Cybersecurity - Attacks on smarthomes and IoT made easy

Cyber industry in transition seminar, Helsinki 2023

Prof. Dr.-Ing. Andreas Noack
<andreas.noack@hochschule-stralsund.de>

Who am I?

Prof. Dr.-Ing. Andreas Noack

Vita

- Born 1982, married with 3 children
- Applied Computer Sciences (B.Sc.)
- IT Security (M.Sc. and PhD)
- Since 2011 Professor for Communication Networks/IT Security at University of Applied Sciences Stralsund

Misc: *Founder and Head of Stralsunder IT-Sicherheitskonferenz (since 2012), Head of Institute for Secure Mobile Communication (ISMK), Book author (2x), Digitization ambassador of Mecklenburg-Vorpommern, Judo trainer*

Research focus

Efficient cryptographic protocols ⇒ *Internet of Things (IoT), Smarthome, ... [16][20][21]*

Smarthome – Digitization at home

The future of our houses is smart

In the future our houses will be fully automatic: *light, heating, doors and windows communicate with us and with each other, adjust to human needs!*

There are many products on the market:
Brennenstuhl, Homematic (IP), innogy SmartHome (RWE), Magenta SmartHome, ...
...and an even wider range of products on the international market

Smarthome – Smart and secure home?

What do most smarthome products have in common?
– They use **proprietary** radio protocols for which there are **no** open interfaces available to the end user.

However, note that:

Smarthome devices are often very small and are built to consume little energy. . .

What does that mean?
little resources ≈ little security!

What can possibly go wrong?

How to attack radio protocols?

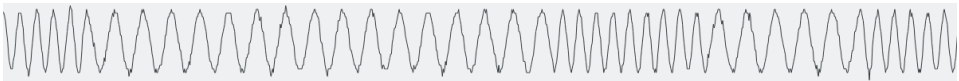
- **Replay/Relay**. Resend old messages (**Replay**), Extending frames via other communication links such as WLAN/ mobile radio (**Relay**).
  ⇒ *Light turns on/off again, heating turns on/off, ...*
  ⇒ *Keyless-Go car opens, Immobiliser disengages, ...*
- **Address-Spoofing**. Change destination/source address in protected messages and replay them.
  ⇒ *Electronic door lock opens, ...*
- **Out-of-Sync DoS**. An attack on sequence numbers can desynchronise a device in a smarthome network.
  ⇒ *Suddenly smarthome devices stop working, ...*

Modulation, Encoding and Encryption

Analysis of a radio protocol on the 868.3MHz band

...needs some **steps**. This makes hacking more difficult, which is **good** for security!

- **Modulation**. Bits are ”hidden” in the frequency (FSK), amplitude (ASK) or phase (PSK) of sine waves.



- **Encoding**. Encodings are often used to add redundancy or prevent long 0/1 sequences (Example: differential encoding).

$$1000101 \rightarrow 100111$$

- **[Encryption]**. Obfuscation or encryption (e.g. AES) is used in some cases.

$$100111 \rightarrow 010101$$

The logic of smarthome protocols

Typical smarthome messages (middle/upper price segment)

Received, demodulated, decoded and displayed as hexadecimal values:

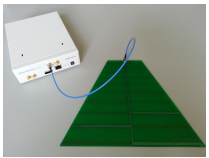
`aa aa aa aa e9 ca e9 ca 0b 24 a6 40 12 34 56 ab cd ef 01 0d c2 03`

- `aa aa aa aa` – *Introduction, preamble: 10101010...*
- `e9 ca e9 ca` – *Synchronisation (manufacturer constant)*
- `0b` – *Length of payload (11 Byte)*
- `24` – *Sequence number (36)*
- `a6 40` – *Message type*
- `12 34 56 ab cd ef` – *Source address and destination address*
- `01 0d` – ***Command**: Open door, Turn light on, Open roller shutter...*
- `c2 03` – *Checksum (CRC16 variant)*

Motivation for the Universal Radio Hacker

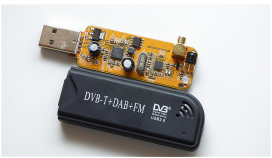
The problem: Many security researchers cannot access radio protocols

- Most of the protocol specifications are not public.
- Proprietary communication hardware does not allow analysing



