3-2020

How Secure Having IoT Devices in Our Homes?

Debora Estrada

Lo'ai A. Tawalbeh

Robert Vinaja

Scientific Research Publishing

Journal of Information Security, 2020, 11, 81-91
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

How Secure Having IoT Devices in Our Homes?

Debora Estrada, Lo'ai Tawalbeh, Robert Vinaja

Department of Computing and Cyber Security, Texas A&M University, San Antonio, Texas, USA
Email: Ltawalbeh@tamusa.edu

How to cite this paper: Estrada, D., Tawalbeh, L. and Vinaja, R. (2020) How Secure Having IoT Devices in Our Homes? *Journal of Information Security*, **11**, 81-91.
https://doi.org/10.4236/jis.2020.112005

Received: December 7, 2019
Accepted: March 16, 2020
Published: March 19, 2020

Abstract

Nowadays, technology has evolved to be in our daily lives to assist in making our lives easier. We now have technology helping us in our lives at home. Devices used to create our "smart home" have done a great deal in making our lives at home less burdensome, but sadly, these devices have secured our personal lives to be more accessible to outsiders. In this paper, the security of home smart devices and their communication will be researched by using other academic articles to support facts found. The operation of the devices will be discussed along with security risks and future trends on security attacks. The results found will be crucial to knowing exactly how well our own home is protected. After understanding where the risks lie and a demonstration of how hackers can take control of our smart home, solutions will be given to shield ourselves from security attacks. We protect our homes from physical threats by locking doors, but it is time we guard ourselves from cyber threats as well.

Keywords

IoT, Smart Home, Cloud

1. Introduction

Over the years, we can find there has been an over-population of IoT devices compared to the human population. This isn't surprising seeing how in just one person, there are plenty of devices to connect them to create their smart home living. There could be devices to control surveillance (cameras to monitor movement when not at home), ease of living (like turning on lights and TV), the progress tracking of appliances (how much time is left for my washer to be done), and our comfort (playing music or setting reminders). With so many IoT devices connected in our homes, we need to be wary of internet attacks. These attacks could lead to our privacy being compromised and our personal information to be accessed. It is imperative that we "lock the door" to prevent intruders to enter our smart home, but in order to do so, we need to make sure we don't leave any "windows" open.

2. IoT Devices

2.1. What Are IoT Devices?

Internet of Things devices (IoT) have grown to be useful in many ways. We use them in automation, electronics, medical field, military purposes, and in the industry system. In automation, you will find things like "point of sales terminals (PoS), multifunctional peripherals, and devices for storage" [1]. In electronics, cameras, TV's and accessing PDAs remotely are among the main IoT functions used. We will find that devices are needed to monitor and regulate patient's health frequently in the medical field and IoT devices give them the ability to access these functions from a distance. The military will obviously need IoT devices to promote security by using them to monitor and manage their operations. The industry system can "implement sensors and special purpose controllers" with the help of IoT; there are plans to implement the idea of a smart home to a larger scale to create a smart city [2]. IoT devices in a home setting are made of many devices connected to create a web of devices which is your smart home. Hardware tools, Software Technology, Communication Interface, and a smart system are all components of an IoT device [3]. The hardware component is needed to make the "physical objects responsive and [to give] them the capability to retrieve data and respond to instructions. Software technology enables data collection, storage, processing, manipulation, and instructing" between the IoT smart home devices. The entire smart system is controlled by the processes, sensors, connectivity, and people enabling smart applications to provide variety of useful tasks [4].

