SDR

Introduction

Maarten Pentinga

Junior-pentester & teacher. Big interest in breaking things, creating hacking challenges & organizing CTF events.

E-mail: mp@warpnet.nl

Roald Nefs

DevOps Engineer at DUO. Big interest in Site Reliability Engineering, Python, RF and more...

GitHub: roaldnefs
E-mail: roald@warpnet.nl

Agenda

Introduction
Exercise: Listen up!
Regulations
Example: Passive IMSI Catcher
Example: Fixed Code
Example: Rolling Code
Hello Barbie!
Exercise: Ring the Doorbell

Exercise: Listen up! 30m

Exercise

- Work in groups of 4,
- Listen very carefully, they might broadcast twice.

Goal

- Listen at least to one radio station,
- Choose whether you would want to receive messages from the P2000 network or monitor air traffic.

Extra

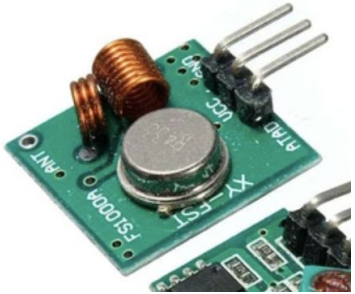
- Try and receive weather satellite images with your RTL-SDR. (Google required)

Frequency regulations

Countries have different regulations. Within the **Netherlands**, sending signals on common frequencies is **illegal**. Therefor a permit is required. For equipment with **limited reach** and **low transmitting powe**r no permit is needed.

Hmh, please do clarify!

Product Model: XD-RF-5V



Transmitter:
Technical parameters of
Product Model: XD-FST
Launch distance :20-200 meters (different voltage, different results)
Operating voltage :3.5-12V
Dimensions: 19 * 19mm
Operating mode: AM
Transfer rate: 4KB / S
Transmitting power: 10mW
Transmitting frequency: 433M
Pinout from left → right: (DATA; VCC; GND)

We legal (:

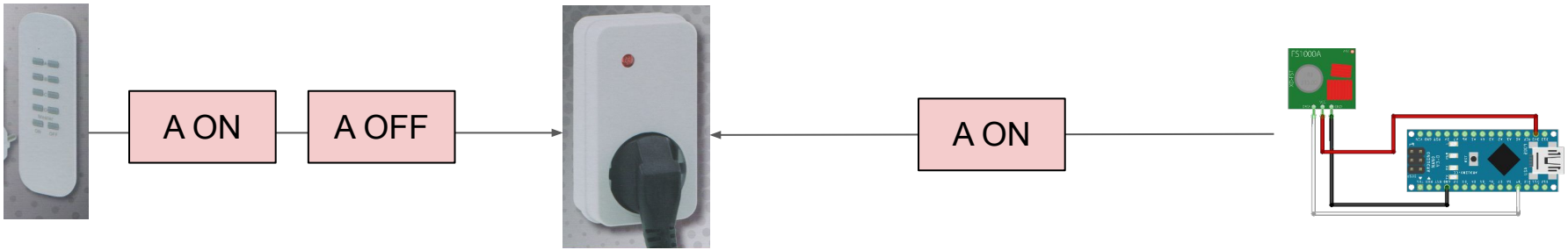
Tabel 1 Algemene toepassingen zoals bijvoorbeeld telemetrie, telecommand, alarmering, data

	Frequentieband	Vermogen/Veldsterkte	Kanaalraster	Duty-cycle
A	6765 - 6795 kHz	42 dBµA/m op 10 m afstand	-	-
B	13,553 - 13,567 MHz	42 dBµA/m op 10 m afstand	-	-
C	26,957 - 27,283 MHz	42 dBµA/m op 10 m afstand of 10 mW e.r.p.	-	-
D	40,660 - 40,700 MHz	10 mW e.r.p.	-	-
E	433,050 - 434,790 MHz	10 mW e.r.p.	-	< 10 %
E1	433,050 - 434,790 MHz	1 mW e.r.p.[1]	-	-
E2	434,040 - 434,790 MHz	10 mW e.r.p.	25 kHz	-
F	863,000 - 865,000 MHz	25 mW e.r.p.	-	< 0,1 %[3]
G	865,000 - 868,600 MHz	25 mW e.r.p.	-	< 1,0 %[3]
H	868,700 - 869,200 MHz	25 mW e.r.p.	-	< 0,1 %[3]
I	869,300 - 869,400 MHz	10 mW e.r.p.	25 kHz	-
K1	869,400 - 869,650 MHz	500 mW e.r.p.	25 kHz[2]	< 10 %[3]

