Vulnerability of information, on the Internet of Things

Vulnerabilidad de la información, en el internet de las cosas

Vulnerabilidade da informação, na internet das coisas

José Custodio Najar Pacheco[1]
John Alexander Bohada Jaime[2]
Helena Clara Isabel Alemán Novoa[3]

Received: May 20th, 2022
Accepted: August 15th, 2022
Available: September 12th, 2022

How to cite this article:
J.C. Najar Pacheco, J.A. Bohada Jaime, H.C.I. Alemán Novoa, "Vulnerability of information, on the Internet of Things," *Revista Ingeniería Solidaria,* vol. 18, no. 3, 2022. doi: https://doi.org/10.16925/2357-6014.2022.03.07

Review article. https://doi.org/10.16925/2357-6014.2022.03.07

[1] Fundación Universitaria Juan de Castellanos, Grupo de Investigación CIyT, Tunja, Colombia
Email: jnajar@jdc.edu.co
ORCID: https://orcid.org/0000-0001-9812-9475

[2] Fundación Universitaria Juan de Castellanos, Grupo de Investigación CIyT, Tunja, Colombia,
Email: jbohada@jdc.edu.co
ORCID: https://orcid.org/0000-0002-3382-0190

[3] Fundación Universitaria Juan de Castellanos
Email: haleman@jdc.edu.co
ORCID: https://orcid.org/0000-0001-7669-7316
CvLAC: https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?-cod_rh=0001038923

Abstract

Introduction: This article is a product of the review of the "Vulnerability of information, on the Internet of Things", developed from the Juan de Castellanos University Foundation in 2021.

Methods: Review of articles and relevant literature on the exposure of information and some vulnerabilities in devices that are part of the Internet of Things (IoT).

Results: Information, as one of the most valuable assets, is essential, which is why it is important to have technology, devices that are part of the IoT, despite vulnerabilities.

Conclusions: Keeping information secure has become a challenge, because it is one of the most important assets of any organization. Its manipulation requires many actors and involves many factors, making it is difficult to control and protect. The constant emergence of technology and their applications in various fields, along with their relative ease of use and smaller sizes, have made significant inroads possible; we must accept that they are a part of the IoT.

Originality: In the bibliographic review of the information, which results from the use of technology, how the IoT is vulnerable and even more so when it is configured with the Internet.

Limitation: Technology is becoming more and more dependent on it, despite the vulnerabilities of IoT devices and the Internet.

Keywords: Internet of Things, vulnerabilities, firmware, cybercriminals, Mirai, ransomware.

Resumen

Introducción: el presente artículo es producto de la investigación "Vulnerabilidad de la Información, en el internet de las cosas desarrollada en la Fundación Universitaria Juan de Castellanos, 2021.

Métodos: Revisión de artículos y literatura relevante, sobre la exposición de la información y algunas vulnerabilidades en los dispositivos que hacen parte del IoT.

Resultados: La información, como uno de los activos más valiosos, es fundamental, por lo cual es importante contar con tecnología, dispositivos que hacen parte del internet de las cosas, no obstante de las vulnerabilidades.

Conclusiones: Keeping information secure has become a challenge, because it is one of the most important assets of any organization, and in its manipulation take part many actors and factors, therefore it is difficult to control and protect, among many reasons. The constant emergence of technology and its applications, in various fields, which due to its ease of use of a large number of electronic instruments, and its smaller size, have made significant inroads, since by being connected to the global network you can overtake countless specific tasks, thus they have become part of the IoT.

Originalidad: En la revisión bibliográfica de la información, que resulta por la utilización de la tecnología, como el internet de las cosas se expone y más aún cuando se configure con Internet.

Limitaciones: La tecnología es cada vez mayor llegando a depender de ella, no obstante de las vulnerabilidades de los dispositivos IoT y del internet.

Palabras clave: Internet de las cosas, Vulnerabilidades, firmware, ciberdelincuentes, Mirai, ransomware.

Resumo

Introdução: este artigo é produto da pesquisa "Vulnerabilidade da Informação, na Internet das Coisas desenvolvida na Fundação Universitária Juan de Castellanos, 2021.

Métodos: Revisão de artigos e literatura relevante sobre a exposição de informações e algumas vulnerabilidades nos dispositivos que fazem parte da IoT.

Resultados: A informação, como um dos ativos mais valiosos, é essencial, por isso é importante ter tecnologia, dispositivos que fazem parte da Internet das Coisas, apesar das vulnerabilidades.

Conclusões: Manter a informação segura tornou-se um desafio, pois é um dos ativos mais importantes de qualquer organização, e na sua manipulação intervêm muitos atores e fatores, por isso é difícil de controlar e proteger, entre muitas razões. O constante surgimento da tecnologia e suas aplicações, em diversos campos, que pela facilidade de uso de um grande número de instrumentos eletrônicos, e seu menor tamanho, têm feito avanços significativos, pois estando conectado à rede global você pode ultrapassar inúmeros tarefas específicas, tornando-se assim parte da IoT.