2.2. Commerzializing the Use of IoT in Our Smart Home

There has been a dramatic increase in the amount of IoT devices used. There are even predictions that by the year 2020, there will be 50 billion IoT devices which is about 7 times the predicted amount of human population around the world [5]. "The latest developments on the IoT field have definitely contributed to the physical connection of an overwhelming number of smart devices, yet we find that the reason behind the IoT device's growth population has grown drastically in the US was for family safety [6]. Now, they can provide us with ease of living. They also provide us with simplifying our daily lives, assisting us with our personal safety, providing us with security, contribute to the feeling of being omnipresent, maintain energy management, implements control to our home appliances, and presents us with entertainment of our choosing. Our smart home devices conveniently relieve us from most of our daily functions. Things like smart appliances help ease our worry of our chores getting done or at least provide us with the ability to control and monitor their progression from afar. The thriving need for smart home systems among us are centralized to the idea that it provides control and convenience [7]. It provides us with the convenience of knowing we could easily monitor our homes and devices within it while also simplifying our lives from bothersome tasks [8]. As mentioned above, there would be a 7× population of IoT devices vs. Human population. With a smart home system in place we could see why this is possible [9]. A smart home user could be sitting in their living room late at night having their security system in place, monitor the activities of someone else (like their pets or children) that are in a different room, check on the progress of their laundry, lower the volume of their television, change the temperature to a comfortable setting, and have control of the lighting in the house. These are 7 tasks that the user could complete all at once due to the efficiency of smart home IoT devices bringing what they promise: control and convenience [10].

2.3. Examples of Smart Home Systems

Some examples of smart home hubs include the Samsung SmartThings, Amazon Echo Dot, and the Google Home. Samsung SmartThings v.3 is the "Best Smart Home Hub" you could buy in the year of 2019. Samsung SmartThings provide you with an easier set-up in its logic and a wide variety of compatible devices for a little under $70. The Amazon Echo Dot and the Google Home are similar in the sense that you can control devices by having them connect to Wi-Fi and operate them using the Alexa and the Google Assistant apps [11]. The differences that lie in the price for an Amazon Echo Dot are now discounted to be $29.99 which granted it the title of being the "Best Budget Smart Home Hub." The Google Home which comes with the Google Assistant allows you to be able to access the Google search database to search for anything, but the price, $99, renders it to be below its competitors [12].

3. Security Issues and Hackings

A major issue with IoT devices lies within its lack of security and privacy in our lives. We use these devices to promote ourselves with ease of living, yet as a side effect, we open the door for others to access our personal lives [13]. These devices were created to benefit our lives, yet in the rush for these devices to be created and sent to the market, it seems we find that the security requirements were not fully implemented in industry specially when it is related to recent technologies such as IoT, Cyber Physical systems, Big Data systems and cloud computing [14]. Different industries like nuclear facilities, steel mills, energy grids, water supplies, hospital, and plenty more have found themselves victims of cyber-attacks due to the IoT devices. In fact, these types of incidents are estimated to increase by 32% in the year of 2020 [6]. Here are a few examples of some vulnerabilities found that affected plenty of people [15].

3.1. Opening Data

According to Reference [16], there was a privacy issue with Fitbit. This wearable technology is used to track health and fitness for their users. It also was able to track your sexual activity. With a Google search string, anyone could have accessed this data [16]. Think about how many marriages would have been compromised if the issue remained oblivious to Fitbit's security team. People could have used this information to build a list of users to blackmail. Even if the users weren't guilty of cheating/fornicating, that was their personal sex life being put on the web for display. IoT users should not have their privacy be compromised in such a way. The companies of IoT devices should take the precautions necessary to avoid such scandals for their users and resolve any potential security threats. In fact, storing any kind of personal data could be detrimental. A company could be hacked and have the information accessed, and this, too, could be used against the users [17].

3.2. Patches and Updates

Jeep Cherokees were found to contain a vulnerability that allowed remote access to brake, accelerate, and steer the vehicle in the year of 2015. Once a company finds a possible threat or breech in security, they need to respond quickly to fix the vulnerabilities, yet we seem to find a lack of patches or updates after the problem is assessed. For instance, the Jeep hacking took ten years to fix. That is way too many years to go by with having a vulnerability exposed. The problem ended up being with the CAN bus. It had three main red flag key points: 1) "the extension from sensors to actuators" had no added security, 2) the CAN bus had no encryption or authentication in the actual device; therefore, hackers could easily attach a device to it to perform attacks, 3) adding a network connection to the CAN bus opened the vehicle up to all kinds of remote attacks [16].

