NTNU – Trondheim
Norwegian University of
Science and Technology

IT Risk Assessment Automation in Healthcare Networks

Daniel del Riego San Martín

Submission date:	June 2022
Supervisor:	Sokratis Katsikas, NTNU
Co-supervisor:	Ahmed Walid Amro, NTNU

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title:	IT Risk Assessment Automation in Healthcare Networks
Student:	Daniel del Riego San Martín

Problem description:

Medical networks have become a big issue in cybersecurity terms as a great number of new connected devices has been introduced. This means more possibilities for the attackers to enter the network and harm by stealing data, denying the service or even modifying the functioning of the devices, directly harming the patient.

Risk assessment methodologies have been developed in many different industrial sectors and they are performed by specialists in cyber risks. However, healthcare is unique as an industry and not many specialists work in this area.

Because of this, the idea of creating a special risk assessment for this kind of network that could be automated emerged. This way, not even a professional is needed, saving costs, and security quality will rise.

Date approved:	2022-03-14
Responsible professor:	Sokratis Katsikas, NTNU
Supervisor(s):	Ahmed Walid Amro, NTNU

Abstract

Cybersecurity has become a hot topic lately because of its importance in almost every industry. However, it has not been given the same relevancy everywhere and healthcare is an example. Millions of new devices have been added to medical networks all over the world and the industry does not have the capacity to assess the risk for all of them, as computer networks are not one of their specialties.

In this thesis, a survey of the different vulnerabilities that these medical networks can have, along with the different attacks that aim especially at them, has been carried out to understand the level of danger they are into. Furthermore, the recommended countermeasures for avoiding these breaches from happening are also studied.

In the next step, both the different standards that are mandatory to comply in healthcare networks as well as the different risk assessment methods that currently exist for healthcare and other industries are studied (quantitative and qualitative), achieving a general view of the possible solutions.

It is then proposed how a good automated risk assessment methodology could be done by mixing the information of the standards, the attacks, the countermeasures and classifying the devices according to their criticality. With all this data, it is possible to create an algorithm that calculates the total risk of each attack in a numerical way for each asset and suggests different ways to face it.

This algorithm is coded in Python, generating different results for three different scenarios in which the criticality of the medical device changes. These three scenarios were also given to an expert in cybersecurity in healthcare networks, who proceeded to perform his own risk assessment in order to be compared with the created tool.

The results were satisfactory as both the tool and the expert coincided in the main attacks and their countermeasures. However, given environments were too small to be considered realistic yet and further development must be done to be able to assess the risk of a whole hospital network.

Preface

Wow, this was hard. I have just finished my Master's Thesis, and I am not pretty sure how to feel. I hope whoever is reading it right now finds it interesting and helpful. If not, at least I did my best to try to give something to the world.

I want to thank my family for supporting me all the way until now that I have become an engineer. Specially my parents, who always provided me with everything I needed to keep on this hard trail. I also want to say special thanks to my sister, now fellow engineer, who has shown me the way. This is as yours as mine. I love you all.

At this moment, I also want to have my closest friends in mind. Some of them have been there during my whole academic life, even elementary school.

I am also grateful to all the teachers that, with their passion, have taught me to love what I do. Very special thanks to Ahmed Walid Amro, who successfully guided me to achieve a thesis after many, many meetings, and Sokratis Katsikas, who gave me the opportunity of doing it even before knowing me.

Lastly, thank you for reading it. This is all. I hope you enjoy it.

- Dani -

Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction

1.1 Motivation

NTNU Healthcare is one of the most sensitive areas. There is a big concern on the importance of not having any failure in the physical world, for example with a proper diagnosis [1]. Nevertheless, some may forget about the importance of the virtual world.

At this very moment, society is living a technological revolution with the appearance of 5G, the latest generation of mobile connectivity, which enables a larger, faster and instantaneous network of devices. This is generating (and will generate even more) a large number of new devices and data that needs to be handled and processed.

Healthcare has not been left behind in this issue, and an IoMT (Internet of Medical Things) has emerged [2], which is an evolution in terms of quality of treatment and monitoring, as sensors and actuators start to be connected to the network and can be accessed from anywhere. However, it also implies that all the data retrieved must be sent through the net to data centers, servers or whatever solution the clinic has installed, exposing personal information and the well functioning of the network to any kind of attack.

These attacks do not only affect with the inconvenience of having to repair their damages, but also may put in danger the health of patients by delaying or deleting appointments, losing personal records or making devices malfunction while using them.

Because of this reason, is paramount to minimize the chances of suffering an attack or a simple malfunction of the network, which can be achieved by a cautious risk assessment of the network.

Apart from its difficulty and even though there are several ways to develop the mentioned risk assessment, including ISO standards, most of them tend to coincide in a big dependence on human opinion and intervention, which, in most cases, works. However, it may lead to human errors because of a lack of knowledge or not being able to audit a whole network.

From these facts, comes the necessity of automation of the whole process. Developing a standardized program that can find out problems in the network configuration that may pose a hazard, what risks can appear after it, evaluate them and take actions against them. This way, the risk assessment will not depend that much on human opinion but on a computer analysis, providing the healthcare company with all the information necessary to solve any issues in a cheaper and more understandable way.

Currently, some programs exist that automate the search for vulnerabilities in networks and that will be explained in the posterior sections of this thesis. However, they are based on testing instead of analyzing theoretically the network and, moreover, they are not specialized in healthcare networks.

1.2 Research Questions

Because of previously explained issues, the Master's Thesis will consist in choosing the best source to perform the risk assessment, finding the way to make it developed by a computer and checking its feasibility. So the research questions covered could be summed up in:

RQ1 What is a risk assessment process that is suitable for healthcare networks?

RQ2 How can that process be adapted to support the automation of certain tasks?

RQ3 How different would be this approach compared to the one made by an expert?

1.3 Thesis scope

In this thesis, not only the previous questions will be researched looking for an answer, but also a first practical approach will be implemented. First of all, a background of the topic as well as a state of the art of the technology will be provided, accompanying a summary of the most important standards in the area. Then, a solution with implementation will take part and lastly the results obtained will be discussed, finding a conclusion and the path to follow after this project.

Chapter 2 Background

In this second chapter, further information regarding the industry, the technologies, the methodologies and more will be provided.

2.1 Healthcare as an industry

According to WHO [3], healthcare is an industry that spends US$ 8,5 trillion, or, what is the same, 9.8% of the global gross domestic product. Only the United States contributed to 42% of that amount.

In high-income countries, most of the investment in health relies upon government sources, so health is considered a service that states provides+ and the tendency is to grow over the years as it has been going on [4].

To mitigate this extra spending, healthcare providers are considering the use of remote patient monitoring (RPM) tools, that enable the stream of real-time data between patients and doctors. These techniques would increase incomes as they keep costs lower. According to the source [4], 30 million US patients will use this kind of tools by 2024.

From the consumer perspective, which in the case of healthcare are named patients, there has been a huge change in the way the industry is seen, specially impulsed by the COVID-19 outbreak. According to Deloitte [5], 77% of consumers that use tracking devices consider that they change their behavior to a more healthy way and that, if needed, more than a half would be comfortable sharing that monitored information with their healthcare provider to receive better care or alert in case of emergency. However, they still consider in-person attendance necessary for a good treatment.

2.2 Medical devices

According to the FDA [6], a medical device is "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease in man or other animals or intended to affect the structure or any function of the body of man or other animals and does not achieve its primary intended purposes through chemical action within or on the body of man or other animals which is not dependent upon being metabolized for the achievement of its primary intended purposes".

These devices, according to FDA [7], are assigned to one of three regulatory classes based on the level of control necessary to assure the safety and effectiveness of the device. The classes considered are: Class I General Controls, Class II General Controls and Special Controls (which in Europe are divided into IIa and IIb) and Class III (General Controls and Premarket Approval). Device classification depends on the intended use of the device and the indications for use. In addition, it also depends on the risk it takes, having Class I the lowest risk and Class III the highest. For the reader to have an idea of how wide a medical device concept is and how it may be classified, a regular wheelchair would be Class I while an implantable pacemaker would be Class III [8].

2.2.1 Connected Medical Devices

Inside medical devices, there are connected medical devices. Deloitte [9] defines them as one which is able to generate, collect, analyze or transmit data or images, and can connect to health care provider networks and transmit data to either a cloud repository or internal servers in order to prevent, diagnose or treat diseases.

2.3 IT in healthcare

2.3.1 IoMT Layers

According to [10], there are 5 layers in IoMT architecture:

Perception Layer

It acquires and collects patients' data using physical equipment and transfers it to the network. It can be divided in:

1. Wearable devices: They enable accurate, continuous, real-time monitoring of patients with sensors for location, temperature, blood pressure, heart monitoring, activity and more.

2. Implantable devices: They are fitted inside a patient's body and can be a swallowable camera capsule or an embedded cardiac, for instance.

3. Ambient devices: They sense the patient's area to monitor activity patterns, sleep quality or bathroom visits, among other things, even provide alerts to caregivers if needed. They may include sensors for motion, temperature, pressure and more.

4. Stationary devices: They are not always with the patient. They might be imaging devices, to create visual representations of the interior of the body (MRI, CT or X-rays), or surgical devices.

Network Layer

It is responsible for content delivery, content discovery, routing content and network addressing. Different kinds of media can be used in this layer. Wired/WiFi is used often in stationary devices because their need for a reliable power source and high speed. Radio communication with technologies like 3G, 4G or LTE is used for long distances whereas Bluetooth is used in wearables or to connect sensors in the same room. Lastly, medical devices may connect via WSNs through WiFI or low-powered wireless personal area network.

Middleware

This layer controls the collecting and filtering of the received data from perception layer devices, performing services discovery and providing access to control the devices. Cloud-based platforms are a trend now for middleware.

Application Layer

It is the interface where users connect with the devices through the middleware. It also defines the applications and services that the user can use. There are different protocols for the application layer as TCP/IP and more.

Business Layer

It handles healthcare's provider business logic and supports the business process life cycle. It also extracts knowledge from IoMT data.

2.3.2 Special characteristics

Healthcare networks are special by themselves and have been growing drastically during recent years due to connected medical devices without properly updating their core. This kind of device presents characteristics and vulnerabilities typical only of this kind of system [11]:

Providing hackers with vital information

A common mistake is that the device information does not include cybersecurity approaches and relies on the secrecy of proprietary ciphers or protocols. Sound security principles dictate that a system's security must not depend on the secrecy of the algorithm or hardware [12]. Apart from that, they publish device verification information, radio frequency transmission data and device working, which opens a gap for hackers to reverse engineer if a not good enough cybersecurity solution is used [11].

Legacy operative system and software

Legacy systems are the ones that have been for a long time in the network and perform critical functions. It is impossible to update because of compatibility issues and in case of replacement, more changes in other devices need to be made. This characteristic also delays the installation of updates in software and patches, because they have to be totally proven for interoperability. [13].

Lack of basic security features

Most hospitals do not have an IT (Information Technology) and MT (Medical Technology) departments altogether, but two separated ones, creating grey zones where none of them actuates [14]. Apart from that, some devices such as computed tomography scanners delivering measured radiation can be tampered, threatening patient safety issues. Moreover, security features added after design can disrupt the clinical flow, slow down the device or reduce battery life (which in some cases is crucial) [15].

Web services are a popular solution for interfacing with existing systems

Because it is useful for the interoperability of different software, the representation of data in a structured way and the possibility of externalizing the services [16]. However, they suppose a weak spot to receive attacks due to its easy accessibility and lack of secure authentication and encryption.

Compromised medical devices can be used to attack other sections of the healthcare organization network

It should never be taken for granted that the surroundings of a device have not been compromised because the propagation of an attack is possible. It is especially important because of the large increase in connected devices. Due to this, all the security measures such as network fragmentation should be considered to stop the spreading of any attack. [15].

Lack of awareness of the cybersecurity issues and poor security practices

The healthcare industry is behind other industries in protecting its infrastructure. In addition, it revealed a lack of awareness among healthcare facilities managers regarding the sophistication of hackers and their means to infiltrate confidential patient data networks [17]. Behaviors such as password sharing, lack of secure disposal of devices and inconsistent education are common yet in this industry.

