Universidad Autónoma de San Luis Potosí
Facultad de Ingeniería
Centro de Investigación y Estudios de Posgrado

Cyberattacks study on healthcare devices using Internet of Things technologies

Para obtener el grado de:
Maestría en Ingeniería de la Computación

Presenta:
Mauricio Jacobo González González

Asesor:
Dra. Alejandra Guadalupe Silva Trujillo

San Luis Potosi, S. L. P. Agosto de 2022

Abstract

Science has had great advances in different branches that have managed to connect people with new technological devices to simplify different tasks. The technologies of the Internet of Things (IoT) have grown. We have surrounded ourselves with devices, making them an essential part of our lives. In this way, they store an enormous amount of personal information. This information could be our health records. Cyber attackers recognize the opportunity that these represent, and they will try to exploit their vulnerabilities. Having secure devices and therefore protecting our privacy continues to be a growing issue. For these reasons, this project's mission is to find a way to protect these appliances against diverse threats in existence. We highlight the common attacks on IoT medical devices and propose solutions that will help to protect them, focusing on wearable technologies that are growing quickly to improve medical diagnosis around the world.

Resumen

La ciencia ha tenido grandes avances en diferentes ramas que han logrado conectar a las personas con nuevos dispositivos tecnológicos para simplificar distintas tareas. Las tecnologías de Internet de las Cosas (IoC) han crecido. Nos hemos rodeado de dispositivos, convirtiéndolos en una parte esencial de nuestras vidas. De esta manera, almacenan una enorme cantidad de información personal. Esta información podría ser nuestros registros de salud. Los ciberatacantes reconocen la oportunidad que estos representan e intentarán explotar sus vulnerabilidades. Tener dispositivos seguros y, por lo tanto, proteger nuestra privacidad sigue siendo un problema creciente. Por estas razones, la misión de este proyecto es encontrar una manera de proteger estos dispositivos contra las diversas amenazas existentes. Destacamos los ataques comunes a los dispositivos médicos de IoT y proponemos soluciones que ayudarán a protegerlos, centrándonos en tecnologías portátiles que están creciendo rápidamente para mejorar el diagnóstico médico en todo el mundo.

UASLP
Universidad Autónoma de San Luis Potosí

FACULTAD DE
INGENIERÍA

16 de junio de 2022

DRA. ALEJANDRA GUADALUPE SILVA TRUJILLO
P R E S E N T E.

Por medio de la presente me permito informarle, que en sesión ordinaria del H. Consejo Técnico Consultivo celebrada el día 16 de junio del presente, fue analizada su petición en la cual solicitó autorización para que el **Ing. Mauricio Jacobo González González** de la **Maestría en Ingeniería de la Computación**, se titule mediante la modalidad: **Publicación de Artículo en Congreso Internacional con Arbitraje o en Revista Indizada**, con el articulo denominado: **"Cyberattacks study on healthcare devices using Internet of Things technologies".**

Al respecto, me permito informarle que su solicitud fue aprobada de conformidad, de acuerdo a las evidencias que avalan el requerimiento de titulación antes mencionada.

Sin otro particular de momento, le reitero las seguridades de mi atenta y distinguida consideración.

"MODOS ET CUNCTARUM RERUM MENSURAS AUDEBO"

A T E N T A M E N T E

DR. RICARDO ROMERO MÉNDEZ
SECRETARIO DEL CONSEJO.

UNIVERSIDAD AUTONOMA
DE SAN LUIS POTOSI
FACULTAD DE INGENIERIA
SECRETARIA

Copia. H. Consejo Técnico Consultivo.
*etn.

ANIVERSARIO DE LA
AUTONOMÍA
UASLP 2023

www.uaslp.mx

Av. Manuel Nava 8
Zona Universitaria • CP 78290
San Luis Potosí, S.L.P.
tel. (444) 826 2330 al39
fax (444) 826 2336

"Rumbo al centenario de la autonomía universitaria"

Table of contents

Chapter 1

Paper

This chapter contains the acceptance letter for the *Industry 4.0 Academic Conference -UPPA 2020-2021* and then the paper as submitted to the conference.

Anglet, 26 de febrero del 2021

Aceptación de artículo
Conferencia Industry 4.0

Estimado Mauricio Jacobo González González,

Nos complace informarte que tu trabajo estipulado "**Cyberattacks study on healthcare devices using Internet of Things technologies**" ha sido aceptado para su presentación en "**Industry 4.0 Academic Conference -UPPA 2020-2021**", que tendrán lugar en Anglet, del 4 al 5 de marzo de 2021.

El tipo de presentación será oral. Por favor, lee atentamente los comentarios de los revisores, con el objetivo de mejorar el documento para la versión final del mismo. Esta versión definitiva deberá enviarse a través de EasyChair para que sea incluida en las actas antes del lunes 1 de marzo (plazo estricto).

Nos vemos en Anglet durante las conferencias.

Un cordial saludo,

Industry 4.0 Academic Conference -UPPA 2020-2021

SUBMISSION: 15
Cyberattacks study on healthcare devices using Internet of Things technologies

PhD. Ernesto EXPOSITO GARCIA
Professor
Head of the Computer Science Master Industry 4.0
College STEE Science - Anglet
Université de Pau et des Pays de l'Adour
ernesto.exposito@univ-pau.fr

Cyberattacks study on healthcare devices using Internet of Things technologies

Mauricio Jacobo González González [1]
Computer Science department
Université de Pau et des Pays de l'Adour
Anglet, France
mj.gonzalez@etud.univ-pau.fr

Alejandra Guadalupe Silva Trujillo [2]
Facultad de Ingeniería
Universidad Autónoma de San Luis Potosí
San Luis Potosí, S.L.P., México
asilva@uaslp.mx

***Abstract*— Science has had great advances in different branches that have managed to connect people with new technological devices to simplify different tasks. The technologies of the Internet of Things (IoT) have grown. We have surrounded ourselves with devices, making them an essential part of our lives. In this way, they store an enormous amount of personal information. This information could be our health records. Cyber attackers recognize the opportunity that these represent, and they will try to exploit their vulnerabilities. Having secure devices and therefore protecting our privacy continues to be a growing issue. For these reasons, this project's mission is to find a way to protect these appliances against diverse threats in existence. We highlight the common attacks on IoT medical devices and propose solutions that will help to protect them, focusing on wearable technologies that are growing quickly to improve medical diagnosis around the world.**

Keywords—IoT, cyberattack, healthcare.

I. Introduction

Internet of Things (IoT) technologies have received a great deal of attention in different scopes. Various areas, such as industrial, biomedical, educational, and entertainment, increasingly demand the use of integrated systems to offer a better user experience through connectivity and the effective use of technologies. The IoT has engaged in both industry and people activities including health care, where a person can access the hospital's information systems to view their medical and personal information.

Throughout history, there have been three great milestones in technology. IoT is part of the Fourth Industrial Revolution (Industry 4.0) or the Industrial Internet of Things (IIoT), where the programmed computer systems are working together with machine learning algorithms to solve multiple tasks [1]. These continually improve their ability to control and deliver different processes or services with little human interaction. The IoT has been promoted thanks to four very important elements: i) increase in computing capacity, storage, and connectivity; ii) better capacity for business analysis and intelligence; iii) new forms of human-computer interaction; iv) better methods for transferring digital instructions to the real world, such as robotics and 3D printers [2]. The IoT is a trend that promises innovative business models and better user experience through strong connectivity and the effective use of new generation embedded devices. These systems generate, process, and exchange an immense amount of data, much of that critical and sensitive. This can be considered a big opportunity for cybercrime.

Cyberattacks on IoT devices are considered high risk and even more so when managing the health data of people, which could cause physical harm and endanger their lives. Vulnerabilities will not only affect the functionality of these devices, but also the health of people. And it is that being devices that are expected to be in high demand in the population, manufacturers seek to optimize their components to offer low costs and focus on providing minimal functionality, leaving aside basic security requirements. In addition, many of the manufacturers of these devices do not offer software updates or the placement of security patches to mitigate or prevent damage after an attack.

Researchers reported that over 68,000 medical devices were identified in Shodan to be exposed and therefore accessed on the public internet. Some of the devices were Magnetic Resonance Imaging (MRI) machines, infusion pumps, and pacemaker systems. These devices were having default configuration settings. Researchers were able to extract some information related to office numbers, employee names, default credentials, software versions, operating systems, and more [3]. In some cases, the attackers didn't realize what devices they were infecting. If they had acknowledged they would have been able to get a lot of sensitive information and could have caused damage to the hospital's IT infrastructure.

Doctors are now able to program implantable cardioverter-defibrillators (ICD) to monitor a patient's heart condition. These devices can send the right level of electrical shock to get the heart beating properly [4]. It was found out a way how attackers could cause a malfunction in these devices provoking a dangerous shock in the patient.

Due to the events that are currently happening globally, the use of IoT technologies has become more necessary than ever before. In these times of change that require little face-to-face interaction between people, these devices are very useful for communicating, working, finding out about daily events, learning, entertainment, monitoring your health, and leading a healthy life. Their use has been increasing due to the need of people around the world.

Knowing the health of an individual plays a very important role today, due to the consequences that this can bring. IoT technologies can affect a very important role in this detection,

where people require continuous monitoring to avoid putting a larger group of people at risk.

The privacy of the data will be a very important point that will have to be established. Because a violation of this privacy causes individuals to reject this type of technology, the increase in devices also makes these gadgets a target for an attacker. Thus, it will be a great challenge to have the necessary protection for each person's data.

Different strategies are starting to appear involving COVID-19 and smart devices. An effective contact tracing adds importance to the user's privacy. Trying to identify individuals who have been exposed to an infected person during the contagious window while preserving our privacy [5].

The main objective of this project is to show the security and privacy vulnerabilities of healthcare IoT devices and propose a solution to protect them against these potential threats. Section II will cover the state of the art, showing how previous works have handled this kind of technology. In section III a proposal will be described on how to increase security in these devices. To finish this paper, in section IV, our conclusions of this project will be explained, and it will show some ideas on how future works can continue to apply our discoveries.

II. IoT for Healthcare: Security and Privacy

Healthcare applications are promising fields for IoT, where patients can be monitored using these technologies with medical sensors. Current health research trends focus on reliable communication and patient mobility, as well as efficient energy management.

Nowadays much of the adult population has considered monitoring their health for their well-being. With the incorporation of technology in the activities of daily life, there is a strong tendency to seek improvements in the quality of care without altering the comfort of people, that is, reducing the time of attention. In this sense, IoT technologies are very useful tools for monitoring the health of people and those who need constant monitoring. For this reason, health care that uses wireless sensor networks constitutes a field with many challenges. for scientific research. It is anticipated that the future of modern health care in an aging world will require ubiquitous health monitoring with the least real interaction between physicians and patients [6]. The European Commission and IBM estimated that, in this decade, more than 50 billion medical devices will be compatible with the Internet [7] [8].

However, the implementation of many of the new technologies in healthcare applications does not consider security as a primary issue, thus making personal data and even the patient's life itself vulnerable. Furthermore, an individual's physiological data are highly sensitive. Therefore, security is a fundamental requirement for healthcare applications and devices, especially in the case of patient privacy, if the patient has a disease that requires continuous monitoring.

In some studies, RFID-controlled systems that promise to revolutionize our medical experiences are susceptible to buffer overflow, code insertion, and SQL injection [9].

Also, in the IoT range of medical devices, it can be found specific descriptions of how an attacker could hook our device to perform a direct attack or anonymously track private patient information [10].

The great technological advances that have occurred in the health sector make dependence on these devices a vital part of our lives. Increasing functional complexity, more software programmability, and growing wireless network connectivity provide a great advantage in the use of this class of devices. However, this brings with it, becoming targets of various attacks, trying to exploit the various vulnerabilities found [11]. These types of vulnerabilities can range from the lack of availability of a service or even having your private health data exposed without your permission. This type of circumstance means that the weight of the advantages presented by these devices is outweighed by the risks that they can bring [12].

