Vehicle alarms' insecurity and something else

March 2019
Heidelberg - Germany

TALSOFT SECURITY

TROOPERS

Leandro Ferrari
@talsoft
leandroferrari@talsoft.com.ar

“The ability to think differently is more important than the knowledge acquired.”

- David Bohm -

About Me

Leandro Ferrari

Computer Science Engineer

More than 10 years promoting awareness in cybersecurity in companies and university education based on ethical, professional and service values.

CEO / Founder of the TalSoft TS, we offer protection against computer attacks, to companies and the community, with the aim of improving the computer security, at a national and international level.

Professor of computer security in FASTA University.

TALSOFT
SECURITY

Linkedin: https://www.linkedin.com/in/leandroferrari/

Twitter: @talsoft / @avatar_leandro

Timeline

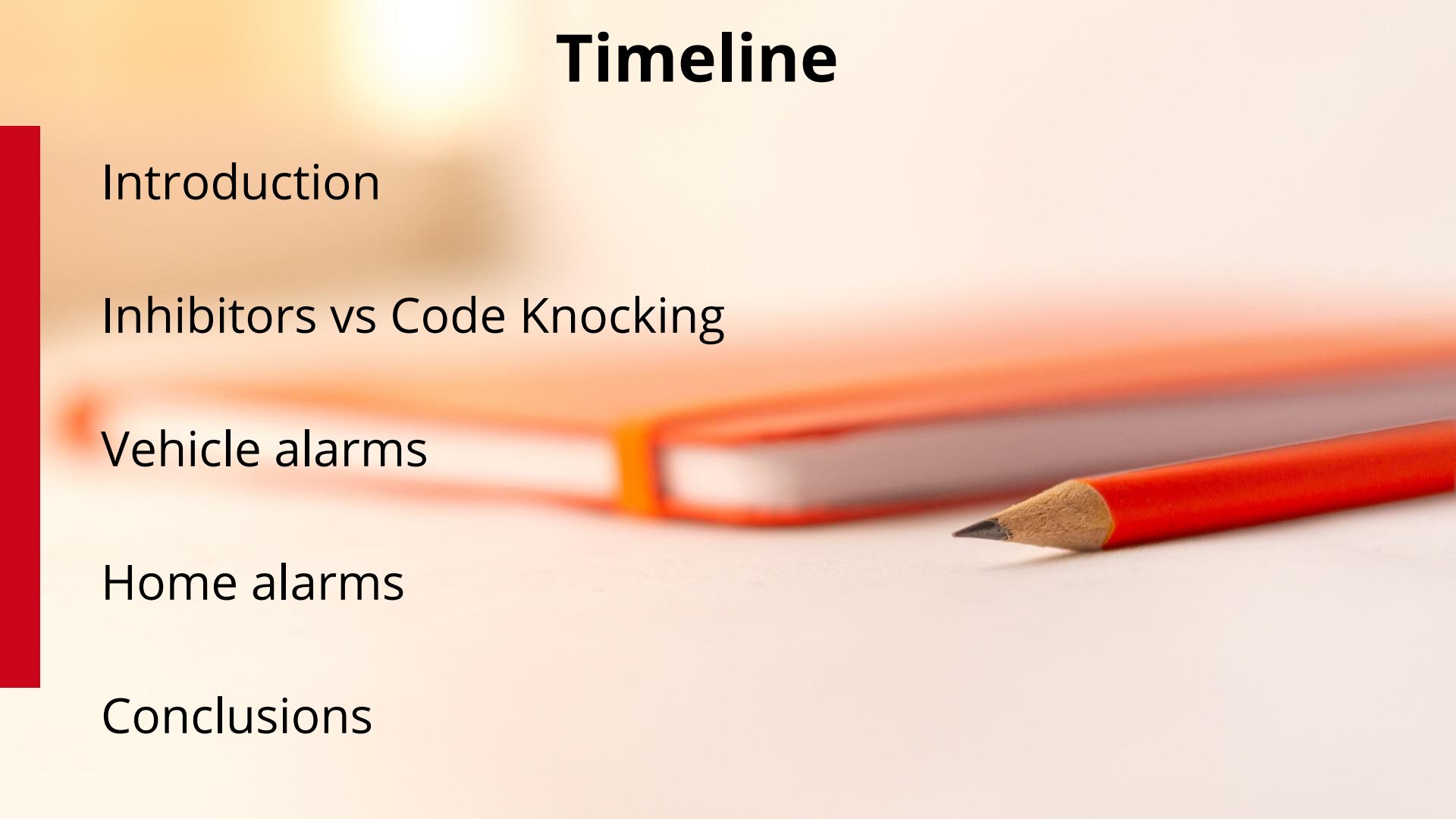
Introduction

Inhibitors vs Code Knocking

Vehicle alarms

Home alarms

Conclusions



Introduction

2014

Logan Lamb - “Home Insecurity No Alarms False Alarms” DefCon 22

Silvio Cesare - “Breaking the Security of Physical Devices” Blackhat USA

USRP B200
U$S 1.000.-

USRP N210
U$S 1.700.-

Introduction

2014

Logan Lamb - “Home Insecurity No Alarms False Alarms” DefCon 22

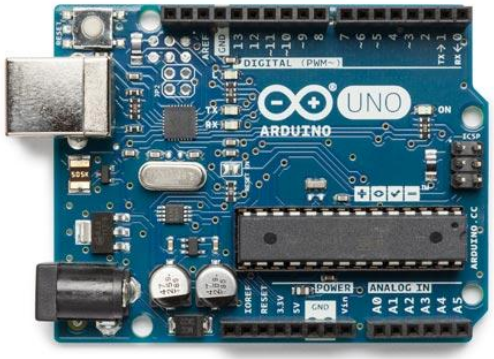
Silvio Cesare - “Breaking the Security of Physical Devices” Blackhat USA

2017

COSIC research group - “Fast furious and insecure passive keyless entry and start in modern supercars”

Unicorn Team - “Car keyless entry system attacks” HitbSecConf

Introduction



Arduino ONE + RTL2832
U$S 40.-

Introduction

I started the research in 2017

I focused in motorcycles’, cars and houses alarms

I used devices from model 2010 to 2016

Inhibitors

VS

Code knocking

Supplier Case One

2.5

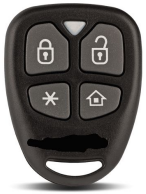
Millions

“The exclusive Flex Code technology, …, offering the maximum security …”

