

# Universal Radio Hacker

A Suite for Analyzing and Attacking Stateful Wireless Protocols

Johannes Pohl and Andreas Noack

University of Applied Sciences Stralsund

August 13, 2018

# Proprietary wireless protocols everywhere

## Smart Home

- Increase comfort through wireless sockets, door locks, valve sensors...
- Devices are designed under size and energy constraints
- Less resources for cryptography



## Risks of Smart Home

- Manufactures design custom *proprietary wireless protocols*
- Hackers may take over households and e.g. break in without physical traces

*How can we eavesdrop and manipulate the wireless communication between such devices to assess the security?*

# Software Defined Radio

## Why Software Defined Radios?

- Send and receive on nearly arbitrary frequencies<sup>a</sup>
- Flexibility and extendability with *custom software*

<sup>a</sup>e.g. HackRF: 1 MHz - 6 GHz



(a) USRP N210



(b) HackRF

# Software Defined Radios are affordable

Last Checked: July 21, 2018



## NooElec HackRF One Software Defined Radio (SDR)

by NooElec

**\$317<sup>95</sup>** ✓prime

Get it by **Wednesday, Jul 25**

FREE Shipping on eligible orders



## NooElec NESDR SMARt - Premium RTL-SDR Software Defined Radio

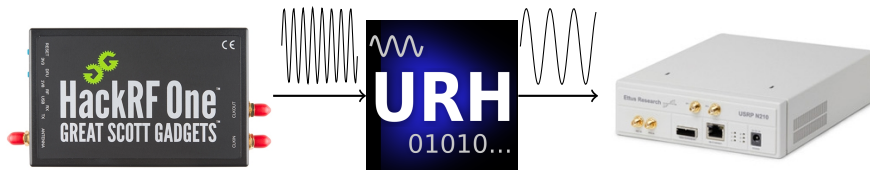
by NooElec

**\$23<sup>95</sup>** ✓prime

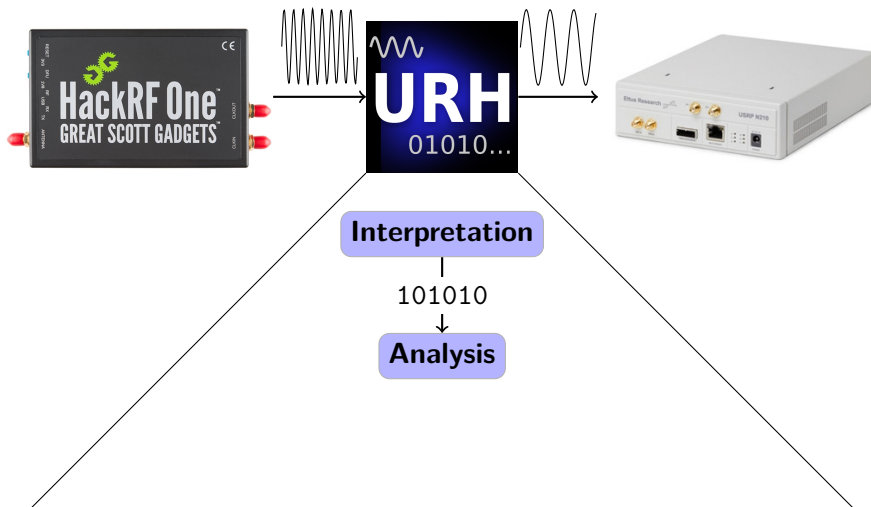
Get it by **Wednesday, Jul 25**

FREE Shipping on eligible orders

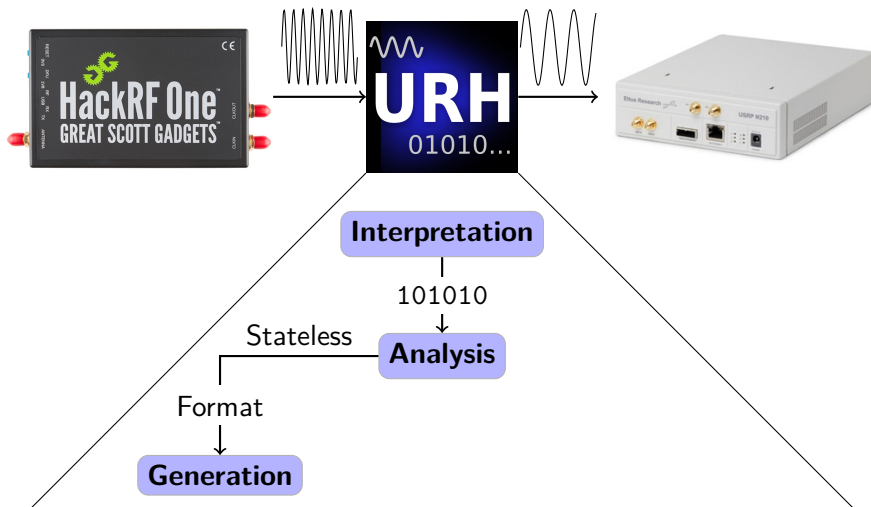
# Universal Radio Hacker



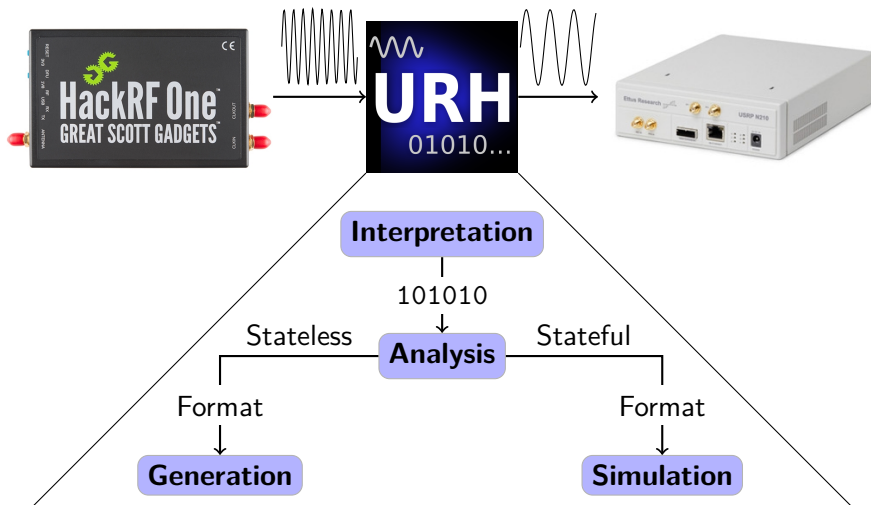
# Universal Radio Hacker



# Universal Radio Hacker

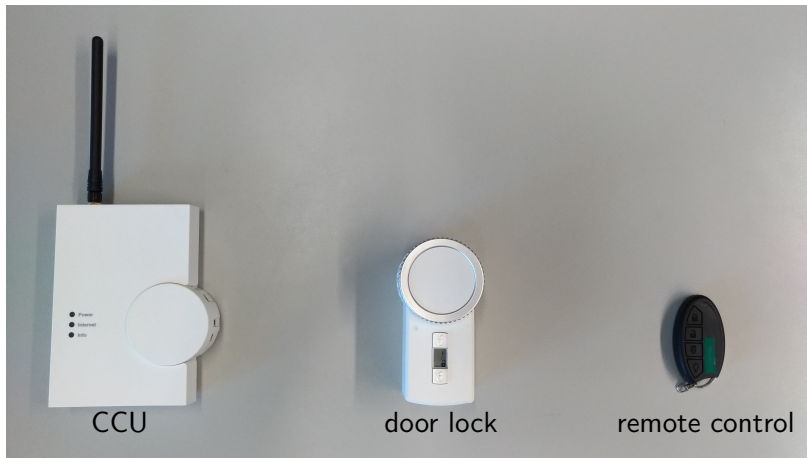


# Universal Radio Hacker

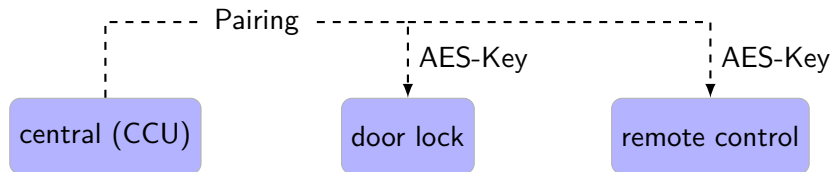




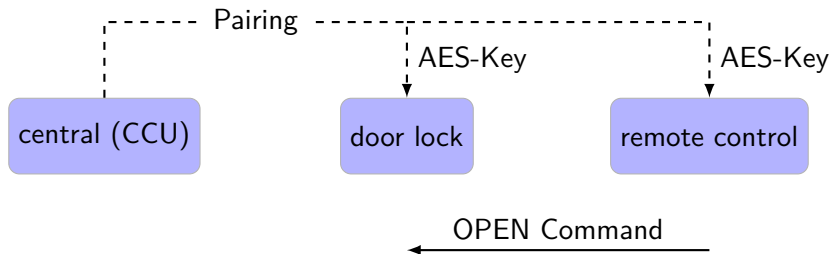
# Setup



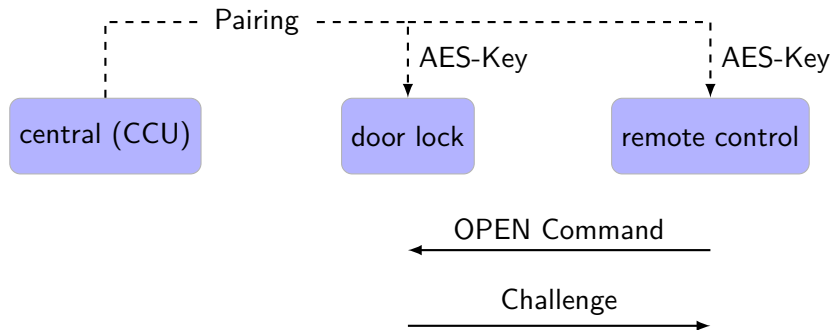
# Overview



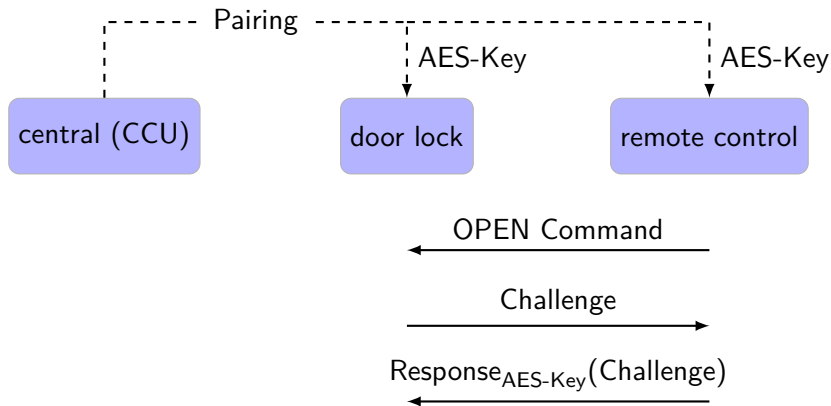
# Overview



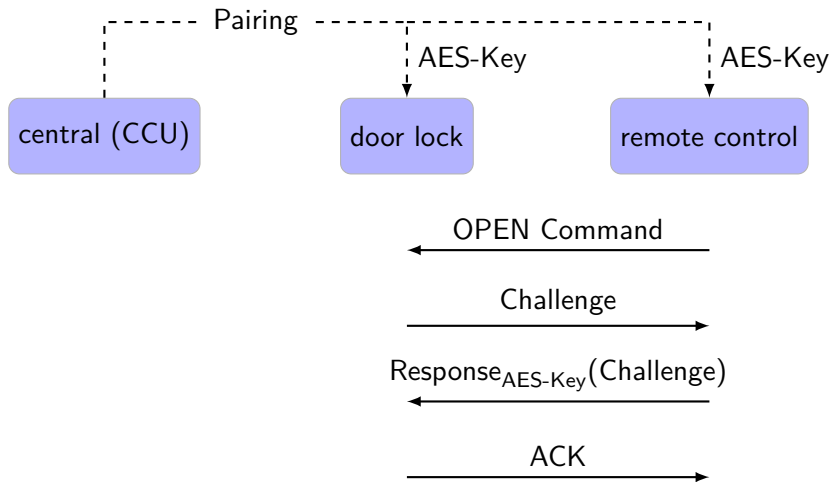
