

# **Ethical Hacking van Radio Signalen**

## **Hacking Radio**

UBA MWV / RSL Op Post  
Zaterdag 4 Maart 2023



# Even mezelf voorstellen

Kristoff Bonne

Interesses: Netwerken, IT (unix/linux), Programmeren, cybersecurity & privacy, hardware en electronica (inclusief radio)

Amateur Radio: ON1ARF

Fediverse: @on1arf@mastodon.radio



# Workshop: Hacking RF signals

- DragonOS
- Radio signalen ontvangen met gqrx
- Analyse met inspectrum
- Analyse met Universal Radio Hacker (urh)
- Demo signalen uitzenden
  - Gnuradio / HackRF
  - sx1276

# 2 minuten theorie

Radio communicatie heeft 3 belangrijke onderdelen

- Hardware

Electronica, Antennes, besturing, testen en meten, mechanische bouw, ...

- Applicaties

Stem, beeld, video, data, infrastructuur (repeaters, data netw), web-ontvangers, Nood communicatie, ...

- Propagatie

LOS, HF, tropo, Es, ducting, rain-scatter, meteoscatter, planesscatter, sat, EME, ...

# 2 minuten theorie

Hardware  
Applicaties  
Propagatie

←--- Signaal-verwerking:  
tussen Hardware en Applicatie

- Low-level: **SDR**  
modulatie, filteren, clock-recovery (bit-sync), ...
- High-level: **bits**  
frame-sync, error-correction / detection

# Antennes en connectoren

## Antenne

- Waar?
- Relatie met Frequentie
- Kopen of bouwen?

## Connectoren

- BNC, IEC “de distributie”, SMA, MCX
- SMA vs RP-SMA

# RTL-SDR dongle

## “Geluidskaat voor radio-signalen”

- Oorspronkelijk: ontvangst van DVB-T (Terrestie digitale TV), FM en DAB
- 2012: Eric Fry maakt er een generieke SDR-ontvanger van
- Goedkoop: 20 to 35 euro
- 24 MHz tot 1.7 GHz
- RTL2832U (realtek Taiwan)
- Enkel ontvangst



<https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/>

# Hulp achteraf

- Matrix (\*)
  - #sdrbe:gnuradio.org
  - #electronics\_homebrew:c1.uba.be
  - #chitchat:c1.uba.be
- <https://lists.uba.be/l/homebrew>

(\*) Via matrix of XMPP



# RTL-SDR dongle

## Uitbreidingen

- TCXO
- Ingebouwde Bias-T
- Extern
  - Voorversterker
  - Up-convertor
  - Down-convertor
    - → rtl-sdr.v3 “direkt mode”



# RTL-SDR dongle

## Alternatieven

Receivers

- SDRplay

Transceivers:

- HackRF
- PlutoSDR