Electronic Access Control Security

Matteo Beccaro || HackInTheBox

Amsterdam, May 27th, 2016

HITB

OPPOSING FOR

Me

- **Matteo Beccaro**
- **Founder** & **Chief Technology Officer** at **Opposing Force**
  - The first Italian company specialize in offensive physical security
- Twitter: **@_bughardy_ | @_opposingforce**

What do you need?

Extract the zip

What you will find in the archive:

- **VM with all tools and libraries for the hands-on parts**
- **VirtualBox installer**
- **VirtualBox guest-addition**

username: opposingforce

password: opfor2016

Workshop's index of contents

- **Module 1 – Introduction**
  - Historical introduction on access control attacks
- **Module 2 – Attacking NFC**
  - NFC: what are we talking about?
  - Weapons for NFC-based solutions
  - Penetration test methodology
  - Hands-on
  - Case studies

Workshop's index of contents

- **Module 3 – Attacking RF communications**
  - Radio Frequency and EAC Systems
  - Exploring Radio Frequency communications in practice
  - Hands-on: receiving your first transmission
  - SIGINT with GNU Radio
  - Understanding RF communications security
- **Module 4 – The challenge**
  - Introducing the challenge
  - The awards ☺

Module 1 || introduction

Introduction

- Access Control system?

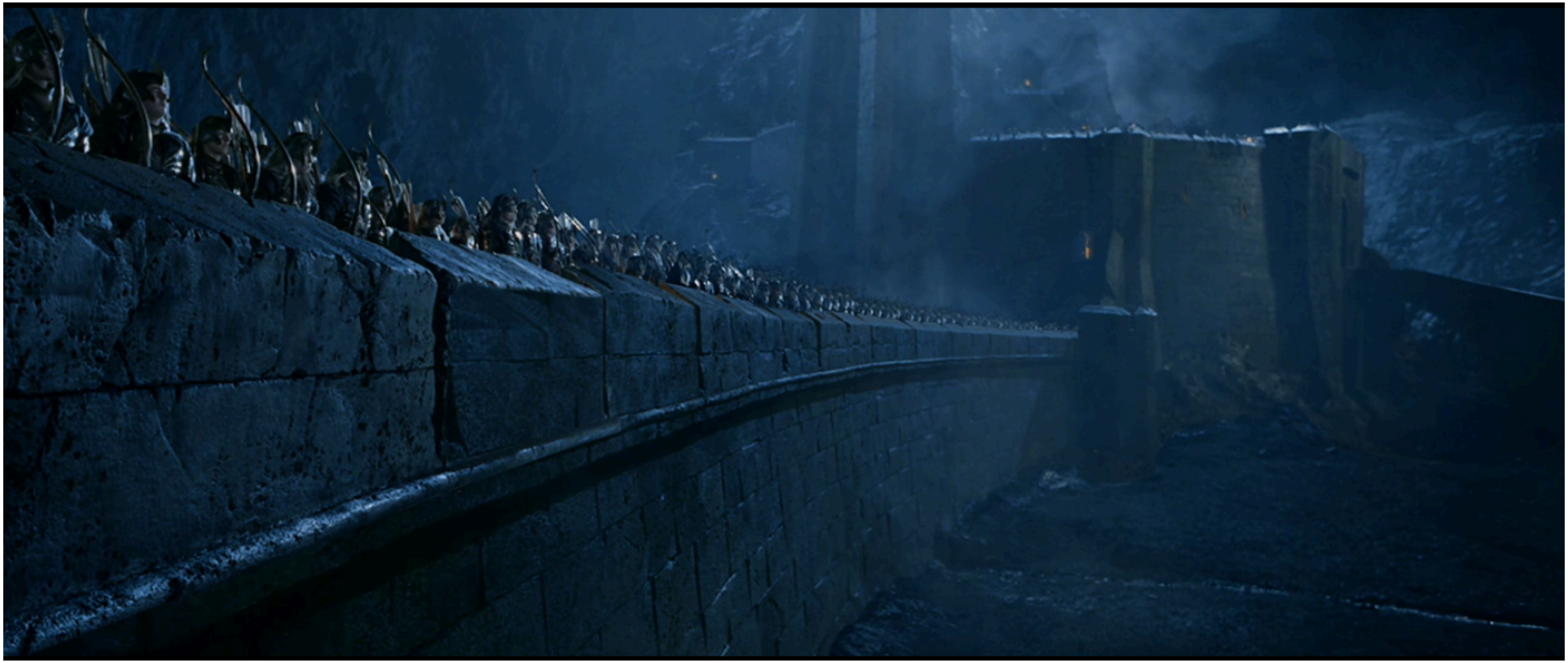
A system composed by several elements which aim is to limit the access to certain resources only to authorized people.

The system is composed by two type of elements:

Human **Technological**

- What was an Access Control system?

The **technological** elements



- What **was** an Access Control system?

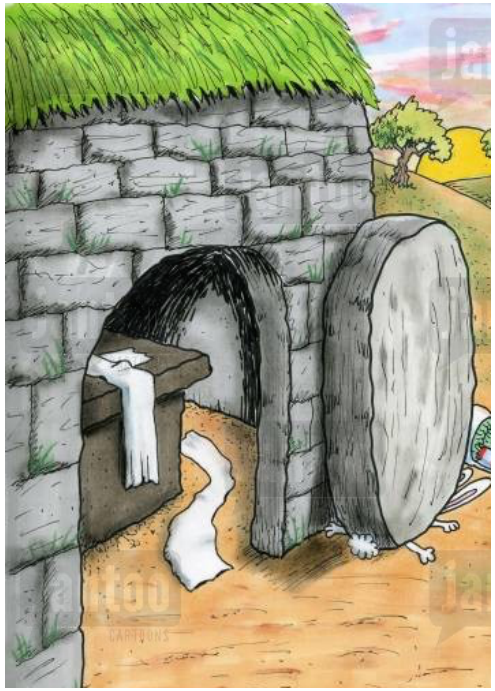
The **human** elements…

- What was an Access Control system?

…often fail

- First access control hackers?

Magicians..



- First access control hackers?

Social Engineers

- What is an Access Control system?

What is an Electronic Access Control system?

- It may employ different technologies
  - NFC
  - RF
  - Biometrics
  - Mag-stripe
  - Mobile phones
  - etc.

Module 2 || attacking NFC

Agenda

- Module 2 – Attacking NFC
  - NFC: what are we talking about?
  - Weapons for NFC-based solutions
  - Penetration test methodology
  - Hands-on
  - Case studies

What is NFC?

- NFC stands for Near Field Communication
- Frequency at 13.56 MHz
- 3-5 cm of range
- Widely used for
  - Access control systems
  - Electronic ticketing systems
  - Mobile phone applications

Notorious NFC families

- MIFARE
  - MIFARE Classic
  - MIFARE Ultralight
  - MIFARE DesFire
- HID iClass
- Calypso
- FeliCa

MIFARE Classic

- 1-4 KB memory storage device
- ~~Strong~~ access control mechanisms
  - A key is required to access data sectors
  - Use of ~~Crypto1~~ **Crapto1** algorithm
  - Sadly broken..
  - ..but still so widely used (!) – RFID door tokens, transport tickets, etc.

MIFARE Ultralight

- 64 byte memory storage device
- Basic security mechanisms
  - OTP (One-Time-Programmable) sector
  - Lock bytes sector
  - Mostly used for disposable tickets
  - It has some more secure children:
    - ULTRALIGHT C
    - ULTRALIGHT EV

MIFARE DesFire

- 2 KB, 4KB or 8 KB memory size
- Advanced security mechanisms (3DES, AES, etc.)
- File system structure is supported
- Several variants are available
  - DESFIRE
  - DESFIRE EV1
  - DESFIRE EV2

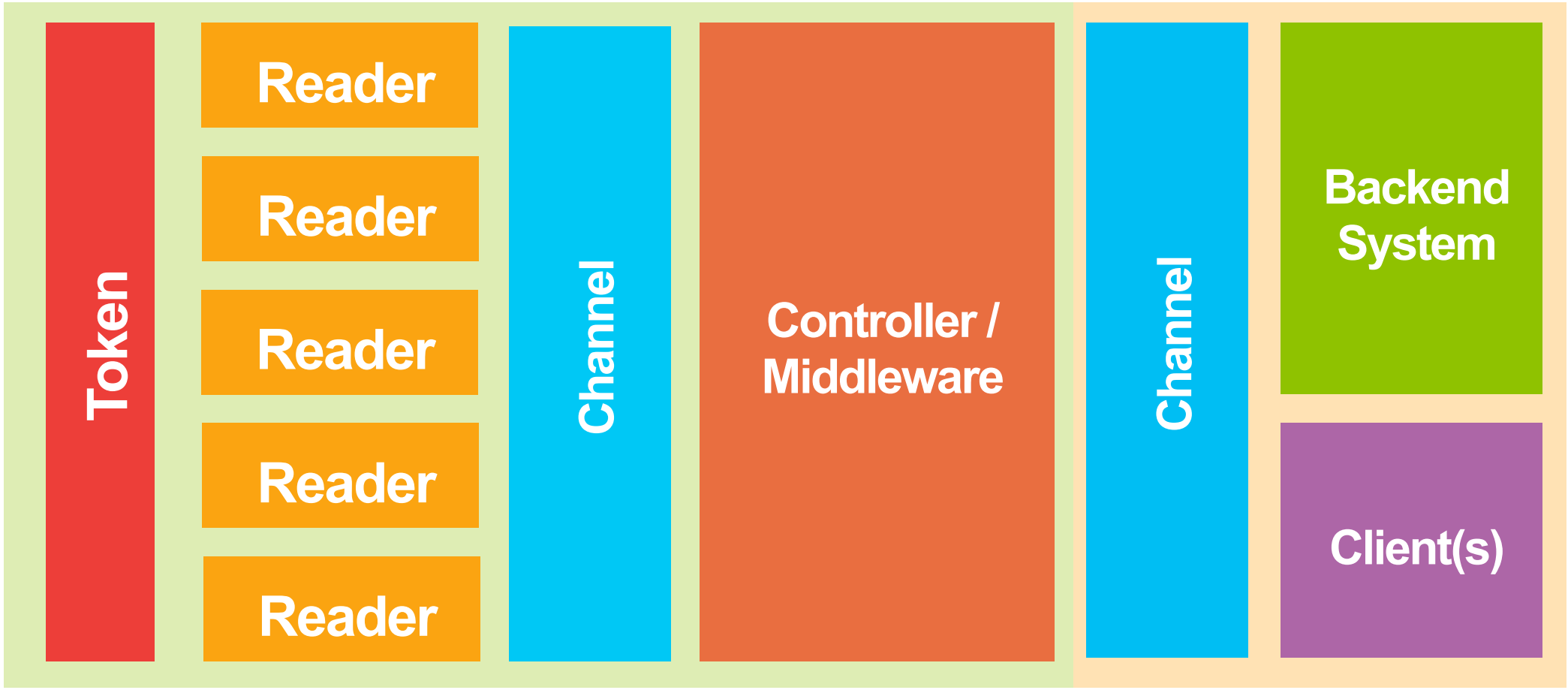
HID iClass

- Same encryption and authentication keys are shared across every HID iClass Standard Security installations (!)
- Keys have already been extracted (!!)
- Two variants
  - iClass Standard (very common)
  - iClass High Secure (not that common)
- **Both variants are BROKEN**

NFC-based Electronic Access Control systems

- We need to create a common **methodology**
- We need **tools** to effectively assess these systems
- We need **secure architectures** as references and best practices

NFC-based Electronic Access Control systems



The token

- Usually a NFC card
  - MIFARE Ultralight
  - MIFARE Classic
  - HID
- The card can store
  - Timestamp of the last stamping
  - Details on the location where we used the toke
  - Credentials, access level, etc.

The token

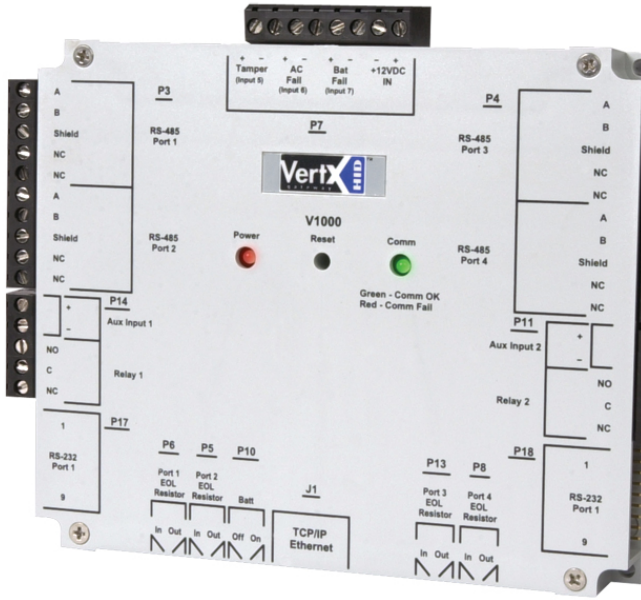
- What about MIFACE Classic?
  - It is just BROKEN
- What about MIFARE Ultralight?
  - Well, it’s bleeding..
    - Lock attack
    - Time attack
    - Reply attack..
- HID
  - BROKEN, again

Readers

- Can operate offline or online
- Wire or wireless connected to the controller
  - RS232, Ethernet, etc.
- Usually supports multiple standards
- Can store secrets and keys used for authentica
- Usually it can
  - Read token(s) data
  - Send token data to the controller
  - Give a feedback to users on operation's success

Controller

- Connected both to readers and backend
  - Wiegand, Ethernet, rs232
- Receives data from the reader(s)
  - Support multiple readers technologies
- Sends the data to the backend
  - Open the door
  - Deny the access



The backend

- It can be cloud-based or not
- Usually wired connected
  - RS232, Ethernet, etc.
- Performs multiple operations
  - Provide token validation “logic”
  - Statistics
  - Logging

Agenda

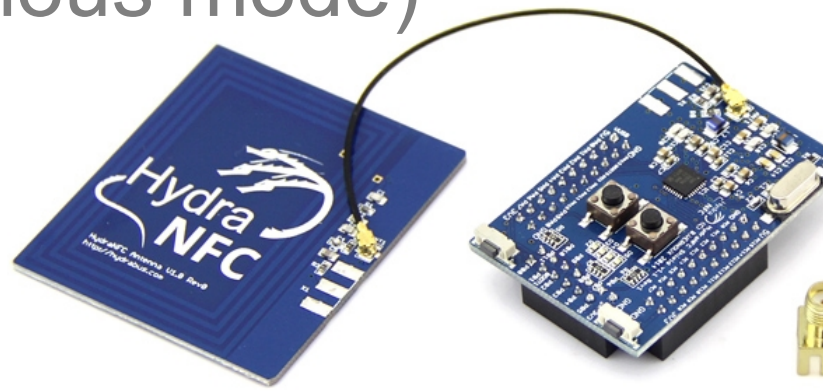
- Module 2 – attacking NFC
  - NFC: what are we talking about?
  - Weapons for NFC-based solutions
  - Penetration test methodology
  - Hands-on
  - Case studies

Tools of the trade

- HydraNFC
- ProxMark3
- ChameleonMini
- NFCulT

HydraNFC

- HydraNFC (~90 €)
  - **http://hydrabus.com/hydranfc-1-0-specifications/**
- Users Texas Instrument TRF7970A NFC chipset (**13.56MHz only**)
- MIFARE 1k and 14443A UID emulation
- ISO 14443A sniffing (also autonomous mode)
- 2 different raw modes



ProxMark3

- ProxMark3 (~200 €)
- HF and LF capabilities
- Very large community
  - **http://proxmark.org/forum/index.php**
- Supports almost every known RFID ta
- Support sniffing and emulation

ChameleonMini

- ChameleonMini (~100 €)
  - **http://kasper-oswald.de/gb/chameleonmini/**
- HF (**13.56MHz**) only
- Almost same capabilities as HydraN
- Different chipset
- The firmware is only available for olc revision

Opposing Force own weapon

- NFCulT (~0 €)
- Originally designed for ticketing systems, it can be also used for generic EAC system security assessment
- Mobile app for NFC-enabled Android smartphones
  - **Implements Lock, Time and Reply attacks**
- A “custom edit mode” is available for bit by bit data editin
- The app currently supports the MIFARE Ultralight format only
  - **MIFARE Classic support will be released on summer 2016**

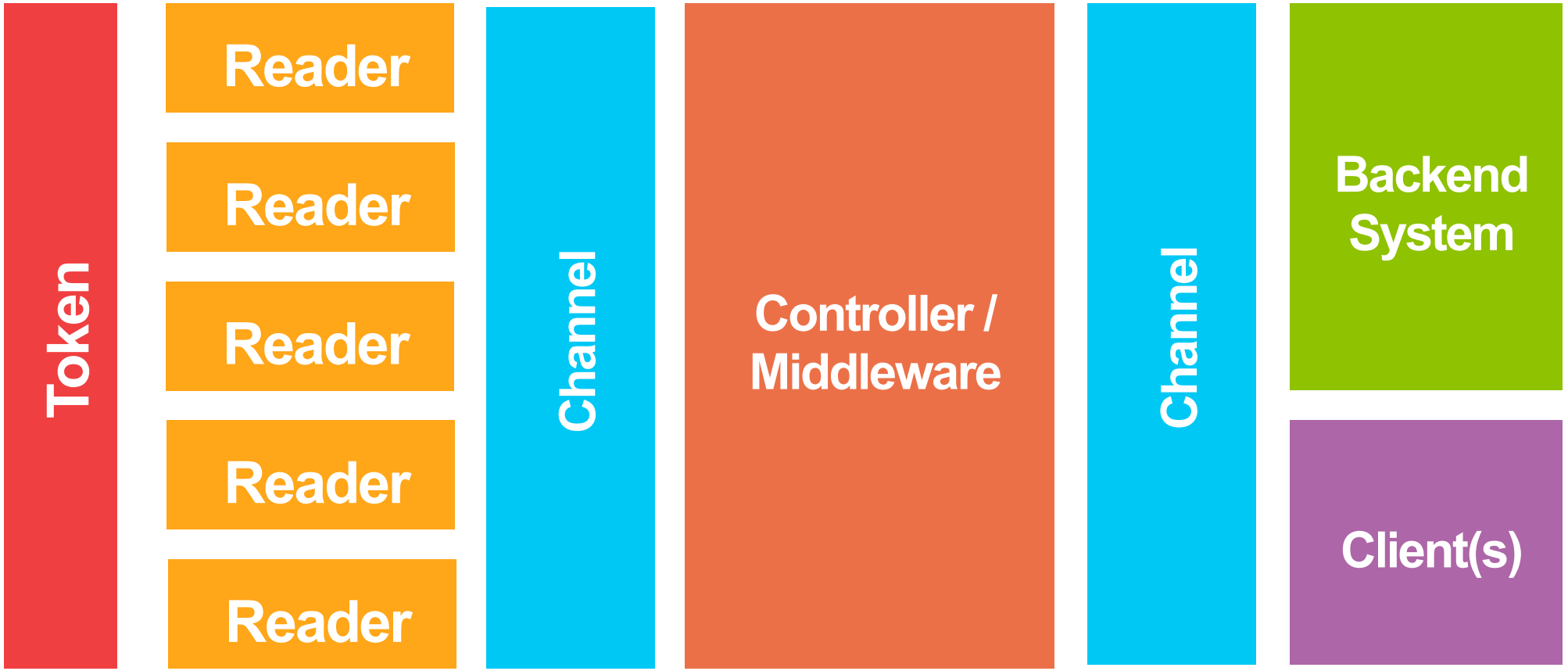
The custom editing feature

- The features is useful to better understand the structure of data stored onto the token
- Quick encoding from hex to bin and back
- The app allows token bit by bit data editing

