HackRF One

Radio Hacking

presenter: Sergei Zaiats

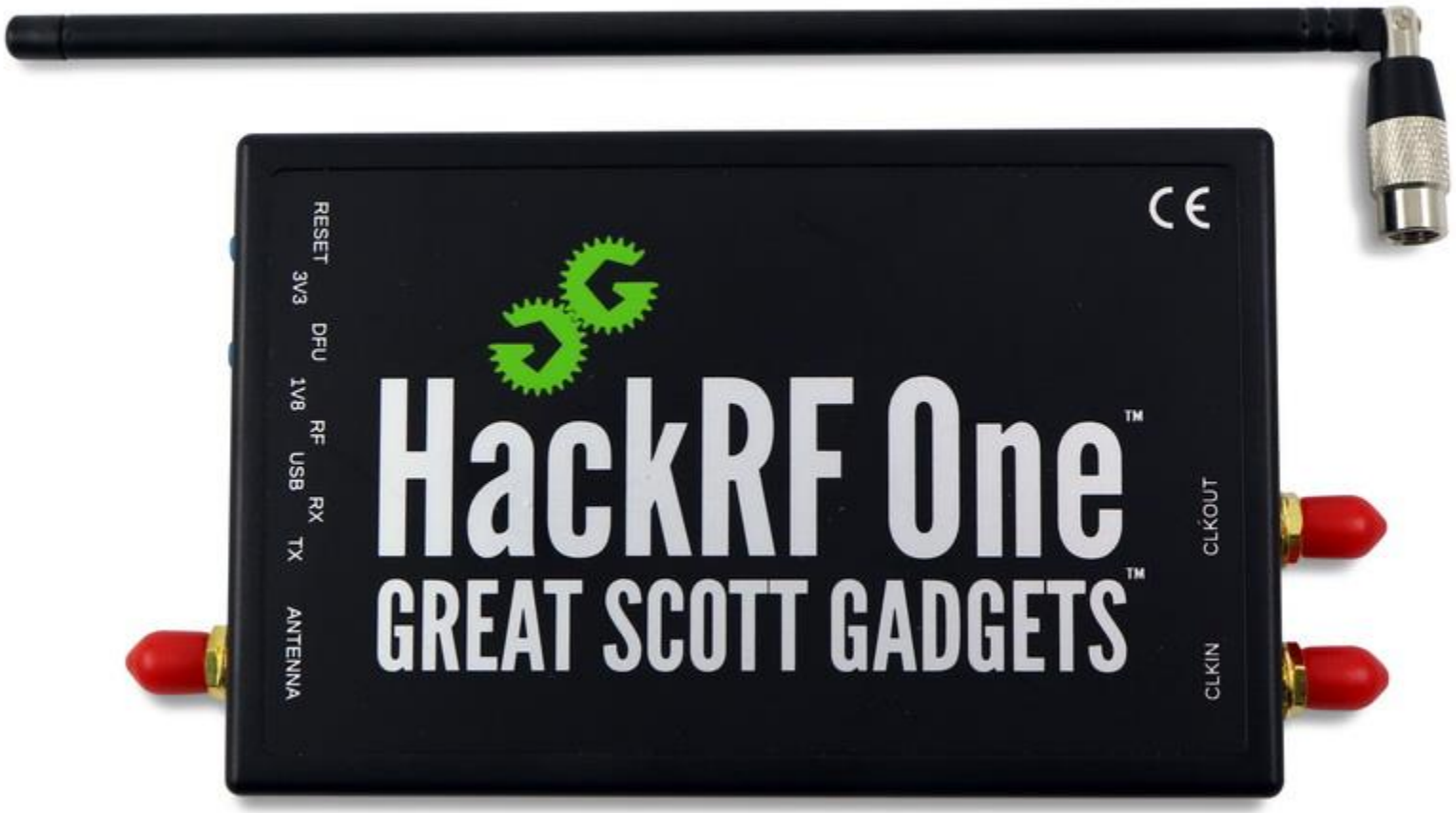
Software-defined radio (SDR)

SDR is a radio communication system where components that have been traditionally implemented in analog hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system.

While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which were once only theoretically possible.

