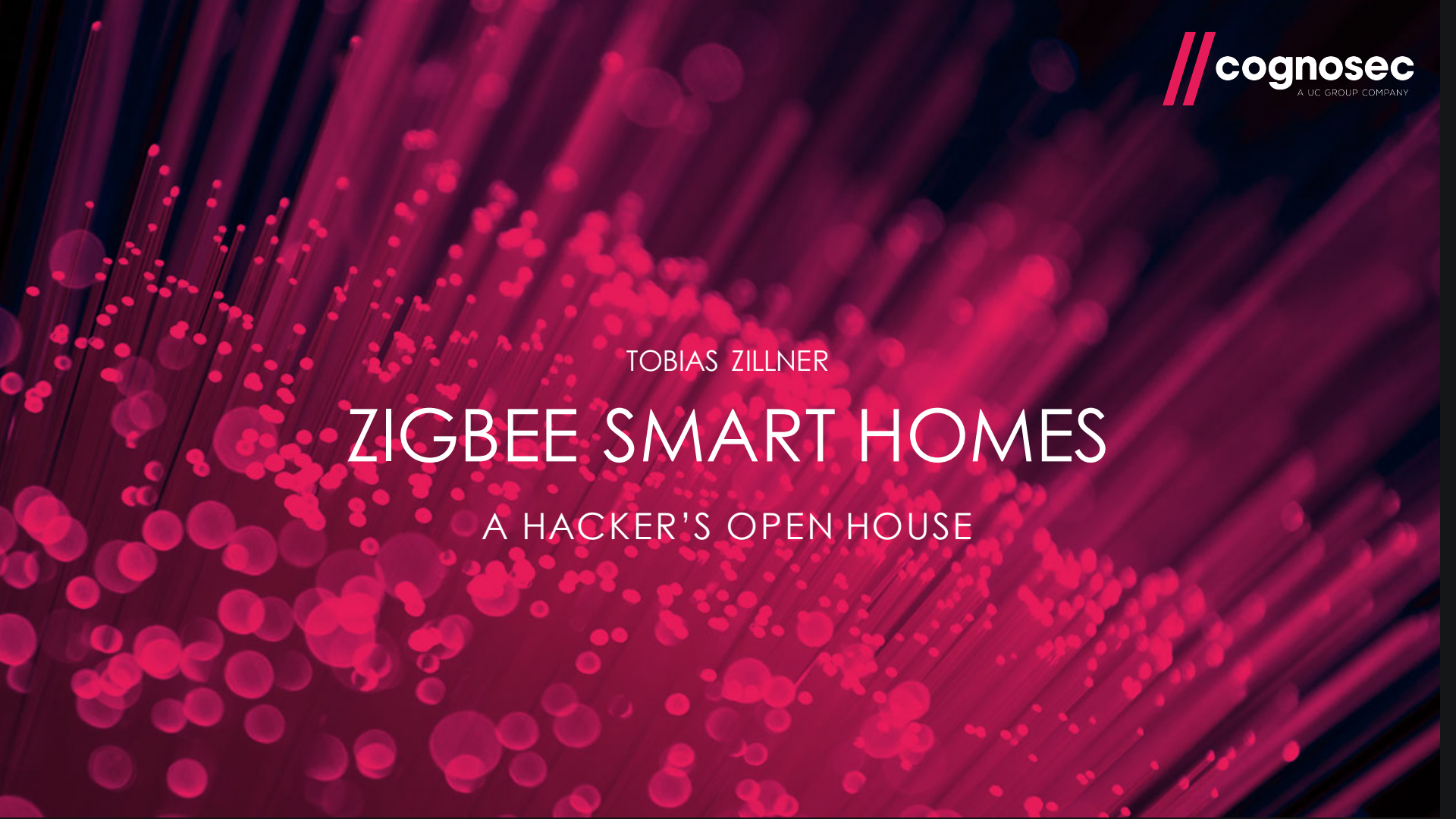
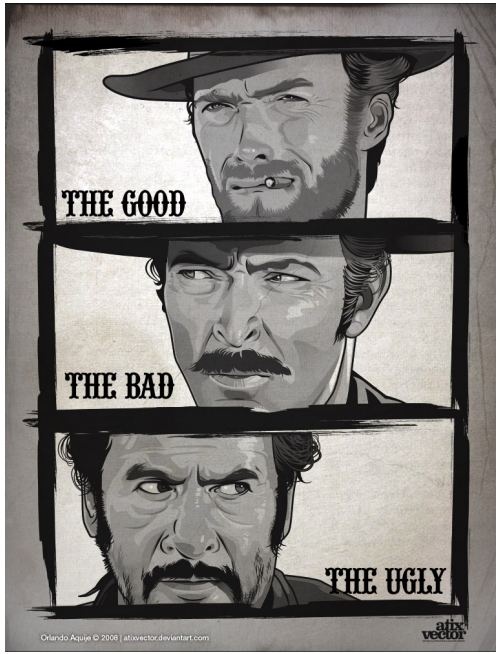

cognosec
A UC GROUP COMPANY
TOBIAS ZILLNER
ZIGBEE SMART HOMES
A HACKER'S OPEN HOUSE

cognosec
A UC GROUP COMPANY

TOBIAS ZILLNER

ABOUT ME

- Senior IS Auditor @ Cognosec in Vienna
- Penetration Testing, Security Audits & Consulting
- IoT Security Research, Playing with SDR
- Owner of a ZigBee based home automation system :D



