(ISC)²

SECURITY CONGRESS EMEA 2016

In partnership with MIS TI TRAINING INSTITUTE

ADVANCING SECURITY LEADERS

emeacongress.isc2.org

#ISC2CongressEMEA

C.I.A. in Your Smart Home?

franjo.majstor@smart-group.hr
Chief Technology Strategist
Smart Group Ltd.
Dublin, October 2016

Table of Contents

- Introduction
- Architecture Overview
- C-I-A Exposure and Solutions
- Q&A

Intro & Disclaimer

- All opinions and suggestions are personal and not endorsed by any vendor
- Any vendor names are mentioned only for illustration purposes

Securing the Virtual Organization

- Home Office is an established working place, a part of your security policy, virtual office
- Smart Home is meant to make your life more convenient, comfortable, more secure
- How does the mix of both impact the security of your organization and your security policies?

What and Where are the Sensors?

- Mux 5-fold sensor
- Smartphone sensors
- Window handle
- Webcams
- SmartTV
- Smarttress
- Drones
- Cars…

Smart Home Architecture

What could possibly go wrong?

Availability Concerns

- Cloud service not available
- DNS service not available
- Internet not available
- Local Wi-Fi failure
- Local SH GW failure
- Radio signal jamming
- Radio congestion

Nest Thermostat Glitch Leaves Users in the Cold

Disruptions
By NICK BILTON JAN. 13, 2016

The Nest Learning Thermostat is dead to me, literally. Last week, my once-beloved "smart" thermostat suffered from a mysterious software bug that drained its battery and sent our home into a chill in the middle of the night.

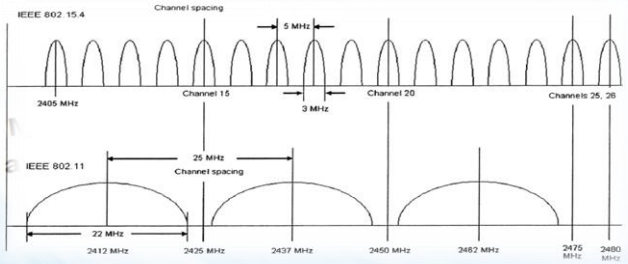
Although I had set the thermostat to 70 degrees overnight, my wife and I were woken by a crying baby at 4 a.m. The thermometer in his room read 64 degrees, and the Nest was off.

This didn't happen to just me. The problems with the much-hyped thermostat, which allows users to monitor and adjust their thermostats on their smartphones (Google purchased Nest Labs for $3.2 billion in 2014), affected an untold number of customers when the device went haywire across America.

Photo illustration by Jim DeMaria/The New York Times and photo by Ben Margot/Associated Press.

Availability Solutions

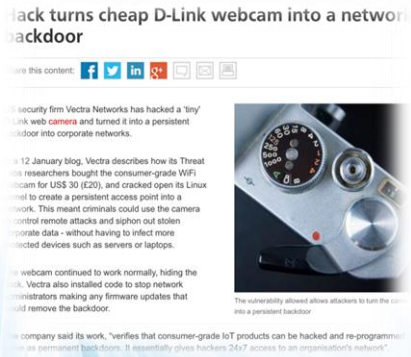
- » Caching local rules
- » Remote control device
- » Local On/Off switch
- » Alternate frequency
- » Local channel coexistence

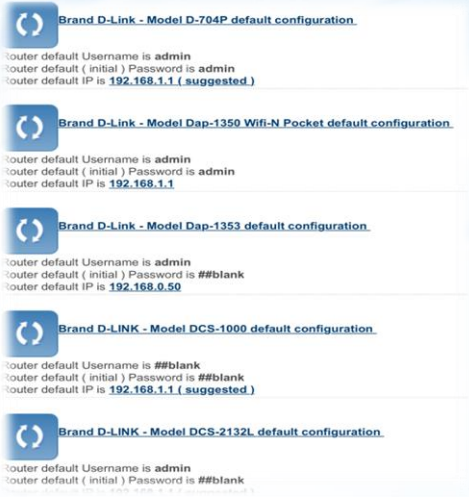


MICAz-Based ZigBee and WiFi Coexistence

Confidentiality Concerns

- Compromised webcam (sound/video)?
- SW patching?
- Defaults?
- Safe initialization?
- Man in the Middle?
- Static encryption keys?
- DMZ?