Security and privacy goals and health care utility and safety can be challenging in case of emergencies

Sometimes the impossibility of access instantly medical records by a doctor may mean the loss of a critical time in the patient's health and safety during an emergency.

2.4 Possible Attacks

Even though the same kind of attack might work in different layers of the architecture, in this project they are going to be separated by its most common scenario as in [10].

2.4.1 Perception Layer

Physical attacks

One strategy to blunt the IoT devices successfully is by the physical attack on the infrastructure of an IoT. For example, an adversary can change the behavior or structure of devices involved in an IoT system [18] to partially or totally stop its functionality by manipulating it, installing software or simply breaking it.

Battery drainage attacks

It is an attack on battery power. As the battery life of the IoT device is more than 10 years, its battery drains very slowly. In this type of attack, the eavesdropper sends a large number of request messages to the device. The device responds according to request, which consumes much energy, i.e., battery usage is very high. As a result, the device's battery drains rapidly. It will create a critical condition for the patient, who implants this healthcare device [19].

2.4.2 Network Layer

According to [20], the generic attacks that may be more dangerous in the IoMT network layer and risk the objectives previously discussed are the following:

Eavesdropping attacks

Eavesdropping is an attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant [21] or just listen to private communication breaking confidentiality [22].

Spoofing attacks

A spoofing attack is faking the sending address of a transmission to gain illegal entry into a secure system [23]. With this attack, the attacker pretends to be a legal device, waiting for the remote application to send the authentication credential of a user for login, which breaks the authentication objective [24].

Traffic analysis attacks

Traffic analysis is gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence. For example, an adversary may be able to detect a signal from a reader that could enable it to infer that a particular activity is occurring without necessarily learning an identifier or associated data [25].

Masquerading attacks

Masquerade attacks are a common security problem that are a consequence of identity theft and that are generally motivated by data theft. Such attacks are characterized by a system user illegitimately posing as another legitimate user [26].

Man-in-the-middle (MITM) attacks

An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them. In the context of authentication, the attacker would be positioned between claimant and verifier, between registrant and CSP during enrollment, or between subscriber and CSP during authenticator binding [27]. A common MITM attack scenario may involve the attacker as a third-party intercommunicating node between a client and a server. In this case, the attacker often decisively captures messages between the client and the server. The client and a server are communicating with each other under this environment of pseudo-safety. Typically, this is achieved in an Ethernet LAN environment by ARP poisoning [28].

Denial-of-service (DoS) attacks

DoS is the prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided) [29]. There are two categories of DoS attacks in IoT: a Distributed Denial Of Service (DDoS) and Ordinary DoS. For a common DoS attack, a tool is required to send packets to an intended system that crash the network or sometimes force the system to restart. Meanwhile, DDoS can be a single attacker but not as powerful as a proxy attacker. The impact of this attack not only disables the network but also prevents it to be accessible by a very large number of devices [18].

Impersonation attacks

In this type of scenario, the attacker impersonates the verifier in an authentication protocol, usually to capture information that can be used to masquerade as a claimant to the real verifier [30].

Message fabrication/modification/replay attacks

In message fabrication/modification and replay attacks, the adversary can construct, change, or resend already transmitted messages between legitimate entities with the intent of producing an unauthorized effect or gaining unauthorized access [31].

2.4.3 Middleware

As middleware often uses web services to provide of value-added services [32], attacks may be similar to and shared with the application layer.

Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application where they are currently authenticated. With help from social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state-changing requests. For most sites, browser requests automatically include any associated credentials, such as the user's session cookie, IP address, Windows domain credentials, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim [33].

Session Hijacking

The Session Hijacking attack exploits the web session control mechanism, which is normally managed for a session token. Because HTTP communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server [34].

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser-side script, to a different end-user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site [35].

2.4.4 Application Layer

SQL injection

A SQL injection attack consists of the insertion of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands [36].

Account hijacking

Many IoT devices communicate in clear text format at the network level or have weak encryption in place. An attacker can perform account hijacking by intercepting the packet while an end-user is being authenticated. Old operating systems that have unpatched vulnerabilities are the main factor in the rise of this attack, as described in many incidents [10]

Malware attacks

Malware attacks consist of a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim [37]. Worms are probably the most destructive and dangerous form of malware on the internet. It is the self-replicating program which harms the computer by using security holes in networking software and hardware. It can delete the files in the system, steals the information like passwords, they can also change the passwords without your notice, cause computer lockouts, etc [18].

Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system by locking the users' files (which may contain patient records) until a huge ransom is paid. More modern ransomware families, collectively categorized as crypto ransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decryption key [38]. An infected machine can spread the virus through the whole network.

Brute force attack

A brute force attack can manifest itself in many different ways, but primarily consists of an attacker configuring predetermined values, making requests to a server using those values, and then analyzing the response. For the sake of efficiency, an attacker may use a dictionary attack (with or without mutations) or a traditional brute-force attack (with given classes of characters, e.g.: alphanumeric, special, case (in)sensitive). Considering a given method, number of tries, efficiency of the system which conducts the attack, and estimated efficiency of the system which is attacked, the attacker is able to calculate, approximately, how long it will take to submit all chosen predetermined values [39].

Denial-of-service (DoS) attacks

DoS is the prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided) [29]. There are two categories of DoS attacks in IoT: a Distributed Denial Of Service (DDoS) and Ordinary DoS. For a common DoS attack, a tool is required to send packets to an intended system that crash the network or sometimes force the system to restart. Meanwhile, DDoS can be a single attacker but not as powerful as a proxy attacker. The impact of this attack not only disables the network but also prevents it to be accessible by a very large number of devices [18].

2.4.5 Business Layer

Information disclosure

Information disclosure happens when an application fails to properly protect sensitive and confidential information from exposure to users who are not normally supposed to have access to that data. While such issues are not exploitable in most cases, they are still considered web application security issues because they allow malicious hackers to gather valuable information that can be used later in the attack lifecycle. Armed with such data, attackers can achieve much more than they could without it [40].

Deception

The general definition of deception is the use of dishonest or illegal methods to make people believe that something is true when it is not [41]. Adapted to the information and communication technology by [42] is "the intentional control of information in a technologically mediated message to create a false belief in the receiver of the message". Briefly explained, it consists of introducing fake information for the system to treat it like proper data. The system is unable to differentiate a corrupted file from a real one.

2.5 Countermeasures

A different set of countermeasures should be taken in each layer in order to avoid the attacks. According to [43], these countermeasures may include:

2.5.1 Physical Layer

Proper authentication is needed to identify all the devices and to allow access to the network only to those who are supposed to. Mutual authentication is needed to achieve a higher level of security and, with the small computational power of most IoT devices, new algorithms and mechanisms must be used [44].

Checking the integrity of the data received in the actuator (not only because of an attacker modifying it but because of errors in the actual sender) is also important to preserve the patient's health, and mechanisms such as parity bit [45] or checksum [46] should be used as well as a hash, if the computational power allows it.

The usage of an up-to-date protocol to communicate as IPSec will provide the architecture with identification through IP and will reduce the CPU load (which is critical in IoMT) by 20% [47].

Lastly, there must be physical security in the devices. Apart from considering good hardware for the design, it should not be easily accessible or replaceable if it contains or manage critical data or can affect the availability of the system, for instance [48].

2.5.2 Network Layer

To achieve the objective of data privacy, all the information must travel encrypted. However, encryption can happen at network level (by-hop encryption mechanism) [49] or application level (end-to-end encryption mechanism)[50]. The problem with encryption at network level is that each node must decrypt and encrypt, having the data in plain text, while, in end-to-end encryption, this does not happen. However, network layer encryption works for all the different business applications, making all of them equally safely implemented. To achieve the highest level of security, as it is needed in a medical environment, specific made encryption, only achievable with end-to-end encryption, should be used. This is why encryption does not occur in this layer but in the Application layer [51].

Routing security should be guaranteed, not letting routing hijacking happen [52] or the devices not being reachable. This is not an easy-to-solve issue, but can be achieved using different paths to communicate, which increases error detection in the network and redundancy [53]. This solution, working together with a hash [54] (that must be high-quality-generated as well as low consuming)[55], is useful to guarantee data integrity and availability.

2.5.3 Middleware

The use of cloud dedicated servers for this function has improved the quality and the possibilities of data processing. However, it implies sending private information outside of the healthcare network. Solutions such as VPC (Virtual Private Cloud) have emerged to try to solve this issue [56], but it is not enough when talking about health information.

To achieve data security, a solution might be distributing the data over multiple cloud service providers in such a way that none of the providers can successfully retrieve meaningful information from the data pieces allocated at their servers

[57]. Apart from that, redundancy in data distribution is crucial to guarantee the availability of the system [58]. This technique is called: Fragmentation Redundancy Scattering (FRS). Other authors like [59] suggested the idea of using blockchain technology when storing data, but it is disregarded yet due to the impossibility of changing or deleting that information (legal reasons) and the massive amount of information that healthcare generates, much more than finances, which are what blockchain was created for.

To avoid decrypting the data and working with it in plaintext, fully homomorphic encryption (FHE) should be considered [49]. This mechanism allows anyone to transform an encryption message into an encryption of any function of that message, which allows to operate the ciphered data [60].

Apart from that, vigilance over the web weaknesses or accesses to the database through it must be done with programs such as web application scanners and firewalls [61].

2.5.4 Application Layer

In this layer, it is essential to have control over the users accessing the system. A good authentication system with strong passwords by the users [62] and which does not allow SQL injection is mandatory, with solutions such as [63].

Moreover, different levels of privileges for that users are necessary after authentication [64]. The administrator should be capable of doing more things than regular users and must be defined in a good policy. This is of utmost importance to avoid human errors or possible breaches in the system through social engineering and phishing, which can be prevented as well with biometric identification [65]. To be more secure in this aspect, a firewall that only allows access to the system or to some privileges to specific addresses can also be used [66].

Lastly, software such as antivirus, antispyware or antiadware is essential to protect the system [67].

2.5.5 Business Layer

As a business, it is important to have a company security policy well defined, that must take into account all the possible risks and adequately assess them, with measures to take in case of attacks or breaches and a recovery plan [68].

Apart from that, active security measures must be considered, especially in a business in the healthcare department, as stated in [69].

Employees must be involved in the security of the business [70], having multifactor authentication [71] in their devices when having business information and knowing the threats that may occur in their email or their mobile phone through social engineering.

In the figure 2.1, a relationship among the attacks of each layer and its countermeasure can be found.

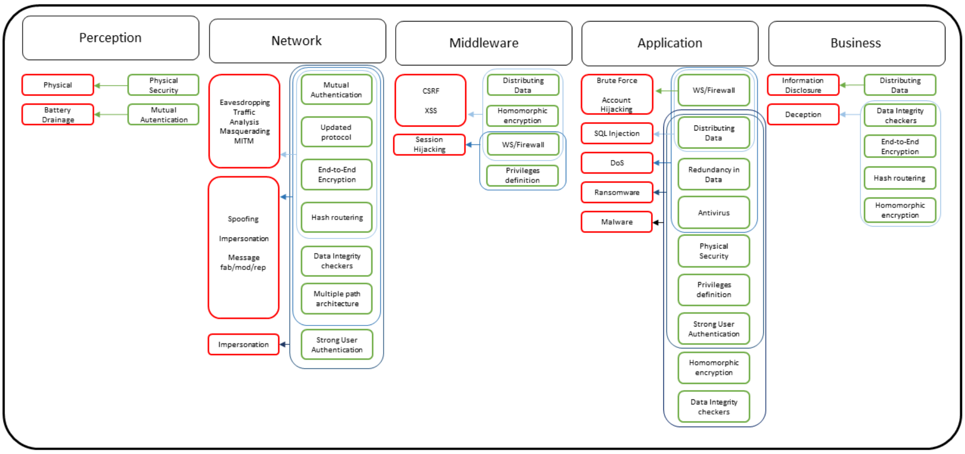

Figure 2.1: Relationship among attacks (red) and their countermeasures (green)

2.6 IEC 80001: Application of risk management for IT-networks incorporating medical devices

This standard is used to normalize the process of risk management in healthcare organizations with proper guidance. Even though there are other standards about the same topic, this is extensive with many parts that contains information from others such as [72]. It is divided into:

- Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software
- Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples
- Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- Part 2-3: Guidance for wireless networks

- Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations
- Part 2-5: Application guidance – Guidance on distributed alarm systems
- Part 2-6: Application guidance - Guidance for responsibility agreements
- Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self assess their conformance with IEC 80001-1
- Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
- Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

Even though all of them will be useful for the development of the project, the most important one and which is going to be explained in this section is Part 1 because it is focused on the risk management part of the process.

