Security in the smart home office, what you should think about

Whitepaper
July 2016
v1.0

Franjo Majstor
Smart Group Ltd.
franjo.majstor@smart-group.hr,

Abstract

In the age of always on connected homes and more jobs that could be done from remote, a home office is becoming pervasive and usual working environment for many people that simple and efficient do their job from home. At the same time another direction of technology has taken place in home automation that leverages the always on connected homes too. Light, sunshades and heating could be turned on and off remotely easiest then ever. Wi-Fi connected webcams we could easily check what is going on at home while we are away too. Both trends of a modern home usage that are together actually happening at the same place, are not necessarily controlled or supervised together even though that they may non intentionally but severely impact each other. This is the whitepaper that only highlights the home automation impact on the work happening at very same home place too.

1. Introduction

Smart home or home automation systems are on the market already for a while, however the explosion of their usage has really started with standardized protocols like Zigbee or Z-Wave that allowed multiple components from different vendors to be a part of the same home system. Another factor that have significantly impacted the growth of smart home systems on the market is the availability of low cost sensor elements that could be easily embedded into multiple different devices. Additional factors that stimulated growth in use and availability of smart home systems are mobile apps and pervasive use of before so called proxy and now simple called cloud based services on the Internet. They both allow almost any smart phone with an App to become a smart home control device when connected to a home network or with a help of cloud services have same function from anywhere in the world.

2. Architecture Overview

As already mentioned, pervasive availability of a low cost and affordable sensors became one of the driving factors in use of home automation systems, so let's start first with a view on what or where is the sensor that could make our home smart today. Sensors are input devices that give the vital information to our smart home systems so it can make smart decisions. Temperature, humidity, motion, air quality or brightness detector are all examples of sensor and inputs based on what we can increase the temperature by turning the heating on or lower it by turning the AC on or putting down our sunshades. They are all on that size that multiple of them could fit into a table tennis ball shape or be a part of a window handle. Combination of inputs and actions could really simplify our lives, increase the comfort of living or simple make our home more secure and give us a peace of mind that all is well at our home place while we are away.

Figure 1. Different Sensor Examples

Some new inventions go that far that they build a sensor in the bed mattresses to recognize your sleeping habits or warn you when someone else is in your bed. Putting the motion sensor in your distance mail box could simple warn you when the post man have opened it so you can check you post couple of floors away only when you know that the post is there. Or, …if you for example combine the motion sensor input with the CO2 sensor in your bedroom, that could pretty accurately detect the number of breathing souls in the room, you can get some interesting conclusions…

Figure 2. Smart Home Architecture

Sensors used to be connected to a smart home system with wires that made them difficult to install and required pre-installed or add on wiring system. Since the development and standardization of low power consuming radio communication protocols like ZigBee that operates at 2.4GHz or Z-Wave that operates in 800-900Mhz range of frequencies, became really easy to put battery operated sensor almost everywhere and without needed wires.

A bit of history overview could help to understand where we are with that. First radio control protocols were proprietary, unsecure, analog and unidirectional. They sent one way messages over but had by nature of unidirectional communication really no feedback of weather the message has arrived or not so it was necessary to have several retries programmed to be sure that message has arrived on target. Example of that is 433Mhz frequency based equipment that on a side of several limitations has still one big advantage and that is a low price. Other newer protocols still have to reach that. ZigBee and Z-wave are both low power consumption, bidirectional and secure radio communication protocols that are gaining ground but still have a path to go to get devices that use them their pricing down. Both also require a separate gateway between home network and radio sensor network, however there are few solutions on the market already that have both WiFi and for example Z-Wave radio support in the single device. As standards mature we can expect only more to come.

3. C.I.A exposures and solutions

Confidentiality, availability and integrity of the smart home solutions are amongst the very first three topics that we from the security perspective have to look into. This could give as at least an idea, where the things could go wrong or get broken. No wonder that, if we look at the communication path, actually every single link or single hardware element that is vulnerable to failure is a single point of failure in this architecture as illustrated in Figure 3.

Figure 3. Single Point of Failures in Smart Home Architecture

4. A for Availability

It used to be so that the uplink and connectivity to the Internet service was the most unreliable and most vulnerable spot for the availability of the whole system. This is however nowadays by far or better to say at least in urban areas not any more the case. Internet connectivity is pretty reliable service that has outages comparable to the electricity supply service. Some issues we could still experience today with a DNS infrastructure availability, and that of course affects the Internet service in general too, but is fortunately getting less frequent too… How about the cloud based centralized software services? Even though that history tells us, and few recent examples in Figure 4 could only confirm that, centralized cloud services could be the most reliable part of the architecture. If they are built with all redundancy and resiliency that is needed for such a service, verified and certified with standards that are norms for cloud services today, there should be no excuses nor reasons to have the single point of failure in that part.

