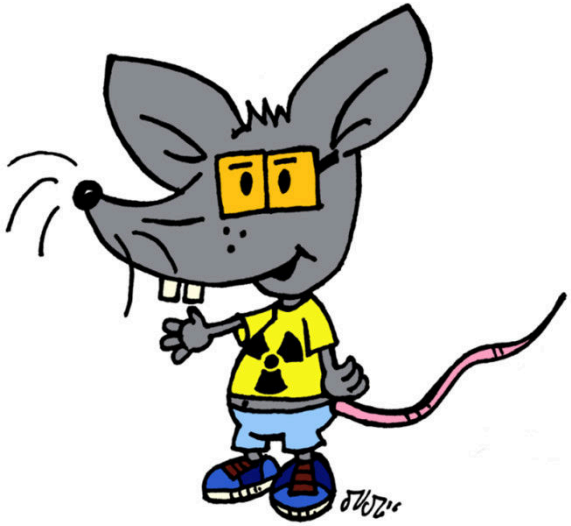
Software Defined Radio: Weniger Theorie, mehr Praxis

SYSS THE PENTEST EXPERTS.

SICHERHEITS KONFERENZ



Who am I?

Dipl.-Inf. Matthias Deeg

Expert IT Security Consultant

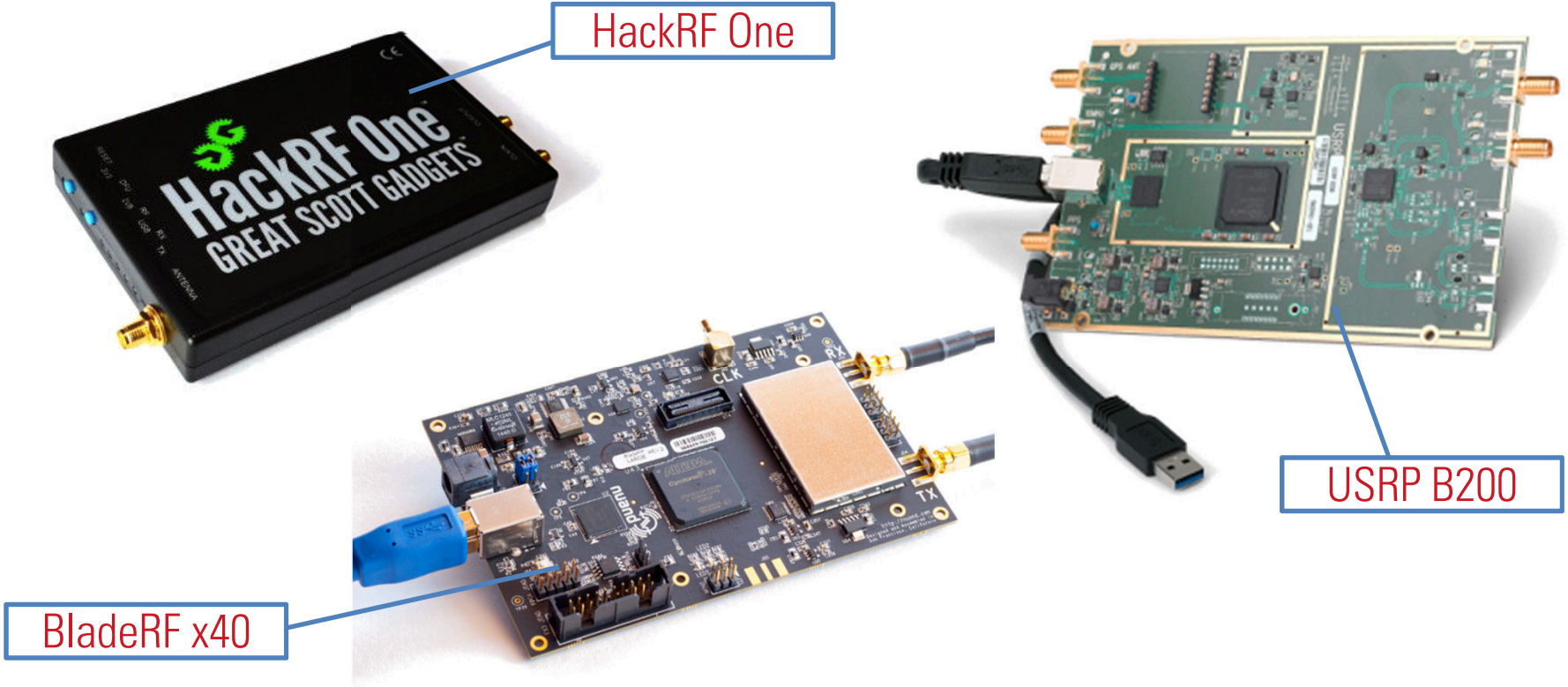
CISSP, CISA, OSCP, OSCE

- Großes Interesse an Informationstechnik – insbesondere Informationssicherheit
- Studium der Informatik an der Universität Ulm
- IT-Security Consultant bei der SySS GmbH seit 2007
- Leiter Forschung & Entwicklung

Agenda

1. SDR-Hardware
2. SDR-Software
3. SDR-Herausforderungen
4. SDR-Testmethodik
5. SDR Hacking by Example
6. Fragen & Antworten

SDR-Hardware



SDR-Software

- GNU Radio (https://www.gnuradio.org/)
- GNU Radio Companion (https://www.gnuradio.org/)
- osmocom_fft (https://github.com/osmocom/gr-osmosdr/blob/master/apps/osmocom_fft)
- inspectrum (https://github.com/miek/inspectrum)
- baudline (http://www.baudline.com/)
- Universal Radio Hacker (https://github.com/jopohl/urh)
- diverse Python-Skripte

SDR-Herausforderungen

- Mathematische Grundlagen
- Grundlagen der digitalen Signalverarbeitung
- Modulationsverfahren (AM/ASK, FM/FSK, PM/PSK und Kombinationen davon)
- Zahlreiche Funkstandards
- Zahlreiche Funkprotokolle (offen und proprietär)
- Zuverlässige Werkzeuge (Hard- und Software)
- Effizienter Workflow

SDR-Testmethodik

SySS THE PENTEST EXPERTS.

1. Hardware-Analyse

   PCBs analysieren, Chips identifizieren, Datenblätter studieren, interessante Schnittstellen finden (z. B. UART, SPI, I2C, JTAG), Speicherchips auslesen, …

2. Firmware-Analyse

   Firmware disassemblieren, SDKs nutzen, Code lesen/schreiben/analysieren, Tests mit eigener Hardware (Evaluation Boards), …

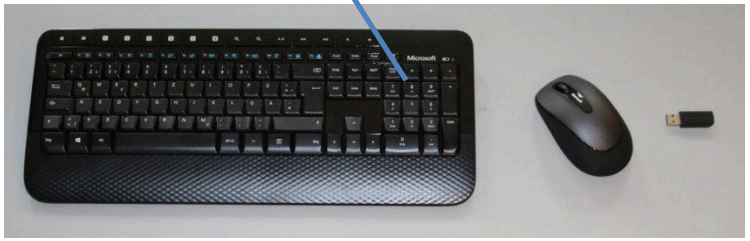
3. Funkbasierte Analyse

   Funkkommunikation aufzeichnen, Funksignal analysieren, Funkempfänger (Receiver) entwickeln/beschaffen, Funksender (Transmitter) entwickeln/beschaffen, Antwortverhalten untersuchen, …

SDR Hacking by Example

Finden und Ausnutzen von Schwachstellen in ausgewählten Produktkategorien:

Wireless Desktop Set

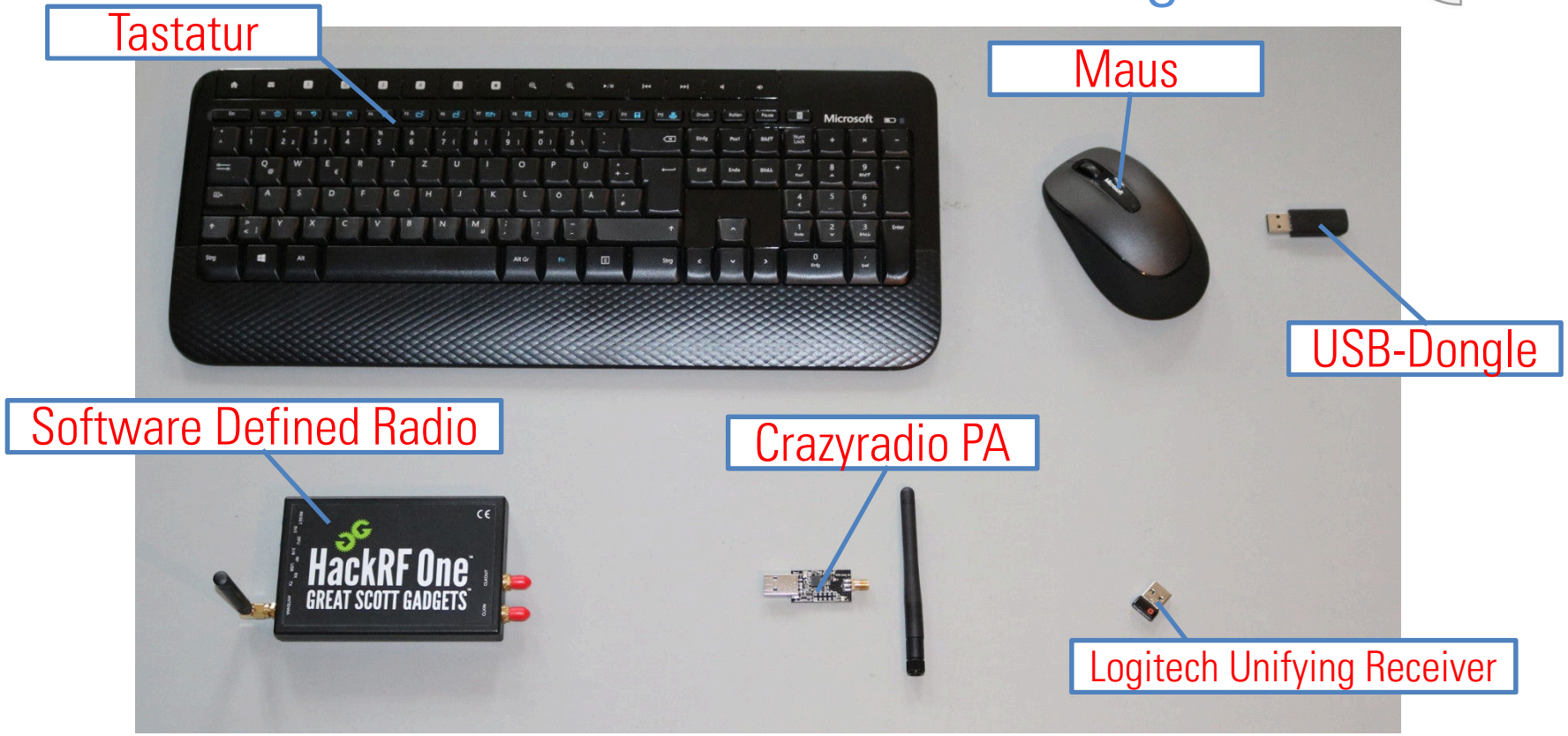


Wireless Alarm System

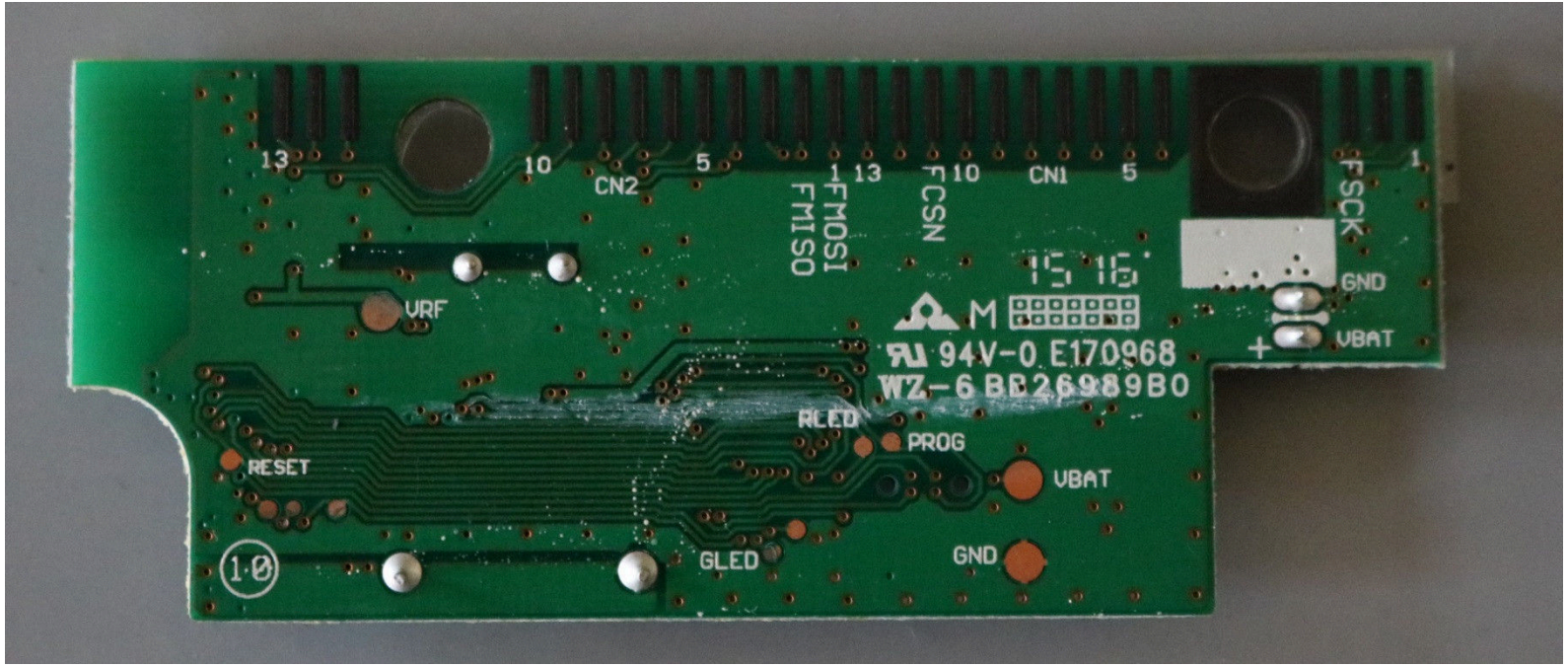
Wireless Presenter

Beispiel 1: Wireless Desktop Sets

Kurzer Überblick verwendeter Technologien

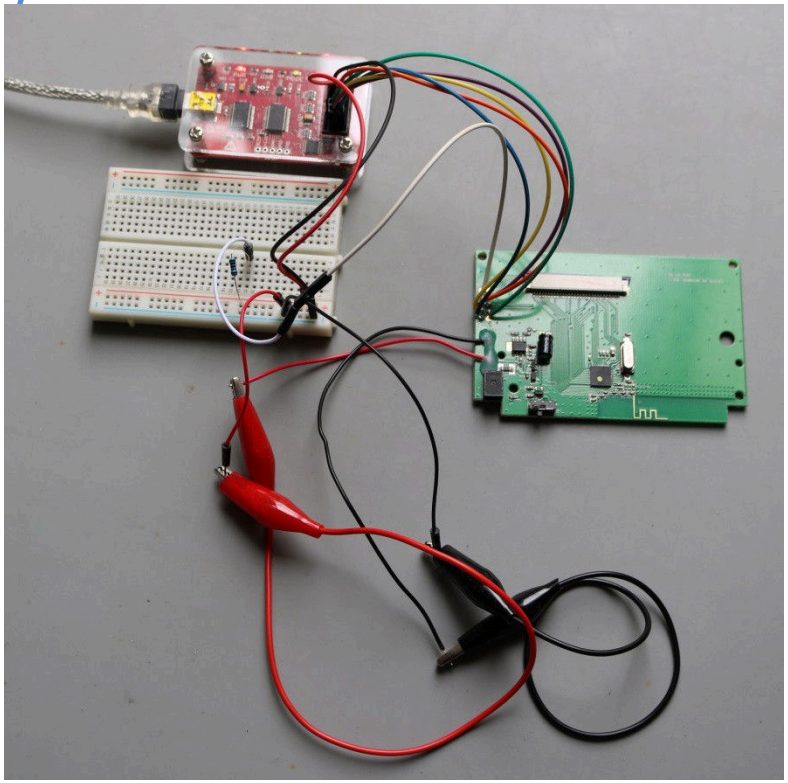


Hardware-Analyse



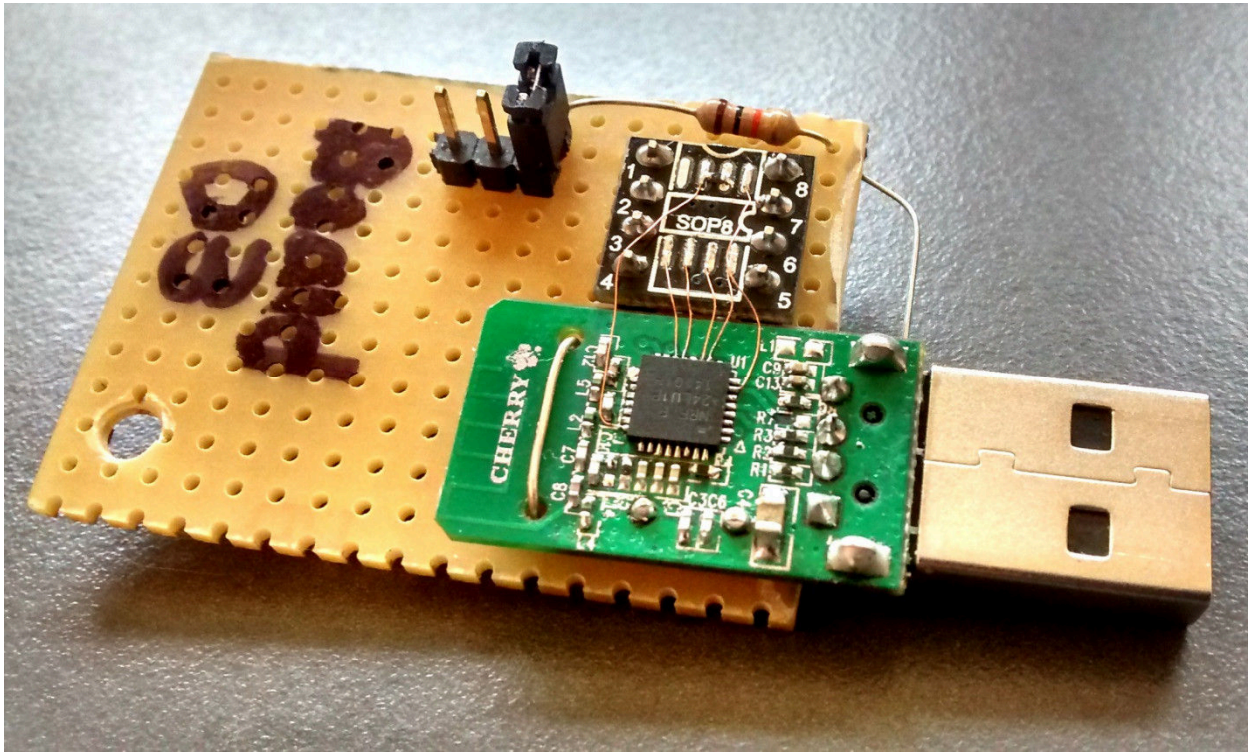
PCB-Rückseite einer Microsoft-Funktastatur

Firmware-Analyse



Lesender und schreibender Zugriff via SPI auf eine Cherry-Funktastatur

Firmware-Analyse



Lesender und schreibender Zugriff auf Cherry-Dongle via SPI (Dank an Alexander Straßheim)

Firmware-Analyse

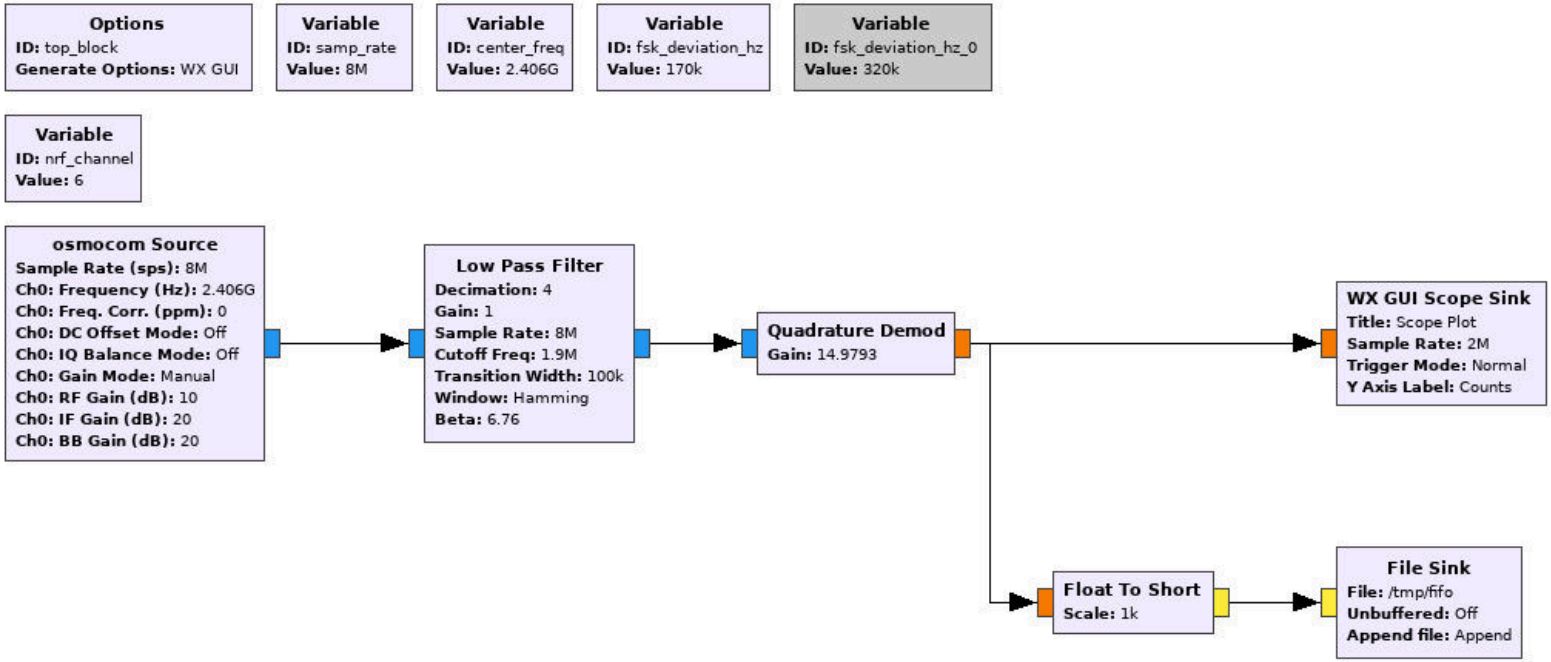
- IDA Pro und Nordic Semiconductor's nRF24 SDK waren sehr hilfreich bei der Firmwareanalyse der Funktastaturen

```
2367
2367                        code_2367:
2367 12 21 13               lcall   add_sub_shift
236A 12 1D DF               lcall   mix_columns_hw
236D AF 2F                  mov     R7, RAM_2F
236F 12 1E 94               lcall   key_upgrade
2372 05 2F                  inc     RAM_2F
2374 E5 2F                  mov     A, RAM_2F
2376 C3                     clr     C
2377 94 09                  subb    A, #9
2379 40 EC                  jc      code_2367
```

```
237B 12 21 13               lcall   add_sub_shift
237E 7F 09                  mov     R7, #9
2380 12 1E 94               lcall   key_upgrade
2383 12 2A 09               lcall   add_key
2386 E4                     clr     A               ; A = 0
2387 F5 2F                  mov     RAM_2F, A       ; init counter, RAM_2F = 0
```