Originalidade: Na revisão bibliográfica das informações, que resultam do uso da tecnologia, como se expõe a Internet das Coisas e ainda mais quando se configura com a Internet.

Limitações: A tecnologia está crescendo, passando a depender dela, apesar das vulnerabilidades dos dispositivos IoT e da internet.

Palavras-chave: Internet das coisas, Vulnerabilidades, firmware, cibercriminosos, Mirai, ransomware.

1. Introduction

Technology plays a transcendental and important role in the development of a country. The internet and communications have facilitated the development of a number of activities and made possible that what was not before. While it is true that the Internet of Things (IoT) is not a new topic, it has recently begun to play a more important role in medicine, industry, agriculture and livestock, controlling a large number of devices that monitor patients, homes, processes, among others.

It is important to emphasize that information security has always been a difficult problem to understand, evaluate and analyze, even more so with the constant incursion of technology together with its applications. Through their diversity and ease of use, the sheer number of electronic instruments, which due to their increasingly reduced size, as well as their costs and intelligent features of the devices, which when connected to the network have thus become part of the IoT [1].

But, how many of these devices can be trusted when, according to CVE details [2], vulnerabilities increase by more than 100% each year? In this complicated situation, even simple devices, such as smart bulbs are being hacked, and every time they do it in a more ingenious way; for example, from drones, infecting the bulb and then taking total control of the network [4]. Any wireless device, from light bulbs to coffee machines and surveillance cameras, will have some degree of vulnerability, compromising the security of information [5]. It is also important to highlight the risks to which the IoT is exposed, as a result of the existence of vulnerabilities, which may

even lead to the demolition of a system completely, according to Belisario Contreras, Program Manager for the Inter-American Committee against the Organized Terrorism of the American States (OAS) [6].

Devices that are part of the Internet of things (IoT) will always be exposed, as evidenced by the research of the team of analysts of Kaspersky Lab, on some connected devices, such as USB multimedia content transmission, cameras, coffee makers and security systems, controlled by smartphones. The results showed that among the most vulnerable were baby monitoring cameras, being manipulated by the *hackers* who could watch videos, launch audios and even obtain user passwords [7] via the network. Mirai malware is capable of damaging devices such as printers, surveillance cameras or home routers, as well as performing denial of service attacks, because millions of IoT devices work with the user configuration and password, which have been configured by default, which facilitates the scanning of thousands of devices and infecting them within a few minutes [13]**.** Recently, a variant of Mirai, the OMG, appeared, apparently very sophisticated, with the aim of changing IoT devices on proxy servers and renting them. Along with the already proven Distributed Denial of Service (DDoS) attacks [8]**,** the situation grows more and more complicated for the IoT, that grows by more than 20% each year [15].

These DDoS attacks have resulted in the fall of thousands of servers and important sites in the world [10]; result of the fragility in the security of the devices that connect to the internet, causing chaos, as the Mirai botnet showed [11] and continues to cause serious difficulties by compromising IoT devices, and using them to trigger Distributed Denial of Service (DDoS) attacks. This has caused great difficulties for cloud computing companies such as OVH [18], because the devices that are part of the IoT come with vulnerabilities; so much so that they can compromise the security of houses, the information of their owners and businesses [13], because at the time of its manufacture safety was not taken into account [14].

The use of these devices in the control of crops, in medicine, education, cars, airplanes among others is important, as we will have to live with them as they enter our lives, even without permission [15]. Approximately 70% of devices are vulnerable, ranging from simple attacks to collecting important confidential information from organizations [16], which becomes very dangerous, as even a simple vulnerability in these devices can lead to total system failure. According to the OAS, innovation must be seized [17], thus, the IoT has managed to enter considerably into society. This carries significant merits, however, in the same way, security is exposed, because when encountering a hyperconnected society, it also manifests incalculable risks that have to do with cybersecurity [18], compromising individuals as much as large organizations,

causing disastrous damage, such as leaving public services without power, as what happened to an Eastern European state; leaving one part without electricity for a few hours [20].

The use of the IoT is a reality. Every day the number of devices that are incorporated grows and are important for the diversity of activities that take place in society. However, in the same way, it becomes a very significant tool that is exploited by cybercriminals. As the use of IoT devices grows exponentially, so will the number of attacks. Thus, everyone, from the individual to large organizations, incorporating these intelligent elements, must think about implementing security policies.