2 X MPS100 FX
2010 / 2013

Duoblock 330fx
2016

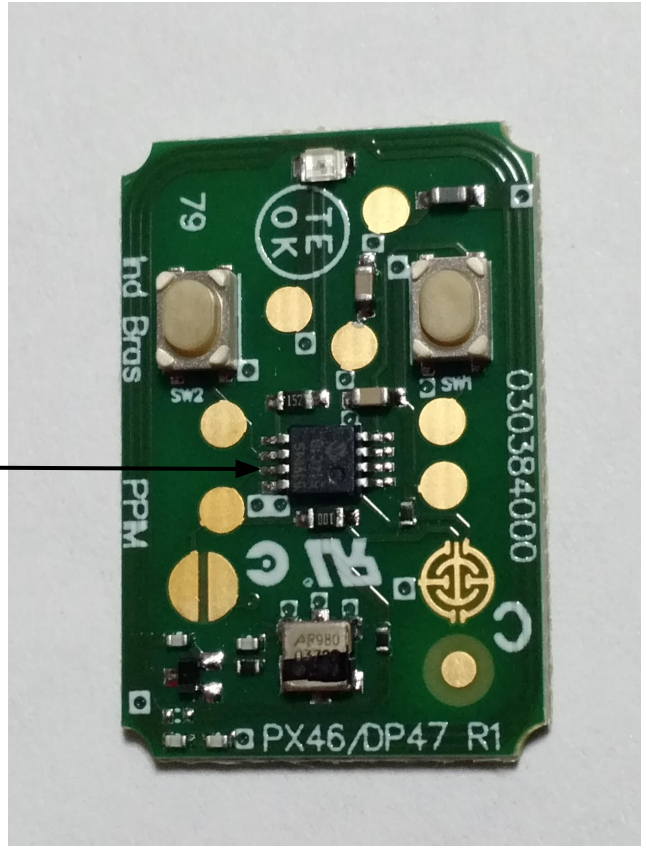
Duoblock 330FX



Control Duoblock 330FX

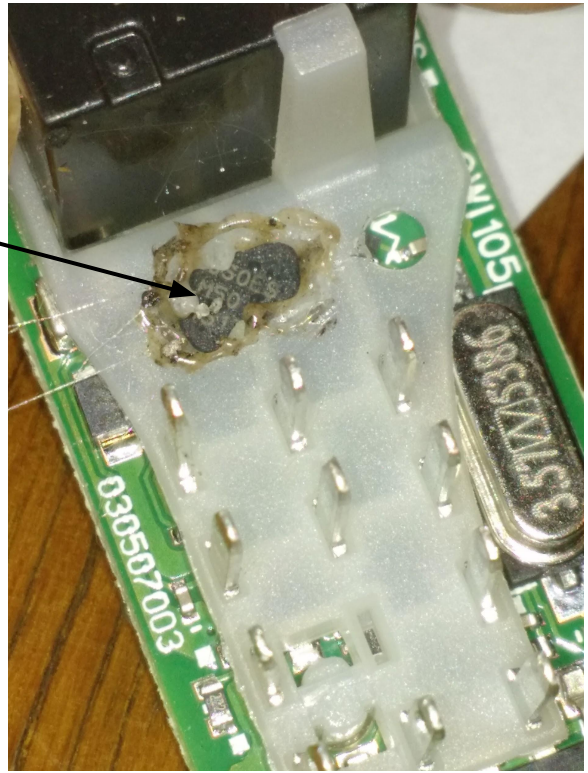
Model DPN52

Microchip 519ims 514C10



Central Duoblock 330FX

Microchip: US0ES A2 M50 25 1517



Signal capturer

RTL-SDR **RTL2832U DVB-T**