Auszug der disassemblierten Cherry-Firmware (hal_aes_crypt)

Funkbasierte Analyse



Einfacher GNU Radio Companion Flow Graph für die Verwendung mit NRF24-BTLE-Decoder

Funkbasierte Analyse

- Zunächst Verwendung von GNU Radio mit ein paar Python-Skripten und einer modifizierten Version von NRF24-BTLE-Decoder

```
$ cat /tmp/fifo | ./nrf24-decoder -d 1
nrf24-decoder, decode NRF24L01+ v0.1

Address: 0xAD2D54CB8B length:11, pid:0, no_ack:1, CRC:0xAAB9 data:D149491545452AAA248925
Address: 0xAB5554B46B length:29, pid:1, no_ack:0, CRC:0xDFA5
data:D55AD4B55A956A554BDCDD6D5A956554ACAD55ACAD4AACA9555DF5F7D9
Address: 0x6BB7E29E31 length:16, pid:0, no_ack:0, CRC:0x2D58 data:0294EF5368E70FB11AB685B818819388
Address: 0x6BB7E29E31 length:16, pid:0, no_ack:0, CRC:0x2D58 data:0294EF5368E70FB11AB685B818819388
Address: 0x6BB7E29E31 length:16, pid:0, no_ack:0, CRC:0x2D58 data:0294EF5368E70FB11AB685B818819388
(...)
Address: 0x5535D0A4B5 length:21, pid:1, no_ack:1, CRC:0x38C9
data:32C4B1A925A4D7252EACB29AC7354AC6C9425A552B
Address: 0x6BB7E29E31 length:16, pid:0, no_ack:0, CRC:0x2D58 data:0294EF5368E70FB11AB685B818819388
Address: 0x6BB7E29E31 length:16, pid:0, no_ack:0, CRC:0x2D58 data:0294EF5368E70FB11AB685B818819388
Address: 0x6BB7E29E31 length:16, pid:0, no_ack:0, CRC:0x2D58 data:0294EF5368E70FB11AB685B818819388
(...)
```

Funkbasierte Analyse

- Nach der MouseJack-Veröffentlichung im Februar 2016 Nutzung von Bastille's nRF24-Toolset (Vielen Dank an Marc Newlin)
  - Bitcraze Crazyradio PA
  - Bastille's nrf-research-firmware
  - nrf24-sniffer und nrf24-scanner
- Entwicklung von Python-Tools unter Verwendung von Crazyradio PA und nrf-research-firmware

Gefundene Schwachstellen

1. Unzureichender Schutz von Code (Firmware) und Daten (kryptografisches Schlüsselmaterial)

   ⇒ *Zugriff auf sensible Daten mit physischem Zugriff*

2. Unverschlüsselte und nicht authentifizierte Funkkommunikation der Maus

   ⇒ *Mouse Spoofing Attacks*

3. Fehlender bzw. unzureichender Schutz vor Replay-Angriffen

   ⇒ *Replay Attacks*

4. Fehlerhafte Implementierung der AES-Verschlüsselung

   ⇒ *Keystroke Injection Attacks*

Gefundene Schwachstellen

SyS THE PENTEST EXPERTS.

Zusammenfassung unserer Ergebnisse

Produktname	Insufficient Code/Data Protection	Mouse Spoofing	Replay	Keystroke Injection
Cherry AES B.UNLIMITED	✓	✓	✓	✓
Fujitsu Wireless Keyboard Set LX901	?	?	✓	?
Logitech MK520	X	✓	✓	✓*
Microsoft Wireless Desktop 2000	✓	✓	✓	X
Perixx PERIDUO-710W	✓	✓	✓	✓

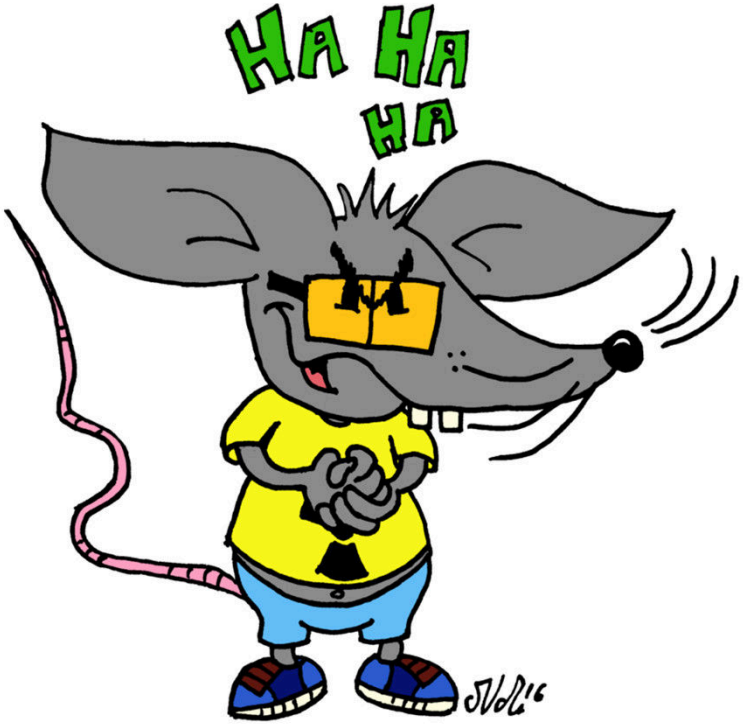
✓ Sicherheitsproblem vorhanden

X Sicherheitsproblem nicht vorhanden

? Existenz des Sicherheitsproblems noch unklar

* zuerst von Bastille Networks gefunden und gemeldet

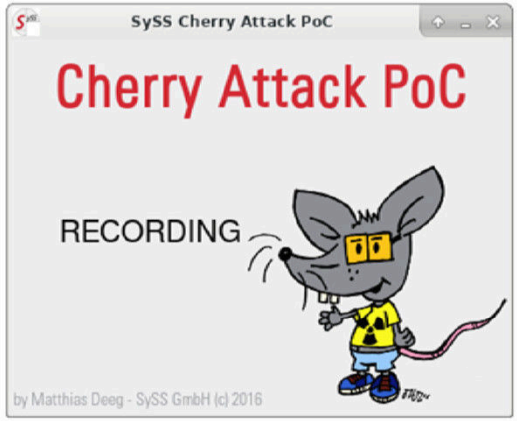
Demo Time



„One small keystroke injection for me, one giant injection attack for mousekind.“

