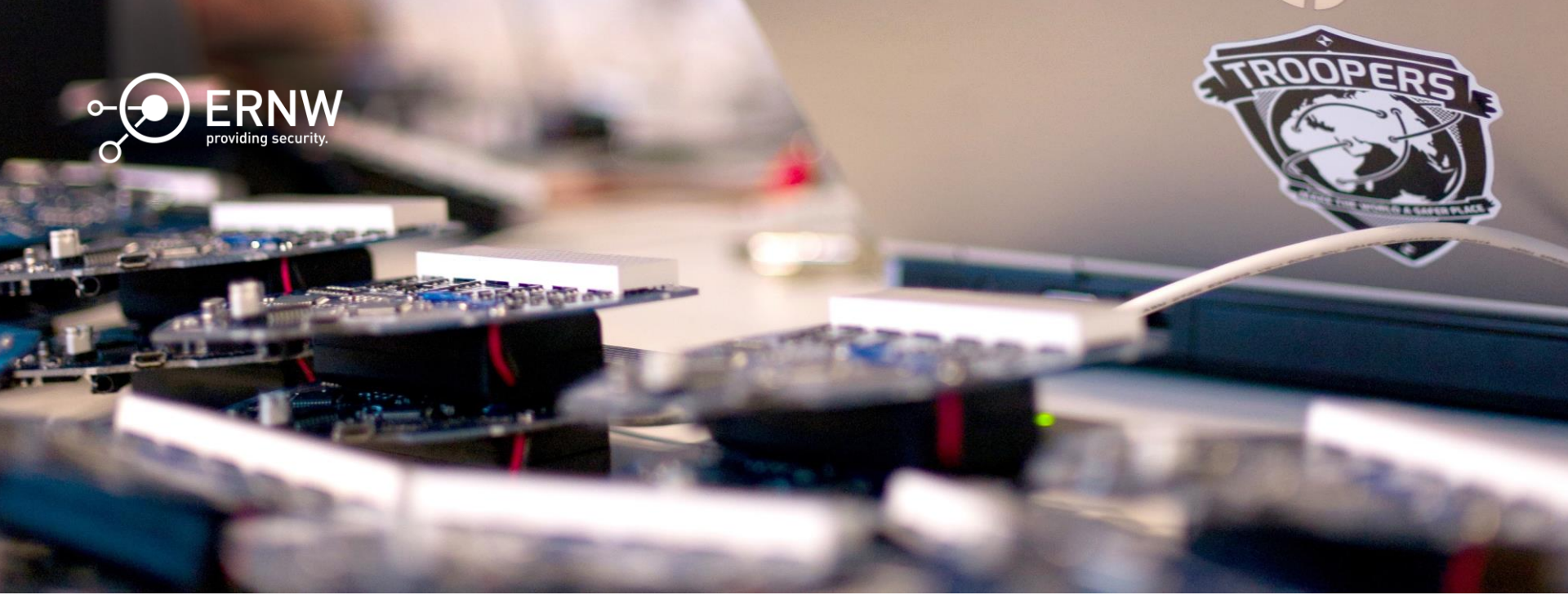


Rage Against The Radio

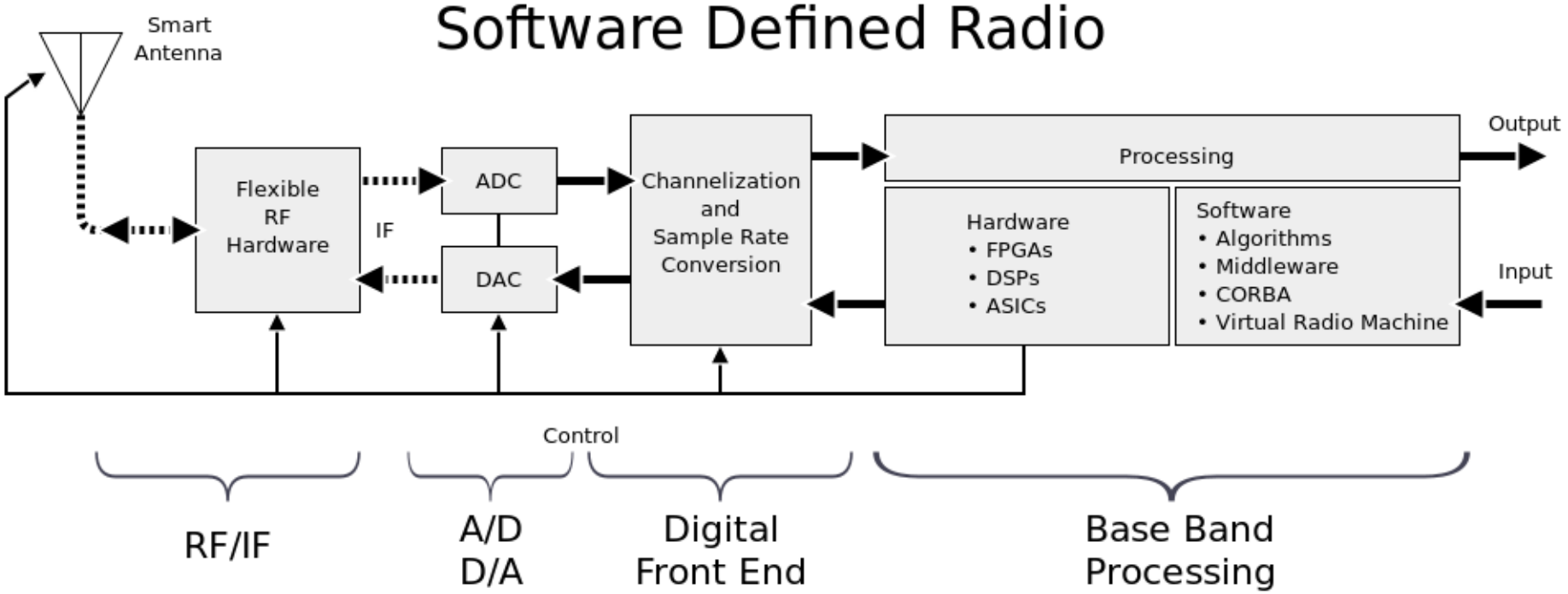
Stefan Kiese, skiese@ernw.de, @net0SKi

04.11.2016 – IT-SeCX, St. Poelten, Austria

ERNW
providing security.

About Me

- Security Analyst and Researcher at ERNW in Heidelberg, Germany
- Background in electronics
- Love to play around with technical stuff; not only electronics



SDR – A Definition

ERNW
providing security.

Wikipedia says:

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