Frequency 24 – 1766 MHz

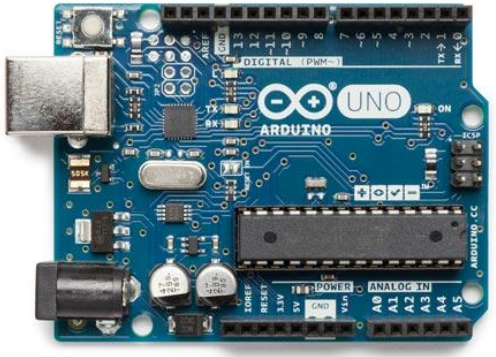
http://www.rtl-sdr.com/

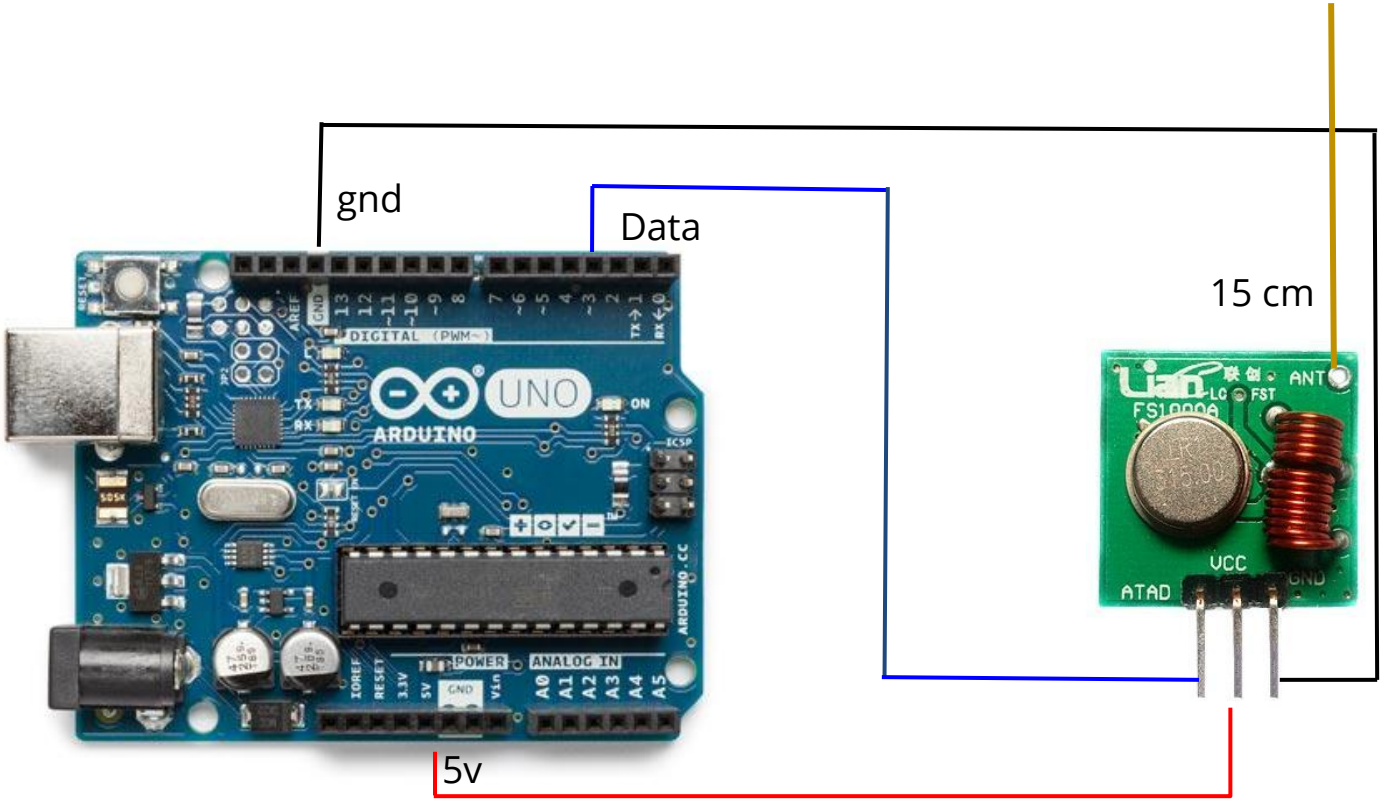
Signal transmitter

Arduino Uno

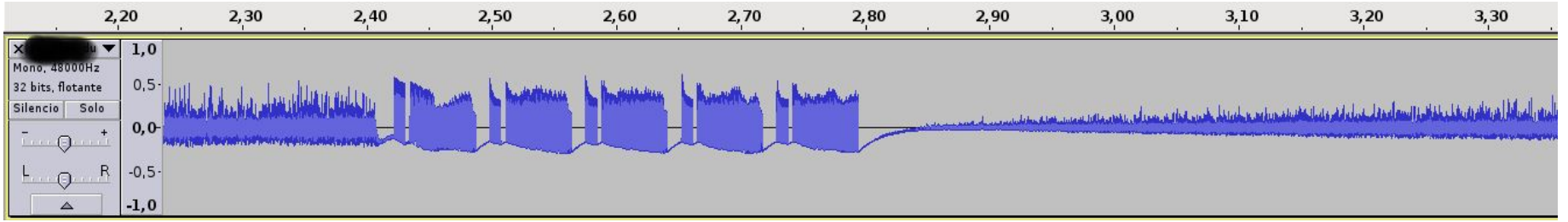
Transmitter FS1000A
433.92mhz

Modulation ASK/OOK

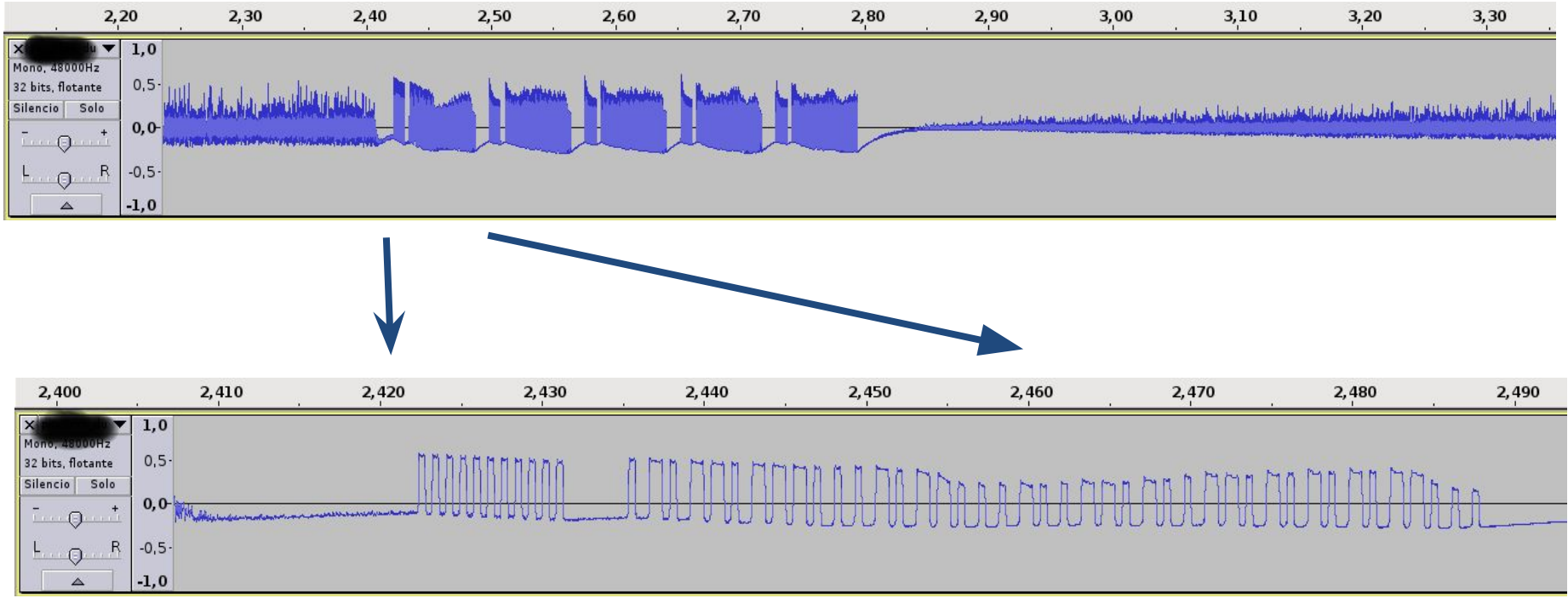



gnd
