A View on Vulnerabilities within IoT Devices in the Smart Home Environment

Annika Nykänen, Andrei Costin

Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, Jyväskylä, 40014 Finland {TODO,ancostin}@jyu.fi https://jyu.fi/it/

Abstract. The number of different devices connected to the Internet is constantly increasing. There is a high demand for these devices, and their benefits are clear for certain groups of users. Some of these devices, the Internet of Things (IoT), are part of smart homes, making the residents' everyday lives easier and safer. In general, the security of IoT devices is constantly improving, but overall, they are still full of vulnerabilities. The purpose of this paper is to explain the most significant threats to IoT devices in the smart home environment and propose a number of different ways to eliminate these threats and vulnerabilities in smart home IoT devices. It is important to acknowledge that both the manufacturers of IoT devices and their users are responsible for taking care of the vulnerabilities.

Keywords: Internet of Things, smart homes, cybersecurity, vulnerability

1 Introduction

Cybersecurity has gained a lot of visibility in recent years compared to before, as the number of information security and cyberattacks is increasing. For example, the number of malware detected annually increased from 100 million to more than 700 million during the years 2012-2017. This means an average of 400,000 new malware every day [17].

The objects to be protected can be anything within cyberspace, for example, the Internet of Things devices of a smart home. The Internet of Things (IoT) refers to devices whose purpose is to connect virtual environments to the physical environment and maintain communication with people [6]. IoT devices are an integral part of a smart home, which consists of various devices connected to the same home network, so-called smart devices, such as smart appliances, smart watches, and smart TVs, and their goal is to make everyday life easier and, for example, make an apartment safer. Because these IoT devices are connected to the Internet, they at risk of becoming or already are vulnerable [11,12], which leads to them being prime targets for IoT specific malware attacks [10] further leading to Internet-wide botnets and attacks [3].

1.1 Motivation and Contribution

According to Wirth [36], Symantec revealed in their study that an average of 5,200 IoT devices per month were under attack. Of these, almost 15 percent were surveillance cameras connected to the network. Thus, security and privacy should be of primary importance in the design of IoT technologies and services. Unfortunately, many commercial IoT products are provided with inadequate, incomplete, or poorly designed security mechanisms [22]. Currently, there is still relatively little research on the cybersecurity vulnerabilities of IoT devices in smart homes, even though the number of these devices has been growing significantly for several years, which means a growing threat to cybersecurity. Therefore, it is vital to increase awareness about the ways to make these devices safer to use.

In this paper, we concentrate on the vulnerabilities of these kinds of IoT devices and suggest several means to increase the safety of these devices. In Section 2, we define the central concepts regarding the vulnerabilities in IoT devices. In Section 3, we present the most common vulnerabilities. In Section 4, we explain possible ways to protect these devices. In Section 5, we summarize the paper.

2 Literature review

2.1 Information Security

The Vocabulary of Comprehensive Security [34], published by The Security Committee and The Terminology Center TSK, defines information security as follows: "Information security means arrangements that aim to ensure the availability, integrity, and confidentiality of information. These arrangements include, for example, access control, data encryption and backup, and the use of a firewall, anti-virus program and certificates."

2.2 Cybersecurity

The Security Committee and The Terminology Center TSK defines [34] cybersecurity as follows: "Cybersecurity is a state in which the threats and risks arising from the cyber operating environment to society's vital functions or other functions dependent on the cyber operating environment are under control. Disruption of the operation of the cyber operating environment is often caused by a realized information security threat, so information security is a key factor when striving for cybersecurity."

2.3 Cybersecurity Vulnerabilities

According to a couple of different definitions, a vulnerability is an error or weakness in a program that an attacker can exploit to gain access to the system [35] or that can cause damage to the system [30].

According to the last definition to be considered, a vulnerability is an opening or weakness in an application that allows an attacker to cause harm to the application's users, the owner, or other parties dependent on the application. The vulnerability described above can be the result of an error during either the design or implementation of the application [27].

For this paper, it is meaningful to look at the last definition presented. Thus, a vulnerability can be thought of as a technical feature that is the result of an application's faulty design.

2.4 Internet of Things

The IoT can be described as devices whose purpose is to shape people's daily lives and completely change the way some tasks work [33].

There is no defined standard for the IoT architecture so far. Previously, the architecture was considered to be three-layered, with a perception, network, and application layer. Following this, researchers also proposed architecture of four and five layers. Each of these layers has its own vulnerabilities and risks [24]. The five-layer architecture is the most common nowadays, so this report examines the structure according to the five-layer model [24].