2.6.1 Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

This part specifies general requirements for organizations in the application of risk management before, during and after connecting a health IT system to their infrastructure. The purpose of a risk management plan is to document and schedule the risk management activities through the life cycle of the system.

All the information about the risk management plan should be contained in the risk management file and updated if any deviations occur apart from the record of all the activities undertaken.

The risk management plan should be flexible and commensurate with the scale and scope of the system. According to the standard, it consists of 3 steps that feedback: it starts with risk analysis, continues with risk evaluation and follows with risk control to start again the risk analysis.

Risk Analysis

It involves establishing the scope of the health IT system in terms of technological architecture, functionality and intended use. Later, it continues to identify hazards that may occur and estimate the risk after that hazard.

The purpose of hazard identification is to uncover and describe events or conditions that have the potential to result in harm. According to this standard, it should be undertaken using the Structured What If Technique (SWIFT) which is a systems-based risk identification technique that employs structured brainstorming, with the use of predeveloped guide words/headings (e.g., timing, amount, etc.) in combination with prompts elicited from participants to examine risks and hazards at a systems or subsystems level [73]. This approach, in which it is necessary the appearance of the human factor, knowledge and criteria, is the one that difficult the automation of the process. Hazards associated with the deployment of the system and identified by the manufacturer should be considered. In case no hazards are identified, good reasoning should be provided.

After identifying the hazards, it is needed to estimate the severity of the consequences, the exploitability, and the resulting risk.

Risk evaluation

After evaluating the risk, it is necessary to determine if it is acceptable according to the risk management plan or if further actions are necessary. The evaluation is usually performed with a matrix that combines severity and exploitability.

Risk control

Risk control is used to either reduce the exploitability or the severity of hazard's consequences. After identifying the measures, assessing them to determine if new hazards are introduced and implementing them, it is needed to evaluate the residual risk. Risk control can be performed in different ways: design changes, administrative and implementation procedures, and user and stakeholder training and briefing.

In some cases, no further measures can be applied to reduce residual risk to an acceptable level, always after a context of the judgment. It is also necessary to consider the aggregated residual risk of all hazards in relation to the clinical benefits.

With this, the **RQ1** "What is a risk assessment process that is suitable for healthcare networks?" is solved, having a standard that establishes the rules and basics that should be complied with.

Chapter 3
Related Work

3.1 Principles and best practices

As IT networks have their own characteristics, as explained in 2.3, several documents with guidelines of best practices and principles of healthcare cybersecurity have been written, for instance [74], [75], [76] or [77]. In this project, the ones provided by the International Medical Device Regulators Forum (IMDRF) [75] are being used as a reference because of being the specialized organization, as it is a group of medical device regulators from around the world that have voluntarily come together to harmonize the regulatory requirements for medical products that vary from country to country [78]. The subsections 3.1.1, 3.1.2 and 3.1.3 are a summary of those guidelines.

3.1.1 General principles

The general principles considered in this document are relevant for all stakeholders. The first one explained is the necessity of global harmonization of healthcare cybersecurity, encouraging all stakeholders to share their approaches to cybersecurity across the entire life cycle of the medical device, including product design, risk management activities, device labeling, regulatory submission requirements, information sharing and post-market activities.

Secondly, the risk associated with cybersecurity threats should be considered throughout the total product life cycle (TPLC) while ensuring device safety and essential performance maintenance. Moreover, all stakeholders should understand their responsibility, including the manufacturer, provider, users, regulator and vulnerability finder, monitoring, assessing, mitigating, communicating and responding to cybersecurity risks and threats.

Lastly, information sharing is foundational for this approach. All involved stakeholders are encouraged to participate in Information Sharing analysis Organizations

(ISAOs) and collaborate. Coordinated vulnerability disclosure is also encouraged as best practice.

Then, apart from the general principles seen, there are others than can be divided into Pre-Market and Post-Market considerations.

3.1.2 Pre-Market considerations

Security Requirements and Architecture Design

At the design stage, cybersecurity threats must be considered by any means, for instance, by threat modeling by inputs that can come from various phases across the life cycle. Several standards, NIST, OWASP and US Healthcare and Public Health Sector Coordinating Council establish the design principles, being the following some of the most relevant but not all of them:

- Secure Communications: How the device would interface with other devices, if wired or wireless, and what method (Wi-Fi, Ethernet, Bluetooth, USB or else). It should also take into account communication with environments with less secure communication as a home network. Moreover, manufacturers should determine how data transfer should work in order to prevent unauthorized access, modification or replay.
- Data Protection: The manufacturer should consider if the data that is stored and/or transferred requires protection and if confidentiality risk control measures are needed.
- Device Integrity: Risks, including unauthorized modifications to device software, should be considered, as well as anti-malware, apart from the evaluation of the system-level architecture to determine if it is needed to ensure data non-repudiation.
- User Authentication: Access controls to use the device and control privileges.
- Software Maintenance: Establish and communicate the process for implementation and deployment of regular updates taking into account the OS software, third-party software or open-source software will update, the new cybersecurity vulnerabilities and what connections will be required to conduct updates.
- Physical Access: Controls to prevent an unauthorized person from accessing the device as locks or requiring authentication to access with a physical cable.
- Reliability and Availability: The device should detect, resist, respond and recover from attacks to maintain its performance.

Risk Management Principles for the TPLC

Any cybersecurity risk that impacts device safety and performance should be considered by identifying the vulnerability, estimating the associated risks, controlling those risks to an acceptable level, assessing and monitoring the risks controls and communicating those risks to key stakeholders. The process is explained in 3.1.

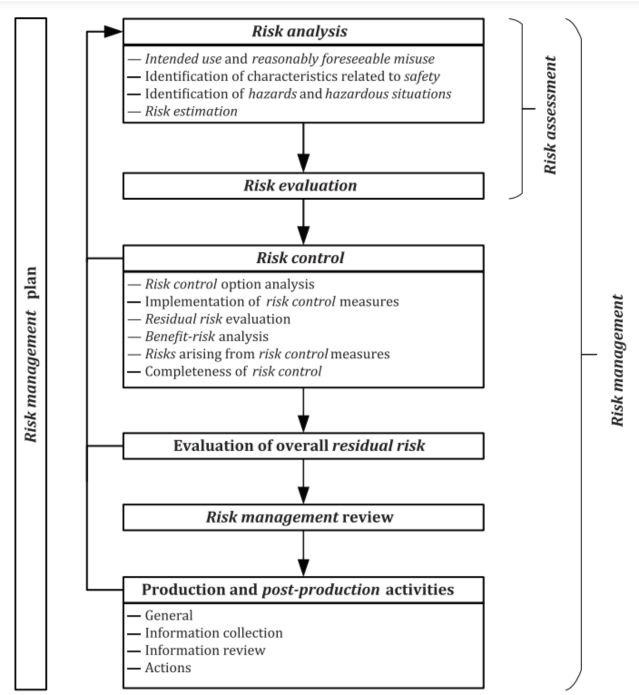
Risk management plan
Risk analysis
— Intended use and reasonably foreseeable misuse
— Identification of characteristics related to safety
— Identification of hazards and hazardous situations
— Risk estimation
Risk evaluation
Risk control
— Risk control option analysis
— Implementation of risk control measures
— Residual risk evaluation
— Benefit-risk analysis
— Risks arising from risk control measures
— Completeness of risk control
Evaluation of overall residual risk
Risk management review
Production and post-production activities
— General
— Information collection
— Information review
— Actions
Risk assessment
Risk management

Figure 3.1: Representation of the security risk management process from [72]

In this project, the research will be focused on the first part, security risk assessment, in which manufacturers consider risks, threats and controls throughout the product life cycle, as it will be seen in 2.6.

Security Testing

The manufacturer should assure that the code is free of known vulnerabilities and that security controls have been implemented. Some considerations are performing target searches on software for known vulnerabilities, conducting technical security analysis and completing a vulnerability assessment.

TPLC Cybersecurity Management Plan

As manufacturers should proactively monitor vulnerabilities and exploits across the product life cycle, a formal plan should be developed in the pre-market stage.

Labeling and Customer Security Documentation

Giving the customer all the information through labeling of the instructions and specifications, description of backup and restore features, list of ports and interfaces expected and sufficiently detailed system diagrams. With the customer security documentation, the client should have specific guidance regarding the supporting infrastructure requirements, secure configurations, secure network deployment, how notifications work and more.

Documentation for Regulatory Submission

Manufacturers should document and summarize their activities related to cybersecurity through design, risk management, security testing, TPLC cybersecurity management planning, and labeling and customer security documentations.

3.1.3 Post-Market Considerations

As cyber threats continue developing over time, a pre-market analysis is not enough and several actions must be done. These actions will be briefly explained here, but much more information for all the stakeholders can be found again in [75].

Operating Devices in the Intended Use of Environment

Healthcare providers should adopt cybersecurity best practices with proper risk management as detailed in standards such as [68] throughout the whole life cycle, since the development of the infrastructure, integration in the network and in the changing of the device, in addition to adhere to general cybersecurity best practices, as well as provide the users with a good formation in the matter. Moreover, manufacturers should involve, ensuring optimal deployment and configuration of the devices.

Information Sharing

Information to improve the security of medical devices should be shared with the main stakeholders, which may include regulators, manufacturers, healthcare providers, users, governments and information-sharing entities. This information will be only shared to improve security and patient safety, not to gain commercial advantage.

Coordinated Vulnerability Disclosure

Coordinated Vulnerability Disclosure (CVD) is a mechanism that enhances transparency in cybersecurity issues. It establishes processes for obtaining information, assessing vulnerabilities, developing mitigations and compensating controls and disclosing this information to various stakeholders. It is a responsible course of action to raise awareness to security issues. On the other hand, this transparency has sometimes turned out to be bad publicity for manufacturers. However, it is a good practice that everyone should implement to collaborate between manufacturers, regulators and vulnerability finders.

Vulnerability Remediation and Response

In this work, the three: manufacturers, healthcare providers and regulators should do their part and collaborate to develop a proper solution in which no one is affected according to the necessities of the patient, the infrastructure and the regulations.

Legacy Medical Devices

These are the devices that cannot be reasonably protected via updates and/or compensating controls against current cybersecurity threats. Many devices were designed before cybersecurity was an issue or their duration is longer than the security maintenance. Some changes or updates may not be feasible for legacy devices, though some compensating controls can be done. Thus, it is important to have the security well-considered by manufacturers before having the device on the market and healthcare providers may not use them for longer than the end of support (EOS) date.

3.2 Risk assessment methods

Regarding risk assessment methods, there is a great diversity, which may be divided into two subgroups: quantitative and qualitative.

Examples of qualitative methods are the Delphi Method [79], SWIFT Analysis [73], Bowtie method [80] or [81]. These methods use the opinion of experts to establish the threats to face, the vulnerabilities and the impact based on their knowledge in a subjective way. Some organizations such as NIST [82], FAIR [83] or MITRE [84] created their own risk assessment method incorporating different techniques.

On the other hand, quantitative methods such as Fault Tree Analysis [85], Bayesian Networks [86] or Markov Chains [87] provide numerical results after calculating their algorithms.

As seen, there are many different methods and different methods may result in different results and that is the reason why CVSS (Common Vulnerability Scoring System) appeared, which produces a numerical score based on the exploitability of the vulnerability to occur and the impact that it may cause [88]. It is widely used and almost considered a standard nowadays. The exploitability is calculated according to the privileges required, the attack vector, the user interaction and the attack complexity as in table 3.1, while the impact is calculated depending on the effect on confidentiality, integrity and availability as in table 3.2.