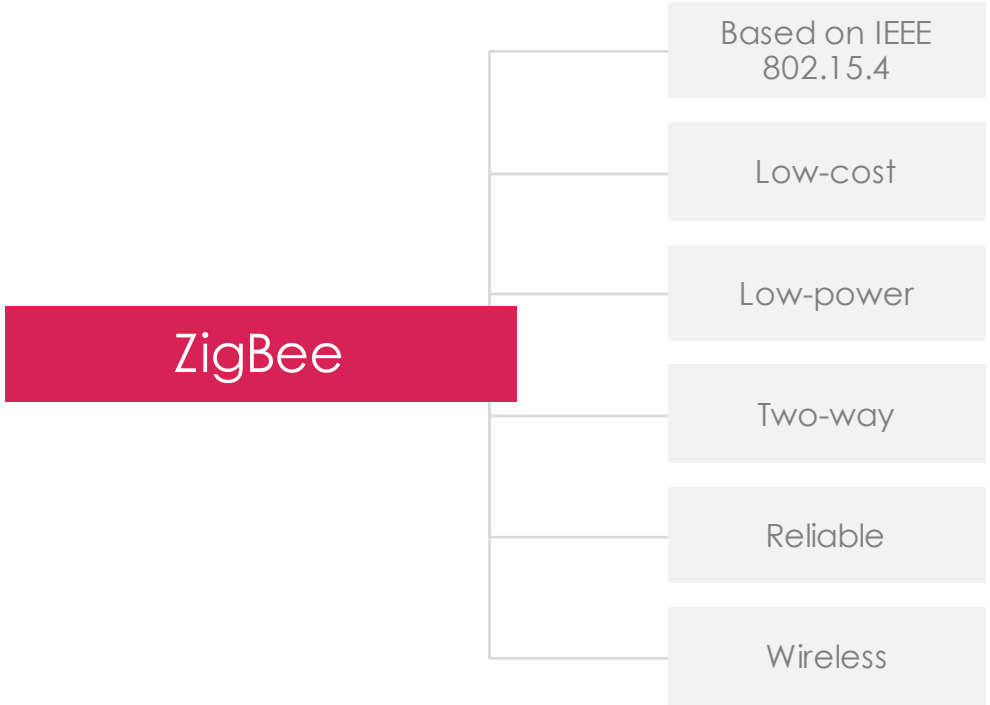
AGENDA

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

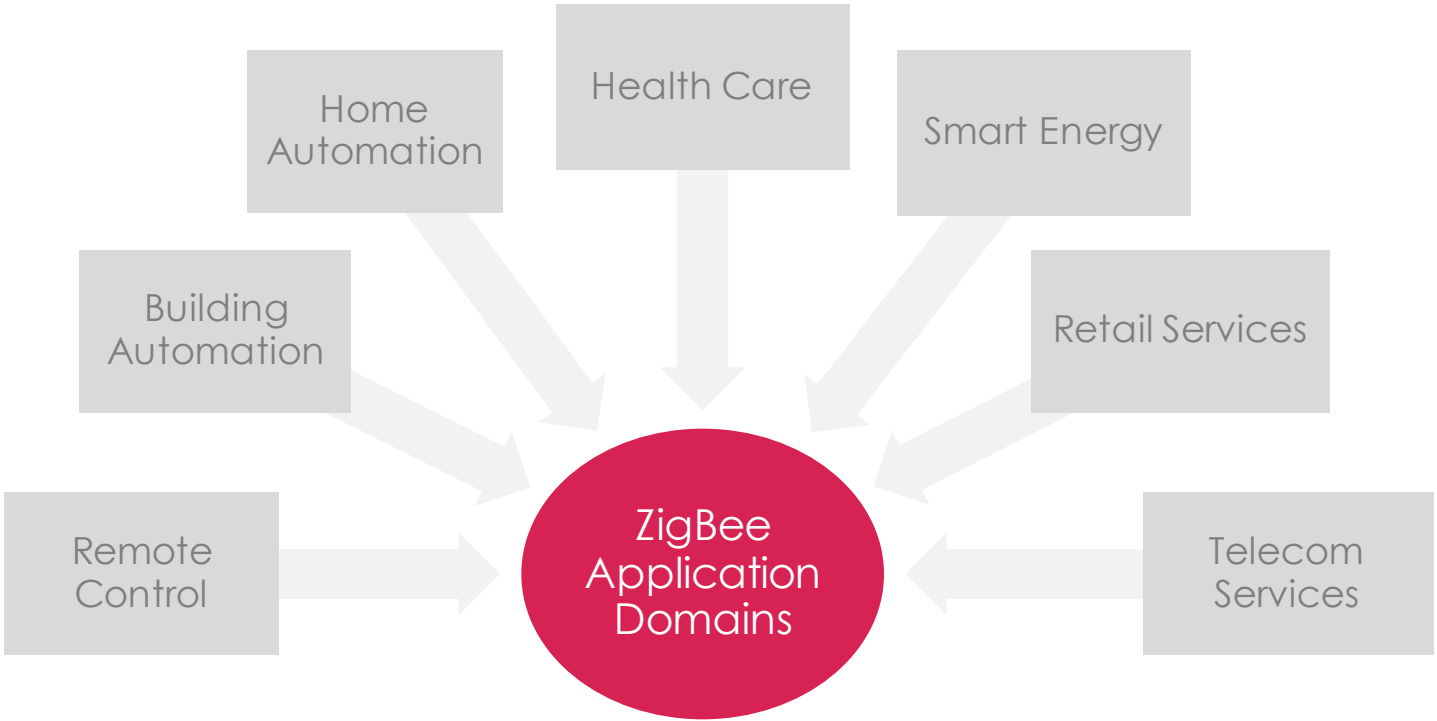
cognosec
A UC GROUP COMPANY

ZIGBEE SMART HOMES

WHAT IT'S ALL ABOUT

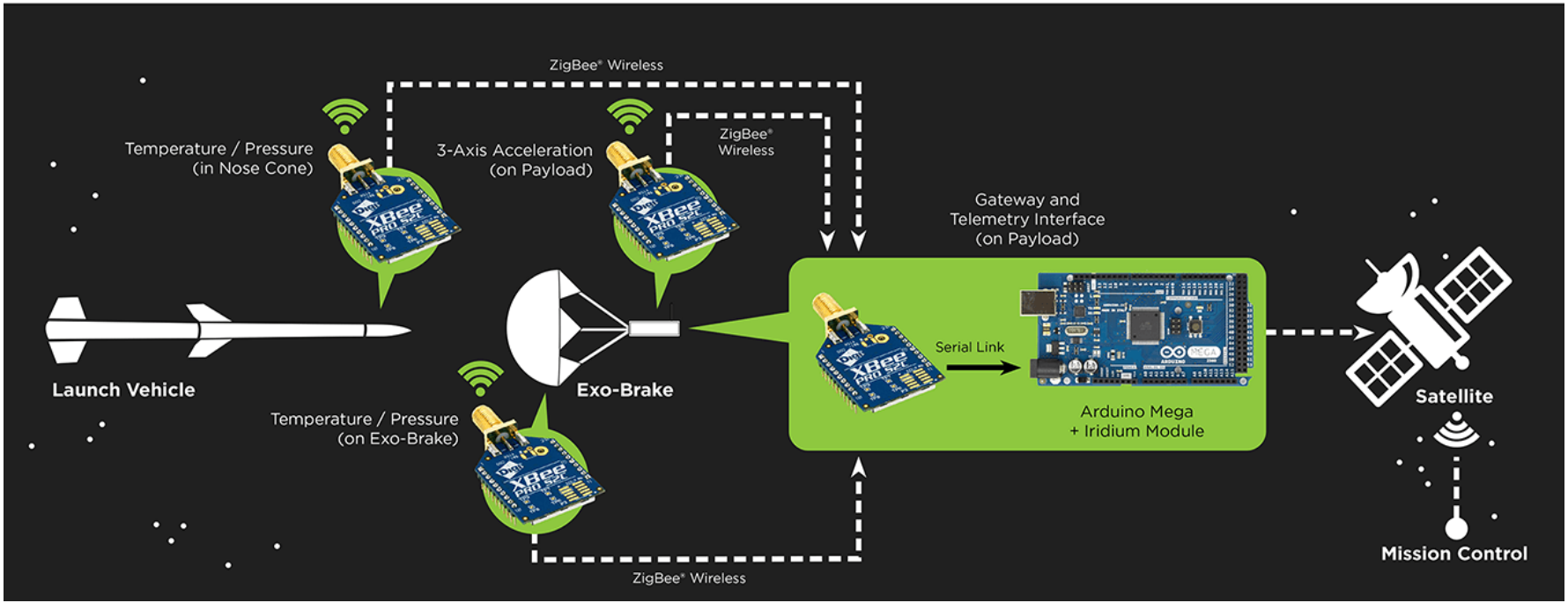

ZigBee
Based on IEEE 802.15.4
Low-cost
Low-power
Two-way
Reliable
Wireless

ZIGBEE SMART HOMES



cognosec
A UC GROUP COMPANY

SOAREX-8 Wireless Sensor Network Flight Configuration
NASA Ames Research Center



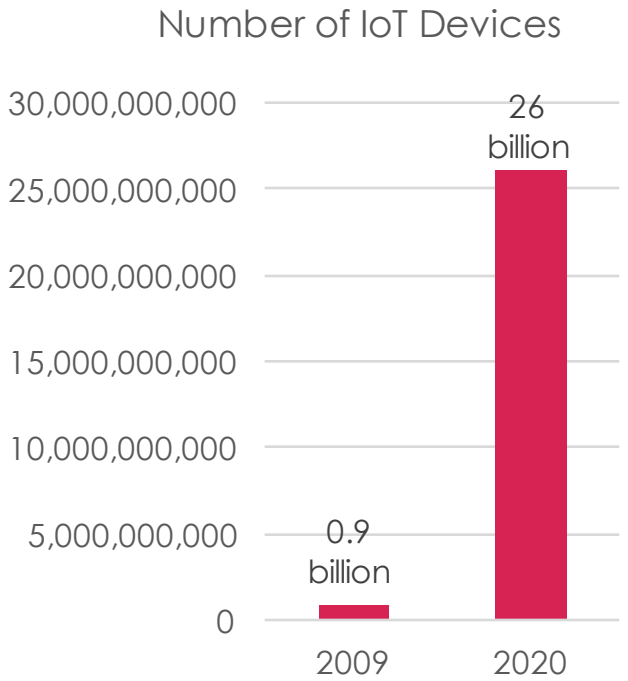
http://www.zigbee.org/zigbee-in-space-xbee-rf-modules-launched-by-nasa/

