



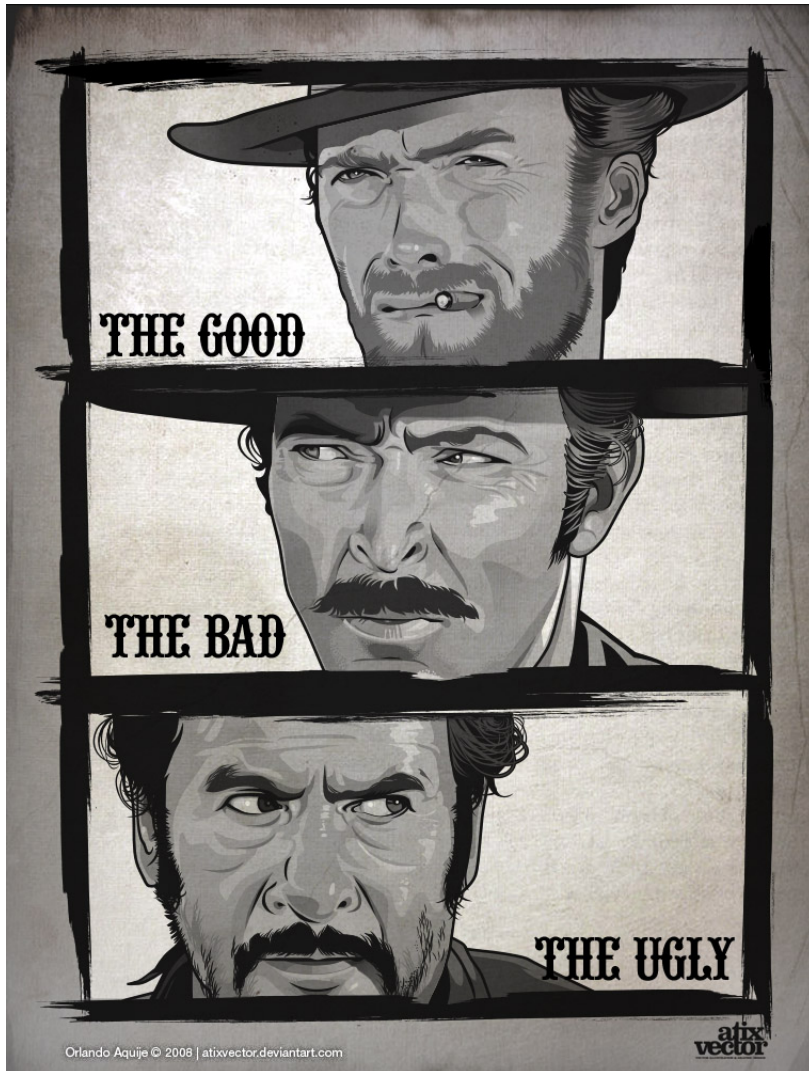
ZIGBEE EXPLOITED

-

The good, the bad and the ugly

WHO ARE WE?

- **Tobias Zillner**
 - Senior IS Auditor @Cognosec in Vienna
 - Penetration Testing, Security Audits, Security Consulting
 - Breaking stuff
 - Owner of a ZigBee based home automation system :D
- **Sebastian Strobl**
 - Principal Auditor @Cognosec in Vienna
 - Plans and leads various types of IT audits
 - Still trying to get his HD drone vision to work
 - Now uses Z-Wave for home automation until we manage to break it too