Example: Fixed Code (1/3)

Devices using a fixed code are vulnerable to a replay and bruteforce attack. The attacker can simple record and replay the signal.

Using a bruteforce approach requires knowledge about the modulation type (FFCID).

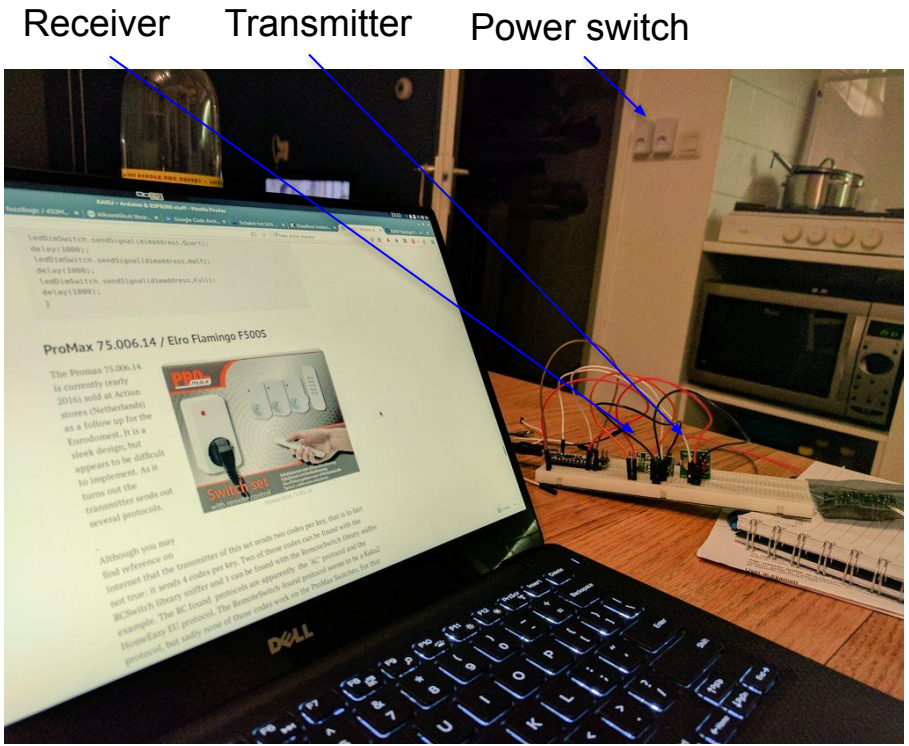


Example: Fixed Code (2/3)

Instead of using an SDR to record the signal you can also use a cheap receiver to listen to the fixed codes.

For more popular devices such as '*Klik Aan Klik Uit*' you will even find libraries:

[kakuarduino]

