The unfortunate journey of radio-protocol mistakes

Marco Balduzzi (@embyte)
Trend Micro Research
7th September 2021

Ignorantia securitatis neminem excusat

Hardware Epoch

Hardware Epoch

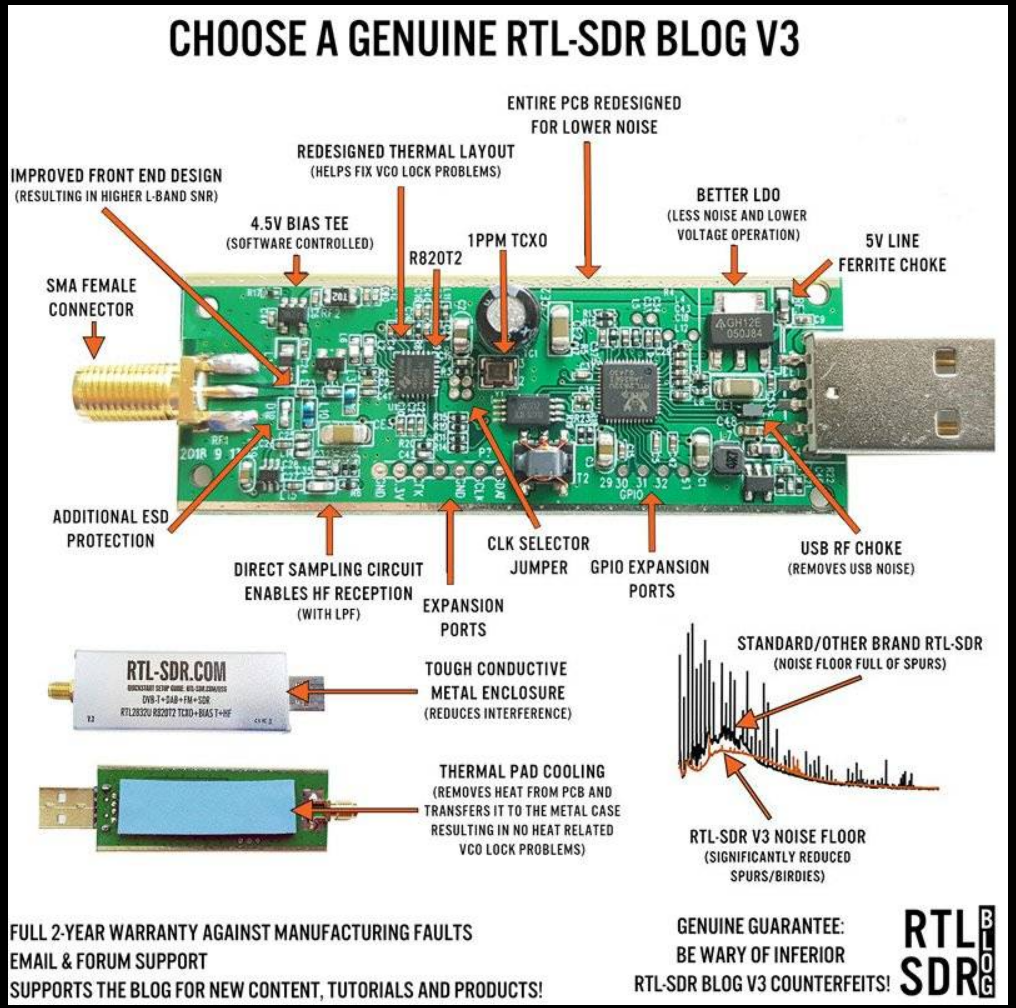
- Standalone systems
- Low-computational power
- “Security through obscurity” paradigm
- Hacking was difficult and cost expensive

Software Defined Radios (SDRs)

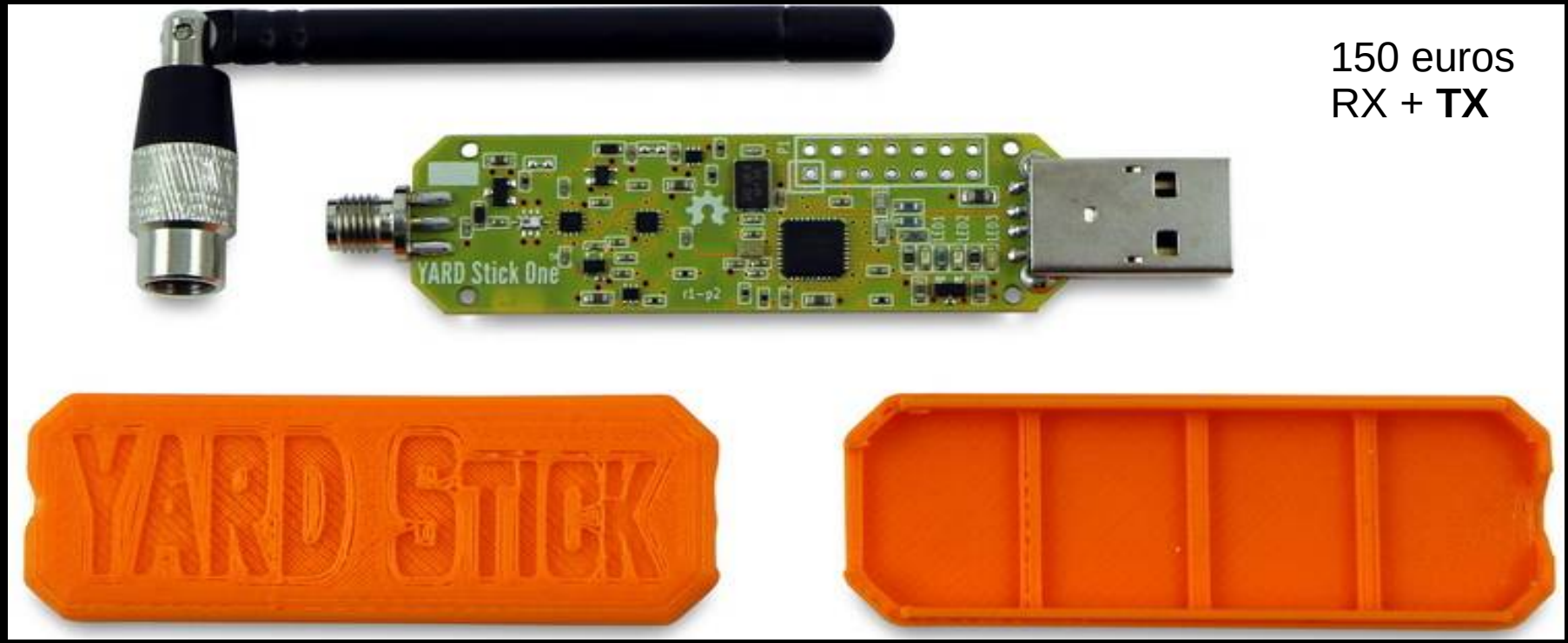
- Reduced costs
- Reduced complexity
- Increased flexibility

- Accessible by many, criminals included!