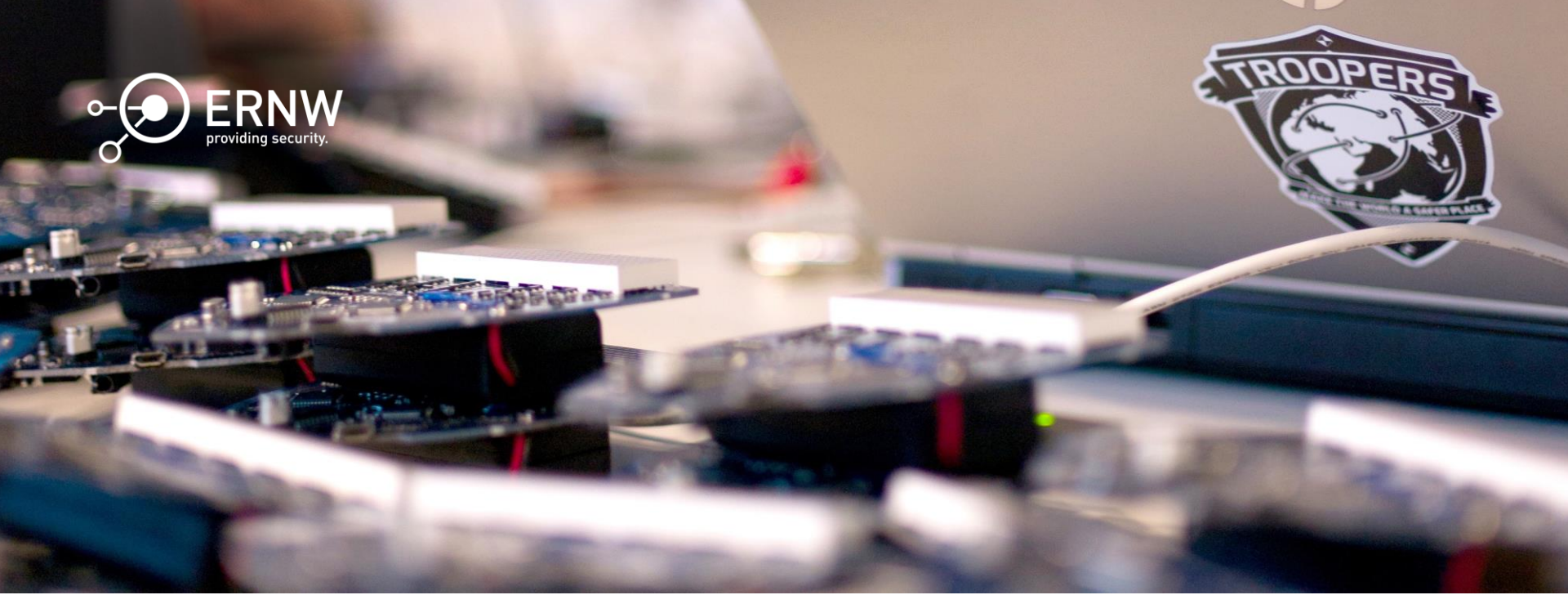
Source: https://en.wikipedia.org/wiki/Software-defined_radio

ERNW
providing security.

…or even shorter:

- "Radio in which some or all of the physical layer functions are software defined”

Source: http://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf



Pros and Cons

Mostly depend on specific use case.

ERNW
providing security.

Pros

- Very cheap (when RX only! E.g. RTL-SDR ~15€)
- Still cheap (starting between 300 - 800€) considering capability
- High flexibility
- ...