Ettus
USRP-N210 (RX&TX)

Great Scott Gadgets
HackRF One (RX&TX)



Realtek
RTLSDR (RX)

The solution

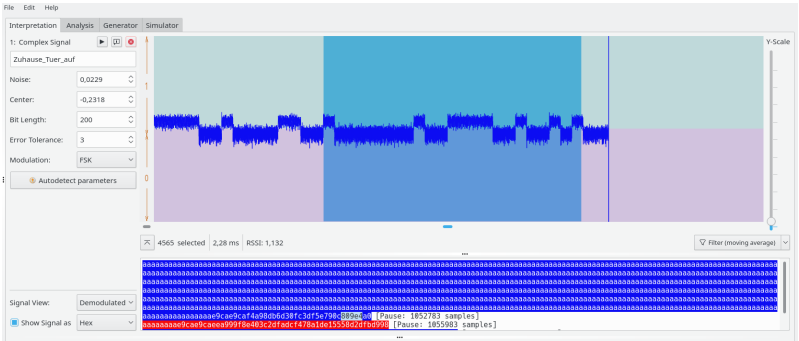
With **Software Defined Radios**, nearly any radio communication can be recorded and sent. *Is there an app for modulation, encoding **and** analysis?*
⇒ **Universal Radio Hacker** [22]

Universal Radio Hacker

Design goals: Universal Radio Hacker

Intuitive operation, abstraction from hardware layer, automatic recognition of parameters and open interfaces [17].

⇒ *Easy access for electrical engineering laymen and theoreticians*

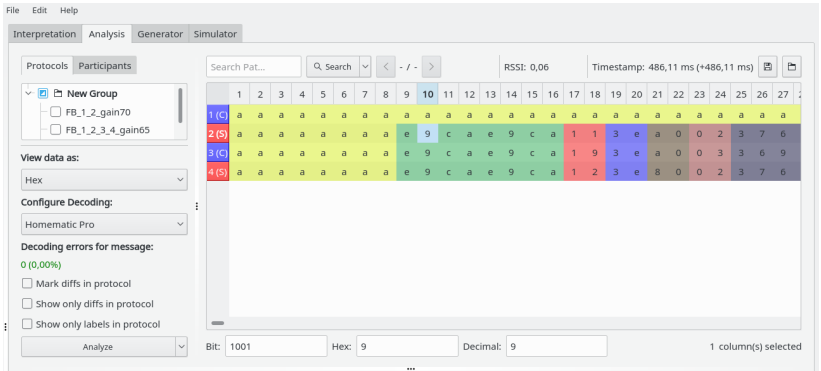


Universal Radio Hacker, **Interpretation** (Demodulation of raw signal, Representation=Square wave signal [Demodulated])

Universal Radio Hacker II

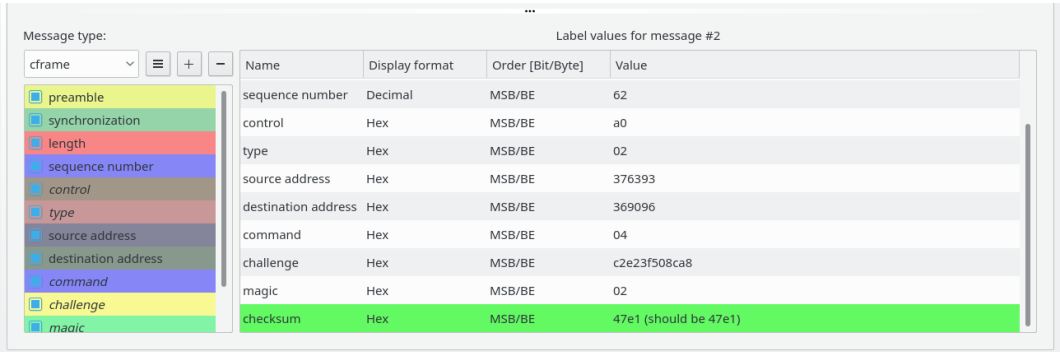
Protocol logic analysis

- **Differential** analysis: Highlighting changes compared to reference line and **automatic recognition** of protocol fields [18].



