Living in a fool's wireless-secured paradise

Stefan Kiese

Topics

- Wireless (consumer) alarm systems
- Hardware
- Software
- Hacking it ;)

About me

- Security Analyst @ ERNW
- Heidelberg, Germany
- Interested in hardware hacking, SDR, IoT
- Beard ;)
- Twitter: @net0SKi

www.ernw.de

www.troopers.de

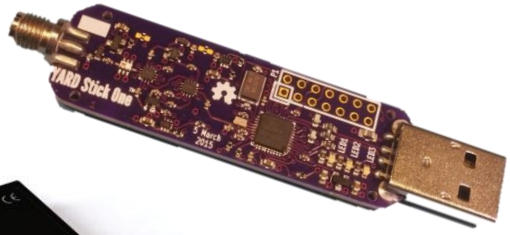
www.insinuator.net

Wireless (consumer) alarm systems

- Cheap ($10 - $250)
- Easy to get
- Easy to install
- WIRELESS
- Mostly, you get what you pay for

Hardware Tools

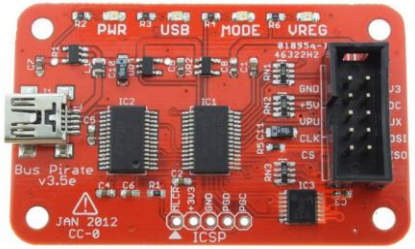
SDR:
HackRF One
Yardstick One

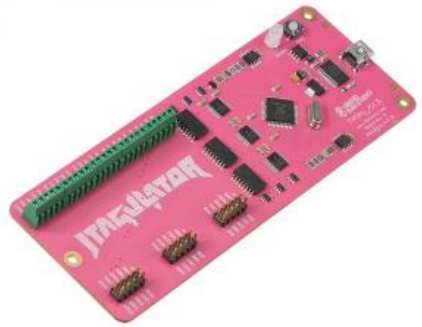


Logic Analyzer:
Intronix LogicPort LA1034

Scope:
Tektronix MSO2012B

All-rounder:
JTAGulator
Bus Pirate

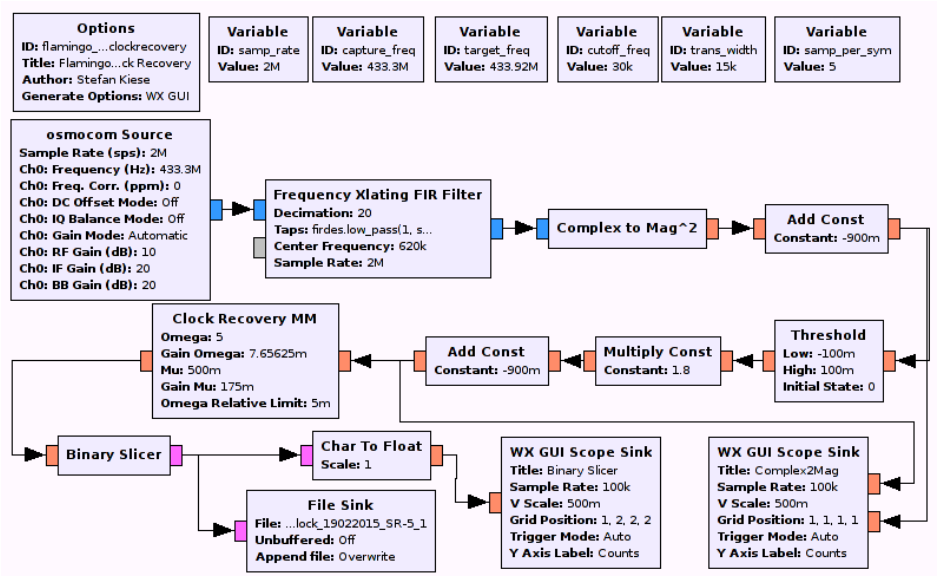




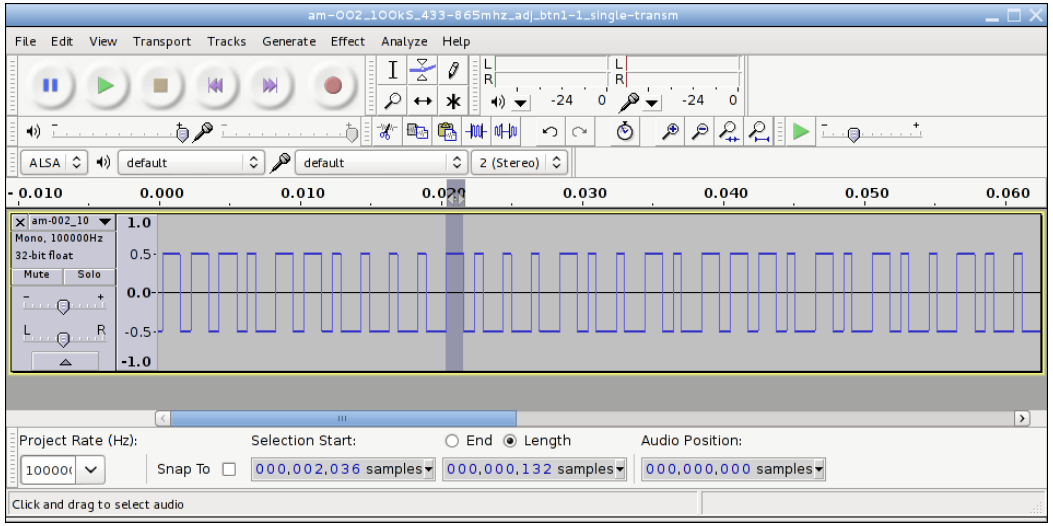
Pix' sources:
HackRF+YS, greatscottgadgets.com
LogicPort, pctestinstruments.com
MSO2012B, tek.com
JTAGulator, jtagulator.com
Bus Pirate v3, dangerousprototypes.com

Software Tools

GNU Radio Companion:



Audacity:



Other useful tools:

- E.g. minicom (for use of JTAGulator and BP)
- Sigrok or other LA-soft
- Baudline
- Rfcat
- Python

Usual attack vectors

- **Hardware:**
  - UART (Debug info, console)
  - SPI (e.g. r/w EEPROM)
  - JTAG (e.g. r/w flash, reprogram µC)
  - I^2C (e.g. comm. w/ components)
- **Over the air:**
  - Wifi
  - Bluetooth
  - Proprietary protocols

