Security of Smart Home-Smartphones Systems

Diogo Teixeira
Instituto Politécnico de
Viana do Castelo, Portugal
diogoteixeira@ipvc.pt

Leonardo Assunção
Instituto Politécnico de
Viana do Castelo, Portugal
leonardoassuncao@ipvc.pt

Sara Paiva
Instituto Politécnico de
Viana do Castelo, Portugal
sara.paiva@estg.ipvc.pt

Abstract — **With technology increasingly present in people's lives, smart homes are gaining more and more impact each day. While in the past smart homes consisted in presence sensors, cameras and automatic shutters, nowadays they are composed of several sensors and equipment that can control and monitor different things, such as temperature or heat. The homeowners want to control and monitor their home through applications on their smartphone which contributed to the smart homes-smartphones system concept. These are systems that control people's privacy, so various security mechanisms must be implemented to mitigate vulnerabilities. In this paper we present main vulnerabilities of these systems and main proposals to mitigate threats.**

Keywords - Smart-home, Smartphone, Security, Threats, Mitigation, IDS.

I. INTRODUCTION

Nowadays, technology is present in people's lives in several aspects. Studies [1] indicate that worldwide in 2010 there were 1.84 devices connected per inhabitant. However, now in 2020, this number has more than tripled, with 6.58 connected devices per inhabitant, as shown in Figure 1. There are many reasons for the high growth of this number. One of the reasons focuses on smart homes. There are several equipment's placed in a house, thus contributing to the growth of the presented number.

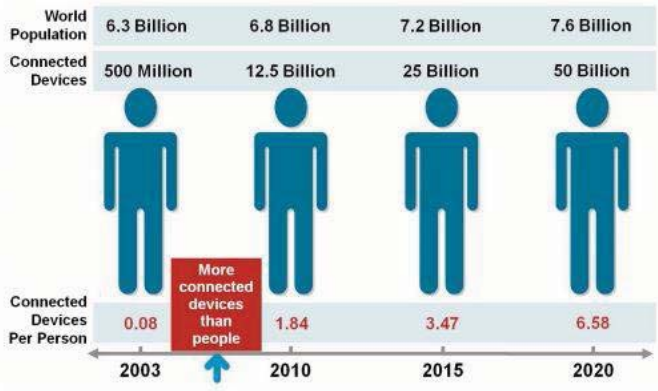

Figure 1. Number of connected devices per person – CISCO – adapted from [1]

At an early stage, smart homes were those homes that had presence sensors, which had cameras to film when they detected movement, or even electric blinds. In practice the goal was to insert technology into homes, and to assist the day-to-day of their owners.

However, in this last few years the concept of smart home has changed. Nowadays, a smart home can control and monitor different parts of the house. A smart home is not just a home with automation because it operates health care, optimizes energy consumption and monitors homeowner's safety [2]. Companies that manufacture the equipment used in a smart home have given their customers the ability to control and monitor their home through mobile phone applications. Thus came the concept of smart home-smartphone system, where the home owner has access to his smart-home through his smartphone.

In different domains, not just smart homes, cyber attacks are becoming more frequent each day. And smart homes are no exception, so these solutions have become a target for hackers. This often exposes system vulnerabilities that could endanger users' privacy. It is important to distinguish the different components of the smart home-smartphone system to understand the different threat points that might exist to hackers to take advantage of them.

Figure 2. Smart Home-Smartphone System Architecture

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

According to Figure 2, the sensors and/or actuators are one of the points of failure of the system. At the same time, the central where all smart-home information is located is another threat point. Opposite, the app and the smartphone where it is installed can also be a problem. Last but not least, communication between all these points is another threat. This system contains information about users' personal lives, their own home, so all data exchanged in it should be completely confidential and transmitted without any infor- mation leakage. Thus, it is necessary to improve the security mechanisms associated with this system. This paper's main contribution is a discussion on system threats, vulnerabilities and mitigation strategies in smart home- smartphone systems.