Figure 4. Examples of recent Smart Home service outages

So where is actually the biggest problem or weakness in architecture that is illustrated in Figure 3? My experience is that the model that is used has actually the biggest compromise with maintenance as well as scalability in introducing new features. What that really means is that the smart home gateway even that we want to have it as smart as possible, actually has to be as simple and as stable device that would require almost no intervention or any SW upgrades ever. You could compare it to an intelligent kitchen appliance that should always work standalone but would require as little as possible or no user maintenance intervention nor software updates. All intelligence in your smart home system hence actually could be in the back end centralized software cloud services that could be easily upgraded and bring new functionality without upgrading or affecting your home setup. That is the reality compromise of such architecture where all what is in your home should be as simple, means as stable, as possible and requiring after the initial setup minimum user intervention, while the complexity, intelligence and new features could be smoothly added on the central side and be driven from the central side only. Logical question than is, what would happen when the connectivity between the two (central cloud software services and a local smart home gateway) is in rare but possible case still lost? The local smart home gateway should have an option to operate independently, That means, keep the last set of rules, or cache the last configuration setup given by the centralized service and with that be able to independently execute operations with and on sensors, send you alerts etc. further without a centralized service. Only changes in configuration, changes in rules or scenarios should be impacted and only until the connectivity to a centralized software service is re-established.

5. C for Confidentiality

Confidentiality of all information that is exchanged within the home environment is a kind of secondary but nevertheless important aspect that we should be aware of.

Here we have to start with basics, which are somehow aligned with previous topic of availability too. As simpler local components are built, that less are the chances that there is a software bug in them and that they would require any, for home user quite difficult task, of upgrading and patching. Why is patching directly related to confidentiality? Well it is, because exactly are the software vulnerabilities in the devices abused first to get to the privileged mode access and then bypass all other security features that are usually there. Example of that would be a vulnerable out of date software in the webcam that is not only a video streaming device with a microphone audio capability. In some sophisticated webcam models they could also be nicely turned and not only see around but also point and zoom into the screen of your home computer and hence get all the data that otherwise is, from the computer via VPN, personal firewalls etc, kept confidential towards the party that is intended for.

When we are referring to confidential communication, encryption is an inevitable topic, so it is also good to have at least an overview of smart home communication protocols from that perspective. Wi-Fi that is usual local area network at home nowadays, have gone through several development iterations before it came to a WPAv2, a solid authentication and encryption standard. Webcams are usually, if not connected via wire, sitting on the Wi-Fi network simple because video streaming requires higher bandwidth. Wi-Fi cameras are also connected to their own power, so if all is configured well, default access credentials are changes and software is up to date, we could say we are ok on that side. Most of the other home automation sensors are usually battery operated and therefor are using low consumption radio standards like ZigBee or Z-Wave. Both ZigBee and Z-Wave claim to have an encrypted communication which is good for the start, however encryption also has to be turned on, properly initialized as well as have a solid key management and that is where their challenges only start...

> ...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 ...

Figure 5. ZigBee encryption bootstrapping weakness

Let's look at the ZigBee encryption key management first. ZigBee protocol that is a subset of 802.15.4 standard has pretty good centralized key distribution

schema where different keys are used for the link or network wide communication. Initial key that is distributed to a new device is encrypted with so called "secret master key" and hence all further communication is depending on it. Secret master key is supposed to be known only to vendors that produce ZigBee products and is supposed to be kept secret.
History tells us that static, fixed secrets are not that long secrets and is the only a question of time when the key that is fixed and static will be, or maybe already is, published on the public net. ZigBee alliance response to this was that initialization key is used only for a very short period of time and in near proximity during the initial device peering process, which is correct, however does not guarantee you that with a bit of social engineering someone would or could lure the harmless user to re-initiate that process while being monitored and is able to capture the follow up keys… Z-Wave encryption seems to be even weaker but mostly on implementation side, as even though the strong encryption with AES and Nounces exchange are defined in standard, they are left as voluntary to implementers that usually save on security to have minimal overhead and delay, lower power consumption etc. Comprehensive encryption is mandatory only with Z-Wave devices that are security related like doors, windows locks and alarm systems.

5. I for Integrity

Integrity of the solutions is most of the time the most mystified, least important concept, however in light of home automation and IoT usage where the accuracy of the data that we are getting from the sensors is actually getting to the front level of importance. The reason for that is that all decisions and actions of a smart home system are based on the accuracy, correctness or not impacted integrity of the data that we are getting from sensors. An example of that would be the case when we need to leave the certain space when the quality of the air is not good or even impacting human life. Protocols used in the smart home have different levels of integrity protection. Wi-Fi based protocols through the WPAv2 got the cryptographic checksum that guarantees that the accuracy and integrity of the data is not impacted by the transmission. Z-Wave protocol has, as we have already seen, their strong encryption by using AES, left as optional while for integrity of the transmitted frame uses simple CRC checksum that guarantees no protection against maliciously targeted integrity changes.