Keystroke Injection-Angriff

```
[root@hackbox nrf24_playset]# python cherry_attack.py
[2016-10-10 12:38:35.779]  Start Cherry Attack v1.0
[2016-10-10 12:38:40.409]  Found keyboard with address 6B:B7:E2:9E:31
[2016-10-10 12:38:41.456]  Received payload: 88e0f93414916ad7c8ca531dfbd663d3
[2016-10-10 12:38:41.546]  Received payload: 8b97b4c62f2fce74f2021ff90870177a
[2016-10-10 12:38:42.272]  Received payload: 596e29b11353aa645341eb30a24ac78b
[2016-10-10 12:38:42.393]  Received payload: c1b16d5ab68ba9f5211ffbdc54f4e3e2
[2016-10-10 12:38:43.697]  Received payload: e4cf505f1d5d106361f9fcb3fe81636f
[2016-10-10 12:38:43.748]  Received payload: eda153b3b8e35d5ecf8837d2dca1436d
[2016-10-10 12:38:45.748]  Got crypto key!
[2016-10-10 12:38:45.748]  Initialize keyboard
[2016-10-10 12:38:55.217]  Received payload: 428ea391a48dbc1c144065c16d08c424
[2016-10-10 12:38:55.255]  Received payload: c9fed3bcfb2180b71d9e079626ada8c8
[2016-10-10 12:38:55.631]  Received payload: 0d46706d0989ac01f2542477e9e4d553
[2016-10-10 12:38:55.691]  Received payload: 91d07c67ed626a89b5d06730102fea57
[2016-10-10 12:38:55.871]  Received payload: 7883d4eb40984f1cd8ece6ea85528614
[2016-10-10 12:38:55.940]  Received payload: bcc20df7b43ee11bab74bb40e9929acd
[2016-10-10 12:38:56.151]  Received payload: 6f9210a70a74bf2a4419accde790f1f1
[2016-10-10 12:38:56.208]  Received payload: cc4d863733b389db7ccf406e517dd19e
[2016-10-10 12:39:02.632]  Received payload: be15865ba027a73287351e7ccf1d314a
[2016-10-10 12:39:02.690]  Received payload: 5c671e64b5ff27d73731859f10dad4e5
[2016-10-10 12:39:02.752]  Received payload: e9ec98ef38129941643a26b1bbe55500
[2016-10-10 12:39:02.897]  Received payload: 122080c94dfd0beb3f0fe33e1b2dec19
[2016-10-10 12:39:02.975]  Received payload: ab95951dad0495919aa4e6893d5deb64
[2016-10-10 12:39:03.028]  Received payload: 01a0bf262707945c2e43d4f5b79b3a78
[2016-10-10 12:39:03.074]  Received payload: b197e871a45a2f1629bb89e5a04cf60d
[2016-10-10 12:39:03.124]  Received payload: f42720acfffdf0f52ba4da2d02af0fd9
[2016-10-10 12:39:03.193]  Received payload: ac230d666e6312eff27ea1df1ac2b675
[2016-10-10 12:39:03.301]  Received payload: 05bb4b188bfc8a423028a52a3c4327fb
[2016-10-10 12:39:03.353]  Received payload: edddb970bb1eec7444a8672158d98084
[2016-10-10 12:39:03.473]  Received payload: 8967ea565c8195e24729d10615b86dc9
[2016-10-10 12:39:03.504]  Received payload: 9155046f0c85bd599c1c2b8a73b9b844
```



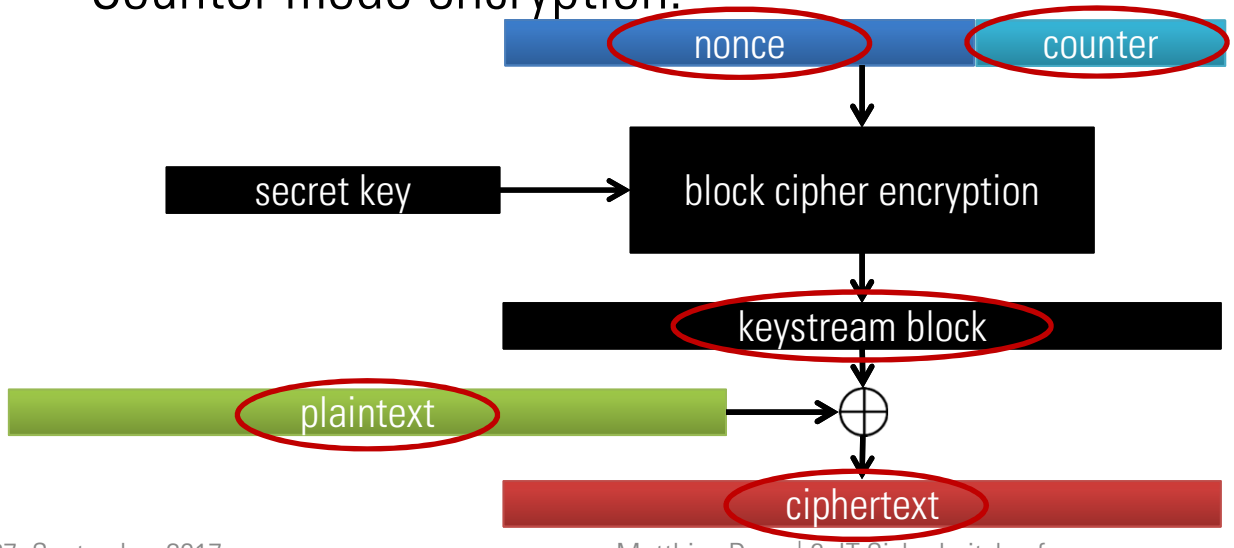
Keystroke Injection-Angriff

- Der Klartext eines Key-Release-Pakets ist wie folgt:

00	00	00	00	00	00	00	00	00	00	00

(11 NULL bytes)

- Counter mode encryption:



Beispiel 2: Wireless Presenter

SySS THE PENTEST EXPERTS.

- Nicht nur Funktastaturen und -mäuse sind von diesen Schwachstellentypen betroffen, sondern auch kabellose Präsentationsgeräte (Wireless Presenter)
- Im Rahmen eines Forschungsprojekt wurden die folgenden fünf Wireless Presenter untersucht:
  1. Logitech Wireless Presenter R400
  2. Targus Multimedia Presentation Remote
  3. August LP205R
  4. Inateck Wireless Presenter
  5. Kensington Presenter Expert (K72425EU)
- Der Fokus der Analyse lag hierbei auf *Keystroke Injection Attacks*

Gefundene Schwachstellen

SySS THE PENTEST EXPERTS.

Zusammenfassung unserer Ergebnisse

Produktname	Keystroke Injection
Logitech Wireless Presenter R400	✓
Targus Multimedia Presentation Remote	✓
August LP205R	X
Inateck Wireless Presenter	X
Kensington Presenter Expert (K72425EU)	X

✓ Sicherheitsproblem vorhanden

X Sicherheitsproblem nicht vorhanden

? Existenz des Sicherheitsproblems noch unklar

Demo Time

„When your wireless presenter knows more buttons than you can press, you may have a security problem."

