International Journal for Scientific Research (IJSR)

المجلة الدولية للبحوث العلمية

Vol. (3), No. (5) May 2024 الإصدار (3)، العدد (5)

Cyber-attacks Risk Analysis of a Connected Pulse Oximeter Device: A Threat Modeling Using STRIDE and DREAD Models

Nebras Sobahi
Electrical and Computer Engineering Department, King Abdulaziz University, Jeddah, Saudi Arabia
nsobahi@kau.edu.sa

Abdullah S. Bamabad
Electrical and Computer Engineering Department, King Abdulaziz University, Jeddah, Saudi Arabia
aawadhbamaabad@stu.kau.edu.sa

Abstract

The term "Internet of Things (IoT)" has gained significant traction in recent years due to its wide-ranging applications across various industries, including the healthcare sector. These medical devices, known as connected medical devices, offer immense benefits to patients with chronic diseases and others. However, despite their advantages, regulatory bodies responsible for issuing medical device sales and usage permits currently lack a standardized method for evaluating the security and cybersecurity resilience of these devices before granting approval.

The proposed threat modeling approach is an engineering tool that utilizes the STRIDE model to identify and categorize potential threats to connected devices, determine the mitigation techniques employed, and generate a comprehensive report. Additionally, the DREAD model is employed to assess the severity of potential threats throughout the development life cycle of the connected medical device.

This paper aims to validate the accuracy and realism of the outcomes derived from this tool and assess the ease of implementation of the proposed methodology by medical device designers and biomedical engineers who lack cybersecurity expertise.

The results of applying the proposed threat modeling approach using the STRIDE and DREAD models to an open-source connected pulse oximeter revealed a low average severity score for the connected medical device against potential cyber threats. Our approach was also compared to other threat modeling methods in terms of the number of steps, implementation complexity, and result realism. The findings demonstrat that our threat modeling approach requires the fewest steps, does not necessitate cybersecurity expertise for implementation, and produces more realistic and stable results.

Consequently, we propose that the FDA adopt and implement our proposed approach to expedite the approval process for the sale and use of these medical devices, enabling healthcare providers to leverage connected medical devices on a wider scale to combat diseases and epidemics, ultimately delivering higher quality and more effective healthcare.

Keywords: Threat modeling, Cyber-security Threats, Connected Medical Device, STRIDE, DREAD.

1- Introduction

The Internet has become a significant part of people's daily lives, as it is used for work, entertainment, education and other activities. It is expected that the number of users will reach 30 billion by 2025 [1].

When medical devices include the Internet of Things technology in their composition, they become connected to the Internet and are called Connected Medical Devices (CMDs). These medical devices may be in the form of medical

devices that are injected under the patient's skin, implanted into the patient's body through surgery, or wearable devices [2] [3].

There was a great demand from healthcare organizations for CMDs, especially in the last four years when the Corona pandemic hit the entire world, as these medical devices were one of the solutions to confront this pandemic by using them on patients infected with Coronavirus, because we need them for monitoring vital signs continuously such as the oxygen level and heart rate of the patient inside Isolation rooms.

This increasing demand for CMD has created great pressure on the Food and Drug Authority (FDA), as it sets mandatory standards to regulate and supervise the process of issuing approval for using medical devices of all kinds. Many connected medical devices have been allowed to be used and widely spread in healthcare organizations around the world.

Unfortunately, there is a possibility of attacking the CMDs and modifying and controlling the software of them remotely by simple means and available devices at a reasonable price [4]. Interpol warned in April 2020 of a global surge in COVID-19-related cyber-attacks [5]. There have been a large number of recalls of CMDs in the last ten years, and the main reason for this is that the FDA has not approved a specific method to measure the level of security of CMDs against cybersecurity attacks and the severity of these attacks on them [4] [3]. There are reasons why the FDA has not approved any method yet: the first is the lack of sufficient knowledge of all inspection protocols for this type of medical devices, and the second is the lack of knowledge of the optimal methods for verifying their security measures against attacks and the mitigation and protection tools applied to them. The reason for the lack of knowledge is the rapid development of the cybersecurity environment and the correspondingly long time to review international standards and republish them again [6]. An important reason why some CMDs have poor security is because

manufacturers do not develop security program because the cost of developing and maintaining security program is greater than the cost of medical software already in CMDs [7].

This paper proposes a solution using a threat modeling tool. This tool performs technical and engineering procedures to identify CMD assets, discover the potential threats and classify them using the STRIDE model, and finally assesses the severity of these potential threats using the DREAD model.

