UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido
https://revistas.udistrital.edu.co/index.php/visele

VISIÓN ELECTRÓNICA
A CURRENT VISION

Vulnerabilities in the internet of things

Vulnerabilidades en el internet de las cosas

José Custodio Najar-Pacheco [1], ***John Alexander Bohada-Jaime*** [2], ***Wilmar Yovany Rojas-Moreno*** [3]

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Enviado: 26/03/2019
Recibido: 11/04/2019
Aceptado: 05/05/2019

Keywords:
Computer criminals
Cybercriminals
Devices
Internet of things
Sensors
Vulnerabilities

Palabras clave:
Delincuentes informáticos
Cibercriminales
Dispositivos
Internet de las cosas
Sensores
Vulnerabilidades

ABSTRACT

The Internet of Things has allowed the connection of a countless number of devices, which has facilitated control and even decision-making by them, but at the same time security vulnerabilities in operating systems, wireless security protocols, its applications, as well as the vulnerabilities in IoT, *acronym in English of Internet of Things*, devices, have allowed considerable sums of money to be paid to health institutions and patients for allowing the functionality of their equipment, according to security experts the world is facing a perfect storm which can allows attacks and system hijackings increasing in number, volume and gravity, since when adding more devices, they become access doors for intruders. However, it is important to be aware that everything that connects to the Internet is vulnerable; it has been demonstrated since birth, as well as the IoT.

RESUMEN

El Internet de las Cosas ha permitido la conexión de un sin número de dispositivos, lo cual ha facilitado el control y hasta la toma de decisiones por parte de estos, pero a la vez las vulnerabilidades en los sistemas operativos, los protocolos de seguridad inalámbricos, las aplicaciones, así como las vulnerabilidades en dispositivos del IoT, han permitido que se tengan que pagar considerables sumas de dinero, a instituciones de salud y pacientes por permitir la funcionalidad de sus equipos, según expertos en seguridad el mundo se encuentra delante de una tormenta perfecta para que los ataques y secuestros de sistemas escalen en volumen y gravedad, pues al agregar más dispositivos, se convierten en puertas de acceso para los intrusos, sin embargo es importante ser consiente que todo lo que se conecte a Internet es vulnerable, se ha demostrado desde su nacimiento, de igual forma lo es el IoT.

[1]BSc. In Systems Engineering, Universidad de Boyacá, Colombia. Specialist in telematics, Universidad de Boyacá, Colombia. Specialist in Telecommunications management, Universidad Central de Bogotá, Colombia. MSc. In Informatic Security, Universidad Internacional de la Rioja, España. Current position: Professor at Fundación Universitaria Juan de Castellanos, Colombia. E-mail: jnajar@jdc.edu.co

[2]BSc. In Systems Engineering, Universidad Incca de Colombia, Colombia. MSc. In Computer Sciences, Universidad Autónoma de Bucaramanga, Colombia. Ph.D. In Software Engineering, Universidad Politécnica de Cataluña, España. Current position: Professor at Fundación Universitaria Juan de Castellanos, Colombia. E-mail: jbohada@jdc.edu.co

[3]BSc. In Electronic Engineering, Universidad Incca de Colombia, Colombia. MSc. In Strategic Management in Telecommunications, Universidad Iberoamericana Internacional, Puerto Rico. Current position: Professor at Fundación Universitaria Juan de Castellanos, Colombia. E-mail: wrojas@jdc.edu.co

Citar este artículo como: J. C. Najar-Pacheco, J. A. Bohada-Jaime and W. Y. Rojas-Moreno, "Vulnerabilities in the internet of things", Visión electrónica, algo más que un estado sólido, vol. 13, no. 2, p.p. 312-321 july-december 2019,
https://doi.org/10.14483/22484728.15163

1. Introduction

The emergence of technology in various fields of the modern world, has made it easier to use it in different areas every day, consequently, due to its wide use, it has allowed a large number of electronic devices to be adapted in the same way, with the appearance and its increasingly smaller size as well as its costs, what is more significant is that progressively intelligent properties have been incorporated into the machines that, when configured with the Internet to carry out different activities, have become this way on the Internet of things (Internet of Things o IoT, by its acronym in English) [1].

In 2017, approximately 8.400 million devices were connected [2], since their use has been found in sectors such as entertainment, leisure, tourism and sports; nevertheless, the technology of connectivity is practically in everything that surrounds us and we coexist daily: traffic lights, bridges, foreign trade, banks and hospitals, in this case the most important and transcendental thing is the power to offer optimal connections that improve the speed of answer, since time is a critical component in this sector, so in the digital age of the internet of things (IoT), has led to the generalization of the Internet of Medical Things (IoMT), it is expected that by the year 2020, there will have a market value of 117 billion dollars, orienting itself to the consumer and its experience.

Likewise, it is estimated that for this same year there are more than 24 billion IoT devices connected to the global network; which will deliver important medical information to clinics and hospitals [3], the constant appearance of a number of digital instruments, has admitted the connection of these easily to the Internet, currently finding millions of digital devices connected, so you can talk about the Internet of things or Internet of all (Internet of things, hereinafter IoT) [4], every day new devices are being added, so that it can be said in reality that the Internet of things, is understood as a conglomerate of mobile devices and control with access to Internet [5].