Data
15 cm
5v
UNO
ARDUINO
DIGITAL (PWM~)
POWER
ANALOG IN
ANT
VCC
GND
ATAD

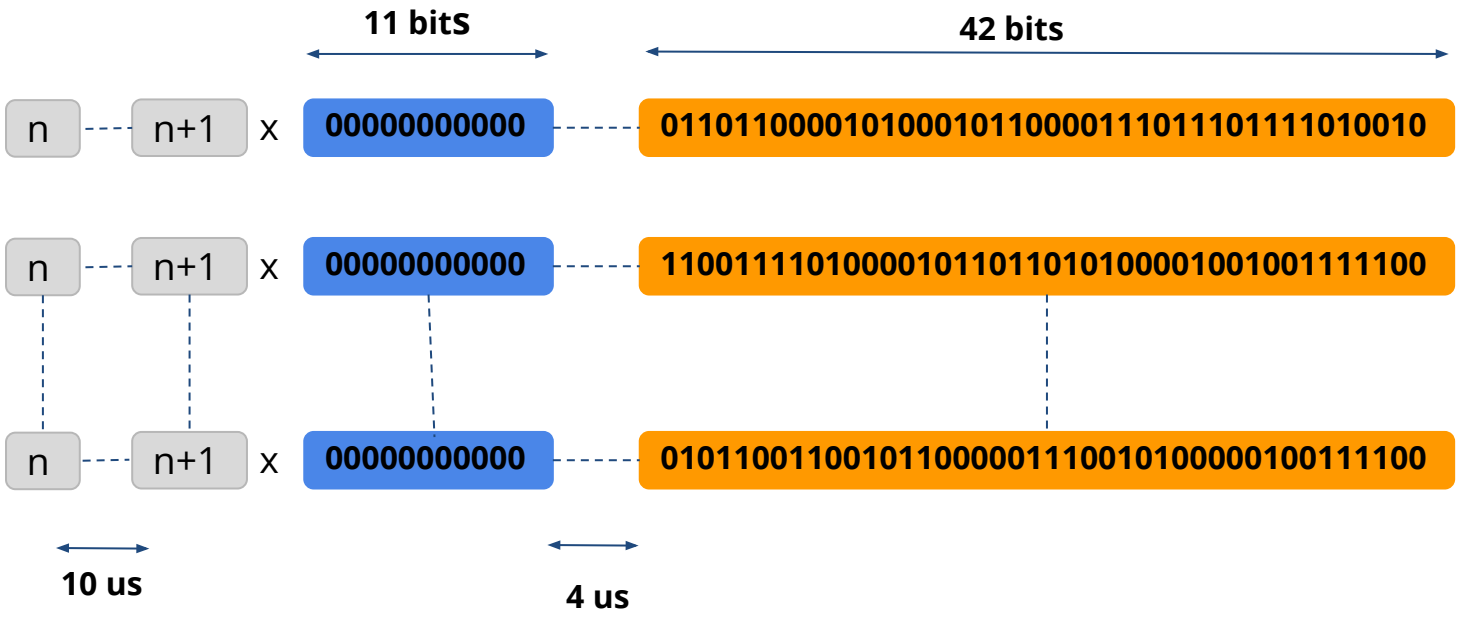
Deactivation



Deactivation

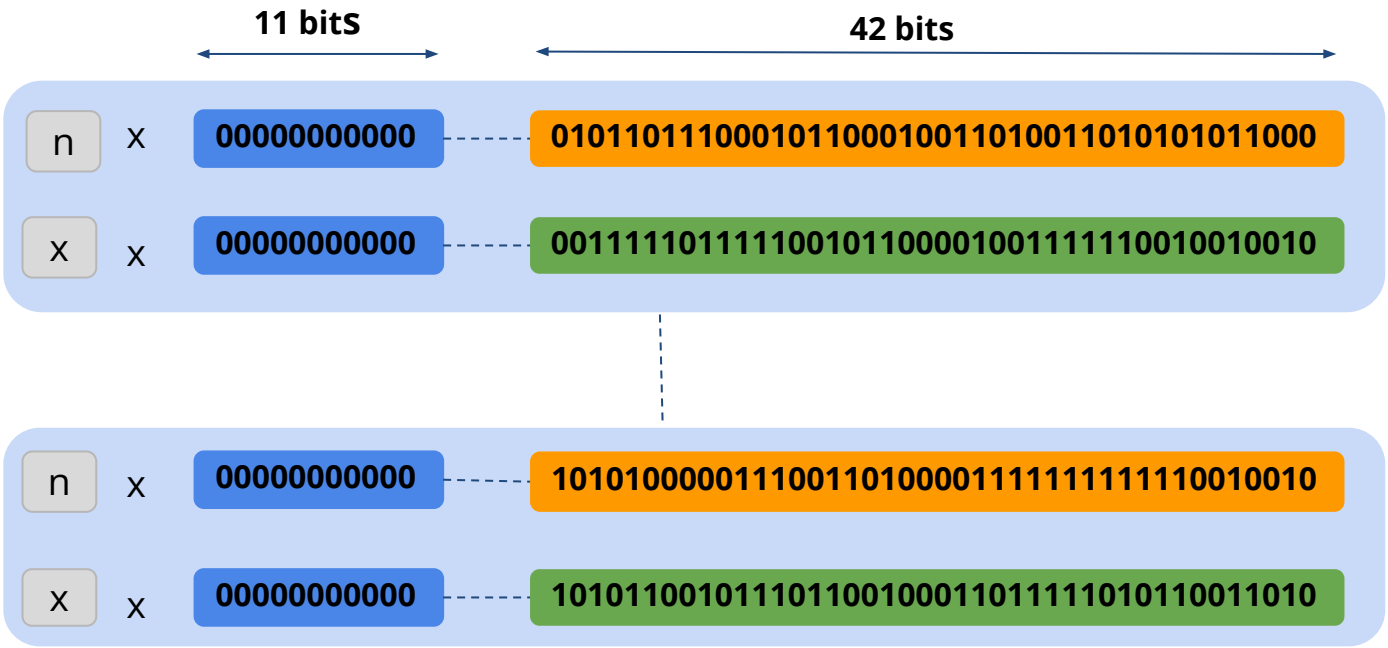


Activation



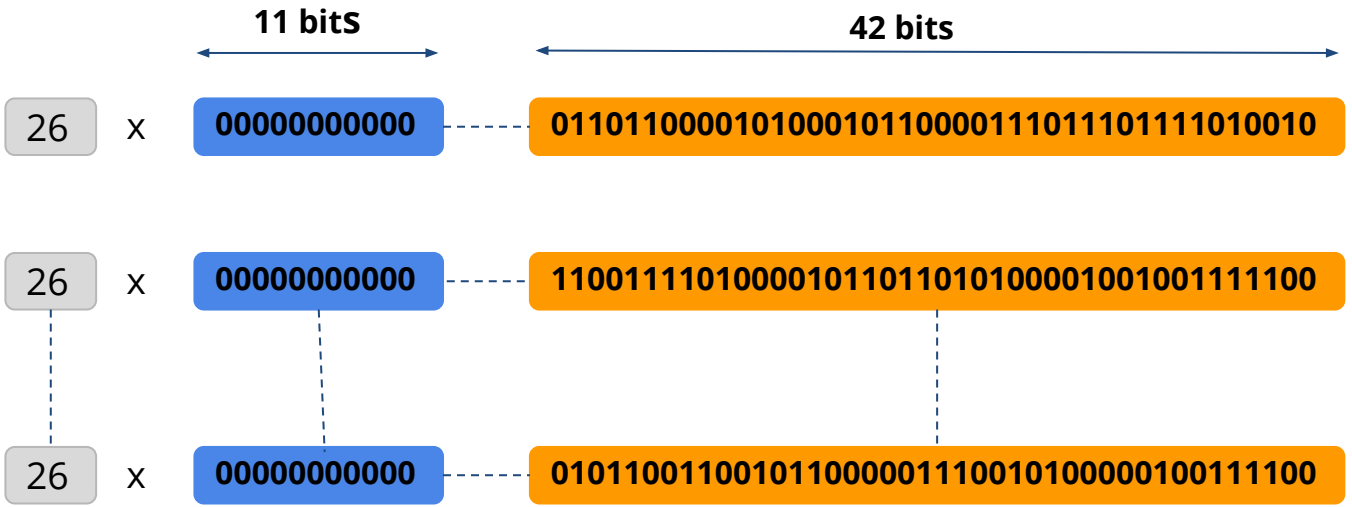
Time between prefix and message: 4 us
Time between message: 10 us

