Security in smart objects, a general view at the physical and logical level

fgcuzme@utn.edu.ec
walter.zambrano@fci.edu.ec
wilner.cuenca@fci.edu.ec
cmoreira@espam.edu.ec
edison.almeida@live.uleam.edu.ec

Fabián Cuzme-Rodríguez[1], Walter Zambrano-Romero[2], Cesar Moreira-Zambrano[3], Edison Almeida-Zambrano[4] and Wilner Cuenca Álaba[5]
[1]Universaidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas, Carrera de Telecomunicaciones, Av. 17 de Julio y General José María Córdova, Ecuador, Ibarra,
[2]Universidad Técnica de Manabí, [3]Escuela Superior Politécnica Agropecuaria de Manabí MFL,
[4]Universidad Laica Eloy Alfaro de Manabí,
fgcuzme@utn.edu.ec, {walter.zambrano, wilner.cuenca}@fci.edu.ec, cmoreira@espam.edu.ec, edison.almeida@live.uleam.edu.ec

ABSTRACT

In this research we addressed an issue of big importance with regard to information and computer science security. Within this area, we know that security is framed within the confidentiality, integrity and availability (CIA) triangle, which refers to confidentiality, integrity and availability of information or objects connected to the Internet, a subject that should be treated with great awareness. We live in an interconnected world where most of devices at home, businesses, industries, organizations, and cities are connected to the Internet. Within that environment, these objects are fulfilling some functionality that facilitates the lives of each individual, although making them somehow dependent on this technology with a high degree of risk to which they are exposed. This study aimed to explain and demonstrate that most of electronic devices or intelligent objects that are developed, locally or overseas, do not have a proper design with regard to making information security a first priority, then, proposing a guiding scheme that allows an adequate development cycle of intelligent objects. The study concluded that we are not 100% safe, as well as cyber-attacks will continue to evolve, so the conception of information security will have to evolve as well.

Keywords: cyber-attack, intelligent object, interconnected, information security, IT security.

Introduction

Information security dates back to ancient times when information was encrypted so that if it were intercepted it would be difficult to understand, but, with the advancement of technology, these traditional methods of security had to be changed to make them more secure, due to hackers who wanted to obtain information or access information systems used the vulnerabilities found in connected environments, both in hardware and software.

When talking about safety in objects, we must settle the following question: What is an object? According to the [1], an object is considered as a thing that defines it as "Inanimate object, as opposed to living being.", so it is important to state that once components such as: sensors or actuators, connectivity, information collection platform, the Internet and the interface to display information are added, we would no longer have an inanimate object, but a device that interacts through the aforementioned components to perform some specific activity for which it was designed [2].

It is important to note that we can find some terms about smart objects that are discussed in this research, one of them is IoT (Internet of Things), a term introduced by Kevin Ashton in 2009, Professor at MIT at that time, [3], although according to Ashton the term was already spoken internally in research groups since 1999. [4], refers to a Verizon publication that pointed out that social networking technologies, as well as the exponential growth of internet applications and services, will lead to the development of the next generation of internet services that will be pervasive, ubiquitous and will affect all aspects of our lives. The number of IoT devices is expected to reach more than 50 billion by 2020.

It is imperative to include the term IoT, since we can associate it with objects or things, where we can give a specific functionality to a simple object to turn it into a device with added value, even more, we can aim solutions to areas such as medicine, industries, sports, education, leisure, work, among others, where each one contributes significantly to people´s daily basis. However, here comes another question: How safe is our private information?

Pacheco & Hariri, 2016, also states that integration of physical and cybernetic systems, as well as human behaviors and interactions (for instance, producers, consumers, and

attackers) will drastically increase the vulnerability and the attack surface of ecosystems of interdependent infrastructure. Smart homes and smart buildings, common architectures that for a long time were isolated, are now being added supervisory control and data acquisition (SCADA) systems. Where these infrastructures are easy targets for cybercriminals, since their structures are not designed to be connected to the Internet, as was the case with the Stuxnet attack [5].

Enrique Mafla, expert in computer security, argues that there are no secure computer systems. "They have even hacked into the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI)," cited by [6], [7], this sets the guidelines that we should not only worry about business environments, where security is treated in a special way, but also to be aware that every day a large number of devices go to market with added functionalities, among the most important it is connectivity and monitoring using an internet connection.