The rest of this paper is structured in the following way: the next section will introduce the main threats in these systems. Section III will present strategies to mitigate threats. Section IV presents future work and section V presents main conclusions of this work.

II. System Threats

A few years ago, the word crime referred only to acts such as robberies or homicides. We were far from imagining that we would reach the era of cyber-attacks where, through a computer, it would be possible to trigger and contribute to a criminal act. The smart home-smartphone system is, as with happens with so many other systems that involve technology, an excellent target for cyber-attacks. Why? On the one hand, they are becoming more frequent, thus increasing the likelihood of being chosen. On the other hand, being systems that monitor and control a home, they have valuable information that motivate these attacks by hackers with malicious intentions. As a result, several threats have already been associated with these systems, all with the same purpose: to access users' private information. Throughout this section some of the system's discovered and exploited threats will be presented.

A. ***Denial of Service (DoS)***

The Denial of Service (DoS) is one of the most common cyber-attacks. As its name implies it is an attack on a system service to make it unavailable to legitimate users. Usually these attacks cause the system to consume all of its resources such as memory or processing time so that it cannot in any way provide the service for its intended purpose. The authors M. Daud et al [3] demonstrate the effects of a DoS attack on a set of sensors that store their data in the cloud. As shown, with the DoS attack sensors can no longer send their data. This is a major threat at all levels as it is capable of putting the entire system down. With such an attack, all monitoring and management of resources will be impossible, and the house may be at risk.

B. Lack of energy and/or Internet

In smart home-smartphone system power is one of the main aspects, because in case of failure the system will not work. For example, in a smart home with a surveillance system that notifies the homeowner if it detects movement, burglars may cut the power to the home and the homeowner will not be notified. Therefore, system devices must have power reserves, batteries, so they continue to function in case of failure. This is a measure increasingly used by manufacturers thus reducing the impact of the threat. Authors [4] discuss the smart grid for smart homes, bringing together various power supply systems to overcome this type of vulnerability.

However, these systems usually need an internet interface to communicate. In the event of a network failure they will no longer communicate with each other, no longer exchange data, and thus the system will cease to function. In [5], authors refer to the importance that the network (internet) has in a smart home. For example, in the case of a fire detector that communicates through the network to the central to warn the homeowner; if the network fails, it will not be able to communicate and could have devastating consequences. The solution may be redundancy in the network, something not much used so far. After an analysis of the possible implementation cost and the benefit obtained, it was concluded that the advantages obtained do not outweigh the investment. However, so far, no mark has commented on the non-implementation of this solution.

C. Malicious Code Injection

Another very common type of threat is malicious code injection. This threat focuses on someone being able to execute code or scripts on a system through an exploit or vulnerability of a service. This is due to a security hole in the software. Often this type of attack is done via the mobile phone where the house control application is installed. Thus, although there is a security breach in the software, the homeowner has also accessed malicious content. Thus, hackers try to inject malicious code into the smartphone to access the house- controlling application and gain full access, as the authors state in [6]. Once the hacker has access to the application that controls the house, he can do everything, which is a very serious problem for homeowners. The purpose of hackers in this type of attack is to gain privileges, that is, to have unauthorized access to areas of the systems.

D. Software failure

Another problem lies in the failure of the software used in the system equipment. According to [7], there are several vulnerabilities in the software used on the thousands of in-stalled devices. These vulnerabilities could be exploited by hackers, putting the correct functioning of the system and/or the privacy of users in question. The solution may include making updates that will fix the bugs. However, this procedure is very uncommon. Typically, brands launch the product, put it on the market, and leave the update as impossible. With the growth of this market, brands should start to pay more

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

attention to this issue. In other words, it will be necessary to provide software support for a few years and allow the equipment to be able to update.