The equations to obtain the final numeric result are:

$$Exploitability = 8.22 \times AV \times AC \times PR \times UI \tag{3.1}$$

$$Impact = 6.42 \times [1 - [(1 - C) \times (1 - I) \times (1 - A)]] \tag{3.2}$$

$$Risk = Exploitability + Impact(Max.10) \tag{3.3}$$

However, as it has been said many times in this document, healthcare is a unique domain and other proposals have emerged inspired in CVSS, like [89], which includes factors as the effects on the patient and on the diagnosis. In other domains, other ways of introducing it were used, as in [90], where only the likelihood was calculated through this method while the other elements in the risk equation were calculated in their own way considering criticality in different sections as well as the detectability of the issue.

Other techniques do not consider CVSS as a basis and developed a complete scoring system by themselves as in [10], who created a method that incorporates factors as the number of attacks that can affect a device, the impact of that attack (based on a metric he decided), the ease of executing an attack, the users' lack of knowledge and the readiness to detect, report and respond to the attack.

3.3 Automation

In terms of cyber risk assessment automation, there have been some proposals as well because of the criticality of the topic in the healthcare domain.

In the case of [91], they created a software to search in real-time for vulnerabilities, evaluate them depending on the criticality of the information involved, and propose countermeasures, including the cost.

On the other hand, [92] created a model of a relational database to include all the assets, the possible vulnerabilities with their score in the CVSS and their countermeasures.

Exploitability			
Exploitability element	Metric	Value	Description
Attack Vector (AV)	Network	0.85	Remotes attack from up to the internet
	Adjacent	0.62	Attack launched from same network
	Local	0.55	Attacking the device locally or through user interaction
	Physical	0.2	Physically manipulate component
Attack Complexity (AC)	Low	0.77	No specialized access conditions
	High	0.44	Attacker invests effort in preparation or execution
Privileges Required (PR)	None	0.85	No need to access settings or files
	Low	0.62	Need of basic user capabilities
	High	0.27	Significant control over the component
User Interaction (UI)	None	0.85	No interaction from users
	Required	0.62	Some action needed

Table 3.1: CVSS exploitability metrics

Impact			
Impact element	Metric	Value	Description
Confidentiality	High	0.56	Total data theft or serious impact of the data (i.e. passwords)
	Low	0.22	No control over what information is obtained
	None	0	No loss of confidentiality
Integrity	High	0.56	Total loss of integrity or serious impact on the device
	Low	0.22	No control over the consequence of a modification
	None	0	No loss of integrity
Availability	High	0.56	Total loss of availability or serious consequence to the component
	Low	0.22	Performance is reduced or there are interruptions
	None	0	No impact on availability

Table 3.2: CVSS impact metrics

Another solution was proposed by [93], in which solutions were proposed before developing the infrastructure according to the stakeholder.

All the previous solutions lack of at least one of the following: transparency on the selection of attacks and countermeasures, transparency in the selection of the assessment methodology and algorithm and, lastly, automation of the whole process.

Chapter 4
Methodology

In this section, the methodology regarding the information used and the decisions made during each step of the project is explained. Firstly, how all the information has been gathered will be discussed. Secondly, what techniques are used for the development of the project and, lastly, the evaluation of the results.

4.1 Literature review

For the development of this thesis, the biggest amount of time was held for literature review. In its vast majority, it consisted in reading information about general networks, healthcare networks and their characteristics, common vulnerabilities that they are exposed to, risk assessment methods in healthcare, standards to comply and mitigation techniques.

The main tools used in this part were: Google Scholar as a search engine because of the large number of sources it includes and the number of citations of a paper, as well as its ease to cite. Then, IEEE, Elsevier, Springer, ACM, ResearchGate and similar were used as libraries when a high-quality article was needed, due to their filter to publish papers. Lastly, the National Library of Medicine was used as a reliable source on healthcare issues. Regarding websites, FDA (U.S. Food & Drug Administration) was consulted again on medical and healthcare issues, whereas NIST (National Institute of Standards and Technology) and OWASP (Open Web Application Security Project) were used for cybersecurity and technological concerns.

To select what paper, article or book was reliable in a certain topic, the date of publishing, the publisher and the number of citations were taken into account. The date because of the short-lasting technologies in the world of computers, the publisher to only rely on trustful sources and the number of citations to check the relevance of the information,

4.1.1 Networks

To research in the network domain, both general and specialized in healthcare, it was necessary to check several sources because of the width of the topic. Many sources coincided in the description of the layers and the special characteristics in medical networks, so the research mainly consisted of a survey through them.

4.1.2 Vulnerabilities and attacks

This section took a great deal of working time because getting to know the most important vulnerabilities and attacks that aim at this kind of network is one of the bases of the project and how it is possible to assess their risks.

The list of vulnerabilities was obtained through an article [11] of more than 200 citations published by PubMed Central in the National Library of Medicine, which is considered a more than reliable source. This helped to obtain a general view of the problem facing. Then, a list of possible attacks is provided. Many sources are consulted, many of them surveys on attacks and, most of them, coincided among them. Some examples of checked articles are [20], [94], [95] or [96], which are highly cited and trusted, and have several similarities among them.

4.1.3 Risk assessment methods

The core of the project relies on this research, as selecting the best method for the automation of the process is required. Main qualitative and quantitative methods were researched. Special interest was put on quantitative methods, as the numerical outcome is believed to be easier to implement in an automation process and most automated solutions found used this type of process. Due to this, special effort was included in the review and understanding of the Common Vulnerability Scoring System as it is widely used for this purpose.

4.1.4 Standards

When researching standards in the cybersecurity domain, the family of ISO 27000 outstood over the rest, especially ISO 27001 [97], which establishes the requirements for the assessment and treatment of information security risks. This standard is mentioned and cited in many of the papers regarding cybersecurity and risk assessment techniques.

Moreover, another standard was found, the IEC 80001 [68], which assesses the same topic with the only difference of being specialized in the healthcare and medical devices domain. This standard was highly studied because it fitted perfectly in the development of the thesis.

A best practices manual was also found in [75], which helped to understand the starting point of the risk assessment from the pre-market considerations through the whole life cycle of the device.

4.1.5 Countermeasures

Similar proceeding as in 4.1.2 has been carried out and of same importance. A list of possible solutions to mitigate attacks was found in [43]. From this point, a further investigation of each proposal, including new sources, as well as the incorporation of different solutions, was done.

4.2 Solution Proposal

After researching all the elements explained in 4.1, decisions had to be made in order to answer the research questions 1.2 asked at the beginning of the project.

The starting point of the risk assessment is to verify that all the pre-market considerations established in [75] are accomplished. Medical devices must be bought from trusted manufacturers, which ensures the best practices.

To create the risk assessment method suitable for healthcare, the [68] was used as a guideline as it is a standard specialized in risk management for medical devices. It established a three-step risk assessment, which started with risk analysis, continued with risk evaluation and the ended with risk control. It can also be explained as: identifying and estimating risks, determining if further actions are needed to prevent that risk to happen and executing those countermeasures.

4.2.1 Risk Analysis

For this step, the standard considered that the best way to work on it is by a Structured What If Technique. Even though it is a great technique widely used in risk assessment [73], it is required to include human interaction for its use. As the last goal of the project is to find a trusting method that can be automated, SWIFT had to be disregarded.

As reviewed in the literature, qualitative models are based on subjective opinions (as SWIFT) and due to this, quantitative models were the main focus of research. There are different quantitative proposals as explained in 3.2. However, even though it has some limitations regarding the diversity of values, the research was centered in CVSS as it is widely extended and used as a base of many other own made methods.

After investigating and considering changes to implement to the method (for example, including variables such as monetary cost, diagnosis error or expected damage to the patient), it was decided that a nice implementation of CVSS as it is accompanied by a proper classification of the devices depending on their criticality and data management would be sufficient.

Asset Identification

The classification method of the medical devices in the physical or perception layer is based on the methodology of [7] explained in 2.2, which is a standard for both Europe and US. With this methodology, confidentiality, integrity and availability can be calculated depending on the potential harm that a patient may suffer and the secrecy level of the information managed, as represented in table 4.1.

Characteristic	Level	Description
Potential harm	High	Working wrongly or not working may cause severe harm or even death
	Low	Working wrongly or not working may cause no severe harm
	None	Working wrongly or not working may cause no harm
Secrecy level	High	Gathers and/or sends critical information about patient's health
	Low	Gathers and/or sends information about the patient
	None	Doesn't gather and/or send information about the patient

Table 4.1: Medical devices characteristics

As medical devices are the only devices that directly interact with the patient, the rest of the devices in the network will only be classified according to the information that they transmit or process and if they store any of that information, as in 4.2. Then, a differentiation between only network devices, as routers or switches, and computers, servers or processing units in general, is made.

With this classification, all devices are included, so the impact of failure can be calculated with the CVSS formula shown in equation 3.2. It is explained in tables 4.4, 4.5 and 4.6.

Threats identification

The other part of the risk analysis is to identify what threats can aim at your assets. For this, the research explained in 4.1 took place and returned the most common

Characteristic	Level	Description
Stored information importance	High	Stores critical information about patient's health
	Low	Stores information about the patient
	None	Doesn't store information about the patient
Transmitted information importance	High	Transmits critical information about patient's health
	Low	Transmits information about the patient
	None	Doesn't transmit information about the patient

Table 4.2: Processing devices characteristics

Characteristic	Level	Description
Transmitted information importance	High	Transmits critical information about patient's health
	Low	Transmits information about the patient
	None	Doesn't transmit information about the patient

Table 4.3: Networked devices characteristics

attacks that a healthcare network can suffer. The selection of this attack was because of its repetition in different specialized papers. It is known that these attacks do not cover the totality of possibilities, but they were thought as a good starting point to create a database of threats.

The likelihood of these attacks happening is calculated according to the exploitability formula of CVSS shown in equation 3.1 as detailed in table 4.7, and always considering the worst-case scenario, which means that if an attack has two possible ways to be introduced, the higher result of exploitability will be the one considered.

Now, it is the turn to relate threats with assets in order to calculate the final impact. However, another intermediate step needs to be done for the good performance of the method, as not all attacks aim to the three confidentiality, integrity and availability (battery drainage, for example, only can attack availability) and results would not be precise. What elements of CIA as well as the component they may attack is detailed in 4.8. Also, a unique Id has been given to each attack.

From this point, taking into account only the objectives that can be aimed, a relationship between the assets and the attacks can be made.

4.2.2 Risk Evaluation

In this part of the risk assessment, it is needed to establish a threshold in the risk from which and above actions have to be done in order to prevent the attacks from happening. This is called risk acceptability criteria and it is part of the risk management plan of each company [68] and must be determined according to their estimations in different terms such as cost-benefit, the value of statistical life, the value of averting a fatality, societal willingness to pay or net cost of averting a fatality [98].

According to the standard, it should be done with a risk matrix, where exploitability and impact are the axes. Once again, another method has been chosen because of the necessity of establishing a numerical limit in order to automate the process.

CVSS separates the risks according to their score in: None (0), Low (0.1-3.9), Medium (4.0-6.9), High (7.0-8.9) and Critical (9.0-10.0). For the purpose of this project and taking into account that it is healthcare what is being discussed, an impact score of 5.0 or more over 10 will be considered mandatory to remediate, while a score over 4.0 will be encouraged to try to solve in a reasonable way.

4.2.3 Risk Control

After knowing the vulnerabilities that have to be solved, finding a solution is needed. For this, a database of countermeasures has been developed. The method followed to decide what countermeasures were best for known attacks was a research through different specialized papers and selecting the most repeated ones. It is the same method as used in 4.2.1. This research also helped to confirm the choice of attacks as the countermeasures were perfectly suitable for them.

Countermeasures used as the first approach to a database, as well as the attacks they can mitigate, are all identified in table 4.9.

Having all the information related in different tables that can be translated into spreadsheets or databases and a computer program can read them. If the devices are correctly introduced according to their categorization, the program can estimate their vulnerabilities and the impact and advice countermeasures to solve them. The algorithms used by the program would be similar to algorithm 4.1 and 4.2:

These algorithms are presented separately in impact and risk because it is easier to understand. However, they could also be merged in a bigger one.

