



Under Pressure

Raziel Einhorn
Inbar Raz

ARGUS
CYBER SECURITY

 @raziel_e / @inbarraz / @ArgusSec

#partnersincrime

*Inbar Raz
Concept & Full Setup*

*Ikea Standing Coat Rack
(don't ask...)*



*Shir Mousseri
Packet Analysis*

*Raziel Einhorn
Radio and DSP*

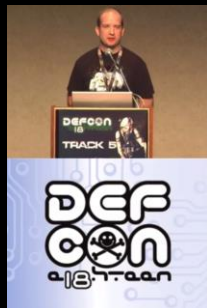
So, TPMS

Tire Pressure Monitoring System



- “An electronic system designed to monitor the air pressure inside the pneumatic tires on various types of vehicles” (Wikipedia)
- TPMS sensor reports in real-time to the driver of the vehicle, either via a gauge, a pictogram display, or a simple low-pressure warning light
- Mandatory in many countries for every new vehicle
- Many models; many suppliers; both by Auto manufacturers and aftermarket suppliers
- We’ll be talking about Direct TPMS technology

Already Researched Extensively



Letting the Air Out of Tire Pressure Monitoring Systems

Mike Metzger - Flexible Creations
mike@flexiblecreations.com



Christopher Flatley
James Pak
Thomas Vaccaro



TPMS Receiver Hacking

Major Qualifying Project completed in partial fulfillment of the Bachelor of Science degree at
Worcester Polytechnic Institute

Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study

Ishtiaq Rouf^a, Rob Miller^b, Hossen Mustafa^a, Travis Taylor^a, Sangho Oh^b

Wenyuan Xu^a, Marco Gruteser^b, Wade Trappe^b, Ivan Seskar^b

^a Dept. of CSE, Univ. of South Carolina, Columbia, SC USA

{rouf, mustafah, taylor9, wyxu}@cse.sc.edu

^b WINLAB, Rutgers Univ., Piscataway, NJ USA
{rdmiller, sangho, gruteser, trappe, seskar}@winlab.rutgers.edu

February 6, 2010

Deemed Mostly Harmless

“This can set off an alarm in the car and possibly cause someone to pull over. More alarmingly, they discuss how tractors have automatic tire inflation systems which work using similar sensors. A false low pressure reading could cause the tractor tires to over inflate and be damaged.”

“Though the study concedes that the potential for danger is very small, it also points to the inherent vulnerability in secure software development for new automobiles..”

