ZigBee and the Smart Home: Is Security An Issue?

Cees Links, Founder and CEO, GreenPeak Technologies – www.greenpeak.com

In one of my earlier blogs I shared that today maybe around 600 million homes have WiFi. People share their lives with their family and friends, and execute their financial transactions wirelessly over the Internet without being overly worried about security, and, despite the recent NSA disclosures, I wonder whether many people have changed their online behavior.

Our homes (from a Smart Home perspective) are still quite primitive. Especially when compared to the sophistication of new cars with all the features that one could wish for a Smart Home: from central door locking to opening/closing windows, energy management/control including heating/air conditioning, and automated sunshades, etc. Why are our cars so smart and our homes so dumb?

How do we think about our Smart Home and security?

Quite recently there was a major article in the Wall Street Journal (31-July-2013): “Hackers Expose How Connected Toilets, Heaters and Light Bulbs Are at Risk” that provided examples of situations where “computer experts” can break into our Smart Homes via the internet and take over control over basic functions. Now, a hacker flushing your toilet maybe a nuisance, but unlocking the front door to let uninvited guests in may be really nasty. So, clearly some work to be done as a lack of security would be really a showstopper for rolling out the Smart Home. Technologists and marketers need to work together to explain how security and the Smart Home go together, as ultimate security does not exist.

The good news for ZigBee is that in the above article and its examples there was no mention of any ZigBee compromised system. This does not mean that ZigBee security cannot be compromised but it means at least that doing so is not trivial. ZigBee has many methods for making sure that the network is kept secure. It has 128-bit AES link encryption, making it virtually impossible to casually listen in to any exchange. It also uses encrypted key exchange for commissioning of new devices and frame counters to avoid replaying of messages ("to open the door again"). ZigBee has learned a lot from WiFi and probably the best news is that the ZigBee Alliance has a system in place to stay alert to emerging issues and to address new and "out of the box" ways to compromise security of a Smart Home system.

To put things in perspective: "ultimate security" will be ultimately cumbersome for the user. There is always a balance between (cost of) security and user friendliness. It is also important to understand that the technology that is secure today may not be secure tomorrow. Over the last 10 years, WiFi went through several iterations of upgrading its security. The current level of security is sure to not be the final one either, as new ways of attack and more powerful computers will continue to find holes in the latest security protocol. And then of course there is the end-user, usually the weakest link in the chain: forgetting to lock the door or losing the key of the safe will compromise the security.

From that perspective, it is also important to understand what type of risks there are and what attacks need to be confronted, and making a trade-off between the risks for such an attack versus the cost of prevention. For instance a critical moment in a system is during installation: like a hacker looking over your shoulder when entering the security key. In that case he needs to be there at that moment, and be able to listen into the radio signals and derive the key information. Protection against something like this is possible, but becomes very expensive. The problem therefore is usually also not during installation, but more with sophisticated ("brute force") attacks over the internet, trying as many possibilities over a longer time – without the victim even being aware.

The usual solution of longer keys and more complex algorithms is possible with more complex systems like computer or smart phones, but entering a long key or supporting a complex security algorithm in a light bulb might be a serious cost adder. And when talking about light bulbs: writing down the key from the back of a router and entering it into a tablet can be done, but entering a key into a light bulb is more of a challenge. Of course: nothing is impossible, and when the light bulb has a radio, that radio can receive a key in a short time window after the moment that it is plugged into its socket – assuming that the key is not encrypted and not someone is just listening at that particular moment, as then the security of the system is compromised.

There are More Challenges

Assuming that one has 100 Smart Home devices, all securely connected to the router, and then for whatever reason one gets a new router, for instance because of changing from one operator to another. With 10 WiFi devices (PC, laptop, table, TV,

game station, etc.) in the home entering the new key in every device is somewhat of a pain, but doing so for 100 Smart Home devices will be of different magnitude. Storing the keys of all the devices in the cloud might be an idea, ah-well… not sure whether people like that either. Although: one can store the keys encrypted in the cloud, and leave the decryption key at home! There are many ways to solve a problem.

Today ZigBee is relatively secure. But this does not mean that there is nothing to improve. In particular today when a consumer buys different applications for the smart home from different suppliers, there is not necessarily one security system.

For example: a Smart Energy system has a different level of security than a Smart Lighting system. It is easy to understand why: utilities are significantly more concerned about the risk of people stealing electricity than consumers are concerned about an unauthorized person switching on/off a light. The question is even whether utilities ever want their energy distribution system compromised with “simple” Smart Home security. But also for consumers the Smart Home security requirements are not uniform: one can imagine that a consumer wants to have his central home door locking system to be really secure and not compromised by using the same keys as the utility for Smart Energy.

So, how will the Smart Home develop from a security perspective?

Today the Smart Home is a set of more or less independent applications, whether for consumer electronics, security, energy management, lighting or home care. Product developers in the different application spaces are developing products independently and these products have a large variety of user interfaces and security solutions. Over time the security protocols for these networks will start to converge and standardize, while at the same time, the user-friendliness will improve.

Today we (relatively) trust the security of our WiFi networks (probably also because many websites are using SSL nowadays), but it has taken a few iterations over the years to get there. The same will happen with ZigBee: more usage will further encourage product providers to strengthen and improve the way security is handled in ZigBee and make it as user-friendly and trusted as WiFi is today.

GreenPeak Technologies is a fabless semiconductor company and is a leader in ZigBee silicon solutions for the smart home. GreenPeak is privately funded. It is headquartered in Utrecht, The Netherlands and has offices in Belgium, USA, Japan and Korea.

GreenPeak has won the prestigious 2012 Red Herring Top 100 Europe award and is recognized as a leader in developing new wireless technologies for consumer electronics and smart home applications, demonstrating rapid growth and adoption by major customers.

For more information, please visit www.greenpeak.com [1].

Links:
[1] http://www.greenpeak.com