# There is Always One More Bug – or More: Revisiting a Wireless Alarm System

22. September 2020

SICHERHEITS KONFERENZ

# Who am I?

Dipl.-Inf. Matthias Deeg
Senior Expert IT Security Consultant
Head of Research & Development
CISSP, CISA, OSCP, OSCE

- Interessiert an Informationstechnik – insbesondere IT-Sicherheit – seit frühen Jahren
- Studium der Informatik an der Universität Ulm
- IT Security Consultant seit 2007

# Agenda

1. Kurze Einführung in verwendete Technologien
2. Überblick unserer Forschungsarbeit
3. Weitere Arbeiten (anderer Forscher)
4. Angriffsfläche und Angriffsszenarien
5. Gefundene Sicherheitsschwachstellen
6. Demos
7. Fazit & Empfehlungen
8. Fragen & Antworten

# Kurze Einführung in verwendete Technologien

# Kurze Einführung in verwendete Technologien

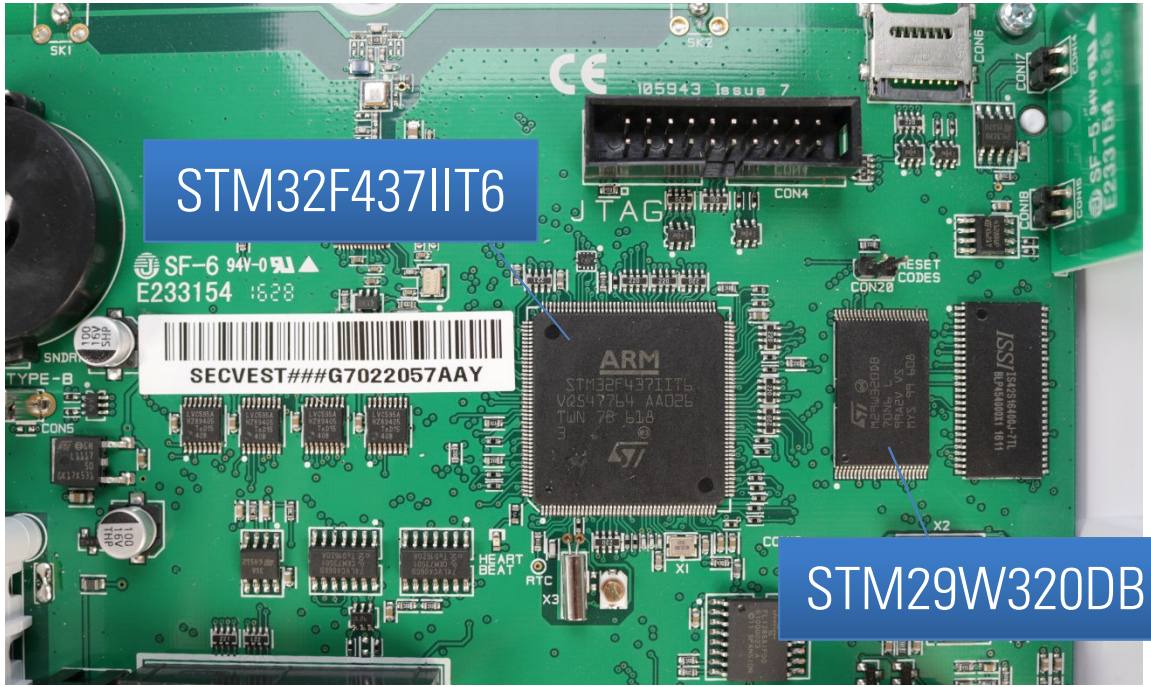
ABUS Secvest Wireless Alarm System (FUAA50000)


Wireless Motion Detector (FUBW50000)

Wireless Remote Control (FUBE50015)

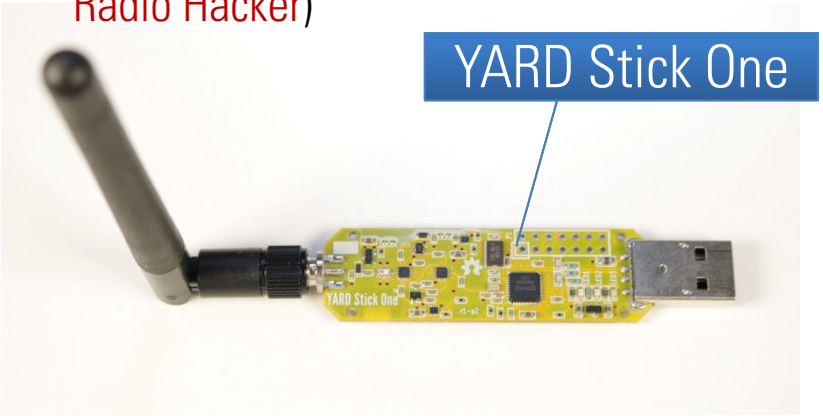
Proximity Chip Key (FUBE50020)