- Originally, distributed as TV receiver (RX only)
- Works well in the general RF spectrum, general recognizance
- Frequency Range: 500 kHz – 1766 MHz
- 25 euros

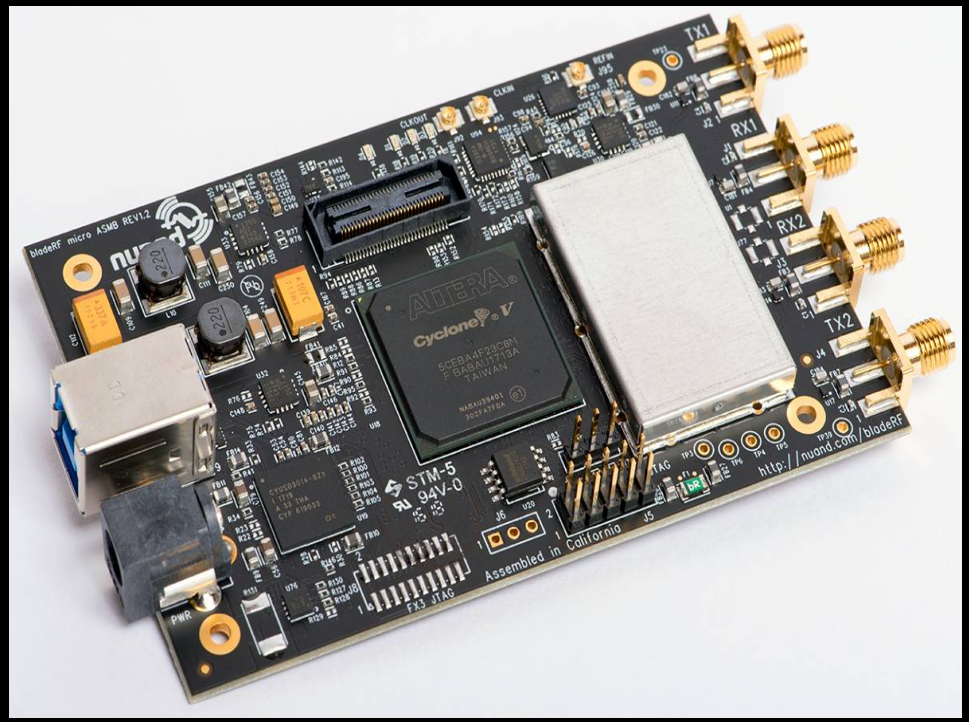


Bidirectional Transmissions



150 euros
RX + **TX**

- BladeRF 2.0 by Nuand
- 47 MHz to 6 GHz frequency range
- 2x2 MIMO, 61.44 MHz sampling rate
- 56 MHz bandwidth
- Automatic gain control, IQ/DC offset correction