The project in its current state has carried out an analysis to identify the architecture of IoT devices. Fig. 1 shows the architecture that must be considered to verify vulnerabilities in each of the layers or phases [13]. Four phases were considered: i) Perception; ii) Transmission; iii) Computing; and iv) Application.

The Perception layer is the first layer for IoT [14]. This phase is where medical devices collect information from the patient, such as their temperature or vital signs, and even other types of information, such as their location. These data are being constantly monitored. Because the information is collected by sensors, they become the main objective of the attackers, trying to obtain the data, or even sending false information to be sent to the following stages.

The second layer is the Transmission layer, it is used to transmit data gathered through the perception layer. This layer is responsible for connecting smart things and networks. It also has many security concerns regarding the integrity and authentication of information that is being transported in the network.

The Computing layer is what the third layer is called. Literature has this layer in some cases within another, however, in this project, it has been considered important of separating it. Encryption for this layer is necessary for data security and IoT surveillance. For these reasons, an in-depth analysis must be carried out at this stage for the development of the project.

The fourth and last layer is known as the Application layer. It defines the applications that use IoT technology. Smart health is one of the many applications included. This layer is no exception to threats and vulnerabilities. Malicious code attacks and cross-site scripting are two of the most common security threats that this layer contains. Another problem in this stage is due to the large number of devices and the big amount of data transmission between users might cause network disturbance and data loss.

Defining the IoT architecture is vital for this project, being able to specify the layers involved in the IoT technologies is much needed for the study, finding the vulnerabilities in each

Fig. 1. IoT Layers.

TABLE I. Systematic Review: IoT Attacks.

IoT Attacks	Papers			
	[15]	[16]	[17]	[18]
Eavesdropping Attacks	✓	✓	×	✓
Traffic Analysis Attacks	✓	✓	×	✓
Information Gathering Attacks	✓	×	×	×
Modification Attacks	✓	×	✓	✓
Masquerade Attacks	✓	×	×	×
Denial of Service attacks	✓	✓	✓	✓
Replay Attacks	✓	✓	×	✓
Attacks Based on Network Properties	×	✓	✓	✓
Malevolent Code Attacks	×	×	×	✓
Phishing Attacks	×	×	×	✓

of the layers that were defined and find a solution. The literature is showing multiple concerns already found in different IoT devices, now, to understand how big these concerns in healthcare devices are, vulnerabilities must be covered due to the importance of this kind of technology and the sensitive information they gather. To keep confidentiality, integrity, and availability, also known as the CIA triad, representing a fundamental concept in cybersecurity, there has been a lot of research, the most common type of attacks that have been made on IoT devices can be seen in the systematic review (Table I).

The big number of attacks that exist on IoT devices [17] gives us an idea of the importance to establish security countermeasures against these threats. The consequences that they bring to healthcare devices could be devastating. Some threats that are found, have to do with privacy and security concerns.

These sensitive data could be at risk with the technique in which data are being sent through devices and because they have poor authentication methods for devices that handle such an important type of data, raising the question marks about confidentiality.

Other types of attacks have the objective to change data information, making the patient's data that were recollected hard to trust, in this way, damaging the integrity part of the healthcare device.

Medical devices recollect real-time information, if they are not available at every moment of the day, not only they are fulfilling their purpose, but they are putting in danger a patient's life, not registering, what might be for some patients, life and death cases.

As it can be seen the biggest fundaments in cybersecurity have been exposed in these types of technology. Correcting these problems would be the following step to take to guarantee confidentiality, integrity, and availability. However, other numerous issues appear when trying to apply new forms of security to IoT devices (Table II).

Discoveries in the literature give us an idea of the problems we must address as soon as possible. Different proposed solutions were made after finding the most common

TABLE II. Systematic Review: Security Challenges.

Challenges	Papers				
	[15]	[17]	[19]	[20]	[21]
Computational Limitations	✓	✓	×	×	×
Memory Limitations	×	✓	×	×	×
Energy Limitations	✓	✓	✓	×	×
Mobility	×	✓	✓	×	×
Scalability	×	✓	×	✓	×
Communications Media	×	✓	✓	✓	×
Multiplicity of Devices	×	✓	×	×	×
Dynamic Network Topology	✓	✓	×	×	×
Multi-Protocol Network	×	✓	×	×	×
Dynamic Security Updates	×	✓	✓	×	×
Tamper-Resistant Packages	×	✓	×	×	×
Design Constraints	×	×	✓	×	×
Price	×	×	×	✓	✓

threats for wearables devices [15]. Energy remains critical in this technology, especially due to the new functionalities and the increased number of requirements they make, asking for more power. New methods to have better energy efficiency are been proposed, and it brings a big advantage for wearables devices to depend on energy harvesting to be self-powered.

Security vulnerabilities were found in smartwatches, including poor authentication [19]. It was easy to take control of these devices by applying a brute force attack. Authentication protocols to access your device are improving day by day intending to create a secret key focusing on measures that are not easy to decipher by an outsider [20].

Still, one of the biggest challenges that would take a long time to overcome is standardization [17]. With a wide type of products and many different manufacturers, it creates interoperability issues, these make the case to have many different security solutions for just one type of device.

III. Security Framework for IoT Healthcare Devices

The year 2020 has had to deal with a global pandemic, which has brought a new way of living for people, and the need for technology is increasing. Health monitoring by devices sounds like a requirement that must be carried out by everyone. The countries have experienced the development of applications to meet people who may have COVID-19 disease, and in this manner inform all the people who have had contact with them. This implies a great responsibility regarding the storage of people's data, which if not well protected can affect people. It has been seen how people out of fear or ignorance, physically and verbally agree to people who can be carriers of COVID-19, which makes this type of application dangerous if they have vulnerabilities that put people's privacy at risk.

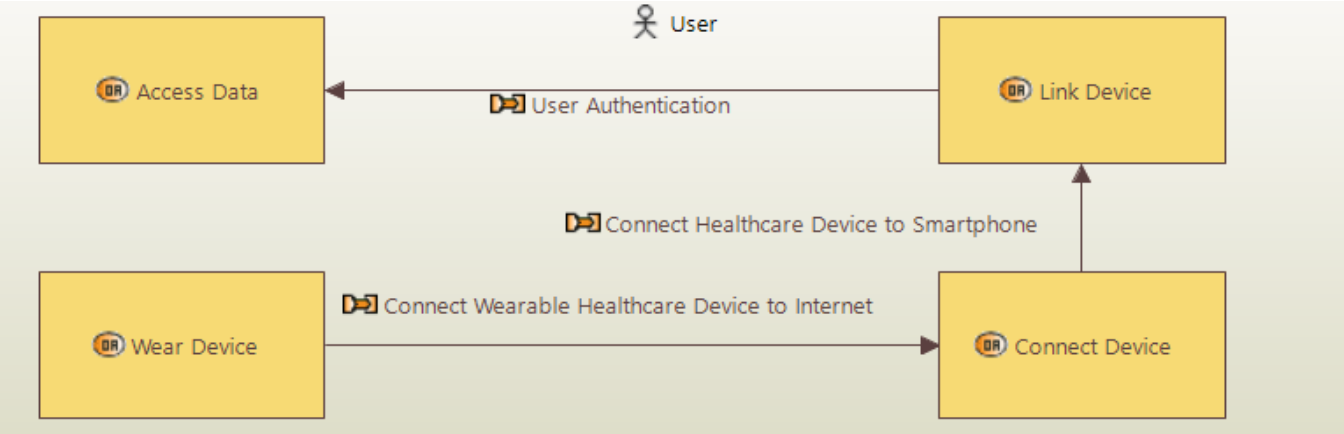


Fig. 2. Operational Architecture

The continuous growth of IoT asks for a much-needed improvement in security matters. New medical devices start to join IoT because of the advantages it can bring. Better, faster, and simpler methods of diagnosis, are not only beneficial for patients but all the healthcare professionals involved: doctors, nurses, biomedical engineers, technicians, radiographers, physicians, physiotherapists, and so forth.

To be monitored daily and for a long time, new devices are starting to become smaller, giving result devices that a person can carry with them all day. Taking advantage of modern sensors, we can see people being able to measure different body signals without worrying about where they are at that precise moment. But even some of these devices are still not easy to interact with. Trying to adapt a monitor that can read your heart rate and pulse and even an electrocardiogram and make it a portable device still brought some difficulties to some users. Because of these, we can now see wearable devices, like smartwatches, which original concept was not reading heart rates or displaying an electrocardiogram, are now able to do that. These devices are in consideration for medical diagnosis. For example, in 2018, the Food and Drug Administration (FDA) cleared the Apple Watch Series 4 and named it a class 2 medical device [21], because of its ability to identify atrial fibrillation (AF).

With medical devices joining the Fourth Industrial Revolution and being part of the IoT technologies, and with some of the wearable devices from other sectors forming now part of the medical environment, the development of healthcare devices is growing fast, covering the needs people have. But with such fast growth, the problems start to expand too. More vulnerabilities are being found. IoT technologies have many security issues, now with wearable devices just as the smartwatches integrating into the healthcare area, they bring and represent more security challenges that must be solved.

Thanks to the systematic review that was carried out in the state of art, we could find the principal attacks done in IoT technologies and what are the biggest challenges to correct wearables devices. We focus on smartwatches, because of the way they are being used to obtain sensitive healthcare data and they are one of the most bought wearables. Here is a proposed methodology to improve security in this kind of technology.

A) Security for data access and data storage.

Security represents costs, you can see it reflected in terms of money and power consumption [20]. The necessity to protect transmitted data to guarantee its confidentiality and integrity has developed many different authentication methods. Due we are working with wearables devices; power consumption is always a challenge to apply an encryption model. To achieve verification, a lightweight and low overhead encryption method for wearable communication should be applied [15] and with the different attributes these devices are sensing, biometric encryption is the best solution to guarantee authentication, especially if the measure taken to access is one that is not that easy to discover, unlike the fingerprint.

B) Communication Protocols.

Unsecure transmission of data via Bluetooth is one of the vulnerabilities that cybercriminals exploited the most [19], and these short-range communications protocols are included in most wearables devices. Nevertheless, with the accelerated growth of IoT, different protocols with long-range communication will be available. Some examples are LoRaWAN and SigFoX [15] or, due to the necessity of real-time data acquisition, Symphony Link and Ingenu could be better options [22]. Another advantage of these methods is that they are considered low-power protocols.

C) Energy.

Harvesting energy methods from multiple sources, some examples could be thermal, mechanical, and solar energy used simultaneously. This is a big necessity for a medical device to guarantee its availability. Many approaches have been developed. One with positive results to achieve self-sustainability exploits thermal and solar energy, and it performs well during high-demanding tasks [23].

Fig. 2 shows the operational architecture of the system, it was developed using the Arcadia methodology. The purpose is to understand what the user needs to accomplish. For this project, it is proposed that the user can access his health records that are being stored thanks to de devices he is wearing.

IV. Conclusions

The solutions proposed in this project focused on guaranteeing system confidentiality, integrity, and availability. We aimed to counter the most common vulnerabilities in healthcare IoT devices, especially wearables

technology. Due to the growth of IoT, challenges are found because of the great number of devices in existence up to now. Different standards for these appliances increase the difficulty to create only one safety protocol for every single one of them, not only the heterogeneity of these devices makes it harder but countries' healthcare policies around the globe, with many different strategies that regulate medical devices, and in different approaches with a diverse set of rules. This project considered all these challenges, and for that reason the proposed methodology can be open for changes, aiming for small substitutions depending on what kind of device you want to study. The proposal can be taken for future works and will adapt to vulnerable healthcare devices in existence. Authentication methods might differ from one device to another. Different attributes, for example, memory and storage capacity will determine what kind of encryption method can work better, at the same time, it depends on what type of data is being recorded and could count with a different-biometric access technique. We can't expect to use an electrocardiogram (ECG) encryption key for an insulin pump, that records another kind of biometric attribute that is not easy to discover. Just like the authentication method, the harvesting energy method shows the possibility to change depending on the healthcare device you have.