3.3. Radio Transmissions

Another potential threat is among vulnerabilities connected to unencrypted radio transmissions. Theoretically, we can find that hackers can easily drive away with your smart car due to unencrypted radio transmissions. While driving right behind your smart car, they could hack into it to access your tire pressure light to turn on. This could successfully get the user to step out of their vehicle and for the hacker to drive away with it [16].

3.4. Users

Although a security issue may have been fixed, the security of our home devices usually fails due to user error. Most of the time, our computers notify us of the need to update to the latest software, but in cases of updating your coffee maker, the act of updating has gotten harder on users. You will find that in majority of the cases, you would have to connect your devices to your personal computer to access the update to your device. Another concern is that users don't understand the need for their refrigerator to be updated because they don't view it as a computer system. It is important that users view their smart home appliances as

IoT devices which require updates regularly just like any other computer system [16]. Users should be required to change default passwords; we find that out of the 439 million households that have wireless connection, 80% of these households never changed the default passwords [4]. They don't seem to realize that they are at fault of "leaving the window open" for intruders to access their network and connected devices.

4. Interview

We now turn to a professional's opinion over this matter. Dr. Robert Vinaja was previously employed with Aetna health insurance, and he oversaw their database information. Insurance companies have unlimited access to our medical data and require database administrators to process the gathered information. Dr. Vinaja used to say that, "the health insurances companies know more about our health than we know about ourselves," which is similar to the government attempting to build a profile on us using data collected. The interview is titled "Interview over Privacy vs. 'Open Data' of Our Lives," and the bullets would be questions asked with the response indented in the next paragraph.

- How would the insurance company get to know our lives so well? Was there a way to avoid our privacy to be compromised?

  Unlike doctors and family members, HIPPA does not protect our privacy from insurance companies. Any changes or actions that happen to your medical history will always go to your insurance. As soon as you decide to have health insurance, your medical life is open to continuously be monitored by them. If you consider this a breach of privacy, there is no way to avoid it from happening. Unlike other medical personnel with whom you need to sign a consent form, the insurance company automatically is granted the right to learn everything about your medical file especially since they are the ones paying our medical expenses. There is no way around that because every test, procedure, or appointment gets approved by them. They pay the bills, so all paperwork goes to them.
- Did you find benefits to "opening our lives", and if so, what were they? Did you think it was an equal measure to having our privacy compromised to the benefits gained?

  Of course, there were health education programs and hotlines to promote healthy choices and lifestyles, but you could argue its purely selfish reasons because they don't want to pay for hospital bills. The companies build a risk assessment on you based on your health. If you are 70, you're chances of dying is greater than if you were 20; that's a fact. It is based on the results of your assessment of how high your premium will go. When you are a low risk, you pay less, but if you are a high risk it goes up. If it comes up that you have a chronic condition, it goes into the database, and it is shared with other companies. Even if you choose to switch companies, that information collected will go to them. People with preexisting conditions will find it hard to get an insurance to cover their health, or if they do, it would be at an extremely high rate because you cannot hide your medical files when it is openly shared amongst health insurance companies. The benefits are for those who are in good health, but it backfires on those who are high risk.