It is important to consider the security of information in accordance with the CIA triangle, that includes three terms: confidentiality, integrity and availability. Where confidentiality refers to give access to authorized user only; integrity is both information and systems are kept intact, that is, without alterations or modifications; and finally, availability states that information and systems remain available at the time they are required [8], [9].

1 Materials and methods

This section addresses the issue of intelligent objects at a physical and logical level, based on a bibliographic research, bearing in mind developments carried out especially within electronics and communication engineering, in addition a specific analysis of physical levels of design and location of the devices where its operation was proposed, as well as at the logical level that corresponds to the functionality of the software that allows the operation of the device.

[4]but it will also interconnect smart buildings, homes, and cities, as well as electrical grids, gas, and water networks, automobiles, airplanes, etc. IoT will lead to the development of a wide range of advanced information services that need to be processed in real-Time and require data centers with large storage and computing power. The integration of IoT with Cloud and Fog Computing can bring not only the required computational power and storage capacity, but they enable IoT services to be pervasive, cost-effective, and can be accessed from anywhere using any device (mobile or stationary, refers to the security framework that shows all levels that should be considered in the infrastructure, as shown in Fig. 1, but it should be noted that this analysis is given for objects that are in first level only, although it is feasible to consider some safety recommendation that fits the other levels as well.

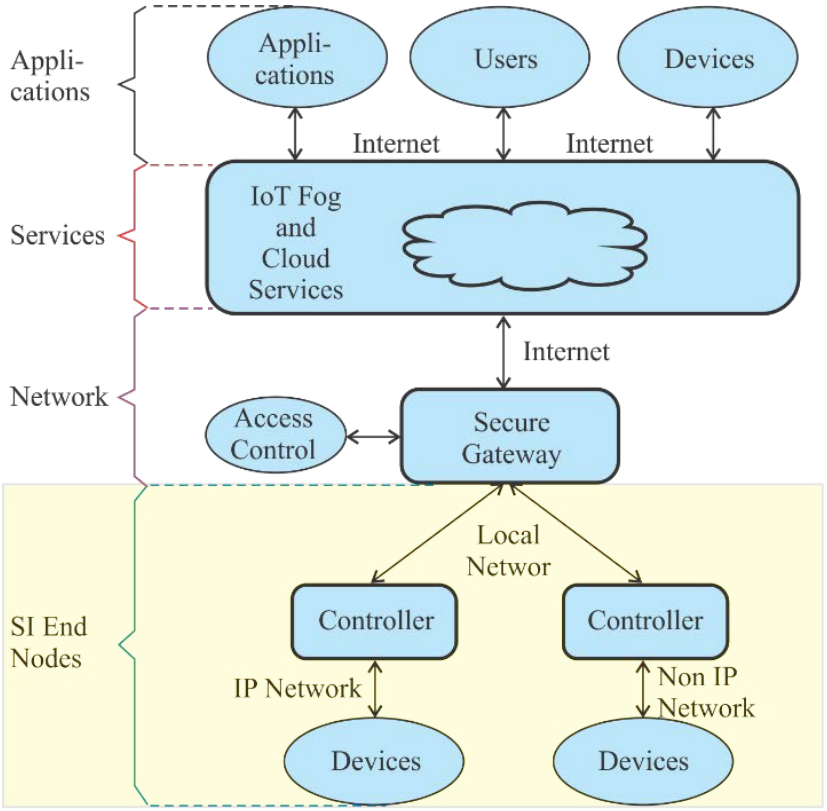

Fig. 1. *Framework for intelligent infrastructures.*

1.1 Physical security

When talking about security at the hardware level we are considering physical access to computers that are commonly connected to the Internet or to an intranet that generate information and is sent through connections to local repositories or to the cloud.

Once a device is part of an interconnected environment, it is important to consider that it could lose its physical security, since it might be located in inhospitable environments and could be reachable by anybody. Attackers could intercept, read or modify information, and could manipulate control systems and modify their functionality [10]. The biggest fear is when users, companies or organizations, use smart objects and they do not take much responsibility about security.

Security at this level is considered as a special way since you cannot compare security levels in hardware in small, medium, and large companies as well as for independent users, where levels of access to objects and data are based on the information they manage, though you should have control to not allow them be manipulated by people outside the interests of users or companies.