# Kurze Einführung in verwendete Technologien



# Kurze Einführung in verwendete Technologien

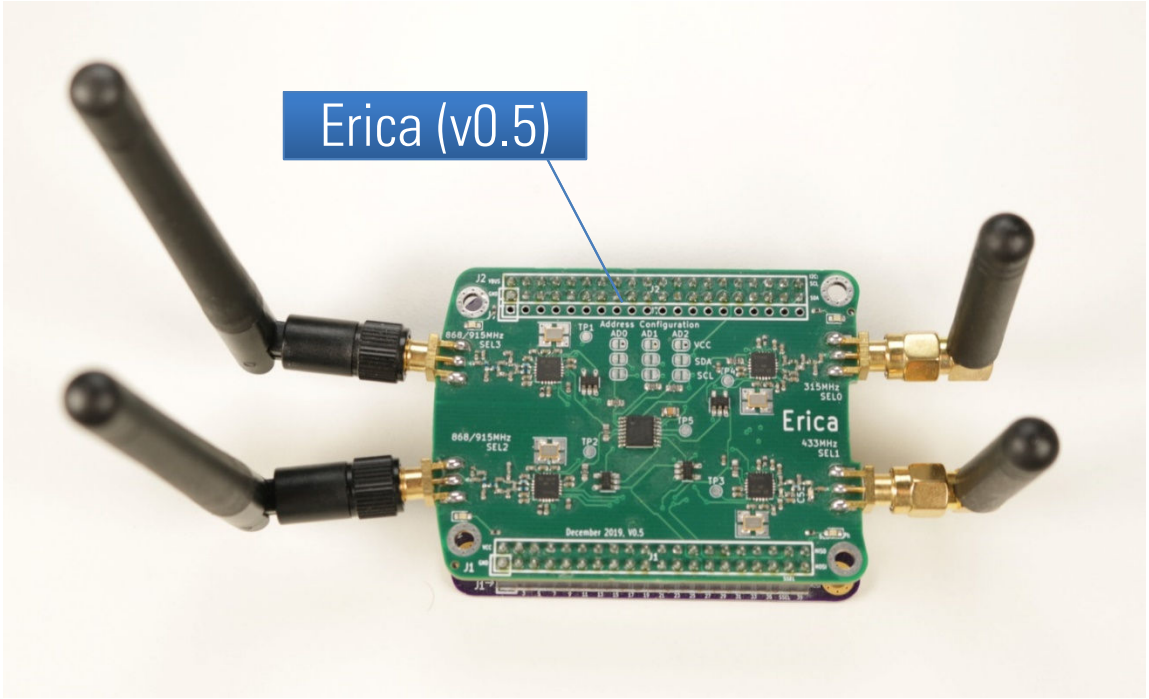

- HackRF One Software-Defined Radio von Great Scott Gadgets
- Zuverlässiges Werkzeug, das von der meisten SDR-Software unterstützt wird (z. B. GNU Radio Companion, Universal Radio Hacker)




- YARD Stick One Radio Dongle mit Texas Instruments CC1111 Transceiver
- RfCat Firmware

# Kurze Einführung in verwendete Technologien

- Erica Neighbor für GreatFET One von Thomas Detert
- 4 Texas Instruments CC1101 Transceivers (für verschiedene Frequenzbereiche, 315/433/868/915 MHz)
- 2 Transceivers pro Frequenzband ermöglichen kurze Reaktionszeiten



# Kurze Einführung in verwendete Technologien

- Die 868.66 MHz-Funkkommunikation der ABUS Secvest-Funkalarmanlage verwendet Differential Manchester Encoding
- Übertragene Pakete nutzen eine 16-bit CRC

# Überblick unserer Forschungsarbeit

- 2016 analysierten Gerhard Klostermeier und Matthias Deeg verschiedene preisgünstige Funkalarmanlagen verschiedener Hersteller auf den einfachsten funkbasierten Angriff hin: Replay-Angriffe
- Alle getesteten Geräte waren anfällig für einfache Replay-Angriffe
- Veröffentlichung unserer Feststellungen im deutschen Fernsehen (Plusminus)
- Die beschaffte ABUS Secvest-Funkalarmanlage, die nicht so günstig war, war nach diesem Projekt weiterhin für Tests verfügbar

# Überblick unserer Forschungsarbeit

- Erhielten wenige Monate später einen Tipp von Thomas Detert, dass der Security Fix für die Replay-Schwachstelle neue Schwachstellen in das System einführte
- Daher warfen wir mit externer Unterstützung weitere Blicke auf die ABUS Secvest-Funkalarmanlage
- Wir fanden und meldeten weitere Sicherheitsschwachstellen
- Beteiligte Personen:
  - Gerhard Klostermeier
  - Thomas Detert
  - Michael Rüttgers
  - Matthias Deeg

# Testmethodik

1. Hardwareanalyse
   - Geräte öffnen, Chips identifizieren, Anleitungen und Datenblätter lesen, Testpunkte finden, Logic Analyzer/JTAG Debugger verwenden
2. Funkbasierte Analyse
   - Nutzung von Software-Defined Radios (SDR) oder Radio Dongles mit speziellen Transceivern, Identifikation/Reverse Engineering des verwendeten Kommunikationsprotokolls (Paketformat/Framing, Nutzdaten, Prüfsummen)
3. Firmware-Analyse
   - Zugriff auf entschlüsselte Firmware erlangen und diese auf Schwachstellen hin analysieren

# Testmethodik

1. ~~Hardwareanalyse~~
   - Geräte öffnen, Chi[illegible]ssen, Testpunkte finden, Logic Analyzer/JTAG Debugger verwenden

nicht genutzt

2. Funkbasierte Analyse
   - Nutzung von Software-Defined Radios (SDR) oder Radio Dongles mit speziellen Transceivern, Identifikation/Reverse Engineering des verwendeten Kommunikationsprotokolls (Paketformat/Framing, Nutzdaten, Prüfsummen)
3. ~~Firmware-Analyse~~
   - Zugriff auf entschlü[illegible]ese auf Schwachstellen hin analysieren

nicht genutzt

# Weitere Arbeiten (anderer Forscher)

- *Analyzing the Radio Interface of an ABUS Secvest Intruder Alarm System* von Martin Schobert, Schobert IT-Security Consulting, 2011
- *Breaking the Security of Physical Devices* von Silvio Cesare, 2014
- *Von wegen sicher – wie leicht Alarmanlagen zu knacken sind* von SySS GmbH and Plusminus, 2016
- *Hacking wireless house alarms* von Andrew Tierney, Pen Test Partners, 2017
- *Hacking Wireless Home Security Systems* von Eric Escobar, SecureWorks, 2017
- *Software Defined Radio: Weniger Theorie, mehr Praxis* von Matthias Deeg, SySS GmbH, 2017

# Angriffsfläche und Angriffsszenarien

1. Direkter physischer Zugriff auf Funkalarmanlage
2. Angriffe mittels Funksignalen (OTA)
   - Replay attacks
   - Brute-force attacks
   - Denial of service attacks
   - Jamming attacks
   - Sniffing attacks
   - Spoofing attacks
   - Cloning attacks

# Angriffsfläche und Angriffsszenarien

1. ~~Direkter physischer Zugriff auf Funkalarmanlage~~ weniger interessant
2. Angriffe mittels Funksignalen (OTA) interessant
   - Replay attacks
   - Brute-force attacks
   - Denial of service attacks
   - Jamming attacks
   - Sniffing attacks
   - Spoofing attacks
   - Cloning attacks

