

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

October 10, 2020



# Who am I?

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

- Interested in information technology – especially IT security – since his early days
- Studied computer science at the University of Ulm, Germany
- IT Security Consultant since 2007



# Agenda



1. Short Introduction of Used Technology
2. Overview of Our Research
3. Previous Work of (Other) Researchers
4. Attack Surface and Attack Scenarios
5. Found Security Vulnerabilities
6. Demos
7. Conclusion & Recommendation
8. Q&A

# Short Introduction to Used Technology

ABUS Secvest  
Wireless Alarm  
System (FUAA50000)



Wireless Motion  
Detector  
(FUBW50000)

Wireless Remote  
Control  
(FUBE50015)

Proximity Chip  
Key (FUBE50020)

# Short Introduction to Used Technology

ABUS Secvest  
Wireless Alarm  
System (FUAA50000)

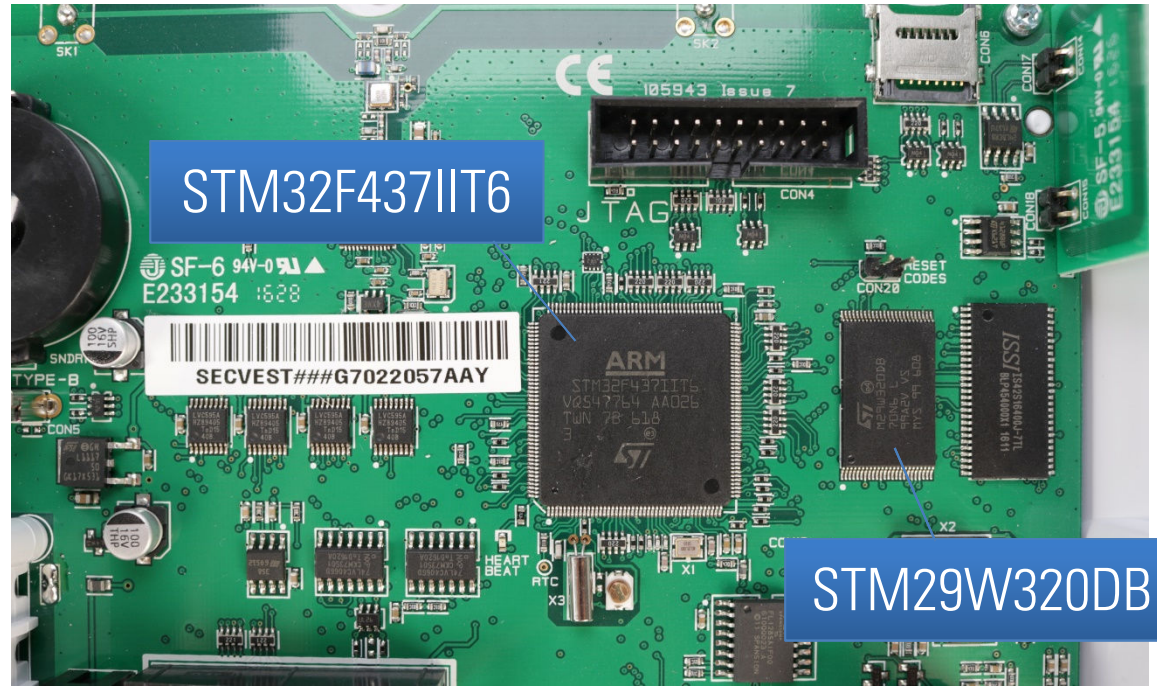


Wireless Motion  
Detector  
(FUBW50000)

Wireless Remote  
Control  
(FUBE50015)

Proximity Chip  
Key (FUBE50020)

# Short Introduction to Used Technology



# Short Introduction to Used Technology

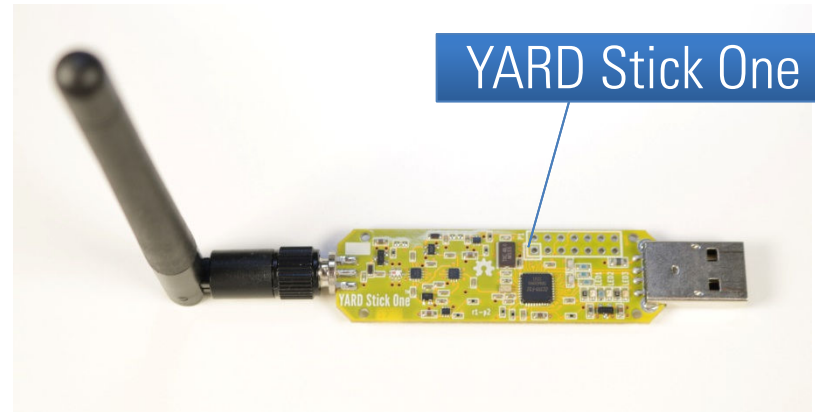
HackRF One



- YARD Stick One **radio dongle** with Texas Instruments **CC1111** transceiver
- **RfCat** firmware