Algorithm 4.1 Impact calculation algorithm

```
for each Asset in AssetList do
    $AttackList \leftarrow AttacksToTheAsset$
    for each Attack in AttackList do
        if $AssetConfidentiality > None$ AND $AttackBreaksConfidentiality$ then
            $C \leftarrow AssetConfidentiality$
        else
            $C \leftarrow None$
        end if
        if $AssetIntegrity > None$ AND $AttackBreaksIntegrity$ then
            $I \leftarrow AssetIntegrity$
        else
            $I \leftarrow None$
        end if
        if $AssetAvailability > None$ AND $AttackBreaksAvailability$ then
            $A \leftarrow AssetAvailability$
        else
            $A \leftarrow None$
        end if
        $AttackImpact \leftarrow 6.42 \times [1 - [(1 - C) \times (1 - I) \times (1 - A)]]$
    end for
end for
return AttackList,AttackImpact
```

Algorithm 4.2 Risk assessment algorithm

```
for each Asset in AssetList do
    $AttackList \leftarrow AttacksToTheAsset$
    for each Attack in AttackList do
        $Impact \leftarrow CalculateImpact$
        $Risk \leftarrow Min(Exploitability + Impact, 10)$
        if $Risk \geq Threshold$ then
            $CountermeasureList \leftarrow CountermeasuresToAttack$
        end if
    end for
end for
return AttackLists,CountermeasureList
```

With this, the **RQ2** "How can that process be adapted to support automation of certain tasks?" is answered, as the process has been adapted to an algorithm that is easily programmable.

Medical Device					
Potential harm	Secrecy level	C	I	A	Impact
High	High	High	High	High	5.87
High	Low	Low	High	High	5.45
High	None	None	High	High	5.18
Low	High	High	High	Low	5.45
Low	Low	Low	Low	Low	3.37
Low	None	None	Low	Low	2.51
None	High	High	High	None	5.18
None	Low	Low	Low	None	2.51
None	None	None	None	None	0

Table 4.4: Impact calculation for medical devices

Computers, servers and similar					
Stored information importance	Transmitted information importance	C	I	A	Impact
High	High	High	High	High	5.87
High	Low	High	High	High	5.87
High	None	High	High	None	5.18
Low	High	High	High	High	5.87
Low	Low	Low	Low	Low	3.37
Low	None	Low	Low	None	2.51
None	High	High	High	High	5.87
None	Low	Low	Low	Low	3.37
None	None	None	None	None	0

Table 4.5: Impact calculation for computers, servers and similar

Routers, switches and similar				
Transmitted information importance	C	I	A	Impact
High	High	High	High	5.87
Low	Low	Low	Low	2.51
None	None	None	None	0

Table 4.6: Impact calculation for routers, switches and similar

Attack	**AV**	**AC**	**PR**	**UI**	**Exploitability**
Physical	Physical	Low	None	None	0.91
Battery Drainage	Adjacent	Low	None	None	2.84
Eavesdropping	Adjacent	High	None	None	1.62
Spoofing	Adjacent	High	None	None	1.62
Traffic analysis	Adjacent	High	None	None	1.62
Masquerading	Adjacent	High	Low	None	1.62
Malware	Network	Low	None	Required	2.84
Man-In-The-Middle	Adjacent	High	None	None	1.44
Denial-of-Service	Network	High	None	None	2.22
Impersonation	Local	High	None	None	1.44
Message fabrication/modification/replay	Adjacent	High	None	None	1.62
Cross Site Request Forgery	Network	High	None	Required	1.62
Session Hijacking	Network	High	None	None	2.22
Cross Site Scripting	Network	High	None	None	2.22
SQL Injection	Network	High	None	None	2.22
Account hijacking	Network	High	Low	None	1.62
Ransomware	Network	Low	None	Required	2.84
Brute force	Network	Low	None	None	3.89
Information disclosure	Adjacent	Low	None	None	2.84
Deception	Adjacent	High	Low	None	1.18

Table 4.7: Threats and exploitability

Id	**Attack**	**Breaks**			**Objective**		
		C	**I**	**A**	**MD**	**CS**	**NW**
1	Physical	X	X	X	X	X	X
2	Battery Drainage			X	X		
3	Eavesdropping	X			X	X	X
4	Spoofing	X	X		X	X	X
5	Traffic analysis	X			X	X	X
6	Masquerading	X	X		X	X	X
7	Malware	X	X	X		X	
8	Man-In-The-Middle	X	X		X	X	X
9	Denial-of-Service			X	X	X	X
10	Impersonation	X	X		X	X	X
11	Message fabrication/modification/replay		X		X	X	X
12	Cross Site Request Forgery	X	X	X		X	
13	Session Hijacking	X	X	X		X	
14	Cross Site Scripting	X	X	X		X	
15	SQL Injection	X	X	X		X	
16	Account hijacking	X	X			X	
17	Ransomware	X	X	X		X	
18	Brute force	X	X	X		X	X
19	Information disclosure	X				X	
20	Deception		X			X	

Table 4.8: Threats, CIA breaking and objective

Countermeasure	**Attack**	**Protects**		
		C	**I**	**A**
Mutual Authentication	2,3,4,5,6,8,10,11	X	X	
Data Integrity Checkers	4,6,7,8,11,20		X	
Updated protocol	3,4,5,6,8,10,11	X	X	
Physical security	1,7,17	X	X	X
End-to-End encryption	3,4,5,6,8,10,11,20	X	X	
Multiple path architecture	4,6,8,10,11,20	X	X	
Hash in router	3,4,5,6,8,10,11,20	X	X	
Distributing data	7,9,12,14,15,17,19		X	X
Redundancy in data	7,9,17			X
Fully homorphic encryption	7,12,14,20	X	X	
Web application scanners and firewalls	9,12,13,14,15,16,18	X	X	X
Strong user authentication system	7,10,17	X	X	X
Privileges definition	7,13,17	X	X	X
Antivirus	7,9,17	X	X	X
Structured recovery plan	All			X

Table 4.9: Countermeasures and their match with attacks

Chapter 5
Assessment Application

In this chapter, the application, automation and evaluation of the process described in section 4.2 are presented. Firstly, by describing the tool that runs the methodology and lastly, by showing the results in four different environments of study.

5.1 Script explanation

The script is coded in Python and executed i on a laptop. It is important to notice that the main goal of this is to test the whole risk assessment, not the programming itself, so no programming issues such as complexity, running speed or similar have been considered. However, the running time of the program with four devices is 0.07 seconds.

The data needed to perform the risk assessment is all detailed in CSV data sheets. There, you can find the attacks, countermeasures, devices classification and the actual devices that are in the network with their characteristics.

The first part of the script consists of reading these data sheets and including their information in the program to work with it. After reading the data sheets, the different methods for the calculation of the impact and risk have been created, as well as the countermeasure finder. All those methods are based on the algorithms described in 4.1 and 4.2.

After running, the program displays in the console the values of the risk analysis, present the most important risks after risk evaluation and suggest the countermeasures as in risk control.

You can access the whole program through this link.

5.2 Test

In this section, a simple environment with different devices will be presented as an example to demonstrate the functionality of the program. This environment consists of the topology presented in figure 5.1 in which the medical device may have different values.

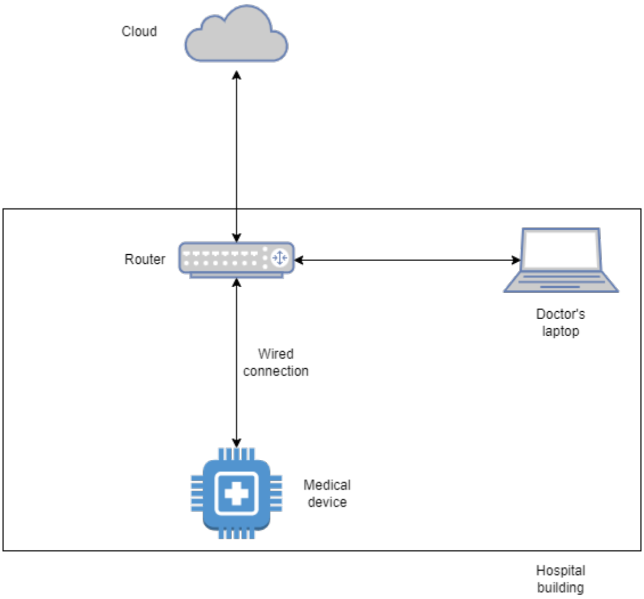

Figure 5.1: Environment to test

It is considered that there are not more devices in the network than the ones presented and the medical device will vary, being a smart insulin pump, a thermometer or both at the same time. The doctor's laptop does not store information about the device, but can access it by connecting to the cloud, which is hosted by a third party and stores the information. It also acts as a web server, which can be used to see the data and control the actuator of the device.

5.2.1 Medical device: Insulin pump

An insulin pump is a device that gathers information about the health status of the patient and supplies some medicine according to a set of parameters. Due to this, it is critical because of the information that manages and because it may harm people. The inputs that will be introduced in the script are:

- Insulin pump: A medical device with high potential harm and high secrecy level.

- Cloud: A processing device with high stored information importance and high transmitted information importance.

- Doctor's laptop: A processing device with low stored information importance and high transmitted information importance.

- Router: A network device with high transmitted information importance.

5.2.2 Results

With these inputs, the script can be run to perform the risk analysis and the results obtained are:

Risk analysis

All the attacks that the insulin pump is in danger are in table 5.1:

Insulin pump		
Attack	**Impact**	**Risk**
Physical	5.87	6.78
Battery Drainage	3.6	6.44
Eavesdropping	3.6	5.22
Spoofing	5.18	6.8
Traffic analysis	3.6	5.22
Masquerading	5.18	6.36
Man-In-The-Middle	5.18	6.8
Denial-of-Service	3.6	5.82
Impersonation	3.6	5.04

Table 5.1: Insulin pump scenario: Insulin pump risk analysis

All the attacks that the cloud server is in danger are in table 5.2:

All the attacks that the doctor's computer is in danger are in table 5.3:

All the attacks that the router is in danger are in table 5.4:

Cloud server		
Attack	**Impact**	**Risk**
Physical	5.87	6.78
Eavesdropping	3.6	5.22
Spoofing	5.18	6.8
Traffic analysis	3.6	5.22
Masquerading	5.18	6.36
Malware	5.87	8.71
Man-In-The-Middle	5.18	6.8
Denial-of-Service	3.6	5.82
Impersonation	3.6	5.04
Message fabrication/modification/replay	5.87	7.49
Cross Site Request Forgery	5.87	7.49
SQL Injection	5.87	8.09
Account Hijacking	5.18	6.8
Ransomware	5.87	8.71
Brute Force	5.87	9.76
Information Disclosure	3.6	5.67
Deception	3.6	4.78

Table 5.2: Insulin pump scenario: Cloud risk analysis

Risk evaluation

For the risk evaluation, a threshold of 5 in the risk values has been selected, so every attack with a higher risk will be considered relevant. The program analyses it and the results are:

For the insulin pump: Physical attacks, Battery drainage attacks, Eavesdropping attacks, Spoofing attacks, Traffic analysis attacks, Masquerading attacks, Man-in-the-middle attacks, Denial-of-service attacks, Impersonation attacks.

For the cloud server: Physical attacks, Eavesdropping attacks, Spoofing attacks, Traffic analysis attacks, Masquerading attacks, Malware attacks, Man-in-the-middle attacks, Denial-of-service attacks, Impersonation attacks, Message fabrication/mod-

Doctor's computer		
Attack	**Impact**	**Risk**
Physical	5.87	6.78
Eavesdropping	3.6	5.22
Spoofing	5.18	6.8
Traffic analysis	3.6	5.22
Masquerading	5.18	6.36
Malware	5.87	8.71
Man-In-The-Middle	5.18	6.8
Denial-of-Service	3.6	5.82
Impersonation	3.6	5.04
Message fabrication/modification/replay	5.87	7.49
Cross Site Request Forgery	5.87	7.49
Session Hijacking	5.87	8.09
Cross Site Scripting	5.87	8.09
SQL Injection	5.87	8.09
Account Hijacking	5.18	6.8
Ransomware	5.87	8.71
Brute Force	5.87	9.76
Information Disclosure	3.6	5.67
Deception	3.6	4.78

Table 5.3: Insulin pump scenario: Doctor's Computer risk analysis

ification/replay attacks, Cross Site Request Forgery, Session Hijacking, Cross Site Scripting, SQL Injection, Account hijacking, Ransomware, Brute force attack, Information disclosure.