The first layer, the perception layer, includes all physically identifiable devices. The function of the sensors is to bring into an electronic form information about things that usually are not electronic, such as temperature or air humidity. By combining the data from the sensors, large-scale information can be collected [8].

The second layer is the network layer, which connects the devices of the perception layer to the network. Typical examples of the network layer are the wireless local area network (WLAN), i.e., Wi-Fi and wireless data transfer, such as Bluetooth Low Energy [14]. The advantage of Wi-Fi is its speed, the strength of its range, and the possibility for a large number of devices to be connected to the same network. The strengths of Bluetooth technology are its affordability and its integration into new systems [8].

The third layer in the IoT architecture is the processing layer, which uses many technologies, such as databases and cloud services. On this layer, for example, the TCP/IP protocol that uses packet-based communication is located [5]. IoT-aware process models are used in various execution environments. The requirements of the IoT service must be defined before a suitable IoT process model can be used correctly [5].

The application layer is the fourth layer, and it is responsible for implementing application-specific services for the user. The application layer contains new types of applications for which the IoT is used [32]. This means smart environments, such as traffic, construction, cities, retail stores, factories, and smart homes. The task of the application layer is to structure the received information in such a way that the production of applications for users is concrete and thoughtful [29].

The last layer of the IoT architecture model is the business layer. It ensures that the services structured on the other layers are brought to market. This

includes the entire IT business, such as applications, business revenues, and user privacy protection. Examples of the business layer are big businesses such as Google, Oracle, and Cisco [32]. Each layer must work in line with other layers so that the IoT architecture remains as intact as possible throughout the entire process.

2.5 Smart Homes

A smart home is a technology that enables the control and monitoring of various home devices automatically using advanced technologies [13]. The most common smart home systems include, for example, various lighting systems connected to the network.

As a rule, different beneficiaries can be divided into three different groups according to different needs. The first group is older people or families who have challenges performing everyday tasks such as cleaning. Another group is people with certain incurable diseases. A smart home can, for example, remind a person to take their medication on time and thus reduce the likelihood of medication abuse. The third group is people living alone. Smart home systems can identify situations when a resident is in danger and call for help [7].

However, no technology is perfect, so like any other technical thing, smart homes also have some drawbacks, such as the problem of managing and controlling several different applications and devices [13]. Also, smart home systems are complex systems because they consist of many different devices and different subsystems, which are all connected to each other [21]. Another drawback is that every time the user's needs change, the configuration of the smart home system must be changed [15].

Despite the disadvantages of smart home technology, it is inevitably coming to people's homes to make everyday life easier. It is estimated that in the near future, approximately 90 million people will live in smart homes and use technology to improve home safety, increase comfort, and reduce energy consumption [26].

3 System vulnerabilities in IoT devices

Because a modern smart home environment with IoT technology is connected to the Internet, its attack surface increases considerably. In addition to physical vulnerabilities, devices can be attacked remotely, either through interfaces or by downloading malicious programs to the hardware [18].

Although the smart home as an environment is unique compared to other IoT environments, its vulnerabilities are theoretically very similar. However, a smart home differs from other IoT environments because smart homes are often managed by a private individual. Compared to companies and other legal entities, they do not have the same resources to maintain the data security of the IoT system. [18].

This paper, however, presents vulnerabilities that are not caused by the end user of IoT devices.

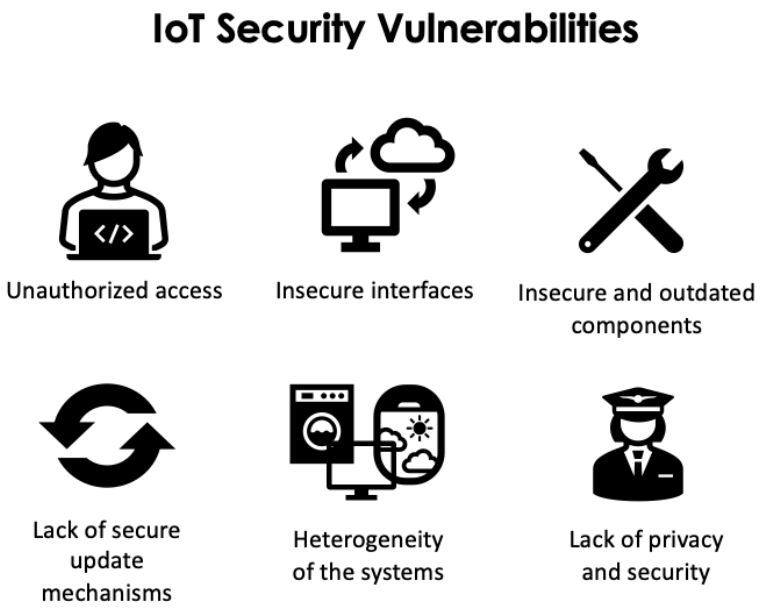

Fig. 1: Summary of the main types of IoT security vulnerabilities.