E. Confidential Data Leakage

The smart home-smartphone system control and monitor a home, so the user privacy is essential. Typically, the home-owners access system equipment through applications on their smartphone. Therefore, it is essential that the communication between the system and the mobile phone is extremely secure, otherwise, privacy of data may be lost. Many times, these systems use very simple encryption mechanisms, making it easy for hackers to intercept communication. A. Gamundani et al. [8] explain how there are several threats in the field of authentication. They explain how no encryption (clear text passwords), allowing weak passwords, or using weak and vulnerable encryption mechanisms will make the hacker's job easier. Again, it will be essential for brands to pay attention to how they protect their data and implement security mechanisms.

F. Man in the Middle

Another type of threat for smart home-smartphone system is named "man in the middle". In this type of attack, as its name implies, the hacker puts himself in the middle of communication with different goals. Basically, it stands between the user and the system so that all data passes through it. Thus, system data is sent to the man in the middle, and it forwards it without any changes to the user. This way the hacker has access to all information without anyone detecting. On the other hand, it can also be placed in the middle of communication, but with the purpose of tampering with the data. For example, the system central may send an alert informing you that it has detected movement. However, the man in the middle "nullifies" this warning and the homeowner continues to receive the information that everything is OK. Authors in [9] demonstrate a man in the middle attack by exploiting an HTTP protocol vulnerability and the consequences the attack could have. Good communication protocols are important to ensure that information is exchanged between the system and the user without any kind of interception.

The mentioned threats target different points in the system. At the same time, the responsibility for the threat is not always only from the system provider. On the other hand, not all threats have the same consequences. Thus, we present in Table I the comparison of the above-mentioned threats, regarding their target, who takes the main responsibility and main impacts.

TABLE I. COMPARISON OF THREATS

Threats	Target	Responsibility (Manufacturer or client)	Impacts
DoS	Application or sensors	Both	System availability; Data corruption
Software failure	Application or sensors	Manufacturer	System availability; Data corruption; Disclosure, theft and loss of information;
Confidential data leakage	Application or sensors	Both	Theft, loss of information; Data destruction; Illegal usage;
Code injection	Application	Both	Elevation of privilege; Disclosure, theft and loss of information;
Lack energy and/or network	Sensors or network	Both	Data corruption; Denial of use system availability
Man in middle	Network	Both	Disclosure of information; Theft, loss of information; Denial of use;

As can be seen from Table I there may be points of failure in all parts of the system with different responsibilities. Thus, all stakeholders have an obligation to work towards greater system security.

III. MITIGATE THREATS

As shown in the previous section, there are several threats associated with smart home-smartphone systems. Throughout this section, we will present ways to mitigate most common threats in these systems.

*A. **Education***

As children are taught to read, do math's, paint, it will also be essential, in this new era of technology, to begin educating them for the cyber physical world. If people are not alerted, they will be easy prey for hackers. Only this level of education, they will not enter their own name, date of birth or nickname as a password. Only this way they will change credentials and never leave default ones. Only then they will

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

be careful about open networks that connect and files that open. It's normal for many people to be unaware of the evil that may exist in this world. From the perspective of many people it is impossible for a password to be discovered. For others, an open network is an offer, not a threat. Downloading a file that don't even know what it is will never cause problems because for many people all files are reliable. These are just a few examples that demonstrate the perspective of some people in this world and the consequences of lack of education for cyber-attacks. Thus, it is essential to educate people, to teach them to live in this technological world [10]. With education, many threats will disappear, and less data will be lost. In parallel, people should be educated on how to use devices. Not only from the software standpoint to know the purpose of each feature, but also from the hardware to know the best way to use it. In other words, do not tamper with configurations without knowledge and open a door for the hacker, nor think that the equipment is for war. According to cyber security incident reports [11], since 2016, successful attack rates have been over 75%, as can be seen in Figure 3. According to them, more than 50% of the attacks result in losses of over $500,000. Unfortunately, however, these values are not yet sufficient for countries to start investing in cyber security, particularly in school training