Cons

- Expensive considering mostly used/needed features
- Not easy to use without RF knowledge
- Difficult, when it comes to timing sensitive things (e.g. frequency hopping)
- Often time intensive
- ...

Tools

What you need to get started.

ERNW
providing security.

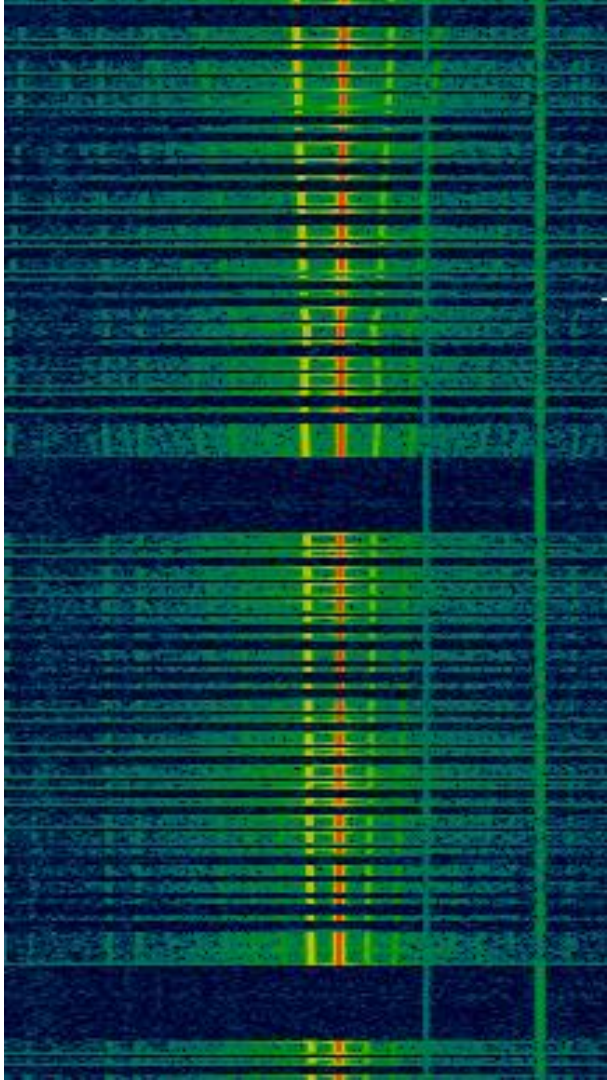
Hardware

- RTL-SDR (RX-only)
- HackRF One (half-duplex)
- bladeRF
- USRP

ERNW
providing security.

Software

- GNU Radio Companion
- GQRX
- Baudline or Inspectrum
- Audacity
- Python



ERNW
providing security.

Open Source Modules / Implementations

- GSM
- LTE
- GPS
- Bluetooth (LE)
- DVB
- Zigbee
- Z-Wave
- TI CCxx
- NRF24
- ...

Targets

What could be attacked?

ERNW
providing security.

Targets

- Everything “smart” (dogs, cats, babies, phones, watches, houses, cities, meters,...)
- Everything “IoT” (dogs, cats, houses,...)
- Everything connected (also wired! Like your cable TV @home)

War Stories

The Stories

- GPS Spoofing
- Unlocking a car
- Disarming an alarm system
- Keystroke injection over the air
- Tire Pressure Monitoring Systems (TPMS)
- GSM

GPS Spoofing

ERNW
providing security.

Setup

- HackRF One or another SDR
- (Signal generator)
- gps-sdr-sim (https://github.com/osqzss/gps-sdr-sim)
- Smartphone or GPS mouse + app


Tektronix
LG
SAMSUNG
CATCH A POKÉMON
Google
Tektronix
AFG2021
Sine
Square
Ramp
Pulse
Arb