Similarly, in the commercial part, the most important thing is to be able to interact with the client, obtaining quality, productivity and reliability, while achieving cost reduction [6], and the most important thing for any organization is that they know it by any means in this case on the Internet because .As Bill Gates says: A company that is not on the Internet, does not exist [7], since it is the only way that these organizations survive and continue in a competitive market, which demands investment, but at the same time they identify themselves, because they allow to be known anywhere in the world [8].

There is also the concern, as it is known the latest operating systems, apparently still have a significant number of vulnerabilities, which are exploited by computer criminals [9], likewise with vulnerabilities in security protocols, exposing organizations, as they are highly exposed to being attacked by cybercriminals organizations, since they are allowed to create accounts as administrator, thus taking control [10], vulnerabilities that become opportunities to benefit the cybercriminals who do not forgive, some organizations assume this problem of these operating systems in a responsible manner, thus creating new versions or updates to provide a solution continuously [9], the same happens with some devices that are part of the internet of things, they are vulnerable, because research conducted according to Avast have declared that more than half a million smart devices, among which are webcams, through which privacy is violated, in addition to monitors for babies, are vulnerable to cyber-attacks [11].

The IoT is not far, as some think, absolutely everything will be connected to the network of networks, mostly what we use daily and more frequently: tablets, smartphones, computers, televisions, also refrigerators, coffee makers, garage doors, among others and even toothbrushes, it is expected that by 2020 250 objects will be connected every second, which will be able to make decisions [12]. ¿But do you know that the Internet is vulnerable? and it continues to be above all with its wireless security protocols in its systems [13], so that security or security can be thinking, then adding vulnerabilities to more vulnerabilities, as well as has been established, no application is safe, according to the organizations dedicated to security and involved in the development of the OWASP Top 10, 77 % of applications have at least one security flaw [14].

Likewise mobile devices, probably due to the massive use, are becoming more vulnerable and insecure every day [15], because they are made up of hardware components that must respond to different wireless technologies, so when running a complex operating system and a large number of wireless applications which demand high computing power, significantly increasing vulnerabilities, this way these devices are exposed, which means greater complexity of the operating system, greater vulnerability in mobile devices [16], There is a responsibility of device manufacturers to not apply norms or industry standards, as well as the risk that

business platforms will be found to be vulnerable, thus giving the opportunity to cybercriminals, so they can commit a crime, Trend Micro predicts an increase in Internet of Things (IoT) vulnerabilities, as there is an increase in these insecure devices [17].

As a matter of fact, Cybercrime has been found in this activity, a way of life, because significant gains are obtained, for the next few years it will be nothing satisfactory, thinking that they will point to an organization in an industrial internet environment of things (IIoT), to a ransomware attack that will interrupt operations and affect the production line [18]. Even so, the number of devices and services will continue to increase, so much that it now exceeds the human population on Earth [19].

Also some vulnerabilities in TCP/IP could support the denial of service [20], likewise TCP/IP could allow elevation of privileges [21], every day vulnerabilities continue to be found in different operating systems in TCP/IP [22], this as regards the ipv4 protocol, as well as the protocol that allows the almost unlimited interconnection of any IPv6 object, is worrisome since vulnerabilities have been detected in the IPv6 TCP/IP protocol, due to which it could cause a condition of denial of service [23], according to the security bulletin of the manufacturer of these operating systems.

Of course it is important to highlight that the IoT brings important advantages, but also risks, likewise it opens an extensive field of technological devices exposed to cyber-attacks [24], what is alarming is that the Internet of Things ïs an innovative dimension that is taking society along the path of digitalization, offering the probability of changing the direction of our daily and work life" [25], as a result of which technological transformation demands it and is opening up a number of new opportunities and challenges for health sector organizations, researchers, doctors and patients, among many others [5], thus the IoT has begun to be part of the normal life of society. In the health sector, its use is greater, but in the same way cyber-attacks on health systems in the world, to pay considerable sums of money, this time not only by ransomware in a hospital in North America [26], likewise the attackers endanger the lives of the sick, by controlling pacemakers or insulin pumps, among other instruments and blackmailing the patient through the intimidation of torpedoing their normal functioning [27], Likewise, DDoS attacks per day and the cost to an organization can range between 14,000 and 2.35 million dollars per incident, and approximately three quarters of all global brands, organizations and companies (73 %) have been victims of a DDoS attack [28].