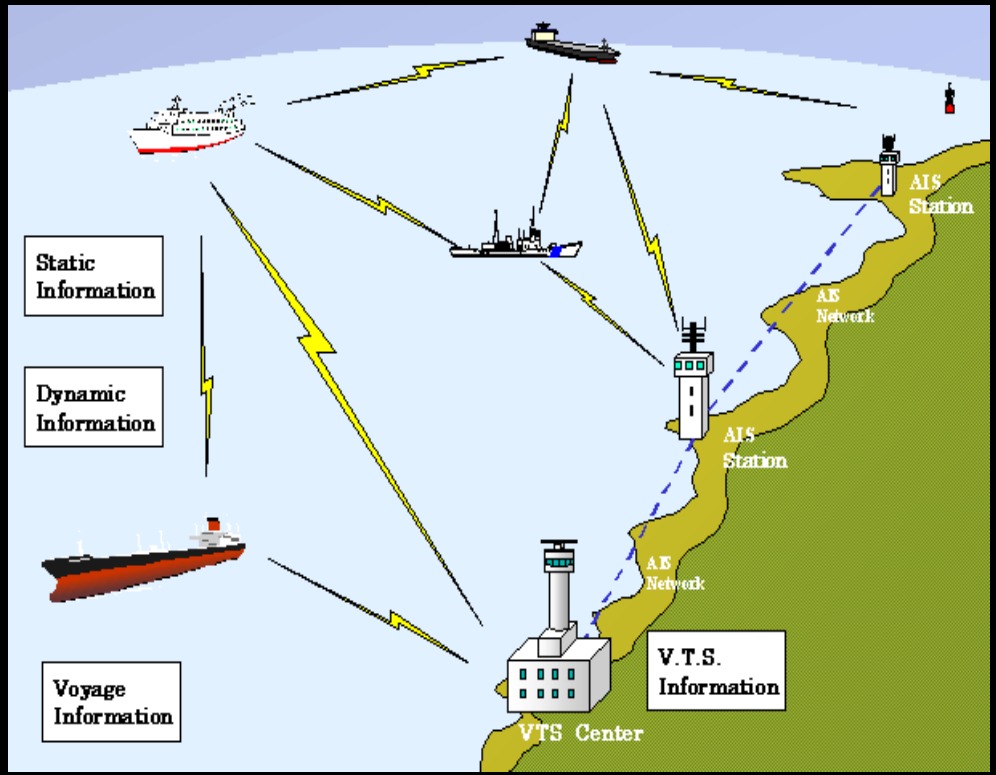
What could go wrong? :D

Let’s walk through some noteworthy cases

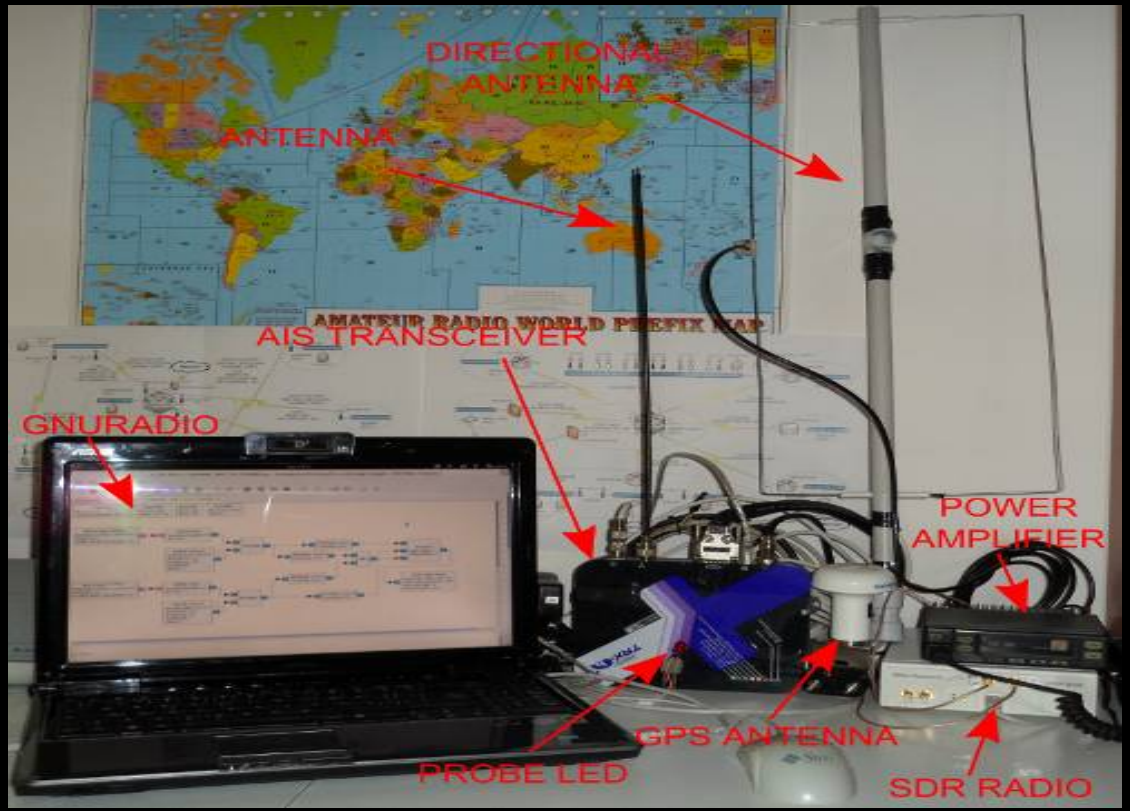
1: AIS

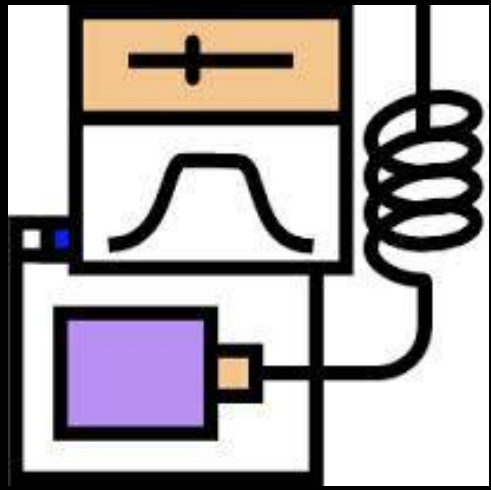
Automated Identification System

- GPS-based radar
- 20 years old standard
- Mandatory. Used by ~300,000 ships
- Lack of integrity and authentication checks