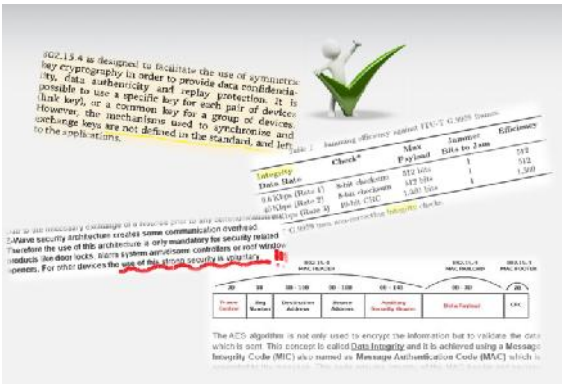

Figure 6. State of Integrity art in Smart Home protocols

ZigBee as a protocol seemed to be in a better shape as in standard has defined MIC (Message Integrity code) and MAC (Message Authentication Code) options that guarantee cryptographic integrity checksum of transmitted data. Stress is unfortunately again on the usage of it, as ZigBee standard developers have left the decision for the key exchange to be used for MAC to an application layer above.

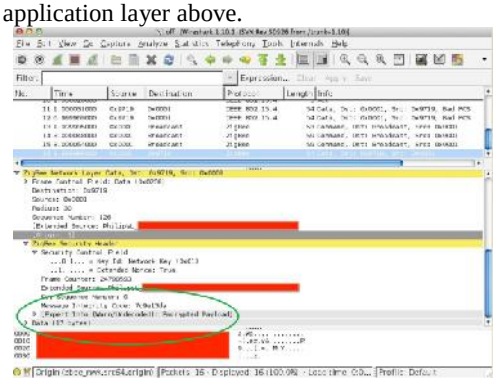

Figure 7. Zigbee MAC (Message Authentication Code) authenticated frame example

6. Safety

As well as integrity of the transmitted data may impact the human life, there are unfortunately many more things that we as humans are vulnerable upon. One of the topics that deserves specially to be mentioned is a high temperature or in particular the consequences of a too high temperature that could cause a fire. As smart home automation components, like smart electricity sockets could be used to control all kind of electricity operated devices, special care or at least clearly visible warnings should be shown to users not to plug in them any heating devices that do not have an extra self check and shut off protection from overheating.

Figure 8. An extra caution should be given to users what not to do with their smart sockets

7. 3rd Parties

In ever connected world where no single solution is developed by single party, it may seem obvious to have 3rd party services connected to your home automation system ad that could bring multiple benefits. It could for example get your heating costs down not only based on the current temperature but also based on the weather forecast or reduce the heating when you go away from the city but you have forgot to tune the heating down. All of that is already possible with open software interfaces on home gateways today or with a small add on App on smart phones that allows access to your geolocation and delivers your position info to to you smart heating system. Convenience and benefits you gain with such services are enormous, unfortunately availability, confidentiality or integrity impact of your overall smart home system is then transferred and heavily dependent as only illustrated in Figure 9., on how well that 3rd party service security features are done too…

Figure 9. Example of IFTTT 3rd party service outage that happened exactly at the time of writing this whitepaper

8. Challenges and Conclusions

There is no doubt still lot of challenges for safe and secure home automation systems ahead; however they are today already in much better shape then proprietary closed and most of the time prohibitively expensive systems a decade ago. Solutions that are reducing the impact and involvement of ordinary users in security based decisions and at the same time are attractive enough in convince of use and comfort, while at the same time offering the energy consumption and cost reduction are making its way into ordinary homes and are overall making homes that are being smart certainly safer and more secure.

9. References

[1] ***ZigBee Alliance:*** *www.zigbee.org*
[2] ***"ZigBee 141 Success Secrets " ";*** *Dawn Rivas, August 2015*
[3] ***"Vision and challenges for realizing the Internet of things";*** *CERP-IoT book, March 2010*
[4] ***Z-Wave Alliance:*** *z-wavealliance.org*
[5] ***"Z-Wave Basics";*** *Christian Paetz, 2015*
[6] ***"Abusing the Internet of Things";*** *Nitesh Dhanjani, August 2015*
[7] ***"ZigBee Exploited";*** *whitepaper from www.zillner.tech Aug 2015*
[8] *"**802.15.4/ZigBee Analysis and Security**"; Dartmouth Computer Science Technical Report. March 2011*
[9] ***Security in 802.15.4 and ZigBee networks*** *David Gascón www.libelium.com/security-802-15-4-zigbee April 2009*
[10] ***"Internet of Things: Challenges and Opportunities";*** *Subhas-Chandra Mukhopadhya, 2014*

10. About Author

Franjo Majstor, *CISSP is the Chief Technology Strategist at Smart-Group Ltd, young Croatian startup in a Home Automation/IoT space. He is an author of several security articles in Information Security Management Handbook series from Hal Tipton & Mickey Krause, was long term security consultant for several vendors as well as frequent speaker on security topics at international recognized security conferences. More about his work you can read at: www.employees.org/~franjo/*