2. Vulnerabilities on the internet of things

The constant appearance of technology and its applications in different fields of the modern world, has made it easier to use it in many different areas every day, so the important thing is to adapt to them, consequently, due to its wide use, it has forced that a number of electronic devices are adapted in the same way, which has allowed them to appear continuously and their size each day is smaller in the same way as their costs, the most important thing is that progressively they have been incorporated intelligent properties to the machines that when configured with the Internet to carry out different activities, has thus become the Internet of Things (IoT) [1], by the end of 2017, approximately 8,400 million devices were connected [2], and their growth will be growing every day, as do sectors such as entertainment, leisure, tourism and sports; nevertheless, the technology of connectivity is practically in everything that surrounds us and we coexist daily: traffic lights, bridges, foreign trade, banks and hospitals which concern, to assist patients as well as offer experiences that improve their physical and emotional state, as well as proposing better care for a large number of patients, the most transcendental to provide optimal connections that improve the speed of response, since time is a critical component in this sector, as well as in the digital age of Internet of Things (IoT), has led to the generalization of the Internet of Medical Things (IoMT), it is expected that by the year 2020 it will have a market value of 117 billion dollars, focusing on the consumer and his experience. At the same time, it is estimated that for this same year there are more than 24 billion IoT devices connected to the network of networks; which will provide important medical information to clinics and hospitals [3], the constant appearance of a number of digital instruments, has also allowed the connection of these easily to the Internet, currently finding billions of digital devices connected, for which indeed, you can talk about the Internet of things or Internet of everything (Internet of things, hereinafter IoT) [4] and every day are growing at an accelerated pace with new devices that are being added, so which can be said in reality that the Internet of things, is understood as a conglomerate of mobile devices and control with access to the Internet [5].

The internet of things is one of the transformative preferences that will shape the future of commercial activity, which is why many organizations see opportunities to interact with the client, achieving quality, productivity and reliability, while achieving cost reduction [6], because the most important thing for any

organization is that they constitute by themselves as a well- known organization by any means, in this case on the Internet, as Bill Gates says: .A company that is not on the Internet, does not exist" [7], since it is the only way that these organizations survive and continue in a competitive market, which demands investment, but at the same time they identify themselves, because they allow being renowned anywhere in the world [8].

However, operating systems are constituted in the soul, because they allow the functionality of a certain number of devices in this case computers, and there is a concern because the latest operating systems, apparently still have a significant number of vulnerabilities, which are exploited by computer criminals [9], likewise these systems, have vulnerabilities in the security protocols, in such way that they compromise the security of the organizations, since they are highly exposed to being attacked by cybercriminal organizations at any moment, since they are allowed to create accounts as an administrator, thus taking control [10], other important vulnerabilities that the different operating systems have and different versions that have not yet been identified are present, which are identified can receive a solution at some time, but the ones that cannot receive the solution is a thought problem, as you can see is a very complex problem and surely has always been present and will continue forever. There are vulnerabilities that become opportunities to benefit the cybercriminals who do not skip any chance to attack, some organizations assume this problem of these operating systems in a responsible way, thus create new versions or updates to provide a solution continuously [9].

Additionally, some devices that are part of the Internet of things, are vulnerable, because some researches carried out by Avast have declared that more than half a million of smart devices, among which are webcams, through which privacy is violated, in addition to monitors for babies, they are vulnerable to cyberattacks [11], so they are at risk and will surely continue for a long time until they are given a solution and the most complicated thing is that they are increasing. However, many organizations see great opportunities in the uses of the Internet of Things (IoT), and some companies trust in the IoT, which promise to improve customer relations and boost business growth by improving quality, productivity and reliability and, on the other, reducing costs [6].

The future for the IoT is not far, as is the perception of someone, absolutely everything will be connected to the network of networks, most of which we use daily and more often, but not only those devices that we imagine because we know them , like tablets, smartphones, computers and televisions, but also refrigerators, coffee makers, garage doors, among others and even toothbrushes will be connected, it is expected that by 2020 250 objects will be connected every second, which obviously, they will have ability to make decisions [12]. From any perspective it sounds very important and unbelievable, because they make the right decisions for us, but the million-dollar question comes from, if we know that the Internet is vulnerable? and it continues to be above all with its wireless security protocols in their systems [13], so that what kind of security can be considered, since it would be adding vulnerabilities to more vulnerabilities, as well as it has been established, no application is safe. According to organizations dedicated to security and involved in the development of the OWASP (Open Web Application Security Project) Top 10, 77 % of applications have at least one security flaw [14], which makes them vulnerable and even more fragile when they are more used, knowing as reported that a considerable number in the iOS App Store, are not safe enough [29], of course is also presented, according to the research laboratory of ESET Latin America, insecure applications that spread among Android users by several reasons, finding recently in Latin America, some countries affected by these applications in more than 50 % [30].

As we can see, the mobile devices, due to their massive use, are becoming more vulnerable and insecure every day [15], because they are made up of hardware components that must respond to different wireless technologies, thus, when executing a complex operating system and a large number of wireless applications which demand high computing capacity, significantly are increasing vulnerabilities, in this way these devices are exposed, which means that the higher the complexity of the operating system, the greater the vulnerability in the mobile devices [16], likewise the so-called "most famous operating systems in the world", and therefore more used, for the same reasons, in mobile devices today, are increasingly insecure and are increasing, until losing reliability, hence benefiting cybercriminals who obtain great profits [31], as showed the report of the Research Laboratory of ESET Latin America 2017.

