Good practice guide around the security of the internet of things in smart homes

L M Sánchez-Pérez, T Velásquez-Pérez, and J C Camargo-Pérez

1 Grupo de Investigación en Tecnología y Desarrollo en Ingenierías, Universidad Francisco de Paula Santander, Seccional Ocaña, Colombia

E-mail: lmperezs@ufpso.edu.co, tvelasquezp@ufpso.edu.co

Abstract. This article presents a guide to good practices around internet safety of things for devices that get involved with smart homes. It is chosen to use a quantitative methodology of descriptive approach, taking into account that it is a topic that is in incursion and it is necessary to begin to establish the elements that are going to incorporate in the guide. The starting point is a study of the internet layers of things, the open web application security project and the components that make up the guide. This research allows to make a contribution with an analysis of the future of the internet of things and to expose the considerations on the security that involve these devices, taking as guide the tools, documents and information that the project proposes for the development of systems of high quality in security.

1. Introduction

The smart house is understood as a home based on technology that responds to the comfort that its inhabitants demand today, giving the concept of sustainability not only as an environmental significance but an economic notion, and proposing a model that can be extended to other areas of citizen relationship [1], is called smart houses because it is a house with an architectural design and advanced technology that allows people or families to stay inside them and at the same time feel safe, relaxed and satisfied.

Information and communication technologies have become an indispensable tool for the exchange of information international telecommunications union (ITU) ministry of science and technology, the convergence of television, telephony, messaging services among others towards a single network of communications makes the Internet a fundamental part of our daily lives. The internet of things is a technological innovation that will allow us to transform all our objects into “smart-objects”. All the things that surround us will be networked transmitting and receiving information to make life easier and make it more efficient, whether in energy consumption, in financial management and even in the use of our time [2].

The internet of things is increasingly becoming a ubiquitous computer service, requiring huge volumes of storage and data processing [3]. So far, we have seen how the phenomenon of the Internet of Things has broken around us, giving life to everyday objects that are interconnected thanks to the Internet and constitute inexhaustible sources of information [4].

In the internet of things, each application is based on its own technology of the information and communication (ICT) infrastructure and dedicated devices, these devices do not share any characteristics for the management of services and networks, which increases costs. Smart cities seek a flexible and horizontal approach, in which the common operating platform will manage the network and services, which will allow a wide range of data sources to be abstracted to allow applications to function
properly, they will no longer work in isolation, but will share elements of infrastructure, environment, network, and a common services platform. The Internet of things refers to the ubiquitous presence of electronic sensors in devices such as smartphones, vehicles, household appliances, home security systems, health care devices and fitness monitors. These sensor-based devices generate detailed information about people involved in daily activities [2].

Security, privacy and information protection are the fundamental concerns of the devices manufacturers for the Internet of Things (IoT), as there is no high degree of reliability with respect to security standards, a low level of security is clearly unacceptable for home services in terms of safety and health of people. For example, when we leave for some time, unnecessary services such as air conditioning, lights, gas and other appliances will be put on standby or turned off to save energy and protect the security of the house, however, attackers can send maliciously from abroad many false requests to a specific device or service in the cloud, so it seriously threatens the security of housing [3].

2. Methodology
The development of this project was based on a descriptive methodology of quantitative cut based on the grounded theory, in which from the documentary analysis the best IoT security practices for Smart House can be established, taking into account the elements and barriers present in the IoT.

Therefore, this methodology consists in characterizing a specific phenomenon or situation indicating its most peculiar or differential features. This type of research seeks to specify and categorize each of the elements and strategies according to security in IoT devices [5]. Descriptive research “includes the description, registration, analysis and interpretation of the current nature, composition or processes of the phenomena,” According to Sampieri, quantitative research involves a process; deductive, sequential, probative and analyzes an objective reality [6].

3. Results
Security is one of the problems that cause greater relevance in the companies responsible for designing electronic, technological, and mobile devices currently, with the implementation of the IoT, these problems have become even more significant since it is necessary to offer client information security. Therefore, it is necessary to clearly identify the IoT components, the security schemes for the IoT environment, analysis of the components of the scheme and at the same time identify the security scheme of an IoT device [6-12].