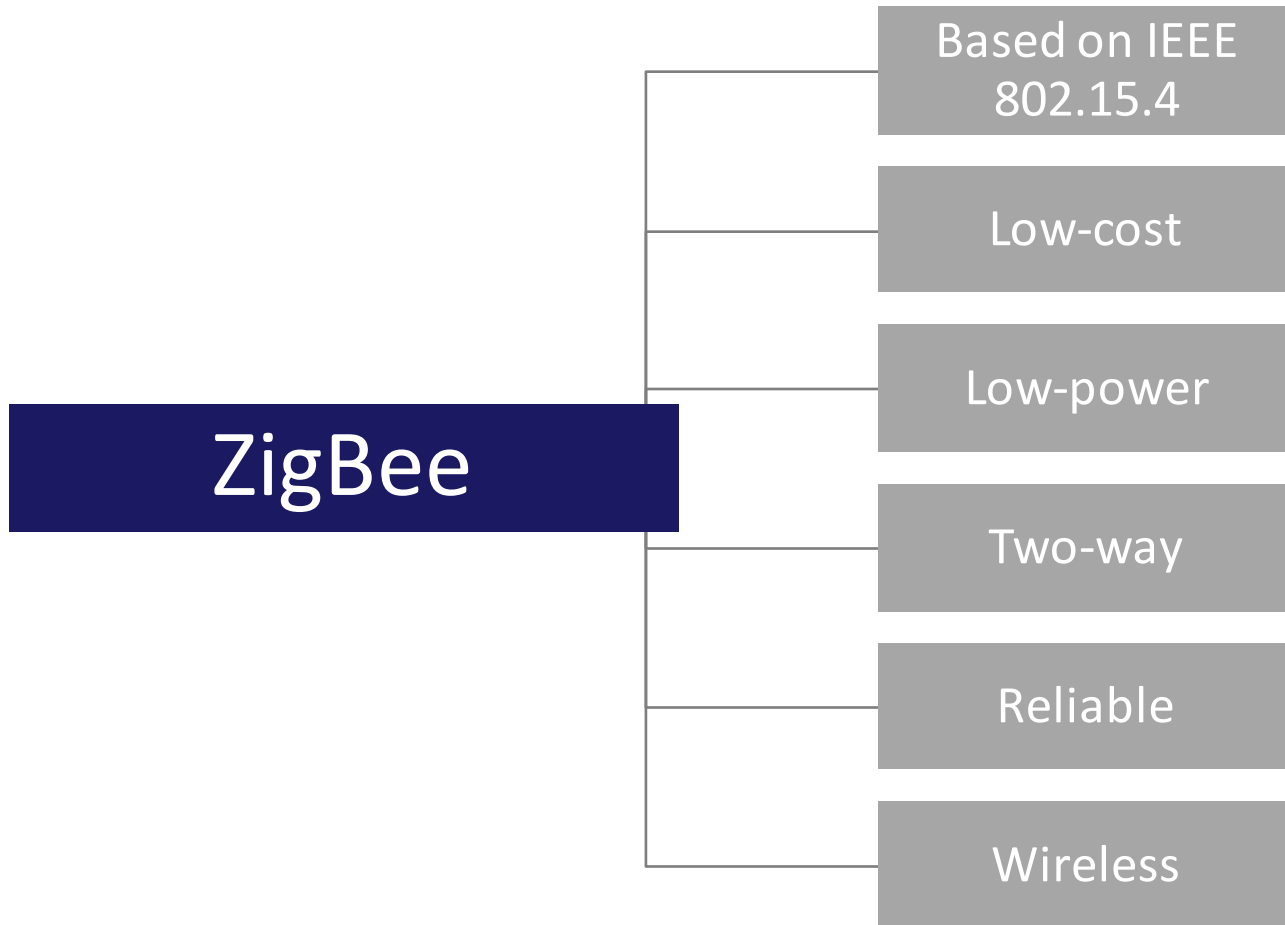


- Introduction
- ZigBee Security Measures
 - The good
- ZigBee Application Profiles
 - The bad
- ZigBee Implementations
 - The ugly
- Demonstration
- Summary