We will try to apply the tool to a real open-source Connected Pulse Oximeter (CPO) device to get realistic results. Also, we will compare our threat modeling method with another threat modeling method and explore which method is most easily to implement with realistic results and which method is suitable for adoption by the FDA. We aspire to provide this tool as an evidence that clarifies the process of assessing the risk of using CMD and the extent of its security against cyberattacks before granting it a marketing license in the local market.

2- Literature Review

Many studies have presented approaches and tools for threat modeling in healthcare. These approaches differ from each other in the type of medical device and system that was tested, their methods and models for identifying the main components and classifying potential threats, models for assessing the level of risk of their use against cyber-attacks, presentation of results, the number of researchers and the level of experience required to apply it, which leads to the inability to compare them with each other. We summarize below these studies, their methodology, the models used, and the results, if mentioned.

Lechner et al., [8] Presented the results of an integrative literature review of published studies on threat modeling methods in the connected medical devices industry. They found that 32 methods and approaches have been experimented with

fig (1). The STRIDE/DREAD models are the most widely used models in previous studies, with 12 studies.

The authors note that there is a lack of previous research on this topic, although their findings suggest that this is an important and active topic of research in recent years. They emphasize the need for more research to investigate the advantages and disadvantages of these models and tools, and to determine whether threat modeling is appropriate for both new and old CMDs or not.

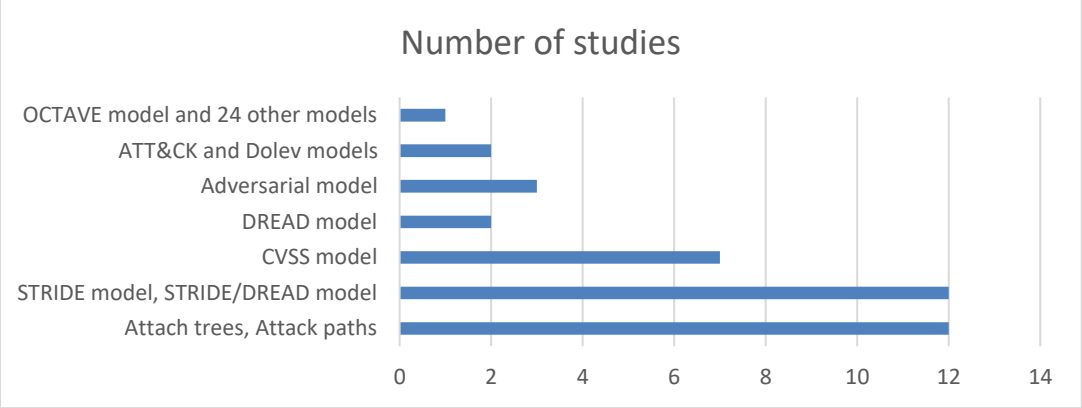


Figure 1: Number of studies for each identified threat modeling method/ approach [8]

M. Cagnazzo et al., [9] present in their paper an overview of the classical information security for a mobile health (mHealth) virtual environment using IoT technology. They identified and classified the threats through the Microsoft Threat Modeling Tool 2017 using the STRIDE methodology, and then determined the risk levels associated with these threats using the DREAD model, and finally explained the possible mitigation strategies to obtain an acceptable safe and reliable environment. The researchers focused on two categories of attacks: physical attacks, such as the physical destruction of medical sensors, or virtual attacks, such as denial-of-service attacks. They assumed that all of these categories of threats could be overcome by using a modern authentication and encryption mechanism. They recommend that

future research should focus on exploration and exploitation of threats, ways to mitigate them, and the relationship between security threats and patient safety. Finally, they stated that in their future work they will validate their approach by implementing it in a real-world scenario.

TSENG et al., [2] apply a strategy based on simulating potential attack hypotheses for health wearable devices and identifying appropriate test and evaluation methods. The overview of the data flow diagram (DFD) in the architecture was created using the Microsoft Threat Modeling tool. The STRIDE model was used to detect the threats and the DREAD model was used to calculate the risk ratio. They used Wireshark, Nmap and Router-Sploit tools to scan the device and ensure there is no risk of information being disclosed or the device being compromised. The results showed that the device does not suffer from the possibility of brute force hacking by remote login. They indicated that in future work they will establish a superior security protection mechanism after referencing to international standards in order to implement more accurate and realistic verification and auditing steps.