2. Literature Review

2.1. VULNERABILITY OF INFORMATION, ON THE INTERNET OF THINGS.

The security of information has always been a difficult problem to understand, evaluate and analyze, because there are so many actors involved, which makes it complex. It is further complicated by the continual appearance of new technologies and their applications in many fields of the modern world. These new technologies are cheap and small, diverse and easy to use with intelligent features. This myriad of devices, being connected to the network of networks, to advance an incalculable number of specific tasks, have become new members of the IoT [1]. But, how much can be trusted when recently it is known that each day on average vulnerabilities increase by approximately 135%, and from one year to the next by almost 128%, according to CVE Details [2].

Moreover, some vulnerabilities that affect the Wi-Fi protocol, although it could have been solved by their manufacturers [3], but surely not by all, on one side and on the other.

Now, vulnerabilities in devices that are part of the IoT will not be the exception. An example of the commonplace occurrence of vulnerabilities can be found with smart bulbs. Hackers showed new vulnerabilities on these devices, infecting smart bulbs and taking full control, distributing malicious firmware throughout the network [4]. Thus, since there are more devices connected to our house wirelessly, such as light bulbs, coffee machines, even surveillance cameras, and knowing that these devices have some degree of vulnerability, they are also expected to cause some degree of damage; for example, the cameras that we use for the care of babies, have

apps that have security problems, in which the security of this information can be compromised [5].

All these devices, in addition to locks, refrigerators and, of course, smart speakers, connect to the Internet, and as you know, there is no absolute security [6]; therefore, they could easily fall into the hands of cybercriminals. It is one of the concerns that were discussed at the Mobile World Congress (MWC), according to a study carried by ESET, a European cyber security company. Connected devices will be a problem [7], because the more devices that are connected increases the risk to people, companies and state institutions. For existing vulnerabilities in these, if we look at a baby-monitoring camera, in addition to using cloud technology, it complies with its objective for which it was installed and configured, providing an image of the baby and keeping the child safe while the parents perform tasks elsewhere in the house, but the question is, Is the child really safe? From the physical point of view, he/she is, but your privacy may be at risk from the threat of cyber-attacks. It is essential to emphasize the dangers to which users can be exposed when using the IoT, according to Belisario Contreras, Program Manager for the Inter-American Committee against Organized Terrorism of American States (OAS) [8].

Likewise, some IT security companies are aware that the IoT really complies with the functions for which they were designed, but security cannot be ignored, which, in one way or another, depends on constant updates by its users. Similarly, ESET disclosed some risks that are latent in the IoT, such as: exploitation of vulnerabilities, where it was shown that 10 best-selling IoT devices had an average of 25 vulnerabilities each in no more than 2 years, according to HP; Likewise, many devices have video cameras for monitoring purposes, so it is important to configure and use secure passwords correctly. In the same way, it is recommended that elements that are connected to the internet be on separate networks; Likewise, if IoT devices, are collecting important private data, the user should be made aware during its configuration, in order to avoid inconveniences in its collection; and, finally, as the data collected by IoT devices are stored on a server, it is essential that manufacturers give them the security they deserve, so that customer data is safe [9].

A team of analysts of Kaspersky Lab, performed research on connected devices, in order to locate them in the IoT, focusing on USB devices transmitting multimedia content, cameras, coffee machines and security systems controlled by smartphones. The research showed that, for the most part, these devices proved to be vulnerable. For example, the camera that is used to monitor babies, that being on the same network and being directed by hackers, transmits videos, launches audios and even obtains the user's passwords [10]. Now, Mirai malware can convert electronic devices,

such as webcams and routers connected to the network, into bots that are remotely controlled. When connecting a WIFI security camera, after only 98 seconds, the Trojan malware related to Mirai appeared, according to Robert Stephens, a veteran in the field of technology [11]; therefore, there are eminently dangers in the IoT, which concerns users of these devices.

Likewise, according to research by Avast at MWC 2017, it was found that a significant number of devices using the Telnet protocol, which is known to have been used to create the Mirai botnet, are vulnerable, as well as a considerable number of webcams, coffee makers, among other devices, which corresponds to 500,000 easy-to-hack devices in Barcelona during the MWC 2017 [12]; therefore, whenever we think about it, the IoT devices will always be exposed more than others, due to the different vulnerabilities. Mirai is capable of damaging devices such as printers, surveillance cameras or home routers, as well as performing denial of service attacks. This happens because millions of IoT devices work with the user settings and password, which have been configured by default, which results in thousands of easy-to-scan devices and infects them in minutes [13]. A new variant of Mirai, the OMG, recently appeared, apparently very sophisticated, with a precise and defined objective; to convert IoT devices into proxy servers and rent them for economic purposes. Along with the already proven Distributed Denial of Service (DDoS) attacks [14], the situation grows more and more complicated for the IoT, that grows by more than 20% each year [15].

