Are Internet of Things Safe and Secure

Carl Brackett

East Carolina University

Abstract

As technology advances, so do the security risks involved. In the last couple of years, a new term has been introduced to society called "Internet of Things". This term can be used for any type of device that now connects to the Internet (Sasso, 2015). The question is how secure are these devices for consumers to be using?

This paper is going to be researching whether these devices are safe for consumers to be using in their businesses or homes. There will be several examples discussed of different devices out on the market that may or may not be secure in their usage. In determining whether these devices are secure or not, this research will look into how information obtained by these devices are or are not being kept private from the rest of the world.

Conclusions will be based off of the findings and examples that were researched in this paper.

Keywords: *internet of things, iot, security, internet, zigbee, z-wave, wifi, privacy*

Introduction

As technology has made advances over the years, the security risk involved has risen with these new technological ideas. A new term has been introduced into society called "Internet of Things". This term can be used for any type of device that has the ability to connect to the Internet (Sasso, 2015). The question is how secure are these devices for consumers to be using?

These new devices come in different shapes and sizes while connecting to the Internet in various ways. Although these devices may make an individual's life more convenient, the security of these devices is questionable. Does this convenience come with a price to the privacy of a consumer using these devices? The answer to this question will vary depending on how the consumer sets the device up initially.

Internet of Things are made so the consumer can remove it from the box and have the device operational in a few minutes. The problem with this scenario is manufacturers of these devices are looking how to make it simple to setup for the consumer, but without adding in the additional security the device may need to make it secure while accessing the Internet. The additional security may make it more complicated for the consumer to get the device operational by adding in extra steps to make sure the device has been secured.

This paper will focus on whether these new devices are safe for consumers to be using on a daily basis. Several different device examples will be provided and discussed to determine if these devices can be safely utilized by consumers. This research will show how these devices are collecting the consumer's information and determining

whether the information is being kept private. Conclusions will be based off of the examples and findings of these devices based on the research found in this paper.

Literature Review

Internet of Things (IOT) may be a new term for most, but people are soon realizing that most of the devices have been made for years with a few exceptions to these devices. What is new is that the devices can now connect to the Internet so that some of the devices functions can be automated or programmed to work automatically without an individual being there to start the device (Morgan, 2014). Devices will be able to connect to the Internet on demand like having an on and off switch for the device (Morgan, 2014).

Home automation has been a popular subject around Internet of Things by connecting most of the devices found in the home or business to the Internet so they can be controlled by the simple push of a button on a smart phone (Griffith, 2016). These devices may include the stove, refrigerator, coffee maker, thermostat or even the cameras monitoring the premises. Now the question is how are these devices actually connecting to the Internet and what security protocols are these devices using to make sure they are secure on the network (Griffith, 2016)?

The protocols used to get these devices connected to the network can be wired, wireless or a combination of the two (Griffith, 2016). Choosing the right protocol to control the devices in the home can be somewhat tricky and confusing (EH Contributor, 2016). Consumers need to be looking at interoperability, cost, security and the number of devices that the protocol can support when deciding to make a purchase for their home (EH Contributor, 2016).

The security protocol plays an important role in home automation, the next sections are going to be discussing the most popular security protocols used today (EH Contributor, 2016). The strengths and weaknesses will be discussed with the type of devices that can be used with each protocol. Each protocol will be determined secure or unsecure for devices to be using it as their protocol.

UPB or Universal Powerline Bus was developed in 1999 and uses the existing electrical wiring in the home for communication between devices by peer-to-peer connections (E-Man, 2014). This protocol is inexpensive to setup and allows for two-way communication (E-Man, 2014). The problems with this protocol is that it is limited to certain devices and provides no encryption (E-man, 2014). A good example for using this protocol would be for the lighting in the home (E-Man, 2014). The next two security protocols are wireless protocols named ZigBee and Z-Wave.

ZigBee and Z-Wave both use a mesh network to communicate with the devices wirelessly (LinkLabs, 2015). Both protocols use a controller to allow the consumer to access their devices by smartphone or tablet. Devices like lights, hvac and other home appliances can be controlled using ZigBee or Z-Wave protocol (LinkLabs, 2015).

ZigBee has a lower operating range of 35 feet for devices compared to Z-Wave which can operate at 100 feet for devices (Parrish, 2015). Z-Wave supports a maximum number of 232 devices where ZigBee can support a maximum of 65,000 devices (Parrish, 2015). Both of these protocols use AES-128 symmetric encryption used by some online banks (Parrish, 2015). Some of the companies that use Z-Wave in their devices are Verizon, Honeywell and AT&T (Parrish, 2015). ZigBee is used in devices by companies like LG, Logitech and Time Warner Cable (Parrish, 2015).

The last security protocol going to be discussed is WI-FI. Almost every home that has Internet probably already contains a wireless access point or wireless router to connect the home's wireless devices (EH Contributor, 2016). The problem with WI-FI is that the devices are going to be competing for bandwidth in the home, possibly creating slower response times from the devices (EH Contributor, 2016). The encryption used for these devices will be as strong as the encryption setup on the wireless router or access point.

Now that the security protocols for home automation have been identified, devices are likely using Zigbee, Z-Wave or WI-FI as their security protocol. The next section is going to be discussing different devices and how they are accessing the Internet. Is the information these devices are collecting being kept private or is it being made public for everyone to see on the Internet?

Internet devices come in many different shapes and sizes. Homes can now have a smart refrigerator that connects with WI-FI to alert the consumer if something is going to spoil or if the refrigerator is low on certain items by scanning the items as they are put into the unit (Itzkovitch, 2013). There is also a downside of the refrigerator being able to send a consumer an alert, the unit can be breached and setup as a botnet for phishing emails or a DDOS attack (Arthur, 2014).