HackRF One

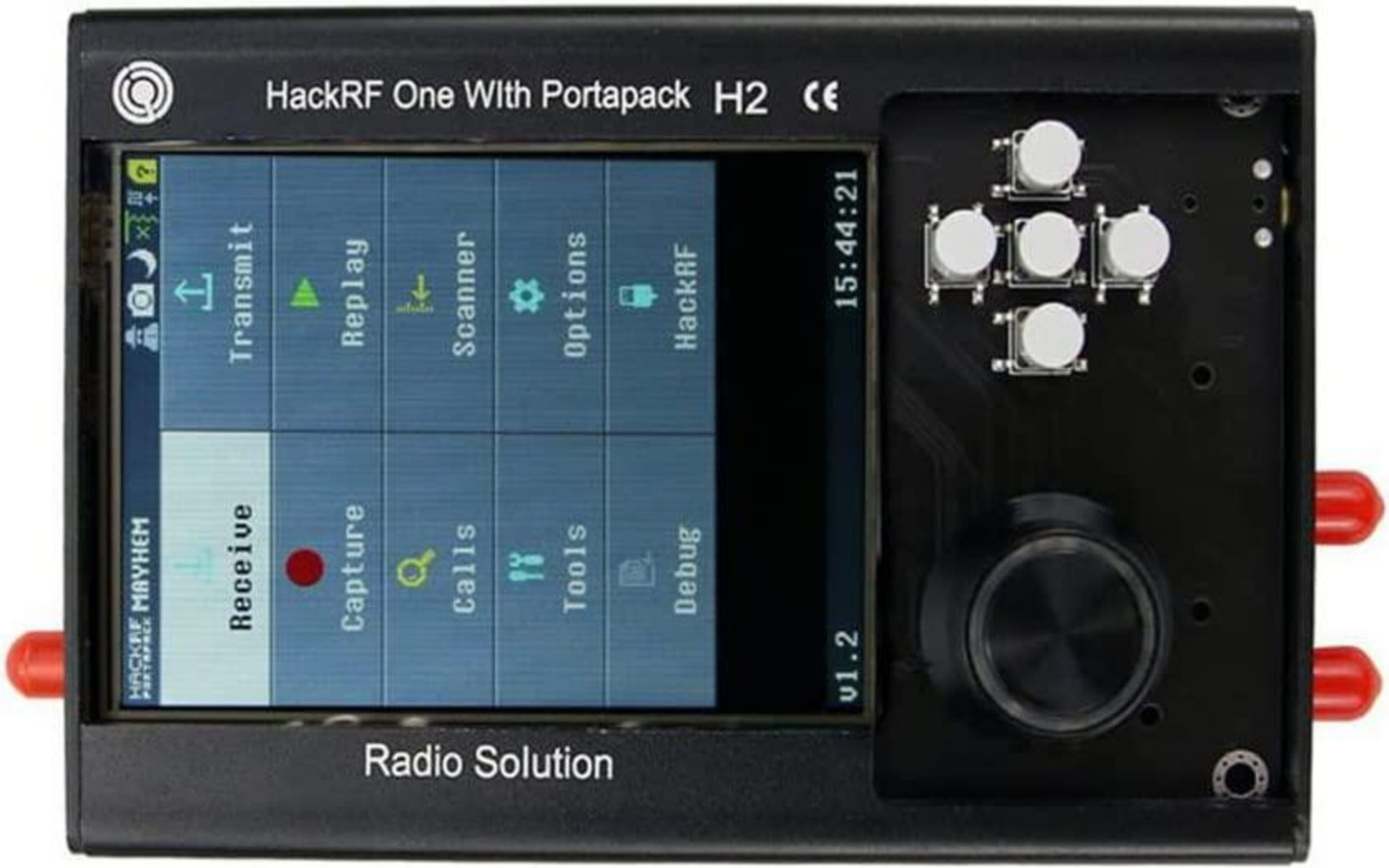
presenter: Sergei Zaiats



presenter: Sergei Zaiats

PortaPack H2

presenter: Sergei Zaiats



presenter: Sergei Zaiats

Possibilities

- Receive
- Record
- Transmit (!)

Use cases

Listen to your favourite radio station

Security Research

Assessment of the product that works over RF:

Record, analyse, reverse engineer the protocol, find vulnerabilities.

Example: Capture the traffic from your garage door remote to understand how it works and how secure it is.