V. Vakhter et al., [3] aim in their work to make the primary stakeholders of Miniature Wireless Biomedical Devices (MWBDs) aware of the risks associated with all categories such as injectable, ingestible, implantable and wearable devices. They recommended that the process of securing MWBDs begin with threat modeling. They introduced a domain-specific qualitative-quantitative threat model dedicated to MWBDs and applied it to hypothetical representative case studies from each category of MWBDs. They mentioned the definitions of the STRIDE and DREAD models only in general, without addressing them in the practical part.

All of the threat models designed were focused on one stakeholder, the user, but they emphasized that in future work they would focus on other key stakeholders in MWBDs, including manufacturers and hospitals.

A. Mohamed et al., [8] established a threat modeling process for telehealth systems using Microsoft Threat Modeling Tool 2014. They identify and analyze system assets, threat agents, adverse actions, threats and their impacts, as well as a list of countermeasures in order to mitigate the threats. The goal of this paper is to develop security requirements and to design and implement solutions to better protect the system against threats to telehealth applications. They disclosed that their future research will be on analyzing external threats in the telehealth system and verifying whether the applied system protection solutions will work effectively and efficiently on the identified threats.

The STRIDE model was used to identify threats, and there was no methodology or model to assess their severity.

A. Omotosho et al., [10] created a website that provides a threat model for some connected medical devices, which helps designers and users of these connected medical devices identify potential threats to their devices through the STRIDE model, and also classify their severity through the DREAD threat classification model.

Also, they suggest preventive measures for all threats to the selected devices in order to mitigate their severity. The study aims to improve the infrastructure for designing CMDs and recommend the safest CMDs.

D. KIM et al., [11] proposed a different multicriteria decision-making model to prioritize medical devices based on security threats against them. The model uses AHP to identify medical devices of high importance that need to be included in hospital MEMPs. The proposed hierarchical structure includes eight assessment criteria: CT, DF, DT, FT, PR, AOP, ASP, and maintenance requirements. The output of the model is an estimate of the total risk considering security threats assessed using ASP, AOP, and PR. They believe that their proposed model will be useful for

biomedical engineering departments in hospitals to establish and regulate programs for safe and reliable medical equipment management.

A limitation of the model proposed in this study is that expert participation is required when applying the model to medical devices. Biomedical engineers may not always be able to accept the outcome of prioritization of security threats [11].

The Saudi Food and Drug Authority (SFDA) [12] provided guidelines for health care providers about the cybersecurity of medical devices connected through the personal Internet, hospital networks, or other medical devices, in order to confront the risk of cyber- attacks or mitigate their impact. Five different ways in which accidents or cyber- attacks on medical devices may occur are mentioned. Seven recommendations have also been formulated for health care providers to avoid or mitigate the impact of cyber- attacks, in order to provide safer, higher quality health care.

Patricia AH Williams and Andrew J Woodward [13] have identified the weaknesses of medical devices in their environment rather than in the technical form, describing them as complex and multifaceted problem. They also defined several concepts that overlap with the medical device environment in relation to vulnerabilities in cybersecurity. They also mentioned a number of weaknesses in the network and wireless, factors complicating the process of protecting medical devices, solutions space and its challenges and the best practice technical controls. The paper was concluded by mentioning the factors that may affect the development of medical devices in the future in terms of cybersecurity.

We noticed that a large number of these studies either presented a small part of the results and discussed them briefly, or did not mention them at all. All studies also emphasized the need for future studies to implement these tools and models on actual CMDs in real-life environments.

3- Methodology

The difficulty of testing the threat modeling tool on a real CMD from the local market and publishing the results of the security assessment lies in two reasons: the first is that this behavior may expose the publisher to legal action for defamation for publishing the vulnerabilities of their product. Second: The lack of sufficient security information for CMD in the market because developers and manufacturers do not publish the security characteristics of their device components and mitigation tools to the public, which makes it difficult to apply the threat modeling steps on them.

Due to our desire to obtain real and logical results, we have made a prototype for a CMD, which is a pulse oximeter device connected to the Internet.

3.1 Connected Pulse Oximeter

The Pulse Oximeter device is a medical device used to indirectly measure blood oxygen saturation (SpO2) (%) and heartbeats per minute (bpm) without harming their bodies [14].

We designed CPO to be used by an elderly patient with COVID-19. The patient is isolated from the rest of his family in a room in his house. The doctor responsible for the patient can monitor the vital measurements live without delay by the Internet through a cloud platform either through the website or a mobile application. The patient and his family can monitor the vital measurements through a small screen connected to the device via wires.