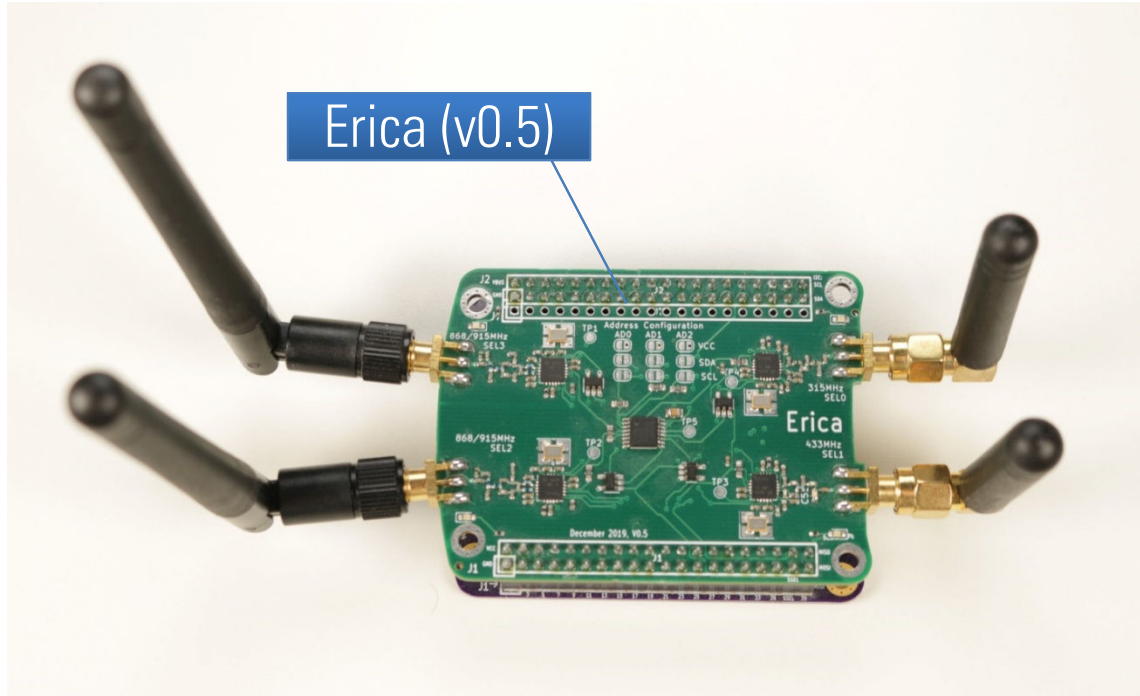
- HackRF One **software-defined radio** by Great Scott Gadgets
- Proven and reliable tool supported by most **SDR software** (e. g. **GNU Radio Companion**, **Universal Radio Hacker**)

YARD Stick One



# Short Introduction to Used Technology

- Erica neighbor for GreatFET One by Thomas Detert
- 4 Texas Instruments CC1101 transceivers (for different frequency bands, 315/433/868/915 MHz)
- 2 transceivers per frequency band allow for short reaction times





# Short Introduction to Used Technology



- The 868.66 MHz radio communication of the ABUS Secvest wireless alarm system uses **Differential Manchester Encoding**
- Radio packets use a **16-bit CRC**

# Overview of Our Research

- In 2016, Gerhard Klostermeier and Matthias Deeg analyzed several, mostly **low-cost**, wireless alarm systems by **different manufacturers** for the simplest radio-based attack: the **replay attack**
- **All tested devices were vulnerable** to a simple replay attack
- Published our findings on German television (Plusminus)
- The obtained **ABUS Secvest wireless alarm system**, which was not so cheap, was still available after this research project for further tests

# Overview of Our Research



- Received a tip from Thomas Detert that the security update for fixing the replay attack introduced new security vulnerabilities
- Had some further looks at the ABUS Secvest wireless alarm system with external support
- Found and reported more security vulnerabilities
- Involved people:
  - Gerhard Klostermeier
  - Thomas Detert
  - Michael Rüttgers
  - Matthias Deeg

# Test Methodology



## 1. Hardware analysis

- Open hardware, identify chips, read manuals, find test points, use logic analyzers and/or JTAG debuggers

## 2. Radio-based analysis

- Use radio test tools like software-defined radios (SDR) or radio dongles with specific transceivers, try to identify and/or reverse engineer the used communication protocol (packet formats/framing, payloads, checksums)

## 3. Firmware analysis

- Get access to decrypted device firmware (memory dump, download, etc.), analyze firmware for security issues

# Test Methodology

## 1. Hardware analysis

- Open hardware, identify test points, use logic analyzers and/or JTAG debuggers

Not used

## 2. Radio-based analysis

- Use radio test tools like software-defined radios (SDR) or radio dongles with specific transceivers, try to identify and/or reverse engineer the used communication protocol (packet formats/framing, payloads, checksums)

## 3. Firmware analysis

- Get access to decrypt (e.g. dump, download, etc.), analyze firmware for

Not used

# Previous Work of (Other) Researchers

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

# Attack Surface and Attack Scenarios

1. Physical access to wireless alarm system
2. Attacking via radio signals (OTA)
  - Replay attacks
  - Brute-force attacks
  - Denial of service attacks
  - Jamming attacks
  - Sniffing attacks
  - Spoofing attacks
  - Cloning attacks

# Attack Surface and Attack Scenarios

1. ~~Physical access to wireless alarm system~~
2. Attacking via radio signals (OTA)
  - Replay attacks
  - Brute-force attacks
  - Denial of service attacks
  - Jamming attacks
  - Sniffing attacks
  - Spoofing attacks
  - Cloning attacks