The method proposed seems to be the best solution when talking about wearable devices, especially smartwatches, but for other types of healthcare devices, different solutions could work in a better manner.

References

[1] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," Bus. Inf. Syst. Eng., vol. 6, no. 4, pp. 239–242, Aug. 2014, DOI: 10.1007/s12599-014-0334-4.

[2] V. Roblek, M. Meško, and A. Krapež, "A Complex View of Industry 4.0," SAGE Open, vol. 6, no. 2, Apr. 2016, DOI: 10.1177/2158244016653987.

[3] C. Tziampazis, "Exposure Assessment on Medical Devices in the Netherlands," Jun. 30, 2019. http://essay.utwente.nl/78845/.

[4] A. Chacko and T. Hayajneh, "Security and Privacy Issues with IoT in Healthcare," EAI Endorsed Trans. Pervasive Health Technol., vol. 4, p. 155079, Jul. 2018, DOI: 10.4108/eai.13-7-2018.155079.

[5] C. Troncoso et al., "Decentralized Privacy-Preserving Proximity Tracing," ArXiv200512273 Cs, May 2020, Available: http://arxiv.org/abs/2005.12273.

[6] W.-Y. Chung, G. Walia, Y.-D. Lee, and R. Myllyla, "Design Issues and Implementation of Query-Driven Healthcare System Using Wireless Sensor Ad-hoc Network," in 4th International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2007), Berlin, Heidelberg, 2007, pp. 99–104, DOI: 10.1007/978-3-540-70994-7_17.

[7] P. Brody, and V. Pureswaran, "Device Democracy: Saving the Future of the Internet of Things", IBM, 2014, https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF.

[8] European Commission, New EU rules to ensure safety of medical devices. European Commission: Brussels, Belgium, 5 April 2017. Available:https://ec.europa.eu/health/sites/health/files/md_newregulations/docs/md_generic_fs_en.pdf

[9] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "Is your cat infected with a computer virus?," in Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06), Mar. 2006, p. 10 pp. – 179, DOI: 10.1109/PERCOM.2006.32.

[10] J. Radcliffe, "Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System." https://scholar.googleusercontent.com/scholar?q=cache:oahwlxXu-DIJ:scholar.google.com/+Jerome(Radcliffe&hl=es&as_sdt=0,5.

[11] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses," ArXiv200507359 Cs, May 2020. [Online]. Available: http://arxiv.org/abs/2005.07359.

[12] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-Health Cloud: Opportunities and Challenges," Future Internet, vol. 4, no. 3, Art. no. 3, Sep. 2012, DOI: 10.3390/fi4030621.

[13] A. G. Silva., J. G. Heredia, P. D. Arjona, A. P. Juárez, A. L. Sandoval , Seguridad y Privacidad en el Internet de las Cosas, In V Jornadas Nacionales de Investigación en Ciberseguridad JNIC 2019, Universidad de Extremadura, España - June 2019.

[14] S. Bandyopadhyay, "Production and Operations Analysis: Traditional, Latest, and Smart Views", Vol 1, December 2019.

[15] S. Seneviratne et al., "A Survey of Wearable Devices and Challenges," IEEE Commun. Surv. Tutor., vol. 19, no. 4, pp. 2573–2620, Fourthquarter 2017, DOI: 10.1109/COMST.2017.2731979.

[16] A. Sivanathan, "IoT Behavioral Monitoring via Network Traffic Analysis," ArXiv200110632 Cs, Jan. 2020, Accessed: Feb. 04, 2021. [Online]. Available: http://arxiv.org/abs/2001.10632.

[17] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678–708, 2015, DOI: 10.1109/ACCESS.2015.2437951.

[18] T. Rao and E. Haq, "Security Challenges Facing IoT Layers and its Protective Measures," Int. J. Comput. Appl., vol. 179, pp. 31–35, Mar. 2018, DOI: 10.5120/ijca2018916607.

[19] K. Ching and M. (Mandy) Mahinderjit Singh, "Wearable Technology Devices Security and Privacy Vulnerability Analysis," Int. J. Netw. Secur. Its Appl., vol. 8, pp. 19–30, May 2016, DOI: 10.5121/ijnsa.2016.8302.

[20] K. Austen, "What could derail the wearables revolution?," Nat. News, vol. 525, no. 7567, p. 22, Sep. 2015, DOI: 10.1038/525022a.

[21] N. Isakadze and S. S. Martin, "How useful is the smartwatch ECG?," Trends Cardiovasc. Med., vol. 30, no. 7, pp. 442–448, Oct. 2020, DOI: 10.1016/j.tcm.2019.10.010.

[22] J. P. Queralta, T. N. Gia, Z. Zou, H. Tenhunen, and T. Westerlund, "Comparative Study of LPWAN Technologies on Unlicensed Bands for M2M Communication in the IoT: beyond LoRa and LoRaWAN," Procedia Comput. Sci., vol. 155, pp. 343–350, Jan. 2019, DOI: 10.1016/j.procs.2019.08.049.

[23] M. Magno, X. Wang, M. Eggimann, L. Cavigelli, and L. Benini, "InfiniWolf: Energy Efficient Smart Bracelet for Edge Computing with Dual Source Energy Harvesting," in 2020 Design, Automation Test in Europe Conference Exhibition (DATE), Mar. 2020, pp. 342–345, DOI: 10.23919/DATE48585.2020.9116218.

Chapter 2

Presentation

This chapter contains the slides of the paper presented at the conference and translated into Spanish to be shown in the final exam. Some slides were added after the previous exam to improve the presentation and to include another research project consequent from the previous paper.

CYBERATTACKS STUDY ON HEALTH CARE DEVICES USING INTERNET OF THINGS TECHNOLOGIES

ALUMNO: MAURICIO JACOBO GONZÁLEZGONZÁLEZ

ASESORA: DRA. ALEJANDRA GUADALUPE SILVA TRUJILLO

CONTENIDO

- Introducción
- Objetivos
- Estado del Arte
- Propuesta
- Análisis de relojes inteligentes
- Resultados
- Conclusiones
- Contribuciones
- Preguntas

Primera etapa

Segunda etapa

PRIMERA ETAPA: ESTUDIO DE CIBERSEGURIDAD DE EQUIPOS MÉDICOS DEL IOT

INTRODUCCIÓN

- Las tecnologías del Internet de las cosas (IoT) han sido objeto de gran atención en diferentes ámbitos. Varias áreas, como la industrial, biomédica, educativa y de entretenimiento, exigen cada vez más el uso de sistemas integrados para ofrecer una mejor experiencia de usuario a través de la conectividad y el uso efectivo de las tecnologías.

https://saharasecuritys.com/como- afecta-el-malware -en-los-dispositivos -iot/

INTRODUCCIÓN

- El IoT ha incursionado tanto en actividades de la industria como en las personas incluyendo el cuidado de la salud, donde una persona puede tener acceso a sistemas de información de un hospital para ver su información médica y personal.

https://thejournalofmhealth.com/improving -adherence -with-technology -innovating -healthcare-through-iot/

https://theiotmagazine.com/iot -in-healthcare- how-it-improves -medical -software-4ca703ea1130

5

1>Introducción

INTRODUCCIÓN

Se identificaron 68,000 equipos médicos expuestos, entre ellos maquinas de imagen de resonancia magnética (IRM), bombas de infusión, marcapasos.

Los médicos ahora pueden programar desfibriladores cardioversores implantables (DCI) para monitorear la condición cardiaca de un paciente.

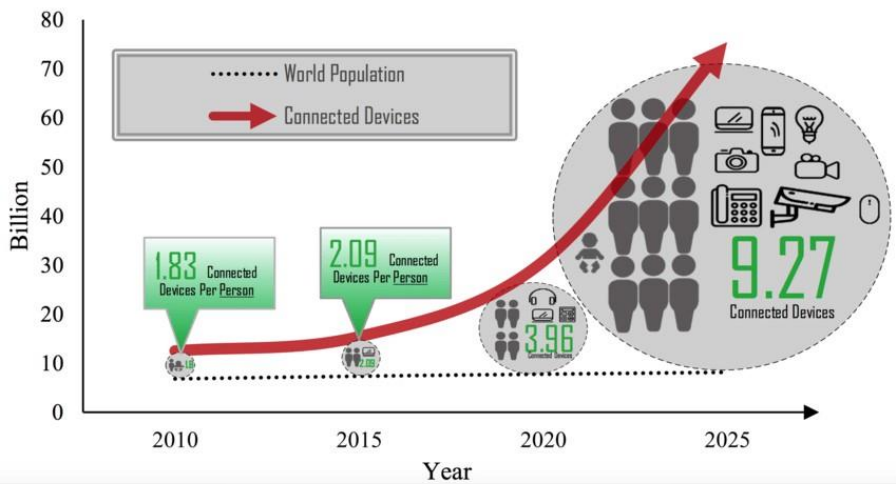
https://www.florence-health.com/latest -news/hospital -administrator/10 -basics-of-cybersecurity -policies- for-small -medium -and -large- healthcare- systems/

6

INTRODUCCIÓN

- La Comisión Europea e IBM estimaron que, en esta década, más de 50 mil millones de dispositivos médicos serán compatibles con Internet. Esto también se traduce en que la industria de la medicina generará una cantidad masiva de información personal a través de estos dispositivos del IoT, la estimación es de más de dos mil exabytes de datos.

DISPOSITIVOS CONECTADOS AL INTERNET DE LAS COSAS



Reliability Side -Effects in Internet of Things Application Layer Protocols - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Estimated -Number-of-Connected-Devices-Per-Person-By-2025_fig3_322050538

NORMATIVA

- Con este crecimiento acelerado en las tecnologías IOT, organismos reguladores y organizaciones gubernamentales se han dado cuenta de los riesgos potenciales de estos dispositivos interconectados si no son desarrollados con las medidas de seguridad correctas. En respuesta a esto sean empezado a crear reglamentos para asegurarse que estén las mejores practicas con estas tecnologías por parte de los diseñadores, vendedores y usuarios finales.

9

NORMATIVA

- La Unión Europea y el Reino Unido han puesto en creación distintos reglamentos que deben ser cumplidos al momento de desarrollar dispositivos de IoT. Por ejemplo en el Reino Unido todos los dispositivos deben de contar con contraseñas únicas y no pueden ser reiniciadas a sus contraseñas por defecto.
- En el 2020 en Estados Unidos agregaron a la ley una legislación que pretende incentivar a las compañías para asegurar los dispositivos que diseñan y venden.
- Hoy en día en México no se encuentra una norma como las previamente mencionadas.

10

OBJETIVOS

- Revisión del estado del arte.
- Encontrar los ataques más comunes en los equipos médicos delloT.
- Identificar las limitantes o retos en los equipos médicos del loT.
- Proponer una arquitectura general teniendo en consideración las limitantes de los dispositivos.