Keystroke Injection-Angriff

- Proof-of-Concept Software Software-Tool für Keystroke Injection-Angriffe

```
# python logitech_presenter.py -a 77:E3:96:AC:07

        _____  ______ ___  _  _     _____  _                      _
       |  __ \|  ____|__ \| || |   |  __ \| |                    | |
  _ __ | |__) | |__     ) | || |_  | |__) | | __ _ _   _ ___  ___| |_
 | '_ \|  _  /|  __|   / /|__   _| |  ___/| |/ _` | | | / __|/ _ \ __|
 | | | | | \ \| |     / /_   | |   | |    | | (_| | |_| \__ \  __/ |_
 |_| |_|_|  \_\_|    |____|  |_|   |_|    |_|\__,_|\__, |___/\___|\__|
                                                    __/ |
                                                   |___/
Logitech Wireless Presenter Attack Tool v1.0 by Matthias Deeg - SySS GmbH (c) 2016
[*] Configure nRF24 radio
[*] Scanning for Logitech wireless presenter ...
[+] Found nRF24 device with address 77:E3:96:AC:07 on channel 32
[*] Press <CTRL+C> to start keystroke injection
^C
[*] Start keystroke injection ...
[*] Done.
```

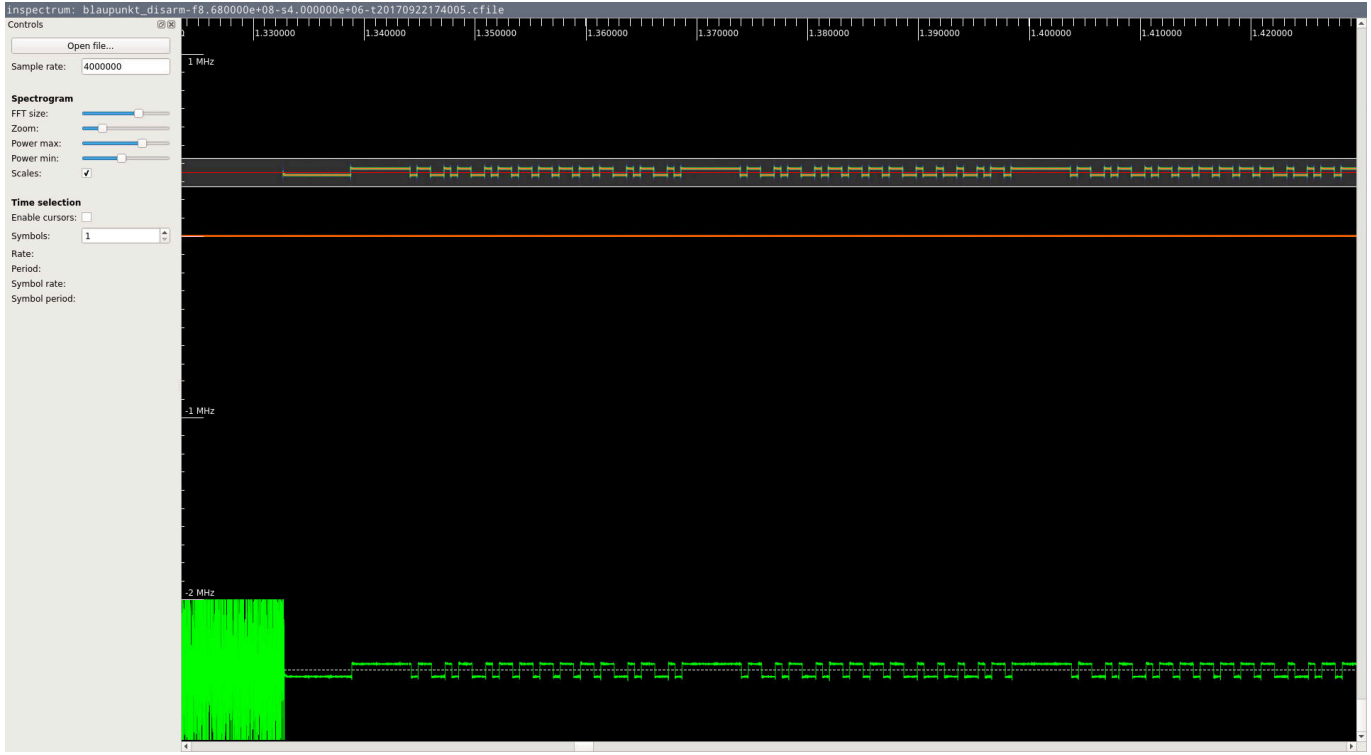
Beispiel 3: Wireless Alarm Systems

(Quelle: http://multikontrade.de/GSM-Funk-Alarmanlage#&gid=1&pid=1

Wireless Alarm Systems

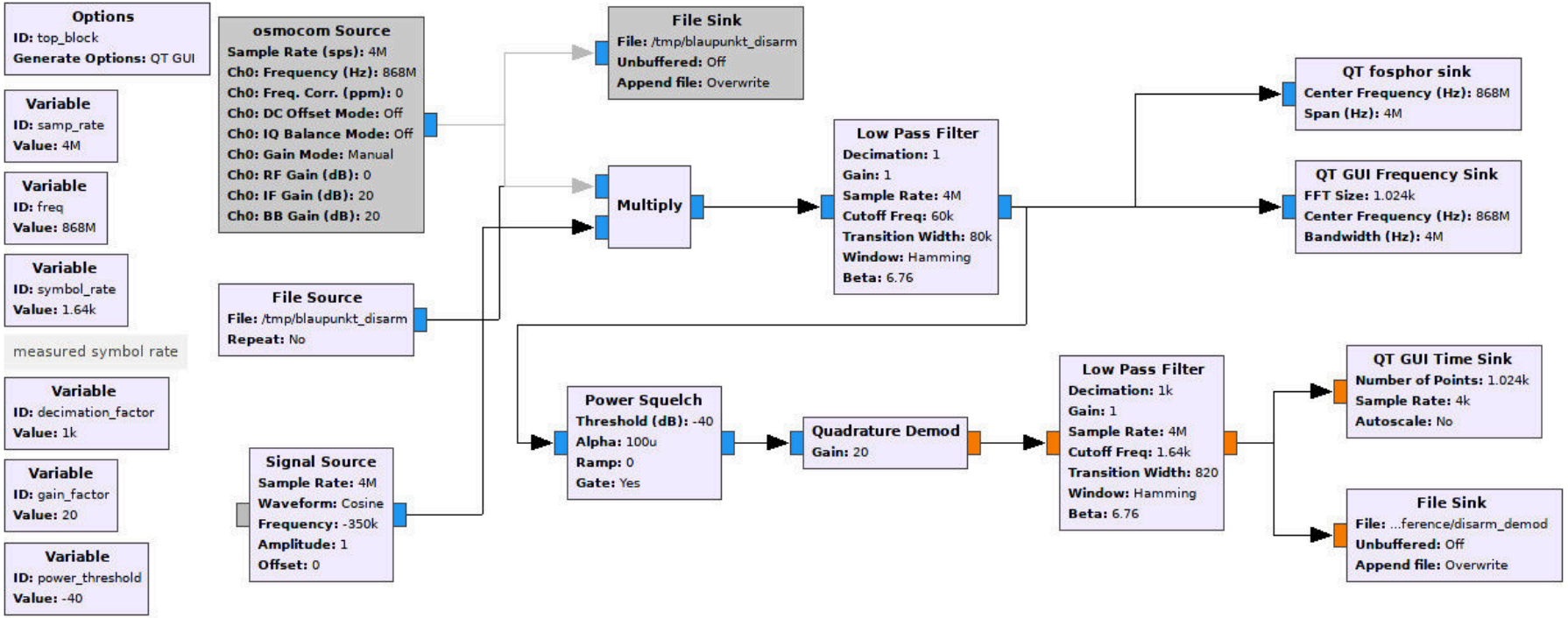
- Im Rahmen eines Forschungsprojekt wurden die folgenden fünf Funkalarmanlagen untersucht:
  1. Multi Kon Trade M2B GSM
  2. Blaupunkt Smart GSM Alarm SA 2500 Kit
  3. Olympia Protect 9061
  4. ALDI EASY HOME Alarmanlagen-Set
  5. ABUS Secvest (FUAA50000)
- Der Fokus der Analyse lag dabei auf den folgenden beiden Fragen:
  1. Bieten die Funkalarmanlagen einen Schutz vor Replay-Angriffen?
  2. Bieten die Funkalarmanlagen einen Schutz vor Bruteforce-Angriffen?