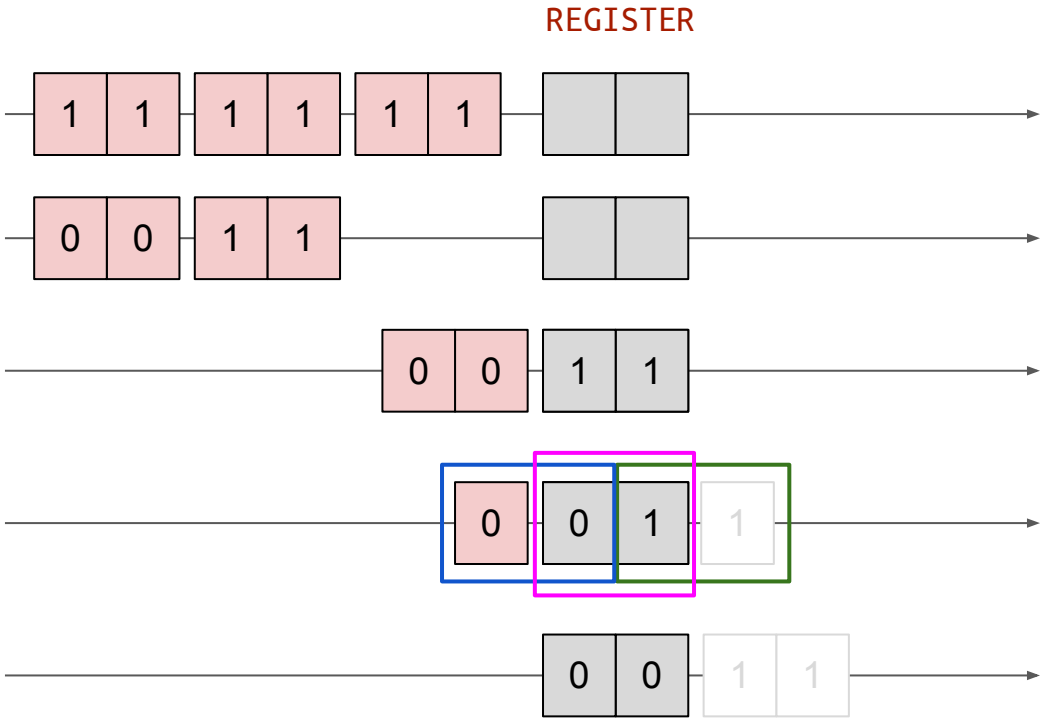


Example: Fixed Code (3/3)

Most devices will repeat the fixed code several times.

Instead of repeating them, you can simple send each code once.

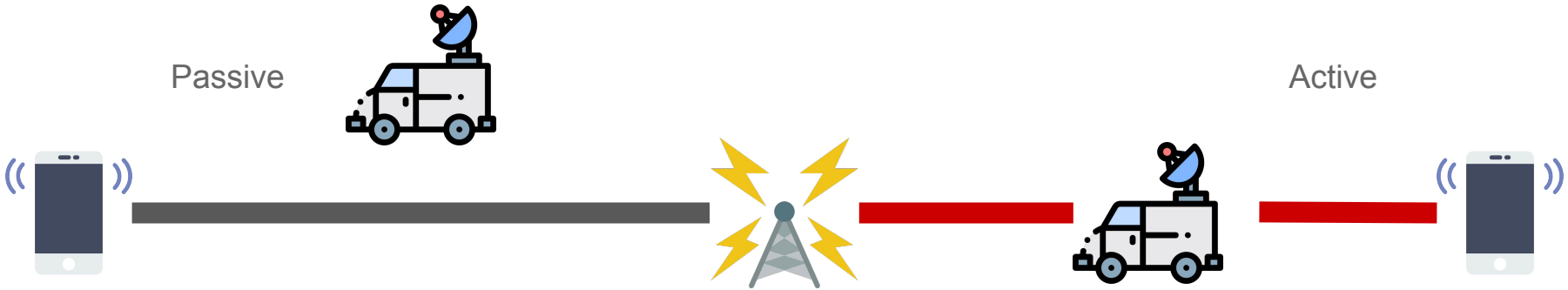
You might want to check of the De Bruijn sequence...