CAPAS IOT

Diseño propio incluido en nuestro artículo de investigación

ATAQUES A DISPOSITIVOS IOT

IoT Attacks	Papers			
	[1]	[2]	[3]	[4]
Eavesdropping Attacks	✓	✓	×	✓
Traffic Analysis Attacks	✓	✓	×	✓
Information Gathering Attacks	✓	×	×	×
Modification Attacks	✓	×	✓	✓
Masquerade Attacks	✓	×	×	×
Denial of Service attacks	✓	✓	✓	✓
Replay Attacks	✓	✓	×	✓
Attacks Based on Network Properties	×	✓	✓	✓
Malevolent Code Attacks	×	×	×	✓
Phishing Attacks	×	×	×	✓

Diseño propio incluido en nuestro artículo de investigación

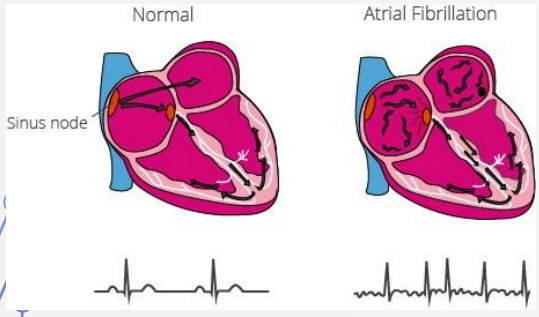
- [1] S. Seneviratne et al., "A Survey of Wearable Devices and Challenges,"
- [2] A.Sivanathan "IoT Behavioral Monitoring via Network Traffic Analysis,"
- [3] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey,"
- [4] T. Rao and El-Hag, "Security Challenges Facing IoT Layers and its Protective Measures,"

PILARES DE LA CIBERSEGURIDAD

https://www.researchgate.net/figure/Information-security-with-CIA-triangle-Image-taken-from_fig3_342787015

1>Estado del Arte

RELOJES INTELIGENTES



https://www.cardiosecur.com/magazine/specialist-articles-on-the-heart/atrial-fibrillation-a-common-heart-condition

https://www.iphon.fr/post/apple-watch-series-4-la-mesure-de-lelectrocardiogramme-desormais-disponible-dans-de-nombreux-pays-dont-france-belgique-suisse-etc

1>Estado del Arte

Challenges	Papers				
	[1]	[3]	[5]	[6]	[7]
Computational Limitations	✓	✓	×	×	×
Memory Limitations	×	✓	×	×	×
Energy Limitations	✓	✓	✓	×	×
Mobility	×	✓	✓	×	×
Scalability	×	✓	×	✓	×
Communications Media	×	✓	✓	✓	×
Multiplicity of Devices	×	✓	×	×	×
Dynamic Network Topology	✓	✓	×	×	×
Multi-Protocol Network	×	✓	×	×	×
Dynamic Security Updates	×	✓	✓	×	×
Tamper-Resistant Packages	×	✓	×	×	×
Design Constraints	×	×	✓	×	×
Price	×	×	×	✓	✓

Diseño propio incluido en nuestro artículo de investigación

DESAFÍOS DE SEGURIDAD

- [1] S. Seneviratne et al., "A Survey of Wearable Devices and Challenges,"
- [3] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey,"
- [5] K. Ching and M. (Mandy)Mahinderjit Singh, "Wearable Technology Devices Security and Privacy Vulnerability Analysis,"
- [6] K. Austen, "What could derail the wearables revolution?,"
- [7] N.Isakadze and S. S. Martin, "How useful is the smartwatch ECG?,"

1>Propuesta

PROPUESTA

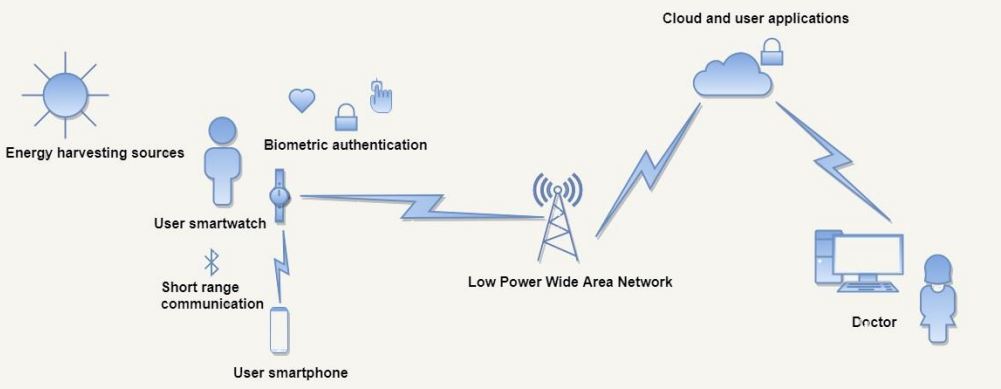
- Seguridad en el acceso a los datos
- Protocolos de comunicación
- Ahorro de energía

Diseño propio incluido en nuestro artículo de investigación

1>Propuesta

PROPUESTA

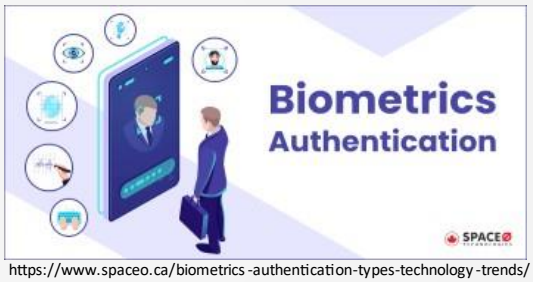
- Seguridad en el acceso a los datos
- Protocolos de comunicación
- Ahorro de energía



Diseño propio

1>Propuesta

- Seguridad en el acceso a los datos
- Protocolos de comunicación
- Ahorro de energía



https://www.spaceo.ca/biometrics-authentication-types-technology-trends/

https://www.dataprint.fr/actualite/lora-et-sigfox-face-au-reste-du-monde

https://www.weonline.com/web/en/electronic_components/produkte_pb/demoboards/energy_harvesting/gleanergy/gleanergy.php

19

1>Propuesta

RETOS

- Heterogeneidad
- Estandarización

https://www.watchhunter.org/2018/01/smartwatch-guide-for-watch-nerds.html

20

TRABAJOS FUTUROS

- Implementación
- Prueba diferentes dispositivos
- Revisar seguridad de los protocolos de comunicación
- Aplicar otros métodos de autenticación y recolección de energía

https://www.horsesforsources.com/cognizant-051411

SEGUNDA ETAPA: ANÁLISIS DE RELOJES INTELIGENTES

UASLP
Universidad Autónoma de San Luis Potosí

OBJETIVOS

- Analizar la comunicación por medio de Bluetooth de los distintos relojes inteligentes.
- Crear una propuesta de requerimientos necesarios para establecer una conexión segura por medio de Bluetooth.
- Crear una propuesta de requerimientos **mínimos** necesarios para establecer una conexión segura por medio de Bluetooth.

23

UASLP
Universidad Autónoma de San Luis Potosí

BLUETOOTH

- Es un estándar para comunicación por radio frecuencia de corto alcance.
- Clasificación:

1. Bluetooth Clásico: *Bluetooth Basic Rate (BR), Enhanced Data Rate (EDR) and High Speed (HS)*
2. *Bluetooth Low Energy (BLE)*
3. Modo Dual

https://www.pinterest.com/pin/632122497693492086/

24

UASLP
Universidad Autónoma de San Luis Potosí

DIFERENCIAS BLUETOOTH CLÁSICO Y BLE

- Bajo consumo de energía
- Requerimientos de memoria reducidos
- Procesos de descubrimiento y conexión eficientes
- Paquetes cortos
- Servicios y protocolos simples

25

UASLP
Universidad Autónoma de San Luis Potosí

SERVICIOS DE SEGURIDAD DE BLUETOOTH

- Autenticación
- Confidencialidad
- Autorización
- Integridad de los mensajes
- Emparejamiento/Vinculación

26

MODOS DE SEGURIDAD BLUETOOTH CLÁSICO

- Bluetooth clásico tiene 4 modos de seguridad: los primeros 3 solo son usados en versiones de Bluetooth 2.0 y anteriores.
- Si ambos dispositivos cuentan con versiones 2.1 o nuevas, se require que usen el modo de seguridad 4.

+ SEGURIDAD –

- Nivel 4 : Requiere una llave de enlace (*Link Key*) autenticada utilizando *Secure Connections*
- Nivel 3 : Requiere una llave de enlace autenticada
- Nivel 2 : Requiere una llave de enlace sin autenticar
- Nivel 1: No requiere seguridad

27

MODO DE SEGURIDAD 4 BLUETOOTH CLÁSICO

+ SEGURIDAD –

Local Bluetooth Version	Most secure Mode 4 Level connecting to a peer which is	
	2.1 – 4.0	4.1 or higher
4.2	Level 3	Level 4
4.1		
4.0		Level 3
3.0		
2.1		
2.0	N/A	N/A
1.2		
1.1		
1.0		

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800 -121r2.pdf

28

EMPAREJAMIENTO BLUETOOTH CLÁSICO

- Se genera una llave secreta simétrica que es esencial para los mecanismos de autenticación y cifrado que provee Bluetooth.
- La llave es conocida como llave de enlace (Link Key).
- En la versión de Bluetooth 2.1 + EDR se introdujo el método de emparejamiento *Secure Simple Pairing (SSP)* para el uso con el modo de seguridad 4.
- La curva elíptica utilizada para el proceso de emparejamiento puede ser P -192 o P-256.

29

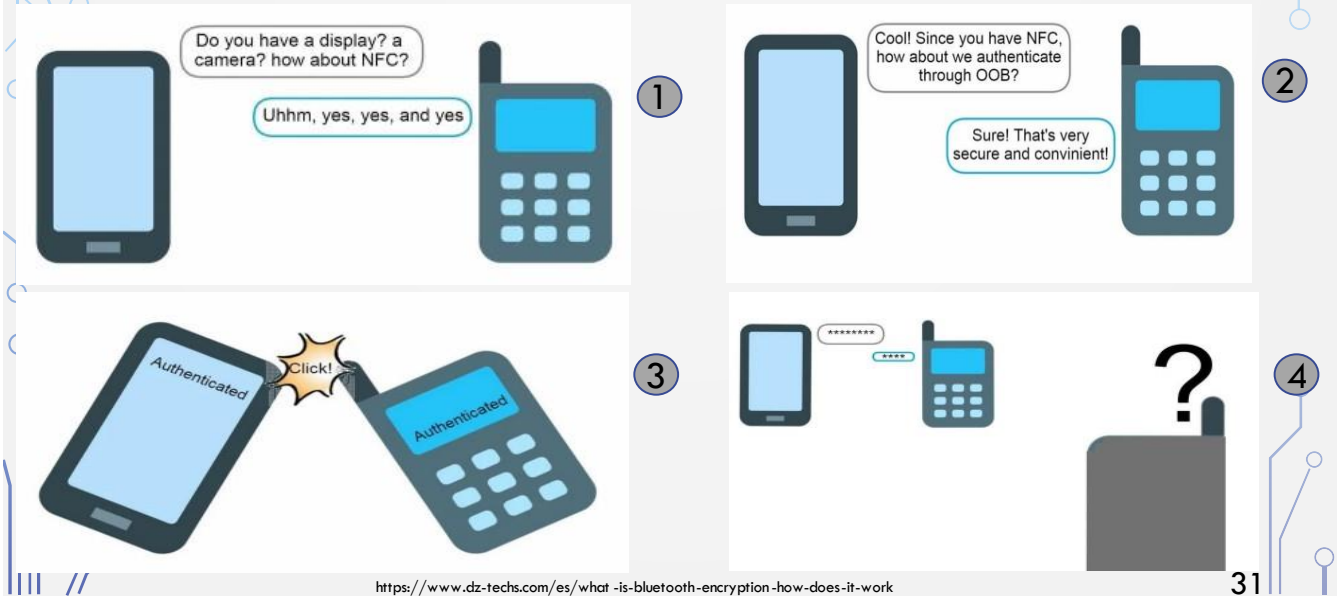
MODELOS DE ASOCIACIÓN *SECURE SIMPLE PAIRING*

- *Numeric Comparison*
- *Passkey Entry*
- *Just Works*
- *Out of Band (OOB)*

30

2>Análisis de relojes inteligentes

PASOS PARA CONEXIÓN ENTRE DISPOSITIVOS POR MEDIO DE BLUETOOTH



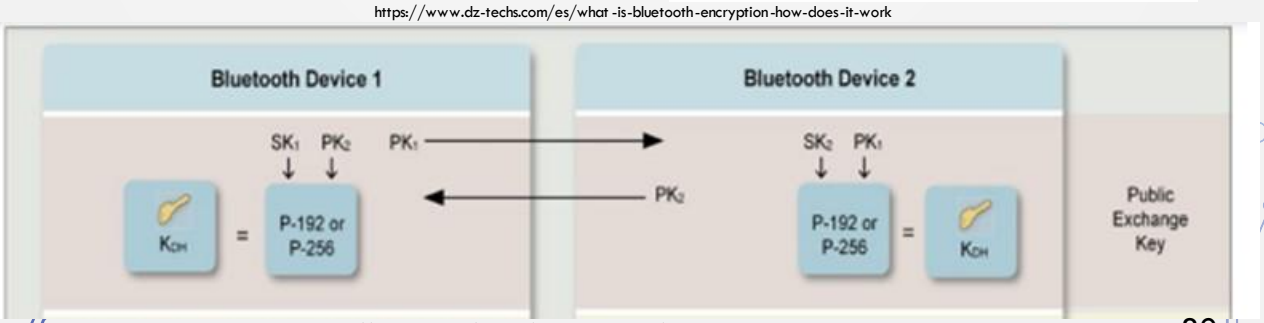
https://www.dz-techs.com/es/what -is-bluetooth-encryption-how-does-it-work