Due to this, there is great concern, because every day there are more devices and technology, which leads to great challenges, such as how to maintain the security of information, by both users and manufacturers, as the devices that are part of the internet of things are being infected and will surely continue to do so as they evolve, since mobile operating systems and applications are vulnerable, as is related in ESET in its report on

the 2017 trends: "Security as a hostage" [32], likewise, there is responsibility on the part of the manufacturers of devices that do not apply the norms nor the standards of the industry, as well as the risk in which the business platforms will be found to be vulnerable, thus giving the opportunity to the cybercriminals, In order to be able to commit crimes, Trend Micro predicts an increase in the vulnerabilities of the Internet of Things (IoT), because of the increasing in these insecure devices [17], consequently we see the use that exists for the increase of the IoT, in that way increasing the demand by the manufacturers of these devices, because they are not interested in the security conditions, but the reduction of costs in order to have a bigger market, with this view is hardly to think that there can be privacy and security, since these vulnerabilities are exploited by hackers, for example those that exist in the transmission of data through the network of networks [33].

Nevertheless, the organizations dedicated to cybercrime, have found in this activity, a way of life, so that every day they improve their actions, for example using extortion, since very generous profits are obtained, so for the next years it will not be nothing satisfactory in the way that we think that they will point to an organization in an industrial internet environment of things (IIoT), for a ransomware attack that will interrupt operations and affect the production line [18].

The real warning is that, as the use of the internet of things increases, so does insecurity, which translates into risks, but still is used in an important way, for the year 2017, according to the report by Gartner, the number of connected devices became greater than the world population, despite HP demonstrating that 70 % of IoT devices which are commonly used have some type of security vulnerability [34].

Therefore, it should not be neglected, that the Internet of things represents a threat to consumers, due to inadequate regulations that affect their safety and use. However, the number of devices and services will continue to increase, so much that currently exceeds the human population on Earth [19], the lack and absence of norms, necessary for the regulation, standardization and application of security measures related to the Internet of things, is due in one way or another to the rapid growth, so much so the few that exist are quickly obsolete [35]. Equally important and interesting is the internet of things, since in one way or another it brings great benefits in the daily life of its users, but at the same time it is necessary to be aware that it must coexist with the risks, which must be evaluated and analyzed to avoid surprises, given that in some opportunities these devices do not have the necessary protection security, they are highly exposed to cyberattacks, due to vulnerabilities [36].

As it is well-known the internet of things, refers to the set of devices using sensors and actuators incorporated in physical objects linked through wired and wireless networks, for its operation it is necessary to use the TCP-IP protocol, in order to connect to the Internet [37], therefore it is very important, since it allows the connection of a large number of devices taking advantage of the internet, but the question arises, is sufficient the addressing offered by the current ipv4 protocol?, thus is important the transition to Ipv6, which will allow almost unlimited interconnection of any object and the evolution and implementation of the Internet of Things [38], which from every point of view is interesting, since there is control of a large number of devices connected through the Internet, but in the same way it is known that operating systems have vulnerabilities in security protocols.

On the other hand, to enable the cybercriminals to create administrator accounts and take control [39], some vulnerabilities in TCP/IP could allow denial of service [20], likewise TCP/IP could support the elevation of privileges [21], and vulnerabilities continue to be discovered every day in different operating systems in TCP/IP [22], this concerning the ipv4 protocol, now if we look at the protocol that allows the almost unlimited interconnection IPv6, it is overwhelming since vulnerabilities have been detected in the TCP/IP protocol of IPv6, due to it could cause a denial condition of service [23], according to the security bulletin of the manufacturer of these operating systems.

It is also very important to emphasize, that you must be aware, that everything that has an Internet connection is vulnerable, is what has been demonstrated since the birth of computer science and the Internet, first were viruses, then the hacking of the systems to alter the protocols and recently the alteration of the protocols, theft, information and device hijacking with the ransomware is shown, responsibility that is attributed directly on the users and the companies that manufacture the devices that are part of the internet of things (IoT) [40], it is also important to highlight that the IoT brings advantages, but also carries risks, likewise it opens an extensive field of technological devices exposed to cyberattacks [24].

Although, unquestionably any device that connects to the Internet will be highly exposed, first because many times these are vulnerable and secondly because the systems that allow the Internet connection in the

same way are vulnerable, so that there is a lack of security, and the most troublesome is that the Internet of Things ïs an innovative dimension that is taking society along the path of digitalization, offering the possibility of changing the course of our daily and work life" [25], since most important technological changes require it and are opening up a number of new opportunities and challenges for health institutions, researchers, doctors and patients, among many others [5], so the IoT has begun to be part of daily life of the society where they become part:

Smart homes, intelligent education, smart health surveillance, wearable devices (Set of electronic devices that are incorporated in some part of our body interacting continuously with the user and with other devices in order to perform some concrete function, smart watches, sneakers with built-in GPS and wristbands that control our state of health), the Internet of Vehicles (IoV), among others [41]. What from any point of view it is important and interesting but the reality is that security is compromised before the existence of vulnerabilities in the devices, applications, interconnection devices and where the information is transmitted, even more so the oversights and non-application of minimum security standards by users [42].