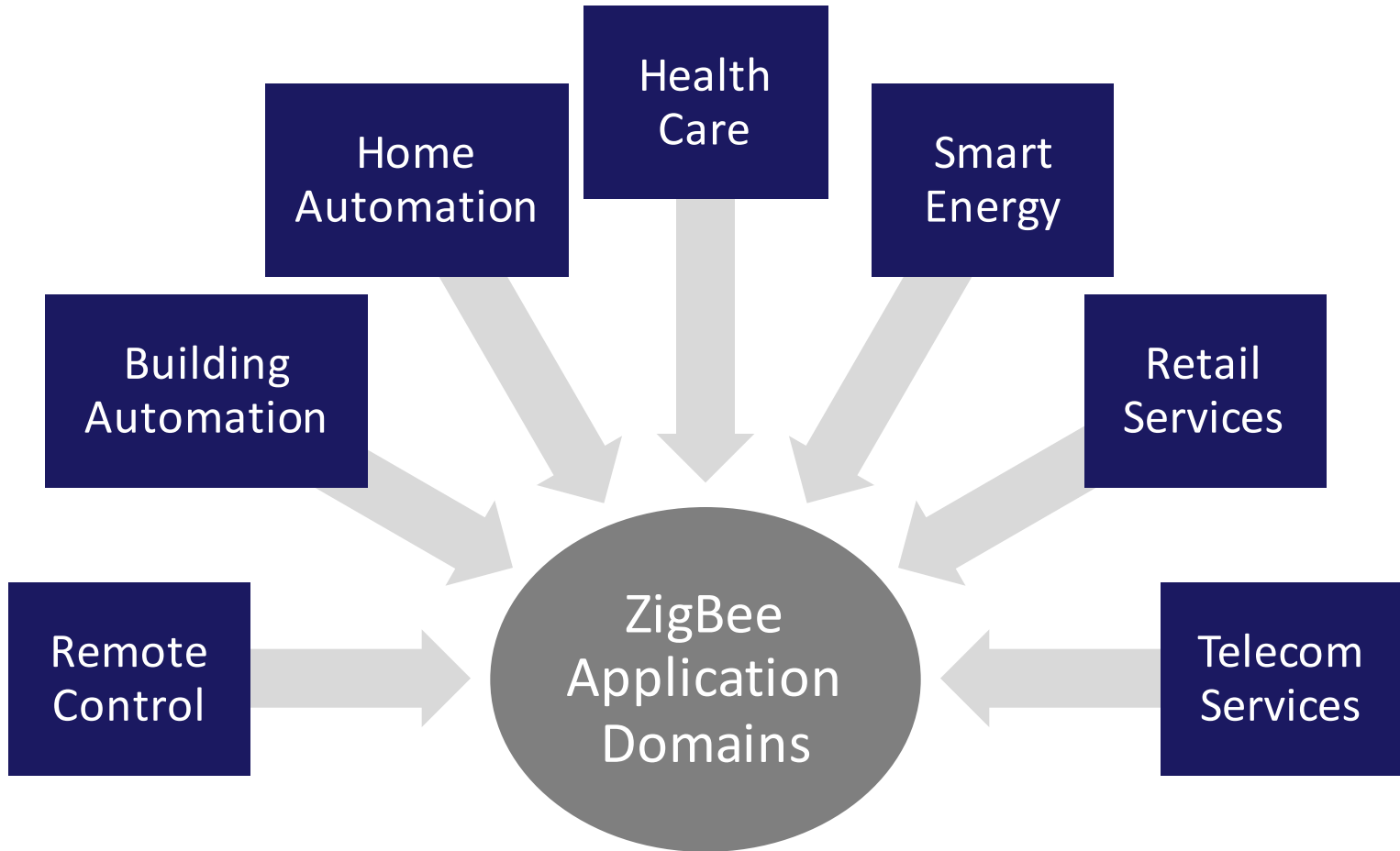
black hat[®]
USA 2015

WHAT IT'S ABOUT?