Less interesting

More interesting



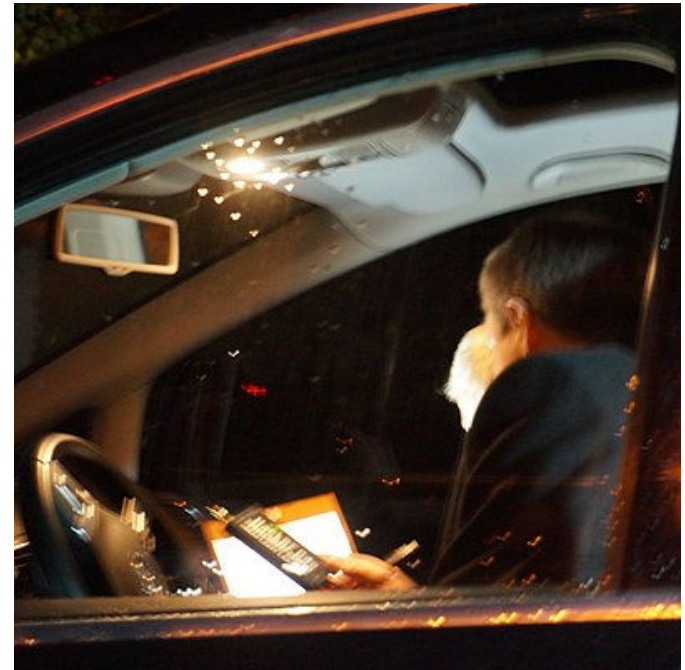
# Found Security Vulnerabilities



#	Product	Vulnerability Type	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 (FUM050110)	Authentication Bypass Using an Alternate Path or Channel (CWE-288)	SYSS-2020-014	CVE-2020-14158

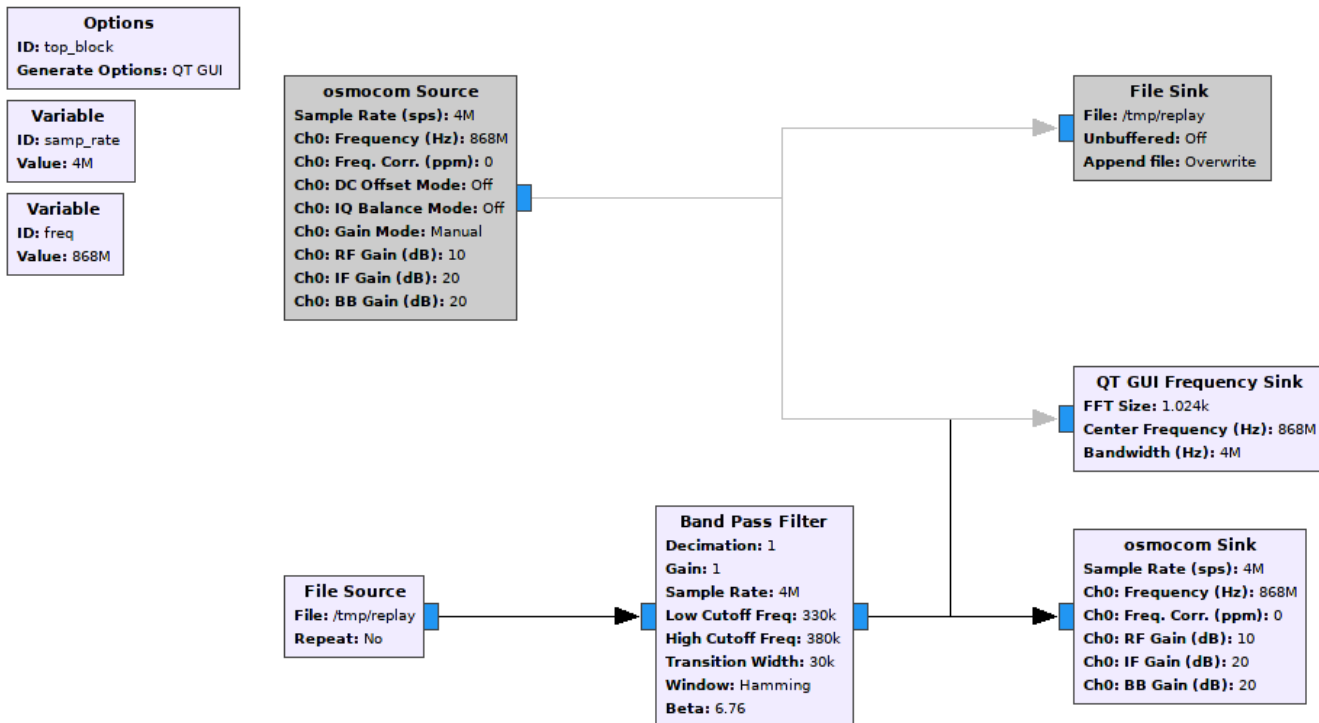
# Replay Attack

- **Very simple** radio-based attack
  - Just **record and later replay** an interesting radio signal (e. g. disarm signal)
  - Still many wireless devices with **proprietary communication protocols** are **missing or having an insufficient replay protection**
  - In 2016, **all the wireless alarm systems** we have tested **were vulnerable** to replay attacks
- ⇒ ***Deactivating the wireless alarm system in an unauthorized manner***



Source: German TV show Plusminus from 2016

# Replay Attack



Simple GNU Radio Companion Flow Graph for Replay Attacks

# Rolling Code Attack



**ABUS**  
Security Tech Germany

ABOUT ABUS | SERVICE | NEWS & PRESS | PARTNER | YOUR ENQUIRY |

HOME SECURITY | MOBILE SECURITY | COMMERCIAL SECURITY | GUIDE | PARTNERS WORLDWIDE

### Secvest Wireless Remote Control (Art. no. FUBE50015)

- ✓ User-friendly remote control with easily identifiable key symbols
- ✓ For use with Secvest, Secvest IP and Secvest 2 WAY wireless alarm systems
- ✓ Features 'arm', 'disarm' and 'status query' keys
- ✓ 8 LEDs provide an overview and display current system status
- ✓ Button for custom configuration available (Secvest wireless alarm system only)
- ✓ Communicates with the Secvest and Secvest Touch via a secure wireless connection