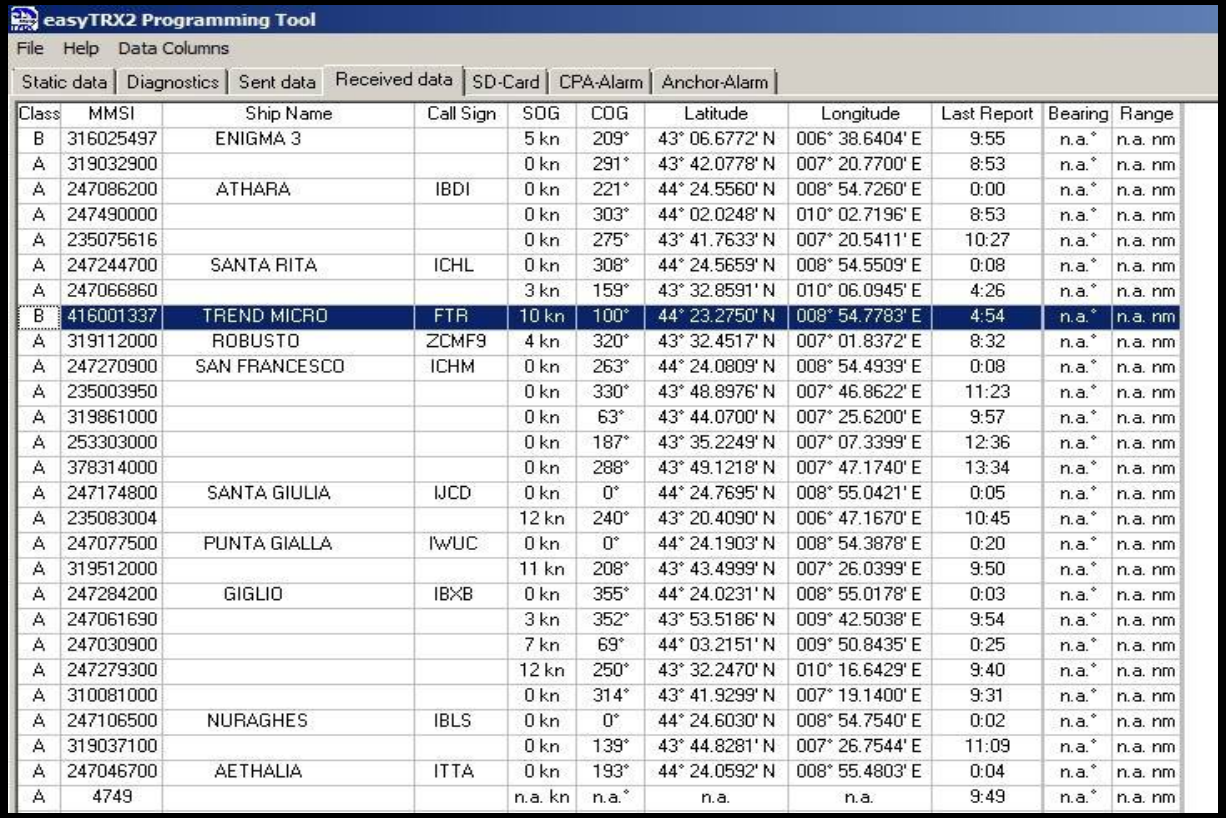


Attack setup



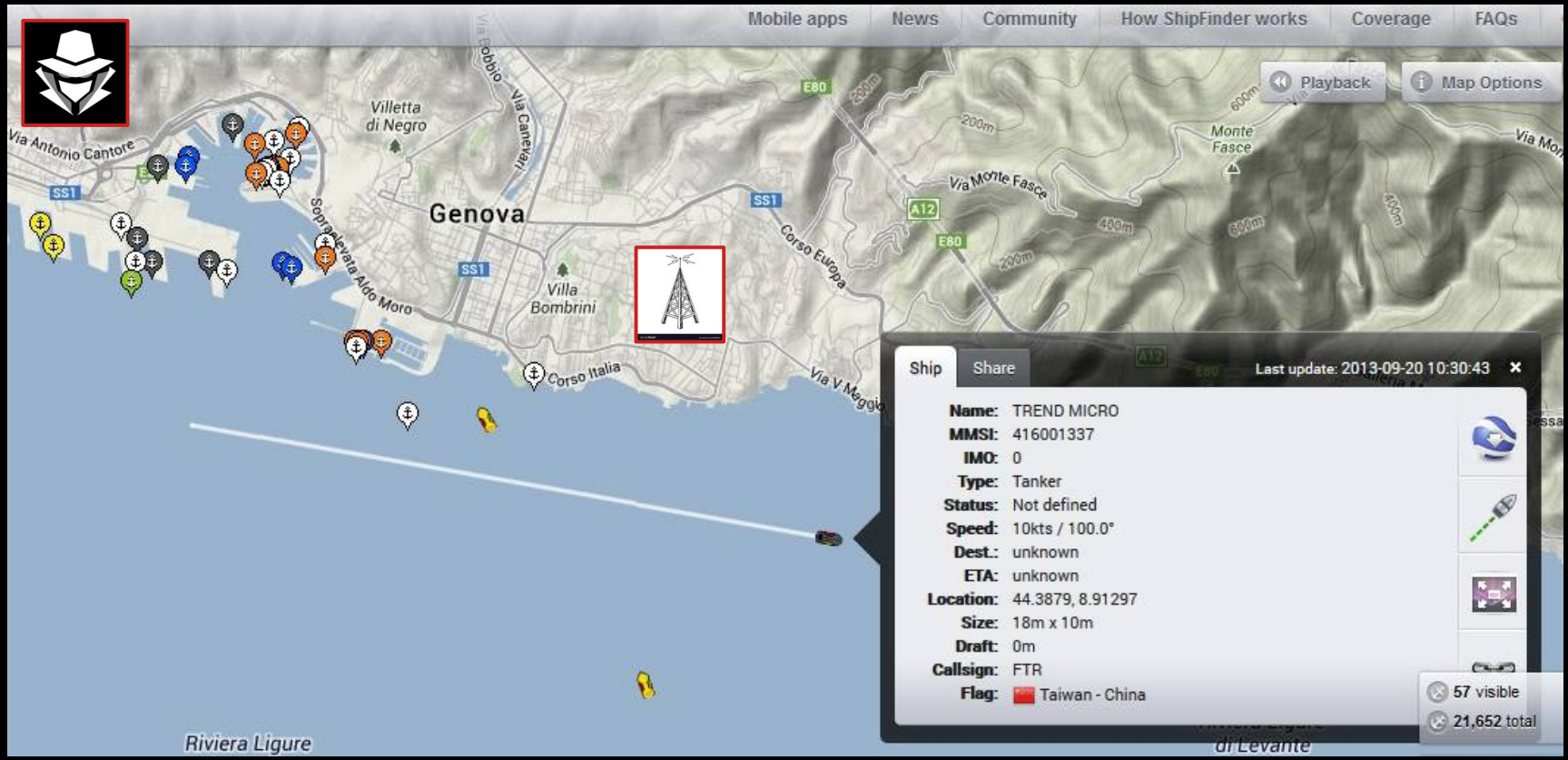


Targeting an AIS transponder



Class	MMSI	Ship Name	Call Sign	SOG	COG	Latitude	Longitude	Last Report	Bearing	Range
B	316025497	ENIGMA 3		5 kn	209°	43° 06.6772' N	006° 38.6404' E	9:55	n.a.°	n.a. nm
A	319032900			0 kn	291°	43° 42.0778' N	007° 20.7700' E	8:53	n.a.°	n.a. nm
A	247086200	ATHARA	IBDI	0 kn	221°	44° 24.5560' N	008° 54.7260' E	0:00	n.a.°	n.a. nm
A	247490000			0 kn	303°	44° 02.0248' N	010° 02.7196' E	8:53	n.a.°	n.a. nm
A	235075616			0 kn	275°	43° 41.7633' N	007° 20.5411' E	10:27	n.a.°	n.a. nm
A	247244700	SANTA RITA	ICHL	0 kn	308°	44° 24.5659' N	008° 54.5509' E	0:08	n.a.°	n.a. nm
A	247066860			3 kn	159°	43° 32.8591' N	010° 06.0945' E	4:26	n.a.°	n.a. nm
B	416001337	TREND MICRO	FTR	10 kn	100°	44° 23.2750' N	008° 54.7783' E	4:54	n.a.°	n.a. nm
A	319112000	ROBUSTO	ZCMF9	4 kn	320°	43° 32.4517' N	007° 01.8372' E	8:32	n.a.°	n.a. nm
A	247270900	SAN FRANCESCO	ICHM	0 kn	263°	44° 24.0809' N	008° 54.4939' E	0:08	n.a.°	n.a. nm
A	235003950			0 kn	330°	43° 48.8976' N	007° 46.8622' E	11:23	n.a.°	n.a. nm
A	319861000			0 kn	63°	43° 44.0700' N	007° 25.6200' E	9:57	n.a.°	n.a. nm
A	253303000			0 kn	187°	43° 35.2249' N	007° 07.3399' E	12:36	n.a.°	n.a. nm
A	378314000			0 kn	288°	43° 49.1218' N	007° 47.1740' E	13:34	n.a.°	n.a. nm
A	247174800	SANTA GIULIA	IJCD	0 kn	0°	44° 24.7695' N	008° 55.0421' E	0:05	n.a.°	n.a. nm
A	235083004			12 kn	240°	43° 20.4090' N	006° 47.1670' E	10:45	n.a.°	n.a. nm