ZigBee…devices on the market are programmed with ***a secret ZLL master*** key, which you are only given after passing certification. …Test houses have Philips Hue products programmed with ***the certification key*** and are used for IOP testing during certification along with all other golden units …

Due to the necessary exchange of a Nounce prior to any communication the Z-Wave security architecture creates some communication overhead. Therefore the use of this architecture is only mandatory for security related products like door locks, alarm system arm/disarm controllers or roof window openers. For other devices the use of this strong security is voluntary.

Confidentiality Solutions

» ZigBee protocol - initialization (static) key solved by the pre-coded key (Philips Hue) or by the QR coded key on the bulb

Integrity concerns

» Fake sensor and corrupted data impact on human health?

19	47	16:46:38.9827	1.886456	0	ZigBee	NWK	Command	0x0000	0xFFFF	44
20	5	16:46:40.0117	1.029048	0	ZigBee	MAC	Acknowledgement			169
21	5	16:46:40.0744	0.062624	0	ZigBee	MAC	Acknowledgement			170
22	12	16:46:40.1794	0.105064	0	ZigBee	MAC	Data Request	0x0C69	0x0000	171
23	5	16:46:40.1802	0.000768	0	ZigBee	MAC	Acknowledgement			171

```
▷ Frame Information: (53 bytes)
◢ MAC Header: (9 bytes)
  ◢ Frame Control: 0x8861
      .... .... .... ·001 = Frame Type: [0x1] Data
      .... .... .... 0··· = Security Enabled: [0x0] No
      .... .... ···0 .··· = Frame Pending: [0x0] No
      .... .... ··1· .··· = Acknowledgement Request: [0x1] Yes
      .... .... ·1·· .··· = Intra-PAN: [0x1] Yes
      .... ··00 0··· .··· = Reserved: 0x0
      .... 10·· .··· .··· = Destination Addr Mode: [0x2] 16-bit Short Address
      ··00 .··· .··· .··· = Reserved: 0x0
      10·· .··· .··· .··· = Source Addr Mode: [0x2] 16-bit Short Address
  Sequence Number: 181
  Destination PAN ID: 0xD320
  Destination Address: 0x0000
  Source Address: 0x0C69
◢ MAC Payload: (42 bytes)
  ▷ NWK Header: 0xC61E0C6900000248
  ▷ NWK Aux Header: (14 bytes)
  ▷ NWK Payload: (16 bytes)
  NWK MIC: 0x604A82D9
◢ MAC Footer: 0xFFFF
  Frame Check Sequence: 0xFFFF
```

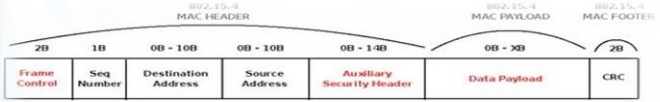
Integrity Solutions

- Z-wave: cyclic redundancy check (CRC)
- ZigBee protocol: crypto CRC, but…
- WiFi: crypto CRC

Table 1. Jamming efficiency against ITU-T G.9959 frames.

Integrity Data Rate	Check*	Max Payload	Jammer Bits to Jam	Efficiency
9.6 Kbps (Rate 1)	8-bit checksum	512 bits	1	512
40 Kbps (Rate 2)	8-bit checksum	512 bits	1	512
100 Kbps (Rate 3)	16-bit CRC	1,360 bits	1	1,360

ITU-T G.9959 uses non-correcting integrity checks.



The AES algorithm is not only used to encrypt the information but to validate the data which is sent. This concept is called Data Integrity and it is achieved using a Message Integrity Code (MIC) also named as Message Authentication Code (MAC) which

802.15.4 is designed to facilitate the use of symmetric key cryptography in order to provide data confidentiality, data authenticity and replay protection. It is possible to use a specific key for each pair of devices (link key), or a common key for a group of devices. However, the mechanisms used to synchronize and exchange keys are not defined in the standard, and left to the applications.