# Overview



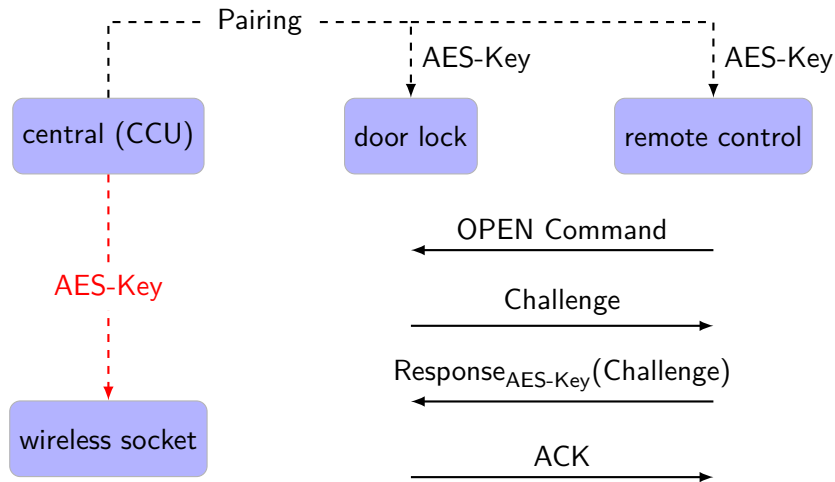
# Overview



# Overview



# Overview

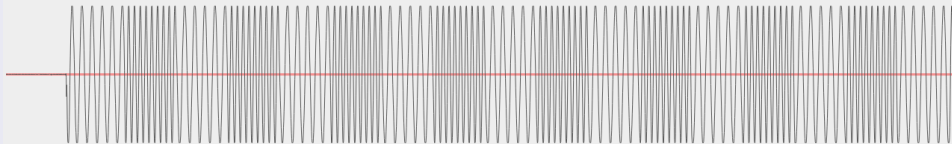


# Record and demodulate signal

## Capture of door lock open communication

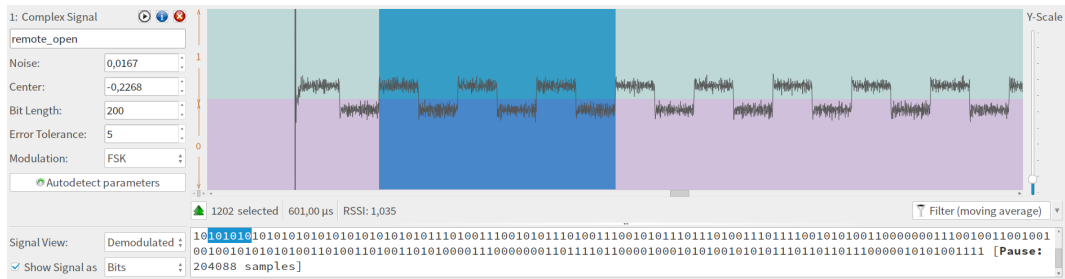


## Zoom into start of second message





# Demodulation and Signal Editing with URH



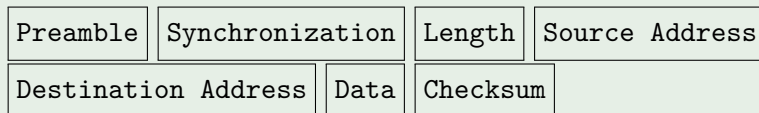
## Further Interpretation Features

- **Synchronized selection** between demodulated and raw signal
- **Signal Editor** i.e. copy, paste, crop, mute signal selections
- Configurable moving average and bandpass **filters**

# Analysis phase

In Analysis phase we reverse engineer the *protocol format*.

## Example format



This includes

- **Decode** messages
- **Labeling** of protocol fields
- **Group** messages by assigning message types

# What kind of decoding does the door lock use?

All messages are encoded in the following way

