OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Mini-review

Living in the Future: Designing a Smart-Home with Information Security in Mind

David Brehmer*

Department of Engineering, Cape Fear Community College, East Carolina University, New York, United States

ABSTRACT

Around the world, there has been an increase in the number of IoT devices found in homes. These devices can range from temperature sensors and thermostats to security cameras and entire home security architecture. One study found that 63% of homes in North America had at least one IoT or 'smart-home' device. While the convenience of IoT devices in our homes is a value to the end user, many IoT makers do not prioritize security over convenience in their development life cycle. The development of IoT devices should include information security among the most important milestones to achieve, and one could argue it should be the top priority. In this paper we will discuss the concepts and best practices when developing a smart home and how information security should play a very large role.

Keywords: Internet of Things; Smart home device; Security; Thermostats; Information Technology

INTRODUCTION

In recent years, the technology industry has made advancements that have fundamentally changed the way the world works. Changes in technology have altered businesses, governments, and even personal life far greater than anyone could have dreamed of just a decade ago. We have devices that have the ability to track our heart rate and warn the user of a heart problem and devices that monitor air quality to study the impacts of pollution [1]. There are countless ways these technological advancements have ushered in ground-breaking and world changing devices. These changes range are far reaching, and the impacts are felt by nearly every person on Earth. The devices that have the highest level of impact are the Internet of Things (IoT) products. These products are defined by small, self-contained, always internet connected devices that provide a service to the users. IoT devices can include thermostats, smart watches, cameras, or any other small device that has a connection to other devices [2].

One of the fastest growing sectors in the IoT realm are smart home devices. These devices go beyond a simple thermostat or camera. Perhaps the most notable device is the voice assistance offered by Google, Amazon, Apple, and Samsung. In addition, we also have smart home security systems such as Simply Safe and Abode, smart home sprinkler systems such as Orbit, video surveillance systems such as Ring and Wyze, and entire ecosystems built on Samsung Smartthings or Hubitat. "Globally, there are more than 120 new IoT devices that make a connection to the Internet per second".These devices and systems provide users with a wide range of benefits; however, experts are now sounding the alarm at just how unsafe these devices can actually be.

Unfortunately, the majority of these smart home devices and ecosystems have major security flaws. These flaws can be found in the development lifecycle, the deployment of cloud services, and deployment in a local network. In this paper we will discuss the security vulnerabilities that exist with smart homes and the steps that should be taken to better protect a smart home.

METHODOLOGY

Smart home device development lifecycle

While device manufactures have different methods when developing a smart home device, an area that has historically been among the weakest is the security architecture phase. "Currently, there are no security standards developed for IoT devices." Because security standards do not exist, some

Correspondence to: David Brehmer, Department of Engineering, Cape Fear Community College, East Carolina University, New York, United States, Tel: 9106160790, E-mail: dbrehmer@cfcc.edu

Received: November 10, 2020; **Accepted:** November 25, 2020; **Published:** December 2, 2020

Citation: Brehmer D (2020) Living in the Future: Designing a Smart-Home with Information Security in Mind. J Inform Tech Softw Eng 11:248.

manufactures are more focused on getting the project to completion and less of the security aspect of the device or service [2]. This has become an ongoing issue. For example, Ring, the most popular video doorbell had a vulnerability that allowed attackers to gain access to the clear-text password stored on the Ring itself. The vulnerability existed in the Ring ecosystem for four months before Ring pushed out an update. Another example is the data breech that Wyze disclosed in late 2019. Wyze is a small security camera startup who provides affordable cameras as well as other IoT devices [3]. Their database was stolen by hackers and forced Wyze to make a public statement and request that all users change their credentials. The vulnerability was an internal programmer set up a public facing server without authentication requirements. This allowed hackers to easily find and copy the database. This happened during the maintenance phase of the development lifecycle. These are common mistakes that many product developers make [4]. The most effective way for product developers to implement security in their devices is for global organizations such as IEEE and IEFT along with country level organizations such as NIST, to create a security framework designed specifically for IoT devices and institute regulations for these devices. There are a few organizations attempting to bring security to IoT devices via laws and regulations [4]. NIST released a document titled "Recommendations for IoT Device Manufacturers". This document "describes voluntary, recommended activities related to cyber security that manufacturers should consider performing before their IoT devices are sold to customers." While the NIST document is not an official regulation, it does provide a framework for developers to adhere. California is close to passing an actual law that would mandate certain regulations for IoT developers in their state.

The bill "SB-327 Information privacy: connected devices" is a detailed action plan for manufacturers to follow and requires security to be implemented. This law would be the first in the US if it passes. Rules and regulations are the first step to a more secure smart home. Companies and developers should strive to implement strong security measures in their devices. They should utilize the NIST IoT security framework as well as future IoT security frameworks.