Of course, organizations have always been concerned with the denial of services in a high percentage, which comes from botnet-like networks. In 2016, they were victims of Mirai, which, as we know, is a botnet focused on the IoT, taking advantage of the lack of protection of these devices, giving the opportunity for criminals to carry out the greatest denial of distributed services (DDoS) attack in history, resulting in the failure of thousands of servers and important sites in the world [16]. This was due, once again, to the existence of fragility in the security of the devices that connect to the internet every day, as the Mirai botnet showed [17], and the most complicated thing is that the Mirai malware continues to cause serious difficulties by compromising a significant number of IoT devices and using them to trigger DDoS attacks, currently causing immense drawbacks to cloud computing organizations like OVH [18]. Because smart devices come with vulnerabilities, they may be compromising, in some occasions, the security of the houses, the data of their owners and damaging businesses [19].

IoT devices connected to the network are searched for by Mirai, as they are known to have little security, such as factory default usernames and passwords [20]. This facilitates the work of criminals, so there is responsibility on the part of the users

of these devices, that although it is true, we know they are vulnerable, in one way or another the work of criminals must be made a little more difficult, by placing secure passwords. Mirai botnet has become a complex problem, infecting many IoT devices, especially security cameras that use default passwords [21], in order to have access to the telnet protocol, which as it is constantly known has been shown to be vulnerable [22]. In this uncertain issue, we could hardly think of security, if each one of the actors that are part of the functionality of the IoT are vulnerable. The growth of the IoT is a reality, and it will be difficult to stop it, as it is foreseen that in the future organizations, will have these devices, despite the knowledge that these devices do not take safety into consideration when manufactured. In this regard, high investments will be required at the Latin American level [23].

Undoubtedly, it is important to highlight the great achievements of the IoT, because it has facilitated and improved, the daily lives of people and some processes, such as carrying out and monitoring crops, achieving the result of optimal harvests, which from any perspective is important. However, at the same time they have brought difficulties to their users, endangering their privacy. There is concern over the growth of incidents in which the elements that are part of the IoT are exposed, since the circumstances in which they are compromised are increasing [24], encroaching on various fields of daily life: in medicine, education, cars, airplanes, among many others [25]; thus the situation every day becomes more complex for users of IoT devices, as approximately 70% of these are vulnerable, with the risks ranging from simple attacks to criminals accessing very important confidential information of organizations [26].

However, the use of the IoT is important, since it facilitates users, such as organizations and even countries, to exercise more control over the technology used, as well as access to information. But, likewise, it is necessary to be aware of the risks to which anyone can be compromised; through a simple vulnerability in some devices, an system can be completely crashed, however, according to the OAS, innovation must be taken advantage of [27]. Technological advances go hand in hand with the existence of the human being, so that nowadays one cannot conceive life without the other. The IoT has managed to penetrate society, which brings significant advantages, but at the same time security is compromised, because by having a hyper-connected society, innumerable risks related to cyber security appear in the same way [28].

One of the sectors in which the IoT has made a representative approach is in the health sector, offering more and more possibilities for patient care in a simple way, with the connection of medical devices to the Internet, such as pacemakers and insulin pumps, among others, which allow the control of these in a simple way and can even save lives; but at the same time, there is the risk that these elements can be

compromised, with examples of hackers interrupting the operation of these devices if patients do not accept to pay for taking back the correct functionality of the attacked device [29].

It is a reality of which we cannot be outsiders, because in one way or another we are part of it, whether we share it or not, a situation that affects all sectors, according to research carried out on 50 intelligent systems that are commercial and that are being implemented in different organizations' headquarters. This study has shown that these should continue to put in place new measures to protect themselves, since these devices and services present security problems, according to Symantec [30]. Thus, in the IoT era, any small, medium or large device that is connected in order to perform any specific activity, is exposed to being controlled at any time by Cybercrime, causing catastrophic damage, such as removing public services from populations, as what happened to one of the eastern European states, leaving a sector without electricity for a few hours [31].

Therefore, people must be informed that the devices that are part of and/or are being added to the IoT are vulnerable. Therefore, it is important to constantly update them with security patches and updates, in order to make them less fragile against vulnerabilities that have already identified. Unfortunately, this is not always the case, due to the variety of actors involved. it will be difficult to reach an agreement, but it does continue to add new devices that, as is known, are vulnerable, which increases the attack surface, thus promoting DDoS attacks supported by the IoT [32].

If organizations wish to be successful, they must become part of the IoT, but similarly, there are difficulties, as some recognize having fear of external attacks while having security problems [35]. Problems that increasingly become more complex, since technological attacks are always directed at devices that are part of the IoT, due to vulnerabilities in their technology, which continue to be widely used, without any security control [36].

Of course, it is to be expected, because more and more devices appear, which are manufactured in an irresponsible manner, by not taking into account the safety nor standards of the industry, thus giving greater opportunity to cybercriminals, as predicted by Trend Micro [37], the situation made more and more alarming, as studies like that of HP show that approximately 70% of IoT devices contain serious vulnerabilities [38].