Universal Radio Hacker, **Analysis** (Protocol logic analysis)

Universal Radio Hacker II



Universal Radio Hacker, **Analysis** (Wireshark-like preview per message)

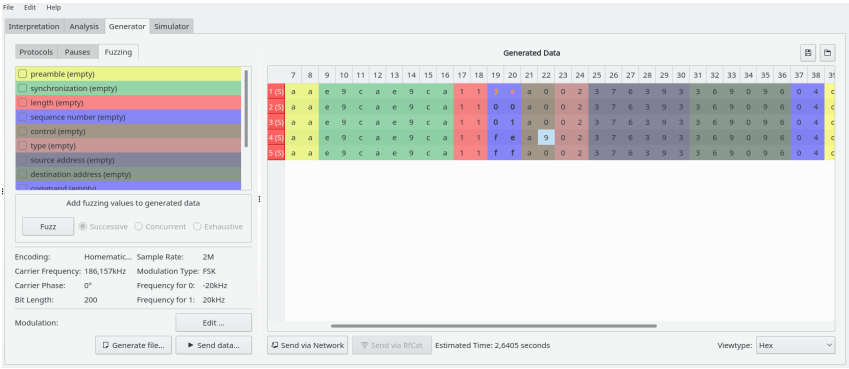
Protocol logic analysis

- Different manually configurable **encodings**, **message types** (*Data, ACK, ...*) and **labels** for protocol fields (*name, color, representation*).

Universal Radio Hacker III

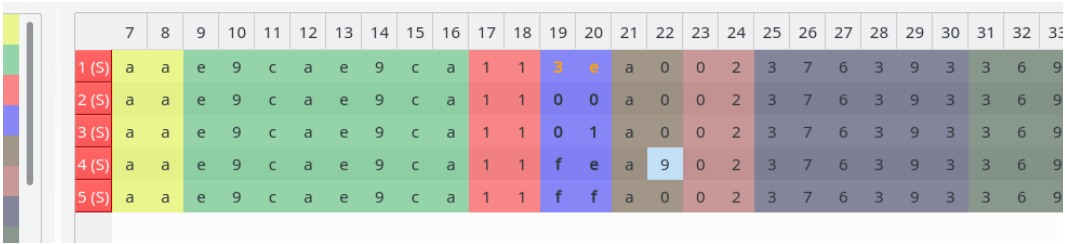
Generating signals

- Wizard with autodetection of **modulation parameters**
- **Encoding** is added automatically before sending



Universal Radio Hacker, **Generation** (Modulation of modified data, incl. fuzzing)

Universal Radio Hacker III

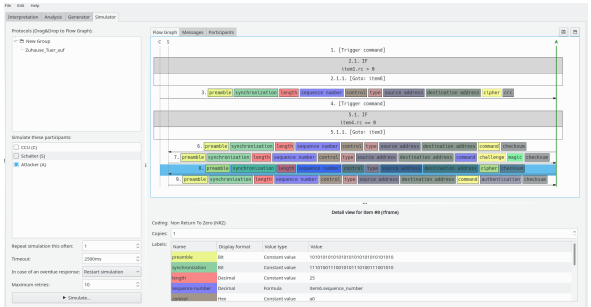


Universal Radio Hacker, **Generation** (Modulation of modified data, incl. fuzzing)

Generation features

- **Fuzzing** (Range, Boundaries, Random) of protocol fields
- Each message is manually **editable**
- Configured **checksums** are calculated automatically

Universal Radio Hacker IV



Universal Radio Hacker, **Simulation** (Real-time simulation of a participant for protocols with statemachines)