How to Open a Car – 90s Style

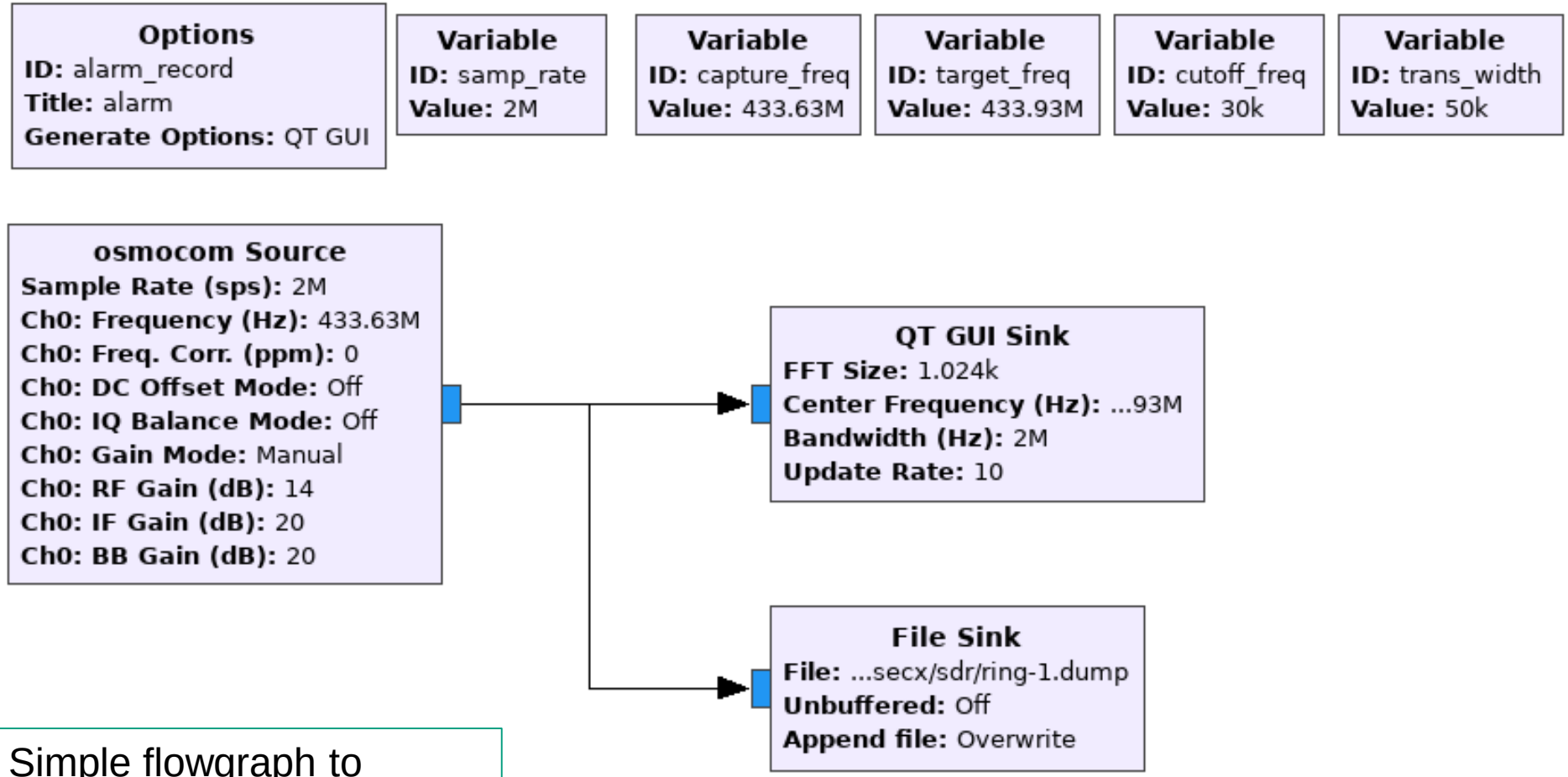
…and what shouldn’t be possible anymore.

ERNW
providing security.