Comparison of the alarm systems

AS 1

- Many unidentified TPs exposed
- Simple record&replay
- Costs about $100

AS 2

- JTAG + UART exposed as TP
- Also simple record&replay
- Costs also about $100

AS 3

- No interfaces exposed
- Rolling Code implemented
- EEPROM
- Costs about $60

Alarm system 1

Loooong transmissions…

Alarm system 1

1. Let‘s start with a simple record&replay attack

→ successful

2. Trying to regain the RF transmission

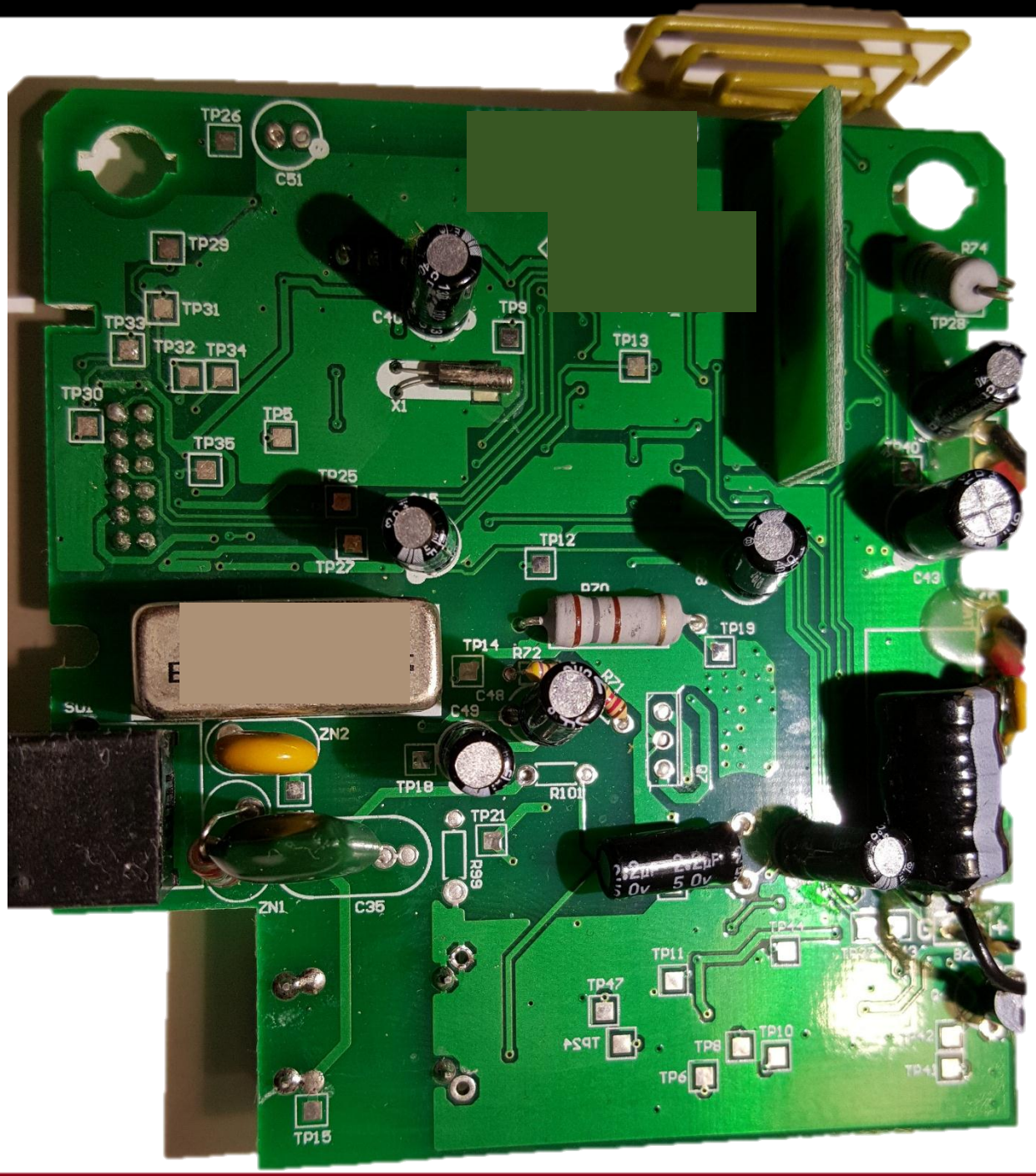
→ 288 Bits x 90, Manchester encoded

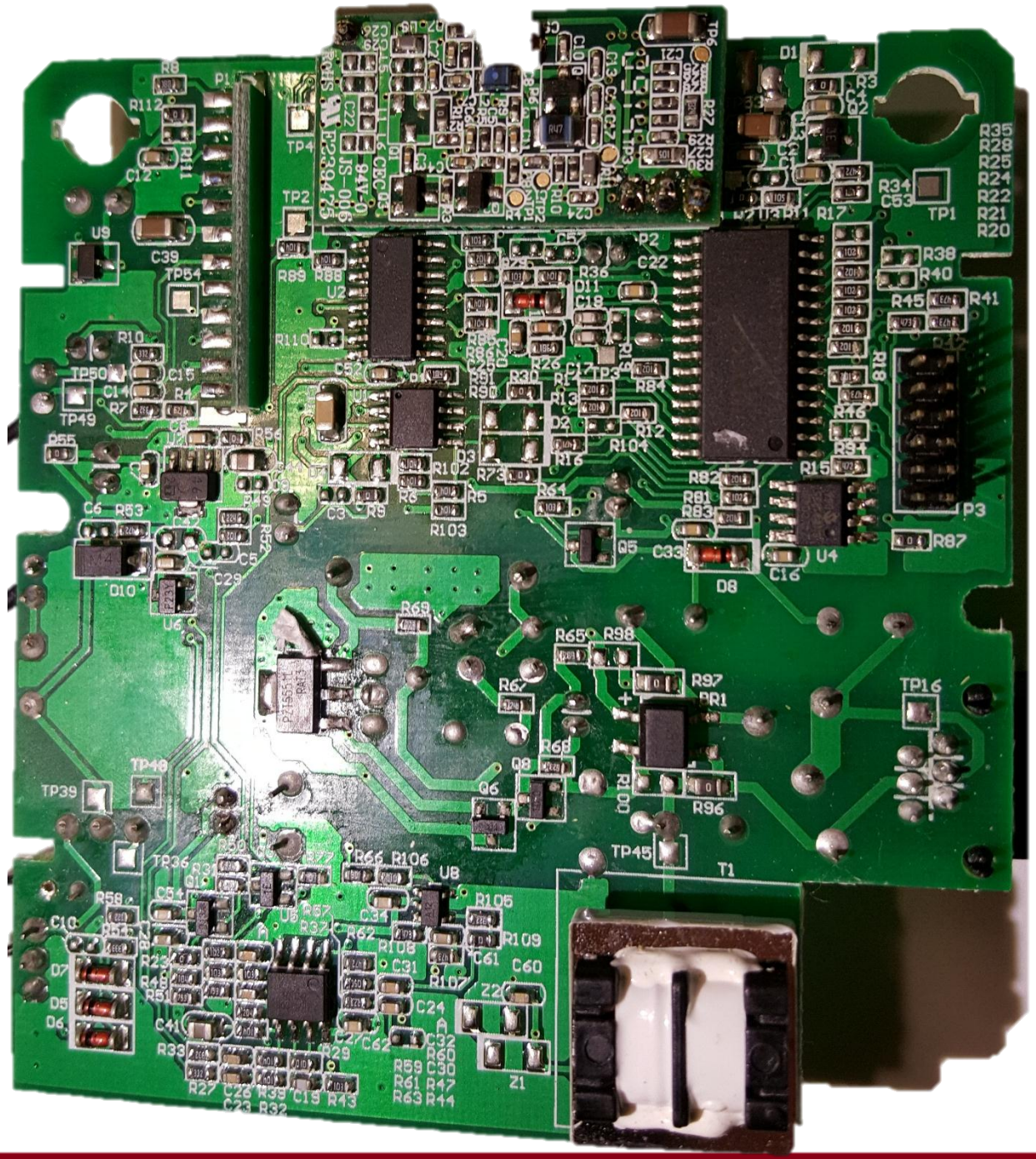
3. „Synthesizing“ signal in GNU Radio

→ successful

4. Manipulating messages

→ unsuccessful