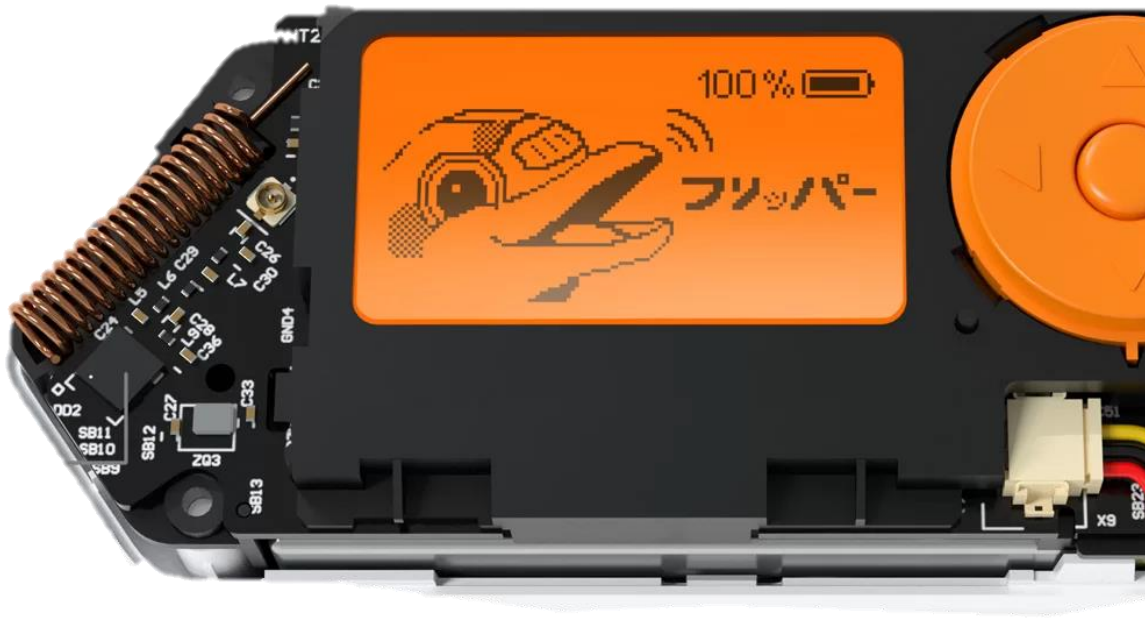
Gray areas

- Jam a certainty frequency
- Replay attack (from walkie-talkie to cloning car keys, camera feed hijacking, etc.)

Similar Tools

Flipper Zero

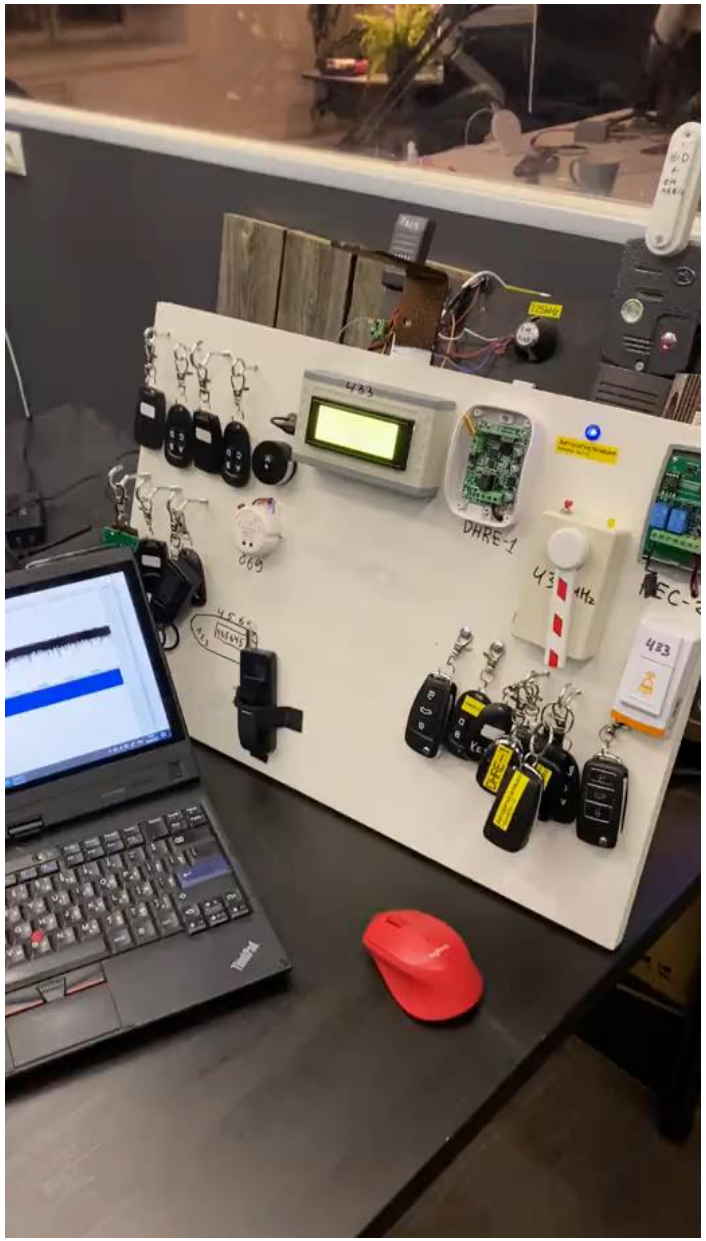
Sub-1GHz antenna
125kHz RFID
NFC
Infrared Transceiver



Similar Tools

RF security is weird field sometimes.

A footage of a doorbell that is opening a car alarm system because they use the same frequency.



Fun Part:
Demo