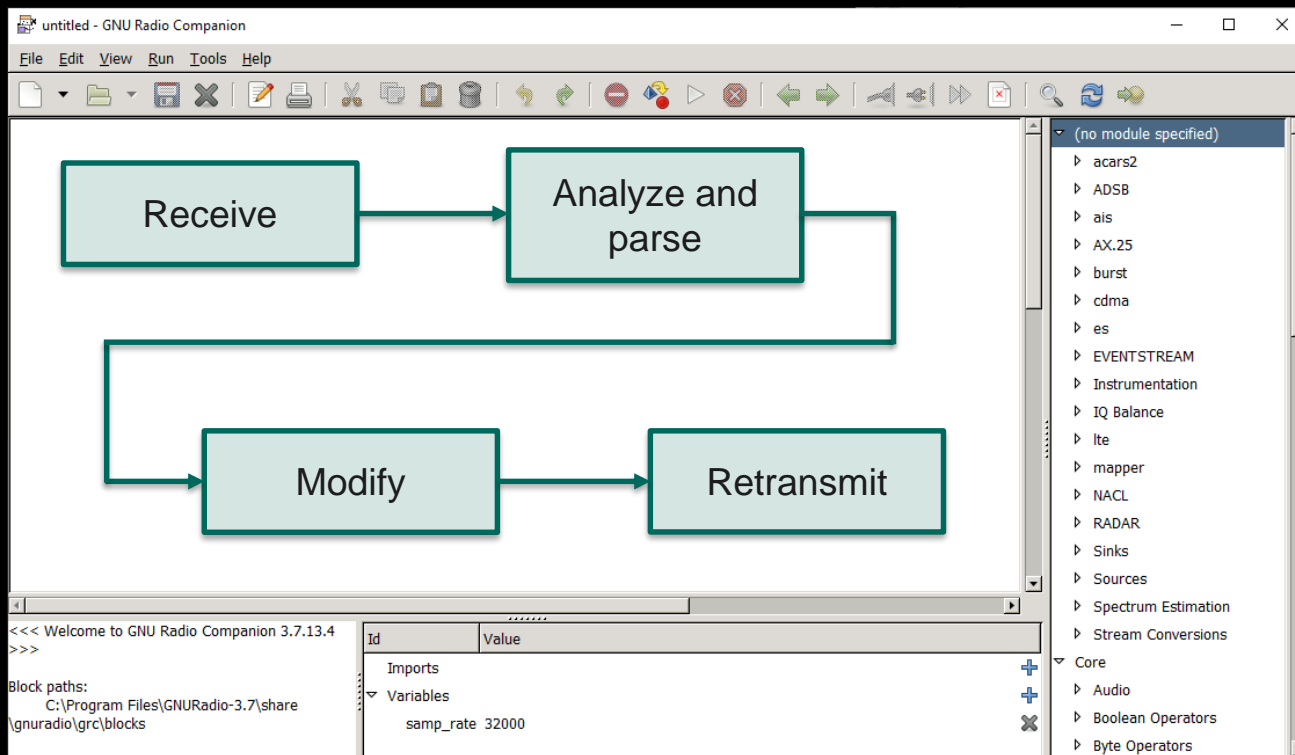




MCL Cinema, Hong Kong



The Plan: One Vehicle



The Plan: One Vehicle

The objective is to decode data



WPI

TPMS Receiver Hacking

Table 3 Packet Structure for Personal Car TPMS Sensor and Example Data.

Trial	Preamble	ID	Temperature (F)	Pressure (kPa)	Flags	CRC
Packet in Binary	1110 0000 0	1000 1000 0111 1100 0110 1001 1111 1001	0101 1010	1111 0000	1111 1000	0101 1100
Packet Values	N/A	887C69F9	90	240	F8	5C