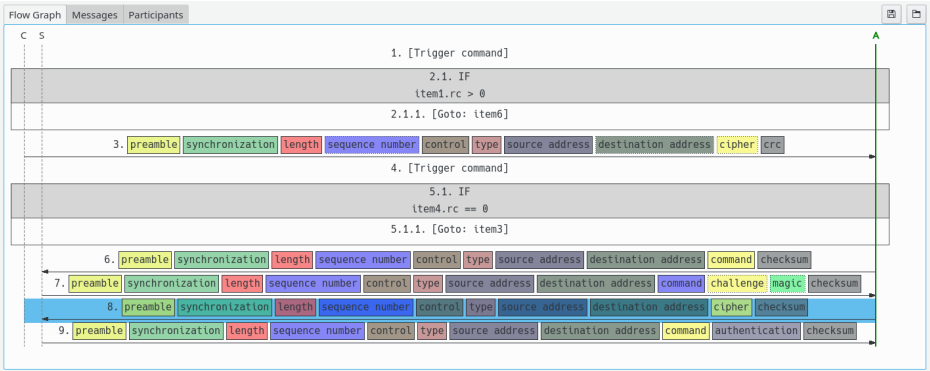
Simulation features

- Real-time simulation with statemachines
- Dynamic **check/calculation** of protocol fields, **external** programs possible!
- Delay depending on SDR and computer (from approx. 100ms)

Universal Radio Hacker IV

Protocol flow for attack on current smarthome system (→ Video)

1. Extract AES key from learning process (2 messages)
2. Open door lock with 4 messages (AES-128)



Universal Radio Hacker, **Simulation** (Real-time simulation of a participant for protocols with statemachines)

Outlook: Typical vulnerabilities

Typical vulnerabilities in IoT products...

- The **key exchange** is often done in plain text.
- **Independence** of hardware and software logic, e.g. addresses or counters are not protected with the included *MAC*, but only by a non-cryptographic *checksum* at the message end.
- **Statemachine**. Problems between hardware and software logic, e.g. incrementing a counter **before** checking the *MAC*.
- **Security-by-Obscurity**. Pseudo-cryptography, mostly ”encryption” with constants
- **Weak cryptography**. Linear systems, short key lengths or poor operation mode for block ciphers.
- **Relay/Jamming**. Extending the signal via e.g. mobile radio or jamming the signal.

`#KeylessGo #CentralLocking #Car #Supermarket`

Conclusion

*Tools such as **Universal Radio Hacker** can be used to analyse proprietary radio protocols and perform penetration testing on IoT systems.*

What does that mean?

IoT protocols can now also be examined by theoretical experts! Manufacturers **must** adapt to this, *security-by-obscurity* is **no** longer an option!

Some results and impressions

- About 50% of the examined devices, especially cheap ones, have **no** security mechanisms!
- There are relatively expensive devices that can be **physically** destroyed via radio (*manufacturer informed*).
- The expertise of many manufacturers in the field of IT security is in need of improvement.

Outlook: Security on the road

Flipper Zero

The **Flipper Zero** is a tiny and portable hacking device with many communication interfaces, e.g. *IR*, *RFID*, *Bluetooth*, *radio ISM bands* and more.

URH can export radio signals directly to the Flipper Zero. Happy hunting!

Source: Stralsund Old Town

Thank you for your attention!

https://github.com/jopohl/urh

Literatur I

[1] Patrick-Benjamin Bök und Andreas Noack. *Technische Grundlagen von Computernetzen – Techniken, Standards und Systeme*. Lehrbuch, W3L-Verlag, ISBN 978-3-86834-054-9. 2015.

[2] C. Müller, I. Szekely und A. Noack. “Ethernet communication for detection of emergency locations and dynamic evacuation in underground infrastructures”. In: *Optimization of Electrical and Electronic Equipment (OPTIM), 2010 12th International Conference on*. IEEE. 2010, S. 1046–1051.

[3] Christoph Müller und Andreas Noack. *Mining Network and the Security Question*. 35th APCOM Symposium - Application of Computers and Operations Research in the Mineral Industry, Australia. Sep. 2011.

Literatur II

[4] Christoph Müller und Andreas Noack. *Safety Support Functions for Underground Network Communications*. 35th APCOM Symposium - Application of Computers and Operations Research in the Mineral Industry, Australia. Sep. 2011.

[5] A. Noack. “Efficient Authenticated Wireless Roaming via Tunnels”. In: *Quality of Service in Heterogeneous Networks* (), S. 739–752.

[6] Andreas Noack. *Efficient Cryptographic Protocols for Wireless Mesh Networks*. Dissertation, Ruhr-Universität Bochum, Universitätsbibliothek. 2011.

[7] Andreas Noack. *Trust Agreement in Wireless Mesh Networks*. WISTP’11 - Workshop in Information Security Theory and Practice, Greece. Juni 2011.