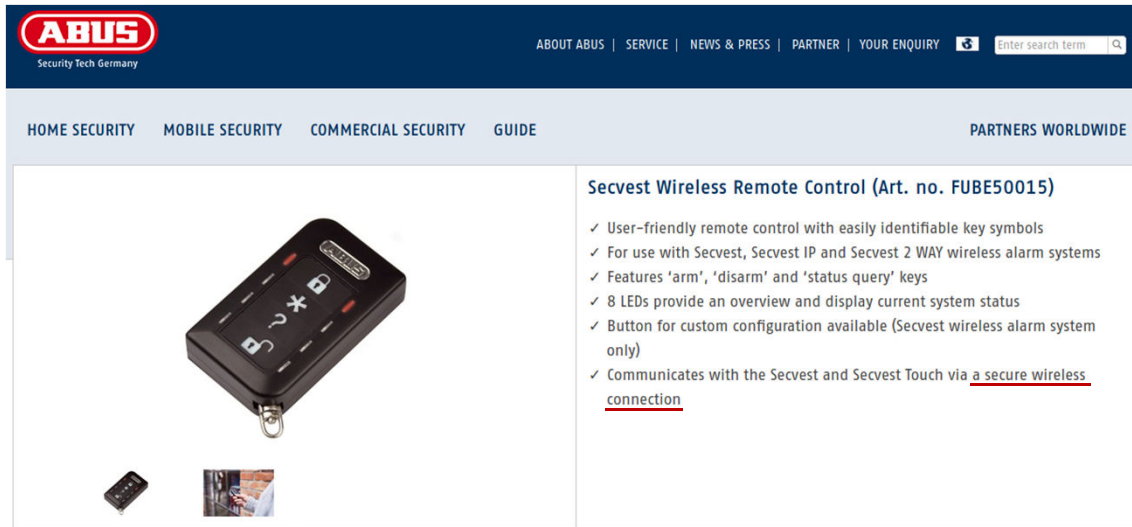
- In order to **fix the replay security vulnerability**, ABUS implemented a **rolling code** in newer remote controls (e. g. FUBE50014, FUBE50015)

Source: Product website for 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



**ABUS**  
Security Tech Germany

ABOUT ABUS | SERVICE | NEWS & PRESS | PARTNER | YOUR ENQUIRY | Enter search term

HOME SECURITY | MOBILE SECURITY | COMMERCIAL SECURITY | GUIDE | PARTNERS WORLDWIDE

### Secvest Wireless Remote Control (Art. no. FUBE50015)

- ✓ User-friendly remote control with easily identifiable key symbols
- ✓ For use with Secvest, Secvest IP and Secvest 2 WAY wireless alarm systems
- ✓ Features 'arm', 'disarm' and 'status query' keys
- ✓ 8 LEDs provide an overview and display current system status
- ✓ Button for custom configuration available (Secvest wireless alarm system only)
- ✓ Communicates with the Secvest and Secvest Touch via a secure wireless connection

Source: Product website for 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.

- In order to **fix the replay security vulnerability**, ABUS implemented a **rolling code** in newer remote controls (e. g. FUBE50014, FUBE50015)
- **Claim to use secure wireless communication now**

# Rolling Code Attack

- Unfortunately, the chosen rolling code implementation was **cryptographically weak**, as Thomas Detert found out
  - By observing the **unencrypted radio signals**, it was possible to **deduce the implemented rolling code algorithm**
  - Thus, valid future **rolling codes can be predicted**
- ⇒ *Deactivating the wireless alarm system in an unauthorized manner*
- ⇒ *Desynchronization of remote control (denial of service)*

# Demo: Rolling Code Attack



# Proximity Key Cloning Attack

- The ABUS Secvest wireless alarm system supports a **proximity key**
  - Unfortunately, the **insecure RFID technology MIFARE Classic** is used
  - Thus, the **information** stored on the used proximity keys **can be read easily** in a very short time from distances up to 1 meter
  - An attacker with **one-time access** can **clone a chip key**
- ⇒ ***Deactivating the wireless alarm system in an unauthorized manner***



ABUS Secvest proximity chip key



# Demo: Proximity Key Cloning Attack



# Reactive Jamming Attack

- The ABUS Secvest wireless alarm system has an **RF jamming detection**
- If there are unusual interferences on the used radio channel (868.6625 MHz), an alarm can be triggered (**RF Jamming** configuration)
- Thomas Detert found out that the implemented RF jamming detection is **insufficient**
- **Short jamming signals** (shorter than ABUS RF messages) are not detected
- Thus, an attacker is able to perform a **reactive jamming** attack

# Reactive Jamming Attack

- The **reactive jamming** simply **detects the start of an RF message** sent by a component of the ABUS Secvest wireless alarm system **and overlays it** with random data before the original RF message ends
  - Thereby, the receiver (alarm panel) is **not able to properly decode** the original transmitted signal
- ⇒ *Suppressing correctly received RF messages of the wireless alarm system in an unauthorized manner*