Alexander Arnold _____

Stephanie Piscitelli _____

TIRE PRESSURE SENSOR - MQP AW1 - CAR1

March 16, 2015 - September 11, 2015

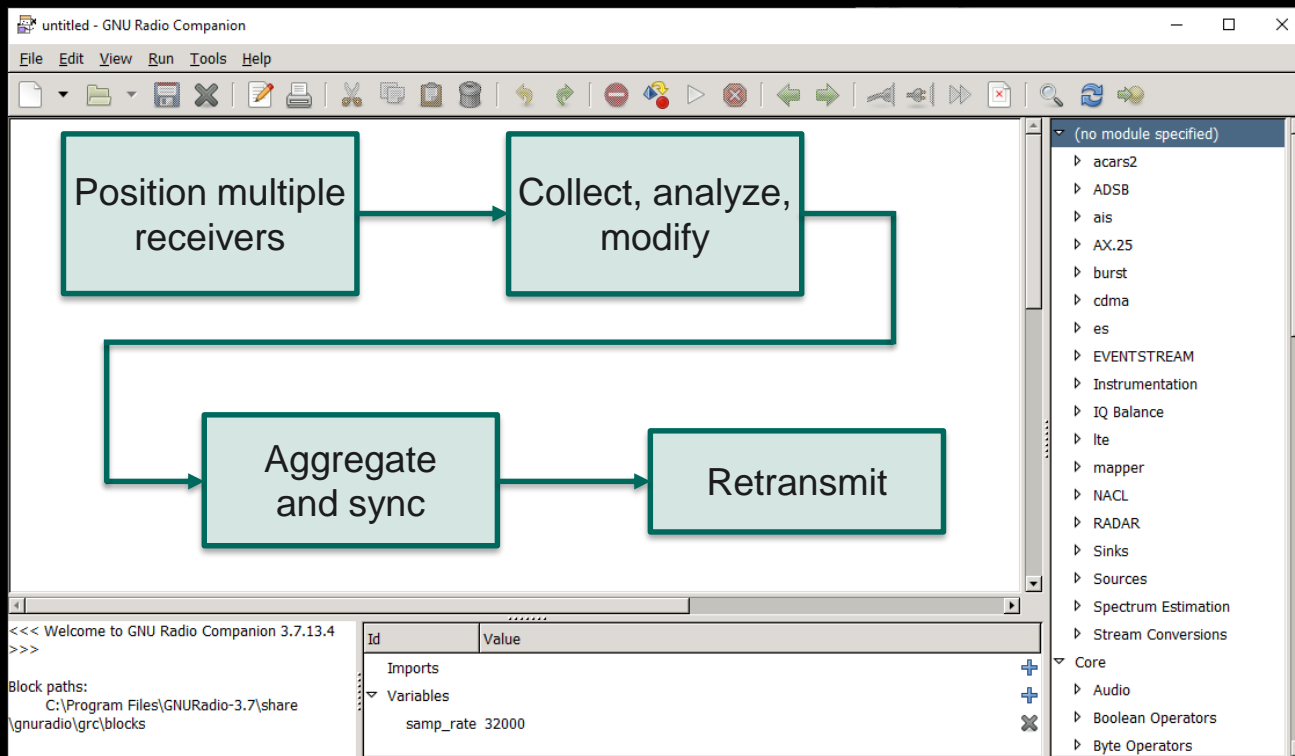
The Plan: Scaling Up

The screenshot displays the GNU Radio Companion (GRC) interface. The main workspace contains a flow diagram with two blocks: "Highway Traffic Capture" on the left and "Analyze & Parse" on the right, connected by a green arrow pointing from left to right. The right sidebar shows a list of modules under the heading "(no module specified)". The bottom panel is split into two sections: the left section shows the "Block paths:" section with the path "C:\Program Files\GNURadio-3.7\share\gnuradio\grc\blocks", and the right section shows a table of variables.

Id	Value
Imports	
Variables	
samp_rate	32000

- acars2
- ADSB
- ais
- AX.25
- burst
- cdma
- es
- EVENTSTREAM
- Instrumentation
- IQ Balance
- lte
- mapper
- NACL
- RADAR
- Sinks
- Sources
- Spectrum Estimation
- Stream Conversions
- Core
 - Audio
 - Boolean Operators
 - Byte Operators

The Plan: Scaled Up



Attack scenario



Status Report

S U C C E S S
F A I L U R E



L₁

E₁

A₁

R₁

N₁

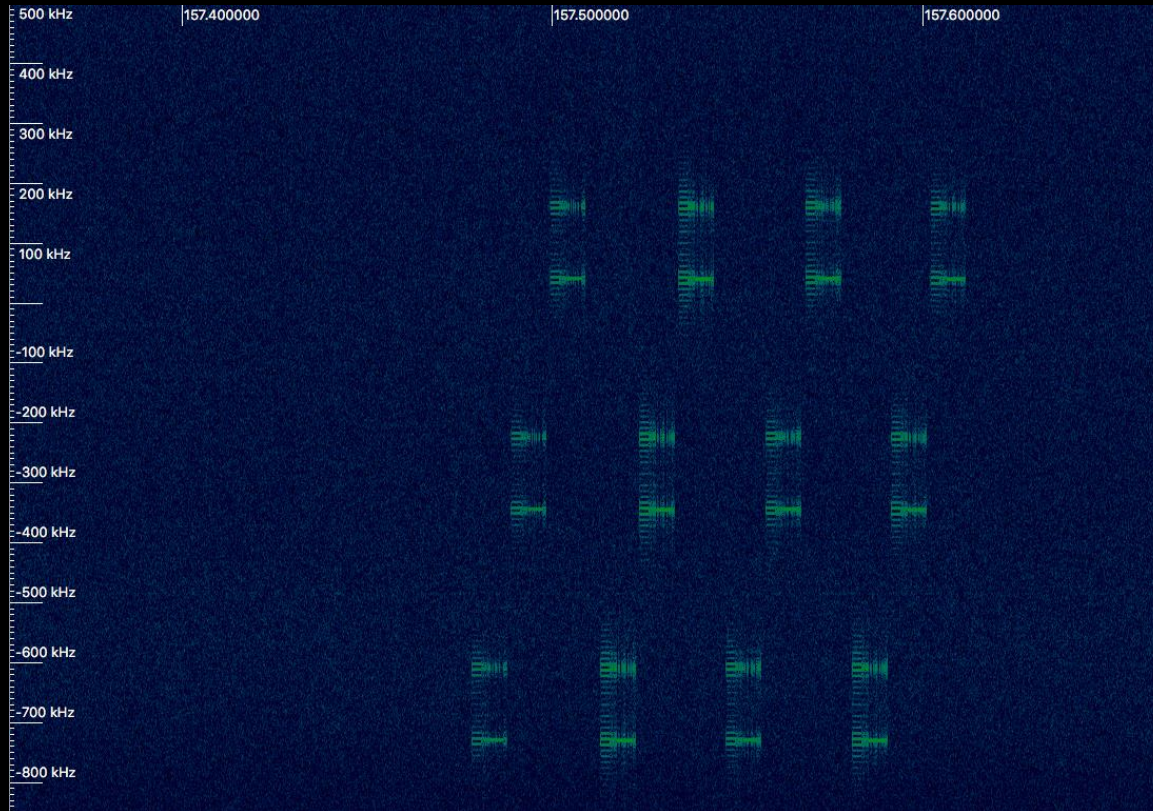


WE SHOUTED OUT ABOUT
SOME NEW INVENTION &
THEN THAT THING HIT HIM!