cognosec
A UC GROUP COMPANY

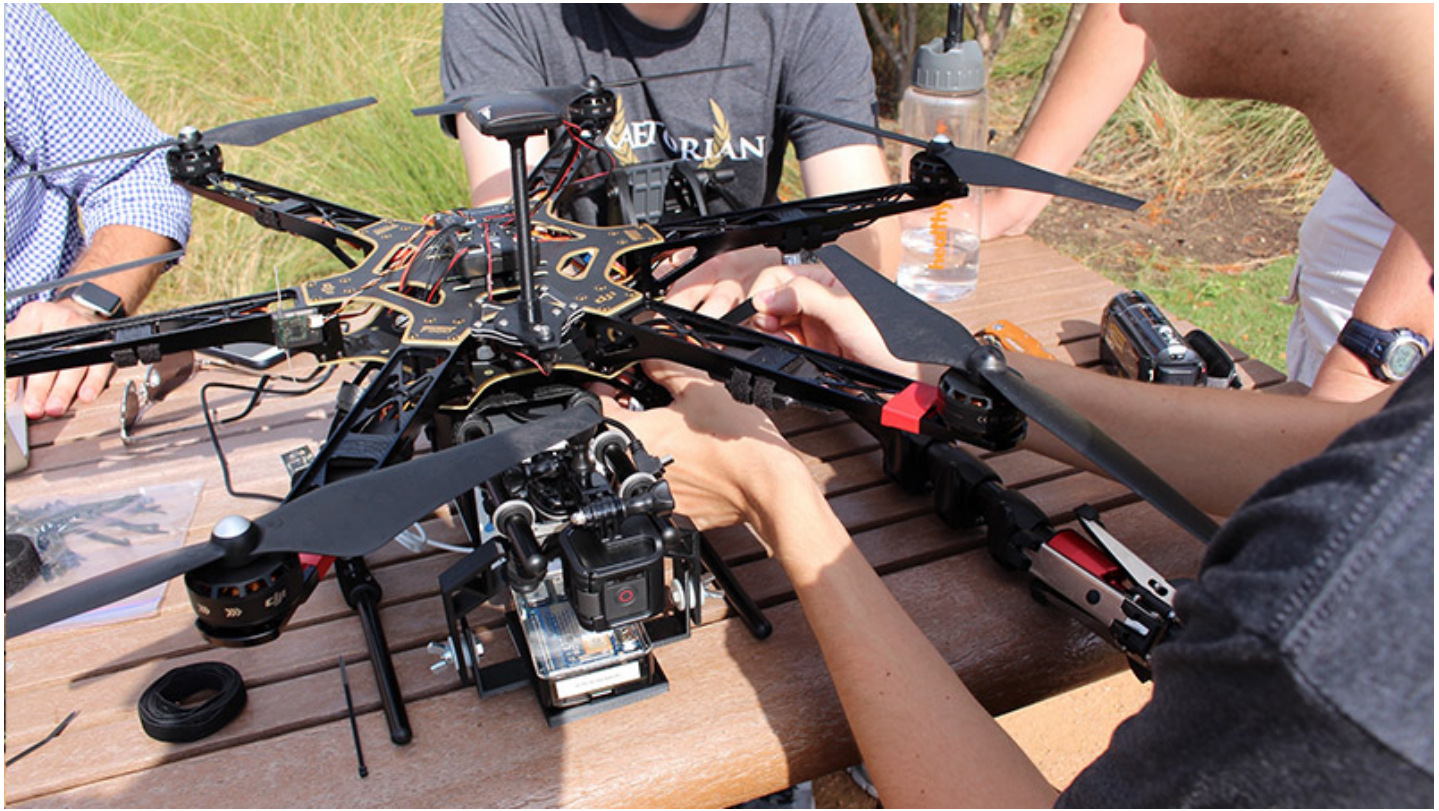
cognosec
A UC GROUP COMPANY

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 2022 [1]



[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://www.praetorian.com/iotmap/

cognosec
A UC GROUP COMPANY

Project Statistics

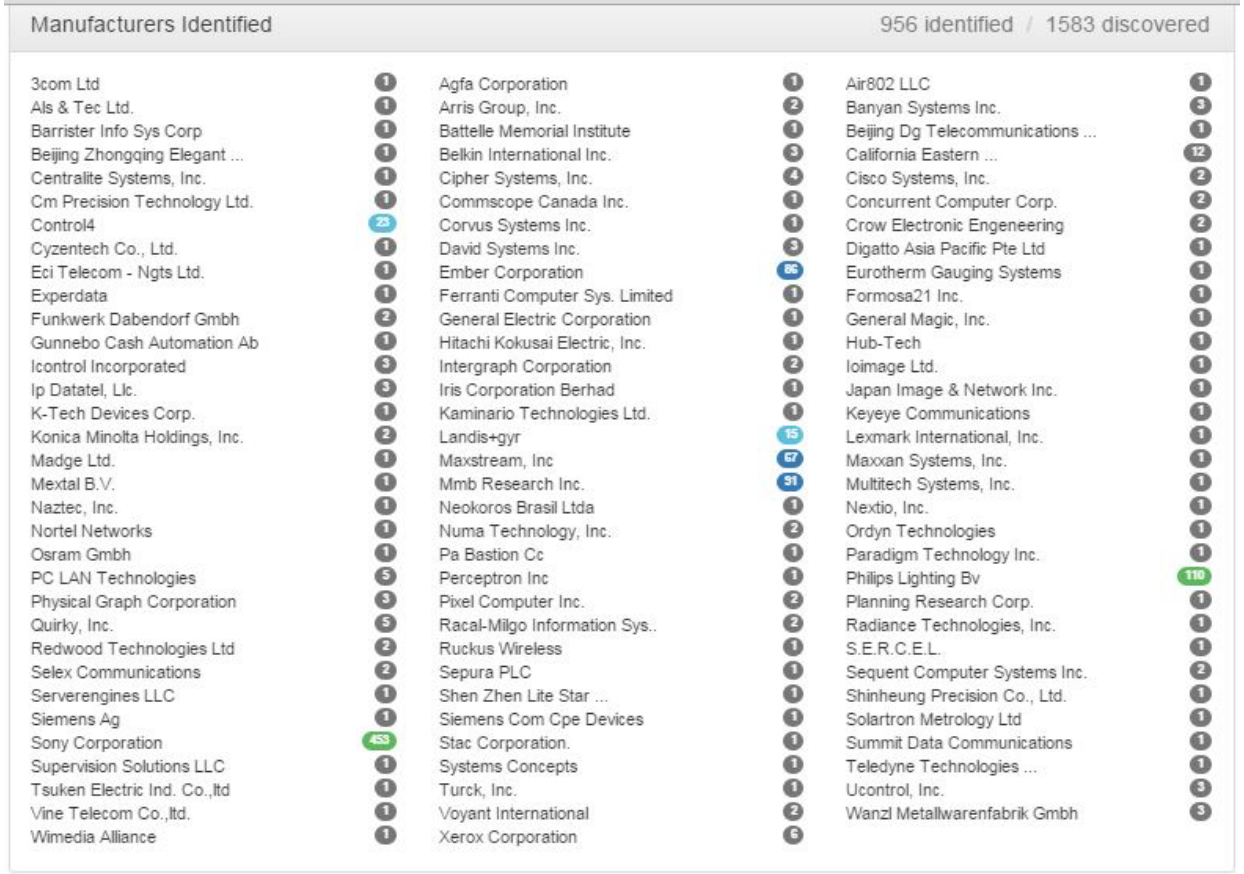
Zone Details

	Identified	Not Identified	Total	
Commercial Zone	172	179	351	Explore zone
Residential Zone	784	451	1235	Explore zone
Industrial Zone	n/a	n/a	n/a	Coming soon