Example: Passive IMSI Catcher (1/5)

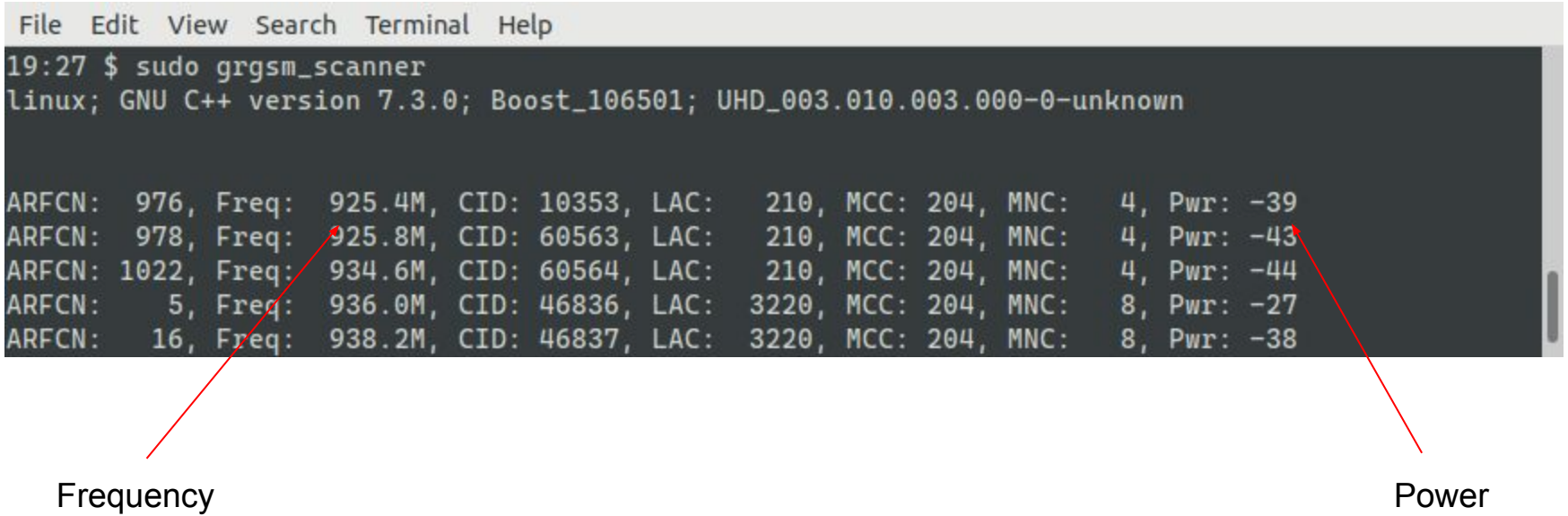
The passive International Mobile Subscriber Identity (**IMSI**) catcher works by capturing an IMSI number when a phone **initializes a connection to a base station**. To protect the privacy of the user all subsequent communication is done with a random Temporary Mobile Subscriber Identity (**TMSI**) number.

Active IMSI catchers perform a man in the middle attack and are definitely illegal!



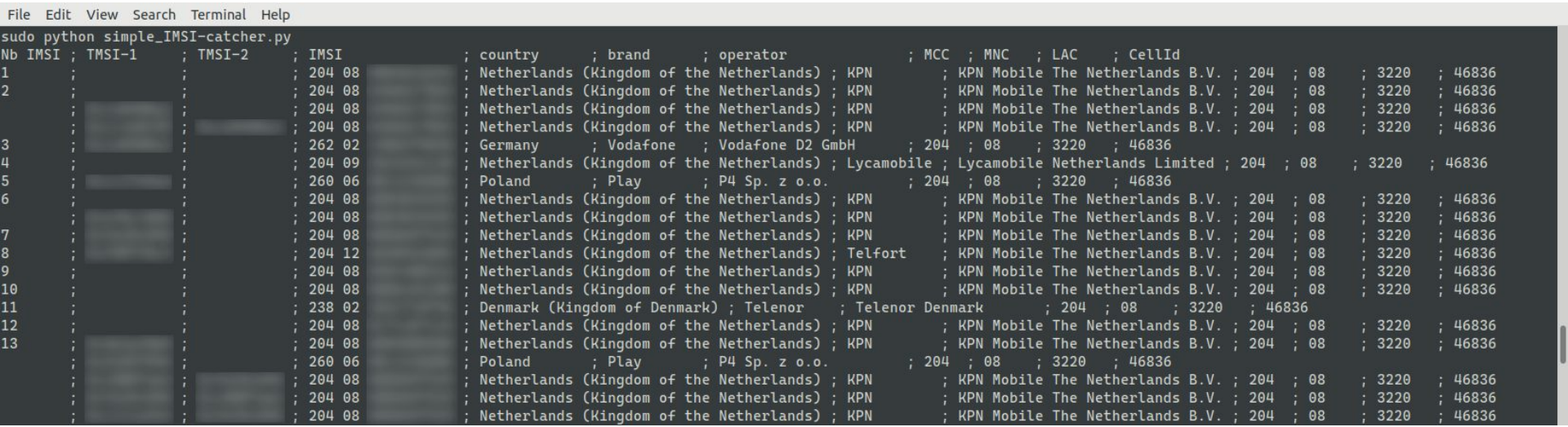
Example: Passive IMSI Catcher (2/5)