The CPO prototype was built using the MAX30100 pulse oximeter sensor, ESP8266 node Micro-Controller Unite (MCU), Oled display, and BLYNK platform. The MAX30100 is an oximetry and heart rate monitoring sensor solution. The ESP2866 microcontroller sends the biometrics from the MAX30100 sensor to the BLYNK platform via the Internet. The best part of this project is that you can connect this

device to the Blynk platform which will record and display data regularly for both SPO2 and BPM online for authorized people only.

3.1.1 CPO components

When assessing the security of any electronic device, the main components used in the device and the important security features related to the assessment must be known.

1- MAX 30100 Sensor

It is named as such because the manufacturing company of this sensor is Maxim. It is an integrated pulse oximeter and heart rate sensor [15].

Here are some of the MAX30100 sensor features:

- An I2C interface is available.
- Operates from 1.8V and 3.3V power supplies.
- Can be powered down through software with negligible standby current.
- It is well applied to Wearable Devices, Fitness Assistant Devices, and Medical Monitoring Devices.
- Can be powered down through software with negligible standby current.
- The high signal-to-noise ratio (SNR) provides strong and motion-free data acquisition.
- High capability for fast data output.

The MAX30100 sensor does not have any notable security features, except that it can only be used by connecting it to a microcontroller through wires, which is considered a more secure method than connecting via Wi-Fi or Bluetooth. This means that it is only vulnerable to physical attacks, such as theft or tampering threats.

2- NodeMCU ESP8266

Espressif Systems, a Shanghai-based Chinese semiconductor company, has launched a small controller called ESP8266 that supports Wi-Fi technology [16].

Here are some security features of the NodeMCU ESP8266:

- **Encryption:**
- WPA/WPA2: Secures Wi-Fi communication between the ESP8266 and access points.
- TLS/SSL: Protects communication with online services and servers.
- **Authentication:**
- Password protection: Requires a password to connect to the ESP8266 over Wi-Fi or access its web interface.
- API keys: Uses unique API keys to authorize communication with cloud services or other devices.
- **Secure Storage:**
- Limited on-board flash memory, but external storage like SD cards can be used.
- **Open-source Community:**
- Large and active community that develops secure coding practices and security implementation tools.

3- Blynk platform

Blynk is an application and platform for creating, deploying, and remotely managing IoT projects. With a code of only 10 lines, any engineer with an electronics background and familiarity with MCUs such as ESP8266, ESP32, or Arduino can create mobile and web applications to interact with a connected device without the need for any additional skills [17].

BLYNK platform specifications and security features [17]:

- **Device Management:**
- Device provisioning
- Built-in Wi-Fi provisioning
- User registration

- Partner management

➢ **Data Management and Visualization:**

- Sensor data visualization
- Secure cloud storage (ready-to-use)
- Data analytics
- Accessing data with 3rd party software

➢ **Remote Control and Automation:**

- Remote control with mobile and web applications
- Over-The-Air firmware updates
- Alerts
- Automation

➢ **App Development (No-code):**

- Drag-n-drop editors for mobile app creation
- Powerful dashboard with drag-n-drop UI editor

➢ **Other:**

- Transactional emails
- Two-day average prototype build time

4- OLED:

The Tiny 128x64 OLED Display is a compact and versatile display module that packs a punch with its high resolution, wide viewing angles, and low power consumption. Its self-luminous OLED panel eliminates the need for a backlight, further reducing power draw. Mounted on an easy-to-solder PCB, the display communicates seamlessly with microcontrollers via the I2C serial bus interface. Its compact size, low power consumption, and high resolution make it ideal for IoT devices [18].

3.2 Threat Modeling

It is a technical engineering tool designed by Microsoft to help companies and developers identify threats, attacks, vulnerabilities, and actions that may affect their application or device [9] [3] [2]. The threat modeling tool is used to shape device design and eliminate or reduce the risk of cyber-attacks to achieve manufacturers' security goals.

This tool can be plugged into the security development life cycle of any system to track problems for the device. Microsoft has provided clear instructions on how to create and analyze threat models, which all developers, even non-security experts, can easily use [19]. The threat modeling tool has made it easier for all developers to visualize system components, data flows, and security boundaries through standard notation; to help them identify the threat categories they should consider based on their device architecture.