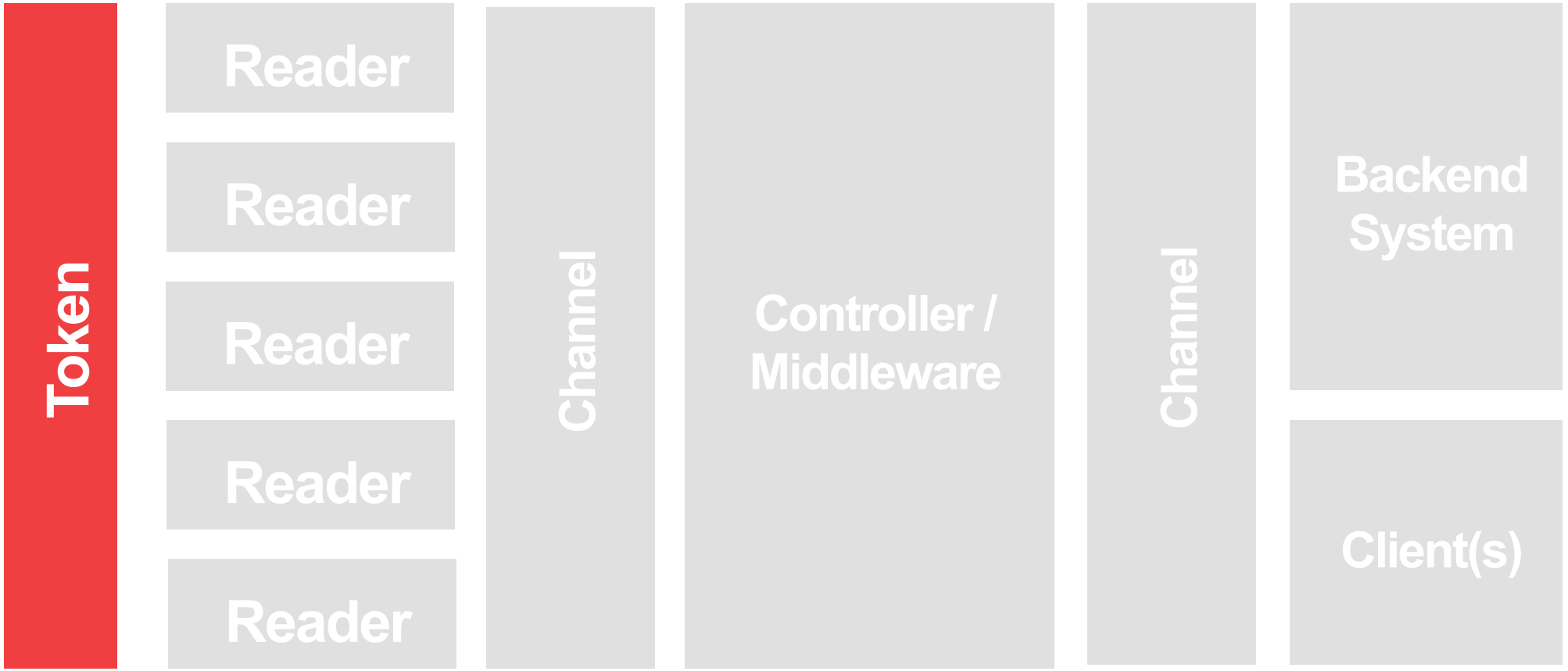
Agenda

- Module 2 – Attacking NFC
  - NFC: what are we talking about?
  - Weapons for NFC-based solutions
  - Penetration test methodology
  - Hands-on
  - Case studies

Access Control system attack surface



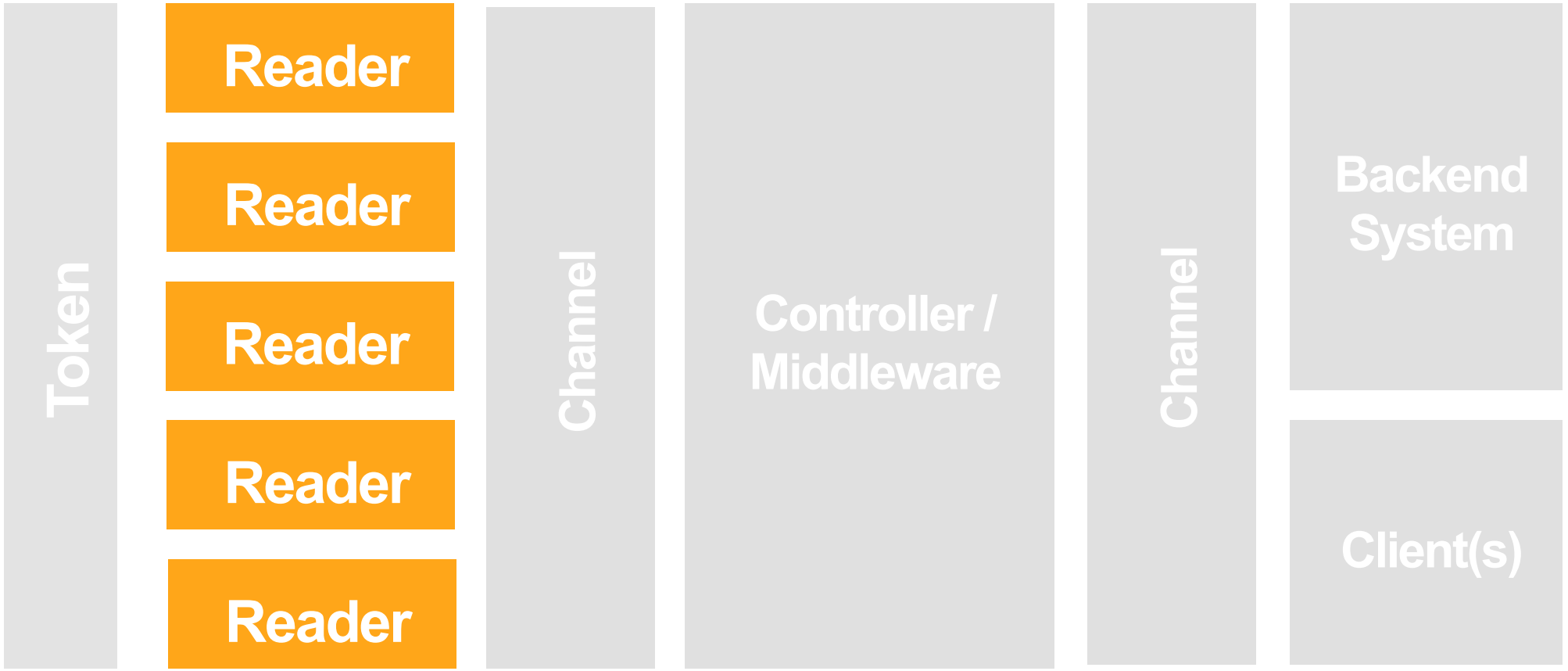
Access Control system attack surface



The token

Attack Surface	Attacks to Perform	Impact
NFC Interface	Analyze the authentication mechanisms	Secrets extraction, MiTM attacks
Hardware board	Side channel attacks	Secrets dumping or guessing
Memory	Assess logic vulnerabilities in the implementation	Bypass security mechanisms

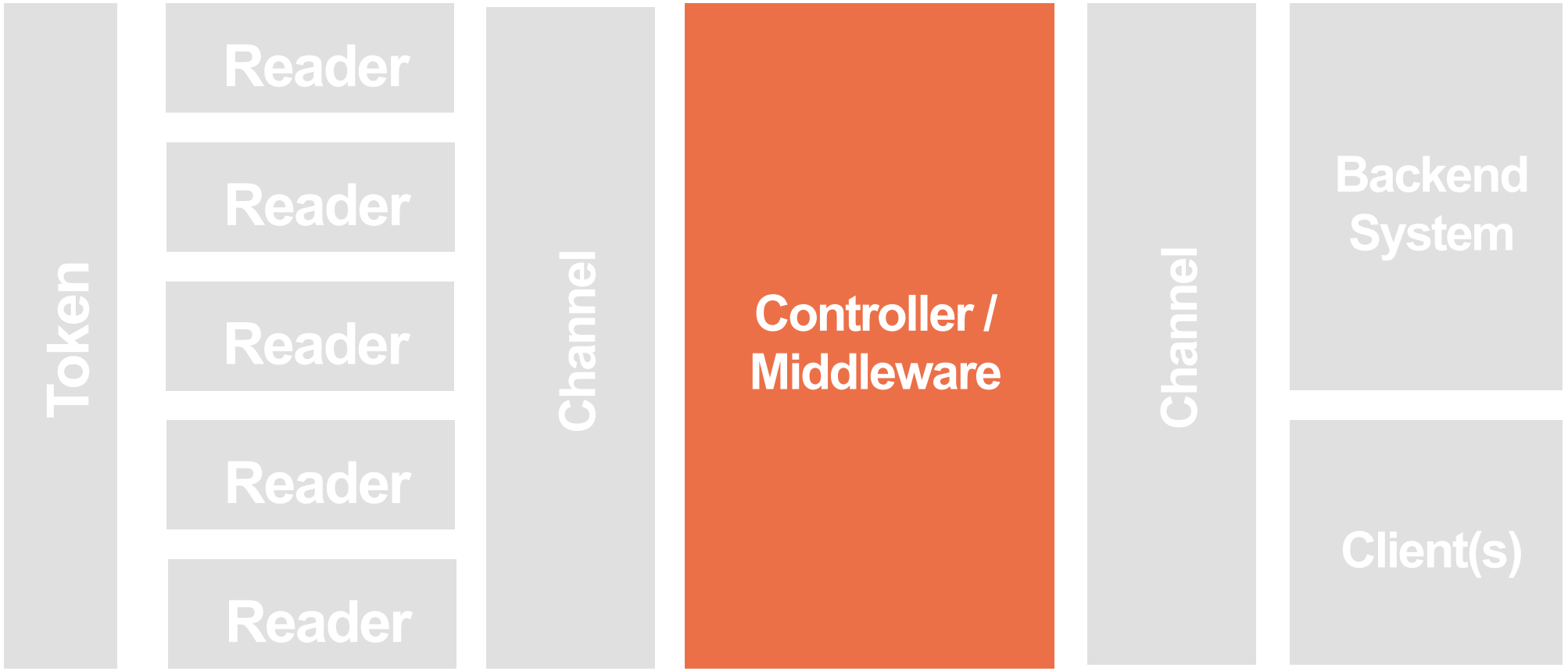
Access Control system attack surface



The reader

Attack Surface	Attacks to Perform	Impact
NFC Interface	Analyze the authentication mechanisms	Secrets extraction, MiTM attacks
Hardware board	Analyze the exposed interface (JTAG, UART, etc.)	Firmware or secrets dumping
Ethernet, wiegand, etc.	Is MITM possible? Intercepting the exchanged data	Intercepting secrets or sensitive data

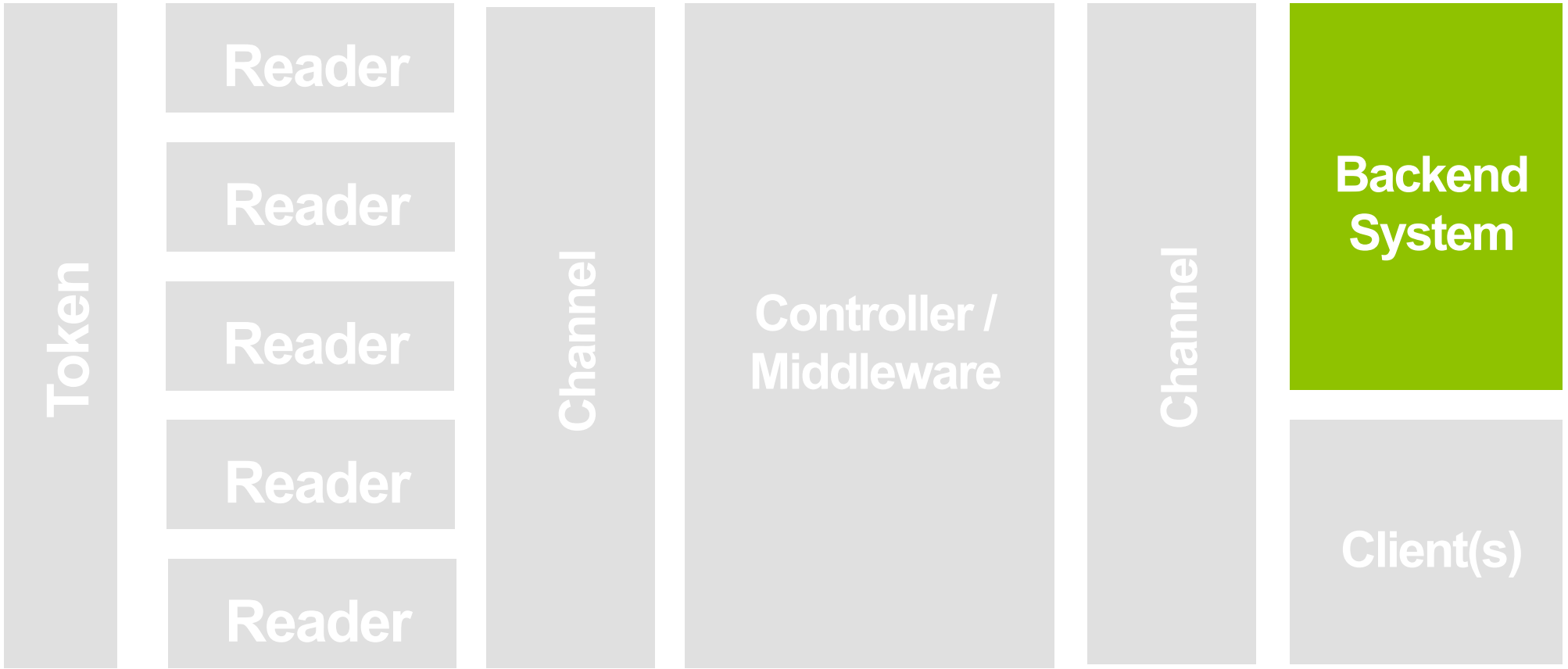
Access Control system attack surface



The controller

Attack Surface	Attacks to Perform	Impact
Hardware board	Analyze the exposed interface (JTAG, UART, etc.)	Firmware or secrets dumping
Eth, serial Interfaces, etc.	Is MITM possible? Intercepting the data	Intercepting secrets or sensitive data
Computer Application	Analyzing exposed network services	Complete control of the machine (e.g., add new users)

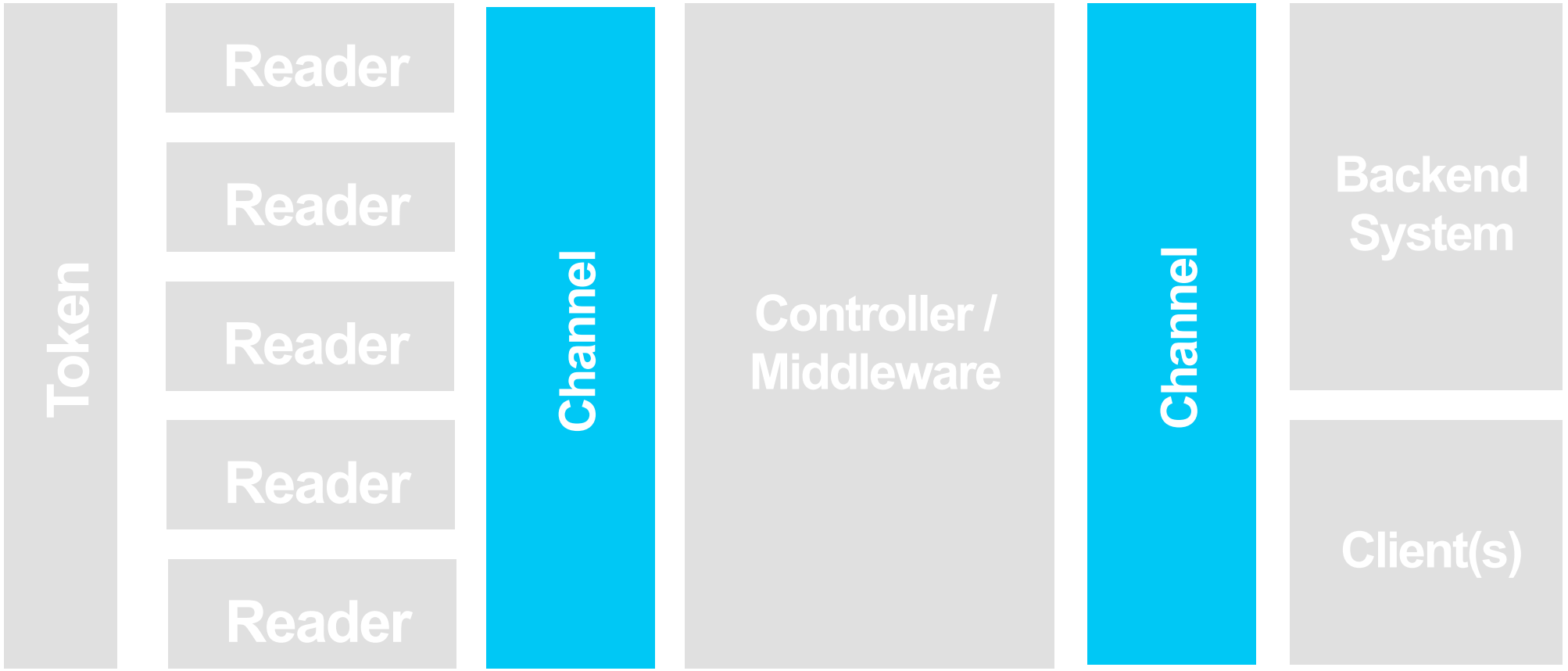
Access Control system attack surface



The backend

Attack Surface	Attacks to Perform	Impact
Web application(s)	Classic web app-related attacks	Data exfiltration, service interruption, etc.
Network service(s)	Classic network services-related attacks	Data exfiltration, service interruption, etc.
Physical location	Try to get physical access to the servers	Basically, heavily PWNED

Access Control system attack surface



The channels

Attack Surface	Attacks to Perform	Impact
Hardware board	Identify forgotten or backdoor pins	Data exfiltration, firmware dumping
External wires	Try to intercept data passing through those wires	Intercepting sensitive information
Wireless connection	Intercept and inject data	Intercepting sensitive information, send spoofed information