In the kitchen with the refrigerator, a home can have a smart oven that allows the consumer to wirelessly access their oven over WI-FI to set times or start it to preheat before they have even arrived at the home. These features are all done with the touch of a button on a smartphone or tablet. The problem with these type of devices is that these companies show the consumer happy about being able to access the device remotely but

they do not promote any kind of security for these type of devices besides stating they can connect them over WI-FI. Security trends through the years show that any device that can connect to the Internet may be vulnerable to an attack.

Camera systems, baby monitors or web cams have the ability for a consumer to access the systems remotely for viewing (Cullinane, 2014). The consumer can easily access them through the Internet with an app, but did the systems allow the consumer to setup a password or does it make the consumer use the default username and password making it easily usable by someone finding the ip address of their camera system.

Companies need to warn the consumer and make the consumer aware of the dangers that these devices can bring if security is not taken in consideration. These kinds of devices should make the user change the password as one of the first steps in getting the unit setup (Cullinane, 2014). Instead these companies are wanting to make sure they are easy and simple for the consumer to start using immediately.

Even a consumer's vehicle is not safe since most newer models are now connected to the Internet. A good example would be when a Chrysler Jeep Cherokee was hacked by a couple of researchers sitting on a couch (Roberti, 2015). Since the vehicle has an ip address, they could remotely control the vehicle through the entertainment dashboard (Roberti, 2015). The AC, radio, brakes and steering could be impacted with a few keystrokes on a laptop by a zero-day exploit, a nightmare for the manufacturer (Greenberg, 2015).

People buy things to make their lives more convenient sometimes even though they may not need them but because they are the popular item for the month or year (Miranda, 2016). Security and privacy should be made a priority with these devices

connecting to the Internet, but is usually placed at the bottom of the list for manufacturers to consider when they having a working device that the consumer wants to purchase and use immediately (Miranda, 2016). Consumers just need to remember that no matter what the device may be, they need to do some investigating on the product before making a purchasing decision.

Conclusion

In conclusion, Internet of Things is a term used to describe devices that are now connected to the Internet. Most of the devices have been around for years, but now have Internet connectivity added to them. Devices can connect to the Internet in various ways depending on what security protocol is chosen. Home automation is done by choosing what security protocol is going to be used whether it be ZigBee, Z-Wave or WI-FI.

Each security protocol was different from one another by number of devices it supported, range of devices or simplicity of setup for the consumer. Security varied between protocols depending on which one was selected by the consumer. Ultimately the chose relies on the customer researching each protocol to make an informed decision on which one to select to control their devices.

Examples of devices were discussed showing how Internet ready devices could be compromised like the smart refrigerator or even a Chrysler Jeep Cherokee just because it was connected to the Internet and was provided an ip address. Privacy becomes an issue when these types of devices access the Internet since the manufacturers are not adding in any additional security to help stop attacks against these devices. They are more concerned with selling a product than trying to protect the consumer from themselves because they wanted the latest product on the market.

Ultimately if these new devices connecting to the Internet are not setup properly and secured by the consumer, their privacy may be at risk or worse their safety. Consumers need to protect themselves and make sure they understand the risks involved by allowing their camera system access to the Internet or setting up their refrigerator to alert them when a certain product is low or out of date. These are the type of devices that hackers are looking for and will use against the consumer as long as it gets the job done.

References

Arthur, C. (2014, January 21). Help! My fridge is full of spam and so is my router, set-top box and console. Retrieved from https://www.theguardian.com/technology/2014/jan/21/fridge-spam-security-phishing-campaign

Cullinane, S. (2014, November 20). Webcam security: What you must do. Now. Retrieved from http://www.cnn.com/2014/11/20/world/europe/uk-web-cam-hacking-explainer/

EH Contributor. (2016, January 11). Home Automation Protocols: A Round-Up. Retrieved from http://www.electronichouse.com/daily/smart-home/home-automation-protocols-what-technology-is-right-for-you/

E-Man, M. (2014, August 25). Universal Powerline Bus. Retrieved from http://buildyoursmarthome.co/home-automation/protocols/universal-powerline-bus/

Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway - With Me in It. Retrieved from http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Griffith, E. (2016, January 29). How to Build Your Smart Home: A Beginner's Guide. Retrieved from http://www.pcmag.com/article2/0,2817,2410889,00.asp

Itzkovitch, A. (2013, September 18). The Internet of Things and the Mythical Smart Fridge. Retrieved from https://uxmag.com/articles/the-internet-of-things-and-the-mythical-smart-fridge

LinkLabs. (2015, October 30). Z-Wave vs Zigbee. Retrieved from http://www.link-labs.com/z-wave-vs-zigbee/

*Miranda, L. (2016, February 11). Internet of Things: Total Control Disguised As Convenience And Status. Retrieved from http://www.thesleuthjournal.com/internet-of-things-total-control-disguised-as-convenience-and-status/

Morgan, J. (2014, May 13). A Simple Explanation Of 'The Internet Of Things'. Retrieved from http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#f5a328768284

Parrish, K. (2015, July 14). Zigbee,Z-Wave,Thread and Wemo: What's the Difference? Retrieved from http://www.tomsguide.com/us/smart-home-wireless-network-primer,news-21085.html

*Roberti, M. (2015, August 16). The Internet of Hacked Things. Retrieved from http://www.rfidjournal.com/articles/view?13372

*Sasso, B. (2015, February 27). Is Washington Ready for the Internet of Things? Retrieved from https://www.nationaljournal.com/tech/2015/02/27/is-washington-ready-internet-things