Experts also warn that IoT devices are rarely patched or updated, which is why different security measures must be implemented [39]. Similarly, the probability of risk is very high because more than 90% have very sensitive information, as well as 70% with some vulnerability [40]. This is largely due to the fact that a significant number

of devices that are part of the IoT, are impossible to update, and the most ironic thing is that the owners of these elements, in general, never find out that they are used to execute attacks [41].

Ultimately, this is a never-ending problem; when ransomware is presented, there will be an obligation to pay to continue working; WannaCry, cancellation of normal activities in institutions; and even, the confrontation of vulnerabilities in the Internet of Things, in this case health institutions becoming a target for cyber criminals [42]. Therefore, it is essential to look for ways to increase security, since every day there are more devices that connect to the network, which, although it is true, increase their usefulness, in the same way, they are exposed due to the existence of vulnerabilities [43].

Taking into account the knowledge we have of ransomware, which shows no signs of reducing in the short-term, another issue to mention is that sensors are being added with new features, which is important, but are designed from the purely operational perspective and with security in mind, which is exploited by cybercriminals [44]. The constant appearance of insecure IoT devices has facilitated that vulnerabilities are exploited on a large scale, because they are becoming simpler to carry out [45]. Additionally, every day vulnerabilities remain within applications, services, and IoT devices increases the risk that they serve as an access point for cyber-attacks, providing valuable information to other users and even exposing the security of fundamental institutions, such as public services [46]. As the concern grows and persists, the role will continue to grow into what is being called the Ransomware of Things, or RoT [47].

The most difficult thing is that this issue is not at all satisfactory, because ransomware will continue spreading, fulfilling its objective of obtaining easy and fast money. It is so lucrative, that hackers are creating organizations in order to extort [48] with experts predicting that the threats will undoubtedly increase year after year [49].

Of course, we cannot forget that the IoT has allowed both people and organizations to connect, taking advantage of technology and, at the same time, a myriad of activities; However, cybercriminals will continue to take data and sell them to third parties or blackmail individuals or organizations in exchange for economic gain [50]

Finally, for the functionality of the IoT, the intervention of a significant number of applications and devices is necessary, such as the operating system, protocols, applications and the mechanisms that are part of the Internet of Things, which are vulnerable as mentioned in the article "Vulnerabilities in the Internet of Things" [51]**,** that as they are used in society, because they are increasingly intelligent and of a reduced size, they allow us to have important information, which is exposed when we become part of the IoT, for its vulnerabilities [52].

Technology facilitates interconnectivity as well as a fast access to more information traffic in less time; additionally, it adds a significant number of devices that are part of the IoT [53]. Society depends significantly on technology, even though people know the risks of information exposure [54]; for example, vulnerabilities within IoT devices have resulted in power failures in the equipment used by the energy industry [55]. Despite the drawbacks mentioned above, IoT device use is increasing; such use has become a dependency because through them daily basis activities are carried out, which leads to an important growth in Internet configuration, no matter the concerns about the threats and attacks that may occur to IoT devices [56].

3. Conclusions

Keeping information secure has become a challenge, because it is one of the most important assets of any organization, and in its manipulation take part many actors and factors, therefore it is difficult to control and protect. The constant emergence of technology and its applications, in various fields, which due to its ease of use of a large number of electronic instruments, and their smaller size, have made significant inroads, since by being connected to the global network you can perform countless specific tasks, thus they have become part of the IoT [1]. From the knowledge we have of the vulnerabilities that increase disproportionately by more than 100%, from one year to the next [2], the concern that the security of these devices will be compromised is born.

In most cases, vulnerable IoT devices compromise security [13]. When connected to the internet that, as is known, is also not safe [6], this facilitates the control of cybercriminals; concerns that are treated according to the ESET study in the Mobile World Congress [7].

Therefore, it can be concluded that the more devices are connected, the more exposure there will be to both public and private persons and institutions, as a result of the existence of vulnerabilities, which may even lead to the demolition of a system completely; according to Belisario Contreras, Manager of the Program for the Inter-American Committee against Organized Terrorism of the American States (OAS) [8]. As it can be evidenced, it is actually difficult to control security in IoT devices, since several factors take part in which, in many opportunities, it is difficult to agree, except to minimize the risks.

Currently, the Mirai botnet has become a problem that is too complex and not easy to solve and is certainly alarming when considering the large number of IoT devices infected, especially security cameras when using passwords by default [21].

These devices for access use Telnet, which as you know has always been vulnerable [22]. Under this uncertain panorama, it would be hard to think of security if each one of the actors that takes part in the functionality of the IoT is vulnerable.