Agenda

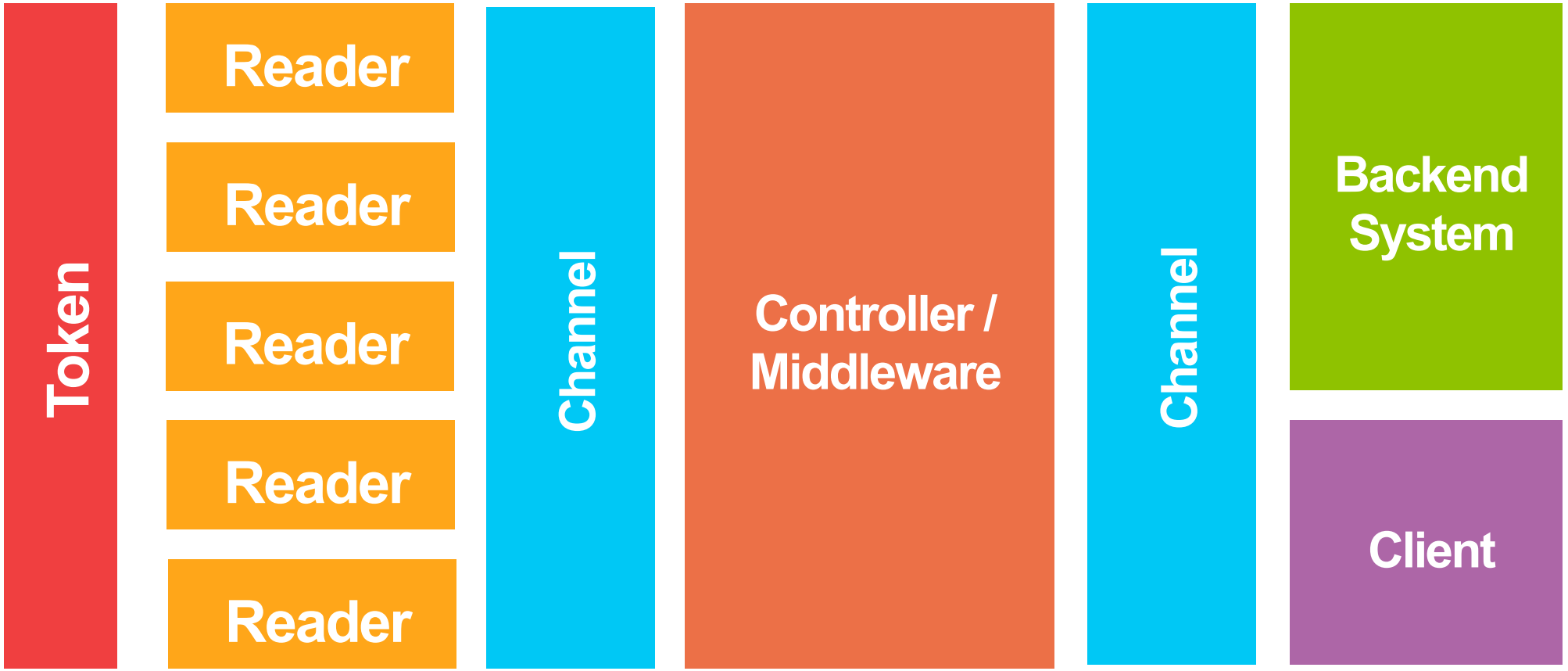
- Module 2 – Attacking NFC
  - NFC: what are we talking about?
  - Weapons for NFC-based solutions
  - Penetration test methodology
  - Hands-on
  - Case studies

Fire up your 

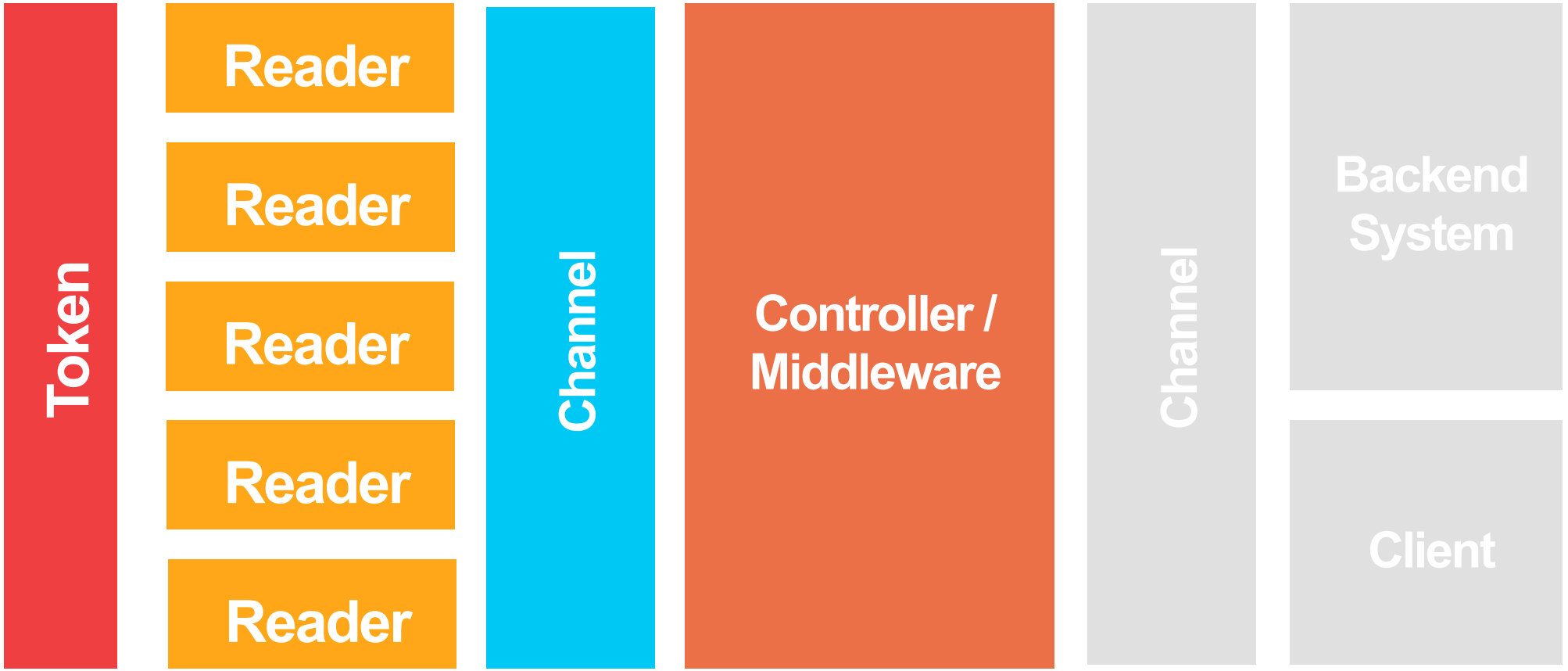
Agenda

- Module 2 – attacking NFC
  - NFC: what are we talking about?
  - Weapons for NFC-based solutions
  - Penetration test methodology
  - Hands-on
  - Case studies

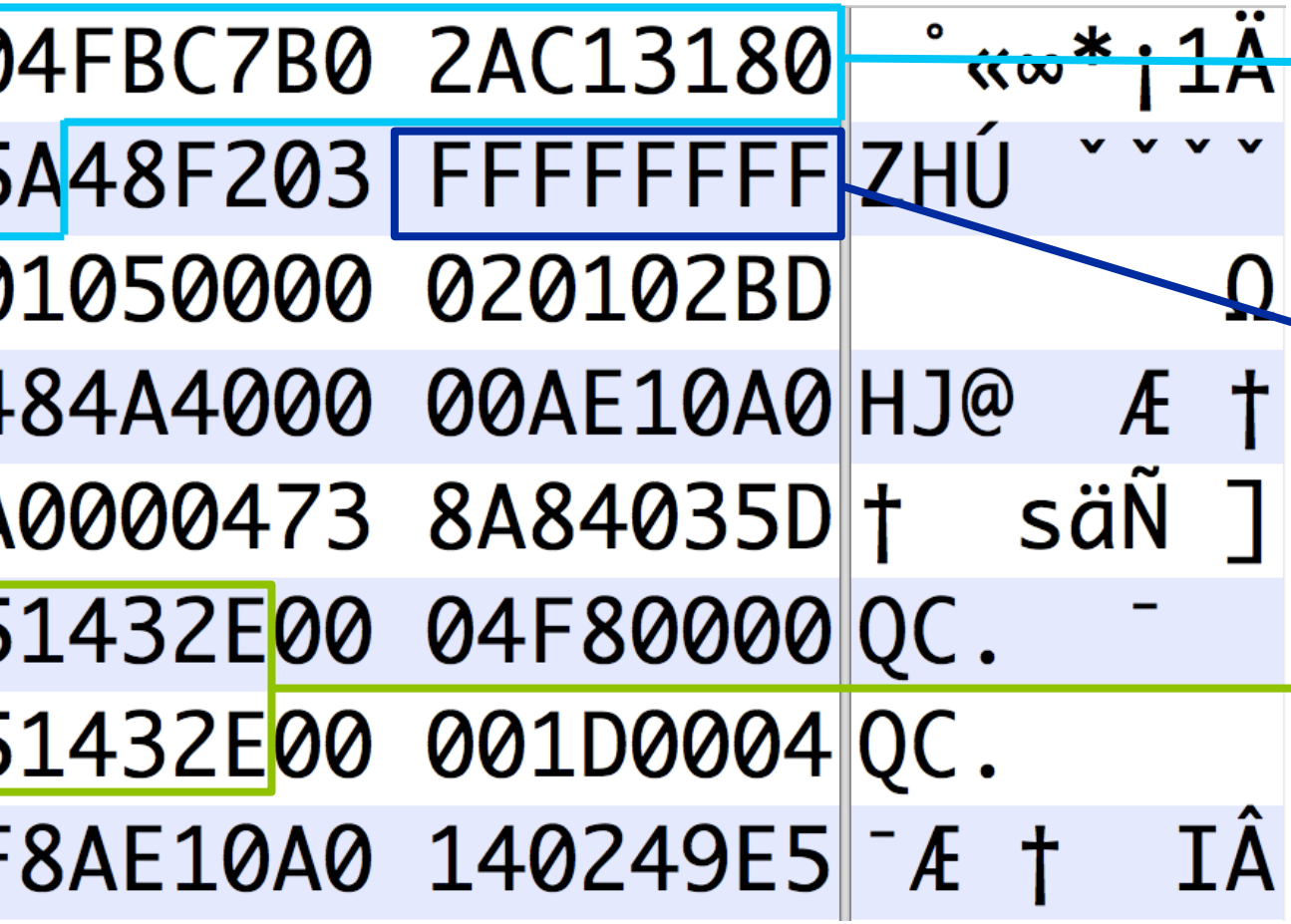
MIFARE Ultralight ticketing system



MIFARE Ultralight ticketing system



MIFARE Ultralight ticketing system

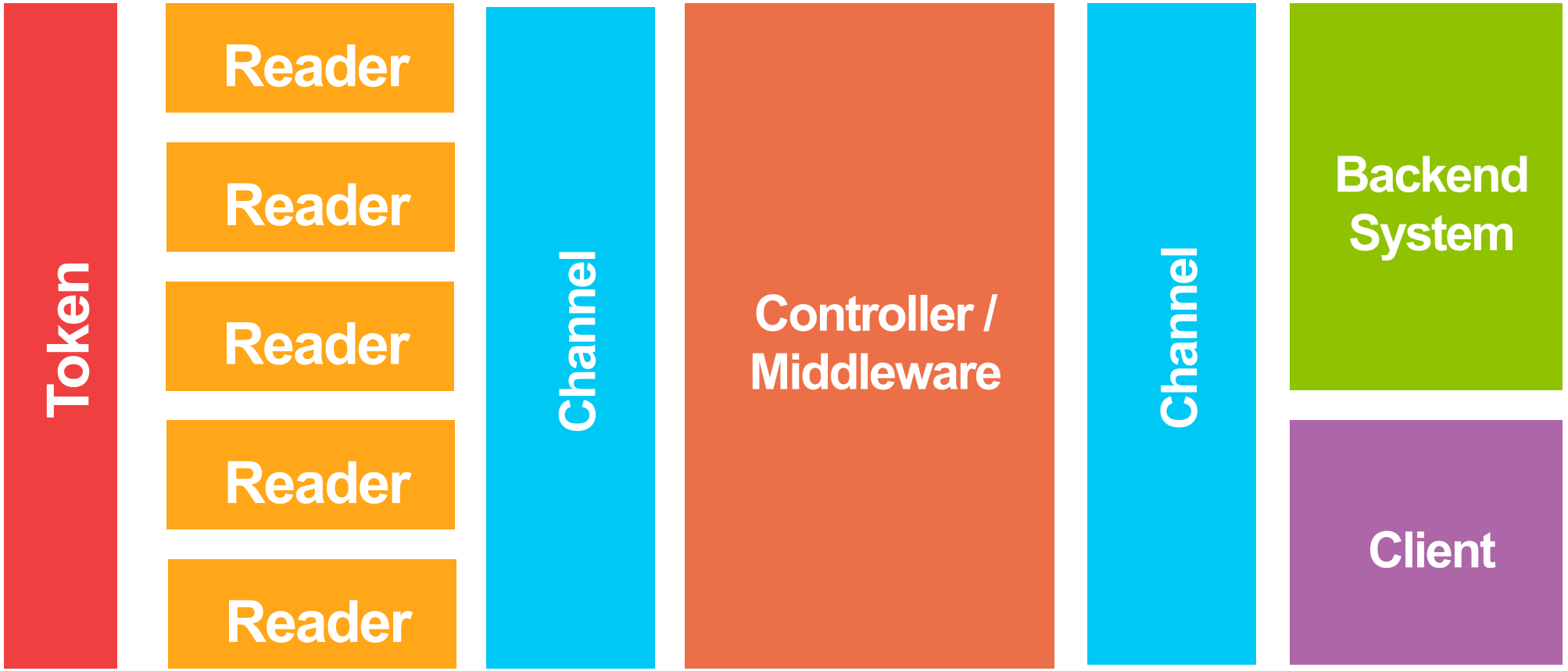


Absence of a UID blackli
in the backend

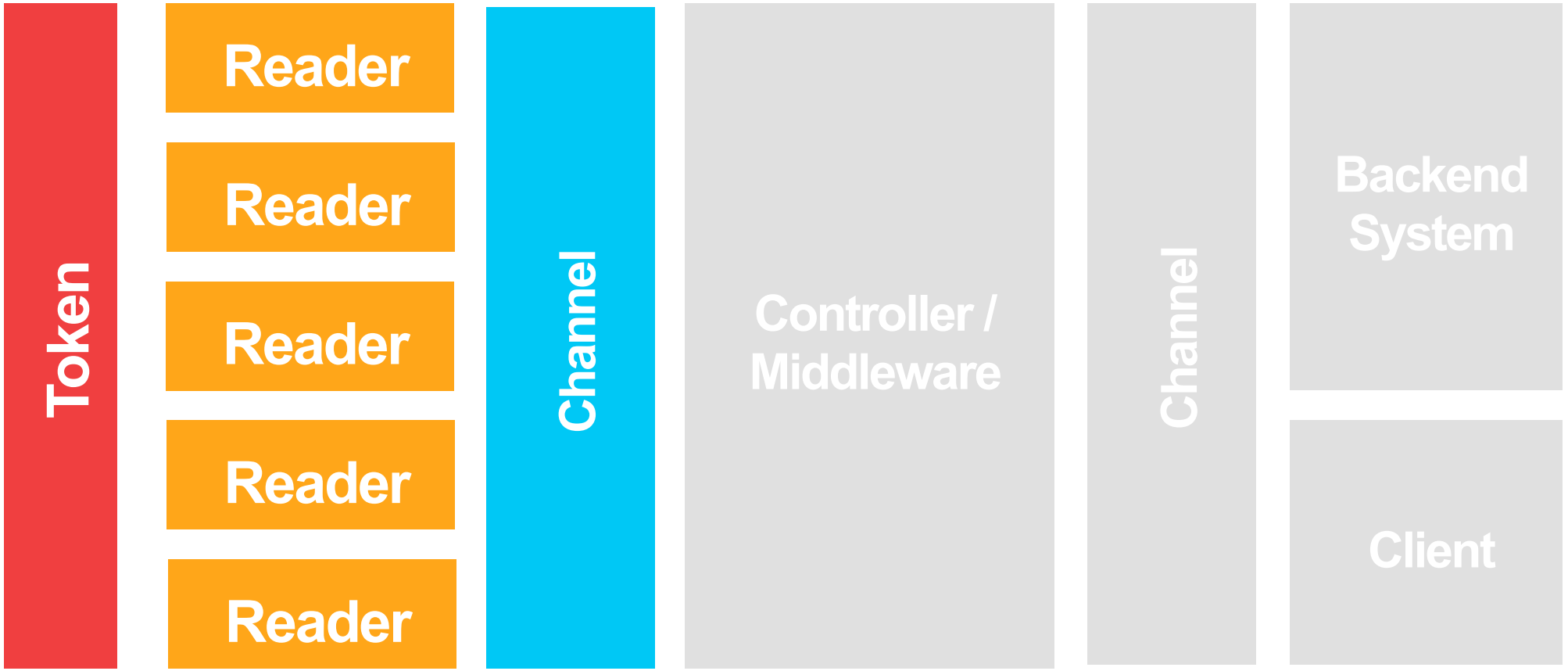
Lock bit for the OTP sect
is not checked by the
stamping machine

Timestamps are not
encrypted nor signed

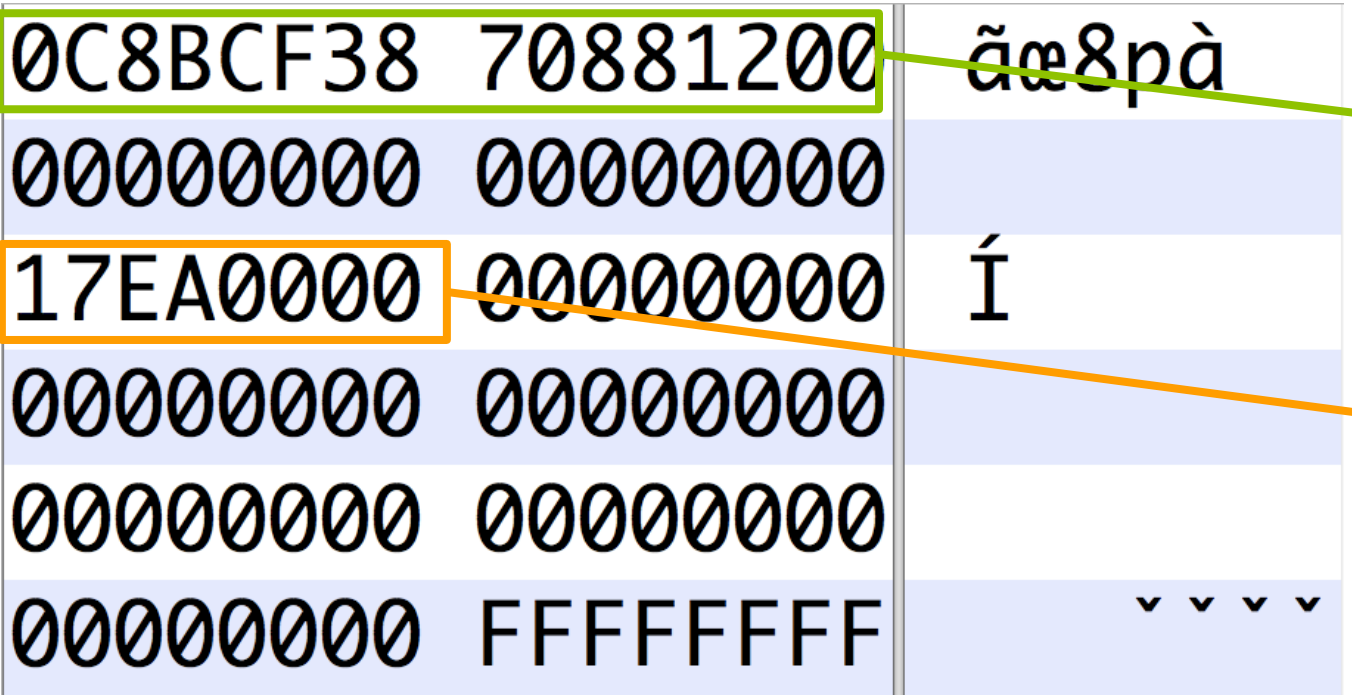
MIFARE Classic hotel door lock



MIFARE Classic hotel door lock



MIFARE Classic door lock



Card's UID

Room number:
int(0x17ea, 16) =
6122

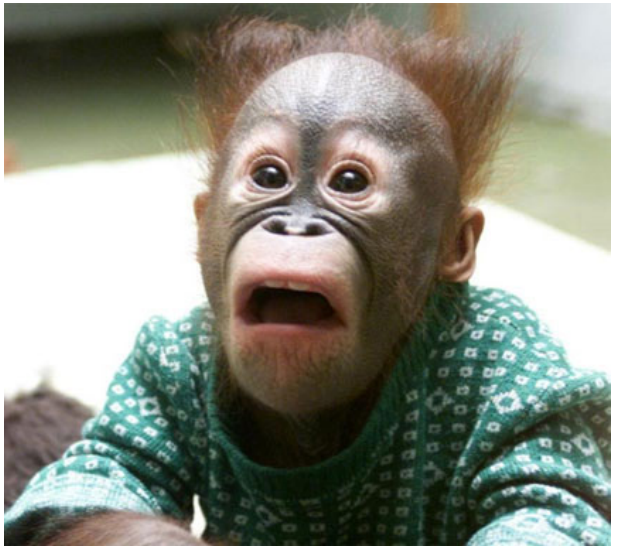
lodule 3 || attacking RF communicatior

Agenda

- Module 3 – Attacking RF communications
  - Radio Frequency and EAC Systems
  - Exploring Radio Frequency communications in practice
  - Hands-on: receiving your first transmission
  - SIGINT with GNU Radio
  - Understanding RF communications security