Scan for nearby base stations:



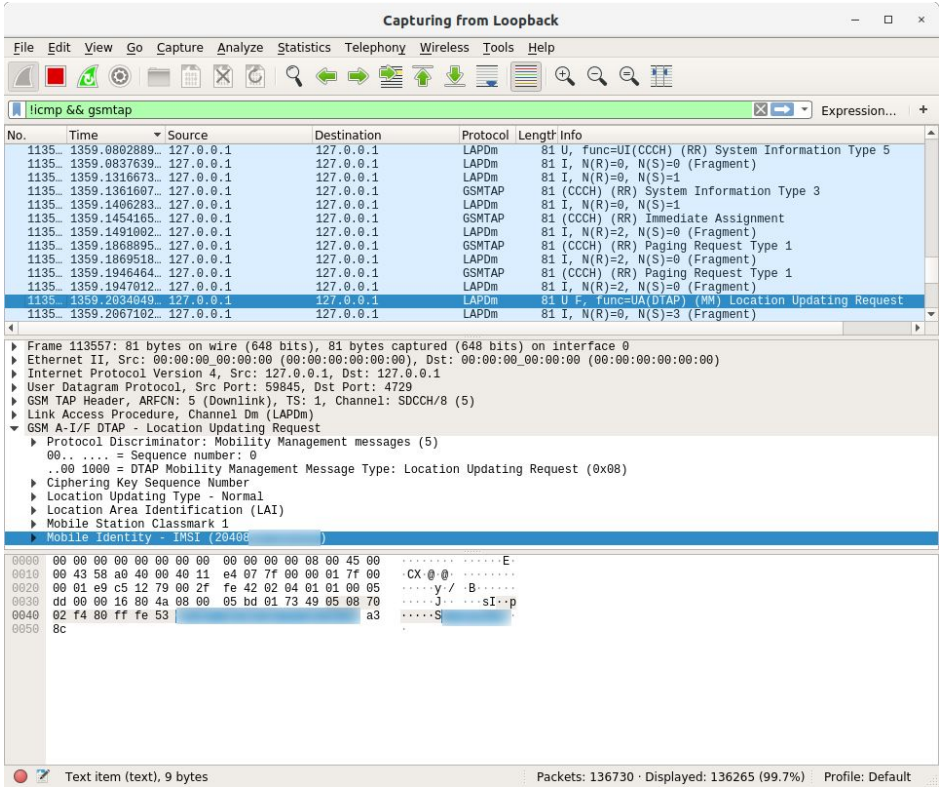
Example: Passive IMSI Catcher (3/5)

Using github.com/Oros42/IMSI-catcher to sniff IMSI numbers (*will automatically scan and select a base station*):



Example: Passive IMSI Catcher (4/5)