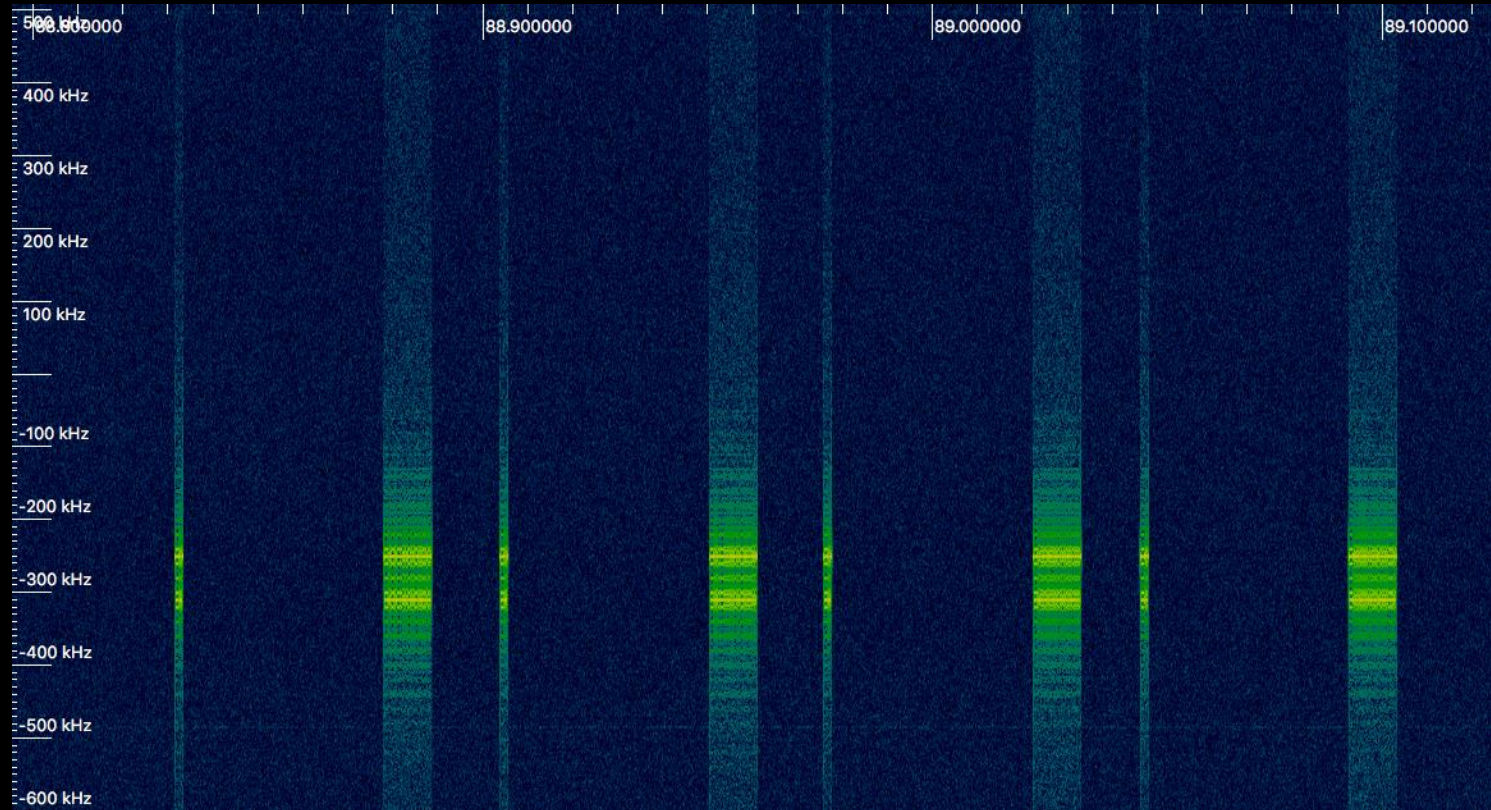


**Things
We've
Learned**

Look For The Signal! Is That It?



Perhaps This One?