Yet, it is important to highlight the great benefits that the use of the Internet of things brings, in this case in the institutions that provide health services, whose implementation is increasing, but in the same way, cyberattacks on health systems are increasing too in a worldwide scale until having to pay considerable sums of money, this time not only for ransomware in a hospital in North America [26], of course "The Internet of things can revolutionize the medical industry, but it can also be an open invitation to cybercriminals who want to blackmail hospitals and patients, steal data and cause real harm", according to Check Point, because it is a very complicated problem the services provided by the professionals of personalized quickly treatment to patients and from considerable distances, which becomes very important because it can go so far as to save lives, even the vulnerabilities in the Internet of Things can allow the attackers to endanger the lives of patients, by taking control of pacemakers or insulin pumps, among other devices and blackmailing the patient through the threat of impeding their normal functioning [27].

What it means in a certain way, that what brings benefits, must take risks by having the Internet of things. It can be mentioned that there is a direct proportionality to a greater amount of devices connected to the internet higher risks, as stated by Derek Manky, expert in computer security the world is facing a perfect storm which can allows attacks and system hijackings increasing in number, volume and gravity as we have more devices connected to the internet, for instance baby monitors or insulin pumps inserted into the patient which become access doors for intruders [43].

Actually, it is a very complicated problem and a risk for patients in that case, of course it is important to emphasize or highlight that the Internet of Things every day penetrates more into modern society, with the appearance of more connected devices that are becoming part of our daily lives with the internet, and at the same time these devices connected with others that perform tasks that humans used to do. This constitutes a revolution and a step forward technologically speaking, but in the same way puts itself at risk, because according to experts in security, thousands of devices affected by an IoT vulnerability have been detected, allowing the execution of malicious code remotely [44], surely these vulnerabilities have already been corrected, but while they were discovered what else could have happened.

The internet of things every day takes more confidence in daily life, so much so that it makes possible the creation of smart homes, by facilitating the connection of devices to the network, but in the same way the risks must also be assumed, since sometimes is presented the non- application of the security requirements in the manufacture, so the cybercriminals exploit these vulnerabilities to commit fraudulent actions, which can lead to their house being controlled by the attackers [45], in the same way it is important to emphasize that facilitating, more and more the connection of devices to the internet, also provides greater comfort to its users and / or consumers which is very significant, but at the same time must be aware of the new risks that may occur as a result of susceptibility of these devices and the information contained therein, when they are used by hackers with bad intentions [46], it is also important to note that every day, online threats are greater, and they continue to increase in the same way as the internet grows, when SQL injections, DDos attacks or attacks via Cross-Site-Scripting (XSS) and Brute Force are presented, as well as the dangers of malware as viruses, worms, Trojans and spyware among many others, as we see is a problem too complex related to security and one of the most important threats related to the Internet of Things (IoT), is that every day is increasing the number of connected devices and in the same way cybercriminals will have more opportunity to have a larger number of gateways for their malware and their attacks, since marketing is more important than

security [47].

And every time it is increasing, because the Distributed Denial of Service attacks of the Internet of Things (DDoS of Things or DoT), every day is becoming more critical, suffering attacks on thousands of devices from service providers, gaming companies to entertainment media companies, since they have carried out a large number of DDoS attacks per day and the cost to an organization can range between 14,000 and 2.35 million dollars per incident, as well as approximately three quarters of all global brands, organizations and companies (73 %), have been victims of a DDoS attack [28].

Above all, the Internet of Things or IoT, is very vulnerable to cyberattacks, therefore hackers have demonstrated the ease with which they can be hacked, for example the smart bulbs that once a virus has been infected, this is responsible for dispersing the malicious firmware throughout the network, causing a number of difficulties [48]. So once again the security on the internet and the internet of things is exposed.

3. Conclusions

Internet has always become an important tool for the functionality of daily life of modern society, banking, commerce, industry, medicine, private and state organizations, accomplish their own activities with the use of the Internet, even a company that is not on the Internet, does not exist [7], as Bill Gates says.

Which is important and interesting, allowing the connection of a large number of devices, using sensors and actuators incorporated in physical objects linked through wired and wireless networks, using the TCP-IP protocol to connect them [37], and at the same time the ipv6 to allow the almost unlimited connection of any object and the evolution and implementation of the Internet of Things [38], but we are aware of the vulnerabilities that operating systems have, in security protocols, which has allowed cybercriminals to create administrator accounts and take control [39], as well as vulnerabilities in TCP/IP that allow denial of service [20], accept the elevation of privileges [21], besides the different vulnerabilities in others operating systems in TCP/IP [22].

As online threats increasing every day and continue to increase, as internet does, when presenting SQL injections, DDos attacks or attacks via Cross-Site-Scripting (XSS) and Brute Force, as well as the dangers of Malware such as viruses, worms, Trojans and spyware among many others, in addition to the important threats related to the Internet of Things (IoT), which are increasing by connecting more devices every day, giving opportunities for cybercriminals to have a large number of gateways to their malware and their attacks, since marketing is more important than security [46].