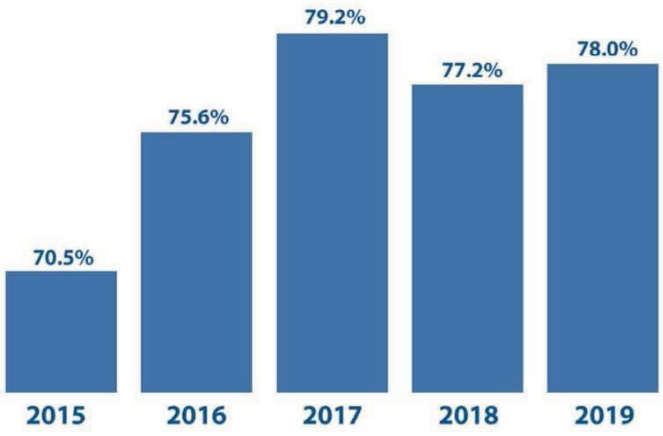

Figure 3. Frequency of successful attacks by year – adapted from [11]

B. Software

The different devices of smart home-smartphone system have software installed. Therefore, companies that develop this software as well as smartphone applications should protect them from malicious attacks. There are different aspects that are essential to increase the security of these systems. It is essential to use strong and secure encryption. That is, an encryption key that cannot be cracked in a timely manner. Thus, during packet exchange in communication it will not be possible to decipher them. This increases the security of system data. In the field of authentication, it must be extremely secure, for example, requiring two-factor authentication. With strong and secure authentication mechanisms, it will be more complex to overcome this first barrier. This is a very important point because if it is vulnerable, hackers can gain access to the entire system. On the other hand, software should have maximum protection against malicious code. In other words, safe code that does not allow malicious code to execute. This way hackers will not be able to damage the system or gain privileges.

The companies that develop the products so far, devel- oped the product, launch to the market and the cycle ended. However, changing the paradigm is essential. Firstly, during development they should think about safety. Then, prior to launch, they must do several tests to ensure they meet the requirements. Finally, upon release, if vulnerabilities arise, they should seek to release updates to mitigate threats. It is essential that these measures begin to increase the security of its users.

C. Hardware

In this field of mitigation, brands should seek to build devices that can withstand some more adverse conditions and more robust. However, once again, education is needed, and people are aware of where and how they use the devices. Although brands must have devices with some rigidity, these devices are not supposed to be used in warfare. Therefore, if users do not want the equipment to stop working due to misuse, they must be careful and use common sense. In parallel, it will also be important for brands to pay attention to the processing capacity of their equipment. Therefore, it will be good practice to improve processing capabilities so that they can use stronger and more secure encryption keys. This will increase data security.

D. Network

Smart home-smartphone systems use several devices that communicate with each other over the network. Most attacks on this system use the network to achieve their goal. Thus, there should be network monitoring mechanisms working in parallel to detect possible attacks, possible malicious code to be injected, i.e. some kind of threat.

IV. Future Work

In the previous chapter we presented some ways to mitigate threats in the smart home-smartphone systems. However, with evolution new threats will arise and will have to be mitigated. There is a long way to go in this area. While, as noted earlier, educating people in the physical cyber world is essential, we believe that creating an Intrusion Detection System (IDS) is very important. Such a proposal and implementation will be part of our future work. Creating an IDS capable of analyzing all exchanged packets in the system, interpreting possible attacks and preventing them. Parallel monitoring that protected the system and would increase user safety. The IDS system will constantly monitor the smart-home network to detect possible intrusions and/or abnormal activities. This system is yet another "firewall help" add-on that performs

ISBN: 978-989-54659-0-3

preventive measures that are actively updated. Likewise, alerts can be configured, and reports of threats found on the network can be obtained. The set of rules used can be customized to accommodate network needs. Thus, the system is able, through customization, to monitor external threats as well as threats operating within the system. Additionally, it has a vast array of scans such as rootkits, system checks, open port scans and more.