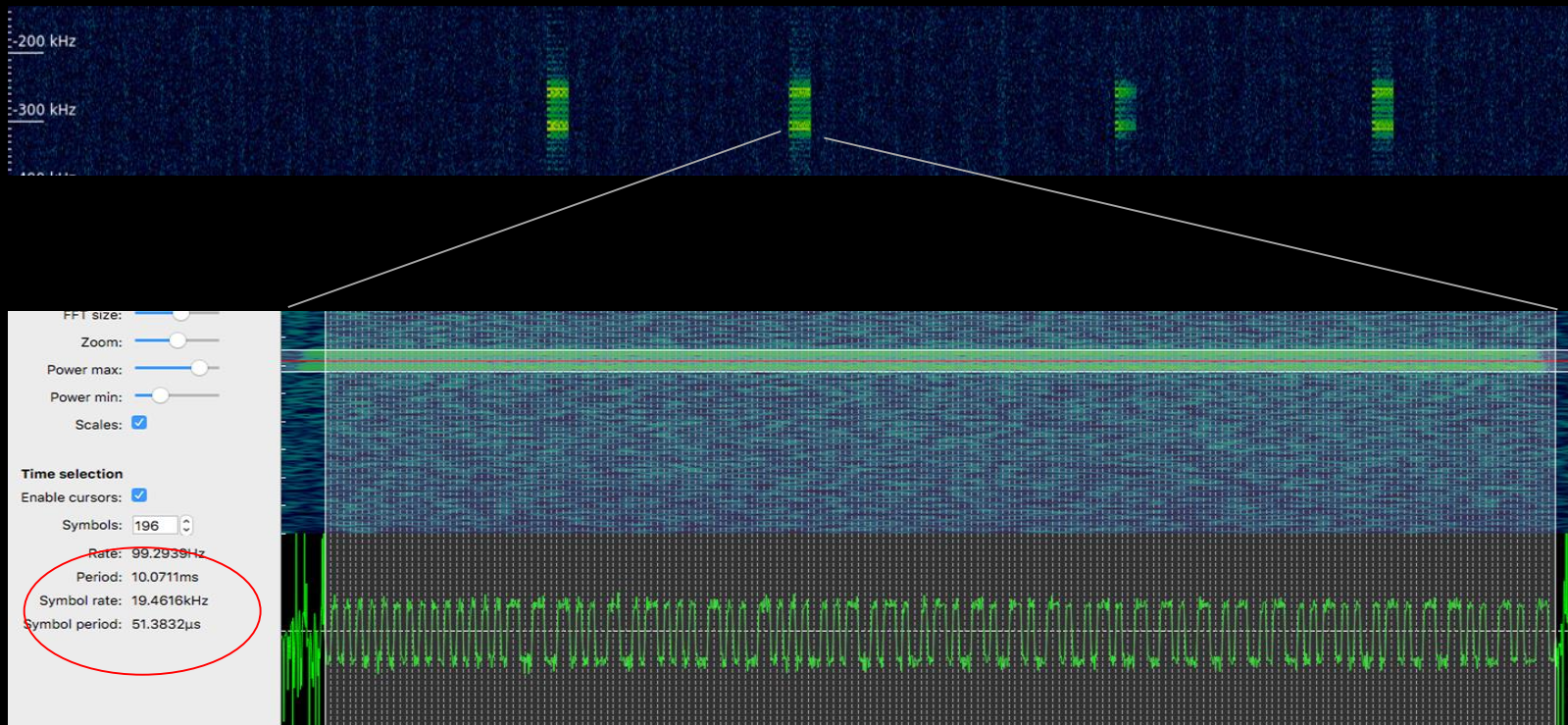
Hard To Get a Good Signal. Wonder Why..