TP26
C51
TP29
TP31
TP33
TP32
TP34
TP30
TP5
TP35
TP25
TP27
TP12
TP13
TP9
X1
R74
TP28
C43
TP19
TP14
R72
C48
C49
ZN2
TP18
R101
TP21
R99
ZN1
C35
TP11
TP47
TP10
TP8
TP6
TP15


D1
R3
C4
C2
R35
R28
R25
R24
R22
R21
R20
R34
C53
TP1
R17
R38
R40
R45
R41
R46
R87
P3
C33
C16
U4
D8
R82
R81
R83
R15
Q5
R64
R102
R103
R104
R12
R16
R84
R26
R30
R13
D2
D3
R73
R6
R5
C3
R9
C6
R53
C5
C29
D10
U6
R69
R65
R98
R97
R67
R68
Q8
Q6
R96
TP16
TP45
T1
TP48
TP39
TP36
R66
R106
U8
R105
R109
C61
C60
C31
R107
C24
C32
R60
R59
C30
R61
R47
R63
R44
Z1
C41
R33
R29
C27
C62
R27
C26
R35
C19
R43
C23
R32
R58
C10
D7
D5
D6
R22
R48
R51
C54
R37
C34
R62
R108
R112
C12
R11
TP4
TP2
U9
C39
TP54
R89
R88
U2
R110
R10
TP50
C14
R7
TP49
C15
R4
R56
C52
R90
R91
R1
R3
R2
C22
R36
D11
C18
R85
R86
R25
R24
R23
R18
R46
R94
R15
R82
R81
R83
R64
R102
R103
R104
R12
R16
R84
R26
R30
R13
D2
D3
R73
R6
R5
C3
R9
C6
R53
C5
C29
D10
U6
R69
R65
R98
R97
R67
R68
Q8
Q6
R96
TP16
TP45
T1
TP48
TP39
TP36
R66
R106
U8
R105
R109
C61
C60
C31
R107
C24
C32
R60
R59
C30
R61
R47
R63
R44
Z1
C41
R33
R29
C27
C62
R27
C26
R35
C19
R43
C23
R32
R58
C10
D7
D5
D6
R22
R48
R51
C54
R37
C34
R62
R108
R112
C12
R11
TP4
TP2
U9
C39
TP54
R89
R88
U2
R110
R10
TP50
C14
R7
TP49
C15
R4
R56
C52
R90
R91
R1
R3
R2
C22
R36
D11
C18
R85
R86
R25
R24
R23
R18
R46
R94

Alarm system 2

You shouldn‘t be allowed to issue this CMD, dude!