The main features presented by the intelligent objects (IO) are directly linked to the design of innovative applications, in which heterogeneity and scalability are included are of vital importance in complex and dynamic systems such as IO, to address these issues they propose that the solution is to look in the architecture sector at the name / identification / address level, to level of assignment of name / object code that will allow the analysis of the aforementioned in order to offer devices with a greater degree of scalability, on the other hand, the fact that starting to minimize objects helps greatly in optimizing operating costs (development, installation, maintenance, materials [2].

Among the main characteristics of the IO, it is that the objects must offer capacities of self-degree of configuration autonomy, self-organization and self-adaptation, auto-reaction to the events and stimuli to which the objects are subjected and auto processing of the amount of data exchanged by third parties. The IO must ensure a secure environment in terms of security of communication / authentication and integrity of data and devices, the privacy of users and personal data, and the reliability of the environment and the parties involved [2].

The characteristics of different underlying networks, addressing modes, mass transmission of devices, high reliability, improved access priority, route selection, mobility, low power consumption, notification and interaction, traffic profile, time-dependent traffic, support of location reports and secure connections, they seek to solve the security problems faced by the devices being the communication one of the main sources of attack, it is for this reason that the credentials or the configuration of the same are sought they are robust, that is to say that they are not compromised to network attacks (hacking and denial of service), thus ensuring the integrity of communications, it is a clear example of being able to
guarantee security, in the following image you can see some of the solutions to improve communications security [2]. The layers related to IoT are perception layer for the identification of objects, network layer for the transmission of data obtained from the previous layer, middle level layer responsible for guaranteeing the same type of service between the connected physical objects and the layer of application responsible for IoT applications from the most diverse types of industries, such as smart hospital, smart city, Smart transportation, among others [7]. Among the main features of the IO, security is essential, since they can be produced at different levels, investing in technology as well as in ethical and security aspects. These security issues are of vital importance as it seeks to guarantee the security of data, services and the entire IO system, in all this a series of properties are presented as; confidentiality, integrity, authentication, authorization, non-repudiation, availability and privacy must be guaranteed to offer highly secure devices [8].

Providing security in IoT scenarios is a challenge, mainly due to a huge amount of heterogeneous devices globally accessible via insecure connections. Security issues are extended from confidentiality, authenticity and integrity of end-to-end communications to network aspects, such as authenticity and integrity of devices, and networks. By fact, hackers may use IoT devices as attack platforms to perform distributed denial-of-service (DDoS) attacks. For instance, in 2014 Proofpoint researchers discovered an IoT cyber-attack, where home appliances like TVs, and a refrigerator, sent malicious email spam. Thingbots were created in order to compromise things. Finally, privacy issues emerge as more complicated to be fixed, since devices in IoT networks may be associated with persons [9].

The OWASP Internet of Things project started in 2014, as a way to help developers make better decisions regarding the creation and use of IoT systems. This continues with the 2018 version of OWASP IoT top 10, which shows developers the ten things to avoid when designing, creating, developing, implementing and managing on IoT systems. This project seeks to solve most of the risks and vulnerabilities to which IoT devices are exposed, for this reason it proposes a unique guide that addresses the problems of highest priority for manufacturers, companies and consumers [10]. Below is the top 10 of the IoT that helps developers and designers of devices to take into account the vulnerabilities to which IoT devices are exposed. The future of the IoT of the top 10 of OWASP IoT, includes a series of activities and topics that will allow to develop planning the processes that will give significant improvements to the project in the future [10], some of the topics are: continue improving the list in a two-year cadence, incorporating comments from the community and taxpayers of additional projects to ensure that we keep up with the issues facing the industry.

The IoT OWASP project provides developers with a safety guide, which will allow to evaluate the level of security in which the IoT systems are located. The following tests based on the OWASP project are a guide of great importance that allows measuring the maturity in terms of the security of these systems developed by organizations, the OWASP IoT project works with 10 categories, each category is composed of a series of considerations to take into account, for the degree project it was worked in such a way that it could measure the degree of compliance for each category where there will be two compliance options that are as follows 1 = compliance, 0 = no compliance.

