SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS

A demonstration of the challenges of the Internet of Things
WHO IS THAT GUY?

// Tobias Zillner, BSc. MMSc.
  – Former student @HGB

// Senior IS Auditor @Cognosec in Vienna
  – Penetration Testing, Security Audits, Security Consulting
  – Breaking stuff :D

// Owner of a home automation system :D
WHAT ITS ABOUT?

// Not Smart Meter
// Special requirements
// Standards used in IoT
// Burglarizing 2.0 ;)
// Annoying neighbors
AGENDA

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

INTRODUCTION
WHAT IS THE INTERNET OF THINGS?

- Dynamic global network infrastructure
- Based on standard and interoperable communication protocols
- Consists of physical and virtual things
- Everything is identifiable, communicates and interacts
IOT APPLICATION DOMAINS

- Automotive
- Intelligent Buildings
- Medical Technology
- Retail, Logistics
- Safety, Security, Privacy
- Entertainment
- Insurance

IOT Application Domains
EVOLUTION

Stage 1: Personification of Dumb Stage

Stage 2: Partially Autonomous Sensor Networks

Stage 3: Autonomous Independent Devices
HOME AUTOMATION

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
FUTURE OF WIRED SMART HOMES

https://hivizme.files.wordpress.com/2012/06/cable-mess.jpg
WHY IS THIS IMPORTANT?

- 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
SECURITY OF WIRELESS HOME AUTOMATION SYSTEMS

PROBLEMS
**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

\(^1\) [www.wired.com/2012/03/petraeus-tv-remote/](http://www.wired.com/2012/03/petraeus-tv-remote/)
**MOTIVATION**

"We’ll spy on you through your dishwasher"¹

-Former CIA Director David Petraeus

[Image: National Security Agency (NSA) emblem]

https://www.pinterest.com/pin/383368987005584547/
PROBLEMS

- Unsecure devices are rolled out
- Now getting connected
- Not managed
- Similar to SCADA problematic
- Physical protection not enough
- CIO of the house
UNIQUE CHARACTERISTICS

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

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

RISKS & THREATS
1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concern
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security
<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outage due to environmental conditions</td>
<td></td>
</tr>
<tr>
<td>Insufficient Planning</td>
<td></td>
</tr>
<tr>
<td>Lack of regulation for frequency usage and disruption through other systems</td>
<td></td>
</tr>
<tr>
<td>Security configurations</td>
<td></td>
</tr>
<tr>
<td>Weaknesses in key management</td>
<td></td>
</tr>
<tr>
<td>Uncontrolled radiowave propagation</td>
<td></td>
</tr>
<tr>
<td>Eavesdropping of communication</td>
<td></td>
</tr>
<tr>
<td>Replay and manipulation of messages</td>
<td></td>
</tr>
<tr>
<td>Simulation of a valid network components</td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td></td>
</tr>
<tr>
<td>Creation of movement profiles</td>
<td></td>
</tr>
</tbody>
</table>
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

- 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
SYMMETRIC CRYPTOGRAPHY

Sender → Plaintext → Encrypt → Ciphertext → Decrypt → Plaintext → Recipient

Same key is used to encrypt and decrypt message

Shared Secret Key
ZIGBEE SECURITY

// Highly reliant on secrecy of keys

  – Network key
  – Link key

// No PKI available

// No digital certificates
HOW ARE KEYS EXCHANGED?

- **Preinstalled Devices**
- **Key Transport**
  - Out of band recommended
- **Key Establishment**
  - Derived from other keys
  - Also requires preinstalled keys
HOME AUTOMATION PUBLIC PROFILE

// Default Trust Center Link Key
- 0x5A 0x69 0x67 0x42 0x65 0x65 0x41 0x6C 0x69 0x61 0x6E 0x63 0x65 30 39
- 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.
SECURITY SUMMARY

Key Transport

Trust Establishment

Device Tampering

Key Rotation

Security Level per network
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.  

5 KNX System Specifications - KNXnet/IP, Version 01.04.02
... 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
PRACTICAL DEMONSTRATION

NETWORK KEY EXTRACTION
1. Motion sensor will be added to the system
2. Hub is going to be paired with sensor
3. Key will be sent to sensor
4. Exchange will be sniffed
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
So, the

1. Timeframe limited
2. Proximity is necessary
3. Key extraction works only at pairing
WHAT WOULD AN ATTacker DO?

Place a malicious device near the target and wait

Try to force repairing
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

DEVICE TAKEOVER
DEVICE TAKEOVER

Devices are paired and working

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

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

SUMMARY
SUMMARY

Standards provide security measures

Implementation very important

Security at the moment is not mature
SUMMARY

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