In spite of everything, the IoT is a reality and can hardly be stopped, a situation that should not be so, since as it is observed, it depends to a large extent on the responsibility of the manufacturers of these devices, because as you can perceive, they do not take into account the minimum safety standards at the time of the manufacture of these elements. This means that every time one is added, it becomes part of the IoT, and in the same way, it becomes part of a system every more vulnerable, and therefore increasingly uncontrollable.

Thus, it is difficult to achieve security in the IoT as these devices are vulnerable, and rarely configured in an appropriate way when installed; in this way, when they come into operation, they are highly exposed.

Technological advancement goes hand in hand with the existence of the human being, so that one cannot be conceived without the other. Thus the IoT has managed to penetrate in a remarkable way in society, which brings significant advantages, but at the same time, security is compromised. By having a hyper-connected society, risks related to cyber security appear [28]. However, its use is important and it is increasing in important sectors such as health, taking advantage of the ease of connection to the internet, but in the same way, patients are exposed to the interruption of the functioning of these devices, if they do not accept to pay a ransom [29].

In spite of everything, the devices that are part of the IoT are vulnerable, but they can be made less fragile if manufacturers, users, as well as those who install and configure the devices agree on the correct functionality of the system that makes up the IoT. The most important thing is to discover and identify vulnerabilities in order to schedule the patches, install them and constantly make the necessary updates, which in one way or another could minimize the risks.

Every day the number of devices that are connected increases and are important for the diversity of activities that take place in society, but in the same way it becomes an important tool for cybercriminals, for which it is estimated that the growth of attacks on IoT devices will increase exponentially, in the coming years, due to vulnerabilities [34].

The use of IoT devices in organizations is important, if they want to be successful, despite the dangers, and they must be aware of the vulnerabilities. Similarly, the appearance of a large number of devices brings difficulties to its users, because manufacturers are not taking responsibility for IoT security leaving opportunities to be exploited by cybercriminals. This will make it difficult to even minimize the risks, and

even more so when it is known that these devices contain vulnerabilities, which means that there is high exposure.

In conclusion, the devices that are part of the IoT are rarely patched or updated, which makes them vulnerable; therefore, other security measures should be considered [39], the probability of risk is very high because more than 90% have very sensitive information, as well as 70% with some vulnerability [40]. This risk is further increased as it is not possible to update a significant number of devices that are already part of the IoT. The most complex thing to understand is that the owners, in general, never find out that these devices are used to execute attacks [41]; in fact, it is a problem with no end: ransomware, WannaCry and now the confrontation of vulnerabilities in the IoT, to institutions such as health, which become the target of cybercriminals [42]. It is important to increase security, because every day more devices are connected to the network, which provides a service, but at the same time they are exposed to the pre-existence of vulnerabilities [43].

Based on the above, it is concluded that the vulnerabilities in the applications, services, and devices of the IoT, has become a point of access for cybercrime, up to compromising the security of important organizations, such as public services [46]. However, the situation is complex, since the ransomware of things or RoT, complicates it even more, by inviting cybercriminals to appropriate and control the devices and ask for a reward [47], which is so profitable for organizations dedicated to extortion have now been created by hackers [48].

Referencias

[1] E. V. Cruz, “E. Security,” 14 Noviembre 2016. [Online]. Available: http://revistaesecurity.com/edgar-vasquez-cruz-intel/.

[2] M. Á. Mendoza, “Welivesecurity,” 04 Enero 2018. [Online]. Available: https://www.welivesecurity.com/la-es/2018/01/04/maximo-historico-vulnerabilidades-2017/.

[3] G. Aldegani, “iT Sitio,” 17 Octubre 2017. [Online]. Available: https://www.itsitio.com/es/protocolo-wpa2-vulnerable-2/.

[4] Xalaka Colombia, 27 Marzo 2017. [Online]. Available: https://www.xataka.com/internet-of-things/continuan-los-hackeos-al-internet-de-las-cosas-el-nuevo-blanco-son-las-bombillas-inteligentes.

[5] J. P. Rey, " Texnoxplora," 08 Febrero 2018. [Online]. Available: http://www.lasexta.com/tecnologia-tecnoxplora/internet/cuatro-formas-hackear-casa-conectada_20161117582ee7200cf24c3ff697ebde.html.

[6] BBC, 17 Octubre 2017. [Online]. Available: https://www.bbc.com/mundo/noticias-41647662.

[7] C. SALZA, "C net MWC," 28 Febrero 2018. [Online]. Available: https://www.cnet.com/es/noticias/como-proteger-tu-casa-conectada/

[8] J. G. Fernández, "Expansión," 05 Febrero 2018. [Online]. Available: http://www.expansion.com/economia-digital/innovacion/2016/02/05/56b4e55622601de9508b463d.html.