For the doctor's computer: Physical attacks, Eavesdropping attacks, Spoofing attacks, Traffic analysis attacks, Masquerading attacks, Malware attacks, Man-in-the-middle attacks, Denial-of-service attacks, Impersonation attacks, Message fabrication/modification/replay attacks, Cross Site Request Forgery, Session Hijacking, Cross Site Scripting, SQL Injection, Account hijacking, Ransomware, Brute force attack, Information disclosure.

Router		
Attack	**Impact**	**Risk**
Physical	5.87	6.78
Eavesdropping	3.6	5.22
Spoofing	5.18	6.8
Traffic analysis	3.6	5.22
Masquerading	5.18	6.36
Man-In-The-Middle	5.18	6.8
Denial-of-Service	3.6	5.82
Impersonation	3.6	5.04
Brute Force	5.87	9.76

Table 5.4: Insulin pump scenario: Router risk analysis

For the router: Physical attacks, Eavesdropping attacks, Spoofing attacks, Traffic analysis attacks, Masquerading attacks, Man-in-the-middle attacks, Denial-of-service attacks, Impersonation attacks, Brute force attack.

Risk control

For the risk control, depending on the attacks that were relevant to the different assets, the countermeasures were selected and the results are:

For the insulin pump: Physical security, Structured recovery plan, Mutual authentication, Updated protocol (IPSec), End-to-End encryption, Data integrity checkers (parity bit or checksum).

For the cloud server: Physical security, Structured recovery plan, Mutual authentication, Updated protocol (IPSec), End-to-End encryption, Data integrity checkers (parity bit or checksum), Distributing data, Redundancy in data, Fully homomorphic encryption, Strong user authentication system (strong passwords, 2-factor authentication), Privileges definition, Antivirus, antispyware, antiadware, Webapp scanners and firewalls.

For the doctor's computer: Physical security, Structured recovery plan, Mutual authentication, Updated protocol (IPSec), End-to-End encryption, Data integrity checkers (parity bit or checksum), Distributing data, Redundancy in data, Fully homomorphic encryption, Strong user authentication system (strong passwords, 2-factor authentication), Privileges definition, Antivirus, antispyware, antiadware, Webapp scanners and firewalls.

For the router: Physical security, Structured recovery plan, Mutual authentication, Updated protocol (IPSec), End-to-End encryption, Hash routering, Data integrity checkers (parity bit or checksum), Multiple path architecture, Webapp scanners and firewalls, Antivirus, antispyware, antiadware, Strong user authentication system (strong passwords, 2-factor authentication).

Thoughts

We find that there are a big number of possible attacks in all the devices. The most relevant ones, possibly against intuition, are in the computer and in the cloud server (not in the medical device itself), as they are the ones really controlling the device. The riskiest attack in the whole network is brute forcing the router, as it has the highest impact while being very likely to happen.

As all the attacks are greatly risky, all the countermeasures are suggested.Physical security is needed for each device, the whole communication process needs encryption, checking the integrity of the information, authentication, redundancy and vigilance.

5.2.3 Medical device: Thermometer

A thermometer is a device that gathers information about the health status of the patient. It is considered non-critical because the information that manages does not suppose an important risk for the patient if it is leaked and it is easy to know if it is malfunctioning just by touching the patient. The inputs that will be introduced in the script are:

- Thermometer: A medical device with no potential harm and low secrecy level.
- Cloud: A processing device with low stored information importance and low transmitted information importance.
- Doctor’s laptop: A processing device with low stored information importance and low transmitted information importance.
- Router: A network device with low transmitted information importance.

5.2.4 Results

With these inputs, the script can be run to perform the risk analysis and the results obtained are:

Risk analysis

All the attacks that the thermometer is in danger are in table 5.5:

Thermometer		
Attack	**Impact**	**Risk**
Physical	2.51	3.42
Battery Drainage	0.0	0.0
Eavesdropping	1.41	3.03
Spoofing	2.51	4.13
Traffic analysis	1.41	3.03
Masquerading	2.51	3.69
Man-In-The-Middle	2.51	4.13
Denial-of-Service	0.0	0.0
Impersonation	1.41	2.85

Table 5.5: Thermometer scenario: Thermometer risk analysis

All the attacks that the cloud server is in danger are in table 5.6:

All the attacks that the doctor's computer is in danger are in table 5.7:

All the attacks that the router is in danger are in table 5.8:

Risk evaluation

For the risk evaluation, a threshold of 5 in the risk values has been selected, so every attack with a higher risk will be considered relevant. It is important to note that, as this is the least critical scenario, these would be the basic attacks that you are always going to face. The program analyses it and the results are:

For the thermometer: No critical risks.

For the cloud server: Malware attacks, Session Hijacking, Cross Site Scripting, SQL Injection, Ransomware, Brute force attack.

For the doctor's computer: Malware attacks, Session Hijacking, Cross Site Scripting, SQL Injection, Ransomware, Brute force attack.

For the router: Brute force attack.

Risk control

It is important to note that, as this is the least critical scenario, these would be the basic countermeasures that you are always going to need. Depending on the attacks

Cloud server		
Attack	**Impact**	**Risk**
Physical	3.37	4.28
Eavesdropping	1.41	3.03
Spoofing	2.51	4.13
Traffic analysis	1.41	3.03
Masquerading	2.51	3.69
Malware	3.37	6.21
Man-In-The-Middle	2.51	4.13
Denial-of-Service	1.41	3.63
Impersonation	1.41	2.85
Message fabrication/modification/replay	3.37	4.99
Cross Site Request Forgery	3.37	4.99
SQL Injection	3.37	5.59
Account Hijacking	2.51	4.13
Ransomware	3.37	6.21
Brute Force	3.37	7.26
Information Disclosure	1.41	3.48
Deception	1.41	2.59

Table 5.6: Thermometer scenario: Cloud risk analysis

that were relevant to the different assets the countermeasures were selected and the results are:

For the thermometer: No actions needed.

For the cloud server: Data integrity checkers (parity bit or checksum), Physical security, Distributing data, Redundancy in data, Fully homomorphic encryption, Strong user authentication system (strong passwords, 2-factor authentication), Privileges definition, Antivirus, antispyware, antiadware, Structured recovery plan, Webapp scanners and firewalls.

For the doctor's computer: Data integrity checkers (parity bit or checksum), Physical security, Distributing data, Redundancy in data, Fully homomorphic encryp-

Doctor's computer		
Attack	**Impact**	**Risk**
Physical	3.37	4.28
Eavesdropping	1.41	3.03
Spoofing	2.51	4.13
Traffic analysis	1.41	3.03
Masquerading	2.51	3.69
Malware	3.37	6.21
Man-In-The-Middle	2.51	4.14
Denial-of-Service	1.41	3.63
Impersonation	1.41	2.85
Message fabrication/modification/replay	3.37	4.99
Cross Site Request Forgery	3.37	4.99
Session Hijacking	3.37	5.59
Cross Site Scripting	3.37	5.59
SQL Injection	3.37	5.59
Account Hijacking	2.51	4.13
Ransomware	3.37	6.21
Brute Force	3.37	7.26
Information Disclosure	1.41	3.48
Deception	1.41	2.59

Table 5.7: Thermometer scenario: Doctor's Computer risk analysis

tion, Strong user authentication system (strong passwords, 2-factor authentication), Privileges definition, Antivirus, antispyware, antiadware, Structured recovery plan, Webapp scanners and firewalls.

For the router: Webapp scanners and firewalls, Structured recovery plan.

Thoughts

We find that the number of relevant attacks is drastically reduced in all the devices, even though the computer and the server keep being important to ensure the availability and continuity of the working process. Thermometer does not even have

Router		
Attack	**Impact**	**Risk**
Physical	3.37	4.28
Eavesdropping	1.41	3.03
Spoofing	2.51	4.13
Traffic analysis	1.41	3.03
Masquerading	2.51	3.69
Man-In-The-Middle	2.51	4.13
Denial-of-Service	1.41	3.63
Impersonation	1.41	2.85
Brute Force	3.37	7.26

Table 5.8: Thermometer scenario: Router risk analysis

any risky enough attack as its information can be gathered manually or changing the device.

As the attacks are reduced in number and quality, the actions needed are also severely reduced. They are mainly focus on the availability of the system.

5.2.5 Medical device: Insulin pump and thermometer

This is a combination of both the above scenarios, in which an insulin pump is a critical device and the thermometer is a non-critical device. The inputs that will be introduced in the script are:

- Insulin pump: A medical device with high potential harm and high secrecy level.
- Thermometer: A medical device with no potential harm and low secrecy level.
- Cloud: A processing device with high stored information importance and high transmitted information importance.
- Doctor's laptop: A processing device with low stored information importance and high transmitted information importance.
- Router: A network device with high transmitted information importance.

5.2.6 Results

With these inputs, the script can be run to perform the risk analysis and the results obtained are:

Risk analysis

All the attacks that the insulin pump is in danger are in table 5.9:

Insulin pump		
Attack	**Impact**	**Risk**
Physical	5.87	6.78
Battery Drainage	3.6	6.44
Eavesdropping	3.6	5.22
Spoofing	5.18	6.8
Traffic analysis	3.6	5.22
Masquerading	5.18	6.36
Man-In-The-Middle	5.18	6.8
Denial-of-Service	3.6	5.82
Impersonation	3.6	5.04

Table 5.9: Insulin pump scenario: Insulin pump risk analysis

All the attacks that the thermometer is in danger are in table 5.10:

Thermometer		
Attack	**Impact**	**Risk**
Physical	2.51	3.42
Battery Drainage	0.0	0.0
Eavesdropping	1.41	3.03
Spoofing	2.51	4.13
Traffic analysis	1.41	3.03
Masquerading	2.51	3.69
Man-In-The-Middle	2.51	4.13
Denial-of-Service	0.0	0.0
Impersonation	1.41	2.85

Table 5.10: Thermometer scenario: Thermometer risk analysis

All the attacks that the cloud server is in danger are in table 5.11:

Cloud server		
Attack	**Impact**	**Risk**
Physical	5.87	6.78
Eavesdropping	3.6	5.22
Spoofing	5.18	6.8
Traffic analysis	3.6	5.22
Masquerading	5.18	6.36
Malware	5.87	8.71
Man-In-The-Middle	5.18	6.8
Denial-of-Service	3.6	5.82
Impersonation	3.6	5.04
Message fabrication/modification/replay	5.87	7.49
Cross Site Request Forgery	5.87	7.49
SQL Injection	5.87	8.09
Account Hijacking	5.18	6.8
Ransomware	5.87	8.71
Brute Force	5.87	9.76
Information Disclosure	3.6	5.67
Deception	3.6	4.78

Table 5.11: Insulin pump scenario: Cloud risk analysis

All the attacks that the doctor's computer is in danger are in table 5.12:

All the attacks that the router is in danger are in table 5.13:

Risk evaluation

For the risk evaluation, a threshold of 5 in the risk values has been selected, so every attack with a higher risk will be considered as relevant. The program analyses it and the results are:

Doctor's computer		
Attack	**Impact**	**Risk**
Physical	5.87	6.78
Eavesdropping	3.6	5.22
Spoofing	5.18	6.8
Traffic analysis	3.6	5.22
Masquerading	5.18	6.36
Malware	5.87	8.71
Man-In-The-Middle	5.18	6.8
Denial-of-Service	3.6	5.82
Impersonation	3.6	5.04
Message fabrication/modification/replay	5.87	7.49
Cross Site Request Forgery	5.87	7.49
Session Hijacking	5.87	8.09
Cross Site Scripting	5.87	8.09
SQL Injection	5.87	8.09
Account Hijacking	5.18	6.8
Ransomware	5.87	8.71
Brute Force	5.87	9.76
Information Disclosure	3.6	5.67
Deception	3.6	4.78

Table 5.12: Insulin pump scenario: Doctor's Computer risk analysis

For the insulin pump: Physical attacks, Battery drainage attacks, Eavesdropping attacks, Spoofing attacks, Traffic analysis attacks, Masquerading attacks, Man-in-the-middle attacks, Denial-of-service attacks, Impersonation attacks.

For the thermometer: No critical risks.