A	247077500	PUNTA GIALLA	IWUC	0 kn	0°	44° 24.1903' N	008° 54.3878' E	0:20	n.a.°	n.a. nm
A	319512000			11 kn	208°	43° 43.4999' N	007° 26.0399' E	9:50	n.a.°	n.a. nm
A	247284200	GIGLIO	IBXB	0 kn	355°	44° 24.0231' N	008° 55.0178' E	0:03	n.a.°	n.a. nm
A	247061690			3 kn	352°	43° 53.5186' N	009° 42.5038' E	9:54	n.a.°	n.a. nm
A	247030900			7 kn	69°	44° 03.2151' N	009° 50.8435' E	0:25	n.a.°	n.a. nm
A	247279300			12 kn	250°	43° 32.2470' N	010° 16.6429' E	9:40	n.a.°	n.a. nm
A	310081000			0 kn	314°	43° 41.9299' N	007° 19.1400' E	9:31	n.a.°	n.a. nm
A	247106500	NURAGHES	IBLS	0 kn	0°	44° 24.6030' N	008° 54.7540' E	0:02	n.a.°	n.a. nm
A	319037100			0 kn	139°	43° 44.8281' N	007° 26.7544' E	11:09	n.a.°	n.a. nm
A	247046700	AETHALIA	ITTA	0 kn	193°	44° 24.0592' N	008° 55.4803' E	0:04	n.a.°	n.a. nm
A	4749			n.a. kn	n.a.°	n.a.	n.a.	9:49	n.a.°	n.a. nm

Targeting an AIS station



Transmit arbitrary commands

Example: Fake a Closest Point of Approach (CPA) alert

- Trigger a collision warning
- Possibly alter course

Demo Time

- Manipulating Closest Point of Approach Alarms final.mov

DoS

- Goal: Disable AIS transponders
  - Single or multiple target(s)
  - Program a desired targeted region
- Frequency hopping
  - Switch to non-default frequency (RX and TX)

Demo Time

- Manipulating AIS SOS Signals and Frequency Hopping.mov

Falsified AIS (Automated Identification System) appearing to show HMS Defender and HNLMS Evertsen approaching Sevastopol, Crimea, On June 19 2021

Odessa, Ukraine

False AIS tracks

Sevastopol, Crimea
(Russian naval base)

Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base

MarineTraffic

Webcams showing HMS Defender (A) and HNLMS Evertsen (B) in Odessa

2: IND

Remote Controllers for the Industry

Remote Controllers for the Industry



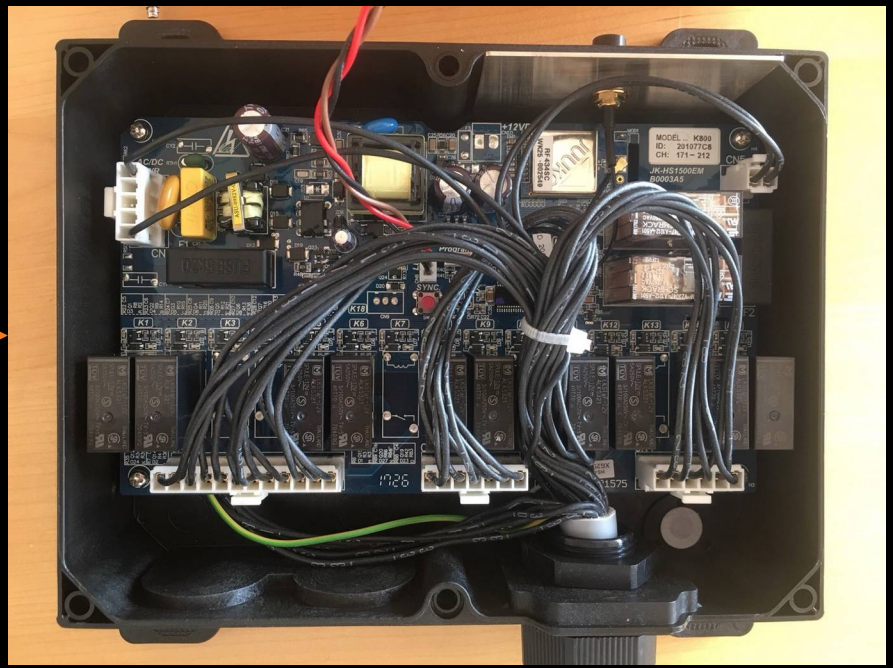




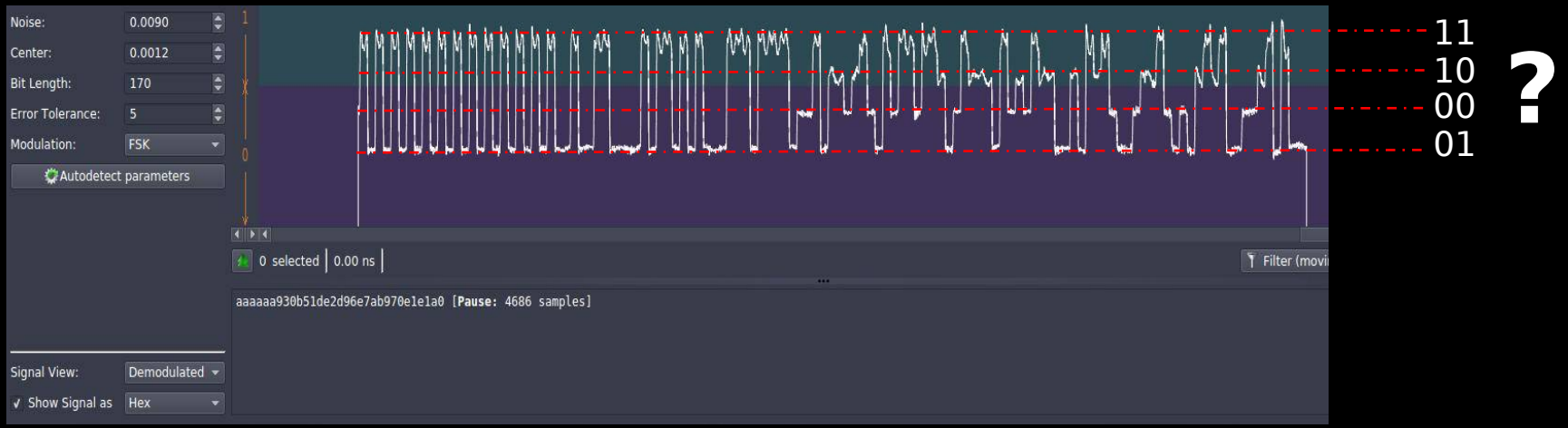


Research


JUUKO
INDUSTRIAL RADIO REMOTE CONTROL
RECEIVER
ERROR
ACTIVE
RECEIVING
WIRING DIAGRAM HS800(C2)
HS series
JUUKO
STATUS
1
2
START

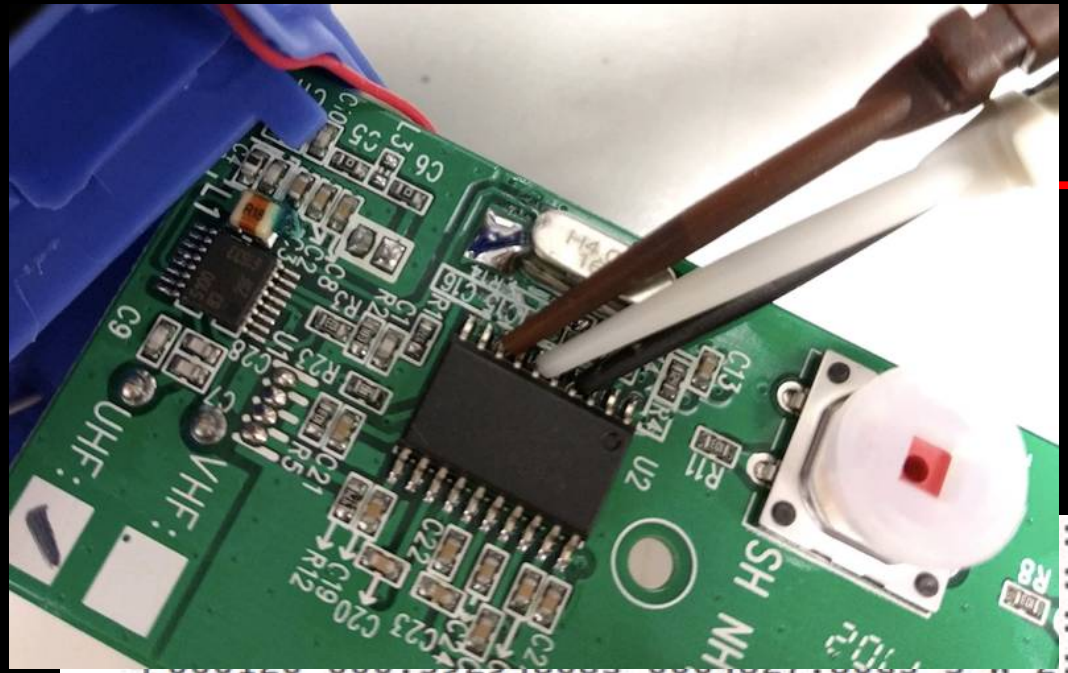


Signal Analysis



- Missing needed information
  - Sync word, encoding, bit length, etc...

SPI emulation



```
                                                :Extended 72:RSSI0          0x07
                                                :Extended 71:RSSI1          0x4c
                                                :Extended 73:MARCSTATE      0x6d
                                                :Command  36:SIDLE
  5 000121 000.39296368s 0000015.00us S R 1:Extended d7:NUM_RXBYTES     0x10
  6 000122 000.39298167s 0000018.00us S R 1:Extended d7:NUM_RXBYTES     0x10
  7 000122 000.39299052s 0000008.85us B R 4:SFIFO    3f:SFIFO           0x0d 0xa2
  8 000123 000.39312045s 0000129.93us S W 2:Command  34:SRX
  9 000124 000.39803355s 0004913.10us S R 1:Extended 72:RSSI0           0x00
 10 000125 000.39805215s 0000018.60us S R 1:Extended 73:MARCSTATE       0x6d
 11 000126 000.40798570s 0009933.55us S R 1:Extended 72:RSSI0           0x03
 12 000127 000.40800443s 0000018.72us S R 1:Extended 71:RSSI1           0xfb
 13 000128 000.40802702s 0000022.60us S R 1:Extended 73:MARCSTATE       0x6d
```

Attack Scenarios

- Industrial Remote Controllers.mp4

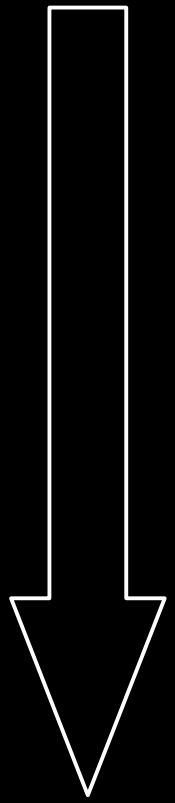
3: FOBS

Key fobs and door openers


YouTube IT
Search
USB
0:36 / 16:32
HAK5
Hacking Ford Key Fobs Pt. 1 - SDR Attacks with @TB69RR - Hak5 2523 [Cyber Security Education]
173,155 views • Jun 24, 2019
3.8K
131
SHARE
SAVE
All
Hak5
Radios
Related