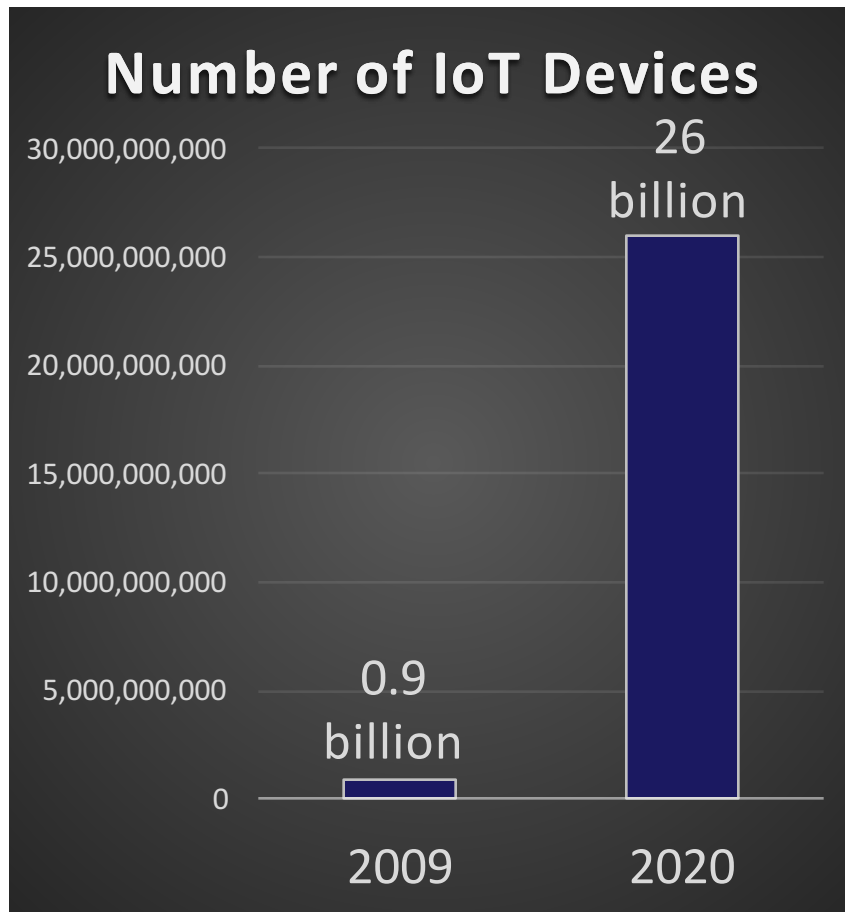
WHAT IS ZIGBEE?



WHERE IS IT USED?



WHY IS IT IMPORTANT?