https://www.praetorian.com/iotmap/

ZIGBEE SMART HOMES

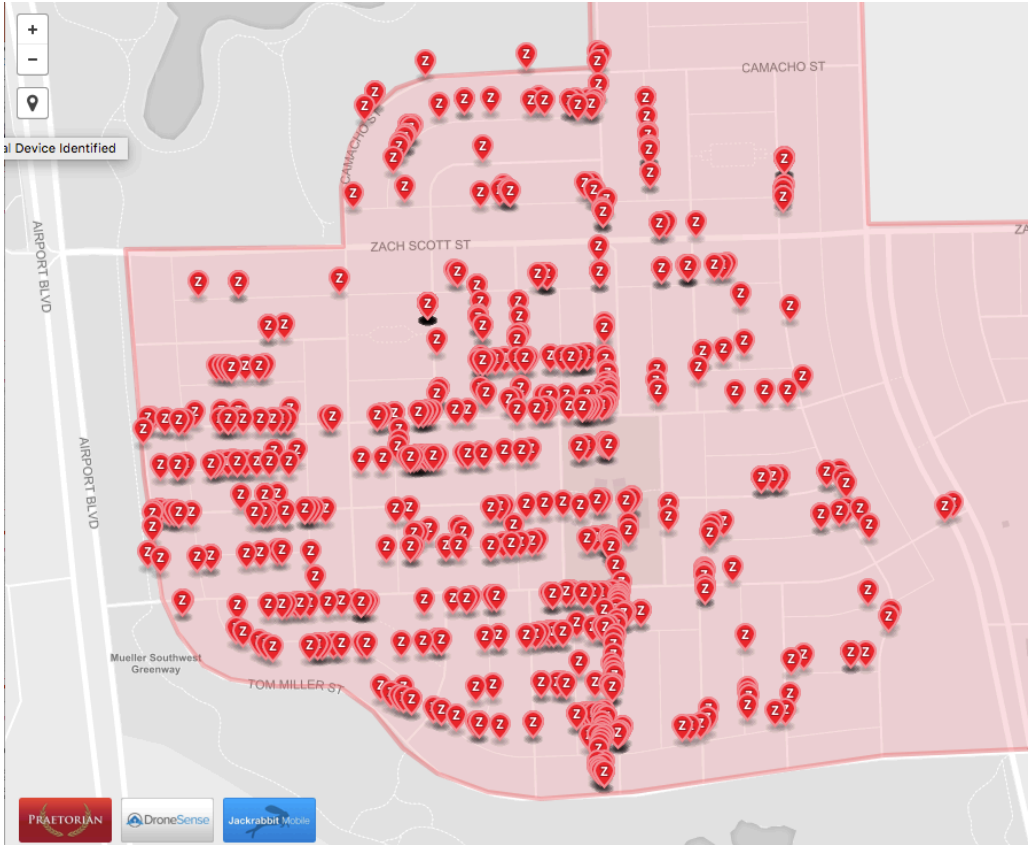
cognosec
A UC GROUP COMPANY



Manufacturers Identified — 956 identified / 1583 discovered

3com Ltd 1	Agfa Corporation 1	Air802 LLC 1
Als & Tec Ltd. 1	Arris Group, Inc. 2	Banyan Systems Inc. 3
Barrister Info Sys Corp 1	Battelle Memorial Institute 1	Beijing Dg Telecommunications ... 1
Beijing Zhongqing Elegant ... 1	Belkin International Inc. 3	California Eastern ... 12
Centralite Systems, Inc. 1	Cipher Systems, Inc. 4	Cisco Systems, Inc. 2
Cm Precision Technology Ltd. 1	Commscope Canada Inc. 1	Concurrent Computer Corp. 2
Control4 23	Corvus Systems Inc. 1	Crow Electronic Engeneering 2
Cyzentech Co., Ltd. 1	David Systems Inc. 3	Digatto Asia Pacific Pte Ltd 1
Eci Telecom - Ngts Ltd. 1	Ember Corporation 86	Eurotherm Gauging Systems 1
Experdata 1	Ferranti Computer Sys. Limited 1	Formosa21 Inc. 1
Funkwerk Dabendorf Gmbh 2	General Electric Corporation 1	General Magic, Inc. 1
Gunnebo Cash Automation Ab 1	Hitachi Kokusai Electric, Inc. 1	Hub-Tech 1
Icontrol Incorporated 3	Intergraph Corporation 2	Ioimage Ltd. 1
Ip Datatel, Llc. 3	Iris Corporation Berhad 1	Japan Image & Network Inc. 1
K-Tech Devices Corp. 1	Kaminario Technologies Ltd. 1	Keyeye Communications 1
Konica Minolta Holdings, Inc. 2	Landis+gyr 15	Lexmark International, Inc. 1
Madge Ltd. 1	Maxstream, Inc 67	Maxxan Systems, Inc. 1
Mextal B.V. 1	Mmb Research Inc. 91	Multitech Systems, Inc. 1
Naztec, Inc. 1	Neokoros Brasil Ltda 1	Nextio, Inc. 1
Nortel Networks 1	Numa Technology, Inc. 2	Ordyn Technologies 1
Osram Gmbh 1	Pa Bastion Cc 1	Paradigm Technology Inc. 1
PC LAN Technologies 5	Perceptron Inc 1	Philips Lighting Bv 110
Physical Graph Corporation 3	Pixel Computer Inc. 2	Planning Research Corp. 1
Quirky, Inc. 5	Racal-Milgo Information Sys.. 2	Radiance Technologies, Inc. 1
Redwood Technologies Ltd 2	Ruckus Wireless 1	S.E.R.C.E.L. 1
Selex Communications 2	Sepura PLC 1	Sequent Computer Systems Inc. 2
Serverengines LLC 1	Shen Zhen Lite Star ... 1	Shinheung Precision Co., Ltd. 1
Siemens Ag 1	Siemens Com Cpe Devices 1	Solartron Metrology Ltd 1
Sony Corporation 453	Stac Corporation. 1	Summit Data Communications 1
Supervision Solutions LLC 1	Systems Concepts 1	Teledyne Technologies ... 1
Tsuken Electric Ind. Co.,ltd 1	Turck, Inc. 1	Ucontrol, Inc. 3
Vine Telecom Co.,ltd. 1	Voyant International 2	Wanzl Metallwarenfabrik Gmbh 3
Wimedia Alliance 1	Xerox Corporation 6	

ZIGBEE SMART HOMES



cognosec
A UC GROUP COMPANY

WHY SECURITY?