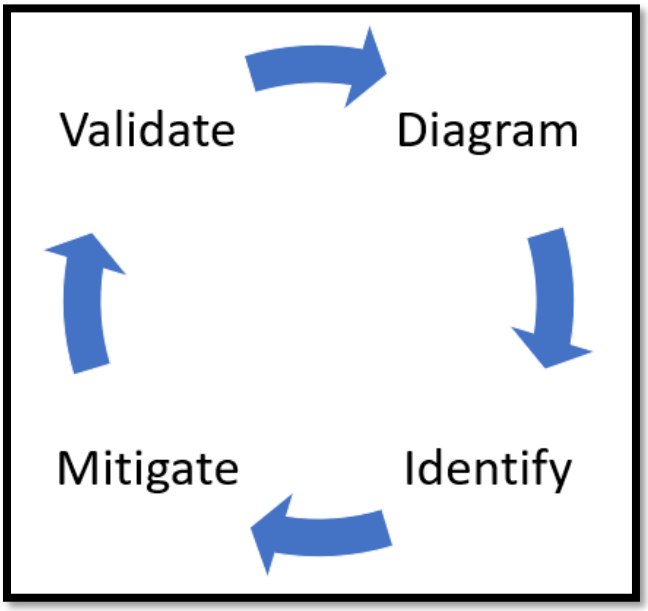


Figure 2: Threat modeling steps [19]

There are 4 main steps for threat modeling:

1. Create a data flow diagram DFD

Data flow diagram is the first main step in implementing threat modeling. In this step, we carefully check and validate the assumptions and information.

The data flow diagram visually illustrates the flow of data between key assets and their interaction with components so that we can comprehensively gather information about the CMD system infrastructure, enabling us to describe the decision-making environment depending on risks.

The data flow diagram should include all possible tasks performed by CMD components and objects, such as sensors, controllers, users, medical personnel, platform, other stakeholders, input sources, and output destinations.

We will use Microsoft's threat modeling tool to create a data flow diagram for the CPO, where all stakeholders, device components, their security properties, ways to connect components to each other, direction of data flow, and security boundaries are defined (See Fig 9).

2. Identifying potential weaknesses and threats

In this step, we will also use Microsoft's threat modeling tool to generate a detailed report of potential threats to the CPO's data flow diagram with single click, and then we will classify them using the STRIDE model to simplify the process of assessing the severity of these threats. This report contains important information such as the date the report was created, by whom, the name of the device or system, description, the number of threats, the number of mitigated threats, the number of threats that need to be investigated, and the total. This report, after being clearly filled out, can be submitted to the FDA as a supporting document that contains a lot of information that will help the FDA identify the components of the CMD, its security properties,

the ways the components communicate with each other, the type of data and operations between them, and the security protocols applied to each component. This detailed report will make it easier for the manufacturer to provide proof that it used safe ingredients and strong security protocols on its CMD, thus increasing the chance of obtaining an FDA license (See Fig 10).

2.1 STRIDE Model

The STRIDE model is one of the most widely used and effective techniques in helping designers and engineers remember and classify potential threats to the connected device they are designing or using. It represents six types of threats, which are:

- **Spoofing**: It means using someone else's credentials to gain unauthorized access to the assets. Spoofing attacks are executed by passing forged or stolen credentials.
- **Tampering**: It is a broad term that includes various cyber-security attacks involving the unauthorized alteration or manipulation of data, systems, or processes.
- **Repudiation**: This type of threat happens when a user denies performing a certain action, and there is no available evidence to prove otherwise. The CPO may be vulnerable to repudiation threats if the actions that could compromise security are not recorded.
- **Information Disclosure**: These threats involve disclosing information to unauthorized users. Any program that passes data to and from a user's cache is vulnerable to information disclosure threats.
- **Denial of Service (DoS)**: These attacks threaten the ability of authorized users to access resources.
- **Elevation of Privilege (EoP)**: It is a critical security vulnerability and attack technique where an attacker acquires unauthorized access or control within a

system or network.

3. Mitigating or eliminating threats

It is the primary goal of threat modeling. This step improves the security of the CPO by providing the engineer or designer with information that can be used to mitigate or completely eliminate the severity of potential threats.

All discovered threats must be mitigated in the design of our CPO device. While active mitigating of each identified threat is ideal, the reality of cybersecurity requires careful decision-making based on the potential impact and feasibility of mitigation strategies.

In our CPO prototype, some mitigations were implemented, as mentioned in the safety properties of the main components of the device. Mitigation measures were implemented by carefully selecting the safest components and replacing less safe parts with safer parts until the final design of the safest CPO device was achieved. Describing the CPO user's situation and surrounding environment also had an impact on mitigating the possibility of some potential threats occurring or reducing their damage.