For the cloud server: Physical attacks, Eavesdropping attacks, Spoofing attacks, Traffic analysis attacks, Masquerading attacks, Malware attacks, Man-in-the-middle attacks, Denial-of-service attacks, Impersonation attacks, Message fabrication/modification/replay attacks, Cross Site Request Forgery, Session Hijacking, Cross Site Scripting, SQL Injection, Account hijacking, Ransomware, Brute force attack, Infor-

Router		
Attack	**Impact**	**Risk**
Physical	5.87	6.78
Eavesdropping	3.6	5.22
Spoofing	5.18	6.8
Traffic analysis	3.6	5.22
Masquerading	5.18	6.36
Man-In-The-Middle	5.18	6.8
Denial-of-Service	3.6	5.82
Impersonation	3.6	5.04
Brute Force	5.87	9.76

Table 5.13: Insulin pump scenario: Router risk analysis

mation disclosure.

For the doctor's computer: Physical attacks, Eavesdropping attacks, Spoofing attacks, Traffic analysis attacks, Masquerading attacks, Malware attacks, Man-in-the-middle attacks, Denial-of-service attacks, Impersonation attacks, Message fabrication/modification/replay attacks, Cross Site Request Forgery, Session Hijacking, Cross Site Scripting, SQL Injection, Account hijacking, Ransomware, Brute force attack, Information disclosure.

For the router: Physical attacks, Eavesdropping attacks, Spoofing attacks, Traffic analysis attacks, Masquerading attacks, Man-in-the-middle attacks, Denial-of-service attacks, Impersonation attacks, Brute force attack.

Risk control

For the risk control, depending on the attacks that were relevant to the different assets, the countermeasures were selected, and the results are:

For the insulin pump: Physical security, Structured recovery plan, Mutual authentication, Updated protocol (IPSec), End-to-End encryption, Data integrity checkers (parity bit or checksum).

For the thermometer: No actions needed.

For the cloud server: Physical security, Structured recovery plan, Mutual authentication, Updated protocol (IPSec), End-to-End encryption, Data integrity checkers (parity bit or checksum), Distributing data, Redundancy in data, Fully homomorphic encryption, Strong user authentication system (strong passwords, 2-factor authentication), Privileges definition, Antivirus, antispyware, antiadware, Webapp scanners and firewalls.

For the doctor's computer: Physical security, Structured recovery plan, Mutual authentication, Updated protocol (IPSec), End-to-End encryption, Data integrity checkers (parity bit or checksum), Distributing data, Redundancy in data, Fully homomorphic encryption, Strong user authentication system (strong passwords, 2-factor authentication), Privileges definition, Antivirus, antispyware, antiadware, Webapp scanners and firewalls.

For the router: Physical security, Structured recovery plan, Mutual authentication, Updated protocol (IPSec), End-to-End encryption, Data integrity checkers (parity bit or checksum), Distributing data, Redundancy in data, Webapp scanners and firewalls, Antivirus, antispyware, antiadware, Strong user authentication system (strong passwords, 2-factor authentication).

Thoughts

In this scenario we find out that the worst case always prevails. Attacks and countermeasures in common devices are the same as in the scenario 5.2.1, which is the most critical, with independence of the addition of a less critical device.

Chapter 6 Study of the results

In this chapter, the results will be discussed. First by themselves and then comparing them with an expert's methodology.

6.1 Results Analysis

6.1.1 General

When looking at the results, it is easily seen that the difference is made by the criticality of the medical device in the network. In the thermometer scenario, almost no countermeasures are needed, meanwhile, in the insulin pump, a lot of actions must be done in the whole environment. It is also noticeable that when both devices coexist in the same scenario, the worst case prevails for the rest of the devices.

6.1.2 Attacks

To gain knowledge about the more relevant attacks, table 6.1 is created. There, it can be seen all the attacks, how many times they appear, how many times have been classified as important (risk over 5) and the average risk.

From this table, we get that some attacks appear in all the devices all the time: Physical, Eavesdropping, Spoofing, Traffic Analysis, Masquerading, Man-In-The-Middle and DoS attacks. This is mainly due to the fact that they are network attacks and all the devices are connected.

However, those are not the riskiest attacks. There are three attacks with over 7.5 points on the risk scale and they are: Malware, Ransomware and Brute Force attacks.

Brute Force is not only the riskiest attack, but also it appears on 9 occasions, being in the second tier of most appearances and its risk is always over the threshold. This

Attack	# Appearances	# Risky	Average Risk
Physical	13	8	5.69
Battery Drainage	4	2	3.22
Eavesdropping	13	8	4.38
Spoofing	13	8	5.78
Traffic analysis	13	8	4.38
Masquerading	13	8	5.33
Malware	6	6	7.88
Man-In-The-Middle	13	8	5.77
Denial-of-Service	13	8	4.41
Impersonation	13	8	4.2
Message fabrication/modification/replay	6	4	6.66
Cross Site Request Forgery	6	4	6.66
Session Hijacking	3	3	7.26
Cross Site Scripting	3	3	7.26
SQL Injection	6	6	7.26
Account hijacking	6	4	5.91
Ransomware	6	6	7.88
Brute force	9	9	8.93
Information disclosure	6	4	4.94
Deception	6	0	4.05

Table 6.1: Threat comparison

is why it would be considered the most powerful attack according to this assessment methodology.

There are some attacks that call attention because of their lack of effectiveness, as it is deception, which never surpasses the threshold and therefore can be disregarded. Other attacks have a very low average risk because their risk becomes 0 in no critical devices, as battery drainage or DoS.

6.1.3 Countermeasures

There are different countermeasures. Some of them are useful for many devices, whereas others are useful only in specific cases. Table 6.2 shows the number of appearances for each device of the different countermeasures to remark which are the most important ones.

Countermeasure	Insulin pump	Thermometer	Cloud	Computer	Router	Total
Mutual Authentication	2	0	2	2	2	8
Data Integrity Checkers	2	0	3	3	2	10
Updated protocol	2	0	2	2	2	8
Physical security	2	0	3	3	2	10
End-to-End encryption	2	0	2	2	2	8
Multiple path architecture	0	0	0	0	2	2
Hash in router	0	0	0	0	2	2
Distributing data	0	0	3	3	0	6
Redundancy in data	0	0	3	3	0	6
Fully homomorphic encryption	0	0	3	3	0	6
Web application scanners and firewalls	0	0	3	3	3	9
Strong user authentication system	0	0	3	3	2	8
Privileges definition	0	0	3	3	0	6
Antivirus	0	0	3	3	2	8
Structured recovery plan	2	0	3	3	3	11

Table 6.2: Countermeasures and appearances

In the table can be seen that an absolutely non-critical device does not need any action, however, the infrastructure surrounding it does. It can also be seen that an structured recovery plan is mandatory, while other countermeasures such as Data Integrity Checkers and Physical Security are basic for almost scenario.

It is also important to notice that, in specific devices, some actions are always needed. Apart from the insulin pump that as it is critical actions are needed, devices as Cloud or Doctor's Computer need Distributing Data, Redundancy in Data, homomorphic Encryption, Web application scanners and firewalls, user authentication, privileges definition and antivirus as basic features for every scenario.

6.2 Comparison with the expert procedure

To finally know if the results are as good as expected, an expert opinion has been asked with the same environment as in 5.1. This way, it can be compared with the results of the tool and know if it is accurate enough.

6.2.1 Expert opinion

For this task, the expert wrote a document of the risk assessment. In this document, a list of hazards was included and it was:

- Medical devices' inaccurate functionality
- Medical devices' non-availability
- Patient's information being compromised
- Patient's information not being available

For this expert, both thermometer and insulin pump are critical and the level of likelihood and impact for the above hazards are high, making it a high risk as the impact on the patient is severe.

As all hazards are of high risk, all of them need countermeasures. These countermeasures suggested by the expert are:

- Using strong authentication mechanisms to prevent the adversary from changing the accurate functioning of the medical device
- Implementing physical security in the wire connected to the medical device to prevent a DoS attack
- Implementing authentication systems to prevent unauthorized access
- Implementing backup measures and redundancies to enhance data availability

In the document, it is also said that when adding more devices into the network, the methodology may change by adding modeling tools such as STRIDE, Bowie or track trees to have a better and more comprehensive overview of the threats.

6.2.2 Comparison

As was expected, there are some parts in which the expert opinion coincides with the tool and some that differ. In this subsection, each will be discussed.

When talking about hazards, the expert reflects mainly the attacks on confidentiality, integrity and availability, which are the base of the tool. Nevertheless, in the tool, the attacks for each characteristic are itemized.

The first important difference between the expert's process and the tool is the classification of the thermometer as critical or non-critical. Methodological speaking, the classification of the device according to criticality is based on the FDA classification [7]. In this classification, a thermometer is considered Class II [99], whereas an insulin pump is Class III [100]. However, if the expert opinion differs, it can set in the tool a different level of harm for the patient or criticality of the information.

Regarding the countermeasures, it is a relevant joint of both methodologies, as both the tool and the expert highlight the same important countermeasures. The tool also offers some more that can be used.

6.2.3 Limitations

The tool has obvious limitations, some of them with an easier solution than others.

The attacks and countermeasures used to run the program are just a selection and some relevant ones under certain circumstances might be missing, as well as some new types of attacks.

The classification of devices, as well as the values to calculate impact, are slightly subjected to bias, as they were chosen by personal opinion. Nevertheless, opinions among experts should not differ much, as the fields are quite objective.

On top of that, it is important to remark that this program has only been tested in small networks and works only for them at the moment, being unknown how it would perform in a bigger one.

6.2.4 Conclusion

The results are satisfying as both methodologies are very similar and it was the main goal. The problem might occur when more devices are added and, in that case, a more precise analysis would be needed. However, it has been proven that in small or partial networks, this tool is satisfactory. Furthermore, having more possible countermeasures and attacks may distract the attention from the most relevant ones.

With this, the **RQ3** "How different would be this approach compared to the one made by an expert?" is answered, making it clear that it would be similar for small environments.

Chapter 7
Conclusion and future work

This have been a big project in which most part of the time was used for documenting through standards and reliable sources the best way to perform a good risk assessment in healthcare networks that could be automated.

When created the risk assessment process, it was coded in Python, generating the results showed in chapter 5. These results were quite satisfying in the studied scenarios, so the development of the project has been successful.

However, these scenarios are not as realistic as they should be, considering the amount of the devices involved and, in bigger environments, changes should be made to generate better results. This has been an introduction to clear the path and set a first stone to keep growing in a topic that has not been researched enough.

For the future it is needed that this thesis keeps growing, improving the size and detail of the database and the programming. Possibly using new technologies as AI to achieve the goal of being able to assess the risk of whole hospitals.

References

[1] H. M. Epstein, «The most important medical issue ever: And why you need to know more about it», *Dx IQ*, 2019.

[2] G. Pandian, V. Vinayagam, *et al.*, «Security challenges of iot and medical devices in healthcare», in *Internet of Things*, CRC Press, 2020, pp. 87–106.

[3] W. H. Organization *et al.*, «Global expenditure on health: Public spending on the rise?», 2021.

[4] I. Intelligence, «Us healthcare industry in 2022: Analysis of the health sector, healthcare trends, and future of digital health», 2022.

[5] D. Betts, L. Korenda, and S. Giuliani, «Are consumers already living the future of health», *Deloitte*, 2020.

[6] FDA, «How to determine if your product is a medical device», 2019.

[7] ——, «Classify your medical device», 2020.

[8] ——, «Device classification panels», 2018.

[9] J. Haughey, K. Taylor, *et al.*, *Medtech and the internet of medical things: How connected medical devices are transforming health care*, 2018.

[10] F. Alsubaei, A. Abuhussein, and S. Shiva, «Security and privacy in the internet of medical things: Taxonomy and risk assessment», in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, IEEE, 2017, pp. 112–120.

[11] P. A. Williams and A. J. Woodward, «Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem», *Medical Devices (Auckland, NZ)*, vol. 8, p. 305, 2015.

[12] W. Burleson, S. S. Clark, *et al.*, «Design challenges for secure implantable medical devices», in *DAC Design Automation Conference 2012*, IEEE, 2012, pp. 12–17.

[13] S. Matthiesen and P. Bjørn, «Why replacing legacy systems is so hard in global software development: An information infrastructure perspective», in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 2015, pp. 876–890.

[14] M. Willing, C. Dresen, *et al.*, «Analyzing medical device connectivity and its effect on cyber security in german hospitals», *BMC medical informatics and decision making*, vol. 20, no. 1, pp. 1–15, 2020.