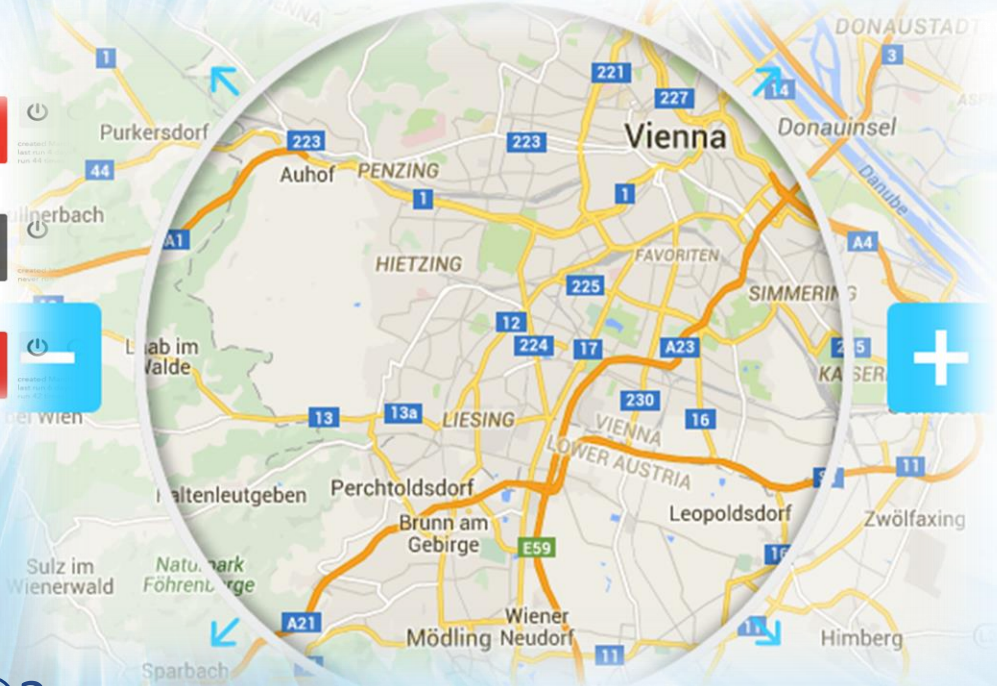
Safety (First!) Concerns

- Safety first - you should **NEVER** connect any heating device to your Smart Electricity Socket, unless it has an additional thermostat to shut off itself!

- …and think what else could go wrong if you loose the automated control…

3rd Party Concerns

Our apologies. Something isn't working quite right.



» Robbery As A Service ☺?

Challenges & Conclusions

- Cloud Services impact, visibility, control
- Standardization vs. proprietary
- Social Engineering
- Thing-Bots
- Smart Home Office & Corporate Policies

References

- **ZigBee Alliance**: zigbee.org
- **ZigBee 141 Success Secrets**, Dawn Rivas, August 2015
- **Vision and challenges for realizing the Internet of things**, CERP-IoT book, March 2010
- **Z-Wave Alliance**: z-wavealliance.org
- **Z-Wave Basics**, Christian Paetz, 2015
- **Abusing the Internet of Things**, Nitesh Dhanjani, August 2015
- **ZigBee Exploited**, whitepaper from www.zillner.tech, August 2015
- **802.15.4/ZigBee Analysis and Security**, Dartmouth Computer Science Technical Report, March 2011
- libelium.com/security-802-15-4-zigbee
- **Internet of Things: Challenges and Opportunities**, Subhas Chandra Mukhopadhya, 2014

Questions?

Thank you!

franjo.majstor@smart-group.hr
Chief Technology Strategist
Smart Group Ltd.
Dublin, October 2016

(ISC)²

SECURITY CONGRESS EMEA 2016

In partnership with MIS TI TRAINING INSTITUTE

ADVANCING SECURITY LEADERS

emeacongress.isc2.org

#ISC2CongressEMEA