31

2>Análisis de relojes inteligentes

CONEXIÓN ENTRE DISPOSITIVOS POR MEDIO DE BLUETOOTH

https://www.dz-techs.com/es/what -is-bluetooth-encryption-how-does-it-work

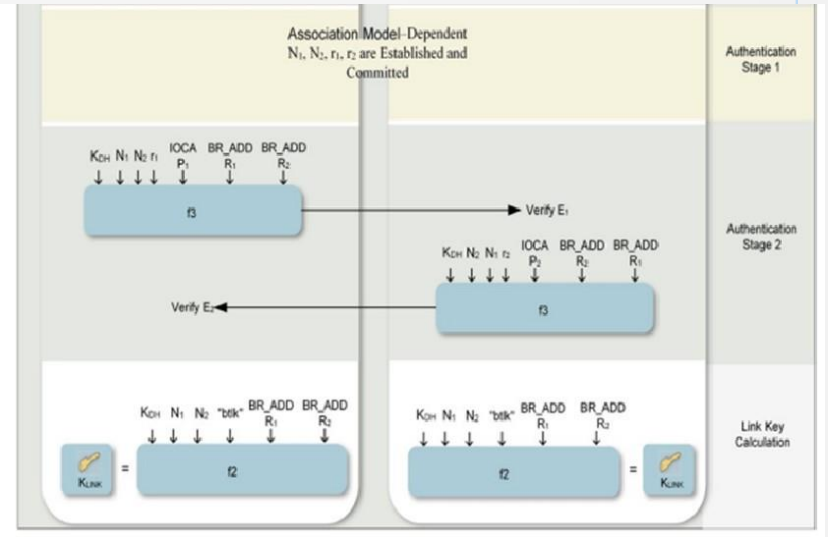


https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800 -121r2.pdf

32

PASOS PARA CONEXIÓN ENTRE DISPOSITIVOS POR MEDIO DE BLUETOOTH

https://www.dz-techs.com/es/what -is-bluetooth-encryption- how-does-it-work



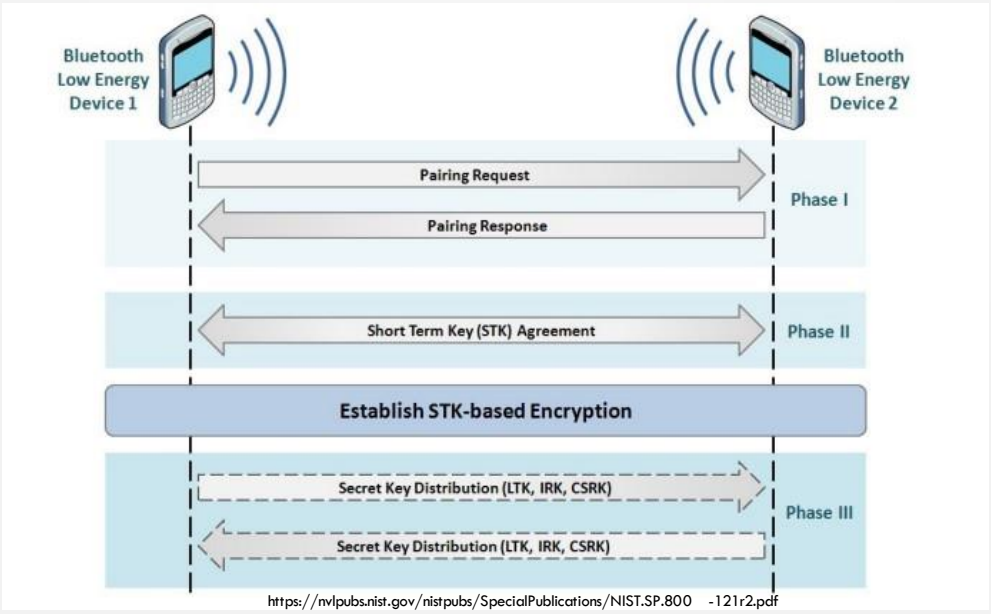
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800 -121r2.pdf

BLUETOOTH LOW ENERGY

- Se genera una *Long Term Key* (en lugar de una llave de enlace).
- Existen 2 llaves complementarias: *Identity Resolving Key (IRK)*, que se encarga de las direcciones privadas y *Connection Signature Resolving Key (CSRK)* que se encarga de asegurar la integridad de los datos que se envían por enlaces no cifrados.
- Existen 2 modos de seguridad:

1. Requiere cifrado
2. No require cifrado

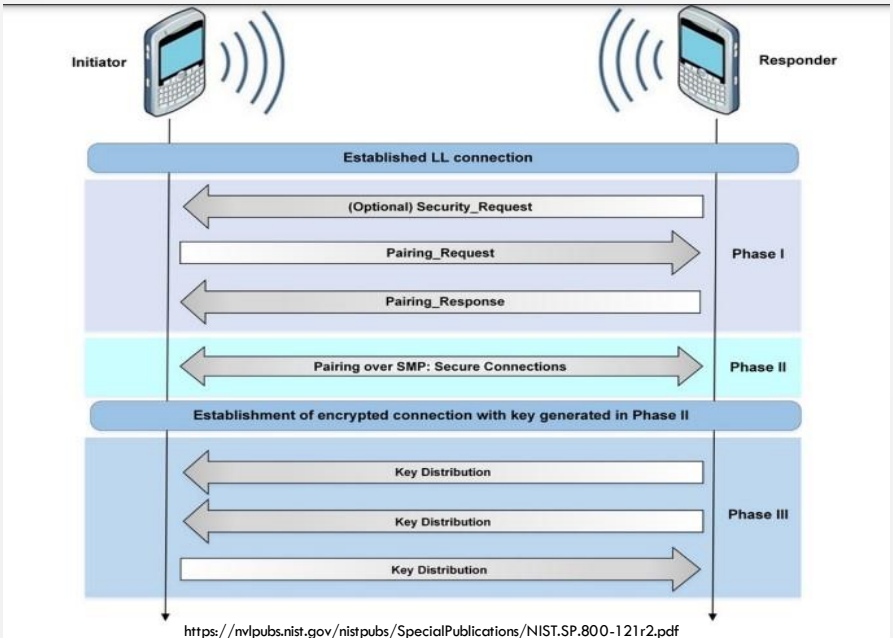
LOW ENERGY LEGACY PAIRING



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800 -121r2.pdf

35

LOW ENERGY SECURE CONNECTIONS PAIRING



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

36

MODELOS DE ASOCIACIÓN BLUETOOTH LOW ENERGY

- *Numeric Comparison* (Únicamente para Secure Connections)
- *Passkey Entry*
- *Just Works*
- *Out of Band (OOB)*

PRUEBAS

- Adafruit Bluefruit LE Sniffer - Bluetooth Low Energy (BLE 4.0)- nRF51822
- *btsnooz* script
- Wireshark

https://www.amazon.com/Adafruit -Bluefruit-Sniffer-Bluetooth-nRF51822/dp/B00SKWGPE0

https://www.wireshark.org/

2>Análisis de relojes inteligentes

- Relojes Inteligentes utilizados:

a) Amazfit GTS 2 mini

b) Apple Watch Series 2 Aluminum

c) Garmin vivoactive 3

d) Fitbit Versa 2

e) Fitbit Versa 3

f) W27 Pro

UASLP
Universidad Autónoma de San Luis Potosí

a

https://www.amazfit.com/us/amazfit-gts-2-mini.html

d

https://www.target.com/p/fitbit-versa-2-smartwatch/-/A-77677108

b

https://www.bestbuy.com/site/apple-watch-series-2-42mm-rose-gold-aluminum-case-pink-sand-sport-band-rose-gold-aluminum/5706570.p?skuId=5706570

e

https://www.amazon.com.mx/Fitbit-Reloj-Inteligente-Versa-Aluminio/dp/B08DFPZG71

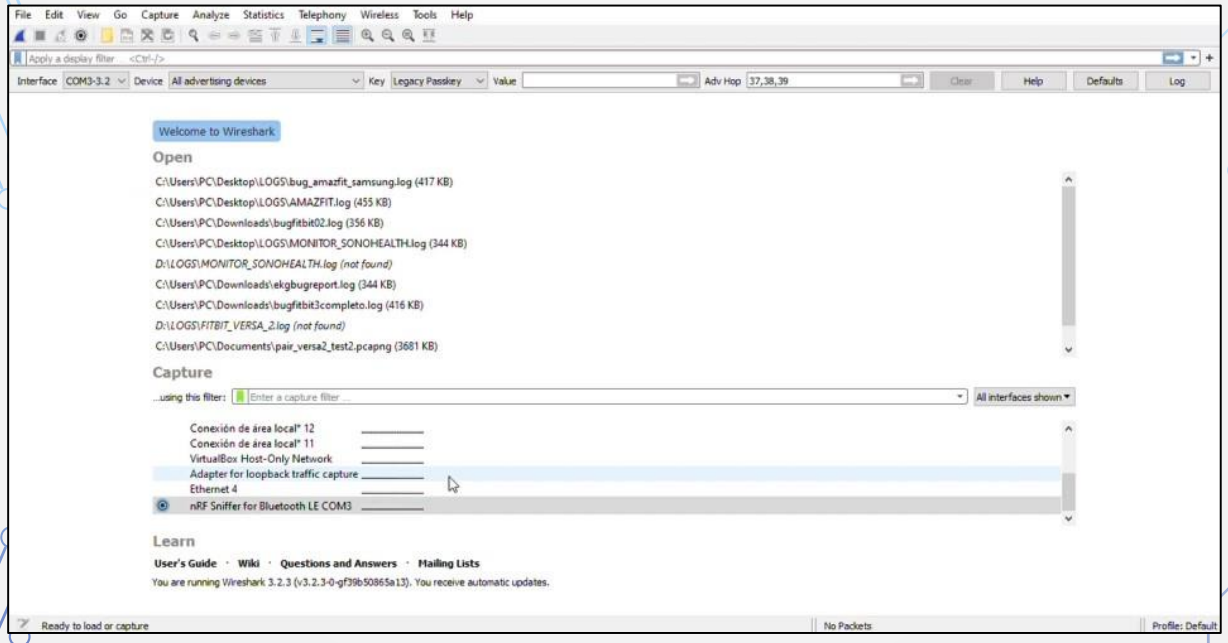
c

https://www.innovasport.com/unisex/entrenamiento/accesorios/garmin/vivoactive-3-negro-con-bisel-gris/p/000000000000073380

f

https://articulo.mercadolibre.com.mx/MLM-1397005465-fralugio-reloj-inteligente-smartwatch-w27-pro-full-touch-hd-_JM