- Could you see a way for an outsider (hacker or an unauthorized user) to access our personal records for their gain?
  Usually, you see hackers access information needed for financial situations. An example would be them trying to get your date of birth or social security number, but all they could access is medical records and claims within our database. I don't see how they could benefit from that.
- Wouldn't our social security and date of birth be on those records? Is there no way they could access our records and use social engineering to pretend to be a bill collector?
  That's very interesting. You're right they could accomplish that. It's funny that you mention that because the paperwork database is the least secure one. It contains claims, billing information and any related paperwork that isn't part of your medical information. It's the one that requires the least amount of clearance; it's the lowest tier of security, so basically anyone who works there can access that database. Then you have your medical profile database which gives a general idea of your history. At the highest level of security, you will find the detailed report of procedures and tests done or any paperwork that was done by the doctor themselves. I believe this is due to HIPPA that the medical history is the most secure. The government has set regulations about the confidentiality of your records, but the paperwork doesn't have federal requirements as strict as keeping your medical records safe. That scenario of social engineering most definitely could play out, and it would be so easy. Usually if you have a hospital bill pending, or if it is in insurance claims for a while, they will send the bill to collections. Collections are very persistent about you making a payment; they'll even say if you could at least make a payment of some amount of dollars, we'll take of a percentage needed to be paid. A hacker could easily use this method to collect financial gain.
- Do you think it's fair that the government know so much about our lives? Do you agree with allowing our privacy to be compromised for the greater good of having potential crime stopped?
  I couldn't decide that. It's like stopping terrorists or criminals at the border by looking through the cellphones for any suspicious texts or information on there. On one hand, this has allowed the border security team to capture criminals, but for those who have nothing to hide, this is found to be an invasion of their privacy. It's very 50/50 with pros and cons on each side. I could not decide with option to side with.
- Do you feel the government should be regulated over how and what kind of data they can access from our IoT devices, and if so, in what way?
  I know that when it comes to wiretapping to listen in on suspects, they must

have a signed consent from a judge to allow them to invade their privacy in this way. I feel the same law should be incorporated for these devices. They must have a probable cause and a warrant to use these devices for people they suspect will commit a crime. This will regulate the government over how much power they have in order to access information from us without our consent.

5. Solutions

Due to the security vulnerabilities in IoT devices, we will find that, according to Table 2 in Reference [7], losing control of our smart home is a major threat. With a score of 41 in the risk assessment, that gives us a ratio of 2 smart homes finding themselves hacked out of 5. This sort of probability and the fact that the security of IoT devices is faltering daily requires immediate attention to find solutions to protect our homes. The core concepts of security revolve around the idea of CIA+, standing for Confidentiality, Integrity, Availability, Authentication, Access control and Non-Repudiation [16]. These will give us a better idea of what needs to be done with our IoT devices to minimally provide security into our lives.

5.1. Confidentiality

Confidentiality is about ensuring our information stays confidential from others. The most common method is encrypting the messages, so that nobody but the recipient could decipher it. Authors in [5] have proposed a lightweight encryption scheme (LES) which could answer the problem of outsiders accessing the device communication. Their scheme is identity-based, so the public keys are identity strings; it also reuses parts of the cryptographic computations which allows the boosting of computational efficiency [5].

5.2. Integrity

With integrity, the basic idea is that the information created by the original user must remain intact, and unable to be modified by hackers. The idea behind it is that once information is created, it will then be given a hash. Any changes, despite how minor, will create a different hash. The original user must sign the hash, so they can tell when a different hash is produced that the information was modified [16].

5.3. Availability

Next, we have availability. This is ensuring that a "System is running, able to serve its customers, and cannot be brought down" [16]. DoS attacks affect this area of the security principle. They cause systems to lag or in other cases, be brought down entirely by spamming the system with an overflow of traffic.

5.4. Authentication

Behind the idea of Authentication is the need to send our messages to the correct intended users. Most of the time, we find that we allow how hacker to take over by having easy to guess passwords or because we never changed the default password on our IoT system or devices. Certificates and multi-factor authentication can go a long way to help resolve this issue. A certificate is obtained when a third-party has identified you to be the intended user, and a multi-factor authentication's most common way of identifying the correct user is requiring them to type in a code they received on their phone after logging in with credentials [16].