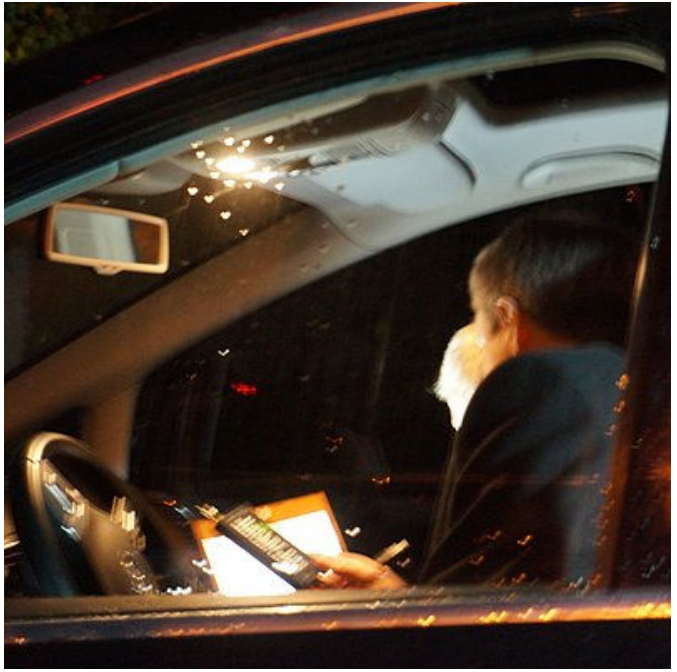
# Gefundene Sicherheitsswachstellen

| # | Produkt | Schwachstellentyp | SySS ID | CVE ID |
|---|---|---|---|---|
| 1 | ABUS Secvest (FUAA50000) | Missing Protection against Replay Attacks | SYSS-2016-117 | - |
| 2 | ABUS Secvest (FUAA50000) | Rolling Code - Predictable from Observable State (CWE-341) | SYSS-2018-034 | CVE-2019-9863 |
| 3 | ABUS Secvest Remote Control (FUBE50014, FUBE50015) | Missing Encryption of Sensitive Data (CWE-311) | SYSS-2018-035 | CVE-2019-9862 |
| 4 | ABUS Secvest Remote Control (FUBE50014, FUBE50015) | Denial of Service - Uncontrolled Resource Consumption (CWE-400) | SYSS-2018-036 | CVE-2019-9860 |
| 5 | ABUS Secvest (FUAA50000) | Message Transmission - Unchecked Error Condition (CWE-391) | SYSS-2019-004 | CVE-2019-14261 |
| 6 | ABUS Secvest (FUAA50000) | Cryptographic Issues (CWE-310) | SYSS-2019-005 | CVE-2019-9861 |
| 7 | ABUS Secvest Wireless Control Device (FUBE50001) | Missing Encryption of Sensitive Data (CWE-311) | SYSS-2020-014 | CVE-2020-14157 |
| 8 | ABUS Secvest Hybrid Module (FUMO50110) | Authentication Bypass Using an Alternate Path or Channel (CWE-288) | SYSS-2020-014 | CVE-2020-14158 |

# Replay Attack

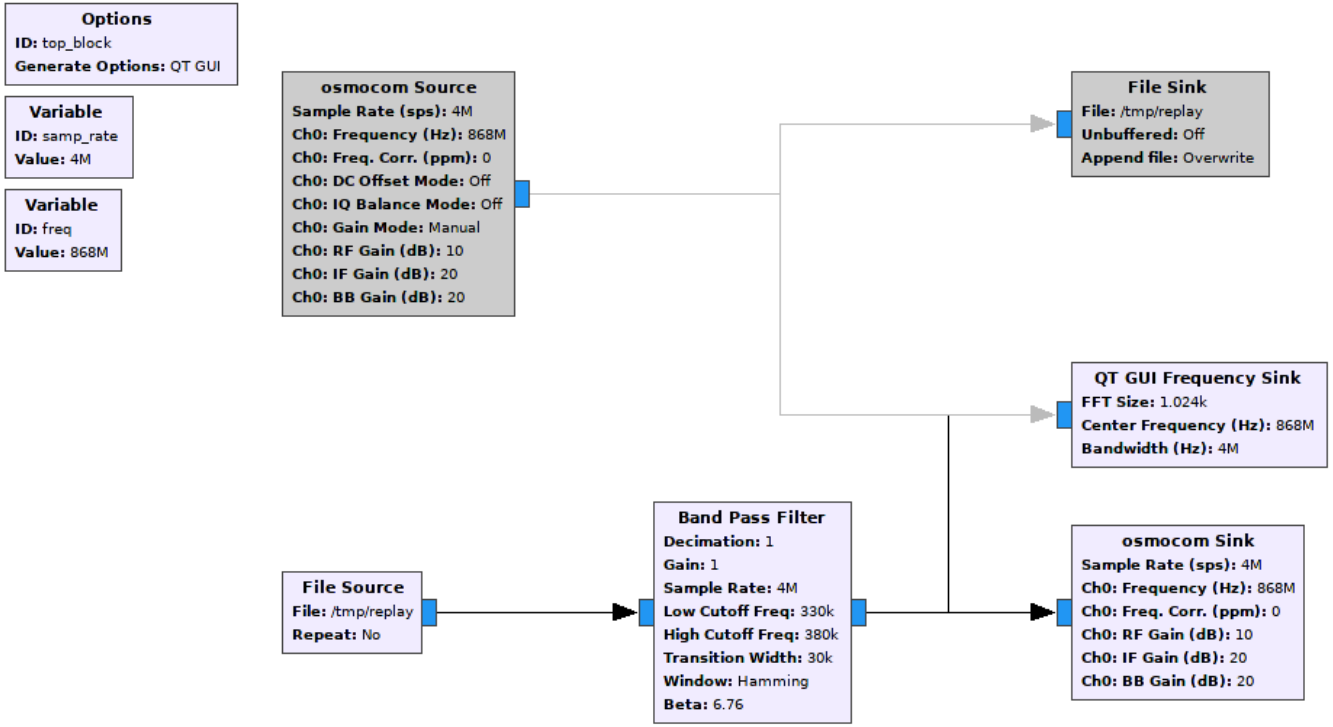
- Sehr einfacher funkbasierter Angriff
- Einfach interessantes Funksignal aufzeichnen und später wiedergeben (z. B.Unscharf-Signal)
- Viele proprietäre Funkprotokolle besitzen immer noch keinen Schutz vor Replay-Angriffen
- Alle Funkalarmanlagen, die wir 2016 getestet haben, waren dafür verwundbar