# Reactive Jamming Attack

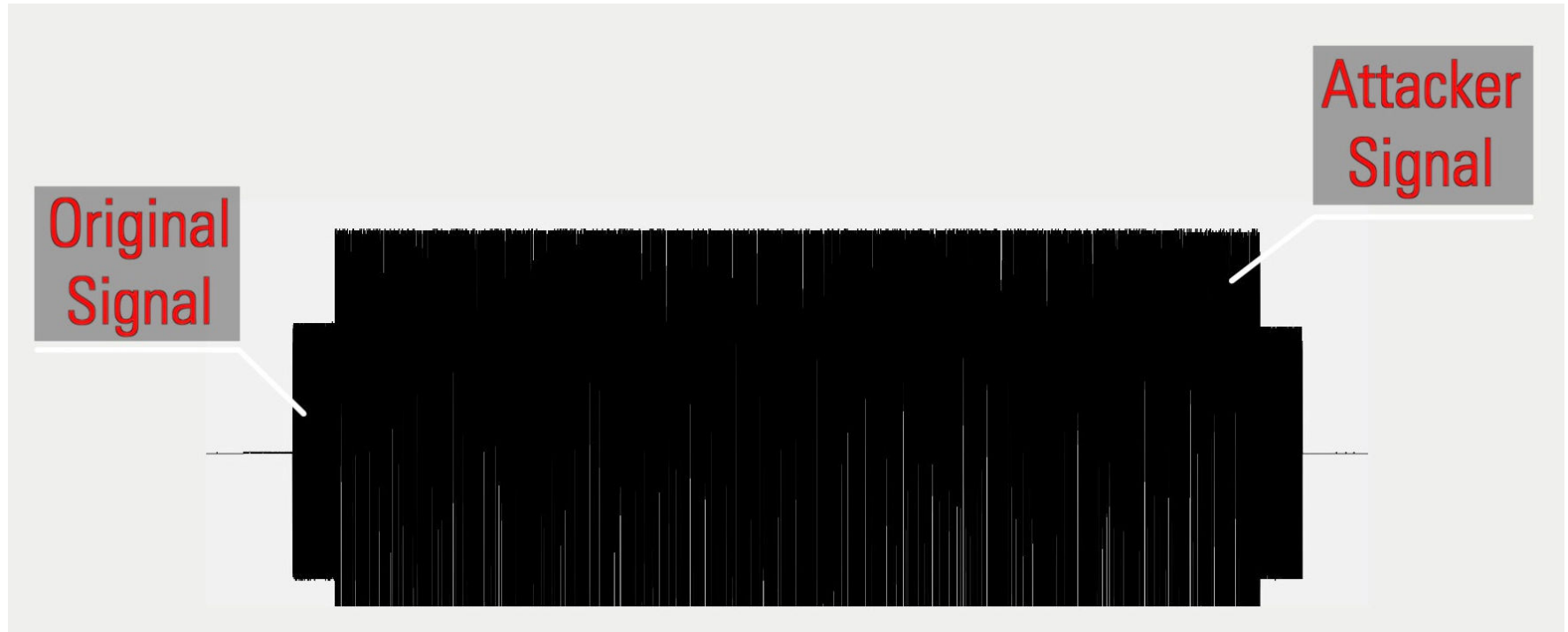
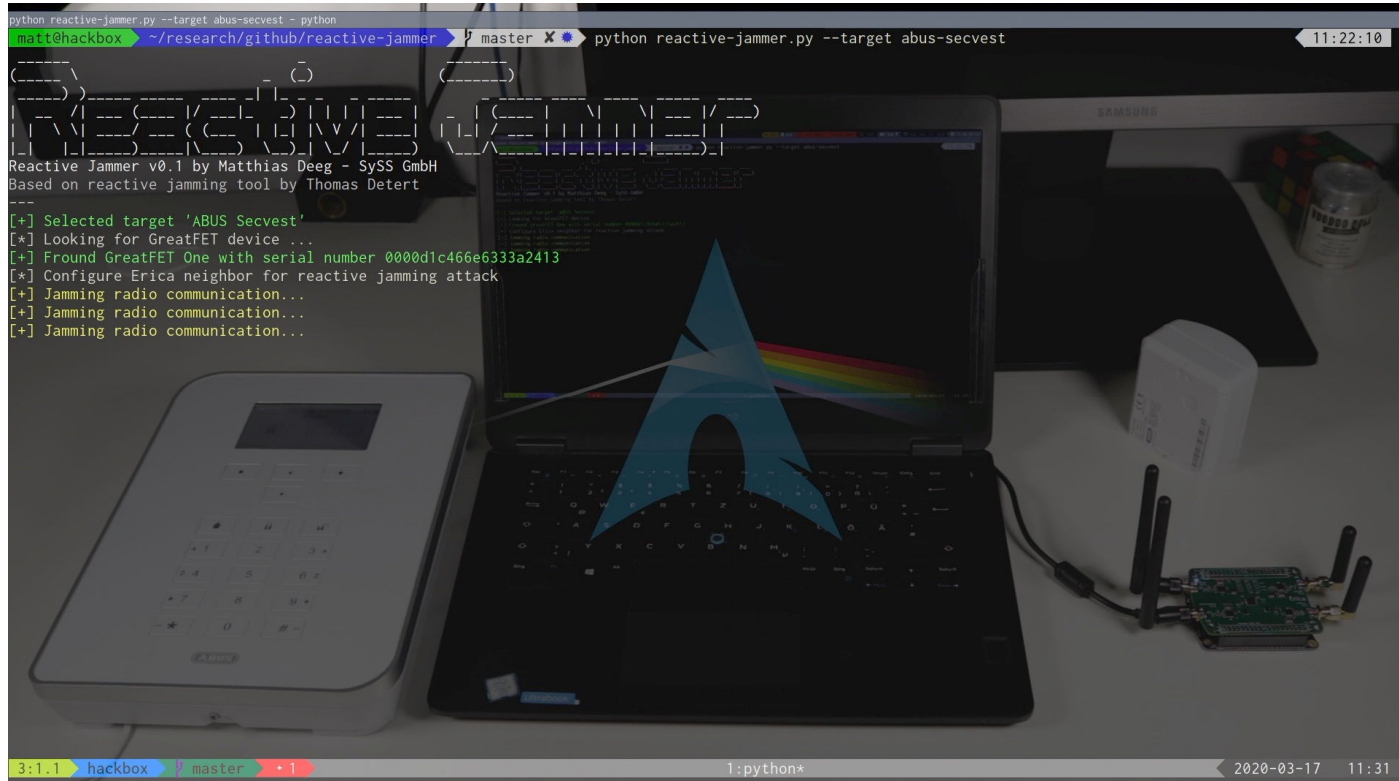
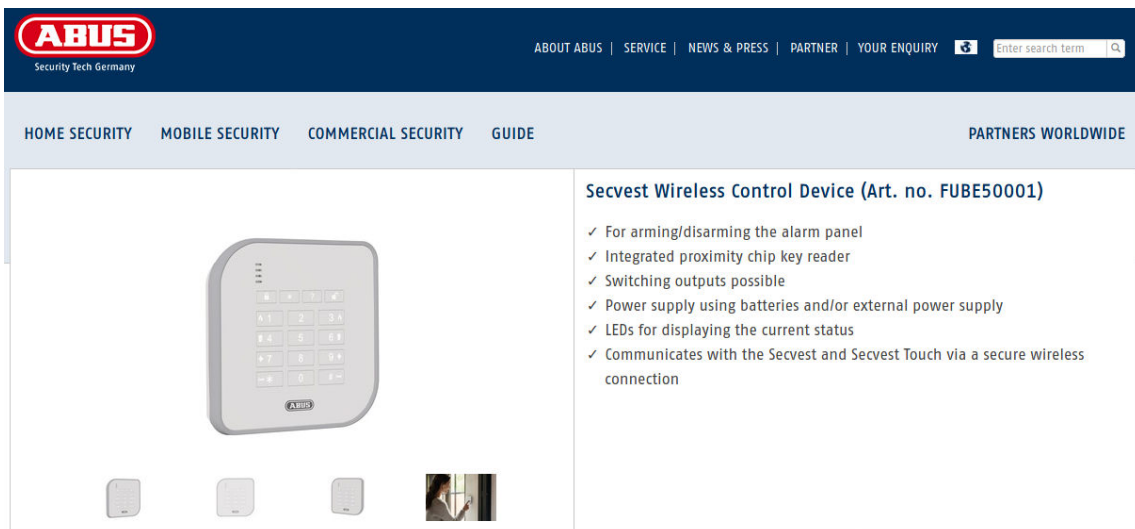