For the realization of this test it is important to have an inventory of software and hardware it is essential to identify the elements or devices that are available and which are working on the system that is being developed or developed; it is proposed that the devices be evaluated independently, in the same way it is also recommended that they be evaluated as a whole, that is, after the installation process, perform the tests together.

As an example, an IoT smart house system is evaluated only to understand how to work with the tests, once the considerations were evaluated, a total score was obtained for each category, this result can be evidenced in the graph that is presented in the Table 1 and Figure 1.

The graph shows the level of compliance of the categories within the evaluation made, where the category of insecure cloud interface obtained a positive value since it is complying with all the considerations that are exposed for that category, for the category insecure mobile interface in the example was the one that obtained the least compliance regarding the considerations, which entails implementing a series of vulnerability controls detected.
It is necessary to appropriately enforce trust management and security in the IoT world starting from the characterization of the different threats related to each specific level of the general IoT system model [11].

Table 1. Evaluation of IoT smart house systems.

| Categories                                      | Value obtained |
|------------------------------------------------|----------------|
| I1: Insecure web interface                      | 6              |
| I10: Bad physical security                      | 4              |
| I2: Insufficient authentication/authorization   | 3              |
| I3: Unsafe network services                     | 2              |
| I4: Lack of transport encryption                | 3              |
| I5: Privacy issues                              | 4              |
| I6: Unsafe cloud interface                      | 9              |
| I7: Unsafe mobile interface                     | 3              |
| I8: Insufficient security configurability       | 4              |
| I9: Insecure software/firmware                  | 3              |

Figure 1. Evaluation result of IoT smart house systems.

4. Conclusions
It was possible to document all the necessary information to be able to identify the layers of the IoT necessary to carry out the design of the guide of good practices, through the collection, compilation and organization of all the information pertaining to the IoT. When inquiring about the IoT OWASP project, and it was taken as the basis for the design of the guide, taking into account the frameworks presented by the OWASP Top 10 IoT, in which 10 frameworks are presented to make the respective recommendations that the creators, designers, developers and analysts of IoT devices, based on this information, an easy to understand guide is designed, so that IoT system developers can follow the necessary frameworks, for improvements in security and vulnerability of IoT systems.

References
[1] Quesada S, Pulido A L 2012 Smart city: Hacia un nuevo paradigma en el modelo de ciudad (Málaga: Universidad de Sevilla)
[2] Borgia E 2014 The internet of things vision: Key features applications and open issues Computer Communications 54 1-31
[3] Chen N, Yang Y, Li J, Zhang T 2017 A fog-based service enablement architecture for cross-domain IoT applications (Santa clara: IEEE)
[4] Barkinter 2011 *The internet of things in a connected world of smart objects executive summary* (España: Fundación Innovación Bankinter)

[5] Hernandez Sampieri R 2017 *Metodología de la investigación, 6ta edición* (México: Mcgraw-Hill)

[6] Sampieri R, Fernández Collado C, Baptista Lucio M P 2010 *Metodología de la investigación* (México: Mcgraw-Hill)

[7] Perez N B, Bustos M A, Berón M, Rangel Henriques P 2018 *Análisis sistemático de la seguridad en internet of things* (Argentina: Universidad Nacional de la Plata)

[8] Dahlan N D, Berardi U, Hoseini A, Ghaffarian A, Makaremi N 2013 *The essence of future smart houses: From embedding ICT to adapting to sustainability principles* *Renewable and Sustainable Energy Reviews* 24 593

[9] Giuliano R, Mazzenga F, Neri A, Vegni A M 2017 Security access protocols in IoT capillary networks *IEEE Internet of Things Journal* 4(3) 645

[10] Miesssler D, Smith C 2018 *OWASP internet of things project* (USA: The OWASP Foundation)

[11] Pasquale M F, Aloi G, Fortino G 2018 Evaluating critical security issues of the IoT world: Present and future challenges *IEEE Internet of things journal* 5(4) 2483

[12] Salazar J, Silvestre S 2016 *Internet de las cosas* (Praga: Techpedia)