Cloud services

Smart homes are made up of various IoT devices and all of these devices must maintain a connection with each other as well as a connection to the internet. The majority of smart home devices require an always-on internet connection. While this may provide the users with a great deal of convenience, this also comes with its own security threat [5]. Any device that has an always- on internet connection is effectively always a target. In addition to this, many devices not only rely on the internet, their entire ecosystem is ran from a cloud service. For example, the Ring Doorbell does not save video locally to the device or a local server. Instead, it uploads the recorded videos to Rings cloud storage. This puts private data at risk to data leaks or breeches. When data is stored locally, the user has full control of the data and can take measures to protect their private data. However, when a cloud service is used, the ability to control the data is relinquished to the cloud provider [6]. As recent exploits have shown, cloud services are susceptible to hacking. Adobe is another example where improper security infrastructure and practices led to a breech in their cloud services, resulting in 7.5 million user accounts being compromised. Unfortunately, because the end user has little control over how a cloud services implements security, we must rely on Governments and organizations themselves for strong security practices. As with the development lifecycle, the best approach to a more secure cloud is via regulations and international frameworks. Many of the major cloud providers such as Amazon's AWS, Microsoft's Azure, and Google's Cloud are all making great strides in the security of their products [7]. With the number of attacks on the rise in the cloud service sector, these large cloud providers are beginning to show how serious their security culture has become. Microsoft, Amazon and Google have been implementing new encryption techniques and much strong credential storage and are now offering Government compliance certificates. Considering the majority smart home IoT devices utilize the cloud in some fashion, the steps these providers are taking are helping protect the end user.

Local connections

The area where the most attention needs to be given is the local connections. Since most IoT smart home devices require some network connection, we must focus on every aspect of the local network. An important rule to remember is that vulnerability in one device can lead to an exploit in a different device. For example, the Ring vulnerability discussed previously would give the attacker the clear-text wifi password. The attacker can then use that password to connect to the network and attack even more devices. Because of this rule, we must utilize the defense in depth approach. We can achieve this by using different security techniques at different layers of the network, much like an artichoke. By implementing multiple layers of security, we make it increasingly less likely that a single point of vulnerability exists.

The router is the heart of the network. Here is where we can implement the most security. According to Symantec, routers are the most targeted devices. He first step to protecting the router is to change the default password and username. Any seasoned hacker will attempt to log into a router with the default credentials. The next vital step is to update the routers firmware. This will be different for every device but should never be postponed.

Once the basic security of the router is put in place, we must turn to the network. It is recommended that all IoT smart home devices be put into their own virtual private network, not vlan. A vlan is a network created in software that allows a logical separation between individual vlans. For example, in

RESULTS

Figure 1 below, we can see the network on the left has all devices in a single network, while the network on the right has the IoT devices isolated in their own network called Vlan 10 and all other devices in another network called Vlan 20. The reason vlan isolation is a strong security measure is that it gives the user

the ability to create custom firewall rules that can either block or allow certain traffic.

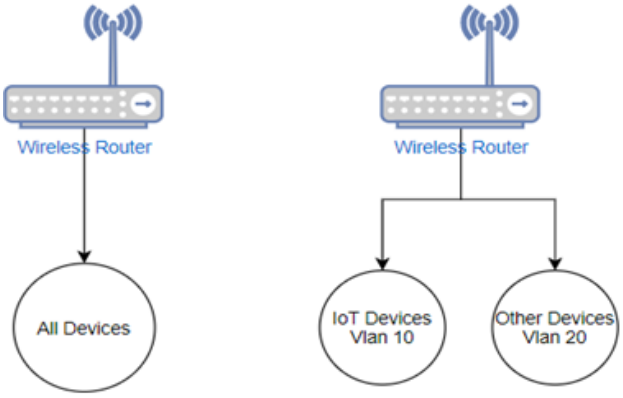

Figure 1: Non-Vlan vs Vlan.

Many IoT devices are low powered, sensor-based products that do not have the ability to upgrade the internal firmware. Some examples of these devices include door locks, temperature sensors, door and window open or close sensors, motion detection sensors, occupancy sensors, humidity sensors, flood sensors, and smoke or carbon monoxide sensors. These devices typically utilize wireless technologies other than WiFi. The most widely used wireless protocols for these devices are Zwave and Zigbee. These two protocols work in a similar fashion. They create a mesh network between all devices. Each device will connect to multiple other devices within a few feet. There is always a central hub that the mesh network connects back to [7]. This hub is then connected to either the WiFi network wirelessly or wired via the ethernet network. The most popular devices that use Zigbee are the Philips Hue Smart Lights, while the most commonly used Zwave hub is the Samsung Smartthings. Both of these platforms' hubs require an always on internet connection to function properly.

There are numerous vulnerabilities in both Zwave and Zigbee. The first version of Zwave, generation 1, sent all network traffic unencrypted. An attacker with an inexpensive Zwave read could intercept a wireless signal sent to the door lock and save it for later [8]. This was a known issue in Zwave and helped force manufacturers to adopt the newer generation 2 Zwave that provides encryption. The problem is that all generation 1 Zwave devices are still compatible with the newer standard. In addition, it is difficult and sometimes impossible to know what generation your device is. Zigbee has also had issue with its protocol in recent years. In February 2020, NIST released the CVE-2020-6007 vulnerability.