Hardware security for intelligent objects should be considered in the structure of products in a way that allows their integrity, furthermore not to admit direct manipulation in case of having access to them. For example, a smart card should have some physical characteristics along with a degree of protection against external agents, so it will not be easily manipulated, for instance, when altering or cloning cards [11]. It is also important to consider providing essential security features, as the following:

ROM booting, verifying security from a very low level, depending on the trusted execution environment where the object is implemented.

Devices that require intensive use of cryptography, hardware implementations can improve performance and extend battery life. However, it is important to understand that ciphers are compatible and they provide a reasonable lifetime for the product.

In circuit design, a possible attack on circuit boards should be considered, that is, its exposure must be taken into account to lessen possible attacks. Whenever possible, circuit boards should not be noticeable.

Interfaces provide access to components of the board, so it can be used to alter several security features. Any interface, console or logic, via USB or serial, must be considered in security contexts. ROM booting often provides a way to download firmware or manipulate the boot process, so that security issues are potentially present.

Components package, the ease of access to memory and the CPU. By selecting certain system options on the chip package, where, for example, the memory is physically located under the CPU, it can complicate hardware attacks that would otherwise be trivial.

Energy administration, it is an important aspect within the hardware platform security, we should consider its resistance depending on storage and capacity processing that will have the object.

1.2 Logical security

Logical security consists on application of barriers and procedures that protect access to data and only those authorized are allowed to access them [12].

The objectives that are proposed will be:

- Restrict access to programs and files.
- Ensure that operators can work without thorough supervision and can not modify programs or files that do not apply.
- Ensure that the correct data, files and programs are used in and by the correct procedure.
- That the information transmitted be received only by the recipient to whom it was sent and not to another.
- That the information received be the same as that which has been transmitted.
- That alternative secondary transmission systems exist between different points.
- That alternative emergency steps be available for transmission of information.

Typically, end users do not take safety into account when they use a system, as security aspects are often ignored. Similarly, these aspects can sometimes be considered a nuisance, because security often goes in the opposite side of comfort and ease of use, in the balance of the design of a system. This is why users can sometimes have a negative image of security, considering it annoying and interrupting their ability to perform a particular task.

In a secure environment, a user can come across with tasks that may be uncomfortable, such as remembering passwords, changing them periodically, etc., actions that can limit the operations that can be performed, as well as the resources to which it is allowed to access [13].

Security flaws of software that can arise based on the analysis done in the document published by Ferrer & Fernández-Sanguino, n.d., on Computer Security and Free Software can be grouped as follows:

- Failures due to unknown errors in software, or known by third hostile entities only.
- Failures due to known errors, but not fixed in the copy in use of the software.
- Failures due to a bad configuration of software, which introduces vulnerabilities in the system.

Each flaw identifies a type of vulnerability. The first one can be attributed to the quality of the code. The second one to the capacity and speed of fixing errors discovered in the code by the provider, as well as the ability of the administrator to receive and install new copies of the updated software. The third type of flaw is due to a lack of software documentation or a lack of adequate training of administrators to make a correct adaptation according to their needs.

The above failures can cause the program to malfunction, so it is necessary to consider the following:

- Algorithms can be implemented incorrectly which can lead to a loss of security, for example, a key generation algorithm that is not based on totally random numbers.
- Services can be designed to, contrary to their specifications, offer undesired functionalities or may compromise the security of the server.
- The necessary measures may not have been taken to ensure the correct handling of the input parameters, by which an external attacker may force the program to perform undesired operations.

There are methodologies for the development of hardware and software, one of the most used is the model in V that includes some stages, used for both types of development, although with regard to software there are other safe development methodologies, OWASP Testing Guide, OSSTMM, ISO 27001, SAFECode, among others[14].

1.3 Developed projects

- Electronic system with artificial vision application for automatic adjustable lighting that provides the optimum amount of light at the focal point of welding in work tables at laboratory scale. Project developed by[15], where a lamp, combined with a number of sensors and actuators as well as the implementation of artificial intelligence, makes the object act on its own to bring light to the user who requires it to weld plates. Here, security is little addressed both physically and logically, because the application does not affect any specific information of great importance.