Deactivation

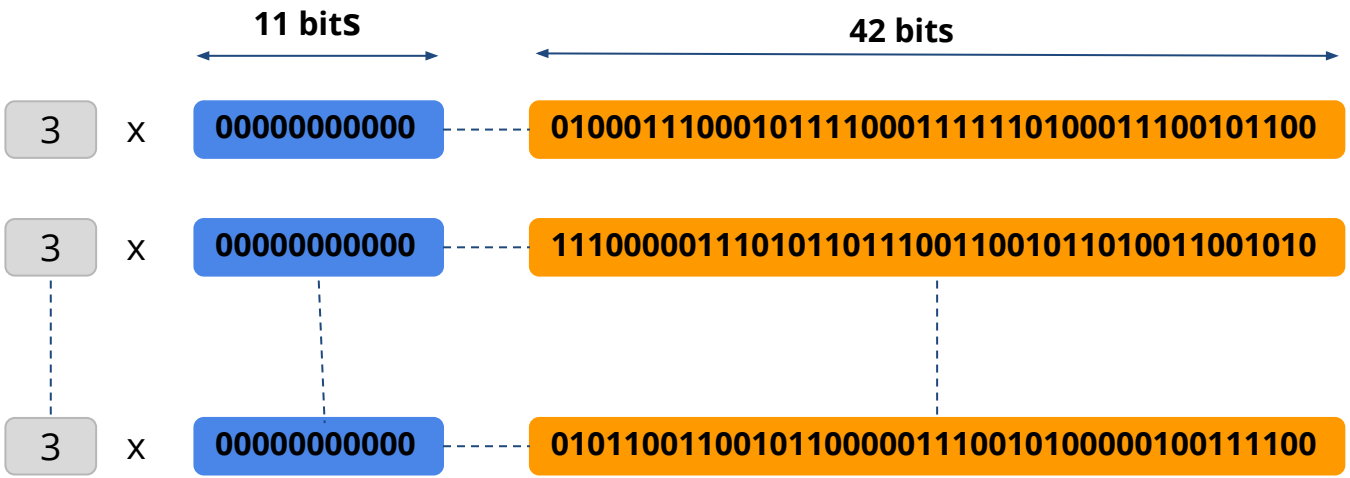


Time between prefix and message: 4us
Time between message: 10 us

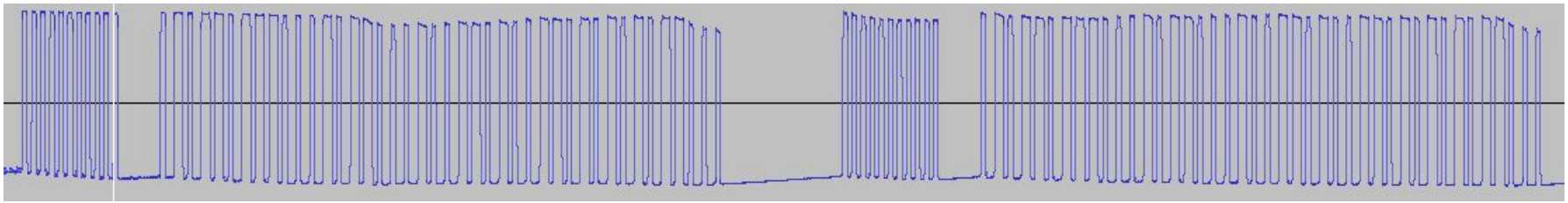
Assault activation



Houses’ garage



Time signal Low and High



Prefix

Bits

Time between messages

Methodology

1.CAPTURE

2. DECODE

8. DONE

6.COMPARE

7. not equal

3.BUILD

5.CAPTURE

4.SEND

Brute force attack

Microchip information

Magic Codes

Master codes

Code knocking

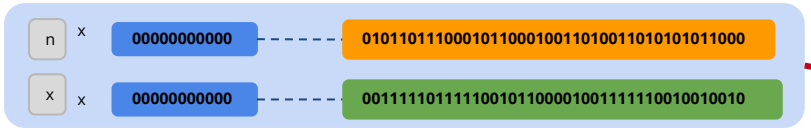
Capture between 5 signals from remote control