Radio Frequency and EAC Systems

- Radio Frequency identification is widely used to control physical accesses
- Advantages
  - Automatic identification
  - High reliability
  - ~~High security~~



Radio Frequency and EAC Systems

- Different technologies based on operating frequency band
  - **L**ow **F**requency (LF) – 125 KHz
  - **H**igh **F**requency (HF) – 13.56 MHz
  - **U**ltra **H**igh **F**requency (UHF) – 433 MHz, 860-960 MHz and 2.4 GHz

Radio Frequency and EAC Systems

Low **F**requency band

- Tags
- Access control token

Radio Frequency and EAC Systems

High **F**requency band

- Door locks
- Ticketing systems

Radio Frequency and EAC Systems

Ultra **H**igh **F**requency band

- Automated Gates
- Keyless Entry Systems
- Alarms
- Smart Locks

Radio Frequency and EAC Systems

- Common technologies and protocols
  - Fixed and rolling code
  - NFC
  - Bluetooth
  - ZigBee
  - Z-Wave

Agenda

- Module 3 –Attacking RF communications
  - Radio Frequency and EAC Systems
  - Exploring Radio Frequency communications in practice
  - Hands-on: receiving your first transmission
  - SIGINT with GNU Radio
  - Understanding RF communications security

Exploring Radio Frequency communication

- How to explore wireless communications?
  - Software Defined Radio (SDR) devices with GNU Radio
- Software implementation of most parts of a radio system
  - Cheap hardware
  - High flexible

Exploring Radio Frequency communication

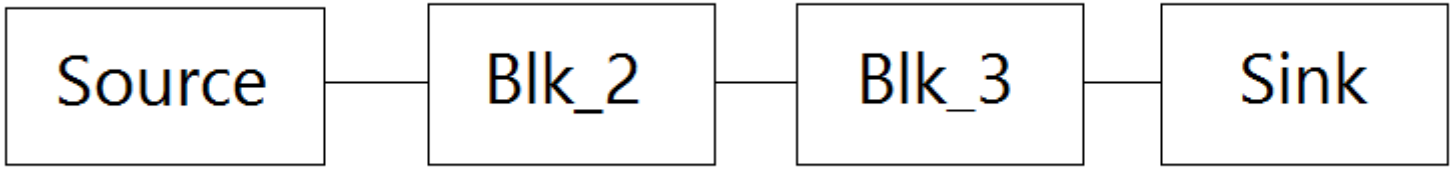
Three SDR-compatible devices

Device	Frequency Range	Bandwidth	Price
RTL-SDR Dongle	24 MHz – 1.76 GHz	2.4 MHz	~ 20 €
HackRF	1 MHz – 6 GHz	20 MHz	~ 300 €
USRP B200	70 MHz – 6 GHz	56 MHz	~ 700 €

Exploring Radio Frequency communication

GNU Radio

- Platform to develop radio applications, called **flowgraph**
  - Series of connected signal processing blocks
- GNU Radio libraries include blocks to perform signal processing

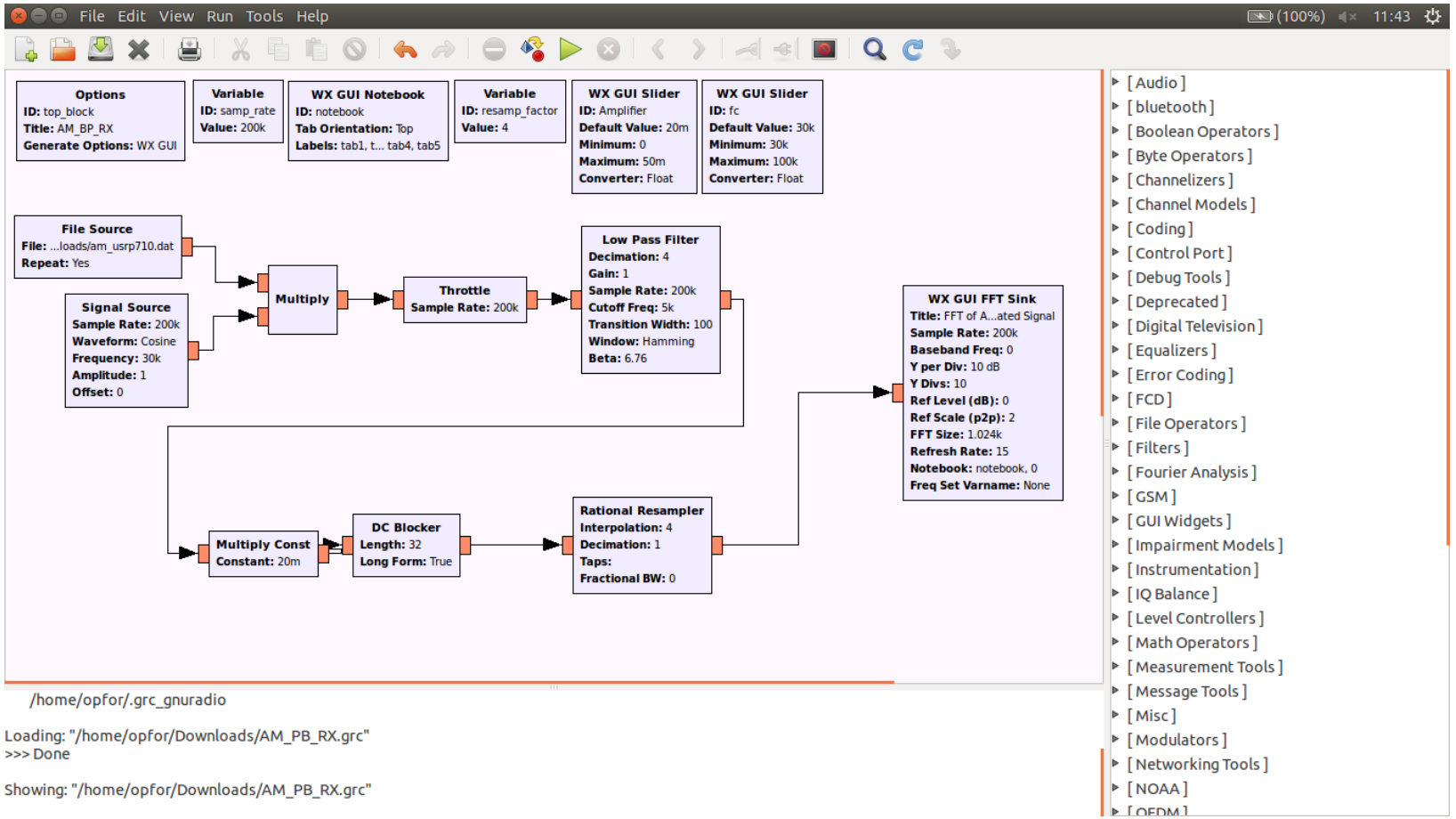


Exploring Radio Frequency communication

- GNU Radio
  - Supports the programming of custom C++ blocks
  - GNU Radio Companion (GRC)
    - Graphical UI to program GNU Radio applications
    - Supports the creation of UI for applications