Attackers were able to force a Zigbee Hue bulb to flash on and off. If the user attempted to disconnect and reconnect the device in an attempt to fix the issue, the attacker could gain access via a remote code execution to the Philips Hue Hub. Once in the hub, they could pivot to other devices inside the network [8]. While the end user has very little ability to prevent either of these attacks, implementing a vlan would isolate these devices and prevent the pivot attempt by the attacker. They would effectively be stuck in the vlan. As an additional layer of security, creating a firewall rule that block all traffic coming FROM the IoT vlan that is destined TO the other vlan, would add even more security.

Another step that is recommended is to create strong firewall rules that block traffic leaving the local network. Because of the need for internet, IoT devices often need to have access to various cloud based services. As an example, Wyze cameras offer person detection. However, in order to provide this feature, the devices need to use a Software as a Service (SaaS). The service used in this case is located in China. One would need to ask themselves if allowing your camera talk to a server in China is a smart decision. For security reason, a firewall rule dedicated to blocking traffic FROM a Wyze devices DESTINED for China might be used. Having the ability to create fine grained and detailed firewall rules is a large part of securing a smart home properly [9].

While vlans and strong firewall rules are highly recommended, many consumer grade routers simply do not offer these features. The industry is starting to realize the need for these features and are beginning to add them to more and more consumer devices [6]. However, the roll out has been slow. Companies like Asus and Google have been adding these features as selling points for smart homes since 2018 but the rest of the market is still behind. Because of large number of routers without these features, we must find ways to implement security in our smart homes without the help of the router.

Devices

The most important aspect of the smart home is the devices themselves. While every device will have security vulnerabilities, we can take a steps to protect our networks. The most important thing to not is location. A popular way for attackers to access parts of a smart home is via an outdoors device. Ring doorbells, IoT cameras, IoT outdoor lights, and even cars can all connect back to the internal network. Keeping these devices in unreachable places is vital when possible. The next step is to focus on WiFi. The WiFi is the first target of any attack on a smart home. The WiFi password should be very strong and should be the same as any other password. Another security practice is to utilize two factor authentications when possible, especially with smart home cloud accounts such as Google, Ring, Amazon, Philips Hue, and Nest. Two factor authentications provide extra security by requiring the user use a second form of authentication. This can be implemented in various ways with a six to eight digit number being sent to the user's phone by way of sms message.

DISCUSSION AND CONCLUSION

Information technology has been changing the way we live and work for decades. Today, one of the most influential technological changes has come from IoT devices and their implementation into smart homes. Smart homes are becoming more popular than ever and security should be at the forefront of this growth. The steps laid out in this paper are some of the first steps that should be taken to better secure the modern smart home. These steps included strong security in the development lifecycle, better security in the cloud and on the local network, strong home network security practices including

vlans, and improved wifi practices along with two factor authentications. These steps are only a first line of protect and multiple layers should be used. The future is dynamic, and the technology will continue to change. Because of this, it is recommended that users with smart homes stay current with their knowledge in the area of information security as well.

REFERENCES

1. Barsocchi P, Calabrò A, Ferro E, Ferro E, Marchetti E, Vairo C. Boosting a Low-Cost Smart Home Environment with Usage and Access Control Rules. Sensors (Basel). 2018;18(6):1886.
2. Han J, Park T. Security-Enhanced Push Button Configuration for Home Smart Control. Sensors (Basel). 2017;17(6):1334.
3. Nelson BW, Allen NB. Extending the Passive-Sensing Toolbox:Using Smart-Home Technology in Psychological Science. Perspect Psychol Sci. 2018;13(6):718-733.
4. Chung J, Demiris G, Thompson HJ. Ethical Considerations Regarding the Use of Smart Home Technologies for Older Adults: An Integrative Review. Annu Rev Nurs Res. 2016;34:155-581.
5. Hasan S, Valli Kumari V. Generic-distributed framework for cloud services marketplace based on unified ontology. J Adv Res. 2017;8(6):569-576.
6. Perkel JM. Make code accessible with these cloud services Nature. 2019;575(7781): 247-248.
7. Pinheiro A, Dias Canedo E, de Sousa Junior RT, Albuquerque RO, Villalba GLJ, Kim TH. Security Architecture and Protocol for Trust Verifications Regarding the Integrity of Files Stored in Cloud Services. Sensors (Basel). 2018;18(3):753.
8. Risso NA, Neyem A, Benedetto JI, Carrillo MJ, Farías A, Gajardo MJ, et al. A cloud-based mobile system to improve respiratory therapy services at home. J Biomed Inform. 2016;63:45-53.
9. Lin SP, Yang CL, Pi HC, Ho TM. Tourism guide cloud service quality: What actually delights customers? Springerplus. 2016;5(1):1712.