Illustration of a reactive jamming attack

# Demo: Reactive Jamming Attack



# Sniffing Attack



**ABUS**  
Security Tech Germany

ABOUT ABUS | SERVICE | NEWS & PRESS | PARTNER | YOUR ENQUIRY |

HOME SECURITY | MOBILE SECURITY | COMMERCIAL SECURITY | GUIDE | PARTNERS WORLDWIDE

### Secvest Wireless Control Device (Art. no. FUBE50001)

- ✓ For arming/disarming the alarm panel
- ✓ Integrated proximity chip key reader
- ✓ Switching outputs possible
- ✓ Power supply using batteries and/or external power supply
- ✓ LEDs for displaying the current status
- ✓ Communicates with the Secvest and Secvest Touch via a secure wireless connection

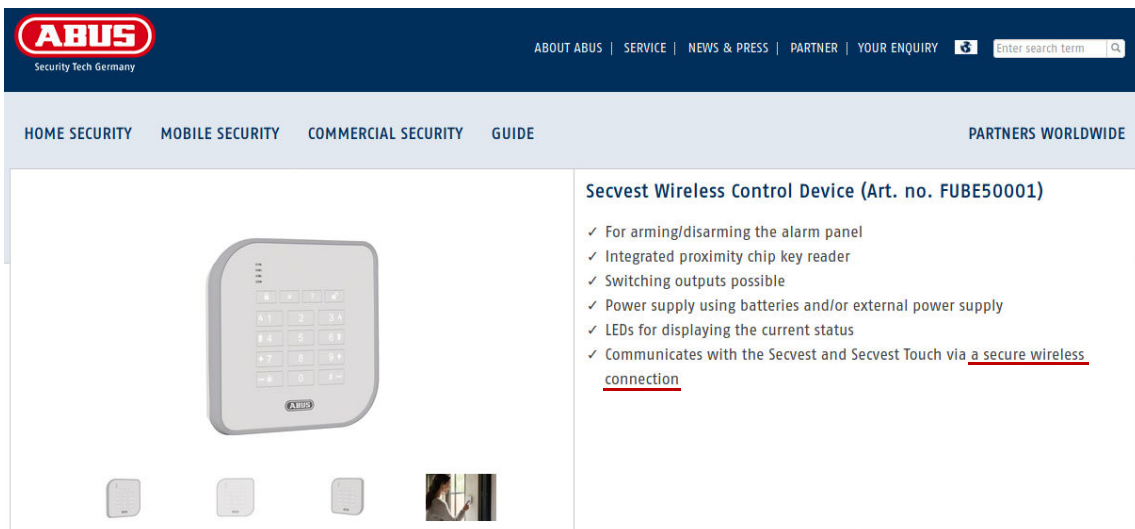
- Besides the wireless remote controls (e. g. FUBE50014, FUBE50015), there is also a wireless control device (FUBE50001)

Source: Product website for 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



