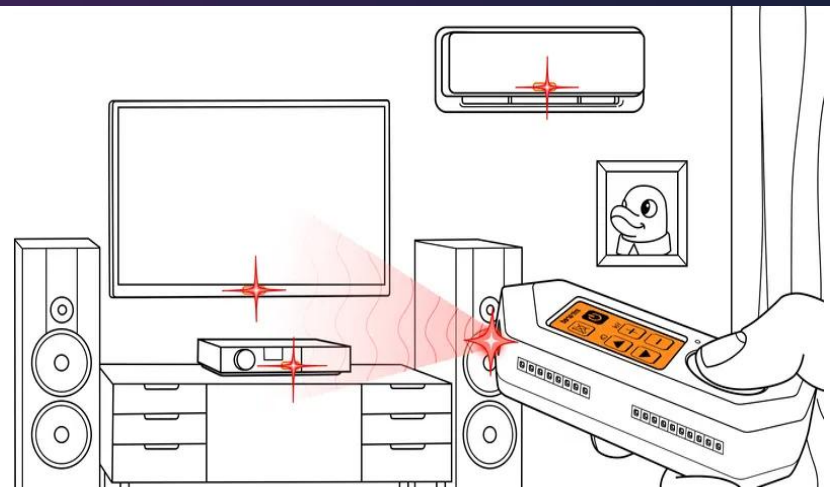
Legal? Sort of…

- Hacking without permission is illegal
- Ethical Hacking only!



What it can: Infrared

- TV Remotes, Air conditioners, Light control, Toys, Business support systems
- Universal remote
- Danger! Flipper can receive, copy, transmit

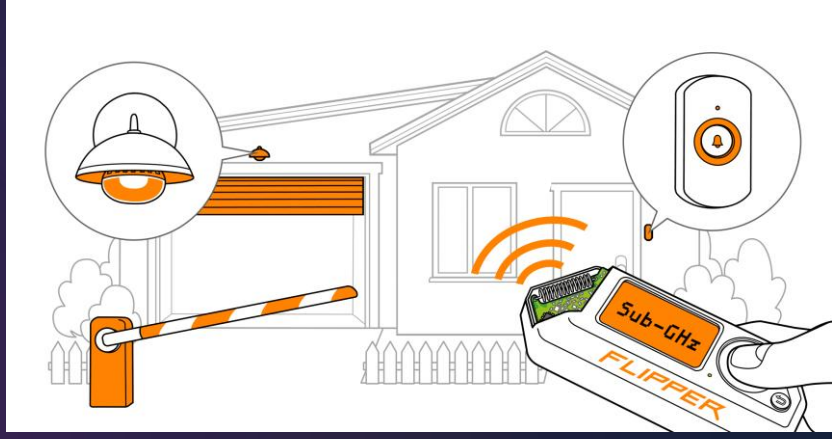


What it can: Radio-frequency Identification

- RFID (low frequency):
- Short IDs, no authentication
- Danger! Easy to read, save, emulate and write

- NFC (high frequency)
- Two-way data transfer, cryptography
- UIDs, higher protection → *dynamic* by credit cards
- Danger! Many access control systems rely on UID only to authenticate

What it can: SubGhz



- Long-range communication
- Danger! Old car keys, garage doors, …
- Modern cars' key fobs user rolling fobs

BleepingComputer

Canada to ban the Flipper Zero to stop surge in car thefts

The Canadian government plans to ban the Flipper Zero and similar devices after tagging them as tools thieves can use to steal cars.

9 Feb 2024

PCMag

Canada to Ban Flipper Zero Devices Over Car Thefts

However, Flipper Devices says the tool can't be used to unlock cars made in the last 30 years.

9 Feb 2024

PCMag

Canada Walks Back Ban of Flipper Zero, Targets 'Illegitimate' Use Cases

Canada Walks Back Ban of Flipper Zero, Targets 'Illegitimate' Use Cases. A Canadian regulatory agency says the aim is to restrict the Flipper...

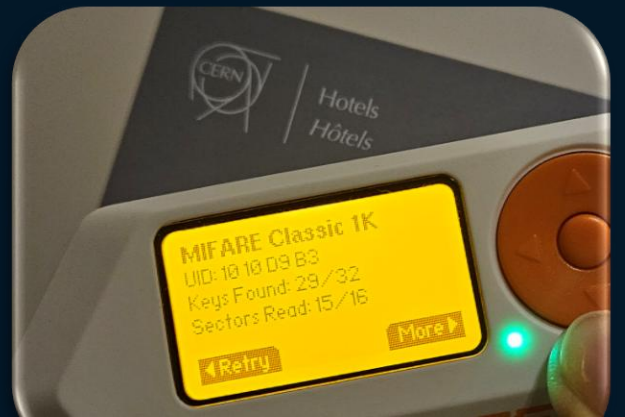
20 Mar 2024

My Ethical Hacking Experiments

- Universal remote

- Copy a swimming pool access card (reported)
- No comment (reported)