⇒ *Deaktivierung einer Funkalarmanlage auf unautorisierte Weise*



Quelle: Plusminus-Sendung aus dem Jahr 2016

# Replay Attack




Simple GNU Radio Companion Flow Graph for Replay Attacks

# Rolling Code Attack

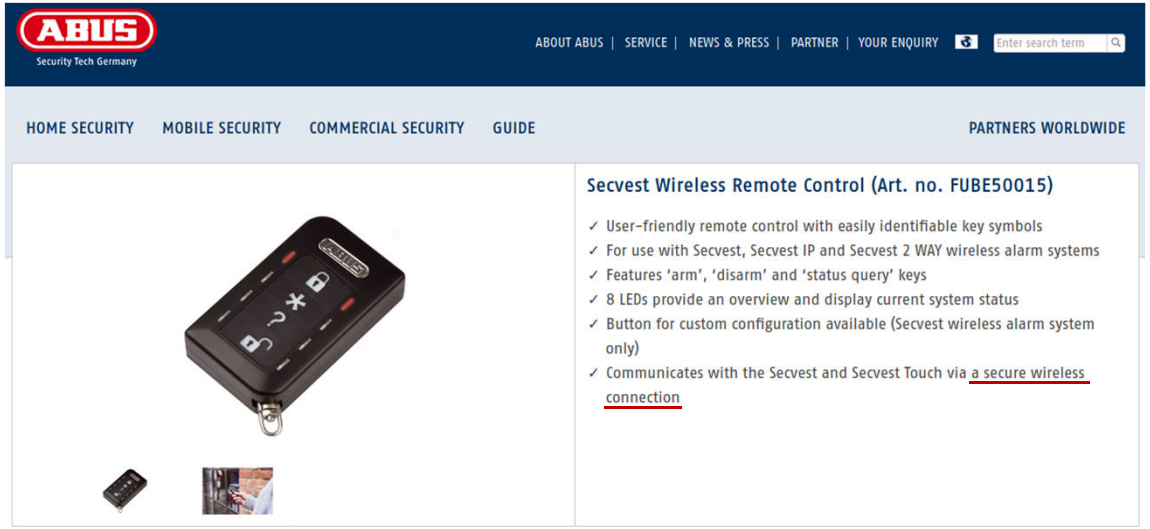

- Um die Replay-Schwachstelle zu heben, hat ABUS Rolling Codes in neueren Funkfernbedienungen implementiert (z. B. FUBE50014, FUBE50015)

Quelle: Produktwebseite der ABUS Secvest Wireless Remote Control (FUBE50015)

**Secure wireless communication**

Thanks to a secure wireless communication procedure, this product is protected against 'replay attacks', as are the Secvest wireless alarm system and Secvest Touch alarm systems. This procedure for preventing third party tampering exceeds the requirements of the "DIN EN 50131-1 level 2" security standard.

# Rolling Code Attack




- Um die Replay-Schwachstelle zu heben, hat ABUS Rolling Codes in neueren Funkfernbedienungen implementiert (z. B. FUBE50014, FUBE50015)
- Mit angeblich sicherer Funkkommunikation

Quelle: Produktwebseite der ABUS Secvest Wireless Remote Control (FUBE50015)

**Secure wireless communication**

Thanks to a secure wireless communication procedure, this product is protected against 'replay attacks', as are the Secvest wireless alarm system and Secvest Touch alarm systems. This procedure for preventing third party tampering exceeds the requirements of the "DIN EN 50131-1 level 2" security standard.

# Rolling Code Attack

- Leider war die gewählte Rolling Code-Implementierung kryptografisch schwach, wie Thomas Detert herausfand
- Durch Beobachten der unverschlüsselten Funksignale konnte der Rolling Code-Algorithmus in Erfahrung gebracht werden
- Damit können gültige Rolling Codes vorhergesagt werden

⇒ *Deaktivierung der Funkalarmanlage auf unautorisierte Weise*

⇒ *Desynchronisierung der Funkfernbedienung (Denial of Service)*

# Demo: Rolling Code Attack

# Proximity Key Cloning Attack

- Die ABUS Secvest-Funkalarmanlage unterstützt sogenannte Proximity Keys
- Leider wird hierfür die unsichere RFID-Technologie MIFARE Classic verwendet
- Daher können die Informationen eines Proximity Keys recht einfach in kurzer Zeit aus Entfernungen bis zu 1 Meter ausgelesen werden
- Ein Angreifer mit einmaligem Zugriff kann einen Chip Key klonen

⇒ *Deaktivierung der Funkalarmanlage auf unautorisierte Weise*


ABUS Secvest proximity chip key

# Demo: Proximity Key Cloning Attack

# Reactive Jamming Attack

- Die ABUS Secvest-Funkalarmanlage besitzt eine RF Jamming Detection
- Wenn ungewöhnliche Interferenzen auf dem verwendeten Funkkanal (868.6625 MHz) erkannt werden, kann ein Alarm ausgelöst werden (RF Jamming-Konfiguration)
- Thomas Detert fand heraus, dass die implementierte RF Jamming Detection unzureichend ist
- Kurze Jamming-Signale (kürzer als ABUS-Funknachrichten) werden nicht erkannt
- Daher kann ein Reactive Jamming-Angriff durchgeführt werden

# Reactive Jamming Attack

- Bei einem Reactive Jamming-Angriff wird der Beginn einer Nachricht erkannt und diese dann mit einem Signal des Angreifers überlagert, z. B. mit Zufallsdaten
- Dadurch kann der Empfänger der Nachricht das ursprünglich gesendete Funksignal nicht mehr korrekt dekodieren

⇒ *Unterdrücken des korrekten Empfangs von Funknachrichten auf unautorisierte Weise*