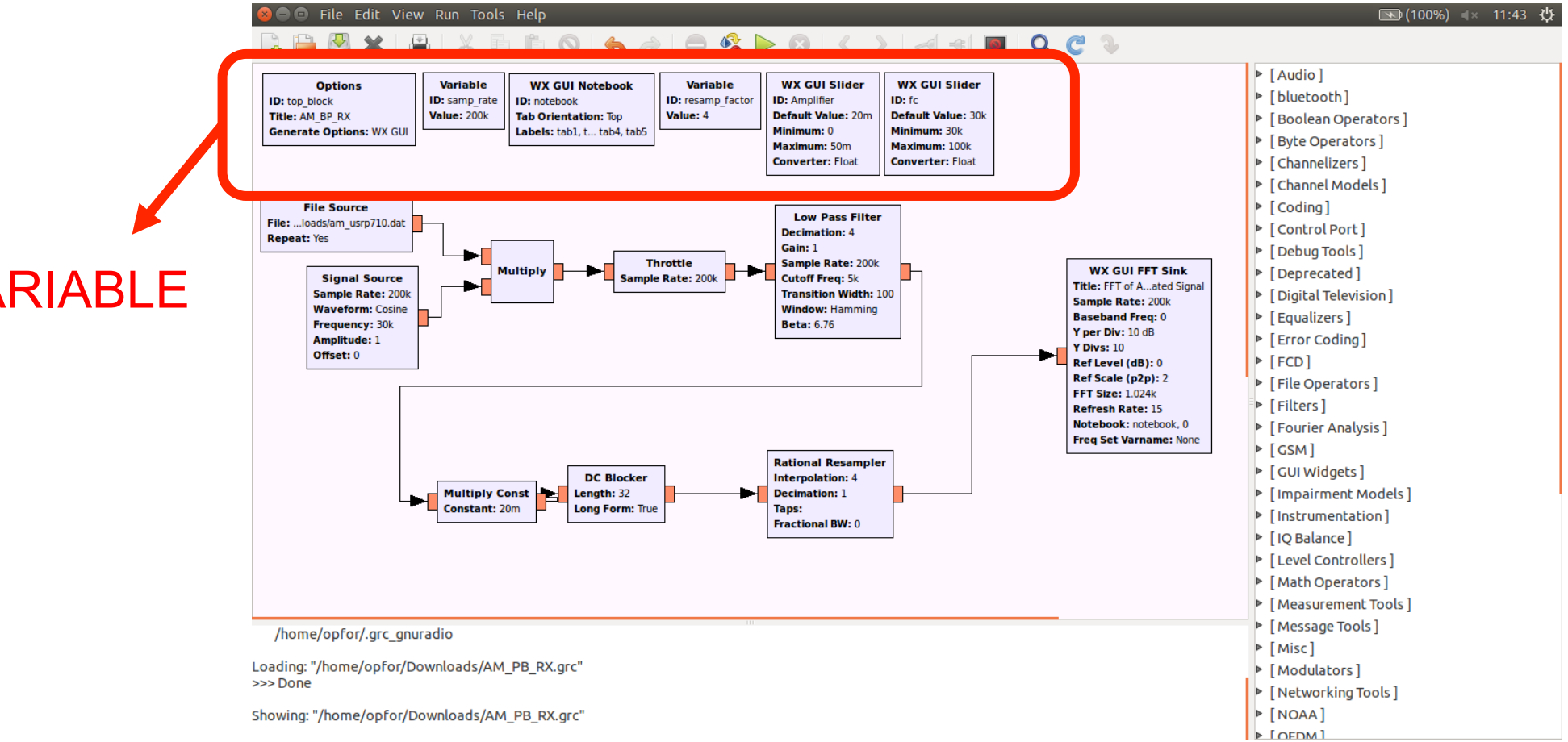
Exploring Radio Frequency communication

- GRC Interface



Exploring Radio Frequency communication

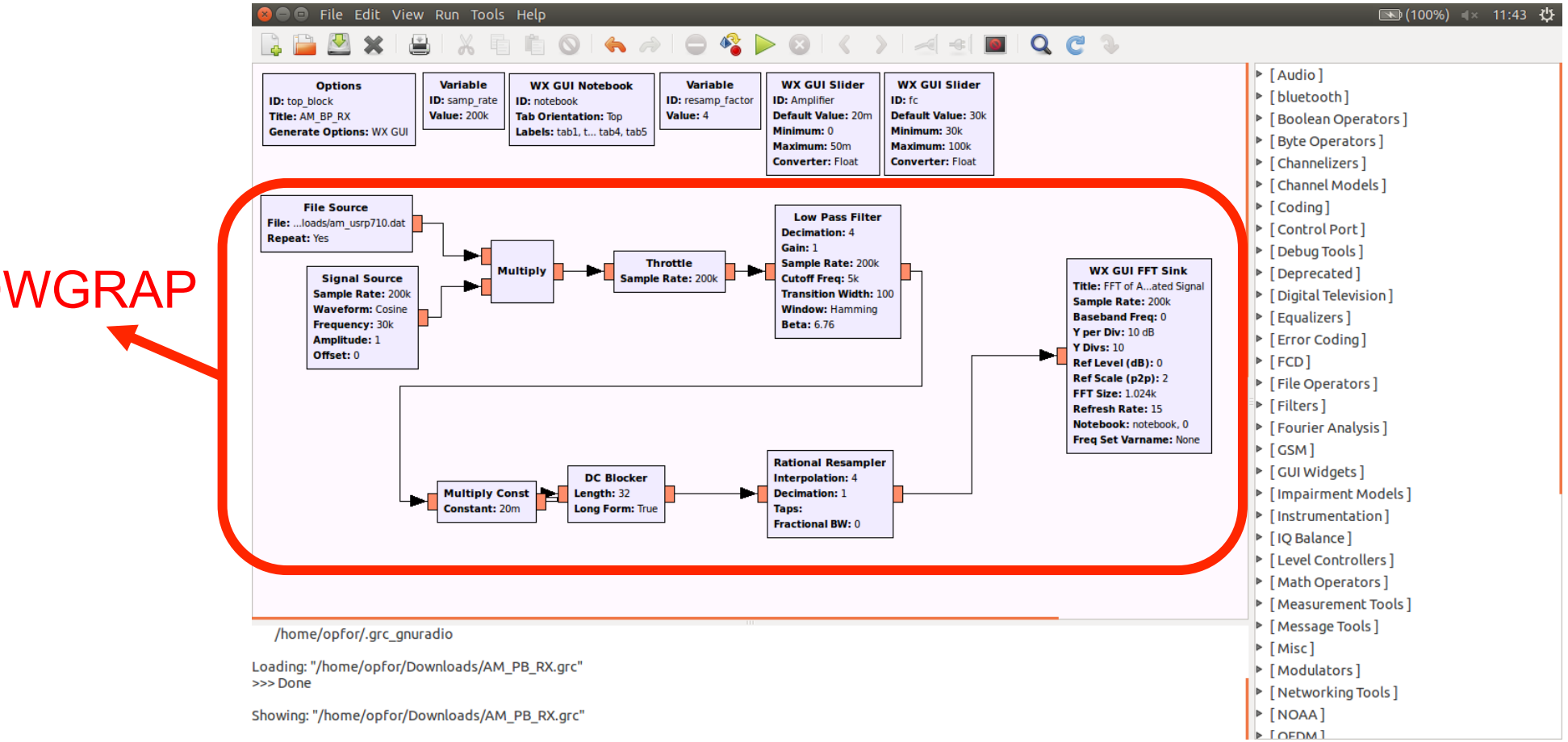
- GRC Interface



ARIABLE

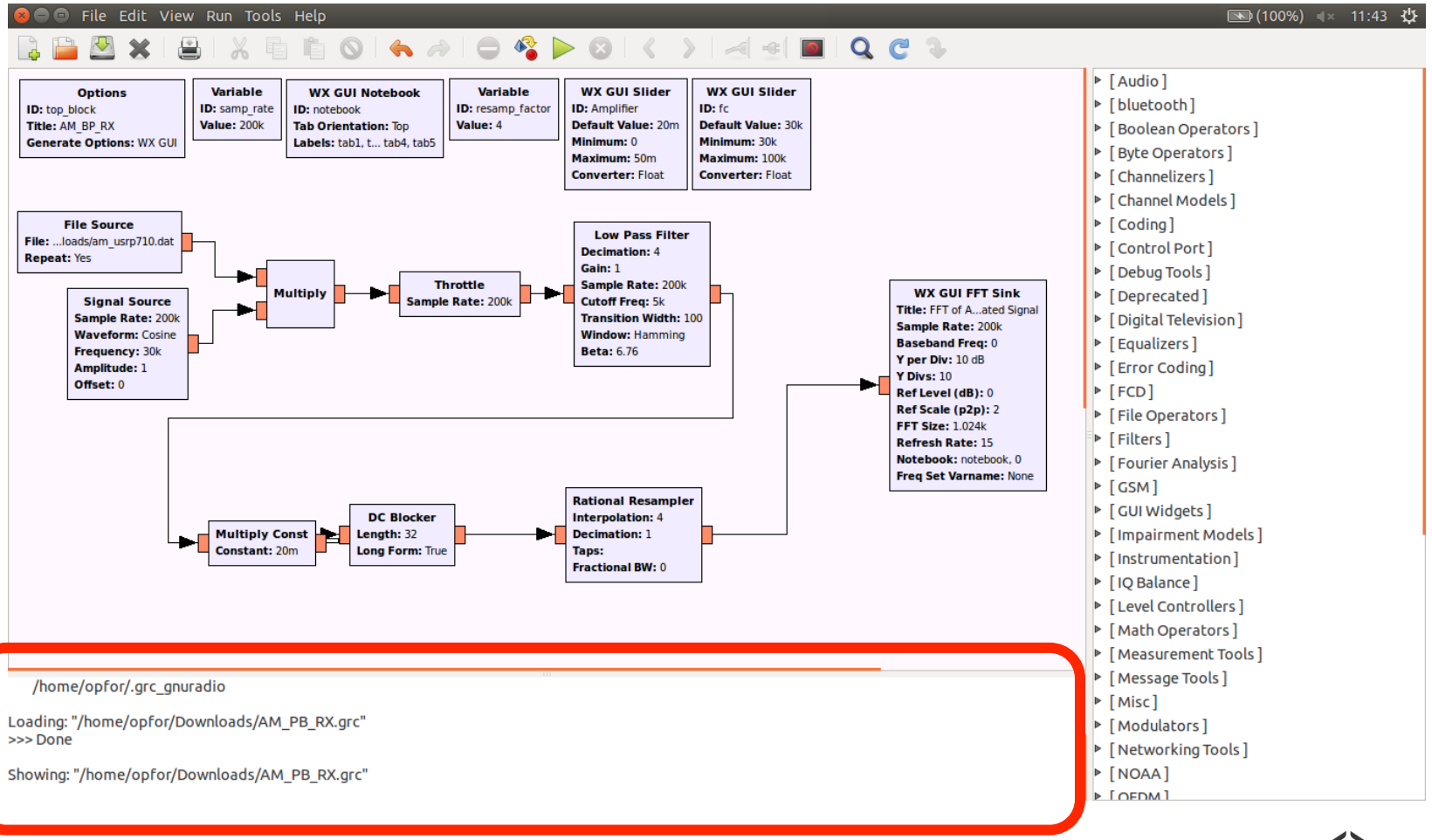
Exploring Radio Frequency communication

- GRC Interface



Exploring Radio Frequency communication

- GRC Interface

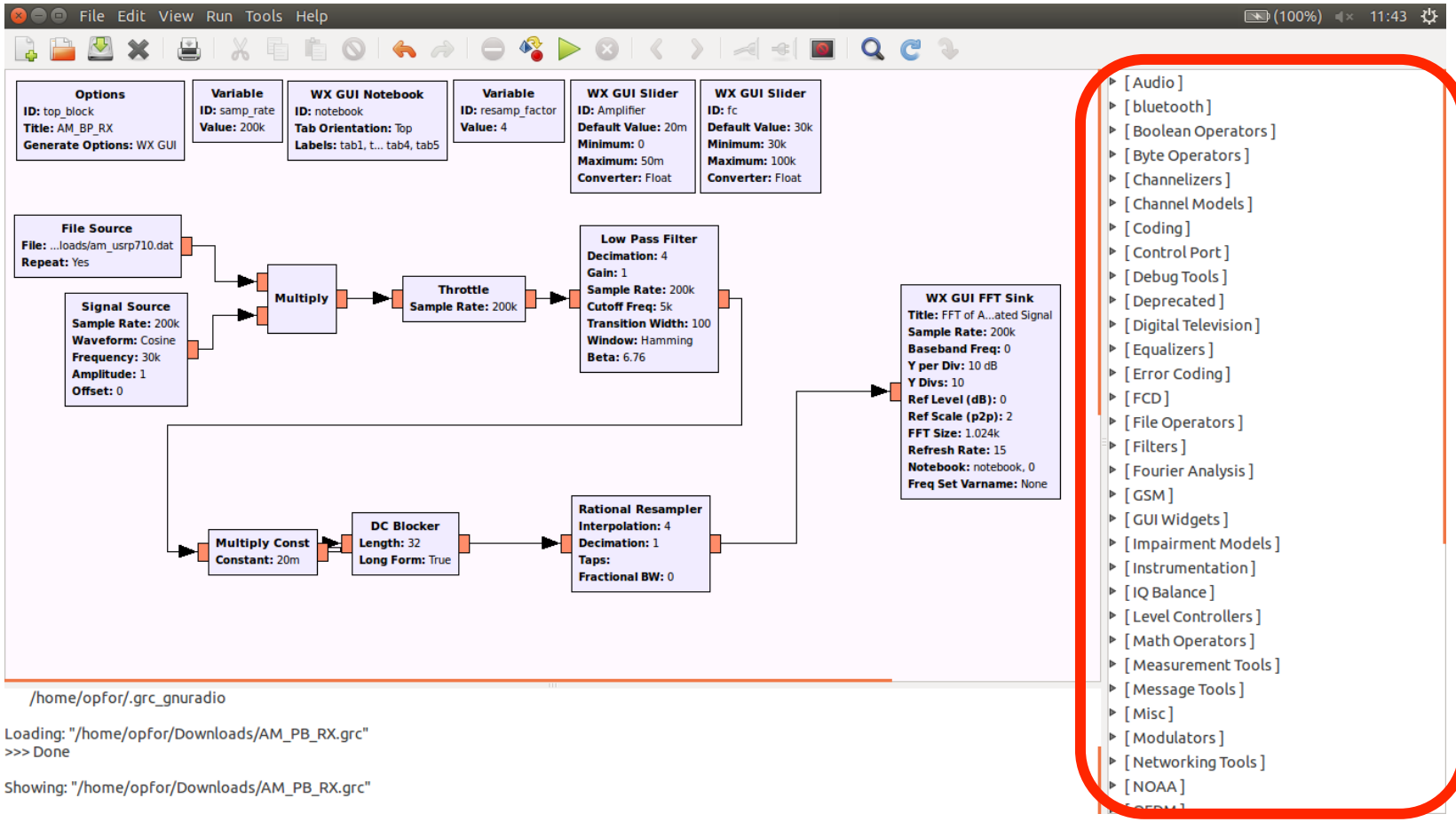


RMINA

OPPOSING FO

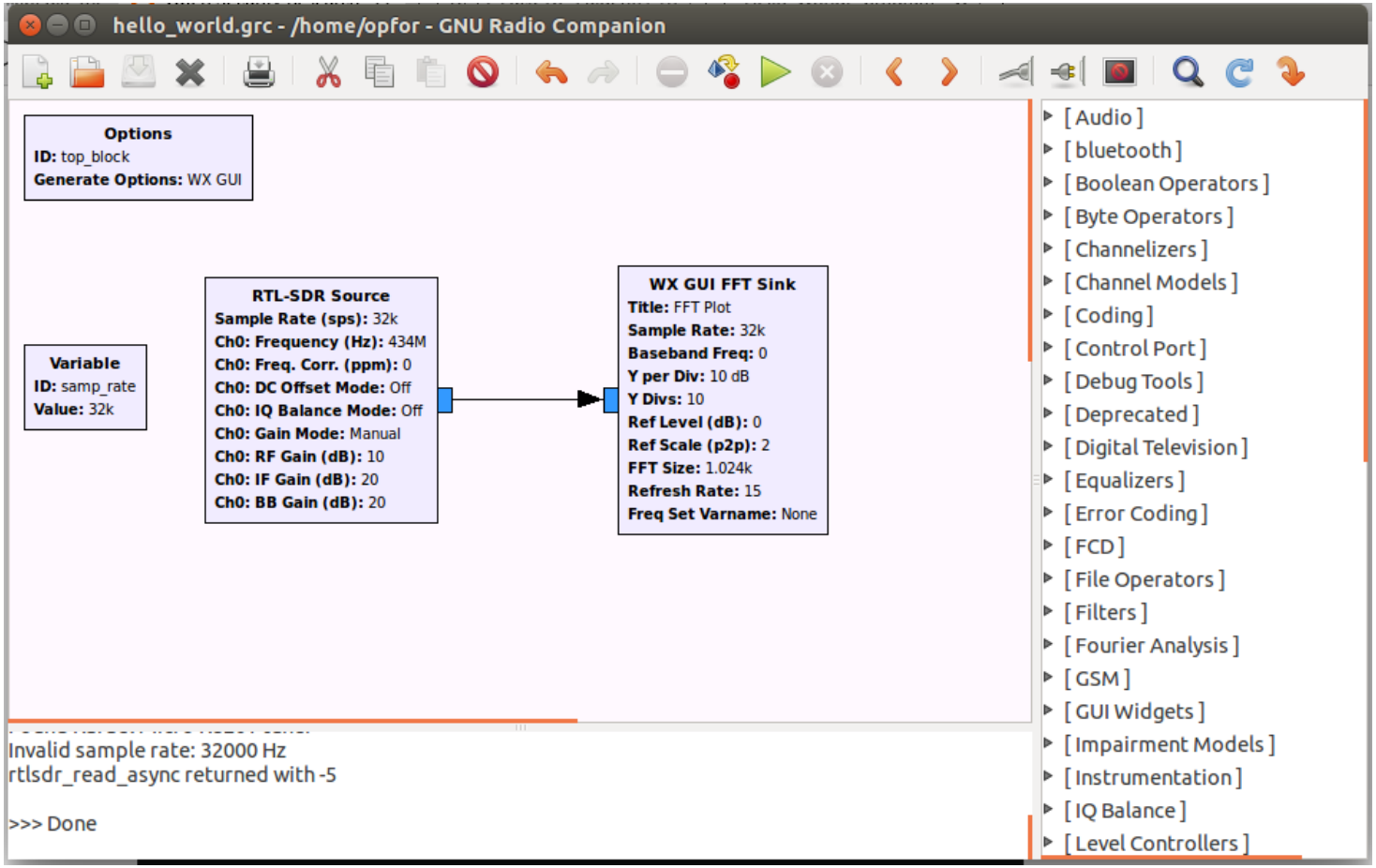
Exploring Radio Frequency communication

- GRC Interface



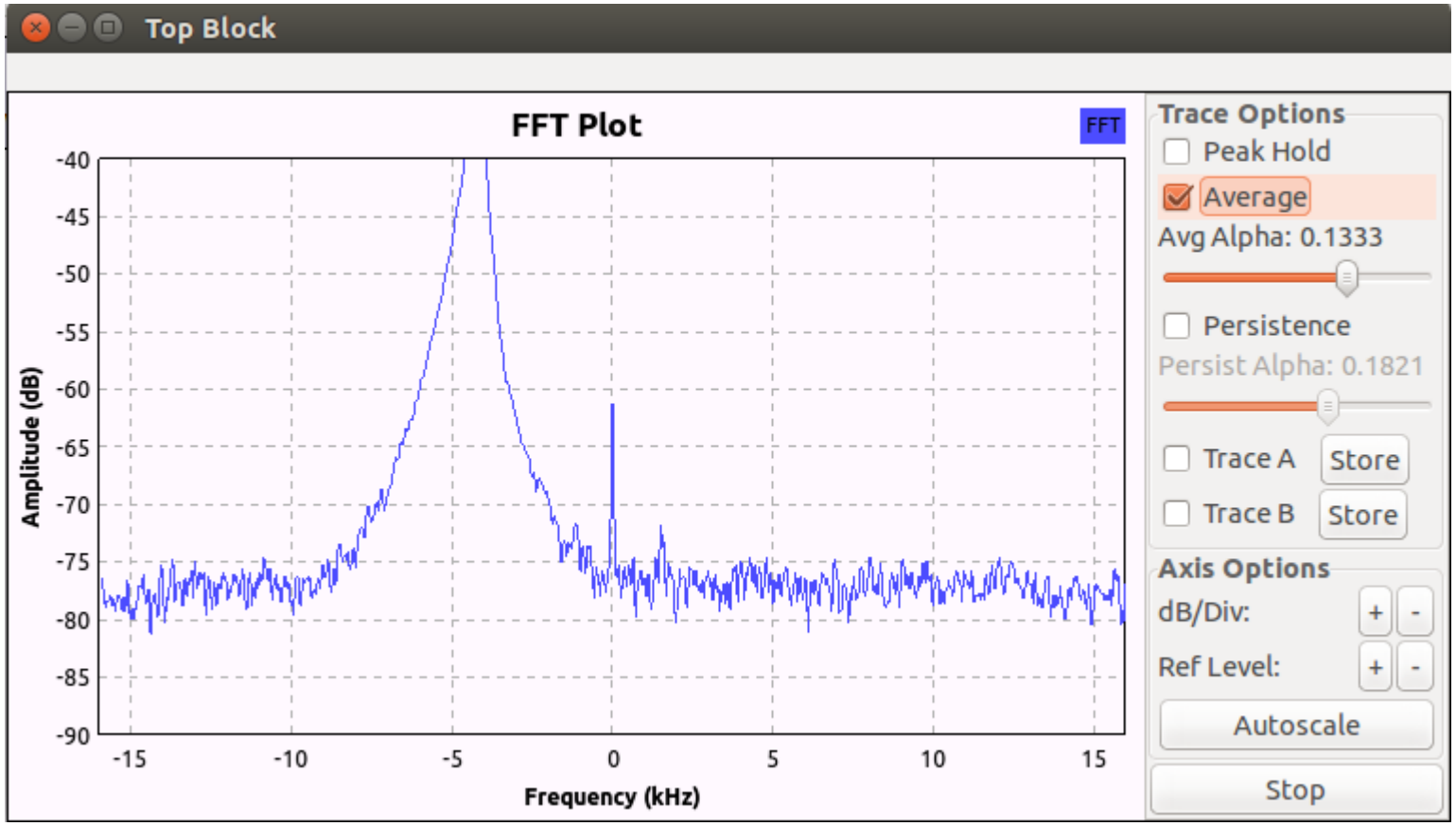
Exploring Radio Frequency communication

- “Hello World” in GNU Radio



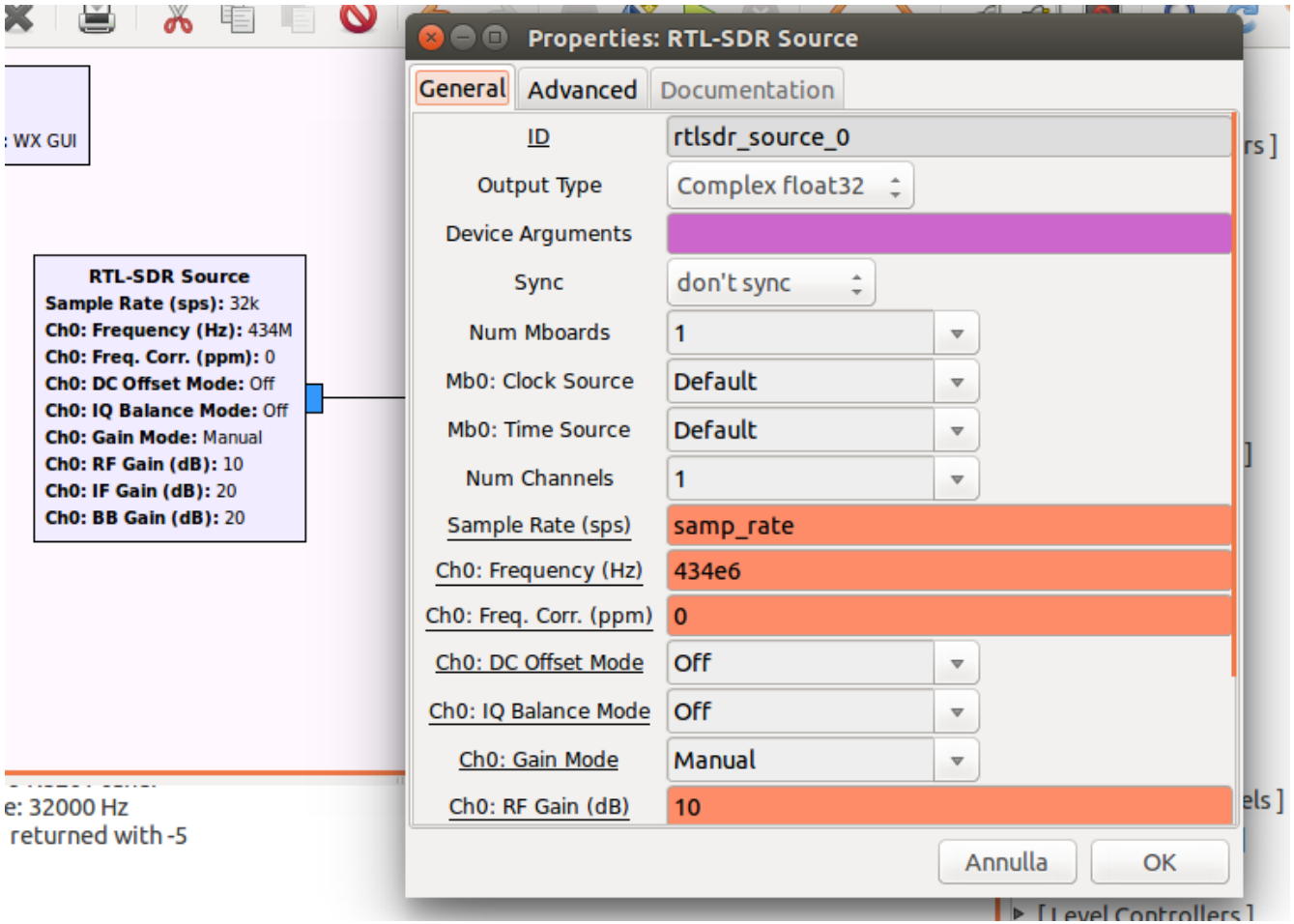
Exploring Radio Frequency communication

- “Hello World” in GNU Radio



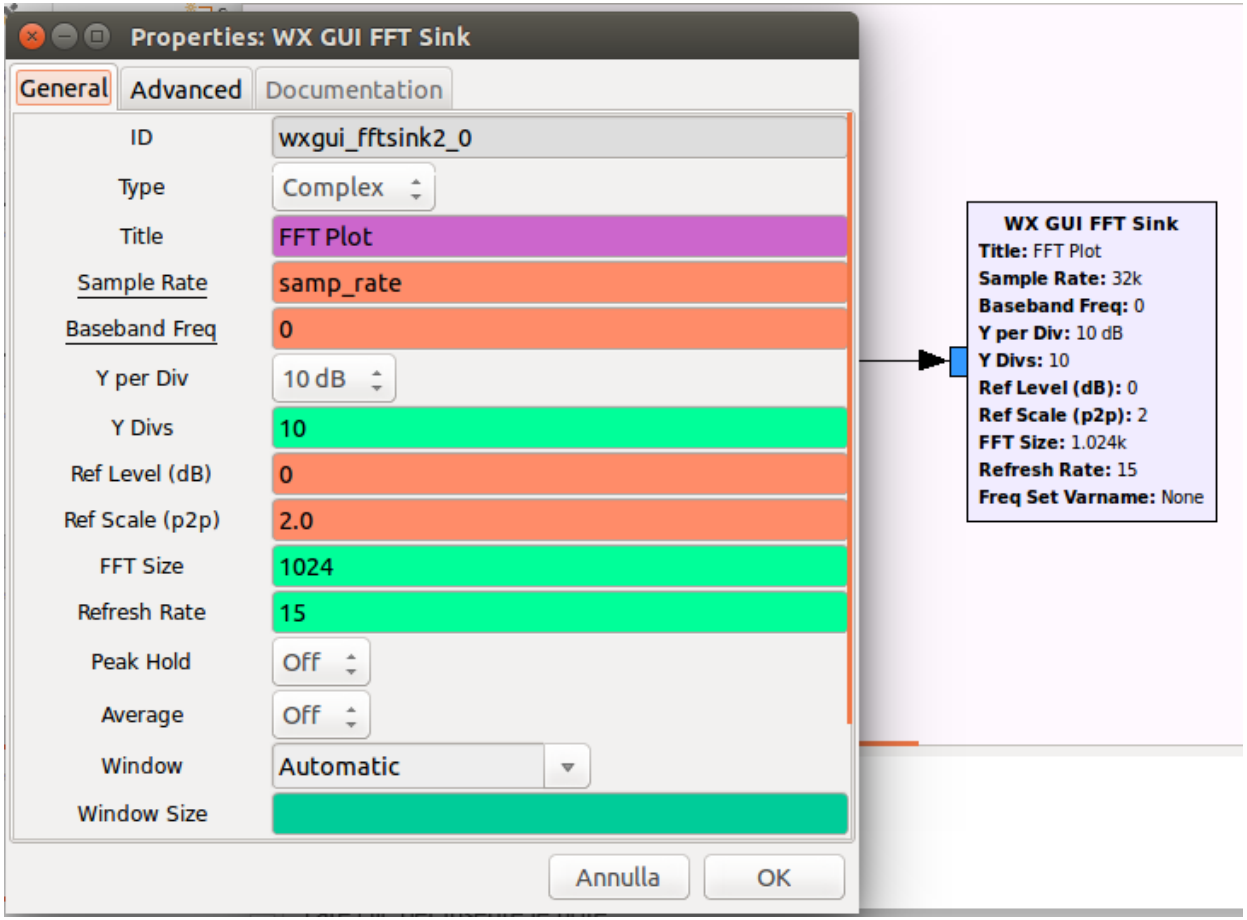
Exploring Radio Frequency communication

- RTL-SDR Source Block



Exploring Radio Frequency communication

- WX GUI FFT Sink Block



Agenda

- Module 3 – Attacking RF communications
  - Radio Frequency and EAC Systems
  - Exploring Radio Frequency communications in practice
  - Hands-on: receiving your first transmission
  - SIGINT with GNU Radio
  - Understanding RF communications security