4. Validate all dilutions (Threat Assessment)

After identifying mitigation tools and techniques for each threat discovered by the STRIDE model, it is necessary to evaluate the risks of each type of the discovered threats and ensure that the mitigation tools and procedures applied to them are effective in mitigating the severity of the threats; because it is not enough to identify the vulnerabilities and types of threats discovered and how to exploit them to attack the CMD and then develop strategies and tools to mitigate them only, rather, we must then evaluate the severity of these potential threats after applying the mitigation strategies, and prioritize them relatively, and develop more secure mitigation

strategies if necessary. Then, we need to repeat the threat modeling lifecycle steps again until we arrive at a secure design for our CMD against cyber-security attacks.

One of these risk analysis methodologies is DREAD model, a threat modeling framework created by Microsoft [19].

4.1 DREAD Model

It is an acronym that describes five threat assessment categories to our CPO. The DREAD model represents the first letters of the words Damage, Reproducibility, Exploitability, Affected Users, and Discoverability.

The DREAD model uses a numerically graded rating system for each category to calculate and evaluate the overall severity level of each threat after applying mitigation tools and procedures. Each category has four levels of severity (from 0 to 3). The average severity score is calculated using the following equation:

Average Severity Score = (Damage Score + Reproducibility Score + Exploitability Score + Affected Users Score + Discoverability Score) / 5

In this paper, we divide the overall severity score for each threat into 3 severity levels:

- Low-risk threats (3 to 7): These threats are unlikely to have a significant impact on the CPO device or its users. They may be difficult to exploit or may only affect a small number of users.

- Medium-risk threats (8 to 11): These threats are more likely to have a significant impact on the CPO device or patients. They may be easier to exploit or may affect a larger number of users.

- High-risk threats (12 to 15): These threats are most likely to have a severe impact on the CPO device or its patients. They are very easy to exploit or affect a large number of users.

As for the definition of the evaluation categories for the DREAD model and the scores for each of them, they are as follows:

- **Damage**: An assessment of the potential impact of a successful attack. The damage may be in the form of changing or losing patient biometrics, viewing or stealing them, or the device's failure to send and receive them over the internet.

Table 1: Definition for Damage scores

Score	Definition
0	No damage, the threat's damage has been completely mitigated.
1	Damage with a backup solution, or the attacker's ability to access only general personal information.
2	The unavailability of sensitive patient data or the attacker's viewing of it with the ability to recover quickly.
3	Changing sensitive data, disabling the system completely, complex recovery.

- **Reproducibility**: A category that measures the extent to which a particular type of cyber threat or attack can be replicated successfully. A threat that can be easily replicated is more likely to be exploited than a security vulnerability that occurs rarely or is unpredictable. For example, the same threat occurs across more than one object or asset in the CPO environment and the same attack can be successful on all of them.

Table 2: Definition for Reproducibility scores

Score	Definition
0	Impossibility of repetition, only in complex cases and situations.
1	Difficult to repeat, requires a long time to repeat.
2	Repetition at specific times, requires a short time to repeat.
3	Can be executed at any time without restrictions.

- **Exploitability**: An assessment of the effort and expertise required to launch a successful attack. A threat for cyberattack that requires highly skilled employees and is expensive to implement is less exploitable.

Table 3: Definition for Exploitability scores

Score	Definition
0	Impossible to exploit.
1	Requires a physical attack, strong network and programming skills, or advanced tools.
2	Requires a skilled programmer, related technical knowledge, or medium-developed tools.
3	A beginner programmer, easy to implement, simple tools such as NFC tools.

When evaluating exploitability, it is important to consider the location and position of potential attackers. A threat that can be exploited by a remote or unknown attacker is more dangerous than a threat that requires a licensed and trusted user.

- **Affected Users:** A category for assessing the severity of the threat by identifying how many users could be affected in a successful cyberattack due to this threat or vulnerability. A threat that will affect single patient will have a low risk assessment score in this category. As for attacks that disrupt the doctor's dashboard, which affecting dozens of patients, such as some denial-of-service attacks, the risk assessment score is higher than that.

Table 4: Definition for Affected Users scores

Score	Definition
0	No one.
1	Only one patient/user.
2	A simple number of patients/users, administrative users.
3	All users, all patients.