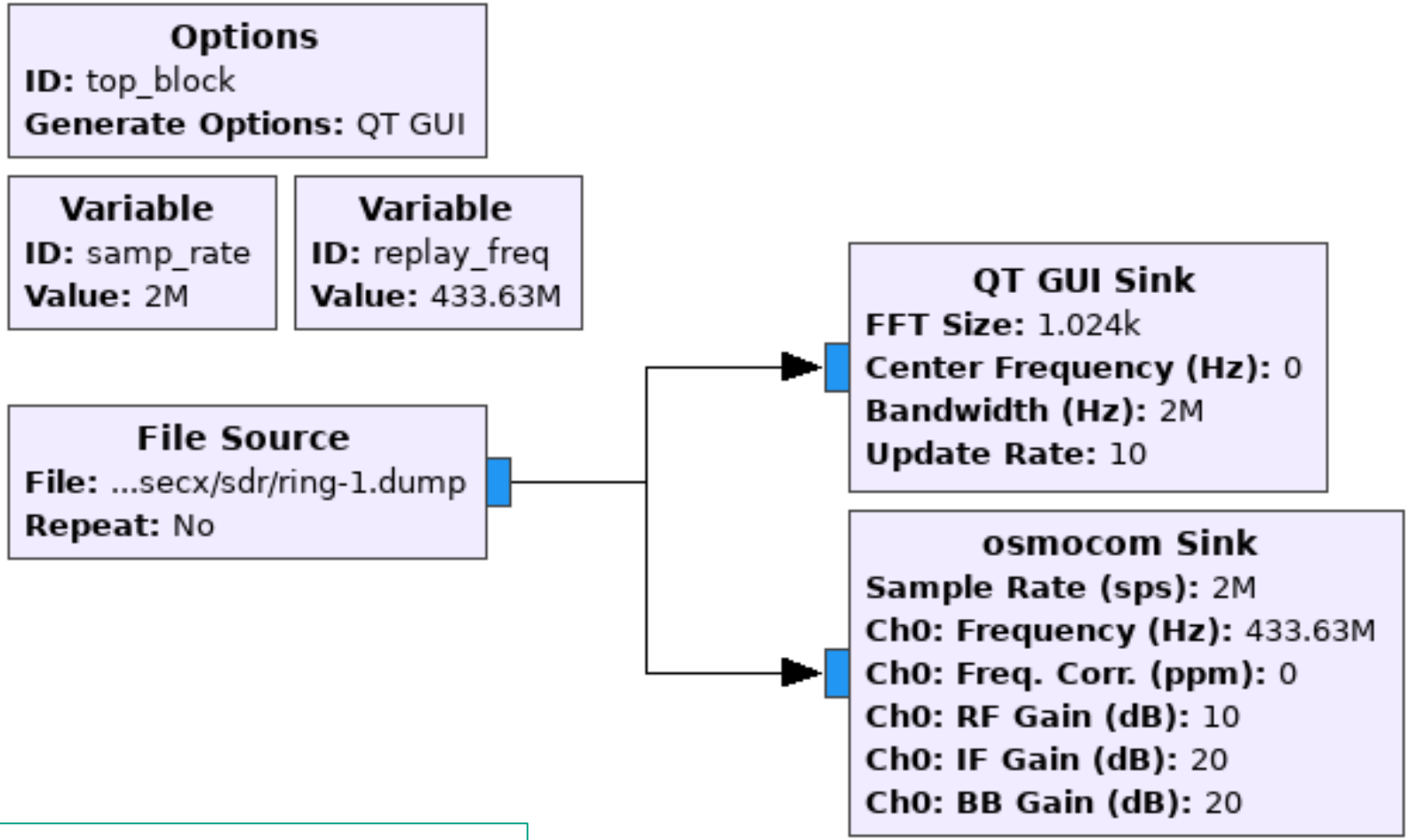
Setup 1

- Some TX-capable SDR
- Software
  - GNU Radio

  or
  - Simpler solution: Software delivered with the SDR's driver, like hackrf_transfer



Simple flowgraph to record a signal w/o any filter



Simple flowgraph to replay a signal w/o any filter

ERNW
providing security.

Setup 2

- Yardstick One
- rfcat

ERNW
providing security.

Setup 3

- Arduino (3 – 25€) or Raspi
- 433MHz Transmitter and Receiver (5€)
- Firmware

Setup 4

- Some 5€ RF keyfob from e.g. ebay
  → Easily clone other keyfobs

ERNW
providing security.

Why does this *technically* work?

- No use of rolling code or other security mechanisms

Disarming Wireless Alarm Systems

ERNW
providing security.

What's possible?

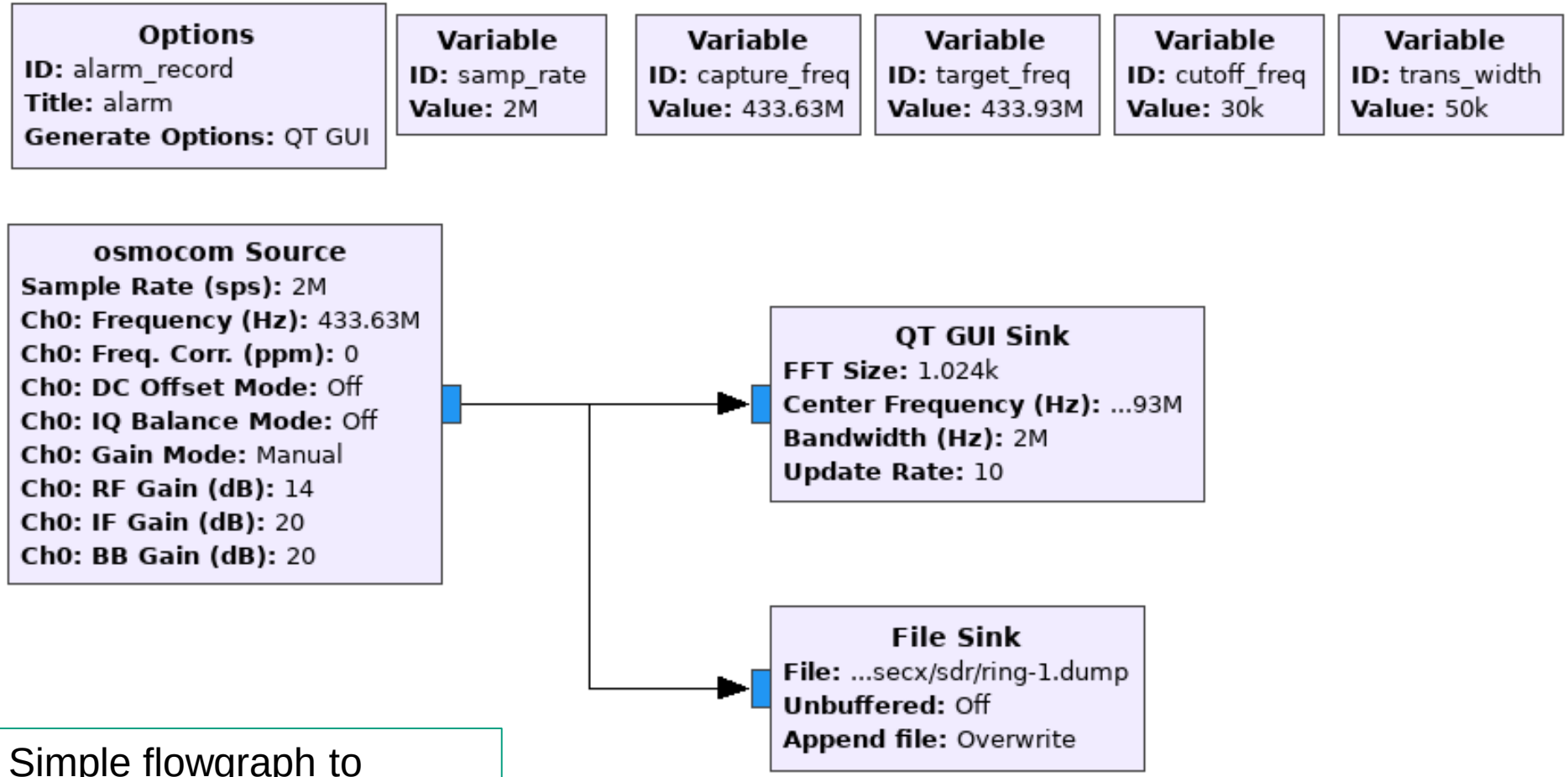
- Jamming signals from sensors, like on the windows, doors or even motion detector
  → This often works, because many of the alarm systems work unidirectional only or are w/o sth. like "still alive" signals
- Replay attacks
  → Many lack rolling code implementations
- Analyze signal and do whatever you want
  → That's why we use SDR! ☺
- DoS them