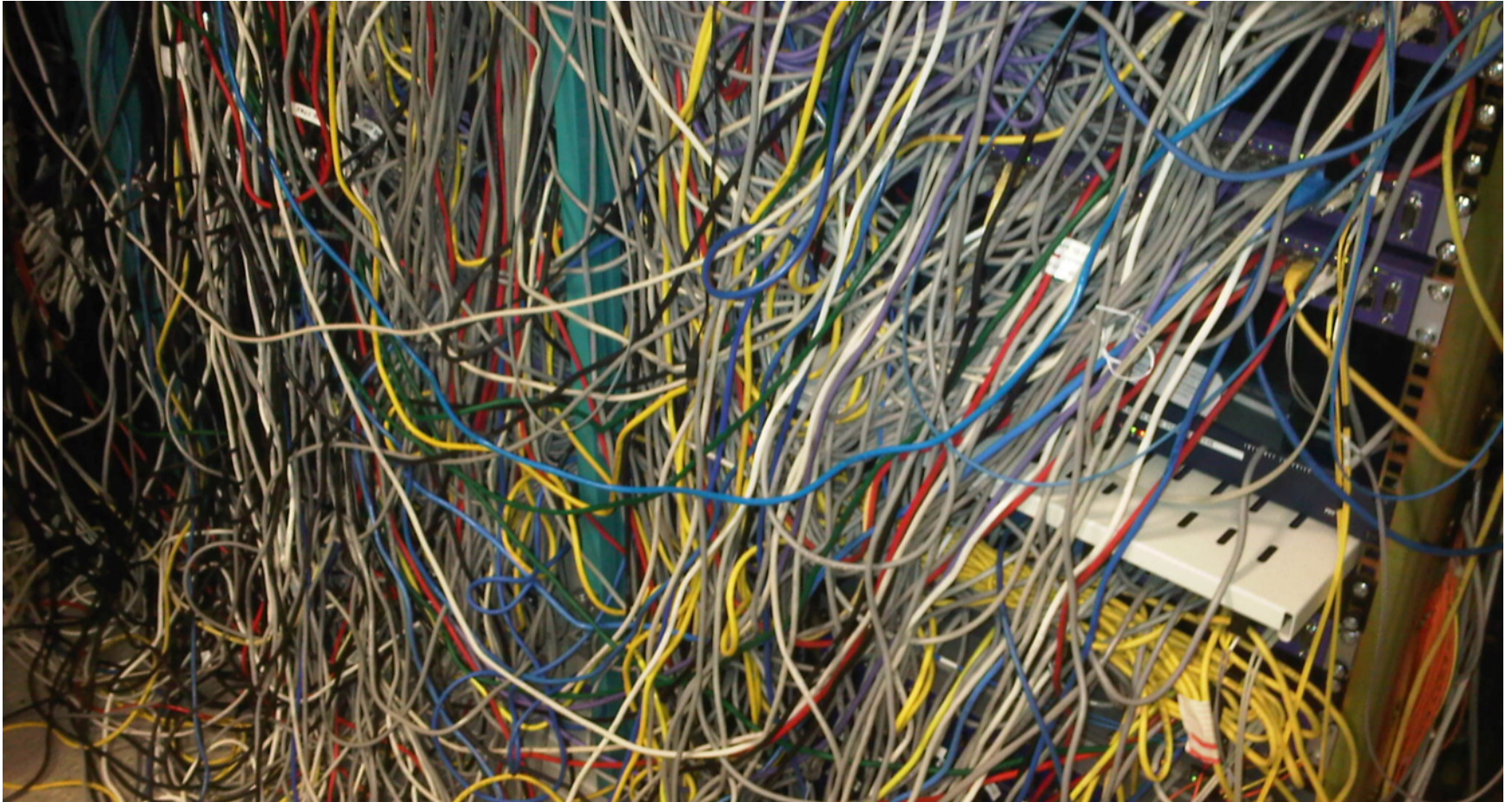


- Trend is wireless connections
- Samsung CEO BK Yoon:
 - *“Every Samsung device will be part of IoT till 2019”*³
- Over 500 smart device per household in 2022¹

¹ <http://www.gartner.com/newsroom/id/2839717>

² <http://www.gartner.com/newsroom/id/2636073>

³ <http://www.heise.de/newsticker/meldung/CES-Internet-der-Dinge-komfortabel-vernetzt-2512856.html>



<https://hivizme.files.wordpress.com/2012/06/cable-mess.jpg>

- **HOME** automation has high privacy requirements
- Huge source of personalized data

Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters - all connected to the next-generation internet¹

-Former CIA Director
David Petraeus

¹ <http://www.wired.com/2012/03/petraeus-tv-remote/>



ZIGBEE SECURITY MEASURES

-

THE GOOD

Security Measures

Symmetric
Encryption

AES-CCM*
128bit

Message
Authentication

Integrity
Protection

MIC
0 - 128 bit

Replay
Protection

Frame
Counter
4 Byte

- One security level per network
- Security based on encryption keys
 - Network Key
 - Used for broadcast communication
 - Shared among all devices
 - Link Key
 - Used for secure unicast communication
 - Shared only between two devices

Trust in the security is ultimately reduces to:

- Trust in the secure **initialization** of keying material
- Trust in the secure **installation** of keying material
- Trust in the secure **processing** of keying material
- Trust in the secure **storage** of keying material

HOW ARE KEYS EXCHANGED?