- Expert system to handle information from sensors for visualization of alerts. Project developed by [16], which is a management platform for the information on forest fire alerts generated by sensors located on the Guayabillas hill. Here, the idea of security changes drastically, because the information handled by sensors and devices is of great importance. A slight approach is made in relation to security both at hardware and software level, where the fact that the computer is chosen as security against vulnerabilities is very subjective, because a computer is considered a little vulnerable. Although the information of the system arrives appropriately, there may be the possibility of manipulation of sensors and the system itself to alter the information that is handled on the platform.

- Design and implementation of a vehicle location and safety prototype system with GPS and GSM communication, based on open software and hardware. Project developed by [17], where no exhaustive security analysis is done so it can be modified at physical level, along with at software level in order to send incorrect location parameters.

These projects as some other developments carried out both locally and overseas are seen to have flaws in their design, although they supply a need to one or more people, the security of those objects is very limited, without considering that there are hackers who are on the lookout to steal information or to use smart devices as points of mass attacks towards other services.

Currently, a variety of intelligent devices are on the rise for every type of need, smart washing machines, intelligent locks, vehicles with automated and intelligent components– which allow users comfort, objects that generate information, among others. At this point, companies and industries that bring solutions in this regard play an important role providing lifelong assistance, and to improving day by day their devices. Although some of these companies may lose customers preference by not being able to offer the security that users could need.

In accordance with this background, we present the SWOT for security in smart objects shown in Table 1.

Table 1. *SWOT of security in smart objects.*

STRENGTHS	WEAKNESSES
Ubiquitous detection. Increase in productivity. Speed and accuracy of the information. Ability to objectively affect the environment of physical world. Improving the quality of life. Experiences solving earlier problems.	Wide attack environment, e.g. data, sensors, systems and devices. Potencial introduction of uncertainty due to high volume of data. Data dissemination through multipl domains. Little awareness of security with connected objects.
OPPORTUNITIES	**THREASTS**
Operational efficiency in real-time. Growth of economic income. New feactures. Steady control for environments at risk. New fields of technology development. Create solutions from earlier problems.	Modality of unanticipated attacks. Little knowledge about IoT security. Thetf or alteration of confidential information. Lask of standards and regulations to create secure IoT objects.

It is important to consider this Table resulting from solutions to prior problems where it has been already clearly identified advantages and disadvantages of any device that solves a need.

2 Results

Fig. 2 shows the components that let us consider a device as an intelligent object, where the first five lower layers are mandatory, and the two upper layers are optional, due to they can be managed from other devices with higher processing, memory and energy capacities.

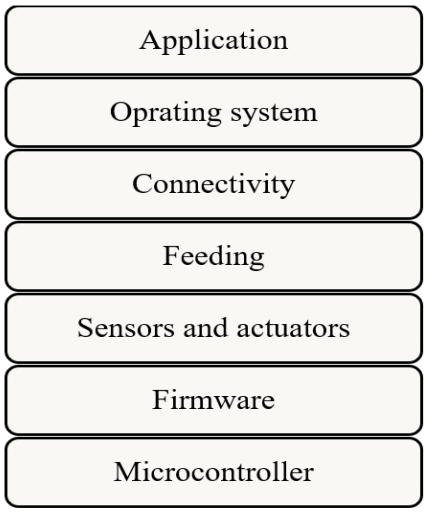

Fig. 2. Components of an intelligent object.

A microcontroller is an integrated circuit or chip that includes in its interior all three functional units of a computer: CPU, memory, and I/O units, that is, it is a complete computer in a single integrated circuit, these are increasingly smaller and not so remarkable.

A firmware is a block of machine instructions for specific purposes, normally recorded in read/write memory (ROM, EEPROM, flash, etc.), which establishes the lowest logic level that controls the electronic circuits of a device of any type.

Sensors collect information about environment, users, or both. For example, light, temperature, movement, location (GPS), etc. Actuators work based on the information gathered by sensors and act in accordance with programmed instructions.

Feeding refers to the battery that objects must have, where there is a serious problem, because the smaller the device is, more limited the energy resources are, therefore, on the one hand, new strategies must be found to reduce energy consumption, or on the other hand, to take advantage of using energy from the environment.