- ***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 internet[1]

-Former CIA Director
David Petraeus"

cognosec
A UC GROUP COMPANY

ZIGBEE SMART HOMES

ZIGBEE SECURITY MEASURES

cognosec
A UC GROUP COMPANY

ZIGBEE SECURITY MEASURES

Security Measures

Symmetric Encryption	Message Authentication	Integrity Protection	Replay Protection
AES-CCM* 128bit		MIC 0 - 128 bit	Frame Counter 4 Byte

cognosec
A UC GROUP COMPANY

OFFICIAL STATEMENT

"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)

cognosec
A UC GROUP COMPANY

ZIGBEE SECURITY

- 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

cognosec
A UC GROUP COMPANY

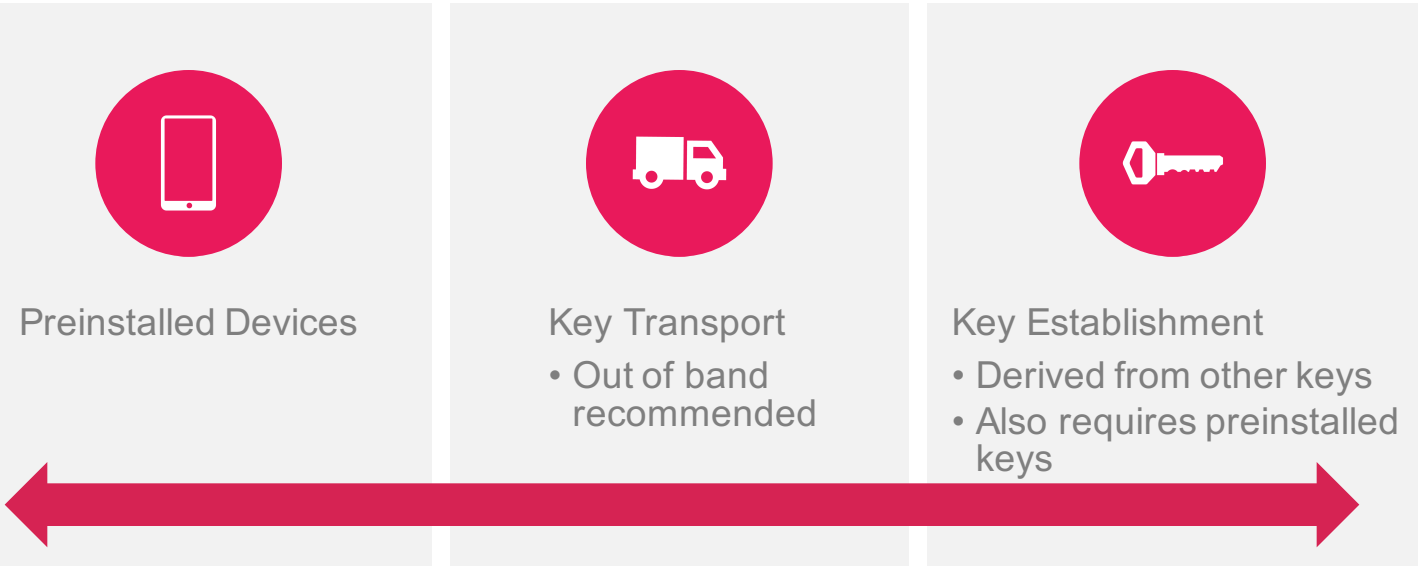
SECURITY ARCHITECTURE

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

cognosec
A UC GROUP COMPANY

HOW ARE KEYS EXCHANGED?



cognosec
A UC GROUP COMPANY

ZIGBEE SMART HOMES

ZIGBEE APPLICATION PROFILES

cognosec
A UC GROUP COMPANY

APPLICATION PROFILES

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

cognosec
A UC GROUP COMPANY

HOME AUTOMATION PROFILE

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.

cognosec
A UC GROUP COMPANY

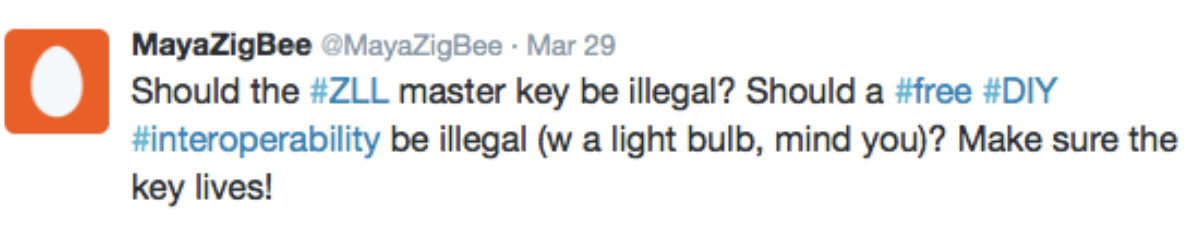
LIGHT LINK PROFILE

- 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"

cognosec
A UC GROUP COMPANY

LIGHT LINK PROFILE

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



cognosec
A UC GROUP COMPANY

LIGHT LINK

nwkAllFresh

- False
- Do not check frame counter

Use insecure join

- True
- Use insecure join as a fallback option.

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

cognosec
A UC GROUP COMPANY

APPLICATION PROFILES SUMMARY

- HA Profile requires support of known encryption key as fallback

- ZLL Profile uses “secret” key for protecting key exchanges

cognosec
A UC GROUP COMPANY

ZIGBEE EXPLOITED

ZIGBEE IMPLEMENTATIONS

cognosec
A UC GROUP COMPANY

REQUEST KEY SERVICE

"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)