- Copy my CERN access card (-)
- Copy my CERN hostel access card (-)
- Open CERN tollgate (-)



What it can: Bad USB + Bad KB

- Flipper pretends to be a USB or a Bluetooth device (keyboard)
- Danger! Injects pre-programmed keystrokes or payloads into a connected computer

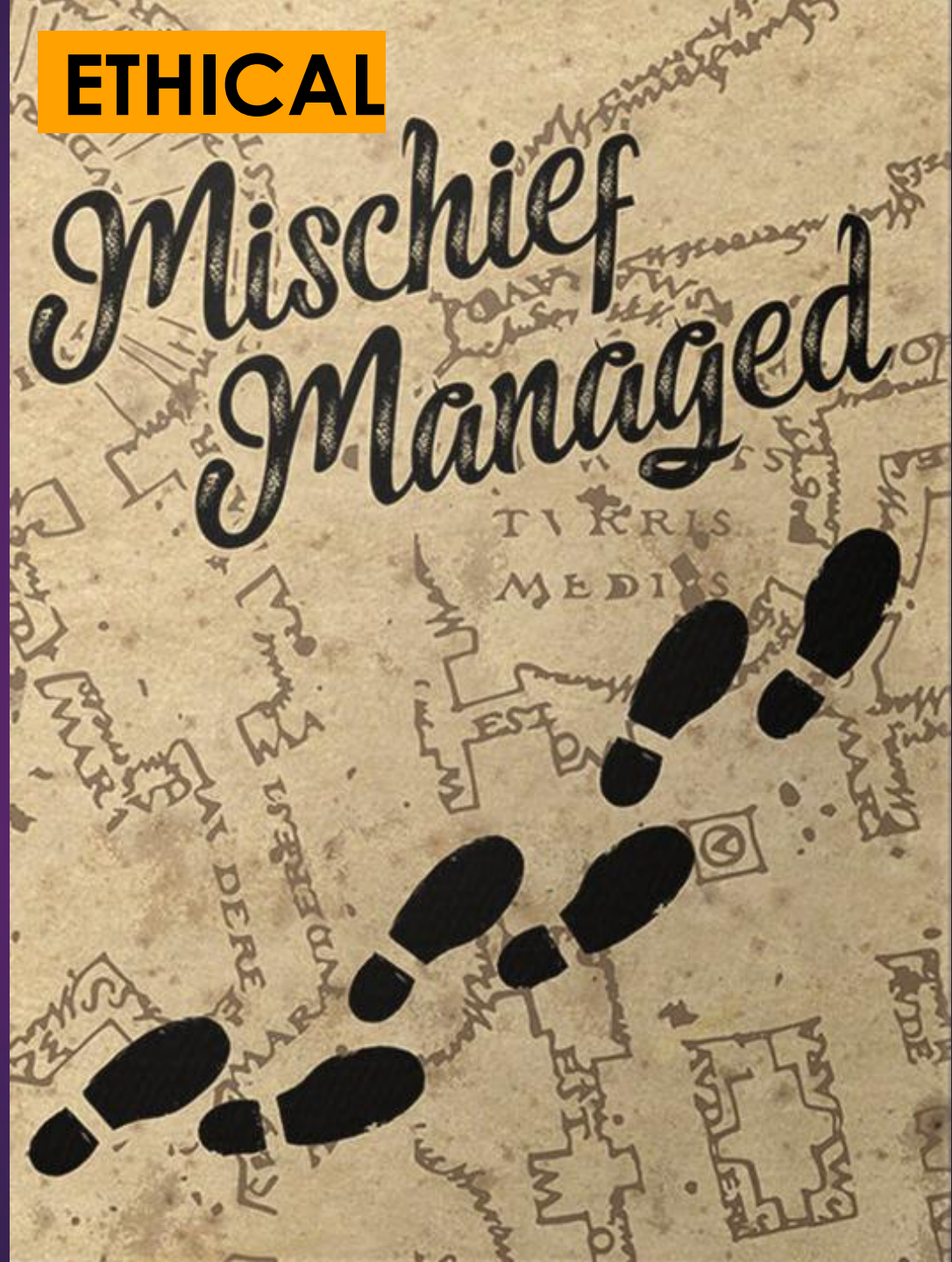
- Open Source payloads from https://payloadhub.com/
  - EXFILTRATE SUDO PASSWORD BY PHISHING
  - EXFILTRATE EMAIL AND PASSWORD BY PHISING - LINUX
  - WIFI WINDOWS PASSWORDS DISCORD EXFILTRATION

DEMO

Takeaways

- Danger! Attacks:
  - Unauthorized Access
  - Communication Interception
  - Infrastructure damage
- Don't trust your systems
- Learning purpose
- Penetration testing

- You credit card and car are probably safe. For now.



Thank you! Questions?

Pictures

- https://lab401.com/
- https://medium.com/@jmbowles26/mischief-managed-e9d5c529e591
- https://www.abposters.com/canvas-print-harry-potter-mischief-managed-v63297
- https://docs.flipper.net/