3.1 Unauthorized Access

In 2018, the Open Worldwide Application Security Project (OWASP) listed weak, guessable, hardcoded passwords, and insufficient authentication as the biggest IoT technology vulnerabilities [28]. In this paper, we will call these unauthorized access.

Unauthorized access can lead to an attacker gaining access to sensitive information [18]. Unauthorized access is aimed at the application level and, in the worst case, can lead to life-threatening situations, such as if an outsider manages to adjust the settings of medical devices or turn on electronic devices when the residents of the smart home are not present.

In addition to the above, the voice command feature increases the risk of unauthorized access. Attackers have been able to create voice commands that are not even audible or comprehensible to the human ear and thus gained unauthorized access to devices [23]. Other vulnerabilities can also indirectly expose the user to unauthorized access.

The risks of unauthorized access would be significantly lower if manufacturers of IoT devices set stricter identification requirements, which would prevent the use of excessively weak passwords [18].

3.2 Insecure Interfaces

IoT communication protocols are not based on cryptographic mechanisms [19], and often, IoT devices use different technical interfaces [20]. Unnecessary or insecure interface services exposed to the Internet may run in the background of the system. Insecure web, backend API, cloud, or mobile interfaces may also exist in the ecosystem outside the device [28].

IoT devices require constant communication with cloud services. The route from the IoT device to the cloud service can be distorted or destroyed, and the flow of data transferred along the route can be blocked. Insecure interfaces and interface services increase that risk and expose devices to information leakage and eavesdropping [19].

3.3 Insecure and Outdated Components

According to OWASP, the use of insecure and outdated components, lack of device management, and insecure default settings are vulnerabilities of the IoT technology [28].

Research also shows that IoT devices often use software with commonly known vulnerabilities; some IoT devices use a reduced version of the Linux OS, which is risky for leaking sensitive information [9].

3.4 Lack of Secure Update Mechanisms

OWASP lists the lack of a secure update mechanism as one of the IoT vulnerabilities [28]. Firmware is vulnerable, as regular software updates are available for only a few devices designed for smart home use. Manufacturers have very little motivation to provide continuous updates to maintain the systems of inexpensive devices. Cybercriminals are constantly finding new vulnerabilities and developing new attack methods, so non-updated devices are more vulnerable to attacks [18].

Because fixed software contains a lot of incomplete data security settings, there is a fair amount of insecure software and incomplete data security settings in IoT smart homes. Naturally, these vulnerabilities increase the risk of a cyberattack and data leakage, which can expose the system to unauthorized access and use.

3.5 Heterogeneous System Within A Smart Home

A smart home is a heterogeneous system and characteristic to it are many types of devices, different connection technologies, applications, and service models [1].

Even though IoT devices are becoming increasingly general, smart home IoT devices are rarely installed in a smart home during the construction phase. Often, the devices also have very little or no documentation about the security mechanisms installed in the internal software [18].

This exposes the smart home to network-level information security vulnerabilities, such as the presence of insecure interfaces, which can lead to equipment and system operation being compromised and information leaking [16].

3.6 Privacy and Security

OWASP lists insufficient privacy protection and insecure data transfer and storage as security vulnerabilities of IoT devices [28].

Many smart homes have sensors that are always on that collect and transport data about users and their movements. Often, the network traffic of a smart home is susceptible to eavesdropping by other parties. Because a large portion of smart home devices do not work without a network connection, data protection and privacy problems cannot be avoided [4].

4 Safe use of IoT devices

As previously stated, IoT devices are usually connected to the Internet. Data security does not depend only on the IoT device itself. It is also affected by other devices and connections. In particular, other devices on the same network can compromise the security of the IoT device. Next, we will review a few examples of how IoT devices can be secured.

4.1 Encryption

It is said that encryption is the most important operation to ensure confidentiality during communication [22]. Even with IoT devices, it is wise to prepare for the possibility that a possible attacker gets the data from the device. With IoT devices, encryption comprehensively secures confidentiality and data privacy, regardless of whether the data is located in cloud or local storage.