Connectivity is framed in communication protocols that allow devices to interact with others, although, we should look for communication protocols that consumes less energy and also to providing security.

The operating system is a piece of software that will allow us to manage a device according to the functions for which it has been designed, where we can install a greater number of applications to have greater functionality of the object, a good example are smartphones.

It is important to note that all earlier components are integrated, although it is possible to exclude some of them, for instance, to choose just the sensor or the actuator, or ignore the operating system and to program the device at the firmware level, where management will be done from another stronger device to allow us handle a greater number of IoT objects.

Applications are also part of the components of smart objects, even though it will just be for devices with greater processing, memory and energy capacities, to allow them have higher performance based on the requirements that they were designed for.

The components described in this section are usually integrated in a single plate, framing them in a single device, though there would be components that could be excluded in the design of certain devices, to make them less noticeable as is the case of wearables– electronic devices incorporated into some part of our bodies, interacting continuously with us, as wall as other devices in order to perform a specific function, that is, smart watches, sport shoes with built-in GPS, and wristbands that monitor our health, are examples, among others, of this type technology that is increasingly present in our lives.

In addition to presenting the intelligent objects layers, an important security scheme is proposed to consider if a device has an acceptable level of security, as shown in Fig. 3. This scheme also considers some stages, such as storage, hardware and software platforms, however they could be excluded because can be complemented with other stronger devices to offer greater security.

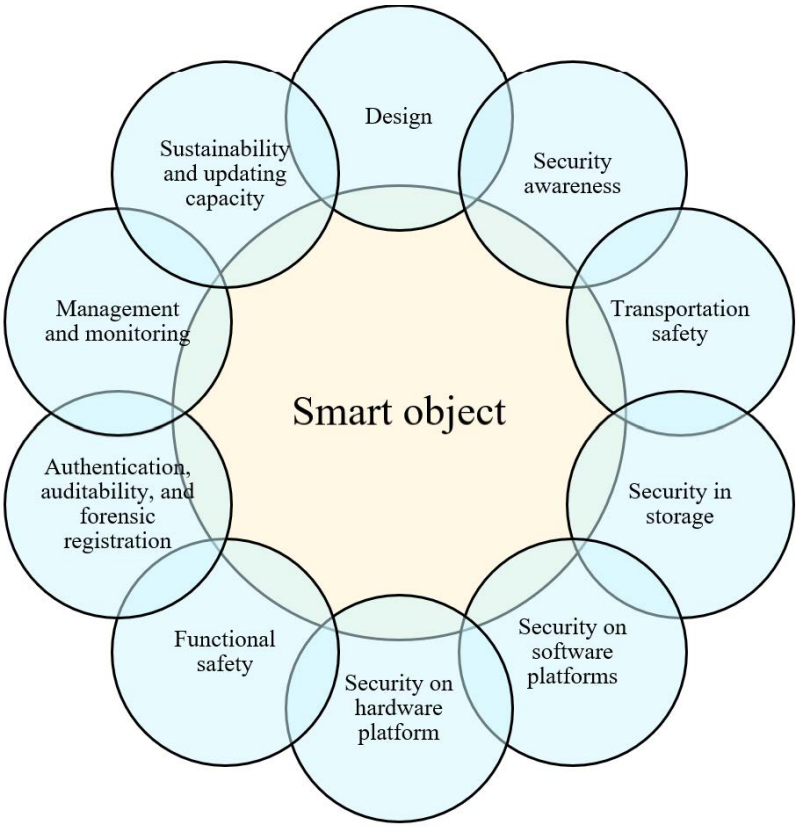

Fig. 3. Security scheme for correct design and implementation of a smart object.

Design, in this initial phase of development a lot of design concepts could de applied, market analysis, competitive analysis, and research support. Here, awareness of security is usually trivial, offering consulting, analysis and advice around high-level concepts, as well as components and technology security capabilities. Although, you could be aware of security assistance regarding the capabilities of competition, and the expected course of market, regulations and legislative forces when it comes to cyber security.

Awareness about safety, there should be considered experiences from the past, records taken during each of the phases, and everything that serves to be conscious of security that devices should have, and take appropriate actions minimizing the risks of vulnerability in objects.

It is possible to apply the ISO 27001 standards, which refers to awareness in a company about security of information, it can also be considered for the physical object as well as the information it manages, that is the security that every component should have to be considered safe.