ERNW
providing security.

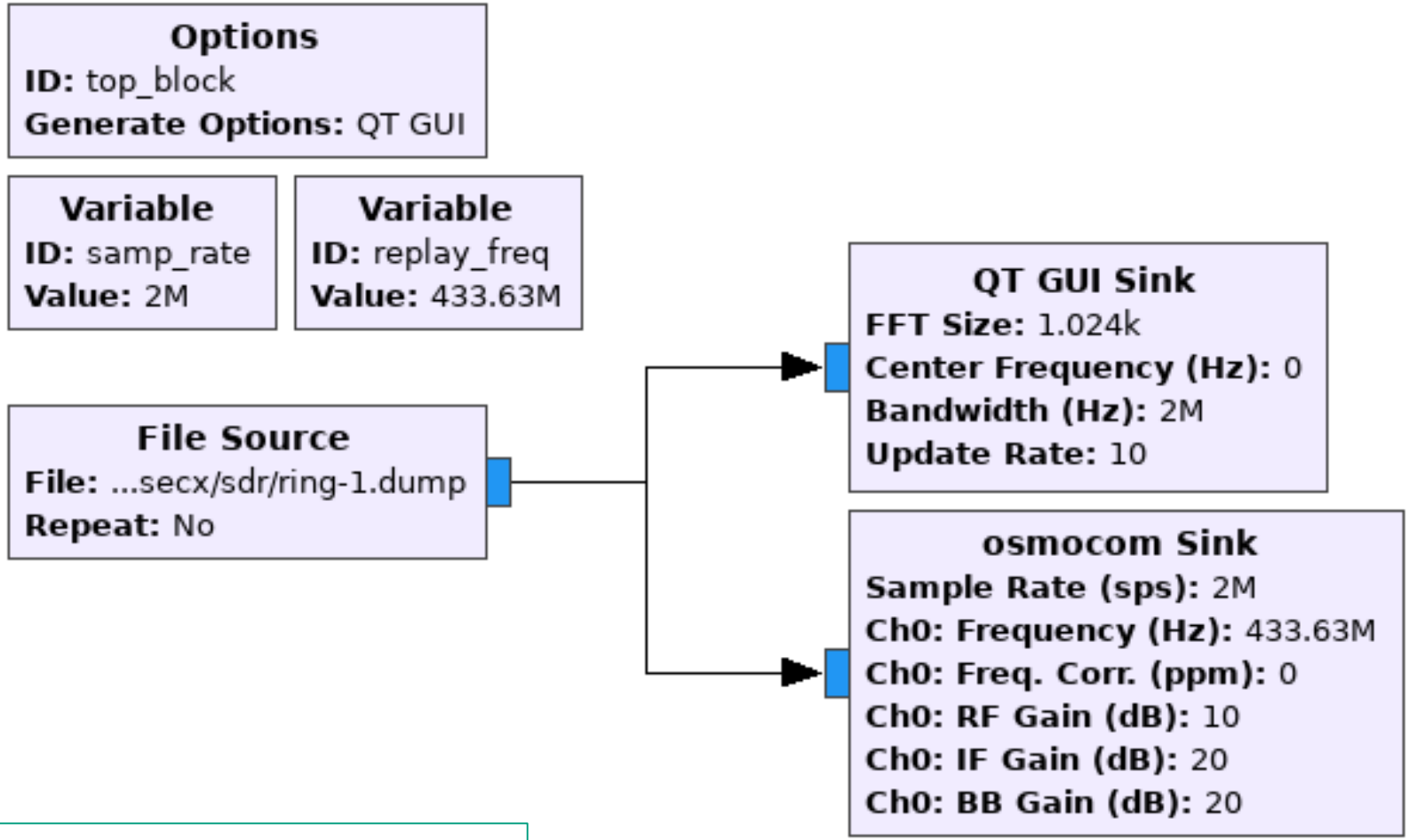
Setup 1

- Some TX-capable SDR
- Software
  - GNU Radio

  or
  - Simpler solution: Software delivered with the SDR's driver, like hackrf_transfer