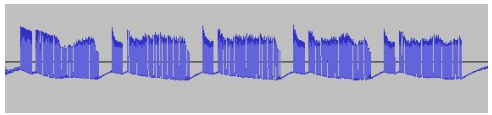
Decode the signals to Arduino

Try to hack

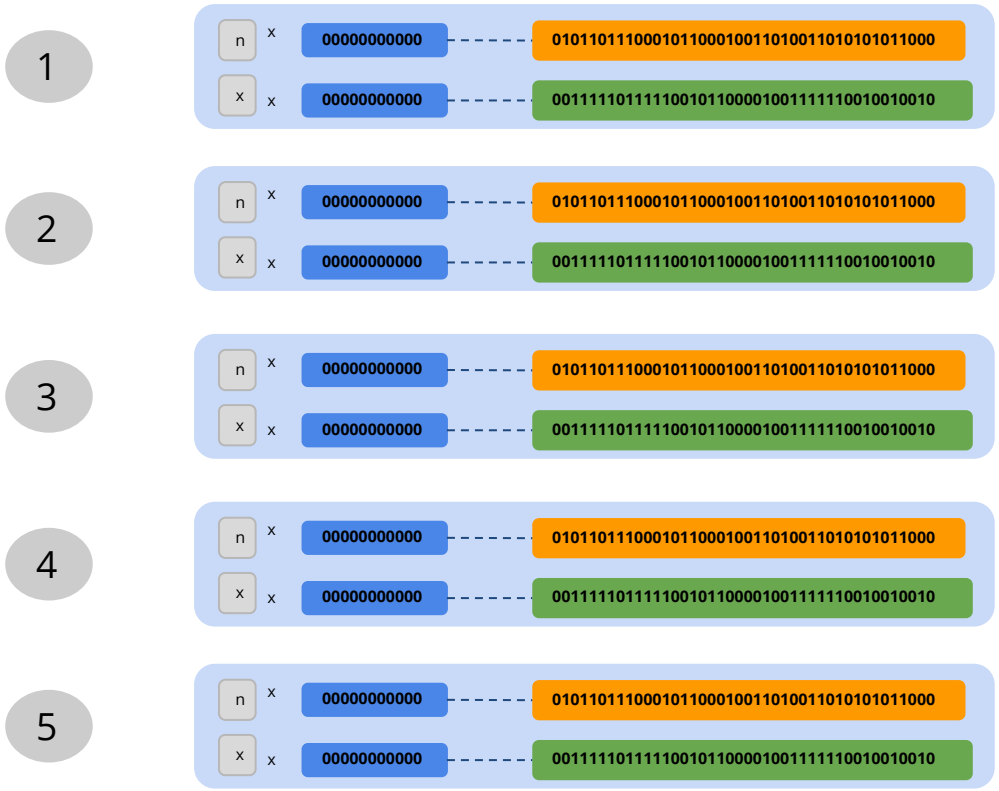
Code knocking

1



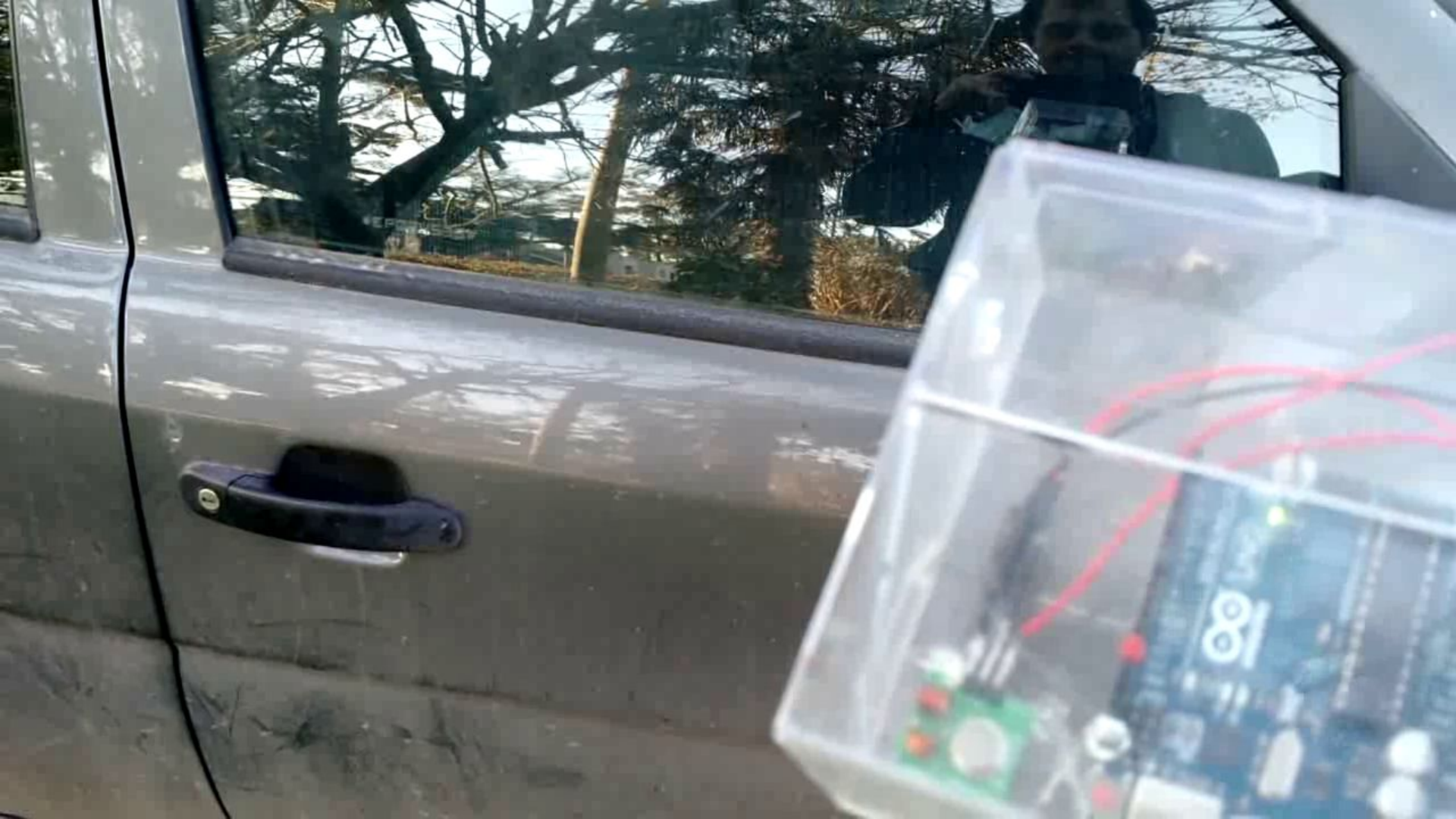


Code knocking



Code knocking

DEMO

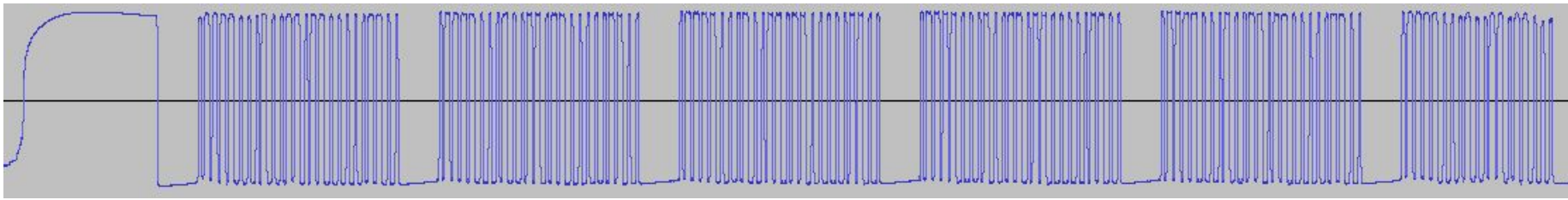


Supplier Case Two

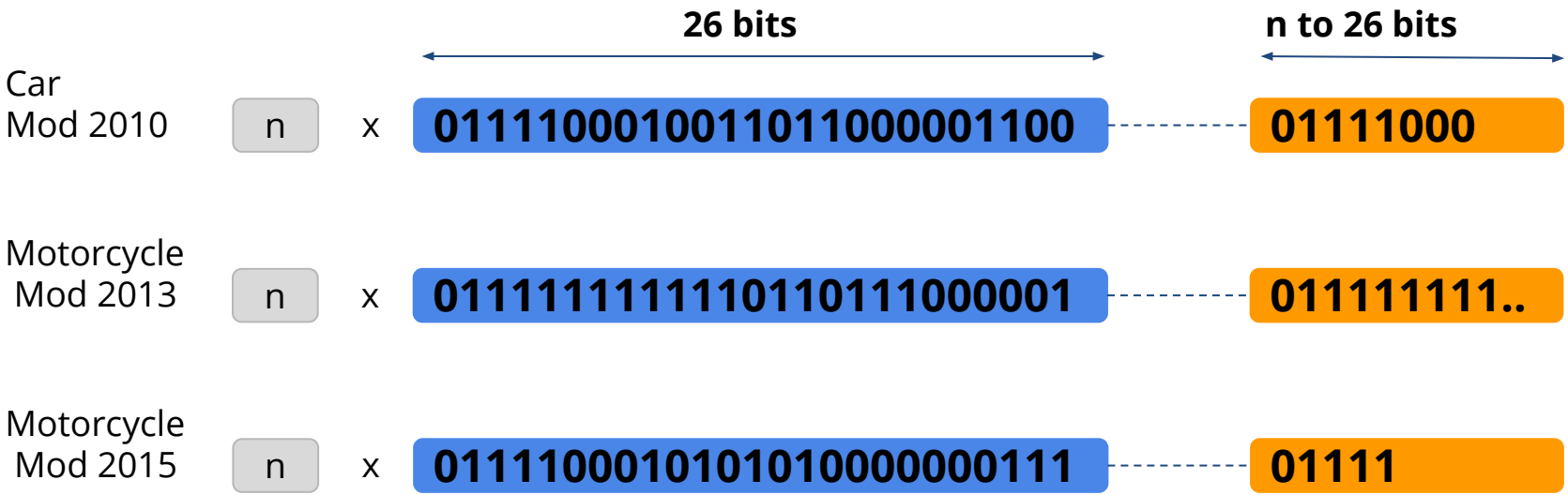
1.6

Millions

Supplier Case Two

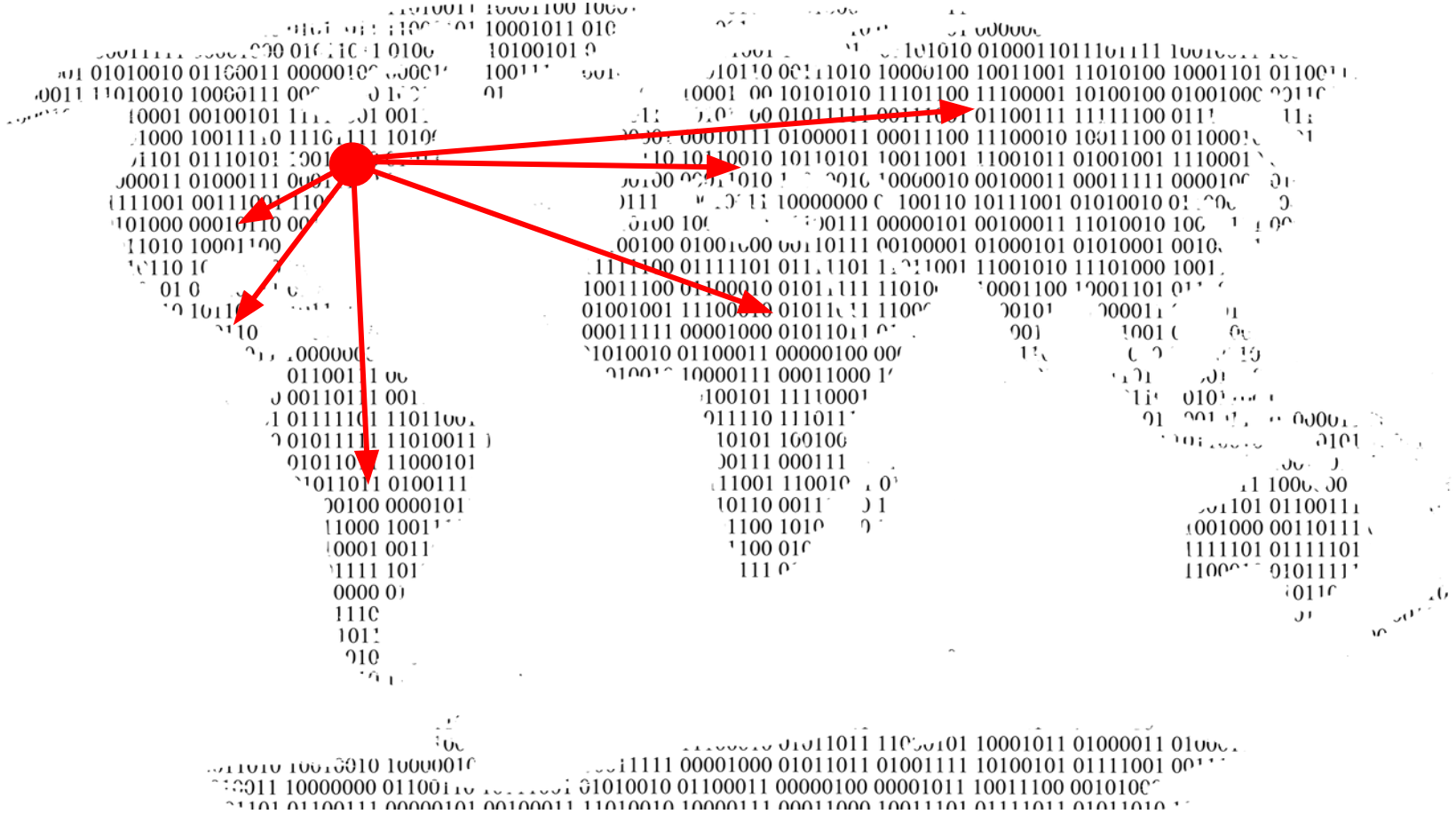


Supplier Case Two



DEMO

Supplier Case Three



WS4945

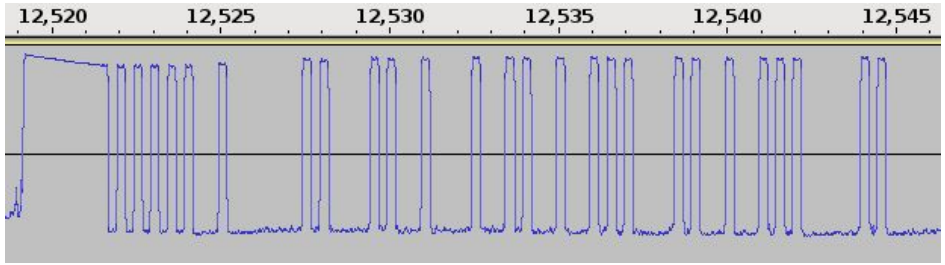
WS4904

WS4939

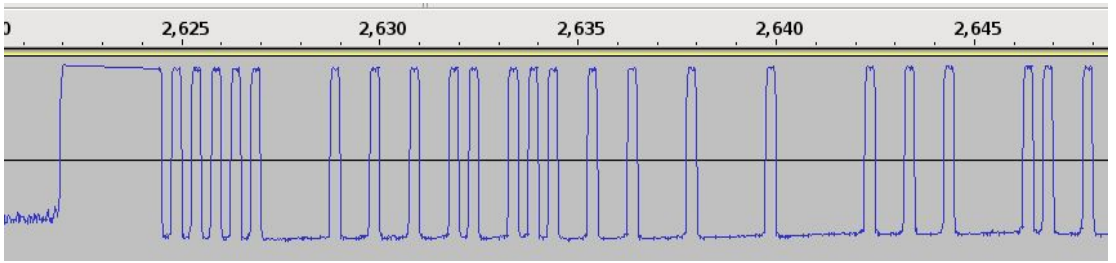