Funkbasierte Analyse



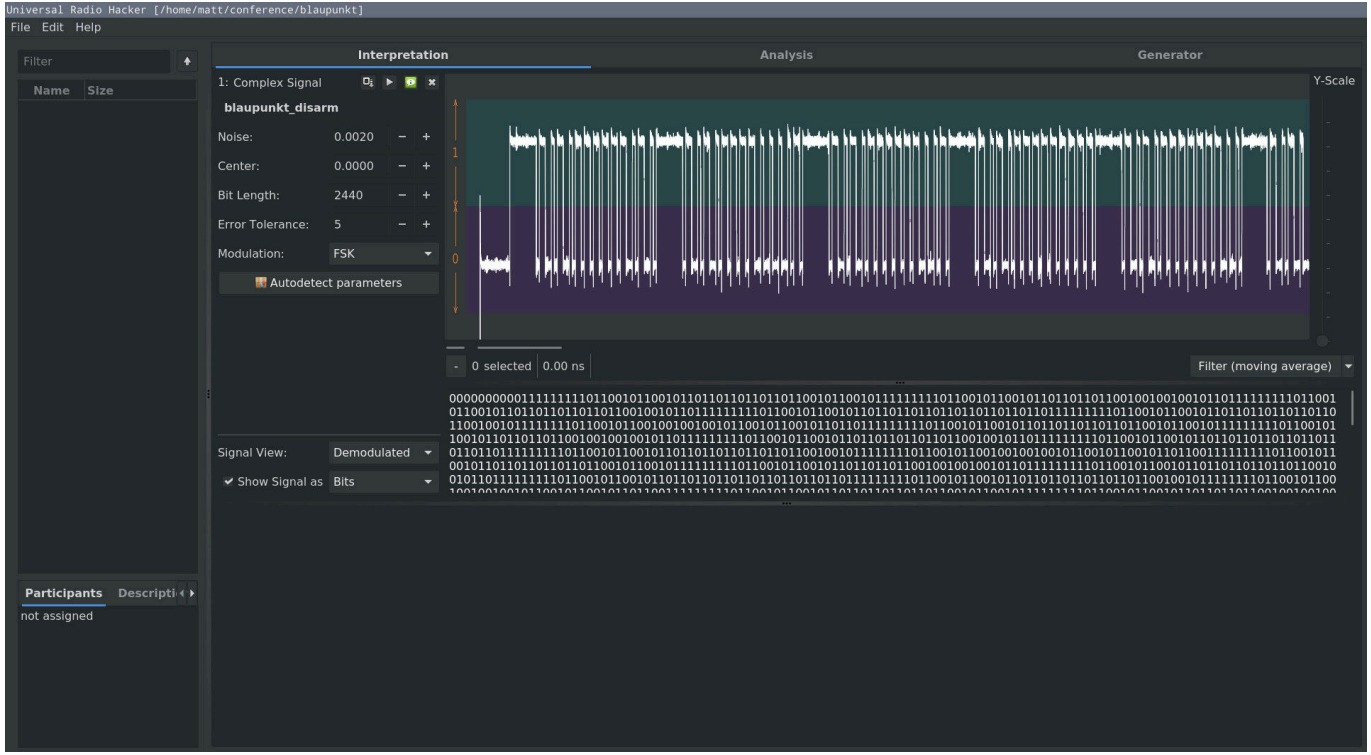
Analyse eines Funksignals mit inspectrum

Funkbasierte Analyse



GNU Radio Companion Flow Graph für die Analyse eines Funksignals

Funkbasierte Analyse



Analyse eines Funksignals mit Universal Radio Hacker

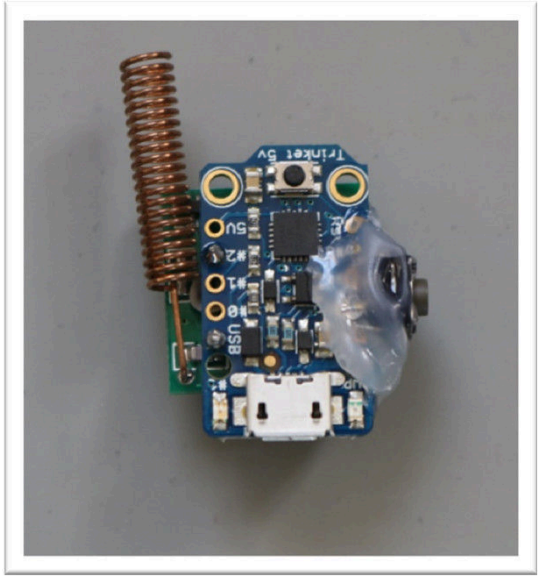
Hardwareanalyse

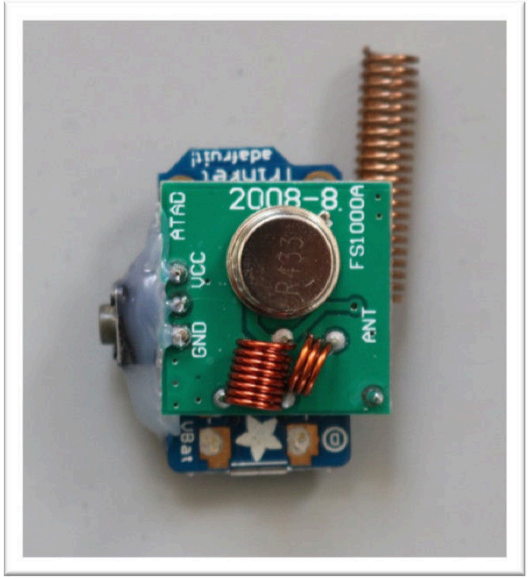
- Hardwareanalyse liefert bisweilen Informationen zum kodierten Funksignal (hier PT 2260 Remote Control Encoder der MKT M2B)

VDD								
Input	**F**	**F**	**0**	**1**	**1**	**0**	**0**	**1**
GND								

Bruteforce-Angriff

- Ist die Anzahl möglicher kodierter Signale gering, sind Bruteforce-Angriffe praktikabel durchführbar





Proof-of-Concept-Hardwaretool entwickelt von Gerhard Klostermeier

Gefundene Schwachstellen

SySS THE PENTEST EXPERTS.

Zusammenfassung unserer Ergebnisse

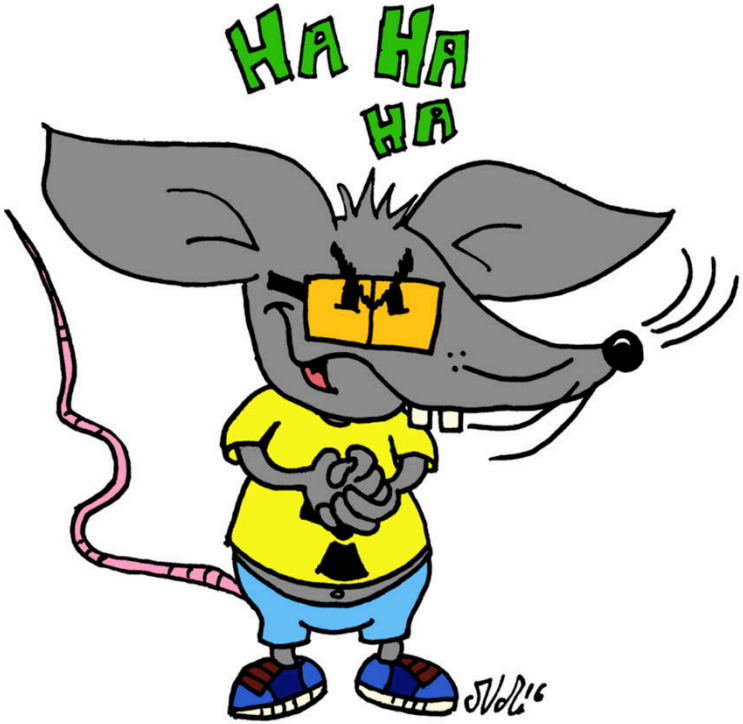
Produktname	Replay Attacks	Bruteforce Attacks
Multi Kon Trade M2B GSM	✓	✓
Blaupunkt Smart GSM Alarm SA 2500 Kit	✓	?
Olympia Protect 9061	✓	?
ALDI EASY HOME Alarmanlagen-Set	✓	?
ABUS Secvest (FUAA50000)	✓	?