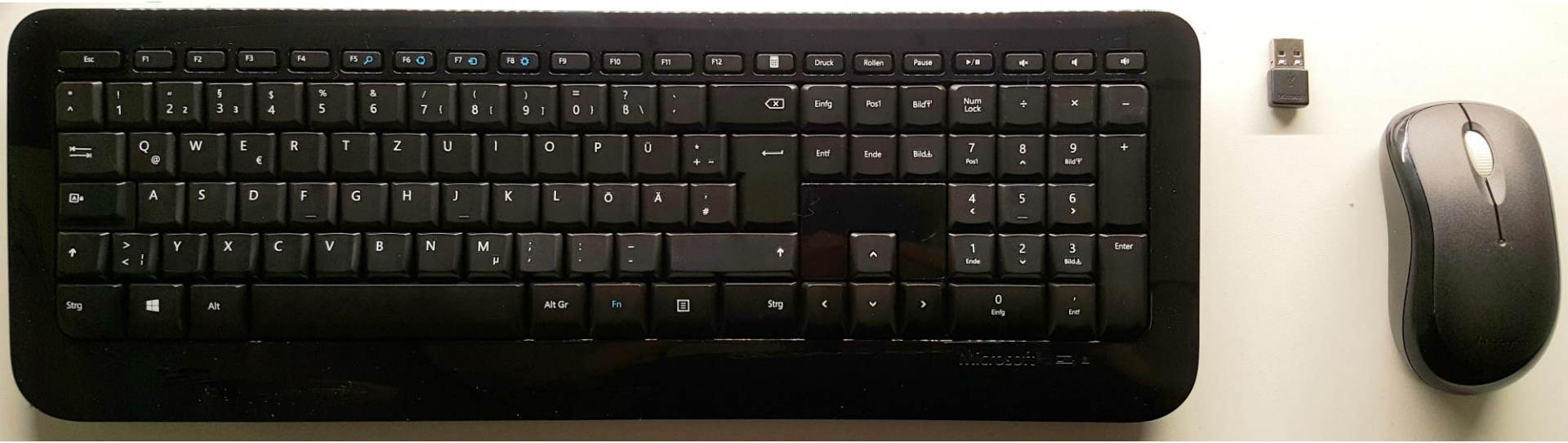
Simple flowgraph to record a signal w/o any filter



Simple flowgraph to replay a signal w/o any filter

ERNW
providing security.

- Same setups as mentioned before.
- Same problems as mentioned before?
  - It's even worse!
  - Many alarm systems on the market are imported from e.g. China and sold under $brand, which often means bad support (and no reaction on vuln disclosure), because nobody wants to be responsible



Your Wireless Desktop

Please don’t use wireless keyboards or mouses at work (or at home)!

ERNW
providing security.

Why you shouldn't use them?

- Ever thought about the difference between wired and wireless? ;-)
- Let's assume:
  - Wired == local
  - Wireless == remote
- So, one does not need to tamper things locally on your PC
- Don't blindly trust "AES" imprints on boxes

Setup

- SDR

  or

- Some custom radio dongle, regarding the target

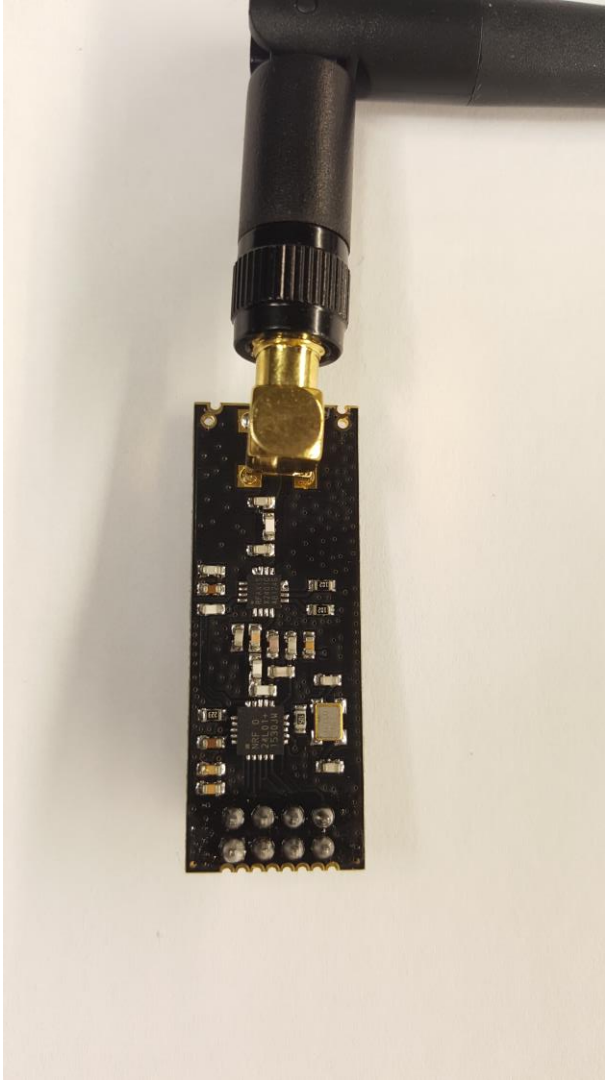
ERNW
providing security.