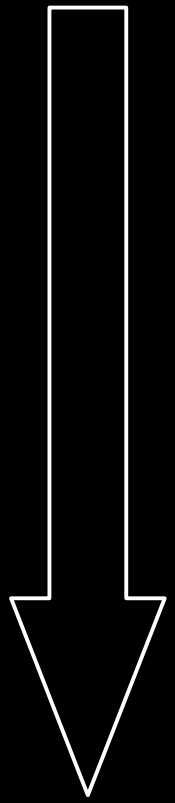
A history of “learning from errors”

Security = f(car_code)



A history of “learning from errors”

Security = f(car_code)



Reply Attack

A history of “learning from errors”

Security = f(car_code)

Reply Attack

Security = f(car_code + rolling code)

A history of “learning from errors”

Security = f(car_code)

Reply Attack

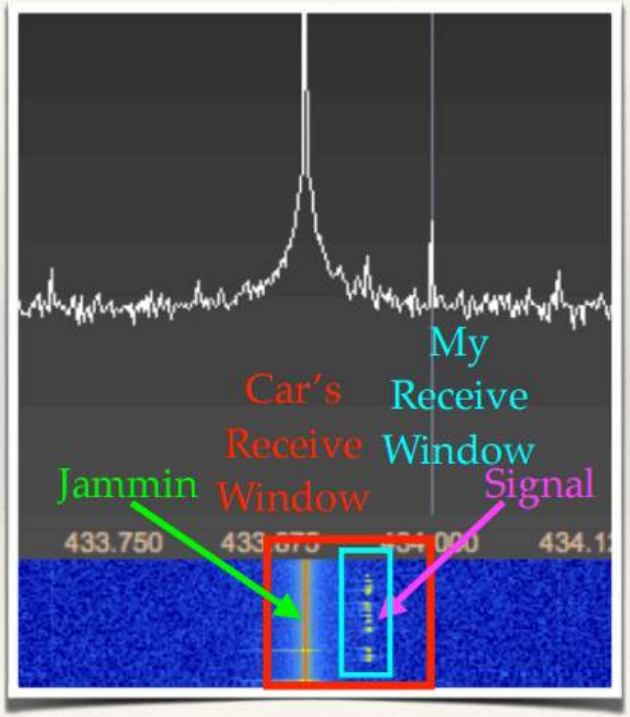
Security = f(car_code + rolling code)

Rolljam

Rolljam

Jam+Listen(1), Jam+Listen(2), Replay (1)

- Jam at slightly deviated frequency
- Receive at frequency with tight receive filter bandwidth to evade jamming
- User presses key but car can't read signal due to jamming
- User presses key again — you now have **two** rolling codes
- Replay **first** code so user gets into car, we **still have second code**



A history of “learning from errors”

Security = f(car_code)

Reply Attack

Security = f(car_code + rolling code)

Rolljam

Security = f(car_code + rolling code + time)

Raise awareness

Sharing knowledge

Growing a community of radio hackers & enthusiasts

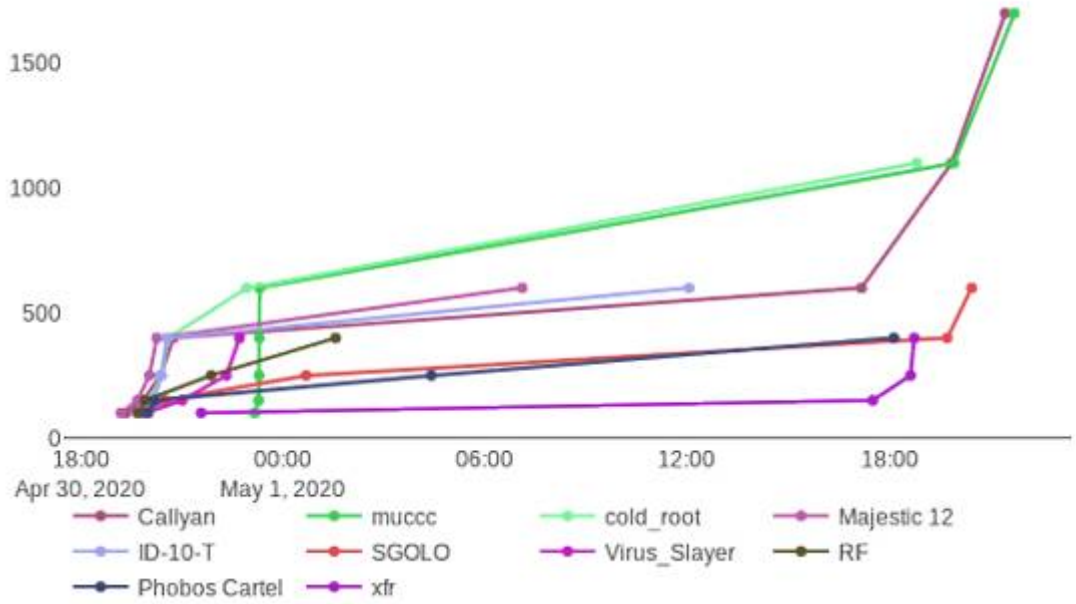

capture the signal

Radio Contest

- Reverse engineering of radio signals (analog, digital)
- Blind signal analysis
- Presence at conferences
- Signals distributed “over IP”
- Increasing difficulty