cognosec
A UC GROUP COMPANY

ZBOSS

```
/**
   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?
*/
```

cognosec
A UC GROUP COMPANY

ZBOSS

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

cognosec
A UC GROUP COMPANY

TESTED DEVICES

- Door Lock
- Smart Home System
- Lighting Solutions

cognosec
A UC GROUP COMPANY

RESULTS

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 14 month

cognosec
A UC GROUP COMPANY

RESULTS

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

cognosec
A UC GROUP COMPANY

ZIGBEE EXPLOITED

DEMONSTRATION

cognosec
A UC GROUP COMPANY

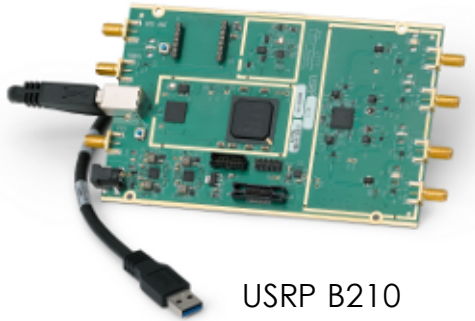
SECBEE

ZigBee security testing tool

Target audience

- Security testers
- Developers

Based on scapy-radio, μracoli and killerbee



USRP B210

Raspbee

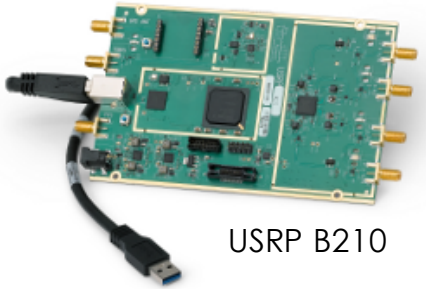
https://github.com/Cognosec/SecBee

cognosec
A UC GROUP COMPANY

SECBEE

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

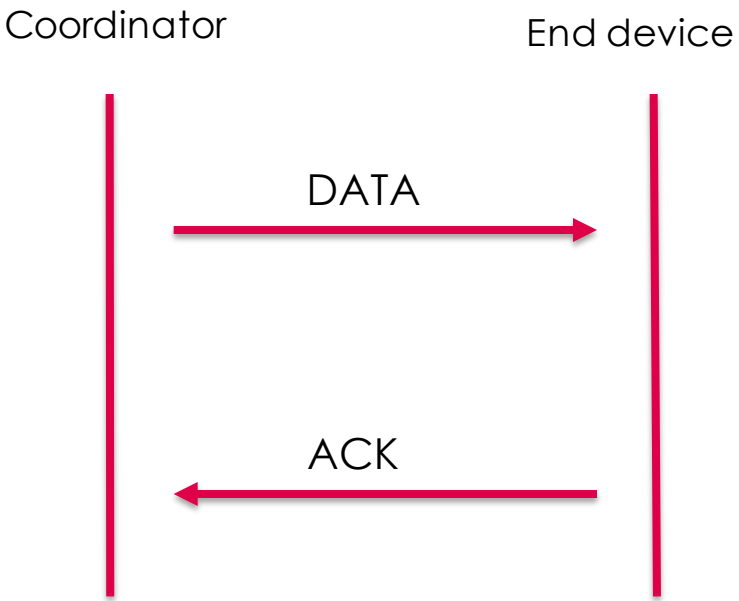


USRP B210

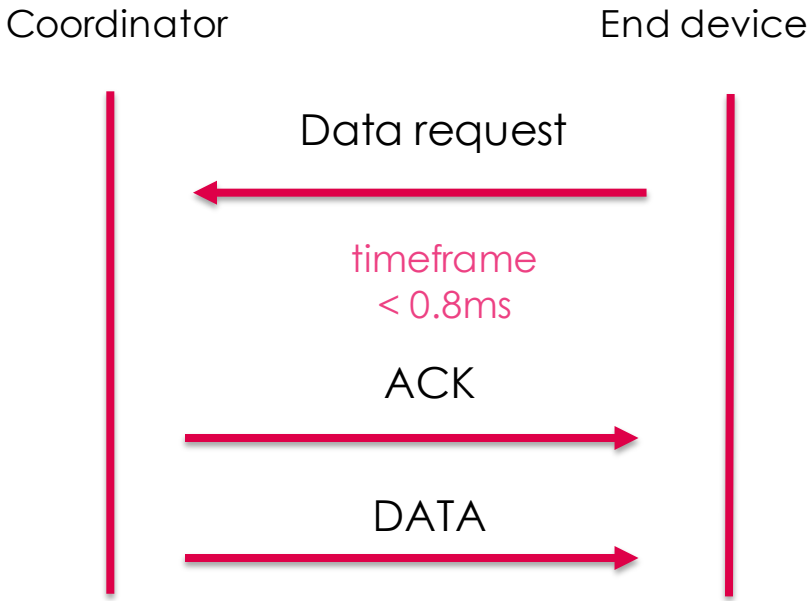
Raspbee

cognosec
A UC GROUP COMPANY

DIRECT



INDIRECT



cognosec
A UC GROUP COMPANY

ZIGBEE SMART HOMES

DEMONSTRATION - KEY EXTRACTION

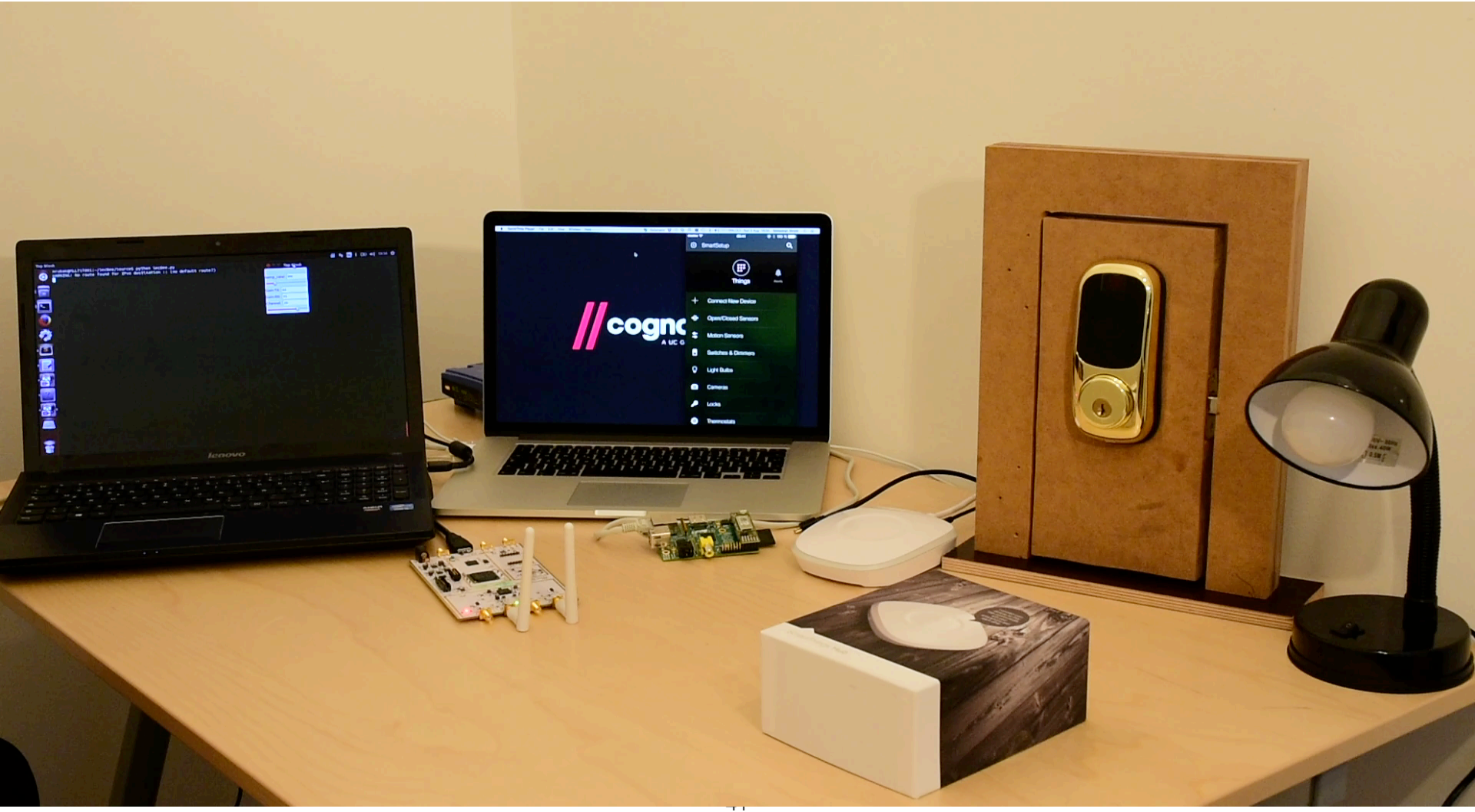
cognosec
A UC GROUP COMPANY

NETWORK KEY SNIFFING

Fallback key exchange insecure

Most vendors only implement fallback solution

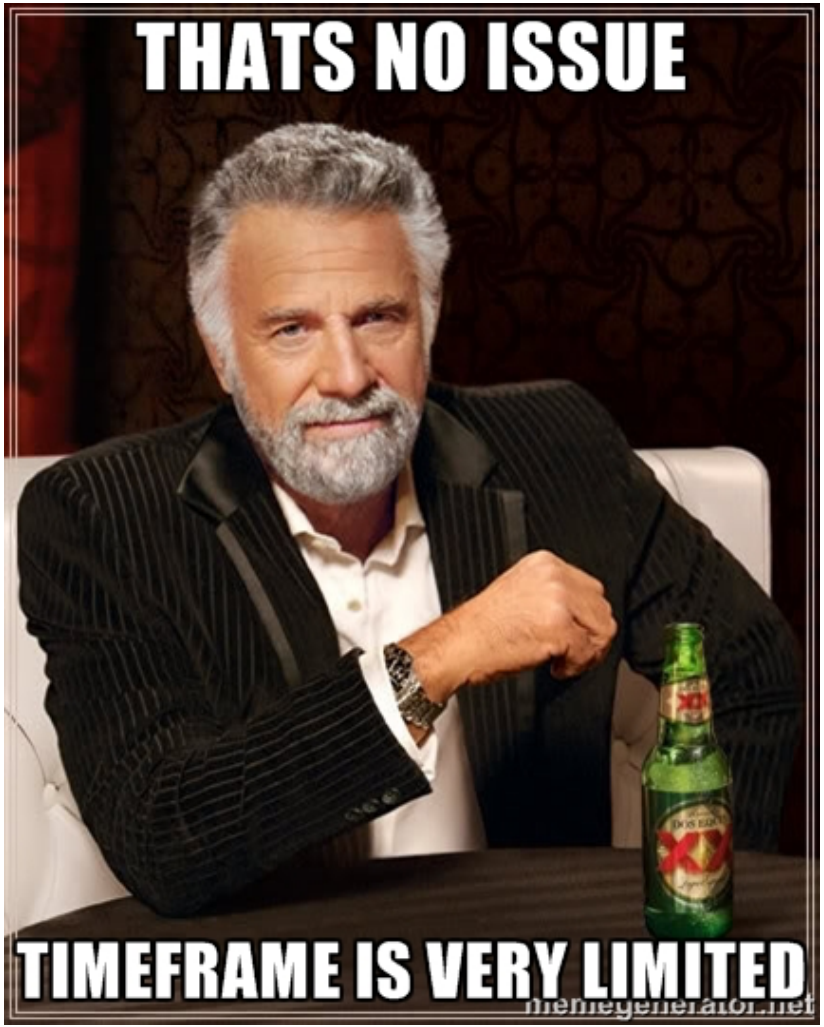
Same security level as plaintext exchange