# Reactive Jamming Attack

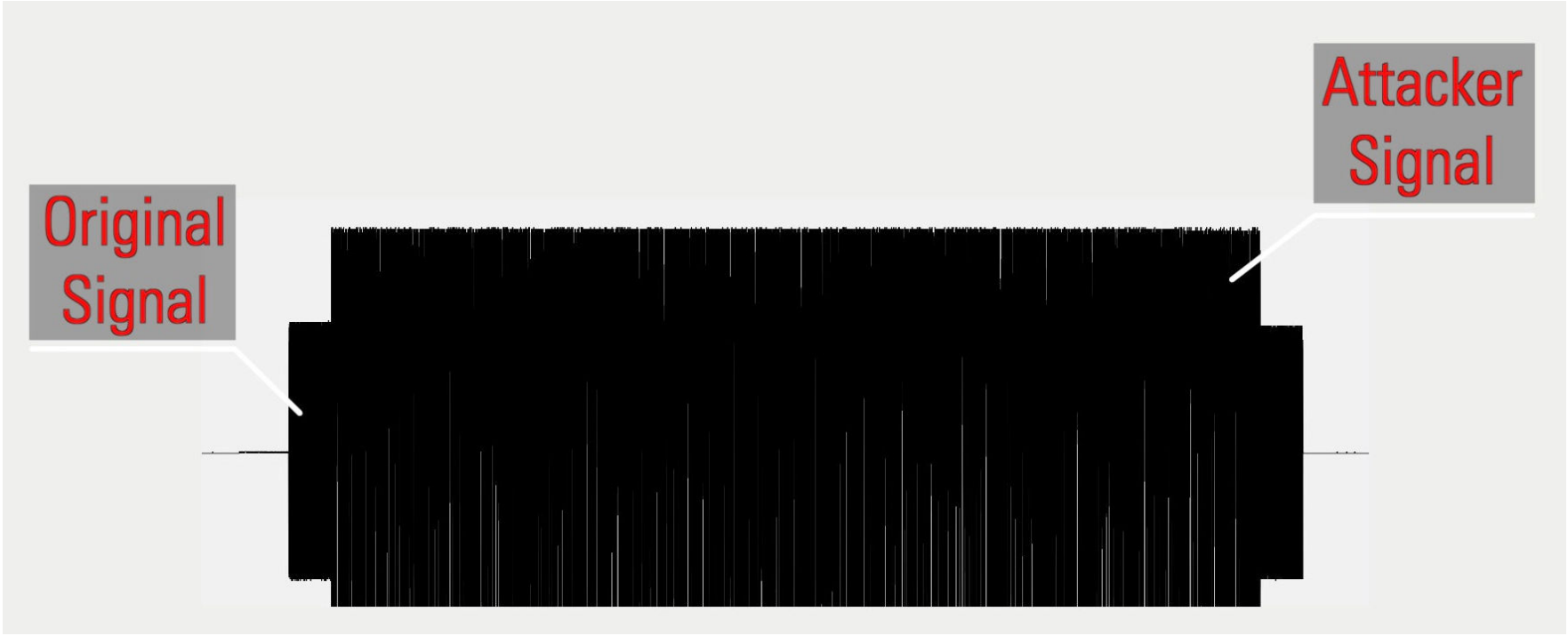
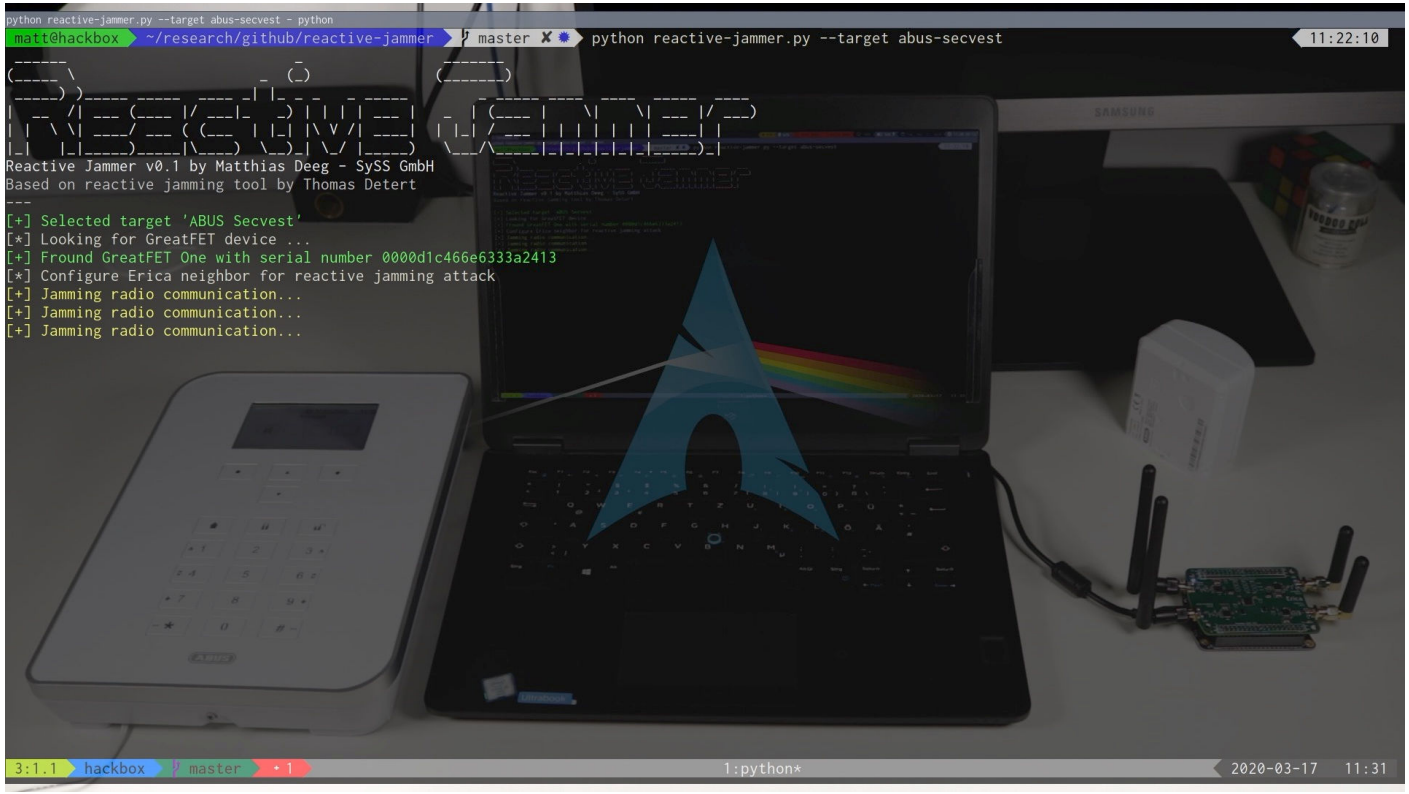