39



40

ANÁLISIS DE RELOJES INTELIGENTES (1era PARTE)

Devices	Bluetooth Protocol	Low Energy Pairing	Pairing Methods	Pairing Association Model	Passkey	Security Mode	Level	Static Address
Fitbit Versa 2	4.0	✓	Legacy Pairing	Passkey Entry	4 digits	1	3	✓
Fitbit Versa 3	5.0	✓	Legacy Pairing	Passkey Entry	4 digits	1	3	✓
Versa 3 Controls	5.0	×	Secure Simple Pairing (Secure Connections)	Numeric Comparison	6 digits	4	4	✓
Apple Watch Series 2 Aluminum	4.0	✓	Legacy Pairing	Passkey Entry / Out of Band (OOB)	6 digits	1	3	×

Diseño propio

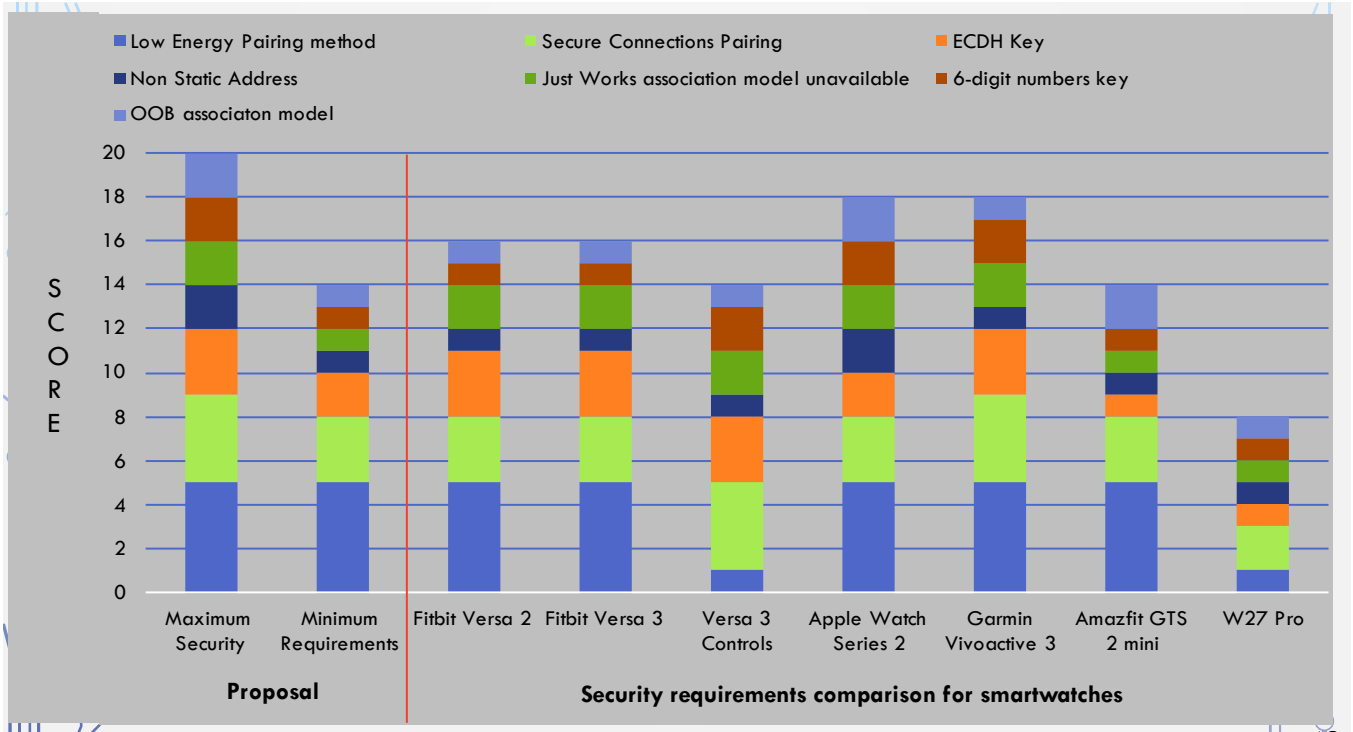
41

ANÁLISIS DE RELOJES INTELIGENTES (2da PARTE)

Devices	Bluetooth Protocol	Low Energy Pairing	Pairing Methods	Pairing Association Model	Passkey	Security Mode	Level	Static Address
Garmin vivoactive 3	4.2	✓	Secure Connections	Passkey Entry	6 digits	1	4	✓
Amazfit GTS 2 mini	5.0	✓	Legacy Pairing	Out of Band (OOB) / Just Works	None	1	3	✓
W27 Pro	3.0+5.0	×	Secure Simple Pairing (unauthenticated link key)	Just Works	None	4	2	✓

Diseño propio

42



Diseño propio

43

2>Análisis de relojes inteligentes

UASLP
Universidad Autónoma de San Luis Potosí

CONCLUSIONES (1)

- Hasta el momento no hay estudios que realicen una comparativa entre dispositivos que muestre los requerimientos necesarios para un emparejamiento seguro.
- Los fabricantes no siguen todas las recomendaciones para lograr tener un dispositivo con la máxima seguridad.
- 1 de 6 relojes inteligentes analizados no cumple con el mínimo de requerimientos necesarios.
- Existen relojes inteligentes que no siguen un protocolo de emparejamiento de baja energía.

44

UASLP
Universidad Autónoma de San Luis Potosí

CONCLUSIONES (2)

- No hay recomendaciones para un uso seguro de emparejamiento vía Bluetooth.
- Un dispositivo nuevo no equivale a un dispositivo con mejor seguridad.
- Existe una relación entre el precio del reloj inteligente y su nivel de seguridad: A mayor precio, mayor su nivel de seguridad.

45

UASLP
Universidad Autónoma de San Luis Potosí

CONTRIBUCIONES

- Publicaciones y Congresos
  1. Towards Services Profiling for Energy Management in Service-Oriented Architectures – WEBIST (International Conference on Web Information Systems and Technologies)– pp. 209-2016 – 26-28, Octubre, 2021 **(Coautor)**
  2. Modeling Energy Consumption in SOA: Requirements and Current Status – Atelier "Évolution des SI" @ INFORSID 2021 – 1, Junio, 2021 **(Coautor)**
  3. Cyberattacks study on healthcare devices using Internet of Things technologies - "Industry 4.0 Academic Conference -UPPA 2020-2021" – 4-5, Marzo, 2021 **(Autor principal)**
- Eventos de divulgación
  1. Cyberattacks study on healthcare devices using Internet of Things technologies - Seminario de Investigación. 26, mayo, 2021
  2. Internet de las Cosas y la pérdida de la privacidad - TBarCampMX 2019: "Smart Cities and Internet of Things the Beginning of a Reality" - 13-14, Noviembre, 2019

46

REFERENCIAS

- [1] S. Seneviratne et al., "A Survey of Wearable Devices and Challenges," IEEE Commun Surv. Tutor., vol. 19, no. 4, pp.2573–2620, Fourthquarter2017, doi: 10.1109/COMST.2017.2731979.
- [2] A. Sivanathan, "IoT Behavioral Monitoring via Network Traffic Analysis," ArXiv200110632 Cs, Jan. 2020, Accessed: Feb. 04, 2021. [Online]. Available: http://arxiv.org/abs/2001.10632.
- [3] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.
- [4] T. Rao and E.Haq, "Security Challenges Facing IoT Layers and its Protective Measures," Int. J. Comput Appl., vol. 179, pp. 31 –35, Mar. 2018, doi: 10.5120/ijca2018916607.
- [5] K. Ching and M. (Mandy) Mahinderjit Singh, "Wearable Technology Devices Security and Privacy Vulnerability Analysis," Int. J. Netw. Secur. Its Appl., vol. 8, pp. 19 –30, May 2016, doi: 10.5121/ijnsa.2016.8302.
- [6] K. Austen, "What could derail the wearables revolution?," Nat. News, vol. 525, no. 7567, p. 22, Sep. 2015, doi: 10.1038/525022a.
- [7] N. Isakadze and S. S. Martin, "How useful is the smartwatch ECG?," Trends Cardiovasc. Med., vol. 30, no. 7, pp. 442448, Oct. 2020, doi: 10.1016/j.tcm.2019.10.010 .
- [8] J. Padgette, K. Scarfone, and L. Chen, "Guide to bluetooth security," NIST special publication, vol. 800, p. 121, 2017

47

GRACIAS

- Preguntas

48

Appendix A

Cybersecurity Analysis of Wearable Device Communication

This appendix introduces the consequent research project, where an analysis of the communication protocol of wearable devices was made.

A.1 Introduction

Internet of Things technologies is evolving and taking part in our daily routines without us even noticing. The continuous growth and acceptance of these devices are going out of proportion, as the new normality shows a person owning multiple IoT devices. It is projected that by the year 2025 there will be over 75 billion connected devices [1]. IoT reaches different scopes, they can be, medicine, education, industry, entertainment, sports, clothes, smart cities, agriculture, and many others. Technology recollects a big amount of data, including personal information, routines, and health records to simplify diverse tasks that we accomplish daily. However, having that great collection of records could be counterproductive, if someone else uses it to gain something. This opens the door for cybercriminals, who understand the value of these types of sensitive data.

Many types of devices are gaining popularity and for this project, we focused on a cybersecurity study of smartwatches due to the diverse amount of data they obtain as they are used all day and recollect data like location, messages, phone calls, and also medical information as heart rate and some type of smartwatches also collect temperature and oxygen saturation (SpO2); the multiple uses they have, as they can be used to track their exercise activities, and their sleeping activity; and the acceptance they have received in the latter years by the public as we see every day more smartwatches, consumers.

This paper focuses on the vulnerabilities of smartwatches during their pairing via Bluetooth with other devices. As Bluetooth has been a victim of different attacks for many years. In section II we show some works done where the authors explain vulnerabilities and different types of attacks done to different smartwatches, also some proposals to the manufacturers and the users to countermeasure these treats. Section III describes the Bluetooth protocol, how it has been evolving, and the security recommendations that are proposed by the Bluetooth guide [2]. Section IV exhibits the difference between pairing methods in Bluetooth devices, exposing the weakest and the safest methods. Section V describes how the cybersecurity study was made and has our findings on the smartwatches that were tested, where a proposal for maximum-security requirements and minimum-security requirements is made with the most necessary security features while pairing two devices via Bluetooth. Section VI expresses the conclusions gathered during this project.

A.2 Communication vulnerabilities of wearable technology

Bluetooth communication has been aimed at multiple types of attacks for years, exploiting the vulnerabilities this technology had in earlier versions. Updates to these protocols have been made to protect devices against eavesdropping and man-in-the-middle attacks. However, the literature shows multiple researchers finding weaknesses in wearable devices, some researchers talk about different attacks that occurred to different IoT devices that communicate via Bluetooth, some countermeasures, and recommendations to users for safer use of this technology, also mention studies that found vulnerabilities in some devices, one of them is a smartwatch, where de PIN that secures its communication with a smartphone was exploited while performing a brute force attack, while the pairing process this smartwatch has is one of the least secure, it shows that smartwatches are prone to attacks [3]. Another study focuses on wearable devices, just as a Fitbit smartwatch, and how they can be a target of man-in-the-middle attacks, using two fake devices, one that disguises itself as a smart device and another one as a mobile app and connects to the Fitbit device, also it adds that Fitbit collects a big amount of sensitive data, and propose to educate the users to be aware of what happens when doing an incorrect use of the device [4]. An investigation shares the importance to teach the users about the correct use of this technology because most of the recommendations always go to the manufacturers, it proposes some guidelines to instruct about wearable devices [5]. Another research worries about the data these devices obtain, for example, the users' location, which exposes them to different types of attacks, also it proposes the constant change of MAC address to avoid any type of targeting [6]. A group of researchers also mention the vulnerabilities of the MAC address in Fitbit devices, as they recollect the MAC addresses of nearby Fitbit devices, and while Fitbit offers a reasonable level of security, they also gather extraneous data about users [7]. In one paper they make passive attacks on wearable devices using Bluetooth sniffers and HCI snoop log and capture an encryption key in plain text [8]. While another article shows the use of Uberthooth and describes an attack where it forces a key renegotiation using eavesdropping techniques [9]. Other works show the potential risks the devices are exposed to when manufacturers do not follow the recommendations of the Bluetooth Special Interest Group, as it happens more often than it should have [10][11].