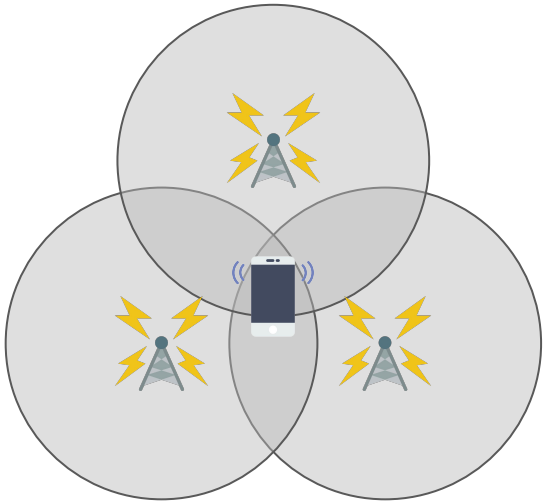
The GSM traffic can be viewed in Wireshark, the `!icmp && e212.imsi` filter will only show packets that contain IMSI numbers.



Example: Passive IMSI Catcher (5/5)

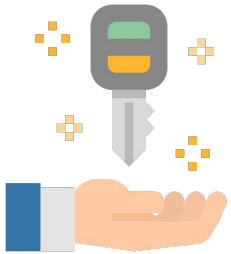
Problems occur when you can associate an IMSI number with an individual.

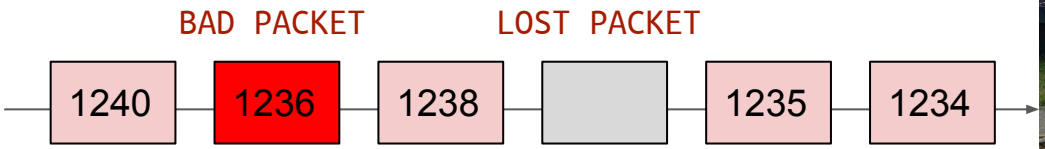
Mobile apps can access a device's IMSI number, e.g. `getSubscriberId` on Android…



Example: Rolling Code (1/3)

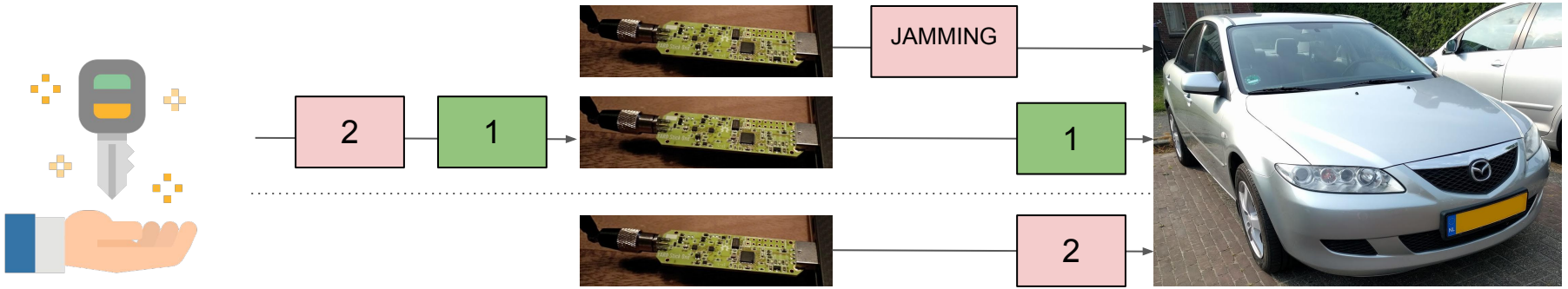
Rolling code is used in keyless entry systems to prevent replay attacks. The car and keyfob use a pseudorandom number generator.





Example: Rolling Code (2/3)

Jam the vehicle's frequency and intercept two codes. Stop jamming an
Immediately send the first received code so the owner won't notice anything...