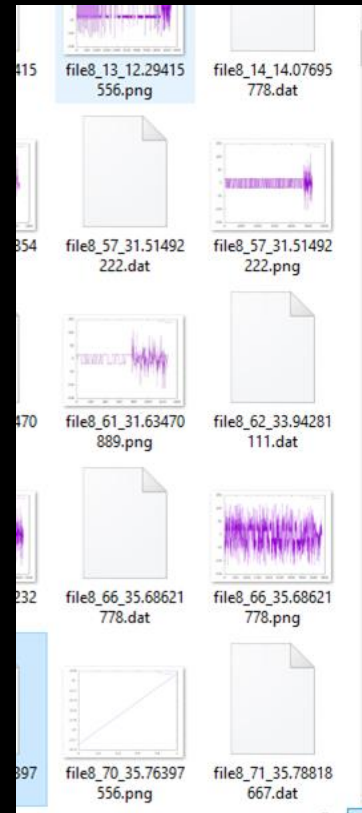
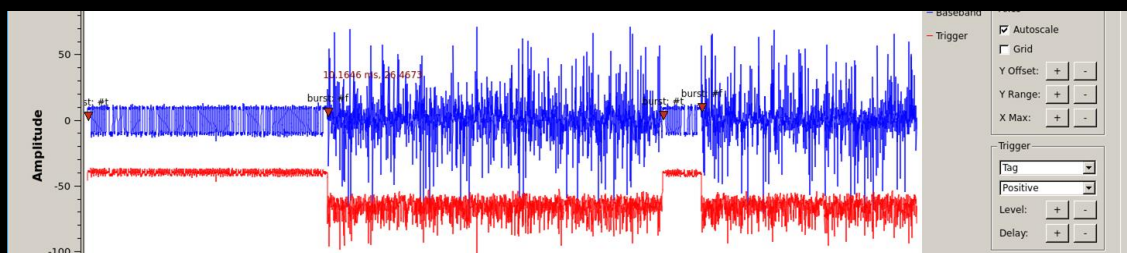
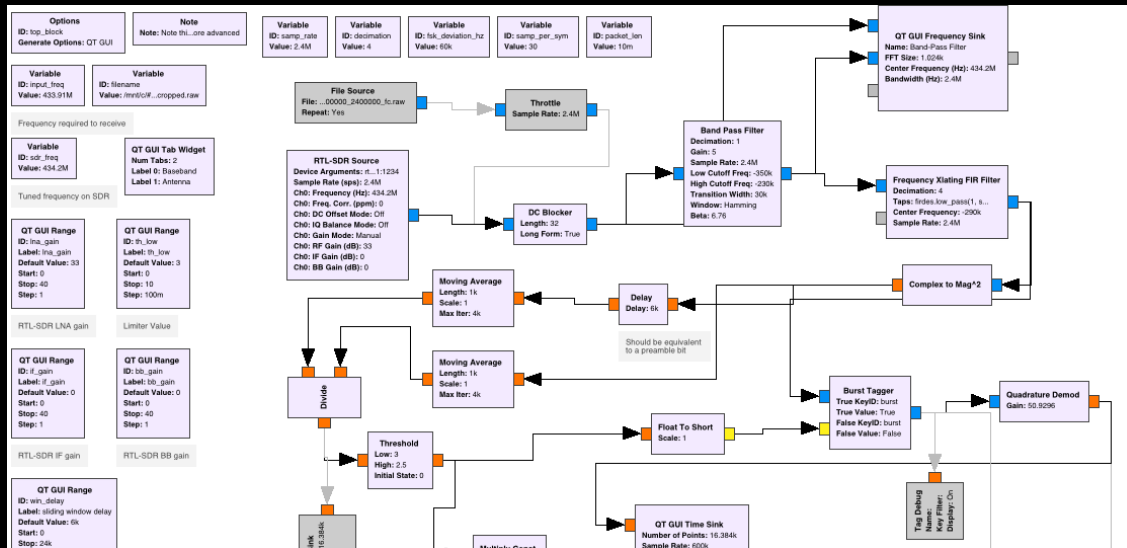
Find the target (like, physically)



There it is!



Collect multiple packets for analysis



Packet Statistical Analysis

Find Tire ID

```
$ ./find_device_id.sh /mnt/c/\#_Record_Files/tpms_records/all_signals_manchester_decoded_ext_preamble.txt 32 96
Range 24:56
c1e721bc 3253150140 1100000111110011100100001101111100: 5 *****
c221d992 3256998290 11000010001000011101100110010010: 13 *****
c23bbcad 3258694829 11000010001110111011110010101101: 23 *****
c23bbcd6 3258694870 11000010001110111011110011010110: 42 *****
```

Find CRC Parameters

```
$ cat /mnt/c/ExClonRepos/bruteforce-crc/out.txt
Polynomial, Initial, Final XOR, Reflected Input, Reflected Output
0x7,0xcb,0x0,false,false
```