Illustration eines Reactive Jamming-Angriffs

# Demo: Reactive Jamming Attack



# Sniffing Attack


- Neben den Funkfernbedienungen (z. B. FUBE50014, FUBE50015) gibt es auch ein Wireless Control Device (FUBE50001)

Quelle: Produktwebseite des ABUS Secvest Wireless Control Device (FUBE50001)

**Secure wireless communication**

Thanks to a secure wireless communication procedure, this product is protected against 'replay attacks', as are the Secvest wireless alarm system and Secvest Touch alarm systems. This procedure for preventing third party tampering exceeds the requirements of the "DIN EN 50131-1 level 2" security standard.

# Sniffing Attack


- Neben den Funkfernbedienungen (z. B. FUBE50014, FUBE50015) gibt es auch ein Wireless Control Device (FUBE50001)
- Mit angeblich sicherer Funkkommunikation

Quelle: Produktwebseite des ABUS Secvest Wireless Control Device (FUBE50001)

**Secure wireless communication**

Thanks to a secure wireless communication procedure, this product is protected against 'replay attacks', as are the Secvest wireless alarm system and Secvest Touch alarm systems. This procedure for preventing third party tampering exceeds the requirements of the "DIN EN 50131-1 level 2" security standard.

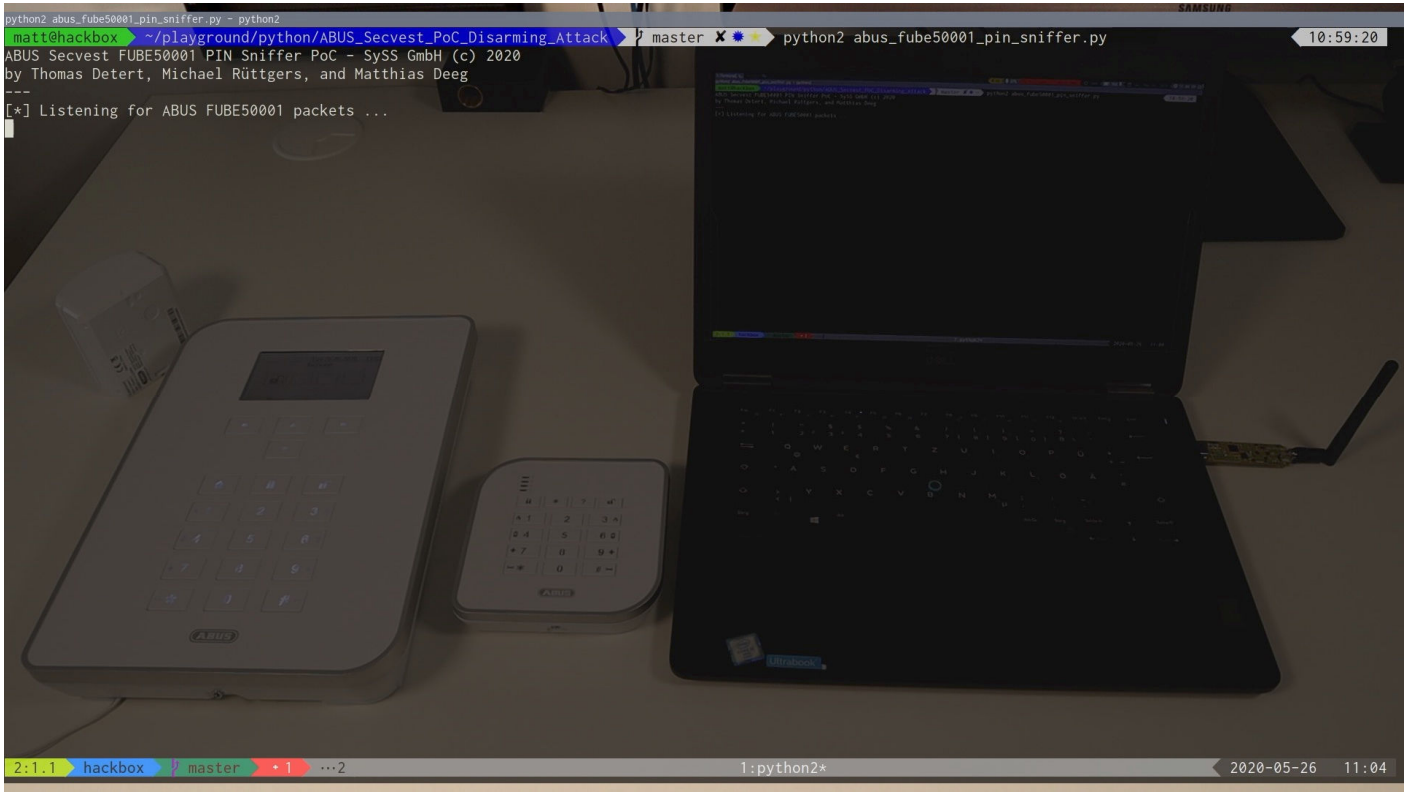
# Sniffing Attack

- Die verwendete sichere Funkkommunikation nutzt keine Verschlüsselung
- Durch Beobachten der Funksignale eines Wireless Control Panel können sensible Daten im Klartext in Erfahrung gebracht werden