Alarm system 2

1. Record&replay again…

→ successful

2. Motion Detector is allowed to disarm the base

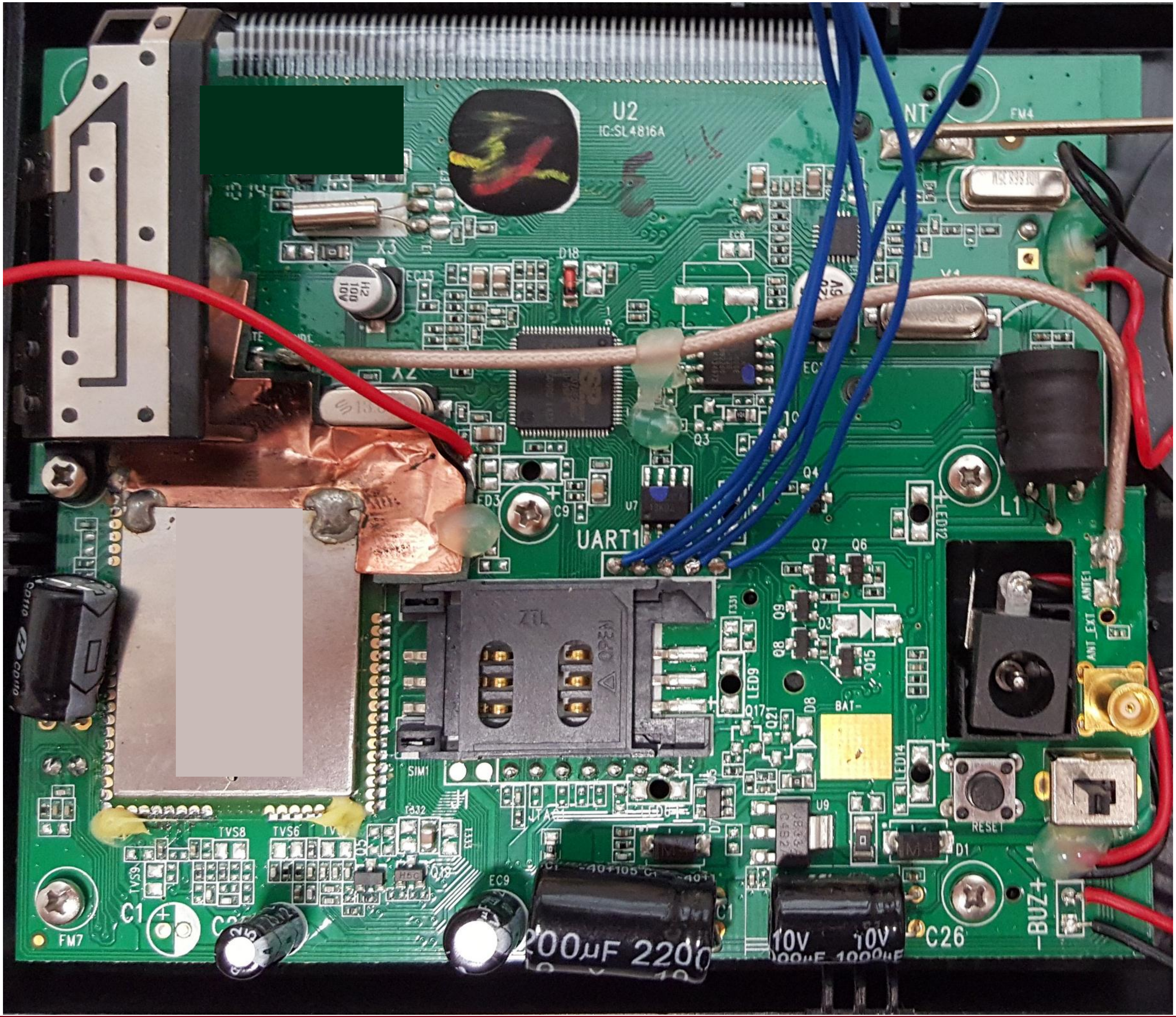
→ Just bruteforce the Device ID

3. JTAGulating UART

→ 2 UARTs exposed, no „valid“ output on common baudrates

4. JTAGulating JTAG

→ unsuccessful


U2
IC:SL4816A
UART1
SIM1
RESET
L1
BAT-
C26
BUZ+

Alarm system 3

Keep on rollin‘, baby!