- 1 Pseudo encryption
- 2 Data Whitening
- 3 (Modulation)

# Pseudo Encryption

## Code

```
enc[0] = msg[0];  
enc[1] = ~(msg[1]) ^ 0x89;  
for(i = 2; i < NUM_BYTES; i++)  
    enc[i] = (enc[i-1]+0xdc) ^ msg[i];
```

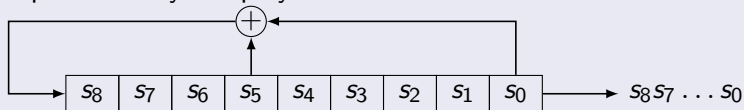
## Use

- Does not increase the security
- Assumption: Obscure method for pseudo security

# Data Whitening

## Data Whitening

- To increase transmission quality a *data whitening* is used
- XOR with each 8 LSB of a pseudo-random sequence generated by an LFSR represented by the polynomial  $x^9 + x^5 + x^0$



- Initial state is 111111111

## First eight states of the LFSR

111111111  $\Rightarrow$  011111111  $\Rightarrow$  001111111  $\Rightarrow$  000111111  $\Rightarrow$   
000011111  $\Rightarrow$  100001111  $\Rightarrow$  110000111  $\Rightarrow$  111000011

# Decodings with URH

The screenshot shows the URH software interface with the following components:

- MyDecoding** dropdown menu and a **Delete** button.
- Base Functions** list: Edge Trigger, Morse Code, Substitution, External Program.
- Additional Functions** list: **Invert** (highlighted), Differential Encoding, Change Bitorder, Remove Redundancy, Remove Carrier, Remove Data Whitening (CC1101), Wireless Short Packet (WSP), Cut before/after.
- Decoder** section: **Signal** (Invert, Change Bitorder, Invert #2) and **Decoded Bits**.
- Information and Options** section: **## DECODING PROCESS ##**, **Invert:**, and *All bits are inverted, i.e. 0->1 and 1->0.*
- Signal (0,1):** Test dropdown and input field containing **10010110**.
- Decoded Bits:** [Decoding Errors = 0] and input field containing **01101001**.
- Waveform** display showing the signal and its decoded state.

# Result in URH after decoding and labeling

Protocols Participants

Enter patter... Search - / -

RSSI: 0,30 Timestamp: 606,92 ms (+124,59 ms)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

1	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	
2	a	a	a	a	a	a	a	a	a	e	9	c	a	e	9	c	a	1	1	0	a	0
3	a	a	a	a	a	a	a	a	a	e	9	c	a	e	9	c	a	1	9	0	a	0
4	a	a	a	a	a	a	a	a	a	e	9	c	a	e	9	c	a	1	2	0	a	8

Other Options: Select all, Filter, Align

Analyze Bit: 11101001 Hex: e9 Decimal: 233 2 column(s) selected

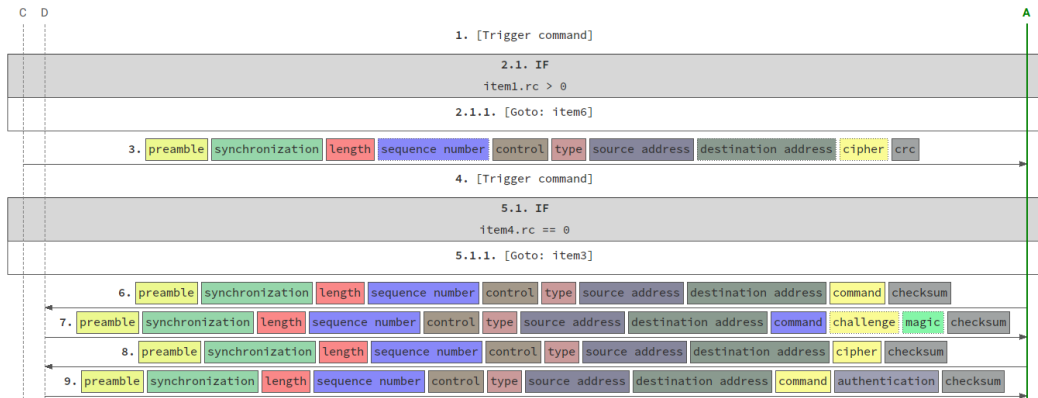
Message type:

Name	Display format	Order [Bit/Byte]	Value
preamble	Bit	MSB/BE	101010101010101010101010101010
synchronization	Hex	MSB/BE	e9cae9ca
length	Decimal	MSB/BE	25
sequence number	Decimal	MSB/BE	10
control	Hex	MSB/BE	a0
type	Hex	MSB/BE	03
source address	Hex	MSB/BE	58a6c8
destination address	Hex	MSB/BE	586505
cipher	Hex	MSB/BE	065d1942f465940f96b71521b83adf52
checksum	Hex	MSB/BE	ddf8 (should be ddf8) ← -- -- Check against configurable CRC

Assign manually or rule based

# Simulation phase

*In Simulation phase we can work on the logical layer. URH takes care of **Modulation** and **Encoding** during simulation time.*





# Demonstration Video

# Summary and future work

## Summary

- **Software Defined Radios** offer a high flexibility when investigating radio protocols
- Tools like **Universal Radio Hacker** abstract the required HF basics and enable analyzing such protocols without having to be a hardware expert
- Smart Home manufactureres have to react, Security by Obscurity is no longer an option

## Ongoing work

- Rule based intelligence for automatic analysis phase
- Enhance accuracy of detecting interpretation parameters
- Support for more complex modulations e.g. 4-PSK



 <https://github.com/jopohl/urh>   

## Contact

- E-Mail: [Johannes.Pohl90@gmail.com](mailto:Johannes.Pohl90@gmail.com)  
E-Mail: [Andreas.Noack@hochschule-stralsund.de](mailto:Andreas.Noack@hochschule-stralsund.de)
- Slack: <https://bit.ly/2LGpsra>
- GitHub: <https://github.com/jopohl>