5.5. Access Control

With access control, we will be implementing the idea that only the responsible parties get certain rights and privileges to obtain information or to perform certain actions. The problem with trying to exercise access control with IoT devices is that the common scenario of admin having all rights and distributing permissions to other users according to their function and duties does not turn out to be effective in securing our privacy. Others could still overuse their privileges and access information for themselves because it was granted to them [16]. The other type of access control approach would be to incorporate "policy-based access controls" [16]. This will allow user to access information and perform action only if they meet a certain scenario. A real-world example to demonstrate the principle behind the idea is when doctors can access all our medical files if and only when we are under their medical supervision or when granted permission by the patient themselves. This concept is too specific to use for our IoT smart home devices. There needs to be a middle-ground for these two access control ideas to satisfy the security of our devices.

5.6. Security Conclusion

All these concepts put together would give us a greater form of security for our devices. Although it is true that what we consider secure today will not be secure tomorrow, it is imperative that we at least try finding solutions for these IoT devices to secure our homes for the present. Intruders will get smarter and come up with other ways to get access information, but we shouldn't make it easy for them to find vulnerabilities. We must cover the basics in securing our devices [9].

6. Conclusions

We have found that IoT devices have been rendered useful in many areas of industry including Automation, Medical, Military, Electronic and Industrial. The idea behind home automation has been upscaled to become the hope of having a future smart city. We discussed the main components of IoT devices (hardware, software, communication, and smart system) and how they operate within the device to provide functionality. We also discussed the ease of living these devices provide and how they are operated when incorporated into home living. Common types of smart home systems were discussed and ranked. The security of these devices was assessed and, with examples of previous security and privacy issues, was found to be lacking. Wondering if there could be anything done politically to fix this growing problem, we realize that the government is one reason why the security of these devices has not been fixed yet. The opinions of an IT professional were obtained in interview format with Dr. Robert Vinaja; he had plenty of insight to offer since he had previously worked at Aetna, a medical insurance company. The basics of what makes a device secure were found to include CIA+, which stands for Confidentiality, Integrity, Availability, Authentication, Access-Control, and Non-Repudiation [11]. Once we satisfy the requirements to fulfill those security basics, we can ensure our homes and privacy to be secure.

With all the benefits that the IoT Smart Home devices can offer, we find that they are very vulnerable to attacks especially over the internet. Having an estimate of 2 homes out of 5 being hacked into should bring about a "wake-up call" to users. These statistics contradict the information in Reference [3] that found the reason that the popularity of Smart Home IoT devices was to increase family safety. There is no safety for our privacy since the IoT devices do not satisfy the minimal CIA+ security foundations. With these IoT devices, we are finding that we are forced to do a "trade-off among convenience and control with security and our privacy" [7]. Intruders can invade our privacy, steal personal information, and monitor our actions inside our smart homes, because the idea of having control to manage our homes and for our convenience of lessening tasks needed to do, appeases the general population [7]. The 32% rise of cybersecurity damages for the year of 2020 across industries should move our Homeland Security to put action to the S. 1691 bill to set a minimal Federal standard for security amongst these devices [6] [10]. In respect to the government being behind our compromised privacy, I agree with Dr. Vinaja's opinions. It's understandable they feel they need full reign on all devices to build a profile on us to prevent crime, but I believe their power should be limited to those with probable cause. We should ensure that our homes are closed off to any and every unauthorized user. It is time we put our smart home in a complete lock-down physically and from cyber-attacks.

Acknowledgements

We would like to acknowledge Dr. Robert Vinaja. We appreciate his time, effort and contributions.