4.2 Intrusion Detection Systems

It is vital to be able to detect ongoing attacks in addition to prevent them. For example, anomalies in system parameters may refer to an ongoing attack. [22]. An intrusion detection system provides a solution by which it could be possible to detect anomalies and other malicious events. By preventing ongoing attacks, it could keep all the IoT devices in the same network safe.

4.3 Software Updates

The manufacturers of IoT devices have the main responsibility for the safe operation of the devices. That is because software updates for IoT devices in particular are problematic: Some devices have no update options at all, whereas other devices are too old for new updates. Updates are usually not up to date in cases where the equipment was purchased many years ago, such as a smart refrigerator, whose updates may only be up to date for the first few years. Even if updates for older devices are still available, applying them is challenging. Some devices require users to update the devices themselves, whereas others are automatically installed to download new software updates [4]. One solution could be to create a standard for secure software updates for IoT devices to improve the secure usage of the devices.

4.4 Physical Security

With good physical security of the devices, attacks on the perception layer in particular can be prevented. To improve physical security, equipment components, such as radio frequency, must have a high level of protection [31]. The technical challenges are largely related to information security problems when designing and manufacturing IoT devices. Security should be considered at every architectural layer of the device application. Heterogeneity of IoT devices should be avoided in order to mitigate security threats. To guarantee the safety of the devices, they must be manufactured in compliance with appropriate safety measures [25].

5 Discussion and conclusion

The security of IoT technology is still in the development phase, and although there are already methods to improve it, there are currently not enough resources to implement them in practice.

For this paper, the aim was to find out the most important cybersecurity vulnerabilities of IoT devices in a smart home environment and suggest proper measurements to improve the safe use of IoT devices.

The best way to protect IoT devices from security threats is to only use devices that are sufficiently well protected. Manufacturers should offer better opportunities to maintain IoT devices safely, for example, with automatic software updates. In addition, manufacturers should clearly present what cybersecurity measures have been taken and what updates have been made to the devices. Users, on the other hand, should try to keep their smart homes safe through their own actions, for example, by using strong passwords and two-step authentication. It would also be worthwhile for users to familiarize themselves with the manufacturers of different IoT devices before making purchase decisions.

Using information security products as an aid to protection is probably becoming more common because IoT device users do not always necessarily want or have time to take the necessary protection measures themselves.

Both manufacturers and users are responsible for taking care of the vulnerabilities of smart home IoT devices. However, the low motivation of manufacturers to provide continuous software updates for inexpensive devices is a problem that makes it difficult to implement solutions in practice. Providing updates is inherently expensive, so adding them would also mean an increase in the prices of IoT devices. As long as users prioritize convenience and trust IoT device manufacturers, and stricter data security standards are not mandated by law, few will find it economically viable to manufacture devices with better data security [37]. In future, there should be international frameworks mandating the use of minimum-security standards in heterogeneous IoT devices and applications [2].

5.1 Future research

Currently, there is still relatively little research on the cybersecurity vulnerabilities of IoT devices in smart homes. Although, as technologies, IoT and smart

home are no longer very new, their combination is a subject area that is still in the development stage. In further research, it would therefore be meaningful to investigate methods by which the cybersecurity of IoT smart homes could be improved. Other possible research topics could be how the security of a cheap IoT device differs from that of a device from a trusted manufacturer or the security differences between heterogeneous and homogeneous smart home systems.

References

1. Amadeo, M., Campolo, C., Iera, A., Molinaro, A.: Information centric networking in iot scenarios: The case of a smart home. In: 2015 IEEE International Conference on Communications (ICC). pp. 648–653 (2015)
2. Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., Kumar, N.: Iot vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges. IEEE Access 8, 168825–168853 (2020)
3. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al.: Understanding the mirai botnet. In: 26th {USENIX} security symposium ({USENIX} Security 17). pp. 1093–1110 (2017)
4. Apthorpe, N., Reisman, D., Feamster, N.: A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic (05 2017)
5. Bassi, A., Bauer, M., Fiedler, M., Kramp, T., van Kranenburg, R., Lange, S., Meissner, S.: Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model. Springer Berlin Heidelberg (2013)
6. Borgohain, T., Kumar, U., Sanyal, S.: Survey of security and privacy issues of internet of things (2015)
7. Chan, M., Campo, E., Estève, D., Fourniols, J.Y.: Smart homes — current features and future perspectives. Maturitas 64(2), 90–97 (2009)
8. Collin, J., Saarelainen, A.: Teollinen internet. Talentum (2016)
9. da Costa, L.T., Barros, J.P., Tavares, M.: Vulnerabilities in iot devices for smart home environment. In: International Conference on Information Systems Security and Privacy (2019)
10. Costin, A., Zaddach, J.: Iot malware: Comprehensive survey, analysis framework and case studies
11. Costin, A., Zaddach, J., Francillon, A., Balzarotti, D.: A large-scale analysis of the security of embedded firmwares. In: 23rd {USENIX} Security Symposium ({USENIX} Security 14). pp. 95–110 (2014)
12. Costin, A., Zarras, A., Francillon, A.: Automated dynamic firmware analysis at scale: a case study on embedded web interfaces. In: 11th ACM on Asia Conference on Computer and Communications Security. pp. 437–448 (2016)
13. Gaikwad, P.P., Gabhane, J.P., Golait, S.S.: A survey based on smart homes system using internet-of-things. 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC) pp. 0330–0335 (2015)
14. Giri, A., Dutta, S., Neogy, S., Dahal, K., Pervez, Z.: Internet of things (iot): A survey on architecture, enabling technologies, applications and challenges. In: 1st International Conference on Internet of Things and Machine Learning. IML '17, Association for Computing Machinery, New York, NY, USA (2017)
15. Kadam, M., Mahamuni, P., Parikh, Y.: Smart home system (01 2015)