**ABUS**  
Security Tech Germany

ABOUT ABUS | SERVICE | NEWS & PRESS | PARTNER | YOUR ENQUIRY |

HOME SECURITY | MOBILE SECURITY | COMMERCIAL SECURITY | GUIDE | PARTNERS WORLDWIDE

### Secvest Wireless Control Device (Art. no. FUBE50001)

- ✓ For arming/disarming the alarm panel
- ✓ Integrated proximity chip key reader
- ✓ Switching outputs possible
- ✓ Power supply using batteries and/or external power supply
- ✓ LEDs for displaying the current status
- ✓ Communicates with the Secvest and Secvest Touch via a secure wireless connection

- Besides the wireless remote controls (e. g. FUBE50014, FUBE50015), there is also a wireless control device (FUBE50001)
- **Claim** to use **secure wireless communication** now

Source: Product website for ABUS Secvest Wireless Control Device (FUBE50001)

## Secure wireless communication

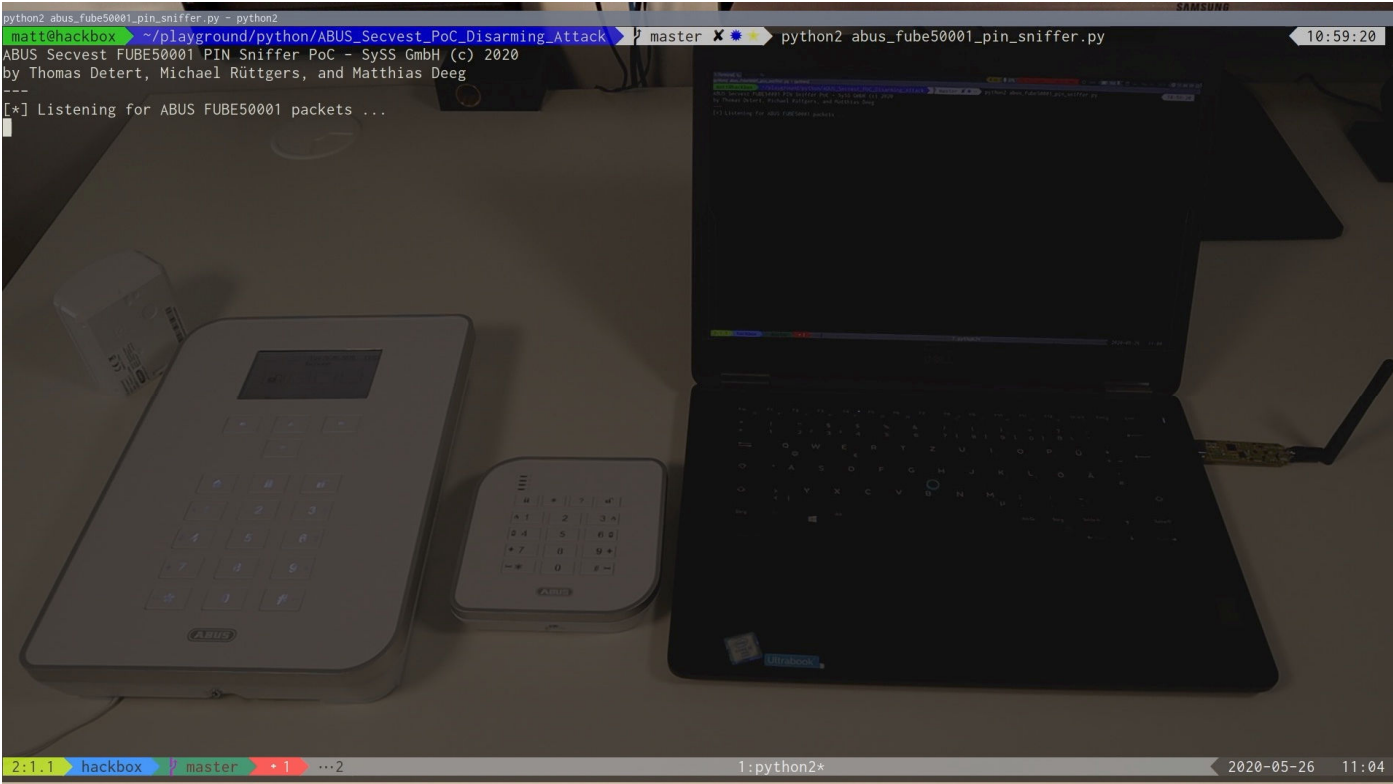
Thanks to a secure wireless communication procedure, this product is protected against 'replay attacks', as are the Secvest wireless alarm system and Secvest Touch alarm systems. This procedure for preventing third party tampering exceeds the requirements of the "DIN EN 50131-1 level 2" security standard.

# Sniffing Attack

- The used **secure wireless communication** is missing encryption
  - By observing radio signals of a wireless control panel it is possible to **see all sensitive data** of transmitted packets **as cleartext** and to **analyze** the used packet format and the communication protocol
- ⇒ *Eavesdropping sensitive data like PINs and proximity token IDs*
- ⇒ *Deactivating the wireless alarm system in an unauthorized manner*