Build a FM receiver

Fire up your 

Agenda

- Module 3 – Attacking RF communications
  - Radio Frequency and EAC Systems
  - Exploring Radio Frequency communications in practice
  - Hands-on: receiving your first transmission
  - SIGINT with GNU Radio
  - Understanding RF communications security

SIGINT with GNU Radio

- Define a methodology to study real world signals
- Three main steps

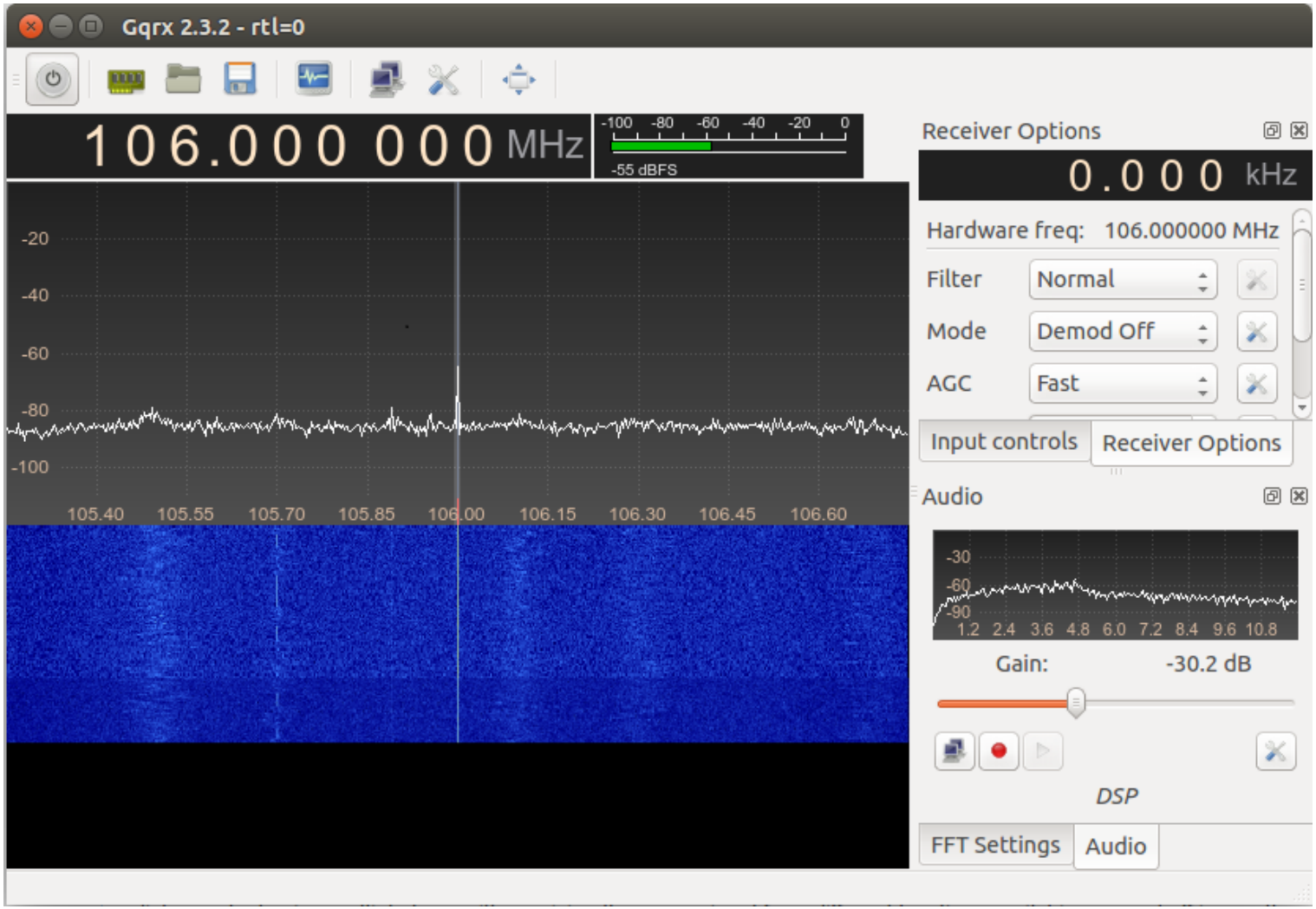
SIGINT with GNU Radio

- Define a methodology to study real world signals
- Three main steps

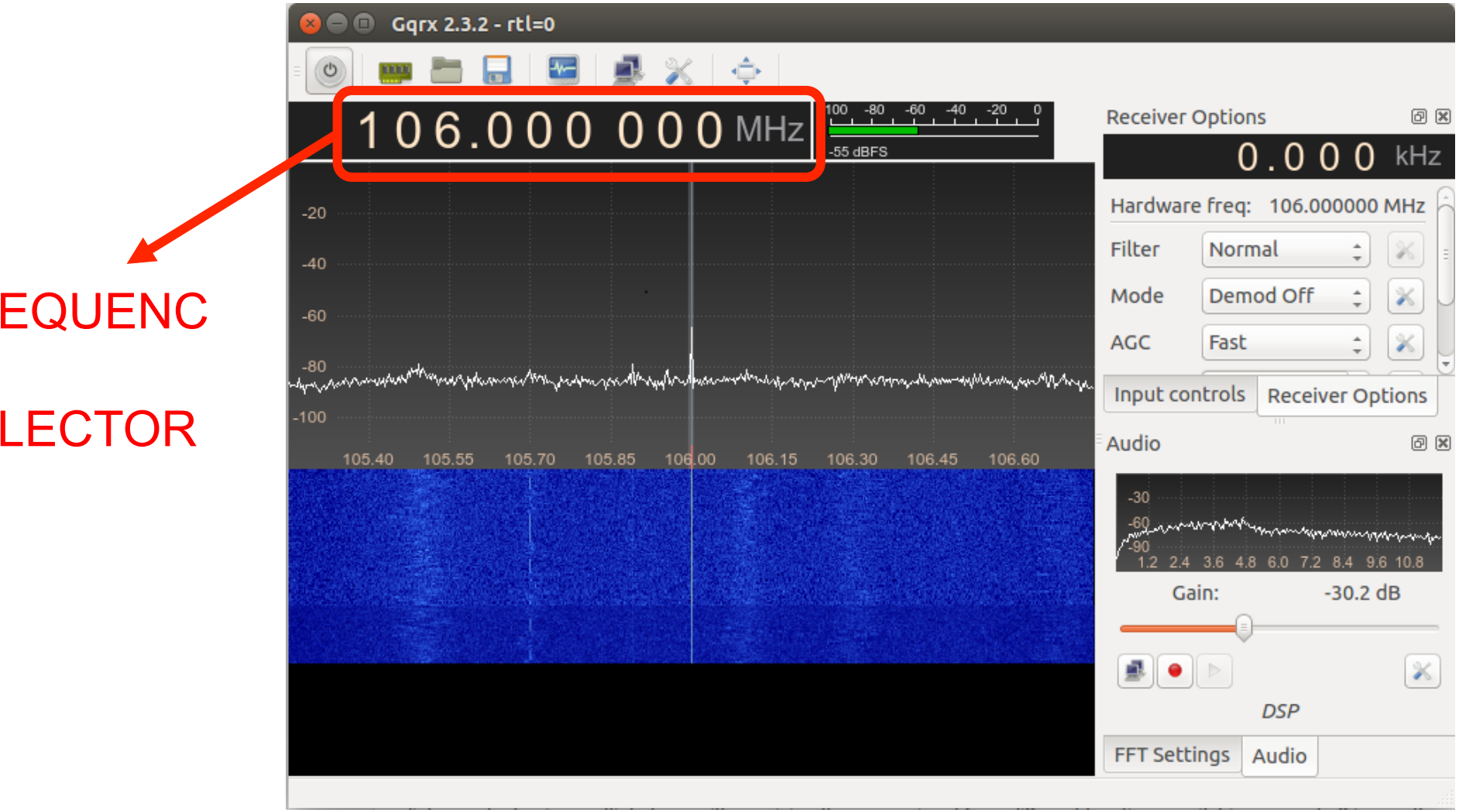
SIGINT with GNU Radio

- GQRX
  - SDR receiver and spectrum analyzer based on GNU Radio and QT Graphical toolkit
  - User-friendly interface
  - Supports RTL-SDR, HackRF, USRP and other SDR devices
  - Records signal to WAV file