Preinstalled Devices



Key Transport

- Out of band recommended



Key Establishment

- Derived from other keys
- Also requires preinstalled keys





ZIGBEE APPLICATION PROFILES

-

THE BAD

- Define communication between devices
 - Agreements for messages
 - Message formats
 - Processing actions
- Enable applications to
 - Send commands
 - Request data
 - Process commands
 - Process requests
- Startup Attribute Sets (SAS) provide interoperability and compatibility

- Default Trust Center Link Key
 - `0x5A 0x69 0x67 0x42 0x65 0x65 0x41 0x6C 0x6C 0x69 0x61 0x6E 0x63 0x65 0x30 0x39`
 - ZigBeeAlliance09
- Use Default Link Key Join
 - `0x01(True)`
 - *This flag enables the use of default link key join as a fallback case at startup time.*
- Return to Factory Defaults
 - *In support of a return to factory default capability, HA devices shall implement a Network Leave service. Prior to execution of the NWK Leave [...] the device shall ensure all operating parameters are reset to allow a reset to factory defaults.*

- Devices in a ZLL shall use ZigBee network layer security.
- *“The ZLL security architecture is based on using a fixed secret key, known as the ZLL key, which shall be stored in each ZLL device. All ZLL devices use the ZLL key to encrypt/decrypt the exchanged network key.”*
- *“It will be distributed only to certified manufacturers and is bound with a safekeeping contract”*

rt: @MayaZigBee

#DIY lover #ZLL master key 9F 55 95 F1 02
57 C8 A4 69 CB F4 2B C9 3F EE 31
#ZigBee #Philips #Hue



MayaZigBee @MayaZigBee · Mar 29

Should the #ZLL master key be illegal? Should a #free #DIY #interoperability be illegal (w a light bulb, mind you)? Make sure the key lives!

- nwkAllFresh
 - *False*
 - *Do not check frame counter*
- Trust center link key
 - *0x5a 0x69 0x67 0x42 0x65 0x65 0x41 0x6c 0x6c 0x69 0x61 0x6e
0x63 0x65 0x30 0x39*
 - *Default key for communicating with a trust center*
- Use insecure join
 - *True*
 - *Use insecure join as a fallback option.*



ZIGBEE IMPLEMENTATIONS

-

THE UGLY

- *"To avoid "bugs" that an attacker can use to his advantage, it is crucial that security be well implemented and tested. [...] Security services should be implemented and tested by security experts [...]." (ZigBee Alliance 2008, p. 494)*

- *"The request-key service provides a secure means for a device to request the active network key, or an end-to-end application master key, from another device"* (ZigBee Alliance 2008, p. 425)

```
/**
```

Remote device asked us for key.

Application keys are not implemented.

Send current network key.

Not sure: send unsecured?

What is meaning of that command??

Maybe, idea is that we can accept "previous" nwk key?

Or encrypt by it?

```
*/
```

/*

Initiate unsecured key transfer.
Not sure it is right, but I really have no
ideas about request meaning of key for
network key.

*/

- Door Lock
- Smart Home System
- Lighting Solutions



- ALL tested systems only use the default TC Link Key for securing the initial key exchange
- No link keys are used or supported
 - Complete compromise after getting network key
- No ZigBee security configuration possibilities available
- No key rotation applied
 - Test period of 11 month

- Device reset often difficult
 - Removal of key material not guaranteed
 - One device does not support reset at all
- Light bulbs do not require physical interaction for pairing
- Workarounds like reduced transmission power are used to prevent pairing problems
 - Devices have to be in very close proximity for pairing

black hat[®]
USA 2015

DEMONSTRATION

-

SecBee

- ZigBee security testing tool
- Target audience
 - Security testers
 - Developers
- Based on *scapy-radio*, *μracoli* and *killerbee*
- Provides features for testing of security services as well as weak security configuration and implementation
 - Support of encrypted communication
 - Command injection
 - Scan for weak key transport
 - Reset to factory
 - Join to network
 - Test security services