Lenovo
Things
Connect New Device
Open/Closed Sensors
Motion Sensors
Switches & Dimmers
Light Bulbs
Cameras
Locks
Thermostats

cognosec
A UC GROUP COMPANY

VENDOR

RESPONSE



cognosec
A UC GROUP COMPANY

NETWORK KEY SNIFFING

So, the

- Timeframe is limited
- Proximity is necessary
- Key extraction works only during pairing

… what would an attacker do?

TYPICAL

END-USER

cognosec
A UC GROUP COMPANY

THE SOCIAL ENGINEERS WAY

Jam the communication

Wait for users to re-pair the device

It is not **only** about technology :D

cognosec
A UC GROUP COMPANY

THE HACKER WAY

Trigger Key Transport

Sniff over the air key exchange

No.	Time	Source	Destination	Protocol	Length	Info
400	1911.170083	0xa642	0x0000	IEEE 802.1…	12	Data Request
401	1911.172085			IEEE 802.1…	5	Ack
402	1911.174714	0x0000	0xa642	ZigBee	49	Data, Dst: 0xa642, Src: 0x0000
403	1911.174736			IEEE 802.1…	5	Ack
404	1911.179743	0xa642	0x0000	ZigBee	45	Data, Dst: 0x0000, Src: 0xa642
405	1911.179921			IEEE 802.1…	5	Ack
406	1911.384174	0xa642	0x0000	ZigBee	29	[redacted] Request, Device: 0xa642
407	1911.385366			IEEE 802.1…	5	Ack
408	1911.421006	0xa642	0x0000	IEEE 802.1…	12	Data Request
409	1911.423036			IEEE 802.1…	5	Ack
410	1911.424106	0x0000	0xa642	ZigBee	39	[redacted] Response, Address: 0x0000
411	1911.424735			IEEE 802.1…	5	Ack
412	1911.427783	0xa642	0x0000	IEEE 802.1…	12	Data Request
413	1911.428614			IEEE 802.1…	5	Ack
414	1911.432617	0x0000	0xa642	ZigBee	65	Transport Key
415	1911.433505			IEEE 802.1…	5	Ack
416	1911.439942			IEEE 802.1…	5	Ack
417	1911.446022	0xa642	Broadcast	ZigBee ZDP	57	Device Announcement, Device: EmberCor_00:02:c4:62:34

```
▶ Frame 406: 29 bytes on wire (232 bits), 29 bytes captured (232 bits)
▶ IEEE 802.15.4 Data, Dst: 0x0000, Src: 0xa642
▶ ZigBee Network Layer Command, Dst: 0x0000, Src: 0xa642
▼ Frame Control Field: 0x1009, Frame Type: Command, Discover Route: Suppress, Extended Source Command
    .... .... .... ..01 = Frame Type: Command (0x0001)
    .... .... ..00 10.. = Protocol Version: 2
    .... .... 00.. .... = Discover Route: Suppress (0x0000)
    .... ...0 .... .... = Multicast: False
    .... ..0. .... .... = Security: False
    .... .0.. .... .... = Source Route: False
    .... 0... .... .... = Destination: False
    ...1 .... .... .... = Extended Source: True
```

No.	Time	Source	Destination	Protocol	Length	Info
406	1911.384174	0xa642	0x0000	ZigBee	29	[redacted] Request, Device: 0xa642
407	1911.385366			IEEE 802.1…	5	Ack
408	1911.421006	0xa642	0x0000	IEEE 802.1…	12	Data Request
409	1911.423036			IEEE 802.1…	5	Ack
410	1911.424106	0x0000	0xa642	ZigBee	39	[redacted] Response, Address: 0x0000
411	1911.424735			IEEE 802.1…	5	Ack
412	1911.427783	0xa642	0x0000	IEEE 802.1…	12	Data Request
413	1911.428614			IEEE 802.1…	5	Ack
414	1911.432617	0x0000	0xa642	ZigBee	65	Transport Key
415	1911.433505			IEEE 802.1…	5	Ack

```
▶ Frame 414: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
▶ IEEE 802.15.4 Data, Dst: 0xa642, Src: 0x0000
▶ ZigBee Network Layer Data, Dst: 0xa642, Src: 0x0000
▶ Frame Control Field: 0x0008, Frame Type: Data, Discover Route: Suppress Data
▼ ZigBee Application Support Layer Command
  ▶ Frame Control Field: Command (0x21)
    Counter: 221
  ▼ ZigBee Security Header
    ▶ Security Control Field: 0x10, Key Id: Key-Transport Key
      Frame Counter: 73730
      Message Integrity Code: ad5179a9
      [Key: 5a6967426565416c6c69616e63653039]
      [Key Label: Default TC Link Key]
  ▼ Command Frame: Transport Key
      Command Identifier: Transport Key (0x05)
      Key Type: Standard Network Key (0x01)
      Key: 144221a817f284c7e6e1f000cd80ff0f
      Sequence Number: 0
      Extended Destination: EmberCor_00:02:c4:62:34 (00:0d:6f:00:02:c4:62:34)
      Extended Source: Physical_07:10:c3:00:01 (d0:52:a8:07:10:c3:00:01)
```