SIGINT with GNU Radio

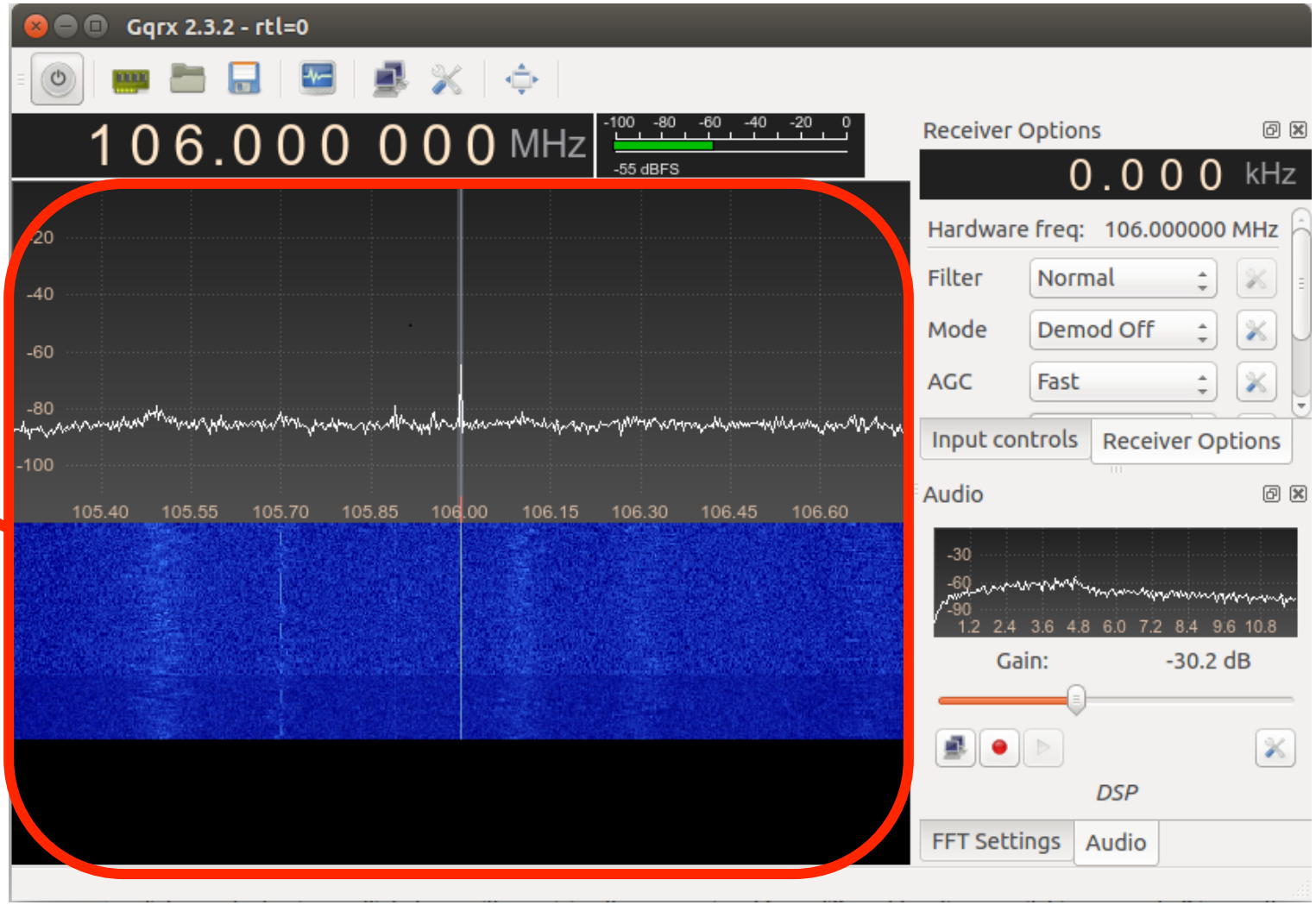


SIGINT with GNU Radio

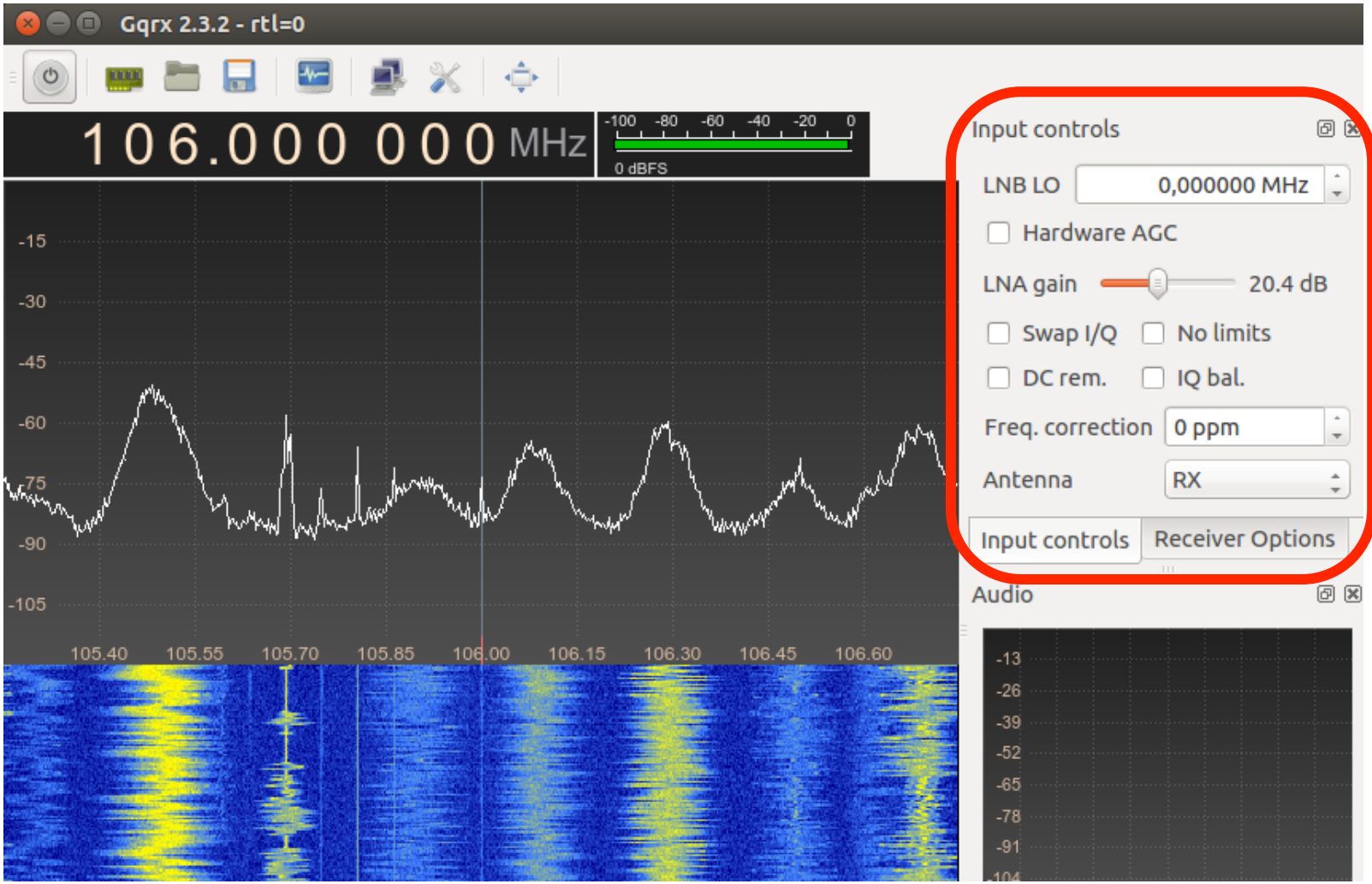


SIGINT with GNU Radio

EAL-TIME
PECTRUM

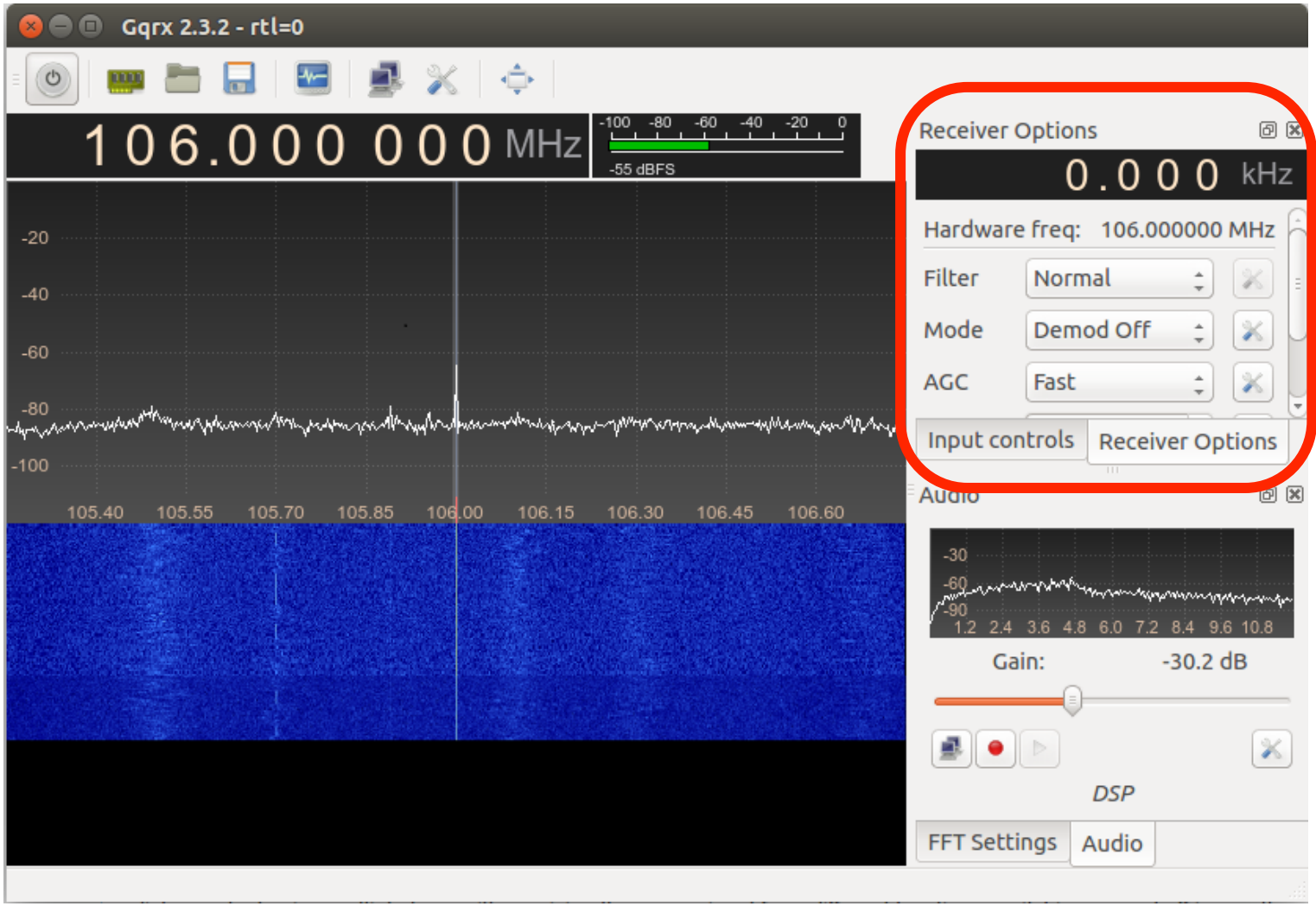


SIGINT with GNU Radio

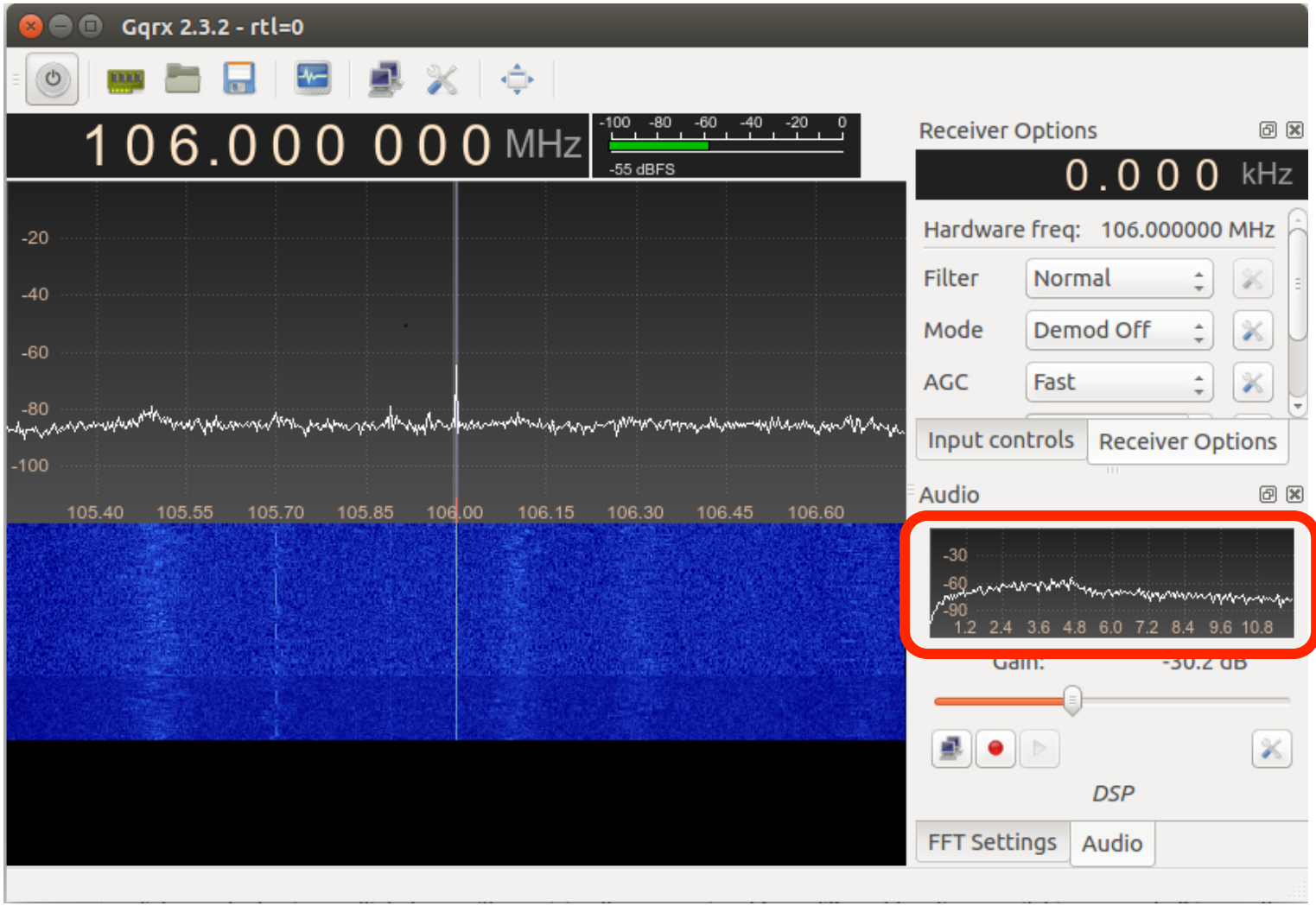


INPUT CONTROLS

SIGINT with GNU Radio

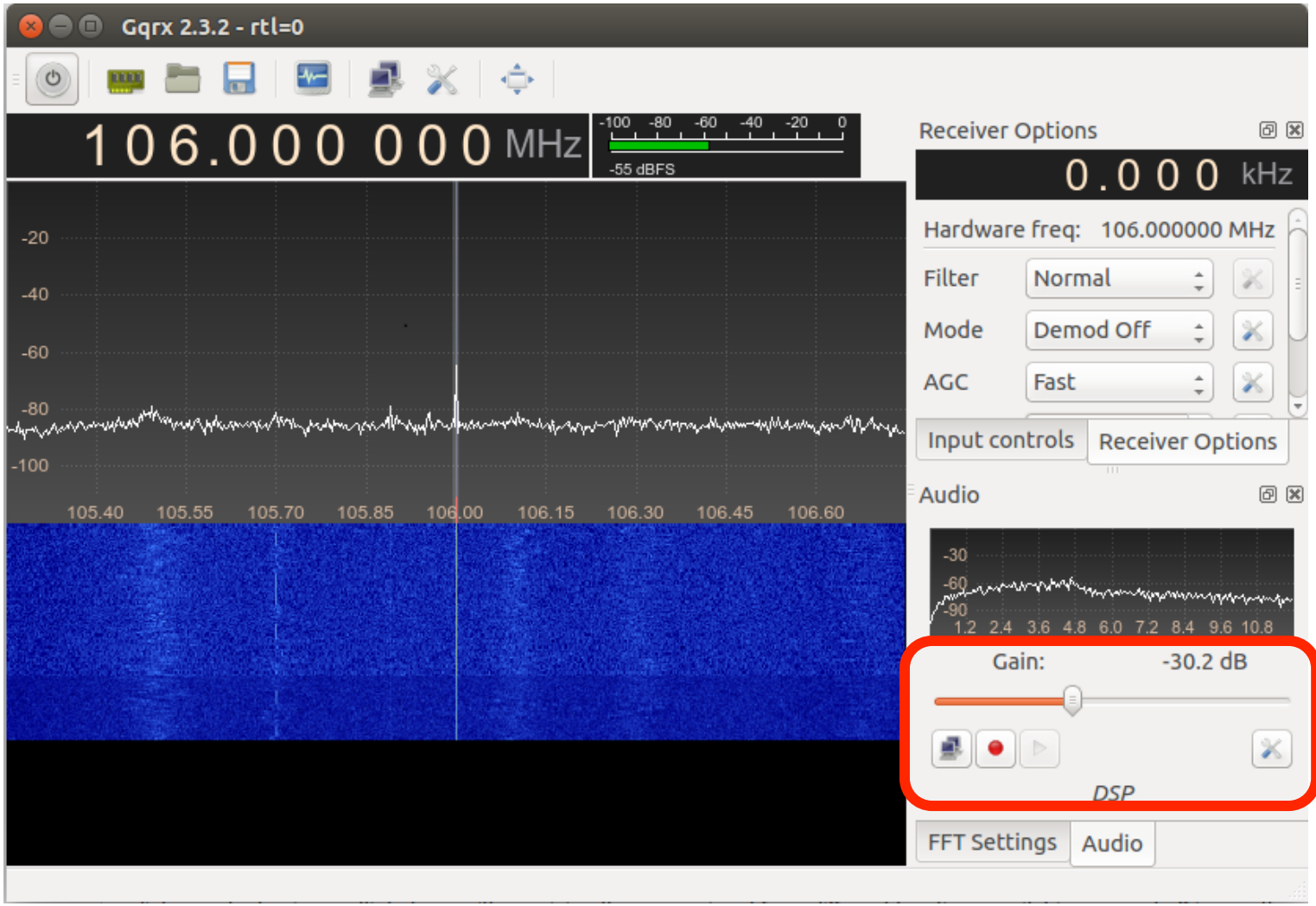


SIGINT with GNU Radio



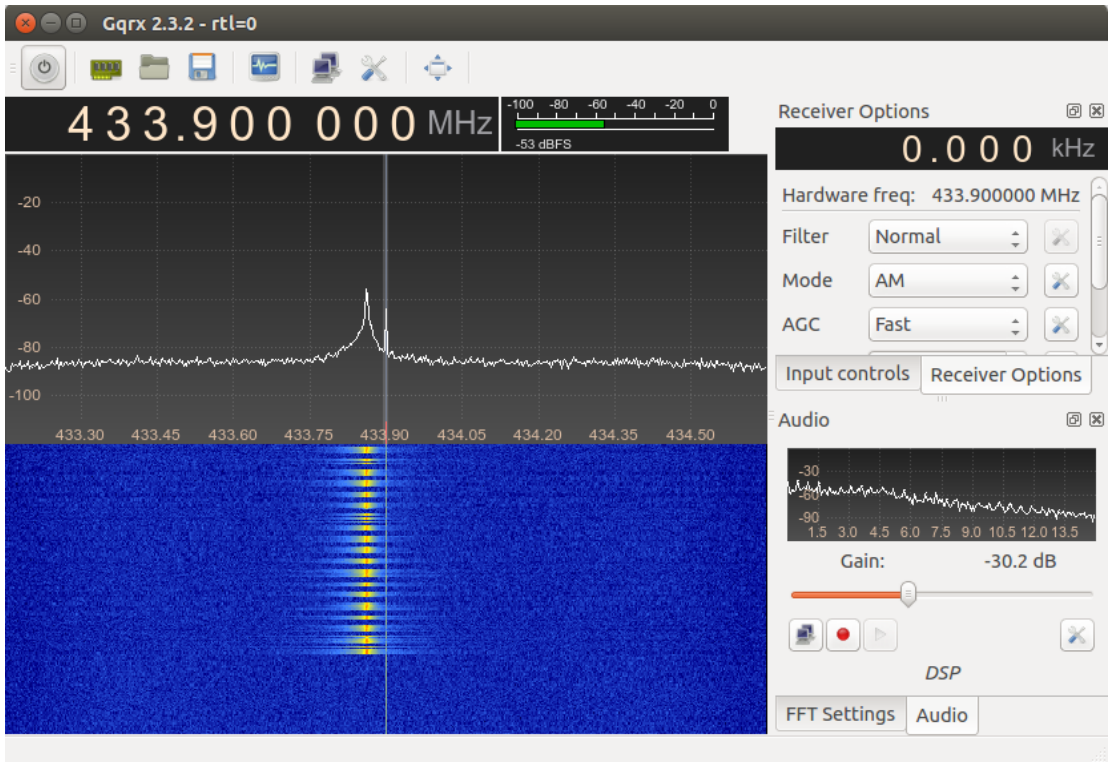
DEMODUL
D SPECTR

SIGINT with GNU Radio



SIGINT with GNU Radio

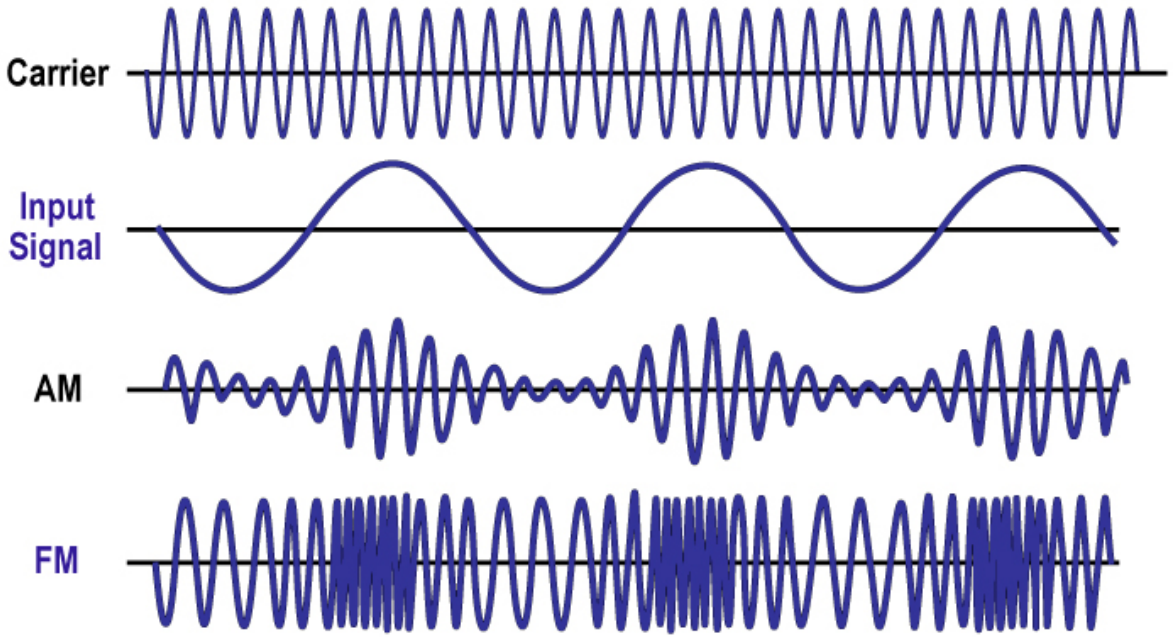
- Black-box interception of a RF signal
  - If the frequency is unknown, search power **peaks** in the spectrum



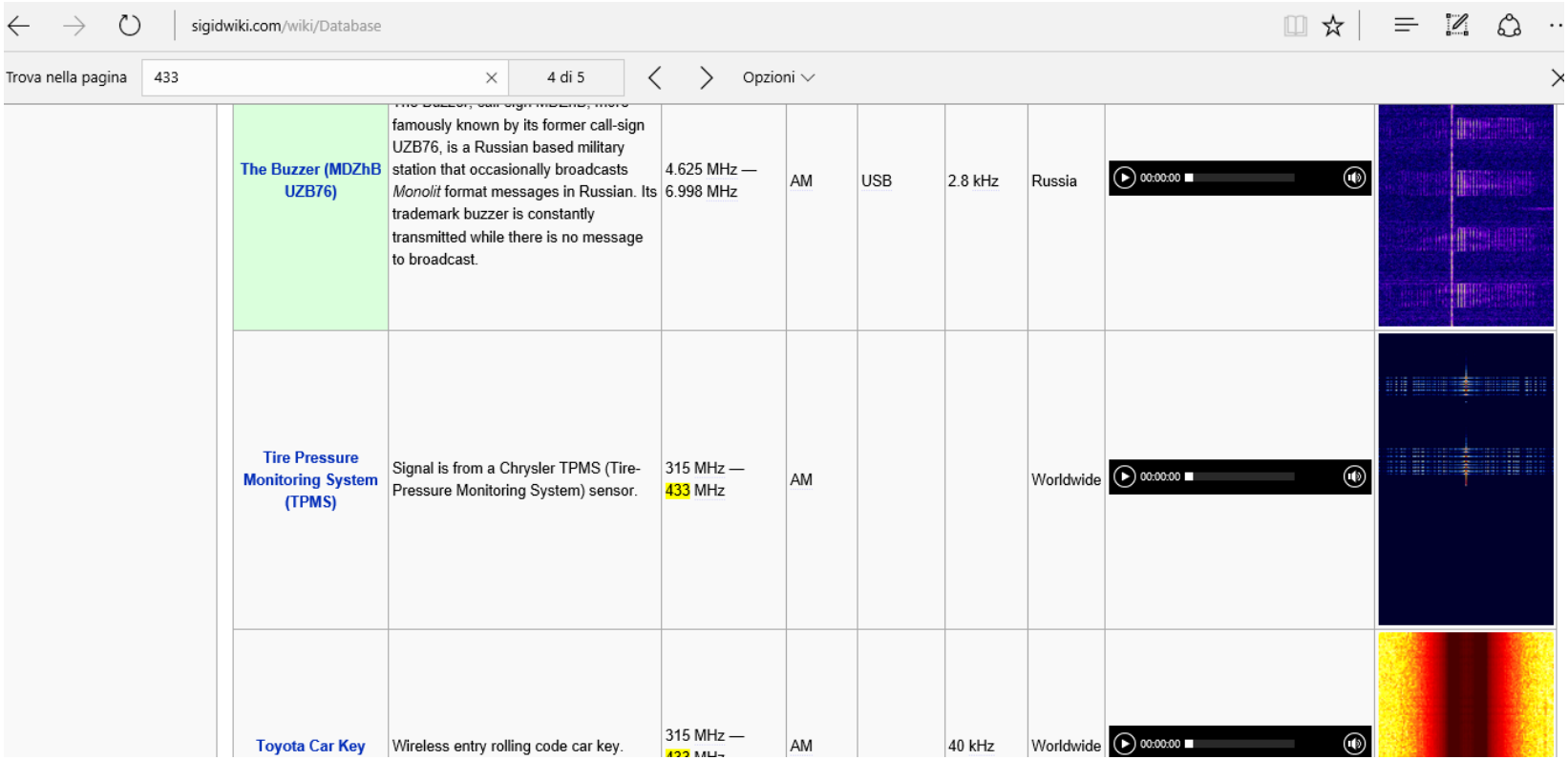
SIGINT with GNU Radio

- Define a methodology to study real world signals
- Three main steps

- Modulation
  - Impresses a waveform, called **carrier**, with another signal that contains data to be transmitted