A.3 Bluetooth

Bluetooth is used for short-range radio-frequency communication. As mentioned before, vulnerabilities can be found in IoT devices and this could be discovered through the Bluetooth protocol, the most common attacks are *man-in-the-middle (MITM)*, where an attacker can obtain the keys that are exchanged between devices, and once obtained these keys to *eavesdrop* in communications [12].

The earliest days of Bluetooth introduced Bluetooth Basic Rate (BR), Enhanced Data Rate (EDR), and High Speed (HS) models. Bluetooth 1.1 and 1.2 versions could only work with BR because they are only capable to support up to 1 megabit per second (Mbps). EDR improves in Bluetooth version 2.0, where it gets data rates up to 3.0 Mbps. HS arrives during Bluetooth 3.0 supporting faster data rates up to 24 Mbps. However, devices that support higher data rates are also able to support lowers lower data rates from earlier Bluetooth specifications. When referring to these versions of Bluetooth are commonly known as Bluetooth Classic.

Bluetooth Low Energy (BLE) was established in the Bluetooth 4.0 specification, later an update was made in versions 4.1 and 4.2. Is useful for wearable medical devices and sensors, because it was primarily made for devices that use a coin cell battery. It reduces power consumption and memory requirements. Improves the efficiency when discovering devices and during connection procedures. This results in packets with shorter lengths, while services and protocols are simpler.

Since Bluetooth 4.0 devices can support both Bluetooth Classic and BLE, this is known as the *dual mode.* Cellphones works as a perfect example, where they might use Bluetooth Classic when connected to earphones and have the necessity to have constant data streaming while also using BLE when connected

to a smart wristband that tracks your activity while doing exercises and you only need the data exchange when you synchronize your devices to check your results.

Bluetooth has five basic security services: *authentication,* using the Bluetooth address to verify the identity of each device during the communication stage, *confidentiality,* guaranteeing that only authorized devices have access to data, avoiding any type of eavesdropping, *authorization,* verifying that a device is authorized to use the service before allowing it to do it, *message integrity* when information is exchanged between two Bluetooth devices, it has to be secure and nothing can be modified, *pairing/bonding,* the generated keys are shared and stored for future use, to create trust between two Bluetooth devices.

To understand the importance of the keys that are exchanged once two devices start pairing, we have to understand the Bluetooth protocols and the security levels to avoid eavesdropping during this process. We are going to discuss these security levels and modes for each Bluetooth specification, first Bluetooth Classic and later Bluetooth Low Energy.

A.4 Bluetooth Classic

Bluetooth includes four security modes, mode 1 has no security, mode 2 has authentication and encryption in the controller while mode 3 has it in the physical link. These 3 modes only exist prior Bluetooth 2.1 version. In this article, we only test communication between devices that have a Bluetooth version higher than the Bluetooth 2.1 version. For these devices, it is mandatory to work with a security mode 4. Security Mode 4 is a service-level enforced security mode, it uses secure simple pairing (SSP) and it uses Elliptic-curve Diffie–Hellman (ECDH) key agreement for link key generation, this helps for protection against eavesdropping and man-in-the-middle attacks. The ECDH that is used could be the elliptic curve 192 or 256. For authentication and encryption, a secret symmetric key is necessary and it is known as the *link key*. Security mode 4 includes five security levels. Starting from security level 0 and ending in security level 4. Level 0 has no security and it is only allowed for service discovery protocol, level 1 also does not require security, level 2 requires an unauthenticated link key, while level 3 requires an authenticated link key, and level 4 requires authenticating the link key using secure connections. Secure connections pairing protocol was introduced in Bluetooth 4.1 and it uses the ECDH 256, improving from the ECDH 192 that was used prior.

A.5 Bluetooth Low Energy

This section explains meticulously BLE, to understand how is possible to protect against the most common attacks on this technology.

Bluetooth 4.0, 4.1, and 4.2 count cryptographic keys to improving security in the devices, these keys are named: *Identity Resolving Key (IRK),* to support low energy private device addresses, and *Connections Signature Resolving Key (CSRK),* to assist data signing. When pairing BLE devices a Long-Term Key (LTK) is generated, and it is important for authentication and encryption (known as the *link key* in Bluetooth Classic), this could result in two different methods. During the first method, one device generates the LTK and sends it to the other device in a secure manner, and this is known as *low energy Legacy Pairing,* also is important to notice that for this method, while pairing, all the keys are distributed in a secure process, during the same stage. For the second method case, both devices create the key without the need to share it through the link, this method is called *low energy Secure Connections,* meanwhile, this LTK is going to be generated while the IRK and the CSRK are created and distributed securely. An important difference between these methods is that low energy Legacy Pairing does not count with Elliptic-curve Diffie–Hellman (ECDH) encryption and this results in being vulnerable against eavesdropping attacks and it lets the attackers the opportunity to find the LTK, while Low energy Secure Connections can countermeasure this threat. We will review these pairing methods with more details later in this paper.

Low energy Security includes two modes. Security Mode 1 has four levels related to encryption. Level 1 does not require encryption and authentication. Level 2 asks for unauthenticated pairing with encryption. Level 3 needs authenticated pairing with encryption. Level 4 uses the Secure Connections method

previously discussed in this section as it asks for authenticated link key using low energy Secure Connections pairing with encryption. Security Mode 2 requires data signing in both of its levels, with the sole difference that level 1 only needs unauthenticated pairing while level 2 asks for authenticated pairing. Because encryption is a great security asset, using Security Mode 1 Level 3 or 4 is strongly recommended over other options.

A.6 Pairing Methods

In this section, we show a more detailed explanation of the low energy pairing methods and describe the phases that occurred during the pairing methods. Starting with low energy Legacy Pairing. In phase one, once explore the input/output capabilities and security requirements in the devices, they will establish an agreement on a Temporary Key (TK), in phase two, they proceed to create a Short Term Key (STK) using random values that are being exchanged and the TK, this STK establish an encrypted link between devices, to end in phase three when it assures a safe key transport for all the keys mentioned earlier in this article (LTK, IRK, CSRK). Low energy Secure Connections works in a different manner, even if phase one works the same way as in legacy pairing, in phase two the LTK is generated without the need of the STK. This LTK is useful in phase three, and the LTK encrypts the links and a key agreement is made to distribute the IRK and CSRK securely instead of using a key transport.

During the pairing process between two devices, it can be applied one out of four different pairing processes. These pairing processes are: a) Out of Band; b) Numeric Comparison; c) Passkey Entry; and d) Just Works. The input/output capabilities of devices play an important role to determine what process can be utilized.

The out-of-band process needs two devices that have out-of-band (OOB) technology, an example is a near-field communication (NFC). A device sends another device a 128-bit number which is the TK using OOB technology. Using low energy Legacy Paring results in one-in-a-million protection from MITM attacks, to guess the TK. Nevertheless, the protection comes from the OOB technology that the device uses because if someone is capable to eavesdrop on the OOB, it will obtain the TK values. For low energy Secure connections, the device address is sent through the OOB and given this even if, an eavesdropper can obtain it, this does not give them any value to decrypt the data.

Numeric comparison is an option for low energy Secure Connections only, this method isn't available for low energy Legacy Pairing. This works when two devices display on a screen a 6-digit number while the user can enter one of the following options: *YES*, in the case when both displays show the same 6-digit number, and *NO*, if the number that is being shown is different. The previous 6-digit number is not used to generate the link key, this is to avoid eavesdropping because even if an unauthorized person can capture this 6-digit number it will not be useful for any further pairing process. It also has protection against MITM attacks, at the moment the user enters one of the options to confirm if the 6-digit number is or is not the same in both devices, this guarantees that no other device can initialize the pairing process.

Another method is passkey entry, it requires that both devices include a keyboard input or at least one does it while the other has a display output. This method works with low energy Legacy Pairing. A passkey is given in a device and entered in the other one, then it generates a TK using the passkey. The passkey is required to be six numeric digits, which would give an entropy of twenty bits that assure the complexity of deciphering the given key. Low energy Secure Connections pairing works differently. After the devices exchange the public keys the six numeric digits passkey is generated and once is entered into the device it starts sending a hash of each bit of the passkey, this procedure is repeated twenty times, to complete the twenty bits of the passkey. Also, the public keys are sent during the previous step. This method offers protection against MITM attacks, when using a passkey of six digits, it gives an attacker a one-in-a-million chance to guess the correct passkey.

The last method is the least secure one and it is used due to the limitation in the input/output capabilities of the devices. For low energy Legacy Pairing the key is always the same and is set to all zeros, leaving the pairing exposed to eavesdropping and MITM attacks. For low energy Secure connections, it will follow the same steps as in the numeric comparison process, but the user is not able to see the 6-digit number

because in this procedure the devices are unable to do this, and it results in not being able to do the final commitments checks.

These 4 pairing methods are not exclusive to Bluetooth Low Energy, they can also be found in Bluetooth Classic, working slightly differently due to the IRK and CSRK being exclusive for BLE. Only the LTK is set to be created but it is known as link key. The association models (out of band, numeric comparison, and passkey entry) provide authenticated link keys, meanwhile, the link key is unauthenticated during the just works pairing model for Bluetooth Classic.

A.7 Cybersecurity Analysis

For this project, we aimed to exploit the vulnerabilities of the Bluetooth protocol in wearable devices due to the increment in use that they are showing in the general public. We chose to study various types of smartwatches because the limitations they might have in hardware and their input/output capabilities gave us reasons to believe that they could be unable to follow every step of the Bluetooth protocol guidelines [2]. Smartwatches are in consideration for medical diagnosis. For example, in 2018, the Food and Drug Administration (FDA) cleared the Apple Watch Series 4 and named it a class 2 medical device [13], because of its ability to identify atrial fibrillation (AF), this shows that manufacturers are designing smartwatches that can obtain sensitive data and because no standard has to be followed to design these devices, they create a world of possibilities for cybercriminals. We tested six different smartwatches, all of them include the heart rate detection function while others also include blood oxygen saturation (SpO2) detection. These features could encourage the user to seek medical advice when necessary and save multiple lives, due to these reasons it is important to guarantee confidentiality, integrity, and availability of these data for the smartwatch users.