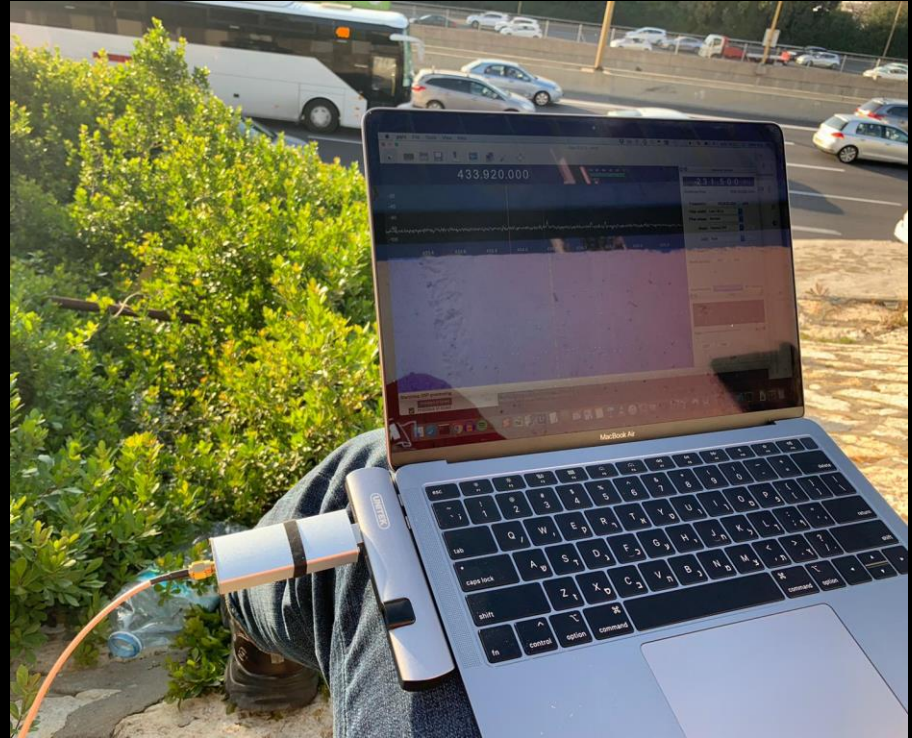
Improving Our Setup: Receiving Multiple Packets

```
n 1:python 2:...epos/tpms/src
```

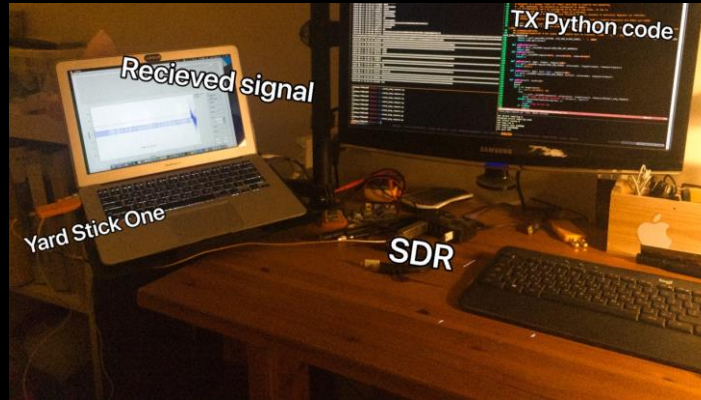
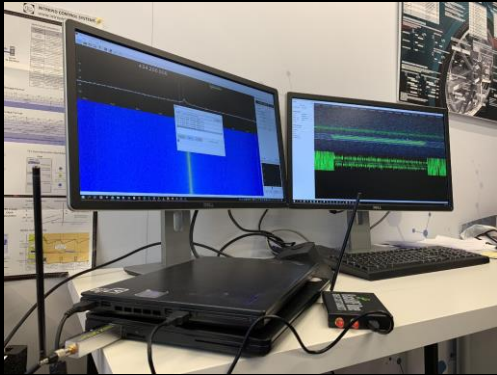
| 24:1.2

```
root@kali:~/Raz0161-PC in /mnt/c/Raz0Apps/IPMS/gnc on git:master [23:00:20]  
python tpms_file_analyze.py | grep -v "XXXXXXXX"
```