[9] Semana, 02 Enero 2016. [Online]. Available: https://www.semana.com/tecnologia/articulo/los-riesgos-de-seguridad-de-la-internet-de-las-cosas/458935.

[10] Dirigentes Digital.Com, 21 Noviembre 2016. [Online]. Available: https://dirigentesdigital.com/hemeroteca/los_riesgos_del_internet_de_las_cosas-KEDD38950.

[11] I. V, " Androidpit," 04 Marzo 2017. [Online]. Available: https://www.androidpit.es/peligros-detras-internet-de-las-cosas-iot.

[12] M. S. Zavia, " Gizmodo," 28 Febrero 2017. [Online]. Available: https://es.gizmodo.com/detectan-medio-millon-de-dispositivos-facilmente-hackea-1792820284

[13] E. Arcos, "Hipertextual," 23 Octubre 2016. [Online]. Available: https://hipertextual.com/2016/10/mirai-ddos-internet-cosas.

[14] E. Security, 14 Marzo 2018. [Online]. Available: http://revistaesecurity.com/el-malware-mirai-omg-acecha-al-internet-de-las-cosas/.

[15] E. Editorial, " Reportedigital," 22 Junio 2016. [Online]. Available: https://reportedigital.com/iot/iot-superar-numero-telefonos-moviles/

[16] ESET Security Report Latinoamérica 2017, 2017. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf.

[17] Ciberamenazas y Tendencias Edición 2017 CCN-CERT I A-16/17, Junio 2017. [Online]. Available: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2224-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017/file.html.

[18] V. Vintegris, “Comunidad Vintegris,” 15 Mayo 2018. [Online]. Available: http://vintegris.info/internet-de-las-cosas-001/.

[19] Vintegris.info, “ Comunidadvintegris,” 23 Julio 2018. [Online]. Available: http://vintegris.info/iot-cuando-la-seguridad-es-propiedad-de-las-cosas/.

[20] OpenMind, 05 Diciembre 2016. [Online]. Available: HTTPS://WWW.BBVAOPENMIND.COM/UNA-LLAMADA-DE-ATENCION-PARA-INTERNET-DE-LAS-COSAS/.

[21] it DiGital Security, Octubre 2017. [Online]. Available: http://www.itdigitalsecurity.es/white-papers/content-download/7d061b42-bcd4-4d61-aa49-a9bc7cd753ff/it-digital-security-001.pdf.

[22] Microsoft, 20 Abril 2018. [Online]. Available: https://support.microsoft.com/es-us/help/960859/ms09-042-vulnerability-in-telnet-could-allow-remote-code-execution.

[23] P. Dubois., “DiarioTi.com,” 10 Abril 2018. [Online]. Available: https://diarioti.com/opinion-internet-de-las-cosas-y-la-seguridad-un-desafio-permanente/107111

[24] D. S. Espitia, “ Reportedigital,” 20 Julio 2018. [Online]. Available: https://reportedigital.com/iot/seguridad-en-internet-de-las-cosas-claves-proteger-grandes-empresas/.

[25] J. S. Onofre, “ El Economista,” 08 Julio 2017. [Online]. Available: https://www.eleconomista.com.mx/empresas/El-Internet-de-las-Cosas-y-sus-riesgos-entraran-sin-pedir-permiso-20170708-0022.html.

[26] secmotic, 31 Mayo 2016. [Online]. Available: https://secmotic.com/internet-de-las-cosas-seguridad/.

[27] Telefonica, 2015. [Online]. Available: https://www.telefonica.com/documents/23283/5538439/Telef%C3%B3nica_Security_IoT_Spanish.pdf/5137cc8e-e572-44c8-aecd-2f29f3f236be.

[28] MásQueNegocio, 26 Abril 2017. [Online]. Available: https://www.masquenegocio.com/2017/04/26/asegurar-internet-de-las-cosas/

[29] Canal Comstor, 13 Febrero 2018. [Online]. Available: https://blogmexico.comstor.com/la-implementacion-del-iot-en-el-sector-salud.

[30] Gerencia, Abril 2015. [Online]. Available: http://www.emb.cl/gerencia/articulo.mvc?xid=3688&sec=11.

[31] D. G. Aparicio, “20 minutos,” 12 Abril 2016. [Online]. Available: https://www.20minutos.es/noticia/2718504/0/hacking/internet-de-las-cosas/mundo-hacker/

[32] S. E. L. C. Karen Rose, “Internet Society,” 17 Abril 2018. [Online]. Available: https://www.internetsociety.org/es/resources/doc/2015/iot-overview.

[33] Bloggin Zenith, 12 Abril 2018. [Online]. Available: https://blogginzenith.zenithmedia.es/internet-de-las-cosas-en-2018/.

[34] R. TICbeat, “TICbeat,” 17 Abril 2018. [Online]. Available: http://www.ticbeat.com/seguridad/la-seguridad-sigue-siendo-el-punto-debil-del-internet-de-las-cosas/.