Connect with the community

Compete



337 users registered

223 teams registered

492 IP addresses

2860 total possible points

9 challenges

Signal 1 has the most solves with 31 solves

Signal 5 has the least solves with 8 solves

Win

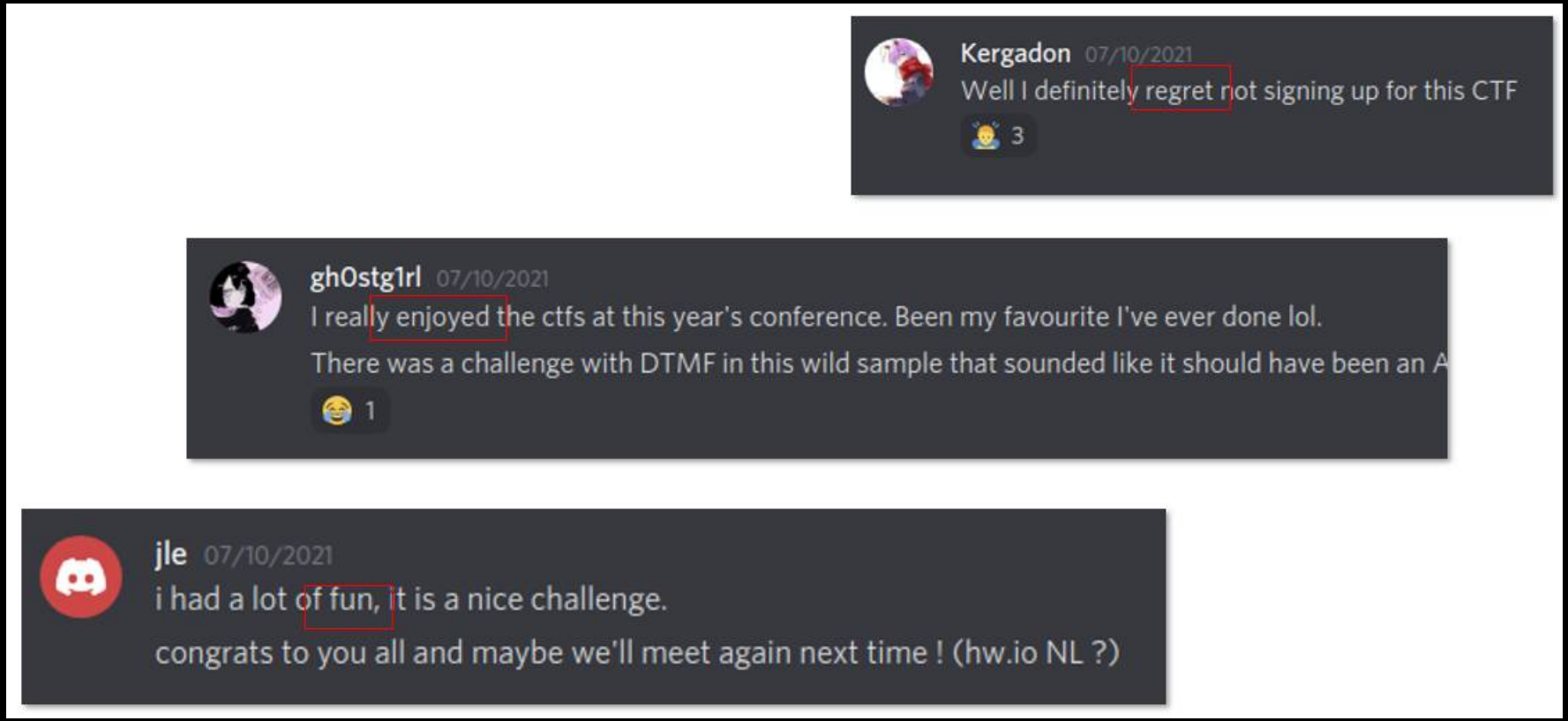
Bronze

Silver

Gold

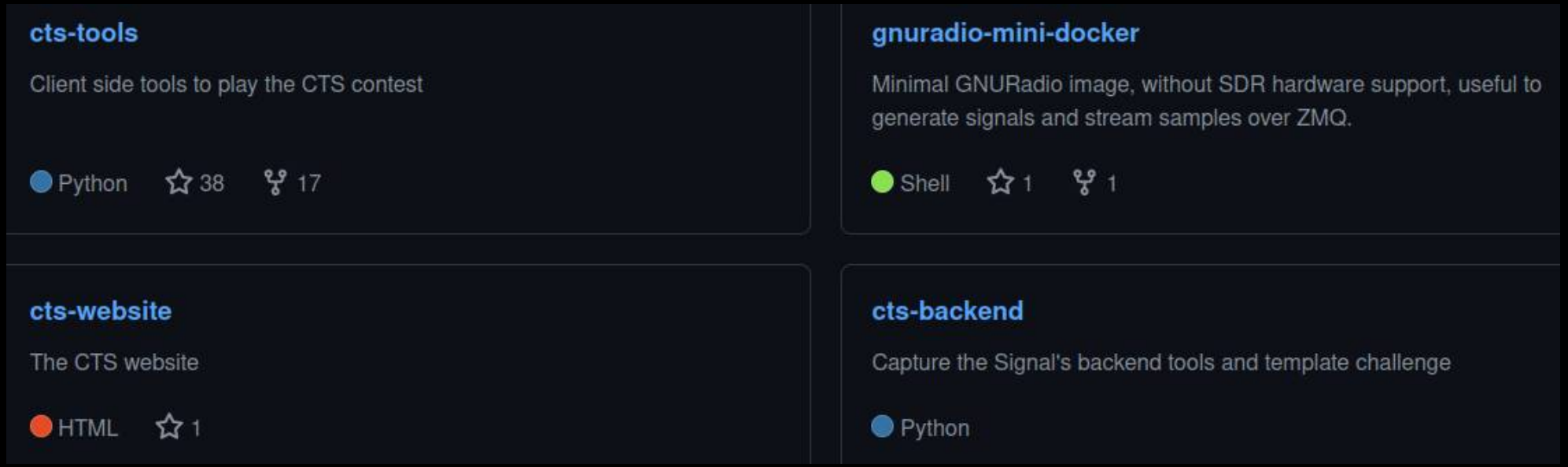
Awards Ceremony ☺

Enjoy


Kergadon 07/10/2021
Well I definitely regret not signing up for this CTF
3
ghOstg1rl 07/10/2021
I really enjoyed the ctfs at this year's conference. Been my favourite I've ever done lol.
There was a challenge with DTMF in this wild sample that sounded like it should have been an A
1
jle 07/10/2021
i had a lot of fun, it is a nice challenge.
congrats to you all and maybe we'll meet again next time ! (hw.io NL ?)

Open Spirit

- Playing scripts and back-end available at `https://github.com/capturethesignal`



Thanks for listening!
Questions?

https://twitter.com/embyte