Example Setup for Logitech / Microsoft

- (SDR – similar to BT LE; AFAIK not easy regarding channel hopping)

  or
- USB radio dongle with NRF24 chipset, like Logitech Unifying Dongle or Crazyradio Dongle

  or
- Some other radio with NRF24 chipset w/o USB + Raspi or Arduino
- Bastille's excellent NRF Research Firmware



ERNW
providing security.

What's possible with this?

- Jamming…
- Eavesdropping in some case

The most interesting thing (from my perspective):

- Keystroke injection! ☺

→ That's why I don't use a wireless presenter today ;-)

TPMS

(Tire Pressure Monitoring System)

ERNW
providing security.

Facts

- Sensors need 125kHz signal to wake up
- Data transmission via 433MHz signal

ERNW
providing security.

What could you do?

- Wake the sensors up (only short range)
  - Well, that's boring…
- Spoof them.
- Fuzz them. Effects to the car? Unknown, should differ ;-)

Setup

- SDR and GNU Radio or some custom tool

  or

- Arduino and 433MHz transmitter

Source: sysmocom.de

GSM

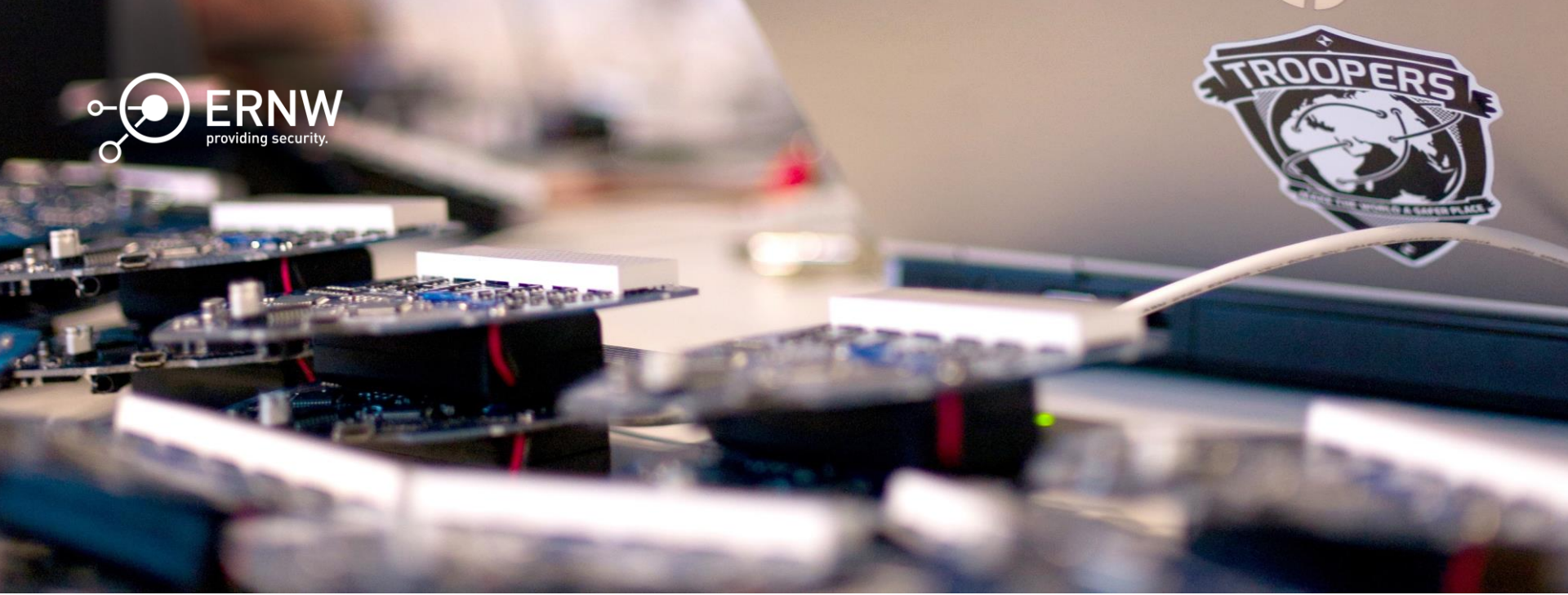
ERNW
providing security.

What could you do?

- Build up a fake cell (BTS)
- IMSI catcher
- IMSI catcher catcher ;-)
- Sniff GSM
- Fuzz sth. over the network
- ...

Setup

- SDR
  - When sniffing only, cheap RX-only SDR works fine
  - Full duplex needed to act as Base Transceiver Station (BTS)
- Dedicated BTS
- Sure, some software, e.g. from osmocom



Demo Time

ERNW
providing security.

Thank you for your Attention!

Any questions?

skiese@ernw.de

@net0SKi

www.ernw.de

www.insinuator.net