This research was supported by Texas A&M University-San Antonio through Research Council Grants.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Dey, N., Hassanien, A.E., Bhatt, C., Ashour, A. and Satapathy, S.C. (2018) Internet of Things and Big Data Analytics toward Next-Generation Intelligence. https://doi.org/10.1007/978-3-319-60435-0

[2] Kang, B., *et al.* (2016) Analysis of Types and Importance of Sensors in Smart Home Services. 2016 *IEEE* 18*th International Conference on High-Performance Computing and Communications*, *IEEE* 14*th International Conference on Smart City*, *and IEEE* 2*nd International Conference on Data Science and Systems*, Sydney, 1388-1389. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0196

[3] Bugeja, J., Jacobsson, A. and Davidsson, P. (2016) On Privacy and Security Challenges in Smart Connected Homes. 2016 *European Intelligence and Security Informatics Conference* (*EISIC*), Uppsala, 172-175. https://doi.org/10.1109/EISIC.2016.044

[4] Cao, K.J., Xu, L., Abdallah, R. and Shi, W. (2017) EdgeOSH: A Home Operating System for Internet of Everything. 2017 *IEEE* 37*th International Conference on Distributed Computing Systems* (*ICDCS*), Atlanta, GA, 1756-1764. https://doi.org/10.1109/ICDCS.2017.325

[5] Salami, S., Baek, J., Salah, K. and Damiani, E. (2016) Lightweight Encryption for Smart Home. 2016 11*th International Conference on Availability*, *Reliability and Security* (*ARES*), Salzburg, Austria, 382-388. https://doi.org/10.1109/ARES.2016.40

[6] Ryoo, J., *et al.* (2017) IoE Security Threats and You. 2017 *International Conference on Software Security and Assurance* (*ICSSA*), Altoona, PA, 13-19. https://doi.org/10.1109/ICSSA.2017.28

[7] Ali, B. and Awad, A.I. (2018) Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors*, **18**, 817. https://doi.org/10.3390/s18030817

[8] Lo'ai, A.T. and Saldamli, G. (2019) Reconsidering Big Data Security and Privacy in Cloud and Mobile Cloud Systems. *Journal of King Saud University-Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2019.05.007

[9] Lo'ai, A.T., Loai, Al-Qassas, R.S., Darwazeh, N.S., Jararweh, Y. and AlDosari, F. (2015) Secure and Efficient Cloud Computing Framework. 2015 *International Conference on Cloud and Autonomic Computing*, Cambridge, MA, 21-25 September 2015, 291-295. https://doi.org/10.1109/ICCAC.2015.45

[10] S.1691-Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S.1691. https://www.congress.gov/bill/115th-congress/senate-bill/1691/text

[11] Bhatt, S., Lo'ai, A.T., Chhetri, P. and Bhatt, P. (2019) Authorizations in Cloud-Based Internet of Things: Current Trends and Use Cases. 2019 4*th International Conference on Fog and Mobile Edge Computing*, Rome, Italy, 10-13 June 2019, 241-246. https://doi.org/10.1109/FMEC.2019.8795309

[12] Prospero, M. (2019) Best Smart Home Hubs of 2019. https://www.tomsguide.com/us/best-smart-home-hubs,review-3200.html

[13] Lo'ai, A.T. and Bakhader, W. (2016) A Mobile Cloud System for Different Useful Applications. 2016 *IEEE* 4*th International Conference on Future Internet of Things and Cloud Workshops*, Vienna, Austria, 22-24 August 2016, 295-298. https://doi.org/10.1109/W-FiCloud.2016.66

[14] Lo'ai, A.T., Jararweh, Y. and Mohammad, A. (2012) An Integrated Radix-4 Modular Divider/Multiplier Hardware Architecture for Cryptographic Applications. *International Arab Journal of Information Technology*, **9**, No. 3.

[15] Tenca, A.F. and Lo'ai, A.T. (2004) Algorithm for Unified Modular Division in GF

(p) and GF (2n) Suitable for Cryptographic Hardware. *Electronics Letters*, **40**, 304-306. https://doi.org/10.1049/el:20040233

[16] Adryan, B., Obermaier, D. and Fremantle, P. (2017) The Technical Foundations of IoT. Artech House.

[17] Mohammad, T. and Eardley, A. (2016) Studying the Energy Consumption in Mobile Devices. *Procedia Computer Science*, **94**, 183-189. https://doi.org/10.1016/j.procs.2016.08.028