- **Detectability:** The likelihood that a vulnerability or threat will be discovered and exploited. Detectability is difficult to estimate accurately. The safest approach is to assume that any vulnerability will eventually be exploited, and then rely on other measures to determine the relative score of the threat. Therefore, many security experts have preferred to move to a modern scale called DREAD-D (meaning DREAD minus D), which excludes detectability and always assumes that detectability is at the maximum evaluation rating (3), especially if the threat is detected by threat modeling tools, and thus relying on the other criteria to determine the overall severity rating of the threat.

Table 5: Definition for Detectability scores

Score	Definition
3	Threat that can be detected by threat modeling tools.

The DREAD model is a simple and effective way to assess the severity of threats to CMD. By assigning a score to each criterion, the model can help designers and engineers to prioritize their mitigation efforts and focus on the most significant and serious threats.

4- Results and Discussion

4.1- CPO Results

After properly and fully connecting the components of the CPO device, we obtained these results, which are displayed through the Blynk application installed on the mobile phone or via the Blynk platform's website.

International Journal for Scientific Research, London Vol (3), No (5), 2024
https://doi.org/10.59992/IJSR.2024.v3n5p10 E-ISSN 2755-3418

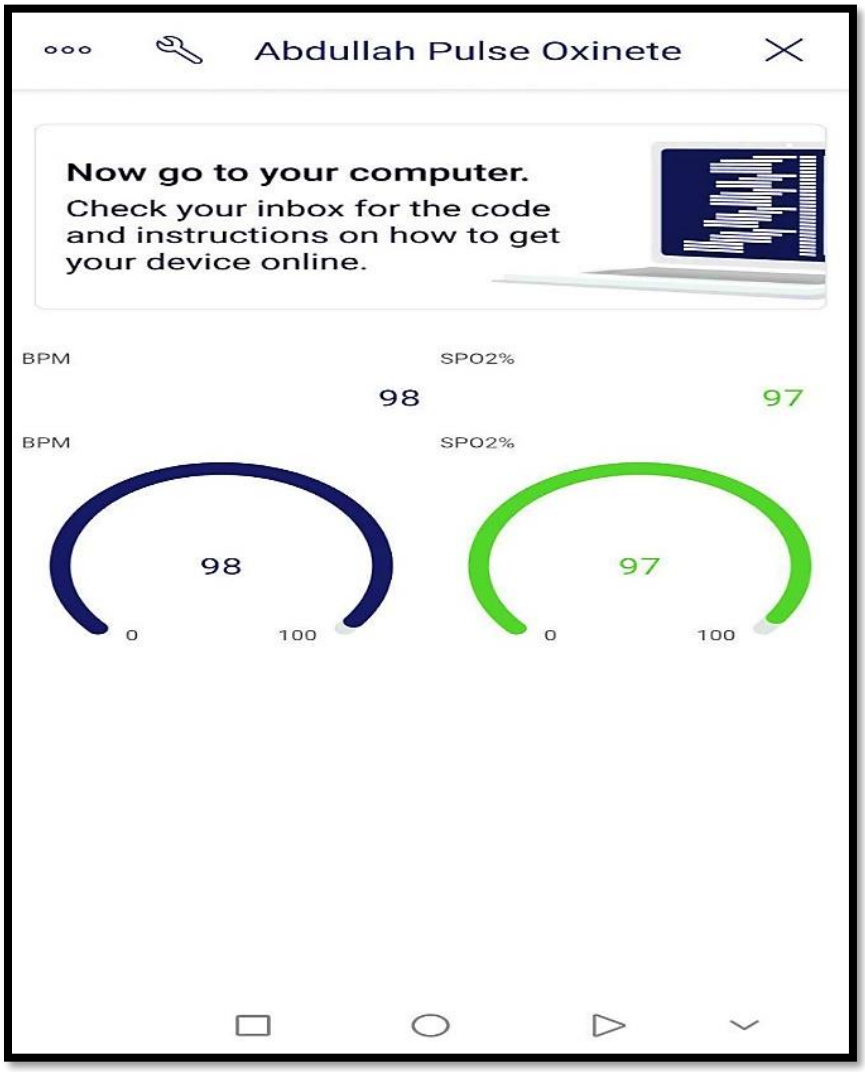


Figure 3: Health measurements from the BLYNK mobile application

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (5) May 2024 الإصدار (3)، العدد (5)