16. Lee, C., Zappaterra, L., Choi, K., Choi, H.A.: Securing smart home: Technologies, security challenges, and security requirements. In: 2014 IEEE Conference on Communications and Network Security. pp. 67–72 (2014)
17. Lehto, M.: Muuttunut turvallisuustilanne ja uhkakuvat. Jyväskylän yliopisto (2018)
18. Lin, H., Bergmann, N.: Iot privacy and security challenges for smart home environments. Information 7, 44 (07 2016)
19. Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., Fu, X.: Security vulnerabilities of internet of things: A case study of the smart plug system. IEEE Internet of Things Journal 4(6), 1899–1909 (2017)
20. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of things (iot) security: Current status, challenges and prospective measures. In: 10th International Conference for Internet Technology and Secured Transactions (ICITST) (2015)
21. Majumder, S., Aghayi, E., Noferesti, M., Memarzadeh-Tehran, H., Mondal, T., Pang, Z., Deen, M.J.: Smart homes for elderly healthcare-recent advances and research challenges. Sensors 17(11), 2496 (2017)
22. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., Zanella, A.: Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. IEEE Internet of Things Journal 6(5), 8182–8201 (2019)
23. Meng, Y., Zhang, W., Zhu, H., Shen, X.S.: Securing consumer iot in the smart home: Architecture, challenges, and countermeasures. IEEE Wireless Communications 25(6), 53–59 (2018)
24. Mrabet, H., Belguith, S., Alhomoud, A., Jemai, A.: A survey of iot security based on a layered architecture of sensing and data analysis. Sensors 20(13), 3625 (2020)
25. Nguyen Duc, A., Jabangwe, R., Paul, P., Abrahamsson, P.: Security challenges in iot development: a software engineering perspective. pp. 1–5 (05 2017)
26. Oracle: The internet of things: Manage the complexity, seize the opportunity (2014)
27. OWASP: Owasp category: Vulnerability (2016)
28. OWASP: Internet of things (iot) top 10 (2020)
29. Patel, K., Patel, S., Scholar, P., Salazar, C.: Internet of things-iot: Definition, characteristics, architecture, enabling technologies, application & future challenges (2016)
30. Pfleeger, C.P., Pfleeger, S.L., Margulies, J.: Security in Computing (5th Edition). Prentice Hall Press, USA, 5th edn. (2015)
31. Rao, T., Haq, E.: Security challenges facing iot layers and its protective measures. International Journal of Computer Applications 179, 31–35 (03 2018)
32. Sethi, P., Sarangi, S.R.: Internet of things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering 2017 (2017)
33. Tewari, A., Gupta, B.: Security, privacy and trust of different layers in internet-of-things (iots) framework. Future Generation Computer Systems pp. 909–920 (2020)
34. TSK, S.: Kokonaisturvallisuuden sanasto (2017)
35. Wang, J.A., Guo, M., Wang, H., Xia, M., Zhou, L.: Environmental metrics for software security based on a vulnerability ontology. In: 2009 Third IEEE International Conference on Secure Software Integration and Reliability Improvement. pp. 159–168 (2009)
36. Wirth, A.: Cyberinsights: Reviewing today's cyberthreat landscape. Biomedical instrumentation & technology 53(3), 227–231 (2019)
37. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home iot privacy. Proc. ACM Hum.-Comput. Interact. 2(CSCW) (nov 2018)