[15] J. Sametinger, J. Rozenblit, *et al.*, «Security challenges for medical devices», *Communications of the ACM*, vol. 58, no. 4, pp. 74–82, 2015.

[16] A. Dogac, G. B. Laleci, *et al.*, «Artemis: Deploying semantically enriched web services in the healthcare domain», *Information Systems*, vol. 31, no. 4-5, pp. 321–339, 2006.

[17] G. Bell and M. Ebert, «Health care and cyber security: Increasing threats require increased capabilities», *KPMG*, 2015.

[18] M. Nawir, A. Amir, *et al.*, «Internet of things (iot): Taxonomy of security attacks», in *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, 2016, pp. 321–326.

[19] V. Kumar, R. K. Jha, and S. Jain, «Nb-iot security: A survey», *Wireless Personal Communications*, vol. 113, no. 4, pp. 2661–2708, 2020.

[20] M. Papaioannou, M. Karageorgou, *et al.*, «A survey on security threats and countermeasures in internet of medical things (iomt)», *Transactions on Emerging Telecommunications Technologies*, e4049, 2020.

[21] NIST, «Eavesdropping - glossary», *NIST*,

[22] M. M. Hossain, M. Fotouhi, and R. Hasan, «Towards an analysis of security issues, challenges, and open problems in the internet of things», in *2015 ieee world congress on services*, IEEE, 2015, pp. 21–28.

[23] NIST, «Spoofing - glossary», *NIST*,

[24] Z. Ling, J. Luo, *et al.*, «Security vulnerabilities of internet of things: A case study of the smart plug system», *IEEE Internet of Things Journal*, vol. PP, pp. 1–1, May 2017.

[25] NIST, «Traffic analysis - glossary», *NIST*,

[26] M. Ben Salem, «Towards effective masquerade attack detection», Ph.D. dissertation, USA, 2012.

[27] NIST, «Man-in-the-middle - glossary», *NIST*,

[28] G. N. Nayak and S. G. Samaddar, «Different flavours of man-in-the-middle attack, consequences and feasible solutions», in *2010 3rd International Conference on Computer Science and Information Technology*, IEEE, vol. 5, 2010, pp. 491–495.

[29] NIST, «Denial of service - glossary», *NIST*,

[30] ——, «Impersonation - glossary», *NIST*,

[31] M. A. Allouzi and J. I. Khan, «Identifying and modeling security threats for iomt edge network using markov chain and common vulnerability scoring system (cvss)», *arXiv preprint arXiv:2104.11580*, 2021.

[32] M. Sher and T. Magedanz, «A vulnerabilities analysis and corresponding middleware security extensions for securing NGN applications», *Computer Networks*, vol. 51, no. 16, pp. 4697–4709, 2007.

[33] KirstenS, «Cross site request forgery (csrf)», *OWASP*,

[34] OWASP, «Session hijacking attack», *OWASP*,

[35] KirstenS, «Cross site scripting (xss)», *OWASP*,

[36] Kingthorin, «Sql injection», *OWASP*,

[37] NIST, «Malware - glossary», *NIST*,

[38] TrendMicro, «Ransomware», *TrendMicro*,

[39] Gsami, «Brute force attack», *OWASP*,

[40] Z. Banach, «Information disclosure vulnerabilities and attacks in web applications», *Netsparker*,

[41] Deception., *Cambridge Advanced Learner's Dictionary & Thesaurus*. Cambridge University Press, 2022.

[42] J. T. Hancock, «Digital deception», *Oxford handbook of internet psychology*, vol. 61, no. 5, pp. 289–301, 2007.

[43] M. M. Ahemd, M. A. Shah, and A. Wahid, «Iot security: A layered approach for attacks & defenses», in *2017 international conference on Communication Technologies (ComTech)*, IEEE, 2017, pp. 104–110.

[44] H.-L. Yeh, T.-H. Chen, *et al.*, «A secured authentication protocol for wireless sensor networks using elliptic curves cryptography», *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[45] T. Richardson and S. Kudekar, «Design of low-density parity check codes for 5g new radio», *IEEE Communications Magazine*, vol. 56, no. 3, pp. 28–34, 2018.

[46] J.-M. Tilli and R. Kantola, «Data plane protocols and fragmentation for 5g», in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, IEEE, 2017, pp. 207–213.

[47] D. Migault, D. Palomares, *et al.*, «E2e: An optimized ipsec architecture for secure and fast offload», in *2012 Seventh International Conference on Availability, Reliability and Security*, IEEE, 2012, pp. 365–374.

[48] K. Saleem, Z. Tan, and W. Buchanan, «Security for cyber-physical systems in healthcare», in *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*, Springer, 2017, pp. 233–251.

[49] C. Gentry, S. Halevi, and V. Vaikuntanathan, «I-hop homomorphic encryption and rerandomizable yao circuits», in *Annual Cryptology Conference*, Springer, 2010, pp. 155–172.

[50] A. Sabelfeld and A. Myers, «Language-based information-flow security», *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 1, pp. 5–19, 2003.

[51] H. Suo, J. Wan, *et al.*, «Security in the internet of things: A review», in *2012 international conference on computer science and electronics engineering*, IEEE, vol. 3, 2012, pp. 648–651.

[52] R. I. M. Milton Mueller Brenden Kuerbis, «Routing security», *Internet Governance Project*,

[53] A. Celik, J. Tetzner, *et al.*, «5g device-to-device communication security and multipath routing solutions», *Applied Network Science*, vol. 4, no. 1, pp. 1–24, 2019.

[54] M. Freedman, «Hashing in networked systems», *Princeton: Computer Networks (COS 461)*,

[55] W. So, A. Narayanan, and D. Oran, «Named data networking on a router: Fast and dos-resistant forwarding with hash tables», in *Architectures for Networking and Communications Systems*, IEEE, 2013, pp. 215–225.

[56] N. Sultan, «Making use of cloud computing for healthcare provision: Opportunities and challenges», *International Journal of Information Management*, vol. 34, no. 2, pp. 177–184, 2014.

[57] P. V. N. Dhawas, P. Juikar, *et al.*, «A secured cost effective multi-cloud storage in cloud computing», 2013.

[58] Y. Singh, F. Kandah, and W. Zhang, «A secured cost-effective multi-cloud storage in cloud computing», in *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2011, pp. 619–624.

[59] C. Esposito, A. De Santis, *et al.*, «Blockchain: A panacea for healthcare cloud-based data security and privacy?», *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[60] Z. Brakerski and V. Vaikuntanathan, «Efficient fully homomorphic encryption from (standard) lwe», *SIAM Journal on Computing*, vol. 43, no. 2, pp. 831–871, 2014.

[61] T. A. Rao and E. Haq, «Security challenges facing iot layers and its protective measures», *International Journal of Computer Applications*, vol. 975, p. 8887, 2018.

[62] D. W. Wilson, J. F. B. Bourdillon, and C. Aabye, *Authentication using application authentication element*, US Patent 9,883,387, Jan. 2018.

[63] K. Wei, M. Muthuprasanna, and S. Kothari, «Preventing sql injection attacks in stored procedures», in *Australian Software Engineering Conference (ASWEC'06)*, IEEE, 2006, 8–pp.

[64] P. A. Porras, S. Cheung, *et al.*, «Securing the software defined network control layer.», in *NDSS*, 2015.

[65] D. Bhattacharyya, R. Ranjan, *et al.*, «Biometric authentication: A review», *International Journal of u-and e-Service, Science and Technology*, vol. 2, no. 3, pp. 13–28, 2009.

[66] A. Razzaq, A. Hur, *et al.*, «Critical analysis on web application firewall solutions», in *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, 2013, pp. 1–6.

[67] M. Dusi, M. Crotti, *et al.*, «Tunnel hunter: Detecting application-layer tunnels with statistical fingerprinting», *Computer Networks*, vol. 53, no. 1, pp. 81–97, 2009.

[68] IEC, «Application of risk management for IT-networks incorporating medical devices», International Electrotechnical Commission, Standard, Oct. 2021.

[69] R. Powell, «10 must-have layers of business security», *LBMC*,

[70] M. Alshaikh, «Developing cybersecurity culture to influence employee behavior: A practice perspective», *Computers & Security*, vol. 98, p. 102 003, 2020.

[71] D. Dasgupta, A. Roy, and A. Nag, «Multi-factor authentication», in *Advances in User Authentication*, Springer, 2017, pp. 185–233.

[72] ISO, «Medical devices - Application of risk management to medical devices», International Standards Organization, Standard, Jul. 2020.

[73] A. J. Card, J. R. Ward, and P. J. Clarkson, «Beyond fmea: The structured what-if technique (swift)», *Journal of Healthcare Risk Management*, vol. 31, no. 4, pp. 23–29, 2012.

[74] FDA, «Cybersecurity», 2022.

[75] IMDRF, «Principles and practices for medical device cybersecurity», 2020.

[76] J. Kurtz, «Securing internet-connected medical devices», *NIST*, 2020.

[77] Healthcare and P. H. S. C. Councils, «Medical device and health it joint security plan», 2019.

[78] FDA, «International medical device regulators forum (imdrf)», 2019.

[79] H. A. Linstone, M. Turoff, *et al.*, *The delphi method.* Addison-Wesley Reading, MA, 1975.

[80] A. de Ruijter and F. Guldenmund, «The bowtie method: A review», *Safety science*, vol. 88, pp. 211–218, 2016.

[81] B. Ale, P. Burnap, and D. Slater, «On the origin of pcds–(probability consequence diagrams)», *Safety science*, vol. 72, pp. 229–239, 2015.

[82] NIST, «Cybersecurity framework», *NIST*, 2022.

[83] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach.* FAIR, 2014.

[84] J. Wynn, J. Whitmore, *et al.*, *Threat Assessment & Remediation Analysis (TARA).* MITRE, 2011.

[85] E. Ruijters and M. Stoelinga, «Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools», *Computer science review*, vol. 15, pp. 29–62, 2015.

[86] D. Heckerman, «A tutorial on learning with bayesian networks», *Innovations in Bayesian networks*, pp. 33–82, 2008.

[87] N. Siu, «Risk assessment for dynamic systems: An overview», *Reliability Engineering & System Safety*, vol. 43, no. 1, pp. 43–73, 1994.

[88] P. Mell, K. Scarfone, and S. Romanosky, «Common vulnerability scoring system», *IEEE Security Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[89] I. Stine, M. Rice, *et al.*, «A cyber risk scoring system for medical devices», *International Journal of Critical Infrastructure Protection*, vol. 19, pp. 32–46, 2017.

[90] A. Amro, V. Gkioulos, and S. Katsikas, «Assessing cyber risk in cyber-physical systems using the att&ck framework», *Preprint at http://dx. doi. org/10.13140/RG*, vol. 2, no. 16531.40484, 2021.

[91] G. Gonzalez-Granadillo, S. A. Menesidou, *et al.*, «Automated cyber and privacy risk management toolkit», *Sensors*, vol. 21, no. 16, p. 5493, Aug. 2021.

[92] K. Seale, J. McDonald, *et al.*, «Meddevrisk: Risk analysis methodology for networked medical devices», in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[93] F. Alsubaei, A. Abuhussein, *et al.*, «Iomt-saf: Internet of medical things security assessment framework», *Internet of Things*, vol. 8, p. 100 123, 2019.

[94] R. Somasundaram and M. Thirugnanam, «Review of security challenges in healthcare internet of things», *Wireless Networks*, pp. 1–7, 2020.

[95] T. Yaqoob, H. Abbas, and M. Atiquzzaman, «Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review», *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723–3768, 2019.

[96] S. A. Butt, J. L. Diaz-Martinez, *et al.*, «Iot smart health security threats», in *2019 19th International Conference on computational science and its applications (ICCSA)*, IEEE, 2019, pp. 26–31.

[97] ISO, «Information technology - Security techniques - Information security management systems - Requirements », International Standard Organization, Standard, Mar. 2017.

[98] S. Haugen and M. Rausand, «Risk acceptance criteria», *NTNU*,

[99] FDA, «Clinical electronic thermometer», 2022.

[100] ——, «Pump, infusion, insulin, to be used with invasive glucose sensor», 2022.