[35] Aruba a Hewlett Packard Enterprise Company, 2017. [Online]. Available: https://www.arubanetworks.com/es/soluciones/el-internet-de-las-cosas/.

[36] A. Casas, “Deloitte,” 2017. [Online]. Available: https://www2.deloitte.com/cr/es/pages/risk/articles/cuales-fueron-los-riesgos-tecnologicos-en-2017-y-que-se-espera-para-este-2018.html.

[37] redseguridad.com, 13 Diciembre 2017. [Online]. Available: http://www.redseguridad.com/que-leer/informes/trend-micro-preve-que-en-2018-los-ciberataques-dependeran-de-las-vulnerabilidades.

[38] TechTarget, “EducacionIT,” 09 Enero 2018. [Online]. Available: http://blog.educacionit.com/2018/01/09/desafios-de-seguridad-en-internet-de-las-cosas/.

[39] P. Dubois, “Search Data Center,” Julio 2018. [Online]. Available: https://searchdatacenter.techtarget.com/es/cronica/En-los-dispositivos-de-internet-de-las-cosas-la-seguridad-es-vital.

[40] J. M. S. Solance, “PublicaTIC,” 01 Diciembre 2015. [Online]. Available: https://blogs.deusto.es/master-informatica/network-connected-devices-internet-of-things-riesgos-parte-2-final/.

[41] E. Arcos, “Hipertextual,” 21 Julio 2017. [Online]. Available: https://hipertextual.com/2017/07/nuestro-futuro-cercano-que-internet-cosas-se-vuelve-peligroso.

[42] Intereconomia.COM, 09 Octubre 2017. [Online]. Available: https://intereconomia.com/tecnologia/los-dispositivos-inteligentes-utilizados-los-hospitales-objetivo-los-ciberdelincuentes-20171009-1127/.

[43] Viewnext, 04 Abril 2018. [Online]. Available: https://www.viewnext.com/principales-amenazas -en-seguridad-informatica-2018/.

[44] C. Vera-Cruz, "TechTarget," Diciembre 2017. [Online]. Available: https://searchdatacenter.techtarget.com/es/cronica/Amenazas-informaticas-que-acecharan-a-las-empresas-en-2018-y-que-hacer-frente-a-ellas.

[45] Deloitte, 2017. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/pa/Documents/technology/2017_TMT_PredictionsSpanish-Americas_Region.pdf.

[46] Internet Society, 17 Abril 2018. [Online]. Available: https://www.internetsociety.org/es/resources/2018/iot-security-for-policymakers/.

[47] A. N.-T. Stock, "TICbeat," 19 Diciembre 2016. [Online]. Available: http://www.ticbeat.com/seguridad/ransomware-de-las-cosas-2017-informe-eset/.

[48] J.Sanz,"redseguridad.com,"22Enero2018.[Online].Available:http://www.redseguridad.com/actualidad/info-tic/las-vulnerabilidades-en-internet-de-la-cosas-aumentaran-en-2018.

[49] Sotesa Informática y nuevas tecnologías, 25 Enero 2018. [Online]. Available: https://sotesa.com/ciberataques-2018-mas-ransomware-malware-movil/.

[50] D. JUSTO, "SER," 23 Abril 2018. [Online]. Available: http://cadenaser.com/ser/2018/04/22/ciencia/1524380027_984529.html.

[51] J. A. B. J. W. Y. R. M. José Custodio Najar Pacheco, "Vulnerabilities in the internet of things," *Vision electrónica,* vol. 13, nº 2, pp. 312 - 321, 2019. https://doi.org/10.14483/22484728.15163

[52] J. M. Díaz, "Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas," *Revista DelawareBioética y Derecho,* nº 46, pp. 85 - 100, 2019. https://doi.org/10.1344/rbd2019.0.27068

[53] J.M.M.EinarJhordanySernaValdivia,21Octubre2020.doi:10.1109/CIMPS52057.2020.9390153

[54] J. M. Díaz, "Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas," *Bioética y Derecho,* no. 46, pp. 85-100, 2019. doi: https://doi.org/10.1344/rbd2019.0.27068

[55] M. L. Ruilian Wangy, "Sistema de adquisición de información de fallas de equipos de potencia basado en Internet de las cosas.," *Revista EURASIP sobre redes y comunicaciones inalámbricas,* p. 65, 09 Marzo 2021. doi: https://doi.org/10.1186/s13638-021-01942-2

[56] Jezreel Mejía, Mirna Muñoz, Juan Martinez., "Análisis de seguridad de Internet de las cosas: una revisión sistemática de la literatura, 2016," *International Conference on Software Process Improvement (CIMPS),* pp. 1,6, 2016. doi: 10.1109 / CIMPS.2016.7802809