Theory Vs. Reality



Spoofing The Signal



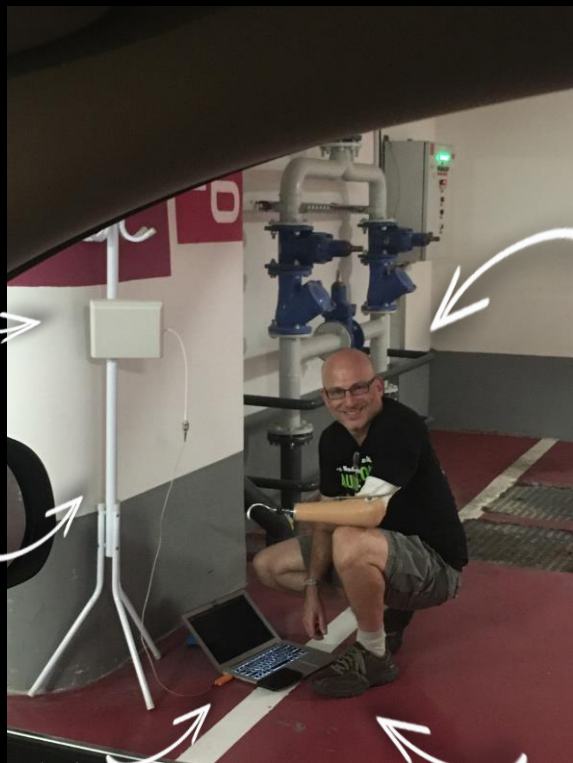
Don't underestimate the value of a lab bench setup...

Experimenting with the transmitter setup

*Directional
Antenna
433Mhz*

*Standing
Coat Rack*

Yard Stick One



Researcher A

*Researcher B's
Laptop*

Experimenting with the transmitter setup



Distance measurement results

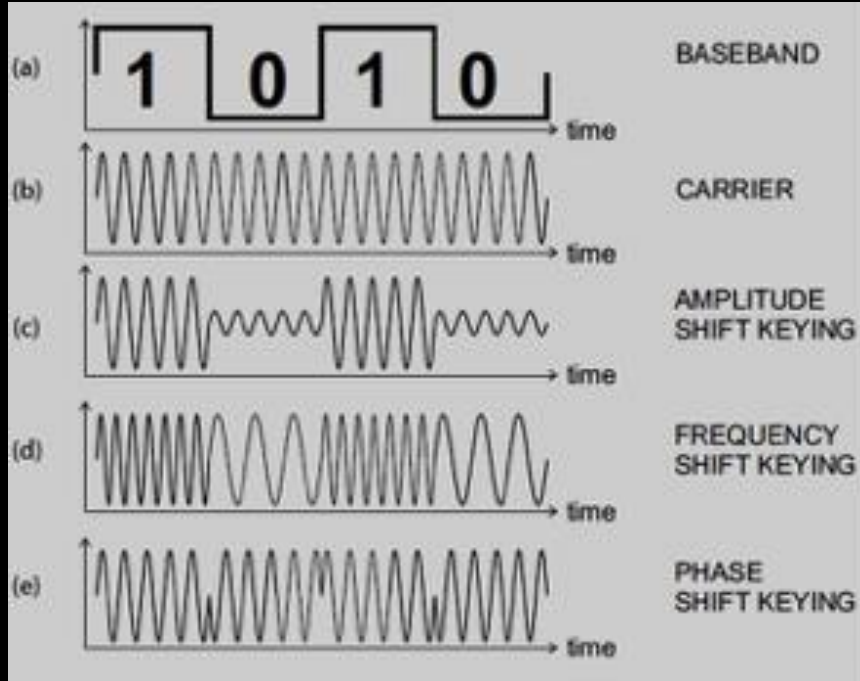
- Managed to receive TPMS transmissions from highway shoulders
- Succeeded in spoofing a vehicle from > 30 meters (approx. 6 lanes!)
- Succeeded stripping a TPMS transmission, rebuilding it and spoofing the vehicle

Backend setup

- Multiple field-deployed Raspberry-Pi devices, with a receiving SDR and an Internet connection
- All devices send the collected data to the processing station
- Implementation used a simple VPN – completely scalable setup

**What's
Next?**

Challenges



- Multiple modulation and encoding methods

Image: ResearchGate/Harpreet Kaur Channi

Challenges



- Multiple modulation and encoding methods
- Multiple vendors and packet formats

Challenges



- Multiple modulation and encoding methods
- Multiple vendors and packet formats
- Signal synchronization

Mitigation

Mitigation

- Encrypt the transmission



Mitigation



- Encrypt the transmission
- Polling-only operation

Mitigation



- Encrypt the transmission
- Polling-only operation
- Correlate with other sensors

**But the easiest
and most
important
mitigation...**



Keep your
eyes on the road

...LIVES DEPEND ON IT

An
Important
Message

It's doable

Where there's a way There's malice

Richard Pietravalle

Scale Matters

FAILURE

Is also a step forward!

Thank you!
Questions?

ARGUS
CYBER SECURITY

 @raziel_e / @inbarraz / @ArgusSec