The security policies and procedures that are considered from now will serve as guidance during the design and implementation of an object for a specific environment, in addition to envisaging possible threats in which they may be compromised.

Also, it should be considered ease of use, fitness factor, energy consumption, and other technological requirements that are important to secure the platform. In addition to people with a security directive, they must be part of this team that participates in the formulation of technical and market requirements, creating a better awareness of the security of objects.

Security in transportation, provide an adequate level of identification, privacy and integrity of the network communication. Understanding how wired or wireless authentication occurs, how credentials are stored, and if they can be relocated into other devices is obviously very important. There are several encryption methods and techniques that you can use, as the hash functions like MD5, SHA-1 or SHA2, among others, but you should also consider processing and memory capacities of objects. In addition to using secure communication channels such as VPNs. Handling IP security protocols that are part of an object security such as IPsec, TLS/SSL, DTLS, HIP, EAP, SSH, in conjunction with the security provided by Wi-fi, 6LowPAN, GSM, and 3G communication protocols, communication security can be improved.

Security in storage, provide the appropriate level of protection of persistent data kept in a device or in a system. Data must be secured when a physical attack occurs. Also the understanding how sensitive data will be secured is vital, both from a perspective of integrity and privacy. We can consider as in the previous argument the encryption for data at rest, then we will protect objects or platforms that stores confidential information not to be so vulnerable to malicious attacks.

Security in software platforms, selection of a modern operating system or platform that provides defense-in-depth properties, including ASLR which is a security technique involved in protecting against battery overflow, memory not executable, segregation process, and sandbox attacks. It is important to consider safe standard coding practices of industries, such as OWASP, SAFEcode, among others, to minimize the risk of attacks to applications.

Security in the hardware platform, ensures that hardware platform provides the essential security features. This involves some aspects, such as booting ROM, cryptography, proper circuit design, device access interfaces, component packaging, and power management.

Authentication, auditability and forensic registration, devices that in a connected environment can not be compromised, or be used as platforms entry points to launch attacks. It is necessary to validate objects that communicate with each other and with the platforms, as well as to consider distribution software such as Kali Linux to perform penetration audits to discover vulnerabilities.

Management and monitoring, ensuring that smart objects can be managed and monitored safely. Therefore, network monitoring systems must be implemented for connectivity of objects to allow us detect any change, or unauthorized access to the information, or to certain parameters of devices. For example, on the one hand, we can mention the proprietary tool PRTG Network Monitor with features such as compressive network monitoring, flexible alert systems, high availability cluster for uninterrupted network monitoring, distributed monitoring with remote probes, publication of data, and maps, on the other hand, we can opt for open software like Nagios.

Sustainability and the ability to update, features that facilitate the ability to safely update devices when vulnerabilities are discovered after release.

Each of these steps of the general scheme must be a continuous movement cycle, that allows us to have feedback based on records that are got in tests during development or in a real operating environment, or also from failures produced by attackers causing great losses, they should be solved immediately though.

3 Discussion of results

Most of smart objects, when talking about security, were not designed to be part of an interconnected environment, hence in some cases, some of them have been compromised, according to Karpesky Lab report [18], in 2017 there were more than 7,000 samples of malware targeting intelligent devices, and the most attacked were DVRs and IP cameras, where the majority of them were in China.

In academic environments where intelligent devices are developed [9], [15]–[17], where everyday objects are integrated sensors and actuators that through software we can interact with other devices or people using the internet, there is no security validation process that these devices must provide both at the logical level referenced according to the protocol stack of the TCP / IP architecture, and at the physical level.

These figures show us an overview of security in smart devices, so they should generate awareness when dealing with devices or objects connected to the Internet, so it is important to increase awareness of the security that must be taken in this regard, whether in academic or industrial environments.

4 Conclusions

Security is a primary issue for people, companies, or industries that use smart objects, not only because there could be financial operations in the middle that could lead to serious consequences in case of data leaks, but there also could be unauthorized access to vital systems that could lead to the loss of human lives or cause a mass disruption of society, that is, where there are smart objects on which people depend on, and they were vulnerable to attacks, such as medical devices, on the other hand, smart vehicles that could be intruded causing the driver to lose control and have an accident, as well as land, air or maritime traffic control systems where an attack to their systems could result in chaos of greater magnitude. With this regard, the aforementioned aspects have to be considered from a basic level of security awareness.