RF5132-433 compatible with
PC585, PC1616, PC1832 y PC1864 control panel. Frequency 433 MHz y 868 MHz

Motion Detectors

WS4904



Remote control



5 bits

39 bits

n x 00000 0101010010001010110111011110101011100 10


1250

SP Intrusion Support Global Email Routing
Fecha 2 de octubre de 2018, 20:44

Hello Mr. Ferrari,

Thanks for your concern. ***Power Series panels wireless devices are using one of the old wireless technology released back in early 2000s***...

We have released a **new product line Power Series NEO** with improved wireless Technology ...

Conclusions

Silent attacks

Problems with insurance companies

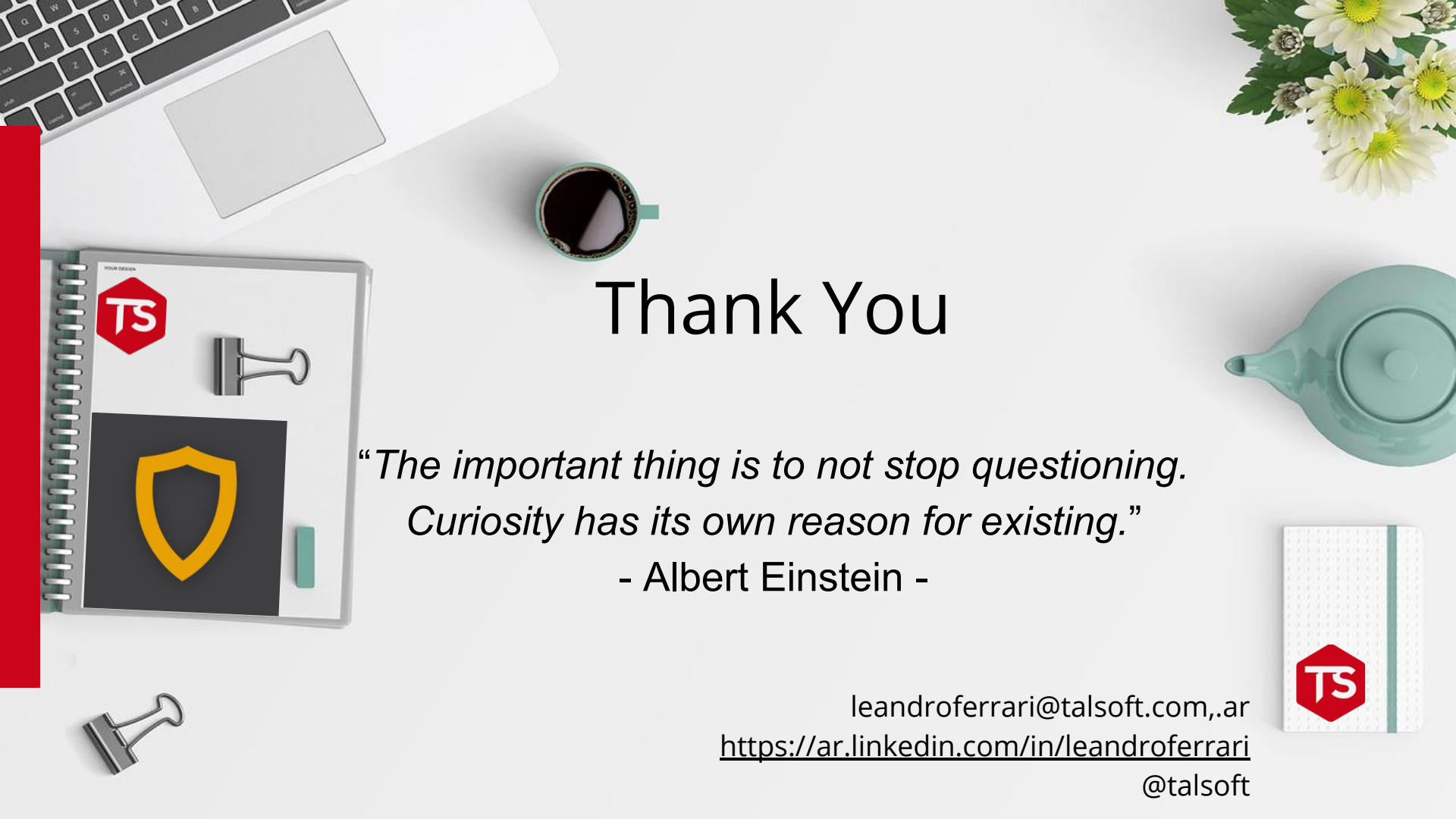
Reuse of the activated codes

Know the failures of this kind of alarms.

Do **yourself own tests** on security devices **to protect your owns**

Share your knowledge to help the **community**

It is everyone’s responsibility



Thank You

"*The important thing is to not stop questioning. Curiosity has its own reason for existing.*"

- Albert Einstein -

leandroferrari@talsoft.com,.ar
https://ar.linkedin.com/in/leandroferrari
@talsoft