cognosec
A UC GROUP COMPANY

NETWORK KEY EXTRACTION


No physical access is required


No knowledge of the secret key is needed

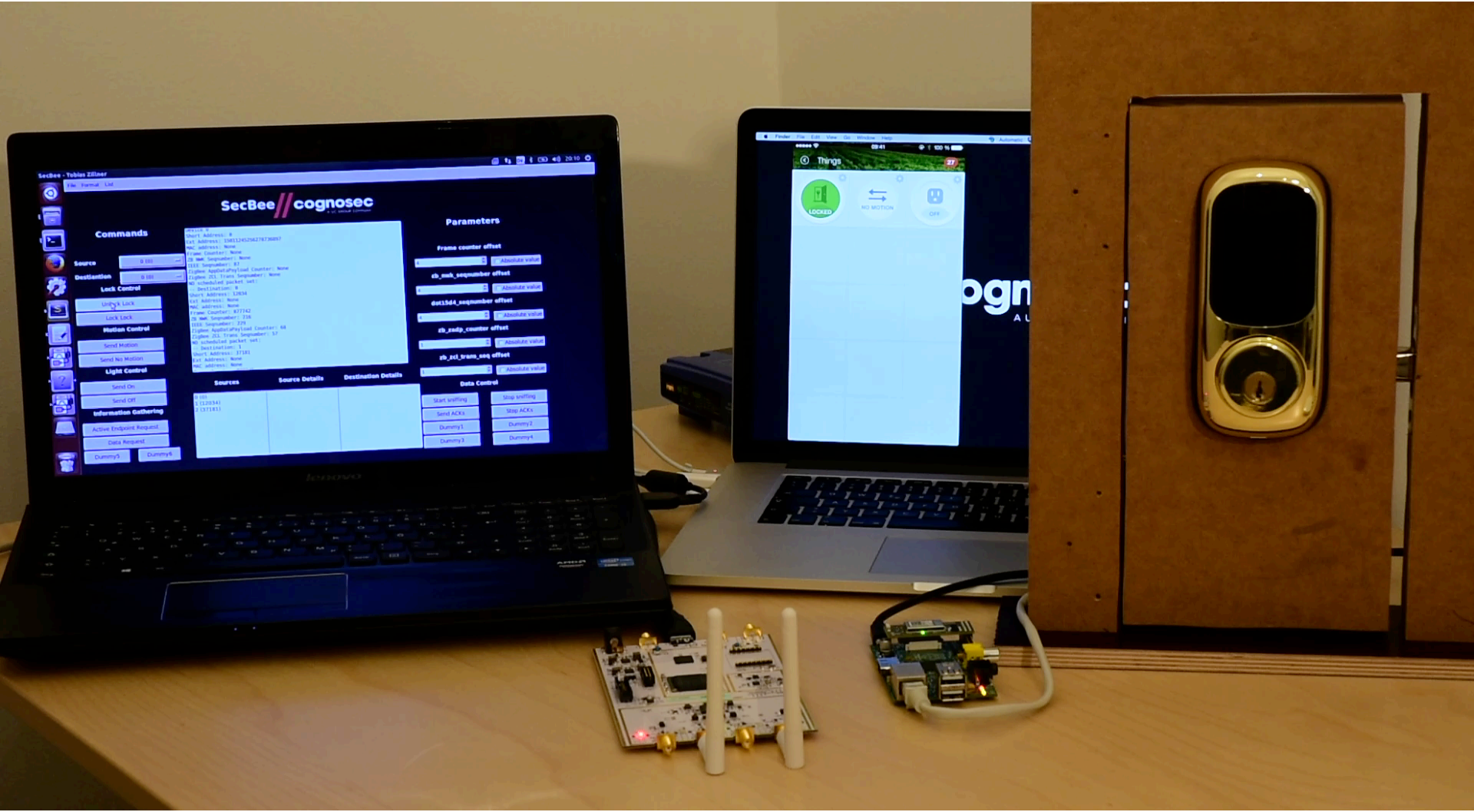

Usability overrules security


Fully compromised system

cognosec
A UC GROUP COMPANY

ZIGBEE EXPLOITED

DEMONSTRATION - COMMAND INJECTION


SecBee - Tobias Zillner
SecBee // cognosec
Commands
Source
Destination
Lock Control
Unlock Lock
Lock Lock
Motion Control
Send Motion
Send No Motion
Light Control
Send On
Send Off
Information Gathering
Active Endpoint Request
Data Request
Dummy5
Dummy6
Parameters
Frame counter offset
zb_nwk_seqnumber offset
dot15d4_seqnumber offset
zb_zadp_counter offset
zb_zcl_trans_seq offset
Absolute value
Sources
Source Details
Destination Details
Data Control
Start sniffing
Send ACKs
Dummy1
Dummy3
Stop sniffing
Stop ACKs
Dummy2
Dummy4
Things
LOCKED
NO MOTION
OFF

cognosec
A UC GROUP COMPANY

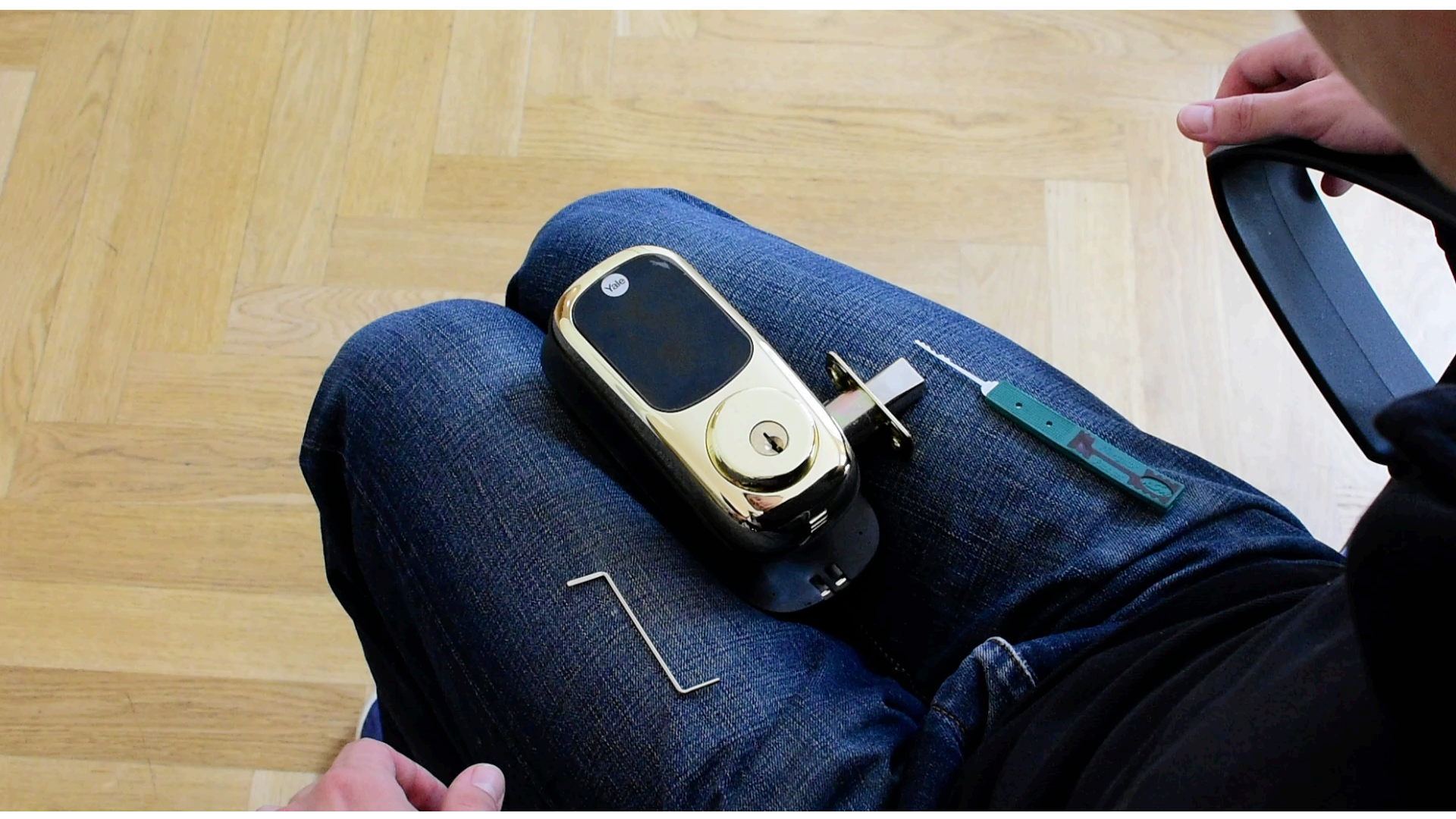
SUMMARY

- 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

cognosec
A UC GROUP COMPANY

DEEPSEC SOUND BYTES

- 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


Yale

cognosec
A UC GROUP COMPANY

THANK YOU!

Contact details

Tobias Zillner, BSc MSc MSc
tobias.zillner@cognosec.com
+43 664 8829 8290


cognosec
A UC GROUP COMPANY
TIME FOR QUESTIONS AND ANSWERS