Literatur III

[8] Andreas Noack, Patrick-Benjamin Bök und Sebastian Krück. *Evaluating the Impact of Transmission Power on QoS in Wireless Mesh Networks*. IEEE ICCCN 2011 Workshop on Context-aware QoS Provisioning and Management for Emerging Networks, Applications and Services - ContextQoS 2011, Hawaii. Juli 2011.

[9] Andreas Noack und Mark Borrmann. “Mutual Preimage Authentication for Fast Handover in Enterprise Networks”. In: *On the Move to Meaningful Internet Systems: OTM 2010*. Hrsg. von Robert Meersman, Tharam Dillon und Pilar Herrero. Bd. 6426. Lecture Notes in Computer Science. Heidelberg: Springer, 2010, S. 583–599. ISBN: 978-3-642-16933-5.

[10] Andreas Noack und Christoph Müller. *Mobile Machine Operation in Underground Networks and the Security Question*. 8th conference: escar’10 - Embedded Security in Cars. Nov. 2010.

Literatur IV

[11] Andreas Noack und Jörg Schwenk. “Group Key Agreement for Wireless Mesh Networks”. In: *34th IEEE LCN & Workshops Conference Proceedings*. 2009, S. 945–952.

[12] Andreas Noack und Jörg Schwenk. “Group Key Agreement Performance in Wireless Mesh Networks”. In: *35th IEEE LCN & Workshops Conference Proceedings*. 2010, S. 176–179.

[13] Andreas Noack und Stefan Spitz. “Dynamic Threshold Cryptosystem without Group Manager”. In: *International Journal of Network Protocols and Algorithms (ISSN: 1943-3581)* 1.1 (2009), S. 108–121. URL: http://www.macrothink.org/journal/index.php/npa/issue/view/14/showToc.

Literatur V

[14] Emmanouil Panaousis u. a. *Game-Theoretic Model of Incentivizing Privacy-Aware Users to Consent to Location Tracking*. RATSP 2015 – The 2015 IEEE International Symposium on Recent Advances of Trust, Security and Privacy in Computing and Communications. 2015.

[15] Marcell Müller Patrick-Benjamin Boök Andreas Noack und Daniel Behnke. *Computernetze und Internet of Things – Technische Grundlagen und Spezialwissen*. Wiesbaden: Springer Fachmedien Wiesbaden GmbH Springer Vieweg, 2020. ISBN: 9783658294083.

[16] Johannes Pohl. *Universal Radio Hacker: Investigate Wireless Protocols Like a Boss - Arsenal Theater Demo*. Black Hat USA - Arsenal. 2017. URL: https://www.blackhat.com/us-17/arsenal.html#universal-radio-hacker-investigate-wireless-protocols-like-a-boss-arsenal-theater-demo.

Literatur VI

[17] Johannes Pohl und Andreas Noack. *Automatic Modulation Parameter Detection In Practice*. Reversing and Offensive-oriented Trends Symposium 2019 (ROOTS) co-located with DeepSec 2019. 2019.

[18] Johannes Pohl und Andreas Noack. “Automatic Wireless Protocol Reverse Engineering”. In: *13th USENIX Workshop on Offensive Technologies (WOOT 19)*. Santa Clara, CA: USENIX Association, Aug. 2019. URL: https://www.usenix.org/conference/woot19/presentation/pohl.

[19] Johannes Pohl und Andreas Noack. *I see you: On Neural Networks for Indoor Geolocation*. ESANN 2015 – European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. 2015.

Literatur VII

[20] Johannes Pohl und Andreas Noack. “Universal Radio Hacker: A Suite for Wireless Protocol Analysis”. In: *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. IoTS&P ’17. Dallas, Texas, USA: ACM, 2017, S. 59–60. ISBN: 978-1-4503-5396-0. DOI: 10.1145/3139937.3139951. URL: http://doi.acm.org/10.1145/3139937.3139951.

[21] Johannes Pohl und Andreas Noack. *Universal Radio Hacker: Investigate Wireless Protocols like a Boss*. Hakin9 OPEN – Open Source Tools, Vol.12, No. 14. 2018.

[22] Johannes Pohl und Andreas Noack. *Universal Radio Hacker: investigate wireless protocols like a boss*. GitHub-Repository: https://github.com/jopohl/urh. 2021.