# Product Security Analysis

## Contents

# 1 Brief overview of communications protocols

There are several ways that Internet of Things product communicate to each other as listed below:-

| Protocol | Advantages | Disadvantages | Comments |
|---|---|---|---|
| **WiFi** | • Reasonably secure if all security measures are in place.<br>• Anyone trying to connect must know the network key. | • The radio range is very poor.<br>• The WiFi radio channels are very congested.<br>• The protocol is "open" and known to hackers.<br>• The same network key is used for multiple devices. | Very few Internet of Things products use WiFi. |
| **Z Wave** | • The radio range is good. | • Encryption is not always enabled by the product's manufacturer.<br>• The protocol is "open" and known to hackers.<br>• The same encryption key is used for multiple devices.<br>• Only one radio channel is available. | Lots of reports of hacked Z Wave devices. |
| **Zigbee 2.4GHz** | • There are lots of radio channels so congestion is low. | • The radio range is very poor.<br>• The encryption key is easily obtained by "sniffing".<br>• The protocol is "open" and known to hackers.<br>• The same encryption key is used for multiple devices. | Lots of reports of hacked Zigbee devices. |
| **Zigbee 868MHz** | • The radio range is good. | • The encryption key is easily obtained by "sniffing".<br>• The protocol is "open" and known to hackers.<br>• There is only 1 channel so congestion is high.<br>• The same encryption key is used for multiple devices. | Lots of reports of hacked Zigbee devices. |
| **CarbonNano** | • The radio range is good.<br>• There are lots of radio channels so congestion is low.<br>• The encryption key cannot be obtained by "sniffing".<br>• The protocol is "closed" and is not known to hackers.<br>• Every device has its own encryption key. | | |

## 2 Brief overview of home gateway designs

There are several ways that the home gateway product communicates to the Internet:-

| Design | Advantages | Disadvantages | Comments |
|---|---|---|---|
| **Software Operating System**<br><br>The Home Gateway has a microprocessor inside that runs a software operating system for internet communications. | This is an "off the shelf" solution, which makes it easy for the product manufacturer to design a product quickly. | Any security holes in the operating system can be exploited by a hacker.<br><br>A hacker can easily overload the operating system by performing DDoS and DoS attacks. | Many home gateways are designed like this.<br><br>✗ |
| **Hardware Operating System**<br><br>The Home Gateway has a special purpose microprocessor inside that runs a hardware operating system for internet communications. | Does not contain a software operating system.<br><br>Any DDoS or DoS attacks will merely slow down the operation slightly. | | CarbonNano uses this system.<br><br>✓ |

# 3 Useful reading:-

*Researchers at Black Hat and Def Con warned about security flaws in Internet of Things devices using the ZigBee protocol, leaving Philips Hue light bulbs, smart locks, motion sensors, switches, HVAC systems and other smart home devices vulnerable to compromise.*

**http://www.networkworld.com/article/2969402/microsoft-subnet/researchers-exploit-zigbee-security-flaws-that-compromise-security-of-smart-homes.html**

*EZ-Wave: A Z-Wave hacking tool capable of breaking bulbs, abusing Z-Wave devices. Interview with the creators of EZ-Wave, a Z-Wave hacking tool released at ShmooCon that can break fluorescent light bulbs and abusing other Z-Wave devices.*

**http://www.networkworld.com/article/3024217/security/ez-wave-z-wave-hacking-tool-capable-of-breaking-bulbs-and-abusing-z-wave-devices.html**

*"we identified a critical protocol implementation vulnerability that could allow an attacker to reset the established network key on a target Z-Wave door lock to a known value of his choice and then issue unauthorised commands. "*

https://sensepost.com/cms/resources/conferences/2013/bh_zwave/Security%20Evaluation%20of%20Z-Wave_WP.pdf

*Virgin Media has told 800,000 customers to change their passwords to protect against being hacked.An investigation by Which? found that hackers could access the provider's Super Hub 2 router, allowing access to users' smart appliances.*

http://www.bbc.co.uk/news/uk-40371373

# 4 Summary

Below is a summary of the various protocols used in Internet of Things devices.

| Item | WiFi | Z-Wave | Zigbee 2.4GHz | Zigbee 868MHz | CarbonNano |
|---|---|---|---|---|---|
| Long Radio Range | ✗ | ✓ | ✗ | ✓ | ✓ |
| Low Congestion | ✗ | ✗ | ✓ | ✗ | ✓ |
| Unknown Communications Protocol | ✗ | ✗ | ✗ | ✗ | ✓ |
| Every Device Has Its Own Encryption Key | ✗ | ✗ | ✗ | ✗ | ✓ |
| Not Easily Hacked | **Depends on how the WiFi is set up.** | ✗ | ✗ | ✗ | ✓ |
| Encryption Key Cannot Be Obtained By Sniffing. | ✓ | **Key could be changed.** | ✗ | ✗ | ✓ |