However, the worrying thing is the increase in Distributed Denial of Service attacks of the Internet of Things (DDoS of Things or DoT), and every day is suffered thousands of attacks on devices which aim service providers such as gaming companies and entertainment media companies, since they have received a large number of DDoS attacks per day and the cost to an organization can range between 14,000 and 2.35 million dollars per incident, as well as approximately three quarters of all global brands, organizations and companies (73 %), have been victims of a DDoS attack [47].

The internet of things has shown that every day is more vulnerable to cyberattacks, which has facilitated hackers the hacking of smart bulbs that once one has been infected, this is responsible for dispersing the malicious firmware in the entire network, causing a number of difficulties [28].

Even so, their use is greater every day, for 2017 around a million devices [2] were found, connected and their growth is increasing when they are used in sectors such as entertainment, leisure, tourism and sports; nevertheless, the technology of connectivity is practically in everything that surrounds us: traffic lights, bridges, foreign trade, banks and hospitals. Regarding hospitals its mission is to take care of patients not only in the basic sanitary aspect, but also to offer experiences that improve their physical and emotional state, making efficient processes to provide better care to a greater number of patients and offer optimal connections that improve the speed of response, since time is a critical factor in the sector, as well in the digital age of the IoT has led to the conceptualization of the Internet of Medical Things (IoMT), it is expected that by the year 2020 it will have a market value of 117 billion dollars, focusing on the consumer and his experience. Likewise, it is expected that by 2020 there will be more than 24 billion IoT devices connected to the network of networks; which will provide medical data to clinics and hospitals [3], the constant appearance of a number of digital devices, has also allowed the connection of these easily to the Internet, currently finding billions of digital devices connected. Indeed, we can talk about the Internet of things or Internet of everything (Internet of things, hereinafter IoT) [4] and every day they are

increasing at an accelerated rate with new devices that are being added, which is why we could support that the Internet of things, is understood as a conglomerate of mobile devices and control with access to the Internet [5]. But the devices that are part of the internet of things, are vulnerable, because researches carried out by Avast have revealed that more than half a million smart devices, including webcams and monitors for babies, are vulnerable to cyberattacks [11].

In the meantime, one of the great beneficiaries of the use of the internet of things is the health sector, in hospitals whose use is increasing but in the same way, cyberattacks too. On health systems attacks are increasing throughout the world, until they have to pay considerable sums of money, this time not only because of ransomware in a hospital in North America [42]. Of course "The Internet of things can revolutionize the medical industry, but in the same way can be an open invitation to cybercriminals who want to blackmail to hospitals and patients, steal data and cause real harm", because it is a very complicated problem the services provided by the professionals of personalized quickly treatment to patients and from considerable distances, which becomes very important because it can go so far as to save lives, even the vulnerabilities in the Internet of Things can allow the attackers to endanger the lives of patients, by taking control of pacemakers or insulin pumps, among other devices and blackmailing the patient through the threat of impeding their normal functioning [26], and it is expected for the next few years to target ransomware attacks that will interrupt operations and affect the production line [18], this is due in part to the irresponsibility in manufacturing because of the non-application of industry norms and standards, when there is an increase in the use of these unsafe devices [17], it is intended to take advantage of a market, where the security conditions are not so important but the reduction of costs to be able to have more supply, thus there can hardly be privacy and security, since these vulnerabilities are exploited by hackers [33].

References

[1] E. V. Cruz, "Intel security", 2016. [Online]. Available at: http://revistaesecurity.com/edgar-vasquez-cruz-intel/

[2] C. F. Caballero, "8.400 millones de dispositivos estarán conectados a Internet a finales de 2017", 2017. [Online]. Available at: https://blogthinkbig.com/8-400-millones-de-dispositivos-estaran-conectados-a-internet-a-finales-de-2017

[3] Corporación Colombia Digital, "2020: Internet de las Cosas Médicas", 2017. [Online]. Available at: https://colombiadigital.net/actualidad/noticias/item/9611-2020-internet-de-las-cosas-medicas.html

[4] J. A. Arévalo, "El internet de las cosas", Desiderata, no. 1, 2016, pp. 24-25.

[5] JVABAD, "El internet de las cosas (IoT) y su aplicación en los servicios de salud", 2015. [Online]. Available at: https://hablandoesalud.wordpress.com/2015/07/20/el-internet-de-las-cosas-iot-y-su-aplicacion-en-los-servicios-de-salud/

[6] A. Banafa, "7 tendencias de Internet de las cosas en 2017", 2016. [Online]. Available at: https://www.bbvaopenmind.com/7-tendencias-de-internet-de-las-cosas-en-2017/

[7] J. de Iruarrizaga, "La mitad de los españoles aún no hace compras en Internet por desconfianza", 2017. [Online]. Available at: http://www.ideal.es/tecnologia/internet/mitad-espanoles-compras-20171219232550-ntrc.html

[8] J. J. Cano M., "Computación forense: Descubriendo los rastros informáticos", México: Alfa omega Grupo Editor, 2009.