To test the security features during the Bluetooth pairing process of these devices, we implemented a passive sniffing attack, where we captured the traffic sent between devices, we used *the Bluefruit LE Sniffer - Bluetooth Low Energy (BLE 4.0) - nRF51822 - Firmware Version 2*, designed by *adafrui*t, it allowed us to listen to only BLE devices and captured its traffic, once we obtained it, we started analyzing the data packets using *Wireshark*, an open-source packet analyzer. We found that once the smartwatches established a bonding with a smartphone, the sniffer stopped capturing data from the devices because their connection is encrypted thanks to the key exchange or agreement they do during pairing. We explored other ways to analyze the pairing process of our devices. Except for the Apple Watch Series 2, all of the devices were paired with a Samsung Galaxy S20, this smartphone has Bluetooth 5.0 dual mode that allows it to connect to devices with BLE and Bluetooth Classic. It also has the feature to generate a *Bluetooth host controller interface (HCI) snoop log*, which gives us the option to obtain records of the Bluetooth data that our smartphone is generating while pairing with other devices. There are multiple ways to obtain the HCI log, for the one we selected we must generate a *bug report* in our smartphone, and after that, we extract all the Bluetooth activity from the *.txt* version of the bug report thanks to the *btsnooz* script.

$$btsnooz.py\ original\_bug\_report.txt\ >\ new\_bluetooth\_snoop.log \quad (1)$$

With the study we were able to find the way different smartwatches work during pairing, the lack of standardization for wearable design shows multiple differences inside the security scope, table 1 includes the devices that were analyzed during this project and their features. We show the Bluetooth version of each device and if their pairing method is done by the Bluetooth Classic mode or the BLE mode. For the smartwatch Fitbit Versa 3, we learned that it works with the Bluetooth dual mode because it has one feature that allows the user to make and receive calls, for this device we decided to separate this feature and list it as another device due to the requirement to do another pairing process to use it. First, you pair your smartwatch to your smartphone via BLE, and then if you want to make use of the phone features to make and receive calls you must start another pairing via Bluetooth Classic. Table 1 also shows the pairing association model these devices use, sometimes they include more than one model, the reason is to be able to pair to smartphones with different input/output capabilities, nevertheless, some of these association models are less secure than others. We can see the security mode and their respective levels previously discussed in this article. Another feature that we noticed during the testing of these devices is that some of

the smartwatches have a static address for the device and this could be identified quickly and reveal what kind of device is and its version, this allows a cybercriminal to discover the objective and gather more information about the device simply.

Table 1: Bluetooth features of the analyzed devices.

Devices	Bluetooth Version	Low Energy Pairing	Pairing Methods	Pairing Association Model	Passkey	Security Mode	Level	Static Address
Fitbit Versa 2	4.0	✓	Low Energy Legacy Pairing	Passkey Entry	4 digits	1	3	✓
Fitbit Versa 3	5.0	✓	Low Energy Legacy Pairing	Passkey Entry	4 digits	1	3	✓
Versa 3 Controls	5.0	×	Secure Simple Pairing	Numeric Comparison	6 digits	4	4	✓
Apple Watch Series 2 Aluminum	4.0	✓	Low Energy Legacy Pairing	Passkey Entry / Out of Band (OOB)	6 digits	1	3	×
Garmin vivoactive 3	4.2	✓	Low Energy Secure Connections	Passkey Entry	6 digits	1	4	✓
Amazfit GTS 2 mini	5.0	✓	Low Energy Legacy Pairing	Out of Band (OOB) / Just Works	None	1	3	✓
W27 Pro	3.0+5.0	×	Secure Simple Pairing	Just Works	None	4	2	✓

After understanding how these smartwatches work during pairing, we started to propose a model for the maximum-security requirements identified that a wearable device must be included while connecting via Bluetooth. Also taking into account the many countermeasures that the Bluetooth standard has applied to the most common attacks, eavesdropping, and man-in-the-middle, it is important to note that there is a minimum of security requirements that must be included in every wearable device to be able to take care of these attacks, for this reason, figure 1 also includes a proposal to meet these requirements to accomplish the minimum standard of security. The features mentioned are a) Low Energy Pairing method, this feature is at the base of our scale, because is the one we consider the most important one because the focus of this research is smartwatches and they are wearable devices that must use the BLE protocol to reach their ideal functionality; b) Secure Connections Pairing, as mentioned earlier, secure connections is the most secure pairing procedure and it was introduced in the Bluetooth version 4.1 for Bluetooth Classic and in version 4.2 for BLE this has significant weight in our scale, nevertheless, lower security methods have authenticated pairing and encryption while they do not offer protection against eavesdropping are better protocols and recommended for their use instead of unauthenticated pairing that also do not offer man-in-the-middle protection; c) ECDH Key, ECDH-based cryptography also offers protection against eavesdroppers, our proposal for minimum security and our proposal for maximum security show a slightly difference due to the existence of two methods for ECDH-based cryptography, to gain the maximum security grade it must work with a P-256 elliptic curve, while another methos might use a P-192 elliptic curve that still offers protection against eavesdrop attacks; d) Non Static Address, even if not changing the address could attract the interest of different attackers, we do not give a big impact to this feature for our scale because in the BLE pairing process the IRK helps to countermeasures attacks that aims to exploit the address of the device, however changing the address occasionally would give our devices the best protection against other type of attacks; e) Just Works association model unavailable, when referring to the association models, it is important to notice that Just Works is the least secure, this is commonly used

when a device or both devices do not have the input/output capabilities required to pair using another method, for the best security practices, smartwatches should not include this feature and use another association model instead, however if they include this pairing process, the user should be responsible and instead choose the safest pairing association model instead; f) 6-digit numbers key, this feature appears in two association models, passkey entry and numeric comparison, as some of these devices only include a 4-digit it is worth to notice that it only makes a great difference if you using the passkey entry model because the secure connections method requires using a 6-digit passkey for maximum security, however, this number is not used to create any security key, this means that even if a cybercriminal gets stole this number generated by the device, it would not be useful to do any type of eavesdropping attack to the smartwatch; and g) OOB association model, for BLE legacy pairing this association model is the one that is considered the most secure, even if we do not consider it necessary for the minimum security requirements proposal, as we just mentioned, for devices that work with BLE legacy pairing as the Apple Watch Series 2, it offers the maximum security a device could have during pairing.

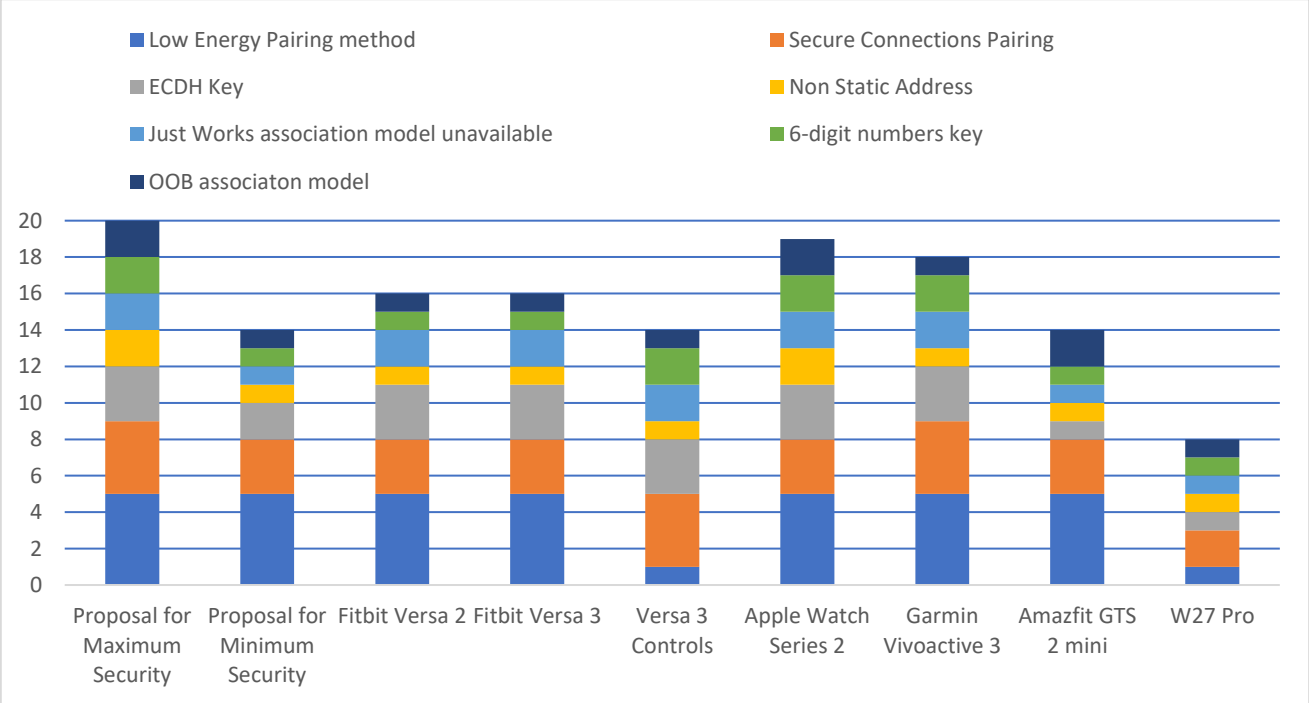


Figure 1: Security requirements comparison for smartwatches

A.8 Conclusions

The increase in popularity of wearable devices and the continuous adoption by a large portion of the population to allow this technology to track their daily routines requires that the manufacturers of these devices can ensure the confidentiality, integrity, and availability of data that is being gathered. As some of the most recent smartwatches collect sensitive data, just as health information, in an accurate manner that allows users to gain trust in these devices and know when to reach for a medical consultation. Protection against all types of cyberattacks is vital for upcoming technology. The guide to Bluetooth security gives recommendations to have the maximum security for this communication protocol, but as we showed during our cybersecurity study, those guidelines are not always followed entirely, some modifications are made to accomplish the main objectives during the design of the devices. The tests exhibited that some devices do not include the most recent security protocol even if they work with the newest Bluetooth version, as seen when comparing Fitbit Versa 2 and Fitbit Versa 3, the former has the Bluetooth 4.0 version, for this reason, it does not work with the safest pairing protocol as it was not created yet,

meanwhile, the latter, includes the Bluetooth 5.0 version, and still uses the same security protocol as its previous version. Another device does not pair with the BLE protocol, ignoring the recommendations given, not only for better security but also for better usability. While the tested devices currently do not follow the safest protocols, the proposal for minimum security that is shown in this paper is met by almost all the devices, revealing that manufacturers accomplish what is required by the Bluetooth standard.

References

[1] L. S. Vailshery, “Iot and non-iot connections worldwide 2010-2025,” Statista, March, vol. 8, 2021.

[2] J. Padgette, K. Scarfone, and L. Chen, “Guide to bluetooth security,” NIST special publication, vol. 800,p.121,2017.

[3] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, “Security vulnerabilities in bluetooth technology as used in iot,” Journal of Sensor and Actuator Networks, vol. 7, no. 3, p. 28, 2018.

[4] F. Blow, Y.-H. Hu, and M. Hoppa, “A study on vulnerabilities and threats to wearable devices,” in Journal of The Colloquium for Information Systems Security Education, vol. 7, 2020, pp. 7–7.

[5] M. Bada and B. von Solms, “A cybersecurity guide for using fitness devices,” in The Fifth International Conference on Safety and Security with IoT, Springer, 2023, pp. 35–45.

[6] C. Zhang, H. Shahriar, and A. K. Riad, “Security and privacy analysis of wearable health device,” in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMP-SAC), IEEE, 2020, pp.1767–1772.

[7] B. Cyr, W. Horn, D. Miao, and M. Specter, “Security analysis of wearable fitness devices (fitbit),” MassachusettsInstituteofTechnology,vol.1,2014.

[8] B. Cusack, B. Antony, G. Ward, and S. Mody, “Assessment of security vulnerabilities in wearable devices,”2017.

[9] M. Ryan, “Bluetooth: With low energy comes low security,” in 7th USENIX Workshop on Offensive Technologies(WOOT13),2013.

[10] Y. Kurt Peker, G. Bello, and A. J. Perez, “On the security of bluetooth low energy in two consumer wearable heart rate monitors/sensing devices,” Sensors, vol. 22, no. 3, p. 988, 2022.

[11] T. Rosa, “Bypassing passkey authentication in bluetooth low energy,” Cryptology ePrint Archive, 2013.

[12] C. T. Hager and S. F. MidKiff, “An analysis of bluetooth security vulnerabilities,” in 2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003., IEEE, vol. 3, 2003, pp. 1825–1831.

[13] M. Basza, B. Krzowski, P. Balsam, M. Grabowski, G. Opolski, and L. Koltowski, “An apple watch a day keeps the doctor away?” Cardiology Journal, vol. 28, no. 6, pp. 801–803, 2021.10.