✓ Sicherheitsproblem vorhanden

X Sicherheitsproblem nicht vorhanden

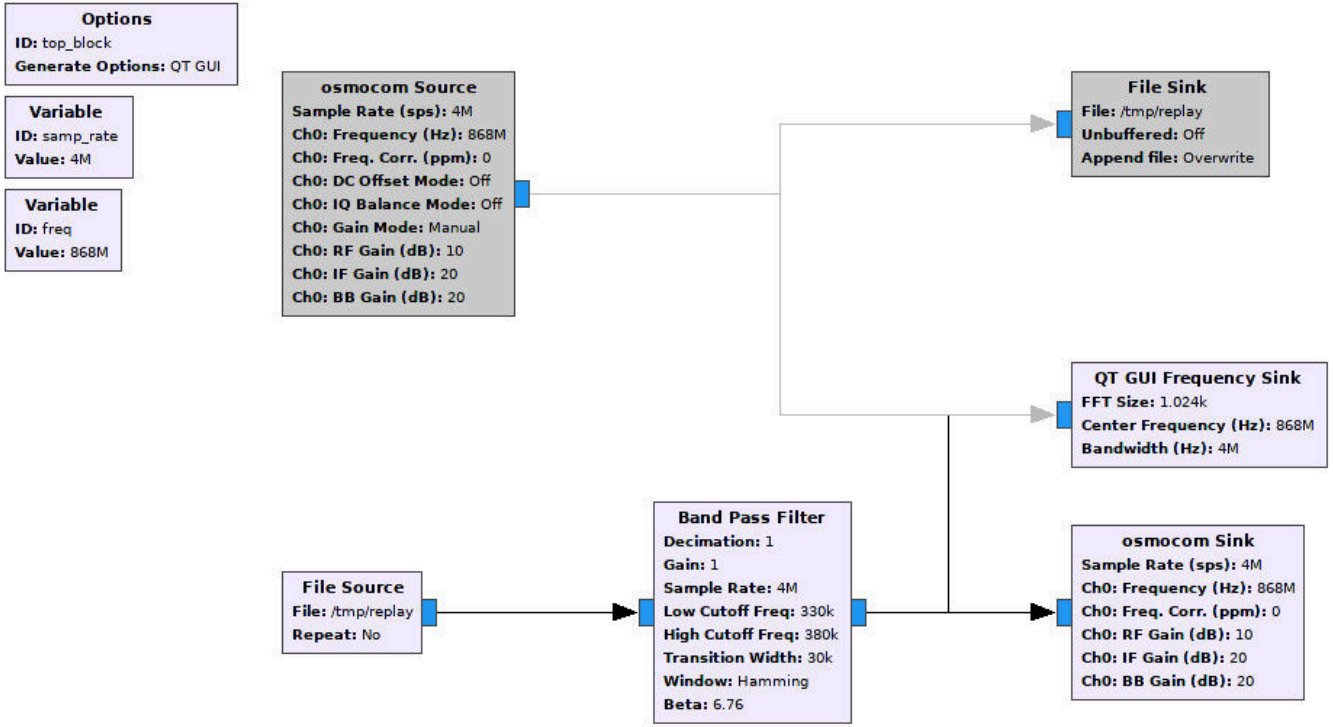
? Existenz des Sicherheitsproblems noch unklar

Demo Time



„Pon de replay!
There's no sound of the police."

Replay-Angriff



Einfacher GNU Radio Companion Flow Graph für Replay-Angriffe

Referenzen

1. *Crazyradio PA*, https://www.bitcraze.io/crazyradio-pa/
2. *MouseJack*, Bastille Networks Internet Security, https://www.mousejack.com/, 2016
3. *NRF24-BTLE-Decoder*,Omri Iluz, https://github.com/omriiluz/NRF24-BTLE-Decoder, 2016
4. *nrf-research-firmware*, Bastille Networks Internet Security, https://github.com/BastilleResearch/nrf-research-firmware, 2016
5. *Of Mice and Keyboards: On the Security of Modern Wireless Desktop Sets*, Hack.lu Konferenzvortrag, SySS GmbH, https://www.youtube.com/watch?v=Ja_VgUMz43Q, 2016
6. *Of Mice and Keyboards: On the Security of Modern Wireless Desktop Sets*, SySS GmbH, https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_06_01_of-mice-and-keyboards_paper.pdf, 2017
7. *Radioactive Mouse States the Obvious – Proof-of-Concept Video*, SySS GmbH, https://www.youtube.com/watch?v=PkR8EODee44, 2016

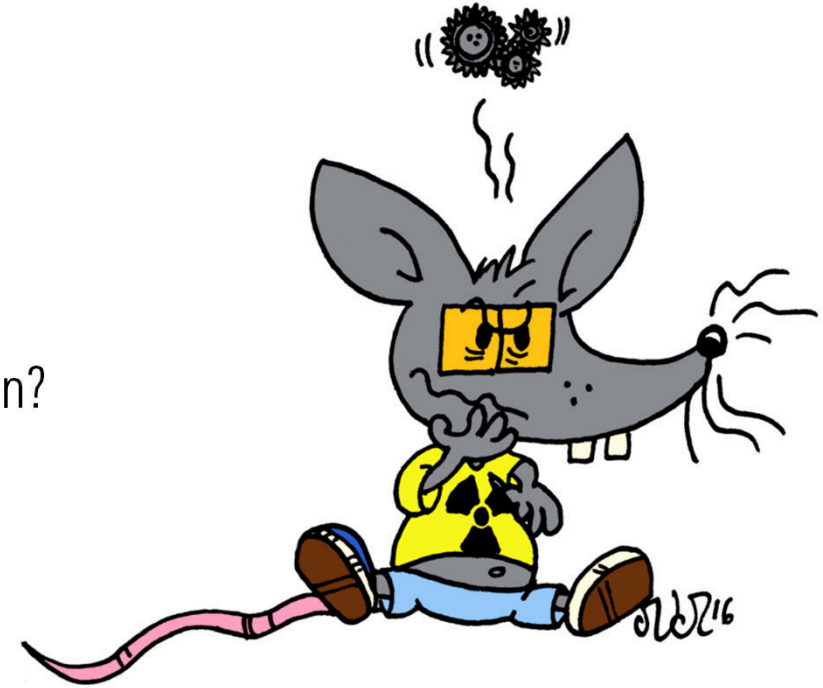
Referenzen

8. *nRF24 Playset*, SySS GmbH, https://github.com/SySS-Research/nrf24-playset, 2017
9. *SySS Radio Hack Box, SySS GmbH, https://github.com/SySS-Research/radio-hackbox, 2017*
10. *There's No Sound of the Police – Schwachstellen in aktuellen Funkalarmanlagen*, SySS GmbH, https://www.syss.de/pentest-blog/article/2016/11/22/theres-no-sound-of-the-police/, 2016
11. *Replay-Schwachstelle in ABUS SECVEST Funkalarmanlage*, SySS GmbH, https://www.syss.de/pentest-blog/article/2017/02/20/syss-2016-117-replay-schwachstelle-in-abus-secvest-funkalarmanlage/, 2017
12. *Von wegen sicher – wie leicht Alarmanlagen zu knacken sind*, ARD-Verbrauchermagazin Plusminus, http://www.daserste.de/information/wirtschaft-boerse/plusminus/videos/von-wegen-sicher-wie-leicht-alarmanlagen-zu-knacken-sind-100.html, 2016

Vielen Dank …

… für Ihre Aufmerksamkeit!

Haben Sie Fragen?



E-mail: matthias.deeg@syss.de

PGP Fingerprint: D1F0 A035 F06C E675 CDB9 0514 D9A4 BF6A 34AD 4DAB

THE PENTEST EXPERTS

WWW.SYSS.DE