SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS – A WORLD BESIDE TCP/IP
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
AGENDA

1. Introduction
2. Problems
3. Standards
4. Practical Demonstration
5. Summary
SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS

WHAT IT’S ABOUT?
Stage 1: Personification of Dumb Stage

Stage 2: Partially Autonomous Sensor Networks

Stage 3: Autonomous Independent Devices
Home Automation

– the introduction of technology within the home to enhance the quality of life of its occupants

Goals

– Save energy
– Increase comfort
– Remote monitoring
SMART HOME Chromebook

- Email Notification Dashboard
- Energy Monitor
- Audible Notifications
- Presence Monitor
- Temp Monitor
- Washer / Dryer Notifier
- Garage Door Monitor
- Security System
- Water Leak Notifier

© https://cdn.hackaday.io/images/2596161408899944332.png
WHY IS THIS IMPORTANT?

![Number of IoT Devices](chart.png)

- Trend is wireless connections
- Samsung CEO BK Yoon:
  - “Every Samsung device will be part of IoT till 2019”
- Over 500 smart device per household in 2022

---

2 http://www.gartner.com/newsroom/id/2839717
3 http://www.gartner.com/newsroom/id/2636073
4 http://www.heise.de/newsticker/meldung/CES-Internet-der-Dinge-komfortabel-vernetzt-2512856.html
FUTURE OF WIRED SMART HOMES

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

-Former CIA Director David Petraeus

---

1 [http://www.wired.com/2012/03/petraeus-tv-remote/](http://www.wired.com/2012/03/petraeus-tv-remote/)
SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS

PROBLEMS
PROBLEMS

Unsecure devices are roled out

Now getting connected

Similar to SCADA problematic

Not managed

Physical protection not enough

CIO of the house
UNIQUE CHARACTERISTICS

- Limited Resources
- Limited Reliability
- Interconnectivity
- Heterogeneity
- Dynamic Changes / Topology
REQUIREMENTS

- Interoperability
- Future proof
- Moderate costs
- Usability
  - Installation overhead
  - User interaction
  - Configuration effort
SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS

STANDARDS
STANDARDS

- Z-Wave
- ZigBee
- HomeMatic
- BidCoS
- Bluetooth LE / Smart
- EnOcean
- Wave2m (Wavenis)
- KNX
- Insteon
THE ZIGBEE STANDARD

ZigBee

- Based on IEEE 802.15.4
- Low-cost
- Low-power
- Two-way
- Reliable
- Purely wireless
ZigBee Application Domains

- Home Automation
- Health Care
- Smart Energy
- Building Automation
- Retail Services
- Remote Control
- Telecom Services
ZIGBEE

// Focused on sporadic real time communication
  – No constant communication

// Remote Control
// Home Automation
// Building Automation
// Smart Energy
// Health Care
ZIGBEE SECURITY

ZigBee Security

Symmetric Encryption

Message Authentication

Integrity

Freshness

AES-CCM*
128bit

MIC
0 - 128 bit

Frame Counter
4 Byte
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
HOW ARE KEYS EXCHANGED?

Preinstalled Devices

Key Transport
• Out of band recommended

Key Establishment
• Derived from other keys
• Also requires preinstalled keys
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 the ZDO Management Leave server service.
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.”

nwkAllFresh

- False
- Do not check frame counter
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!
THE KNX STANDARD

KNX is a bus system for home and building automation

Shared bus used for communication

No Security at the moment

Security not a real concern
It is quite unlikely that legitimate users of a network would have the means to intercept, decipher, and then tamper with the KNXnet/IP without excessive study of the KNX Specifications. Thus the remaining security threat is considered to be very low and does not justify mandating encryption, which would require considerable computing resources. \footnote{\textit{KNX System Specifications - KNXnet/IP, Version 01.04.02}}
KNX WEBINAR

... you will learn how to develop KNX devices that guarantee secure communication and that protect data, within a KNX installation.  

Featuring:

– Authentication
– Data integrity
– Installation freshness
– Confidentiality

SO KNX IS NOW SECURE

ONLY CERTIFICATION ISSUES?
KNX

- Security specification only in draft state
- Security features not included in configuration software
- No products that support security available
SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS

PRACTICAL 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
- Reset to factory
- Join to network
- Test security services
- Command injection
- Scan for weak key transport

https://github.com/zu1na/SecBee
DATA TRANSFER

DIRECT

Coordinator → End device

DATA

ACK

Coordinator ← End device

INDIRECT

Coordinator → End device

Data request

ACK

DATA

timeframe < 8ms
NETWORK KEY EXTRACTION

Fallback key exchange unsecure

Most vendors only implement fallback solution

Same security level as plaintext exchange
WHAT DOES THE VENDOR SAY?

THAT'S NO ISSUE

TIMEFRAME IS VERY LIMITED

---

Cognosec
A UC GROUP COMPANY
So, the

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

... what would an attacker do?
WHAT WOULD AN ATTACKER DO?

DEVICE LOST CONNECTION

WHAT NEXT?
NETWORK KEY EXTRACTION

Jam the communication

Wait for users to re-pair the device

// It is not only about technology :D
PRACTICAL DEMONSTRATION

COMMAND INJECTION
PRACTICAL DEMONSTRATION

DEVICE HIJACKING
DEVICE HIJACKING

Devices are paired and working

1. Reset to factory default settings
2. Setup own network
3. Join the target device to our network
DEVICE HIJACKING

- No physical access is required
- No knowledge of the secret key is needed
- Usability overrules security
SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS

SUMMARY
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.
Last tier communication is, however, still only one part
SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS

TIME FOR QUESTIONS / LETS TALK ABOUT IT
CONTACT

Tobias Zillner, BSc MMSc
Mobile: +43 664 8829 8290
Email: tobias.zillner@cognosec.com