Raspbee



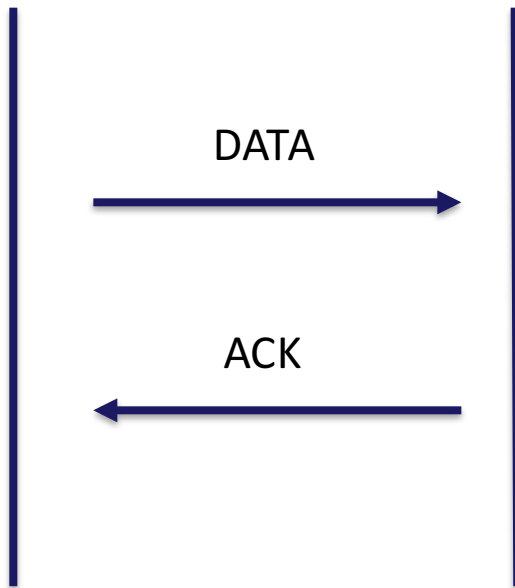
USRP B210

DATA TRANSFER

DIRECT

Coordinator

End device

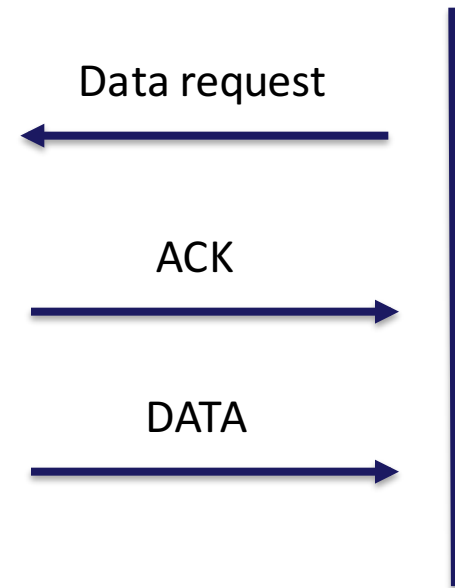


INDIRECT

Coordinator

End device

timeframe
< 8ms



black hat[®]
USA 2015

DEMONSTRATION

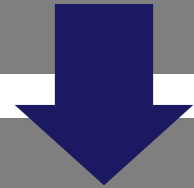
-

KEY EXTRACTION

Fallback key exchange insecure



Most vendors only implement
fallback solution



Same security level as plaintext
exchange



So, the

1. Timeframe is limited
2. Proximity is necessary
3. Key extraction works only during pairing

... what would an attacker do?

Typical End-User



Jam the communication



Wait for users to re-pair the device

It is not only about technology :D



DEMONSTRATION

-

COMMAND INJECTION

black hat[®]
USA 2015

DEMONSTRATION

-

DEVICE HIJACKING

Devices are paired and working

1. Identify the target device
2. Reset to factory default settings
 1. Join the target device to our network



No physical access is required



No knowledge of the secret key is needed



Usability overrules security

black hat[®]
USA 2015

SUMMARY

- Security measures provided are good
- Requirements due to interoperability weaken the security level drastically
- Vendors only implement the absolute minimum to be compliant
- Usability overrules security



- Proper implementation of security measures is crucial - Compliance is not Security
- Learn from history and do not rely on “Security by Obscurity”
- There is a world beside TCP/IP



THANK YOU!



TIME FOR QUESTIONS

-

LET'S TALK ABOUT IT

CONTACT

Tobias Zillner

Mobile: +43 664 8829 8290

Email: tobias.zillner@cognosec.com



Please complete the speaker
feedback survey