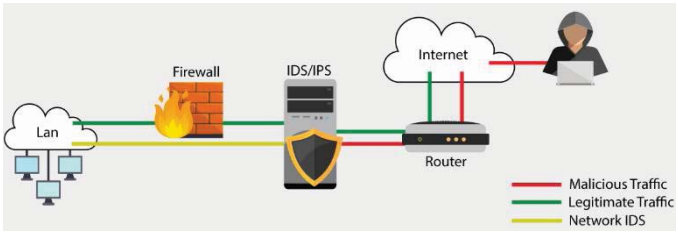

Figure 4. Intrusion Detection System

Thus, whenever the system detects a brute force attack it will block the source of the attack (IP) preventing the hacker from further trying to discover the password. Also, detecting a malicious file could remove it and alert the homeowner. As can be seen in Figure 4, malicious traffic blocked by IDS does not access the internal network, thus protecting devices. An IDS will help the homeowner keep their data protected and their network more reliable.

V. CONCLUSION

The smart home-smartphone system is increasingly present and will continue to grow. At the same time, these systems will inevitably be a part of smart cities. All this constant evolution must be accompanied by strong security. In this paper, we referred to the smart home-smartphone systems, their main threats (such as denial of service, lack of energy and/or internet, malicious code injection, software failure, confidential data leakage and man in the middle) and also mitigation strategies (education, software, hardware and network changes needed). We also presented, as part of our future work, an initial description of an intrusion detection system solution and its main functionalities that represent another way to mitigate the majority of threats in a smart-home smartphone system. In addition to IDSs, it will be essential for people to be educated in this world of technology and to be careful about their smartphones, their credentials, etc. However, it will also be mandatory for companies that create these systems to develop more secure systems, in other words, that are concerned with data encryption, with data authenticity.

Every day new challenges will emerge. However, with everyone's work, these systems will be more secure and efficient in the future. Thus, user data will be placed first and privacy will not be lost. Security for everyone.

REFERENCES

[1] D. Evans, "The Internet of Things - How the Next Evolution of the Internet is Changing Everything", Cisco, April 2011.

[2] K. Karimi, and S. Krit, "Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges", 2019 International Conference of Computer Science and Renewable Energies, August 2019.

[3] M. Daud, R. Rasiah, M. George, D. Asirvatham, A. Rahman, and A. Halim, "Denial of Service: (DoS) Impact on Sensors", 4th IEEE International Conference on Information Management, June 2018.

[4] A. Tascikaraoglu, M. Uzunoglu, M. Tanrioven, A. Boynuegri, and O. Elma, "Smart Grid-Ready Concept of a Smart Home Prototype: A Demonstration Project in YTU", 4th International Conference on Power Engineering, Energy and Electrical Drives, October 2013.

[5] R. Kashyap, M. Azman, and J. Panicker, "Ubiquitous Mesh: A Wireless Mesh Network for IoT Systems in Smart Homes and Smart Cities", IEEE International Conference on Electrical, Computer and Communication Technologies, October 2019.

[6] O. Nisha, and S. Bhanu, "A survey on Code Injection Attacks in Mobile Cloud Computing Environment", 2018 8th International Conference on Cloud Computing, Data Science and Engineering, January 2018.

[7] A. Simpson, F. Roesner, and T. Konho, "Securing Vulnerable Home IoT Devices with an In-Hub Security Manager", 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, May 2017.

[8] A. Gamundani, A. Phillips, and H. Muyingi, "An overview of potential authentication threats and attacks on Internet of Things(IoT): A focus on Smart home applications.", 2018 IEEE International Conference on Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), June 2019.

[9] P. Patni, K. Iyer, R. Sarode, A. Mali, and A. Nimkar, "Man-in-the-middle attack in HTTP/2", 2017 International Conference on Intelligent Computing and Control, March 2018.

[10] S. Choi, and T. Kim, "Understanding Factors Affecting Information Security Practice of Elementary School Students", 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, December 2016.

[11] "Cyber Security & Cyber Crime Statistics" [Online]. Available: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

ISBN: 978-989-54659-0-3