[9] T. Z. Ghiorzoe, "Lanzamiento de actualización de seguridad de Microsoft de febrero de 2018", 2018. [Online]. Available at: https://blogs.technet.microsoft.com/seguridad/2018/02/13/lanzamiento-de-actualizacion-de-seguridad-de-microsoft-de-febrero-de-2018/

[10] C. González, "Descubren dos agujeros en los protocolos de seguridad de Windows", 2017. [Online]. Available at: https://www.adslzone.net/2017/07/12/descubren-dos-agujeros-en-los-protocolos-de-seguridad-de-windows/

[11] A. Soriano Grande, "Las debilidades del Internet de las Cosas ponen en riesgo de ataque a las webcams [Infografía]", 2017. [Online]. Available at: https://blog.avast.com/es/las-debilidades-del-internet-de-las-cosas-ponen-en-riesgo-de-ataque-a-las-webcams-infografia

[12] M. O. Domènech, "Seguridad en el Internet de las Cosas (IoT)", 2017. [Online]. Available

at: http://www.iniseg.es/blog/ciberseguridad/seguridad-en-el-internet-de-las-cosas-iot/

[13] M. D. Adés, "REDES WIFI EN ALERTA: Vulnerabilidad en el protocolo de seguridad WPA/WPA2", 2017. [Online]. Available at: https://equipoantiransom.com/2017/10/19/redes-wifi-en-alerta-vulnerabilidad-en-el-\protocolo-de-seguridad-wpawpa2/

[14] J. D. Peláez and A. Diez, "OWASP publica el Top 10 – 2017 de Riesgos de Seguridad en Aplicaciones Web", 2017. [Online]. Available at: https://www.certsi.es/blog/owasp-publica-el-top-10-2017-riesgos-seguri\dad-aplicaciones-web

[15] D. G. Bilić, "¿Son los teléfonos móviles inseguros por naturaleza?", 2018. [Online]. Available at: https://www.welivesecurity.com/la-es/2018/01/11/telefonos-moviles-inseguros-por-naturaleza/

[16] M. D. Prieto, "Seguridad en dispositivos móviles", 2017. [Online]. Available at: https://www.freelibros.org/programacion/seguridad-en-dispositivos-moviles-marc-domi\ngo-prieto.html

[17] Blog Trend Micro, "Trend Micro prevé que en 2018 los ciberataques dependerán de las vulnerabilidades", 2017. [Online]. Available at: http://blog.trendmicro.es/?p=3248

[18] Trend Micro, "Security Predictions for 2018 Paradigm Shifts", 2017. [Online]. Available at: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018?_ga=2.49298918.155634577.1519693573-201788053.1518233601

[19] F-Secure, "Alerta: Ya es hora de asegurar el Internet de las cosas", 2018. [Online]. Available at: https://blog.f-secure.com/es/alerta-ya-es-hora-de-asegurar-el-internet-\de-las-cosas/

[20] Microsoft, "Boletín de seguridad de Microsoft MS13-018 - Importante", 2017. [Online]. Available at: https://docs.microsoft.com/es-es/security-updates/securitybulletins/2013/ms13-018

[21] Microsoft, "Microsoft Security Bulletin MS14-070 - Important", 2017. [Online]. Available at: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2014/ms14-070

[22] E. Medina, "Hallada una vulnerabilidad en la implementación de TCP en Linux", 2016. [Online]. Available at: https://www.muyseguridad.net/2016/08/12/vulnerabilidad-tcp-linux-android/

[23] Microsoft, "Microsoft Security Response Center", 2014. [Online]. Available at: https://technet.microsoft.com/es-es/library/security/ms14-006.aspx

[24] S. D. Limia, "¿Cómo influye el Internet de las cosas en nuestra vida?", 2017. [Online]. Available at: https://es.semrush.com/blog/iot-internet-cosas-influencia/

[25] S. Alestra, "Vulnerabilidades del Internet de las Cosas", 2017. [Online]. Available at: https://blog.alestra.com.mx/vulnerabilidades-del-internet-de-las-cosas

[26] J. L. Becerra Pozas, "IoT en hospitales, un objetivo para la ciberdelincuencia", 2017. [Online]. Available at: http://cio.com.mx/iot-en-hospitales-objetivo-la-ciberdelincu\encia/

[27] CSO España Computerworld, "IoT en hospitales, uno de los grandes objetivos de los ciberdelincuentes", 2017. [Online]. Available at: http://cso.computerworld.es/alertas/iot-en-hospitales-uno-de-los-grandes-objeti\vos-de-los-ciberdelincuentes

[28] Seguridad UNAM, "Registran aumento de ataques DDoS en IoT", 2017. [Online]. Available at: https://www.seguridad.unam.mx/registran-aumento-de-ataques-ddos-en-iot