⇒ *Belauschen sensibler Daten wie PIN Codes und Proximity Token IDs*

⇒ *Deaktivierung der Funkalarmanlage auf unautorisierte Weise*

# Demo: Sniffing Attack



# Demo: Sniffing Attack

Beispiel eines erfolgreichen PIN-Code-Sniffing-Angriffs:

```
$ python2 abus_fube50001_pin_sniffer.py
ABUS Secvest FUBE50001 PIN Code Sniffer PoC - SySS GmbH (c) 2020
by Thomas Detert, Michael Rüttgers, and Matthias Deeg
---
[*] Listening for ABUS FUBE50001 packets ...
[*] Received packet:
f0f352b4ccb4ccd52aab52d2acd2d34d4cb34cb333332b34d4b530f0f0f352b4ccb4ccd52aab52d2acd2d34
d4cb34cb333332b34d4b530f0f0f3333333333117162f5
[*] Decoded packet : da0a077ed5c549888800626b
[*] Received packet:
f0f352b4b32b4d352ad5332aab2cb34cd3332cccb4ccacb354acaaaaccccd2ab32aab54d30f0f0f352b4b32
b4d352ad5332aab2cb34cd3332cccb4ccacb354acaaaa
[*] Decoded packet : da86937707e4884040a0c8ecff005e1fb9
[*] Detected FUBE50001 packet with FUBE50001 PIN
[+] Sniffed PIN code: 1337
(...)
```

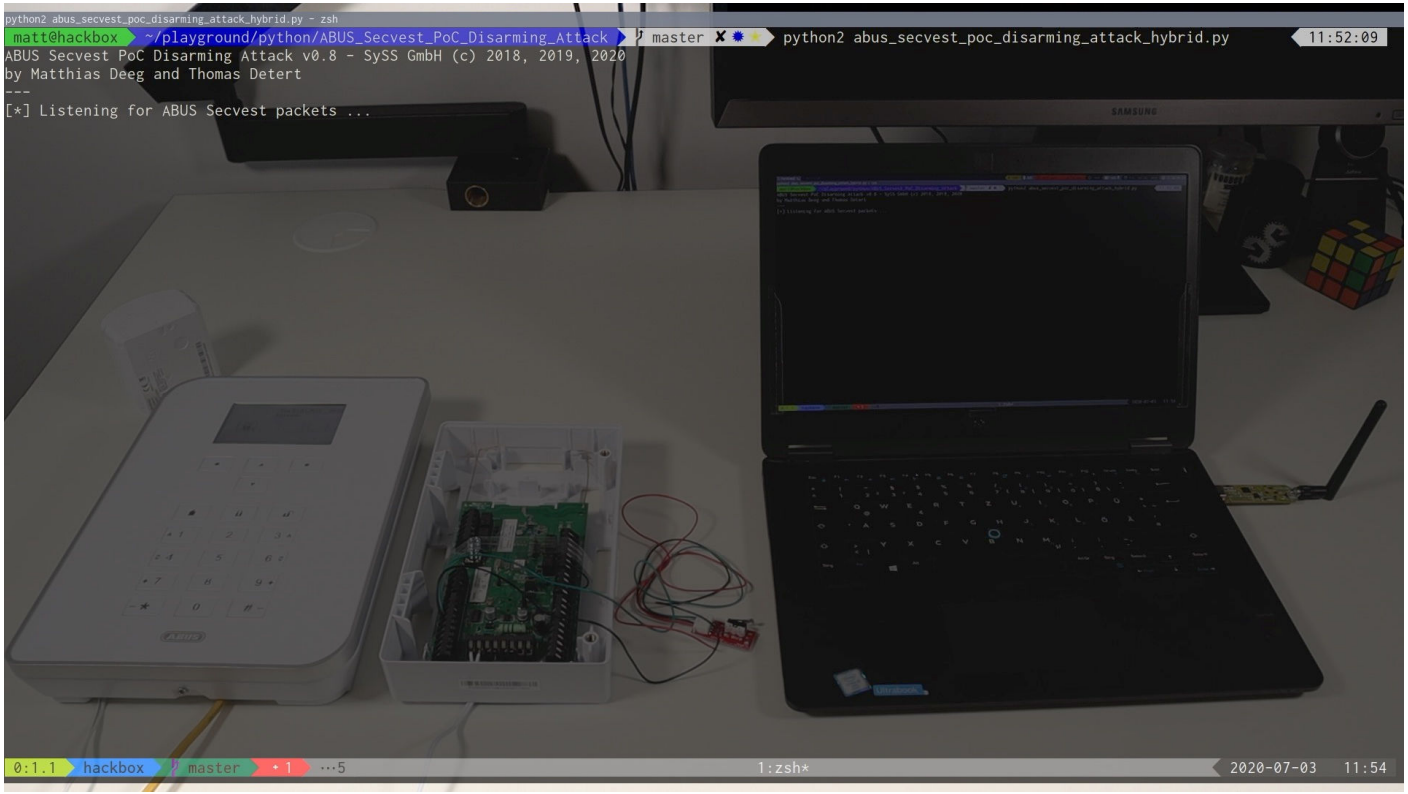
# Spoofing Attack

- Das ABUS Secvest Hybrid-Modul (FUMO50110) kann für die Erweiterung der Funkalarmanlage um drahtgebundene Komponenten genutzt werden
- Dieses Modul erlaubt auch die Integration des ABUS wAppLoxx Access Control-System
- Die verwendete Funkkommunikation besitzt jedoch keine Sicherheitsmerkmale für die Gewährleistung von Vertraulichkeit und Integrität der übermittelten Daten

⇒ *Deaktivierung der Funkalarmanlage auf unautorisierte Weise*

⇒ *Umgehung der Authentifizierung des wAppLoxx Access Control-Systems*

# Demo: Spoofing Attack



# Fazit

| # | Produkt | Schwachstellentyp | SySS ID | CVE ID | Behoben |
|---|---|---|---|---|---|
| 1 | ABUS Secvest (FUAA50000) | Missing Protection against Replay Attacks | SYSS-2016-117 | - | ✓ |
| 2 | ABUS Secvest (FUAA50000) | Rolling Code - Predictable from Observable State (CWE-341) | SYSS-2018-034 | CVE-2019-9863 | X |
| 3 | ABUS Secvest Remote Control (FUBE50014, FUBE50015) | Missing Encryption of Sensitive Data (CWE-311) | SYSS-2018-035 | CVE-2019-9862 | X |
| 4 | ABUS Secvest Remote Control (FUBE50014, FUBE50015) | Denial of Service - Uncontrolled Resource Consumption (CWE-400) | SYSS-2018-036 | CVE-2019-9860 | X |
| 5 | ABUS Secvest (FUAA50000) | Message Transmission - Unchecked Error Condition (CWE-391) | SYSS-2019-004 | CVE-2019-14261 | X |
| 6 | ABUS Secvest (FUAA50000) | Cryptographic Issues (CWE-310) | SYSS-2019-005 | CVE-2019-9861 | X |
| 7 | ABUS Secvest Wireless Control Device (FUBE50001) | Missing Encryption of Sensitive Data (CWE-311) | SYSS-2020-014 | CVE-2020-14157 | X |
| 8 | ABUS Secvest Hybrid Module (FUMO50110) | Authentication Bypass Using an Alternate Path or Channel (CWE-288) | SYSS-2020-014 | CVE-2020-14158 | X |