This research clearly identifies that developers of intelligent devices in academic and industrial environments would not consider safety a priority during design and development. When security is not taken into account in the production process of these devices, there is a serious risk that these objects may be susceptible and vulnerable to cyber attacks, since they were not designed to be in an Internet-connected environment.

5 References

[1.] Real Academia Española, "DLE:Diccionario de la lengua española - Edición del Tricentenario," 2017. [Online]. Available: http://dle.rae.es/?id=B3yTydM. [Accessed: 20-May-2018].

[2.] [Universidad Rey Juan Carlos, (8) Charla sobre Internet de las Cosas en la URJC por Carriots (06/11/2013) - YouTube. 2013.

[3.] B. Cedón, "El origen e historia del Internet de las Cosas (IoT)," 2017. [Online]. Available: http://www.bcendon.com/el-origen-del-iot/. [Accessed: 20-May-2018].

[4.] J. Pacheco and S. Hariri, "IoT Security Framework for Smart Cyber Infrastructures,"

in 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), 2016, pp. 242–247.

[5.] D. Kushner, "The real story of stuxnet," IEEE Spectr., vol. 50, no. 3, pp. 48–53, Mar. 2013.

[6.] C. Bracho, F. Cuzme, C. Pupiales, L. Suárez, D. Peluffo, and C. Moreira, "Auditoría de seguridad informática siguiendo la metodología OSSTMMv3 : caso de estudio," Maskana, vol. 8, pp. 307–319, 2017.

[7.] F. Cuzme, L. Suárez, C. Bracho, and C. Pupiales, "Diseño de políticas de seguridad de la información basado en el marco de referencia COBIT 5," in Innovando Tecnología, UTN., Msc. Daisy Ibaquingo, MSc. Cathy Guevara, MSc. Silvia Arciniega, MSc. Marco Pusdá, and MSc. Pedro Granda, Eds. Ibarra, 2017, pp. 129–137.

[8.] P. Casas, "El Triángulo de la Seguridad | Seguridad en Cómputo," 2015. [Online]. Available: http://blogs.acatlan.unam.mx/lasc/2015/11/19/el-triangulo-de-la-seguridad/. [Accessed: 20-May-2018].

[9.] V. Alvear-Puertas, P. Rosero-Montalvo, D. Peluffo-Ordóñez, and J. Pijal-Rojas, "Internet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones: Revisión de Literatura," Enfoque UTE, vol. 8, no. 1, p. 244, 2017.

[10.] F. Martínez, "Lo que el Internet de las Cosas representa para la seguridad - CIOAL The Standard IT," 2013. [Online]. Available: http://www.cioal.com/2013/10/24/lo-que-el-internet-de-las-cosas-representa-para-la-seguridad/. [Accessed: 20-May-2018].

[11.] Pitkit Zetes Smartech, "Perfil de la compañía: Pitkit Zetes Smartech." [Online]. Available: http://pitkitcards.com/spanish/profile.html. [Accessed: 20-May-2018].

[12.] C. Borghello, "Seguridad Informatica / Seguridad Lógica." [Online]. Available: https://www.segu-info.com.ar/logica/seguridadlogica.htm. [Accessed: 20-May-2018].

[13.] J. Ferrer and J. Fernández-sanguino, "Seguridad informática y software libre.," pp. 1–11.

[14.] F. López Provencio, "Desarrollo dirigido por la seguridad," 2015.

[15.] H. Farinango, "Sistema electrónico con aplicación de visión artificial para iluminación regulable automática que brinde la cantidad de luz óptima en el punto focal de soldado en mesas de trabajo a escala de laboratorio," 2016.

[16.] J. Ruiz, "Sistema experto en el tratamiento de información de sensores para visualización de alertas," 2017.

[17.] T. Morocho and J. Rogelio, "Dispositivo de seguridad para alerta de manipulación, rastreo y localización de motos por medio de tecnología inalámbrica SMS Y GPRS," Jan. 2017.

[18.] Kaspersky Lab, "Karpersky: Boletín de Seguridad Estadísticas Generales de 2017," 2017.