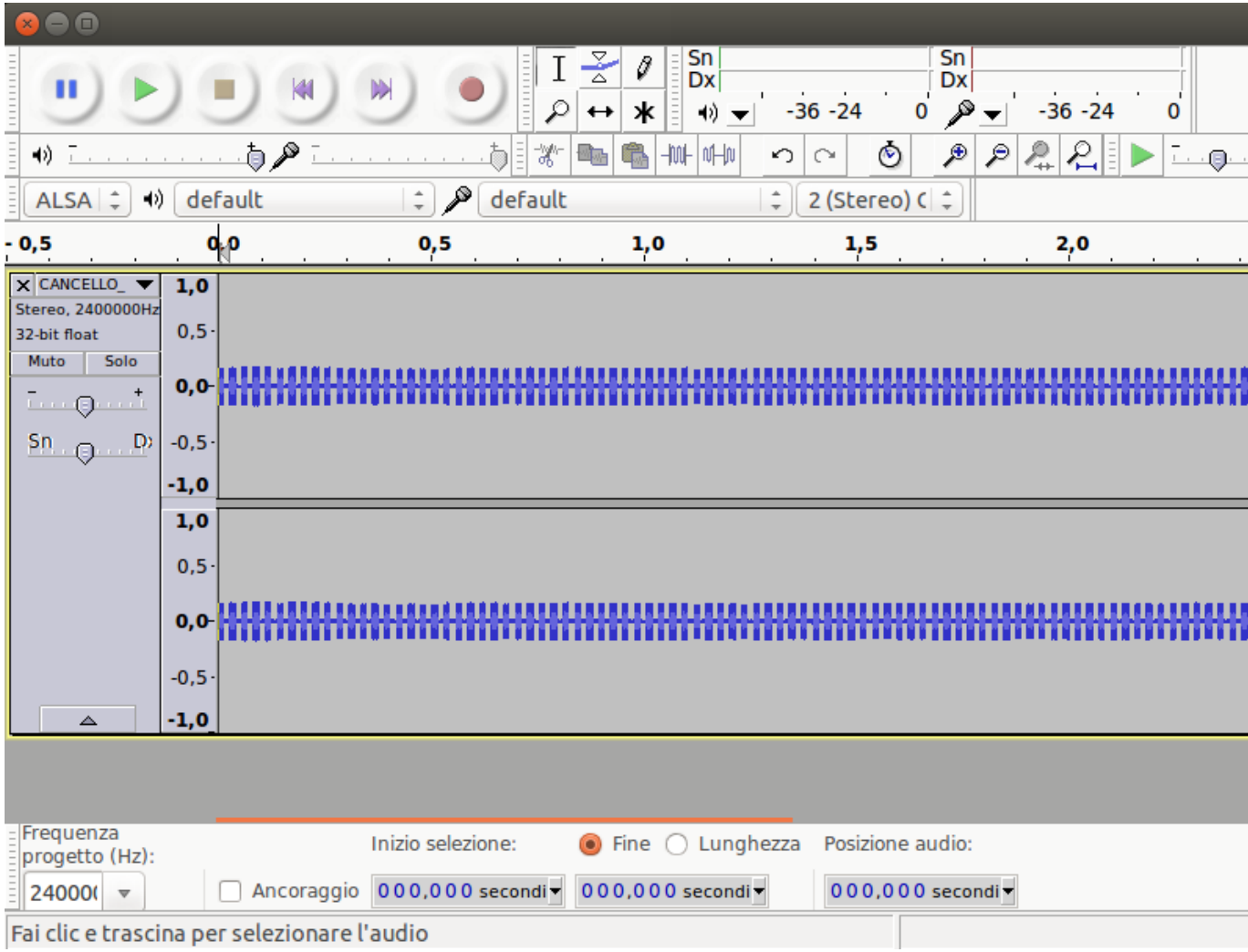
- Signal Identification Guide



The Buzzer (MDZhB UZB76)	famously known by its former call-sign UZB76, is a Russian based military station that occasionally broadcasts *Monolit* format messages in Russian. Its trademark buzzer is constantly transmitted while there is no message to broadcast.	4.625 MHz — 6.998 MHz	AM	USB	2.8 kHz	Russia	00:00:00	
Tire Pressure Monitoring System (TPMS)	Signal is from a Chrysler TPMS (Tire-Pressure Monitoring System) sensor.	315 MHz — 433 MHz	AM			Worldwide	00:00:00	
Toyota Car Key	Wireless entry rolling code car key.	315 MHz —	AM		40 kHz	Worldwide	00:00:00	

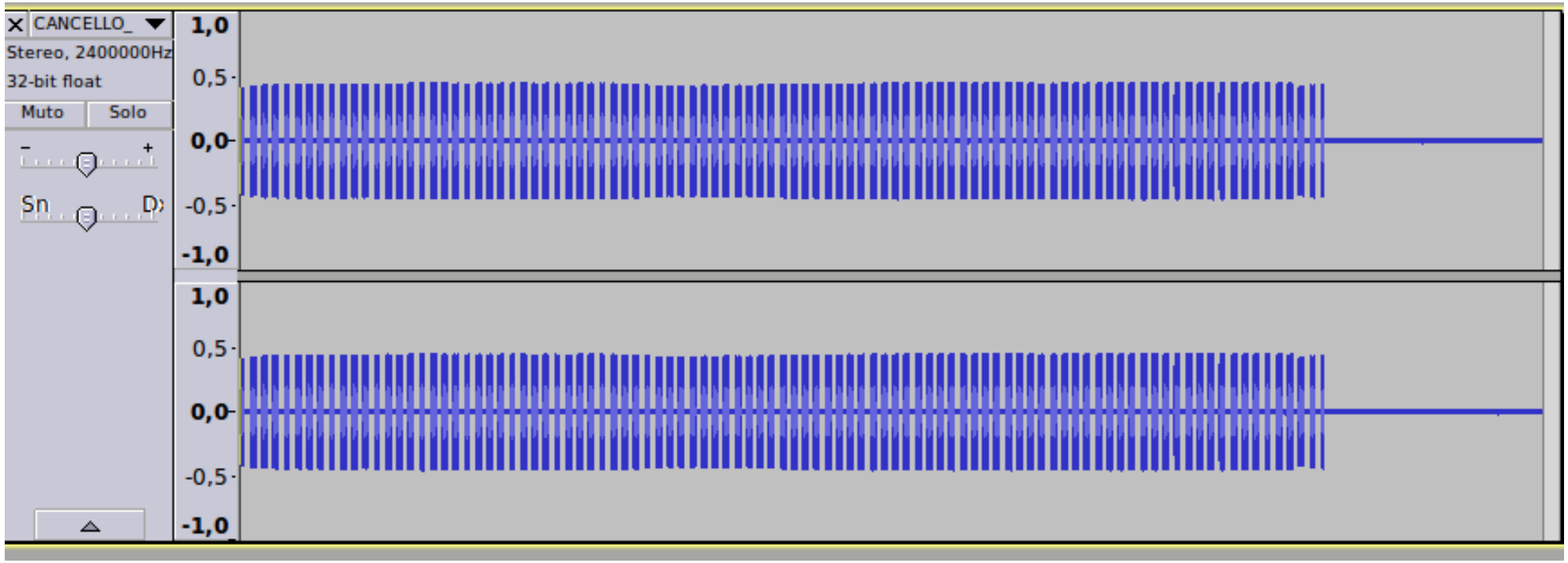
www.sigidwiki.com/wiki/Signal_Identification_Guide

- Audacity
  - Useful to study recorded signals
  - Support RAW data files used with USRP and HackRF utilities

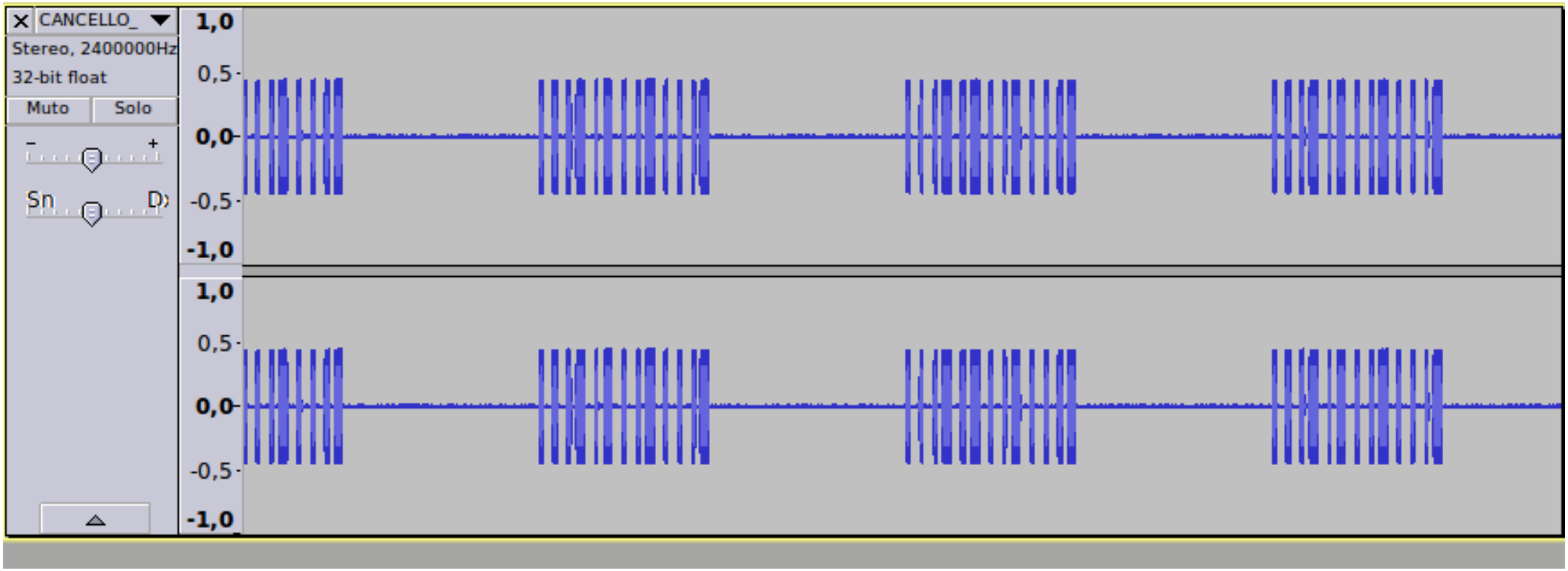


- Case Study: remote control at 433 MHz

- Case Study: remote control at 433 MHz



- Case Study: remote control at 433 MHz

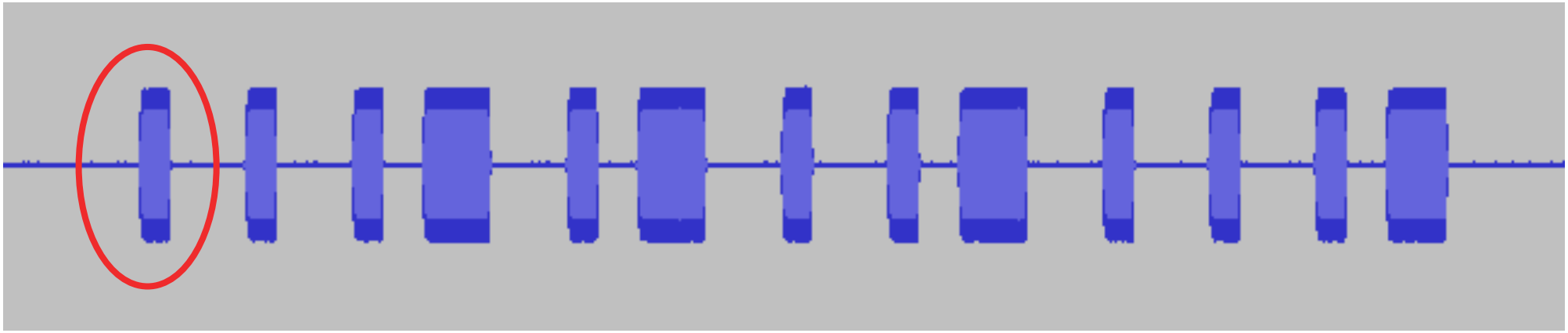


- Let's study the signal
  - Amplitude Modulation (AM)
  - Only two amplitude levels
    - Binary transmission using **On-Off Keying** (OOK) modulation
  - Repeated trains of pulses
    - Different lengths to encode the '0' and '1' bit

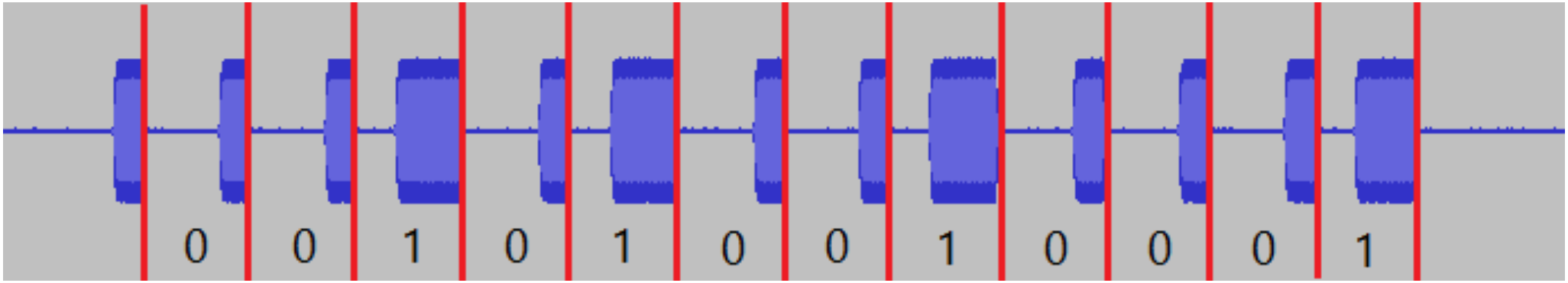
SIGINT with GNU Radio

- Define a methodology to study real world signals
- Three main steps

- Focus on a single train
  - The first pulse indicates the beginning of the “message”



- **Short** pulses represent binary ‘0’ while **long** pulses binary ‘1’



  - Transmitted message is **001010010001**

Agenda

- Module 3 – Attacking RF communications
  - Radio Frequency and EAC Systems
  - Exploring Radio Frequency communications in practice
  - Hands-on: receiving your first transmission
  - SIGINT with GNU Radio
  - Understanding RF communications security

- Case study's solution security
  - The remote control always sends same **fixed** code (!)
  - Malicious people can record and replay signals thus obtaining an unauthorized access
- Solution
  - Rolling code

- Rolling Code
  - Remote control always sends **different** codes
  - Sender and receiver are synchronized with an internal counter
  - An hardware algorithm calculates the ‘next’ code on the basis of the internal counter’s value
  - A widely used algorithm is **KeeLoq**
  - **Rolling code is NOT a unbreakable mechanism..**

Module 4 || the challenge

Agenda

- Module 4 – The challenge
  - Introducing the challenge
  - The awards ☺

Challenge introduction

You are now part of a Red Team, which has been engaged to breach the physical security of a high security facility controlled by a super secret, and “probably” evil, organization known as **h4k3rZ T34mZ**

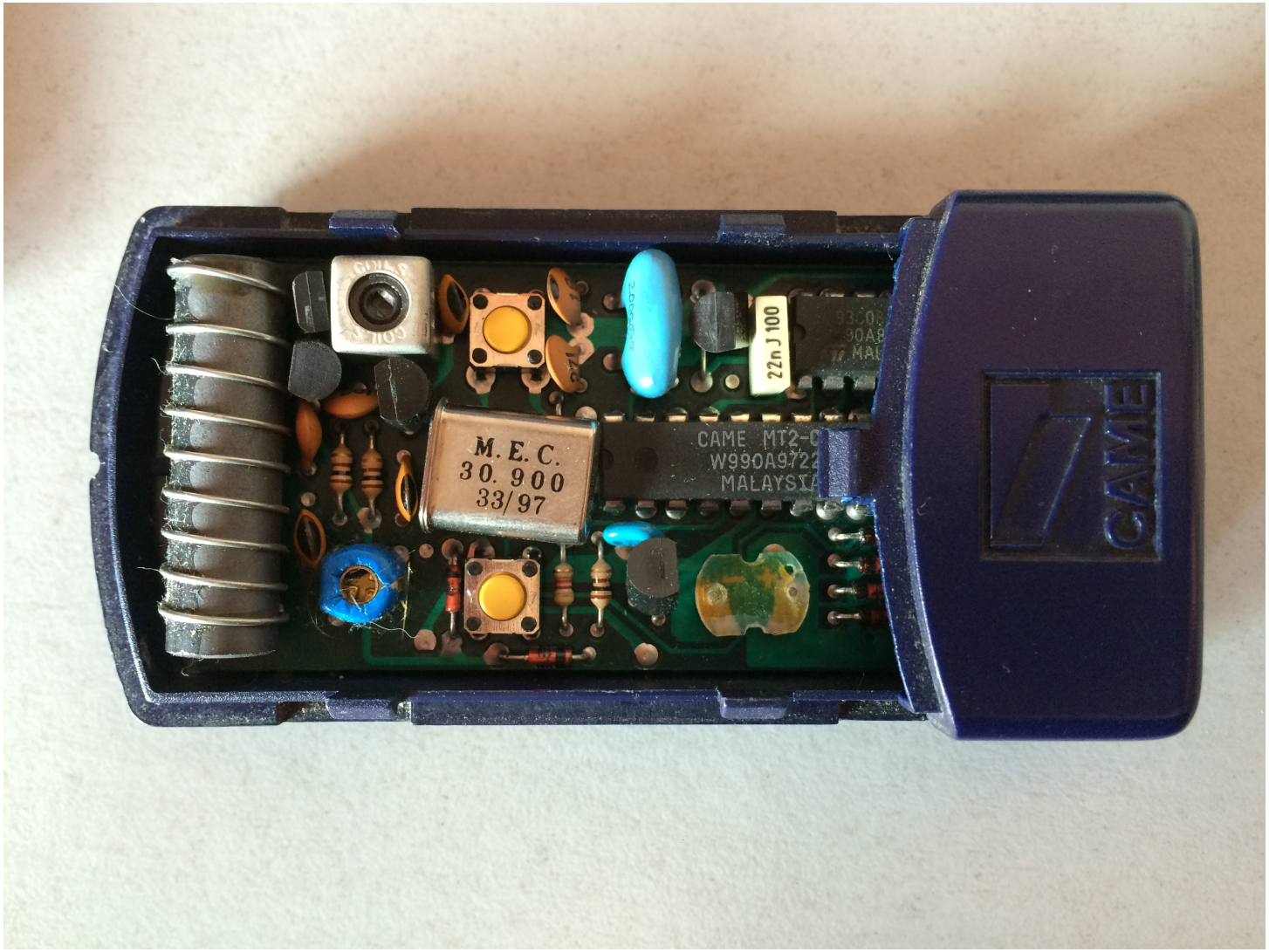
Your task is to open the external facility’s electric gate thus allow your team to enter the facility and proceed with the intrusion..

Hint?

You find one employee’s remote controller..

t seems to be broken and you can’t use it to open the gate but you
lecide to open it to see inside….

Hint?



OPPOSING FO

Agenda

- Module 4 – The challenge
  - Introducing the challenge
  - The awards ☺

Awards

The first two to complete the challenge will win a:

RTL-SDR Dongle from http://www.rtl-sdr.com

OPPOSING FO

Feedback and questions please..
Don’t be shy.. ;-D

OPPOSING FORCE

Thank you

Contacts – engage@opposingforce.it || www.opposingoforce.it || @_opposingforce

Start hack Access Control systems

e have **10 tool box** at the special price of **15 €** NOW!

- Each toolkit contains
  - Plastic box with Opposing Force sticker ☺
  - 1 HydraBus with its case
  - 1 HydraNFC
  - 1 Mini USB cable
  - 1 SDR-RTL dongle with its antenna
  - 1 Breaboard with some jumpers
  - 1 NFC MIFARE ULTRALIGHT card

OPPOSING FO