# Fazit

- Sicherheitsprodukte wie Funkalarmanlagen können verwundbarer für verschiedene funkbasierte Angriffe sein als man zunächst annehmen mag
- Marketing-Versprechen bezüglich Sicherheit sind oftmals nur genau das: Marketing-Versprechen
- Produktzertifikate wie VDS Home und EN 50131-1 Level 2 können einen falschen Eindruck von Sicherheit vermitteln
- Manche Sicherheitsschwachstellen sind schwieriger oder gar unmöglich in Hardwareprodukten zu beheben, die bereits in Verwendung sind
- *Forever bugs* können die Sicherheit eines Produkts bis an dessen Lebensende beeinträchtigen

# Empfehlungen

- Funkalarmanlagen mit Bedacht auswählen
- Eine gründliche Onlinerecherche vor Kauf eines solchen Produkts durchführen
- Die getroffene Entscheidung zum Kauf einer Funkalarmanlage nochmals überdenken
- Nicht allzu viel Vertrauen in Produktzertifikate und Marketing-Versprechen haben
- Nach weiteren Sicherheitstests über eine Produktzertifizierung hinaus und deren Testumfang (sehr wichtig) fragen

# Referenzen


1. *HackRF*, Great Scott Gadgets, https://greatscottgadgets.com/hackrf/
2. *YardStick* One, Great Scott Gadgets, https://greatscottgadgets.com/yardstickone/
3. *Analyzing the Radio Interface of an ABUS Secvest Intruder Alarm System*, Martin Schobert, Martin Schobert IT-Security Consulting, https://sitsec.net/files/secvest_analysis.pdf, 2011
4. *Breaking the Security of Physical Devices*, Silvio Cesare, https://www.youtube.com/watch?v=TMpHB-pWseM, 2014
5. *SySS Security Advisory SYSS-2016-117*, Matthias Deeg, *https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2016-117.txt*, 2016
6. *Von wegen sicher – wie leicht Alarmanlagen zu knacken sind*, SySS GmbH, Plusminus, *https://programm.ard.de/TV/Programm/Sender/?sendung=2810619077021198*, 2016
7. *Hacking wireless house alarms* , Andrew Tierney, Pen Test Partners, https://www.pentestpartners.com/security-blog/hacking-wireless-house-alarms/, 2017
8. *Hacking Wireless Home Security Systems by Eric Escobar* by Eric Escobar, SecureWorks, https://www.youtube.com/watch?v=kERUpg5YMis,2017
9. *Software Defined Radio: Weniger Theorie, mehr Praxis* by Matthias Deeg, SySS GmbH, https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_09_27_SDR_-_Weniger_Theorie__mehr_Praxis.pdf, 2017

# Referenzen


10. *SySS Security Advisory SYSS-2018-034*, Matthias Deeg, Thomas Detert, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2018-034.txt, 2018
11. *SySS Security Advisory SYSS-2018-035*, Matthias Deeg, Thomas Detert, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2018-035.txt, 2018
12. *SySS Security Advisory SYSS-2018-036*, Matthias Deeg, Thomas Detert, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2018-036.txt, 2018
13. *MIFARE Classic Tool, Gerhard Klostermeier, https://play.google.com/store/apps/details?id=de.syss.MifareClassicTool&hl=en*
14. *ChameleonMini*, Kapser & Oswald GmbH, https://github.com/emsec/ChameleonMini
15. *ABUS Secvest Rolling Code PoC Attack, SySS GmbH*, https://www.youtube.com/watch?v=pSdsMVn-7gM, 2019
16. *SySS Security Advisory SYSS-2019-005*, Matthias Deeg, Gerhard Klostermeier, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-005.txt, 2019
17. *ABUS Secvest Key Cloning PoC Attack*, SySS GmbH, https://www.youtube.com/watch?v=sPyXTQXTEcQ, 2019
18. *SySS Security Advisory SYSS-2019-004*, Matthias Deeg, Thomas Detert, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-004.txt, 2019

# Referenzen


19. *Einsatz veralteter Technologien bei Funkalarmanlagen*, SySS GmbH, https://www.ardmediathek.de/mdr/sendung/voss-und-team/, 2019
20. *GreatFET One*, Great Scott Gadgets, https://github.com/greatscottgadgets/greatfet/wiki
21. *GreatFET One Neighbor Erica*, Thomas Detert, https://github.com/AsFaBw/erica, 2020
22. *Reactive Jamming Attack Against ABUS Secvest Wireless Alarm System Using GreatFET One With Erica*, https://www.youtube.com/watch?v=nbJ8CsBmmCo, SySS GmbH, 2020
23. *SySS Security Advisory SYSS-2020-014*, Michael Rüttgers, Thomas Detert, Matthias Deeg, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-014.txt, 2020
24. *ABUS Secvest Sniffing Attack Against Wireless Control Device FUBE50001*, SySS GmbH, https://www.youtube.com/watch?v=kCqAVYyahLc, 2020
25. *SySS Security Advisory SYSS-2020-015*, Michael Rüttgers, Thomas Detert, Matthias Deeg, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-015.txt, 2020
26. *ABUS Secvest Spoofing Attack against Hybrid Module FUMO50110*, SySS GmbH, https://www.youtube.com/watch?v=PidiWcB0tmI, 2020

# Vielen Dank …

… für ihre Aufmerksamkeit!

Haben Sie Fragen?

E-Mail: matthias.deeg@syss.de
Twitter: @matthiasdeeg
YouTube: https://www.youtube.com/c/SySSPentestTV

THE PENTEST EXPERTS

WWW.SYSS.DE