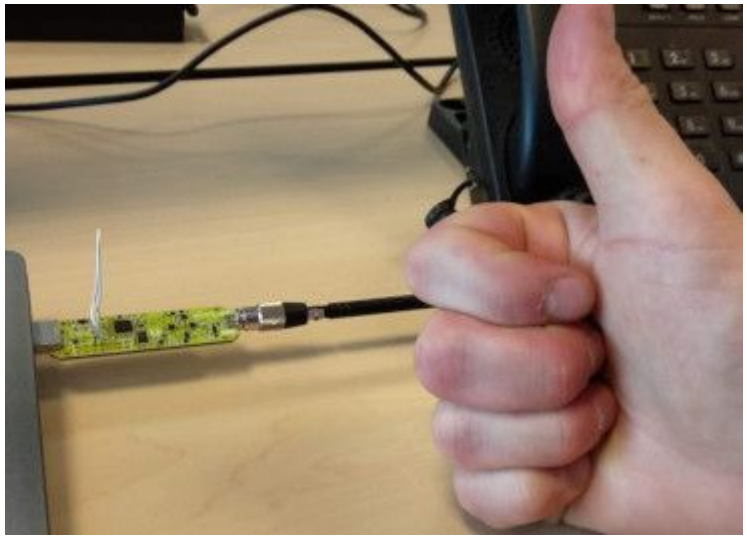
The second captured code is still usable and can be used as long as the owner doesn't (un)lock the vehicle.

Example: Rolling Code (3/3)

Used hardware: two **YARD Stick One's** (Yet Another Radio Dongle), which can transmit and receive digital wireless signals at frequencies below 1 GHz.

The YARD Stick One come with RfCat firmware tnstalled. RfCat allows you to control the wireless transceiver from an interactive **Python** shell.

```
YARD Stick One != SDR
```



Hello Barbie! (1/3)

Let’s take a closer look at Barbie…

Hello Barbie! (2/3)

FCC ID: PIYDKF74-15A5W

Searchable FCC ID Database: fccid.io

Document	Type	Submitted Available
User manual-2	Users Manual Adobe Acrobat PDF (237 kB)	2015-10-16 2015-10-20
User manual-1	Users Manual Adobe Acrobat PDF (4139 kB)	2015-10-16 2015-10-20
Tune up procedure	Parts List/Tune Up Info Adobe Acrobat PDF (25 kB)	2015-10-16 2015-10-20
Letter MCL	Cover Letter(s) Adobe Acrobat PDF (32 kB)	2015-10-16 2015-10-20
Confidential letter	Cover Letter(s) Adobe Acrobat PDF (64 kB)	2015-10-16 2015-10-20
Channel statement	Cover Letter(s) Adobe Acrobat PDF (32 kB)	2015-10-16 2015-10-20
Authority letter		2015-10-16 2015-10-20
Setup photos		2015-10-16 2015-10-20
SZEM150800520001-revised		2015-10-16 2015-10-20
SZEM150800520002 -rev2		2015-10-16 2015-10-20
Label		2015-10-16 2015-10-20
Internal photos	Internal Photos Adobe Acrobat PDF (1999 kB)	2015-10-16 2015-10-20
External photos	External Photos Adobe Acrobat PDF (1418 kB)	2015-10-16 2015-10-20
5200CR PBA	Cover Letter(s) Adobe Acrobat PDF (157 kB)	2015-10-16 2015-10-20