# Demo: Sniffing Attack



# Demo: Sniffing Attack



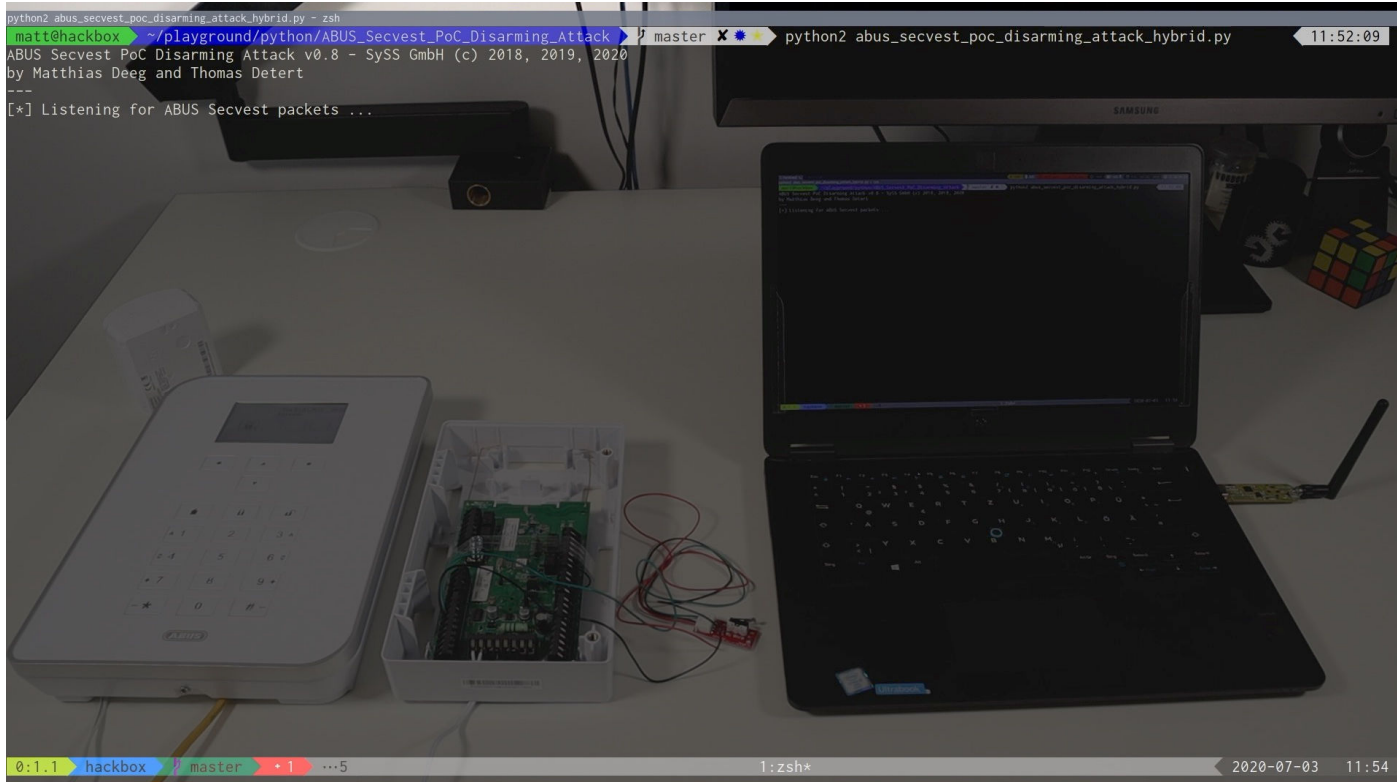
Example of a successful PIN code sniffing attack:

```
$ 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
d4cb34cb333332b34d4b530f0f0f33333333117162f5
[*] Decoded packet : da0a077ed5c549888800626b
[*] Received packet:
f0f352b4b32b4d352ad5332aab2cb34cd3332cccb4ccacb354acaaaaccccd2ab32aab54d30f0f0f352b4b32
b4d352ad5332aab2cb34cd3332cccb4ccacb354acaaa
[*] Decoded packet : da86937707e4884040a0c8ecff005e1fb9
[*] Detected FUBE50001 packet with FUBE50001 PIN
[+] Sniffed PIN code: 1337
(...)
```

# Spoofing Attack

- The ABUS Secvest Hybrid Module (FUM050110) can be used to **extend** an ABUS Secvest wireless alarm system **with wired components**
  - This module also allows to **integrate the ABUS wAppLoxx access control system**
  - The used wireless communication is **missing security features regarding confidentiality and integrity**
- ⇒ *Deactivating the wireless alarm system in an unauthorized manner*
- ⇒ *Bypassing the authentication of the wAppLoxx access control system*

# Demo: Spoofing Attack



# Conclusion

#	Product	Vulnerability Type	SySS ID	CVE ID	Fixed
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 (FUM050110)	Authentication Bypass Using an Alternate Path or Channel (CWE-288)	SYSS-2020-014	CVE-2020-14158	✗

# Conclusion

- Security products like wireless alarm systems **may be more vulnerable** to different kind of **radio-based attacks** than you would first assume
- **Marketing claims** regarding security features may just be that: marketing claims
- Product certificates like **VDS Home** and **EN 50131-1 Grade 2** may give a **false sense of *real word* security**
- Some security vulnerabilities are **hard or even impossible to fix** in hardware products already in use (e. g. no update functionality, compatibility issues)
- ***Forever bugs*** may affect the security of a product until its end of life

# Recommendation

- Choose your wireless alarm system wisely
- Perform a thorough online research before buying such a product
- Reconsider your previous decision for using a wireless alarm system
- Do not have too much faith in product certificates and marketing claims
- Ask for further security testing beyond product certification and the scope of those tests (very important)

# References



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](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](https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_09_27_SDR_-_Weniger_Theorie_mehr_Praxis.pdf), 2017



# References



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

# References



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=PidiWcB0tml>, 2020

# Thank you very much ...

... for your attention.

Do you have any questions?

E-mail: [matthias.deeg@syss.de](mailto:matthias.deeg@syss.de)

Twitter: [@matthiasdeeg](https://twitter.com/matthiasdeeg)

YouTube: <https://www.youtube.com/c/SySSPentestTV>



# THE PENTEST EXPERTS

[WWW.SYSS.DE](http://WWW.SYSS.DE)