[29] M. Hernández, "Las aplicaciones más populares son también las más inseguras", 2017. [Online]. Available at: https://www.actualidadiphone.com/las-apps-mas-populares-tambien-las-mas-inse\guras/

[30] D. G. Bilić, "Aplicaciones inseguras se propagan entre usuarios de Android", 2018. [Online]. Available at: https://www.welivesecurity.com/la-es/2018/03/02/aplicaciones-inseguras-propagan-usuarios-an\droid/

[31] Dinero, "Sistemas operativos iOS y Android se volvieron menos confiables en el 2017", 2018. [Online]. Available at: http://www.dinero.com/empresas/articulo/ios-y-android-tuvieron-mas-vulnerabilidades-\durante-el-2017/253771

[32] Asociación Colombiana de Ingenieros de Sistemas, "ESET lanza su informe sobre las tendencias 2017: La seguridad como rehén", 2016. [Online]. Available at: http://acis.org.co/portal/content/eset-lanza-su-informe-sobre-las-tendencias-\2017-%E2%80%9Cla-seguridad-como-reh%C3%A9n%E2%80%9D

[33] Instituto de Auditores Internos de Argentina, "Internet de las cosas (IOT), Riesgos y Oportunidades emergentes en Seguros", 2016. [Online]. Available at: https://iaia.org.ar/internet-de-las-cosas/

[34] INFOTECHNOLOGY, "Desafíos de seguridad en internet de las cosas", 2018. [Online]. Available at: http://www.infotechnology.com/online/Desafios-de-Seguridad-en-Internet-de-las-Co\sas-20180108-0010.html

[35] Telefonica, "Alcance, escala y riesgo sin precedentes: Asegurar el internet de las cosas", 2015. [Online]. Available at: https://www.telefonica.com/documents/23283/5538439/Telef%C3%B3nica_Security_IoT_Spanish.pdf/5137cc8e-e572-44c8-aecd-2f29f3f236be

[36] Reporte Digital, "Seguridad: el lado más vulnerable del Internet de las Cosas", 2016. [Online]. Available at: http://reportedigital.com/iot/seguridad-vulnerable-internet-cosas/

[37] R. Vega, "Por qué el internet de las cosas se llama así y otras definiciones", 2016. [Online]. Available at: https://ricveal.com/blog/llamamos-internet-las-\cosas-al-internet-las-cosas-otras-definicio\nes/

[38] Domo Desk, "A fondo: ¿qué es iot (el internet de las cosas)?", 2014. [Online]. Available at: http://www.domodesk.com/221-a-fondo-que-es-iot-el-internet-de-las-\cosas.html

[39] C. González, "Descubren dos agujeros en los protocolos de seguridad de Windows", 2017. [Online]. Available at: https://www.adslzone.net/2017/07/12/descubren-dos-agujeros-en-los-protocolos-de\-seguridad-de-windows/

[40] S. Ospina, "¿Qué es el ransomware de las cosas y cómo nos afecta?", 2017. [Online]. Available at: http://www.enter.co/chips-bits/seguridad/ransomware-de-las-cosas-como-nos-afecta/

[41] M. Puente García, "Riesgos y retos de ciberseguridad y privacidad en IoT", 2017. [Online]. Available at: https://www.certsi.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad\-iot

[42] C. García Vega, "Vulnerabilidad del Internet de las Cosas", 2016. [Online]. Available at: https://delitosinformaticos.com/01/2016/seguridad-informatica/vulnerabilidad-del-internet-de-las-cosas

[43] T. Z. Ghiorzoe, "Los beneficios del Internet de las Cosas, la conectividad abre la puerta a intrusos", 2017. [Online]. Available at: https://blogs.technet.microsoft.com/seguridad/2017/06/19/los-beneficios-del-internet-de-las-cosas-\la-conectividad-abre-la-puerta-a-intrusos/

[44] N. Rodríguez, "Miles de aparatos afectados por una vulnerabilidad del IoT", 2017. [Online]. Available at: https://www.solvetic.com/page/recopilaciones/s/internet/miles-de-aparatos-afectados-por-vulnerabili\dad-del-iot

[45] El Tiempo, "Su casa controlada por cibercriminales: riesgos del hogar inteligente", 2018. [Online]. Available at: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/los-riesgos-de-los-hogares-inteligentes-y-\el-internet-de-las-cosas-188100

[46] V. Murgich, "Los riesgos del iot y cómo evitarlos", 2016. [Online]. Available at: https://www.merca20.com/los-riesgos-del-iot-evitarlos/

[47] D. Doll, "Seguridad online en 2018: El Internet de las Cosas esconde grandes riesgos potenciales", 2018. [Online]. Available at: http://www.itdigitalsecurity.es/opinion/2018/01/seguridad-online-en-2018-el-internet-de-las\protect\discretionary{\char\hyphenchar\font}{}{}cosas-esconde-grandes-riesgos-pote\nciales

[48] A. Moreno, "Bombillas inteligentes, el objetivo de los hackers", 2016. [Online]. Available at: https://voltaico.lavozdegalicia.es/2016/11/bombillas-inteligentes-objetivo-hackers/