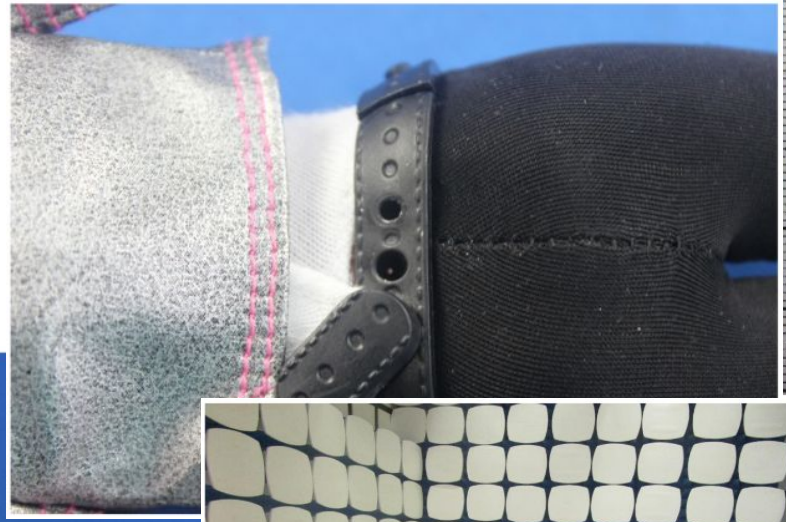
Internal photos

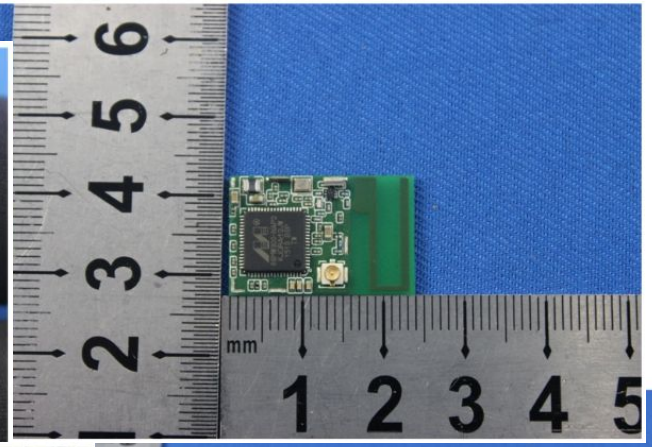
External photos

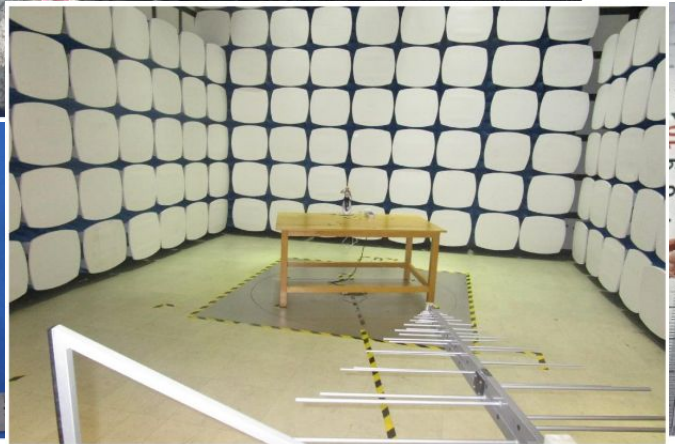
Operating Frequencies

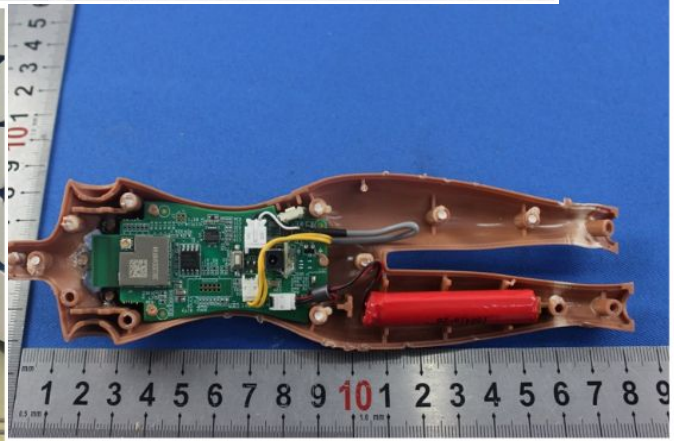
Frequency Range	Power Output	Rule Parts	Line Entry
2.412-2.462 GHz	79 mW	15C	1

Hello Barbie! (3/3)









Exercise: Ring the Doorbell 60m

Exercise

- Work in groups of 4,
- Finish assignment 1 till 7 from chapter 3.

Goal

- Ring the doorbell by recording the signal, demodulation in Audacity and writing your own doorbell script.