Alarm system 3

1. Record&replay again…

→ unsuccessful

2. Trying to regain the RF transmission

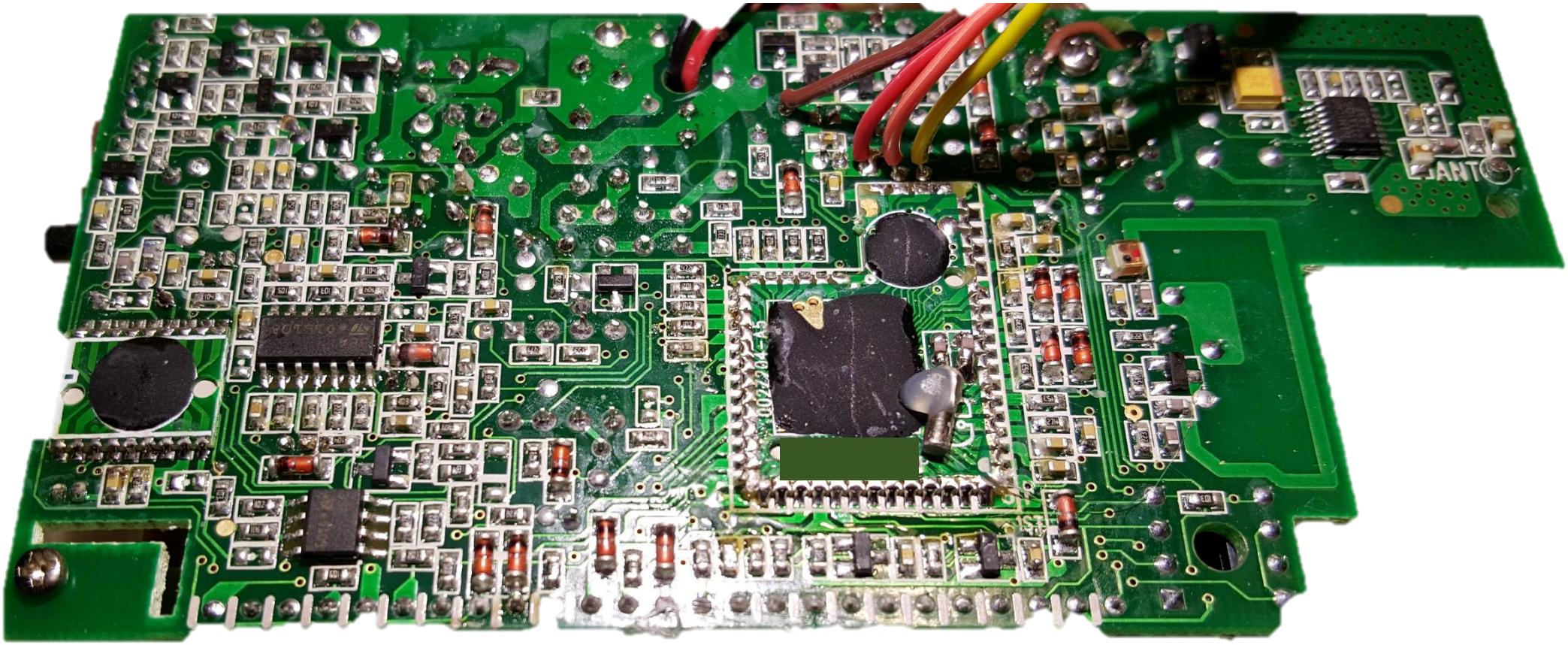
→ 65 bits x 6, two-parted Rolling Code

3. Some interesting unlabelled ICs on PCB

→ acc. to russian board one for signal horn

4. EEPROM

→ Connected to µC via SPI; no results yet



What could vendors do better?

- Use Rolling Code
- Remove IDs from ICs
- Use two-way communication
- Use encryption
- Be aware of the comm. protocols
- Use anti-tampering techniques
- Send keep-alive packets

Any questions?

ERNW
providing security.

Thanks for your…

…and have a nice day!