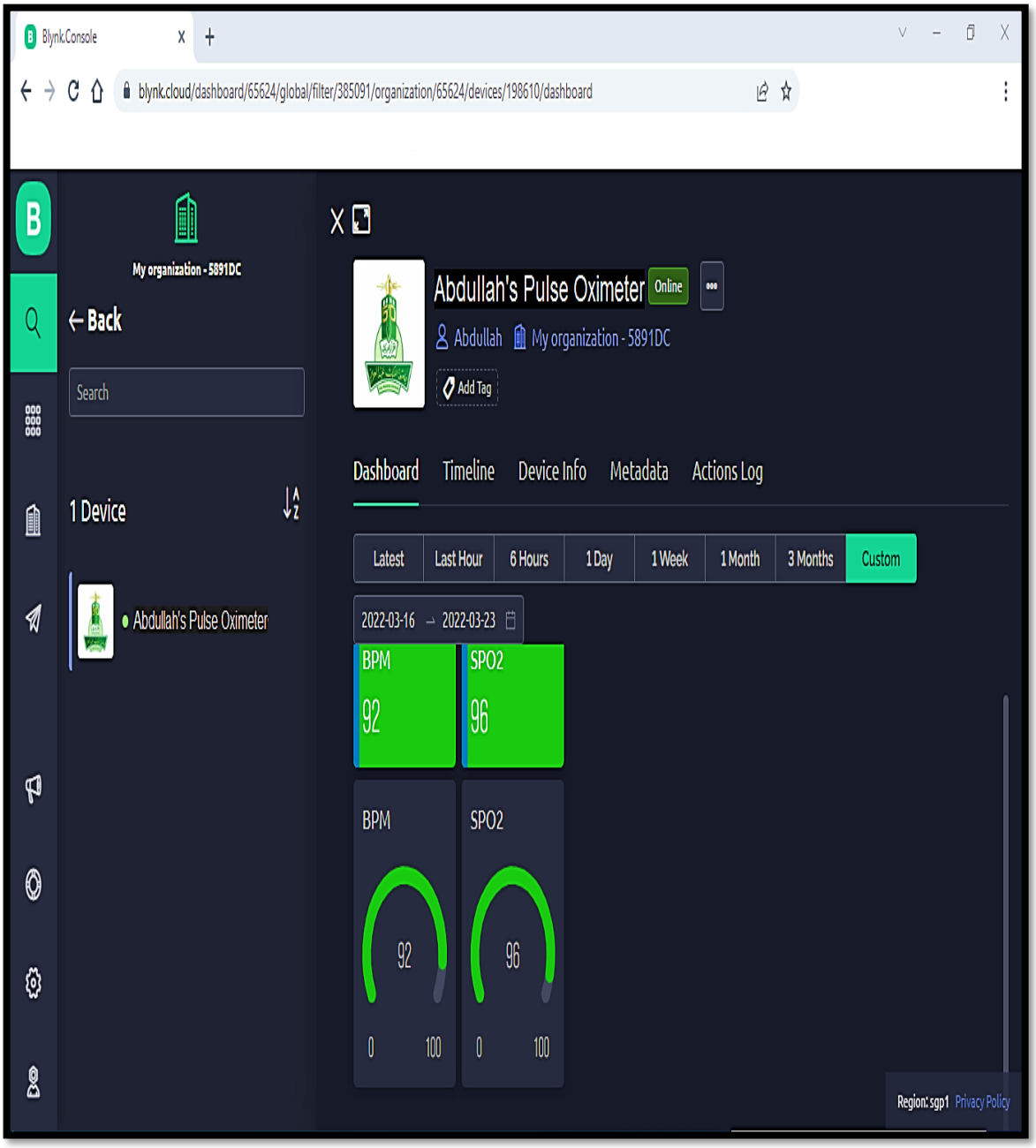


Figure 4: Health measurements from the BLYNK platform website

Now, we have confirmed that the connected medical device is working, the components work together effectively and harmoniously and we are able to implement the steps of the threat modeling tool. This will allow us to verify the tool's effectiveness and ensure that it can provide accurate and reliable results. In addition, we will be able to confirm that the results of this tool can be used as a reliable and informative resource for identifying potential threats to a specific CMD and assessing its security posture against cybersecurity attacks.

4.2- Threat Modeling Results

A graphical representation of the data flow diagram was created using Microsoft Threat Modeling tool for the CPO device, and it was as follows:

Health measurements are obtained from a wearable sensor device (MAX30100) on the patient's body, then transmits the data to a NodeMCU (ESP8622). The microcontroller receives the sensor data, processes it, and displays it on an OLED screen connected to the microcontroller via wires inside the isolation room, allowing the patient and his family members to see the health measurements. Additionally, the health measurements are sent via Wi-Fi to the BLYNK platform.

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (5) May 2024 الإصدار (3)، العدد (5)

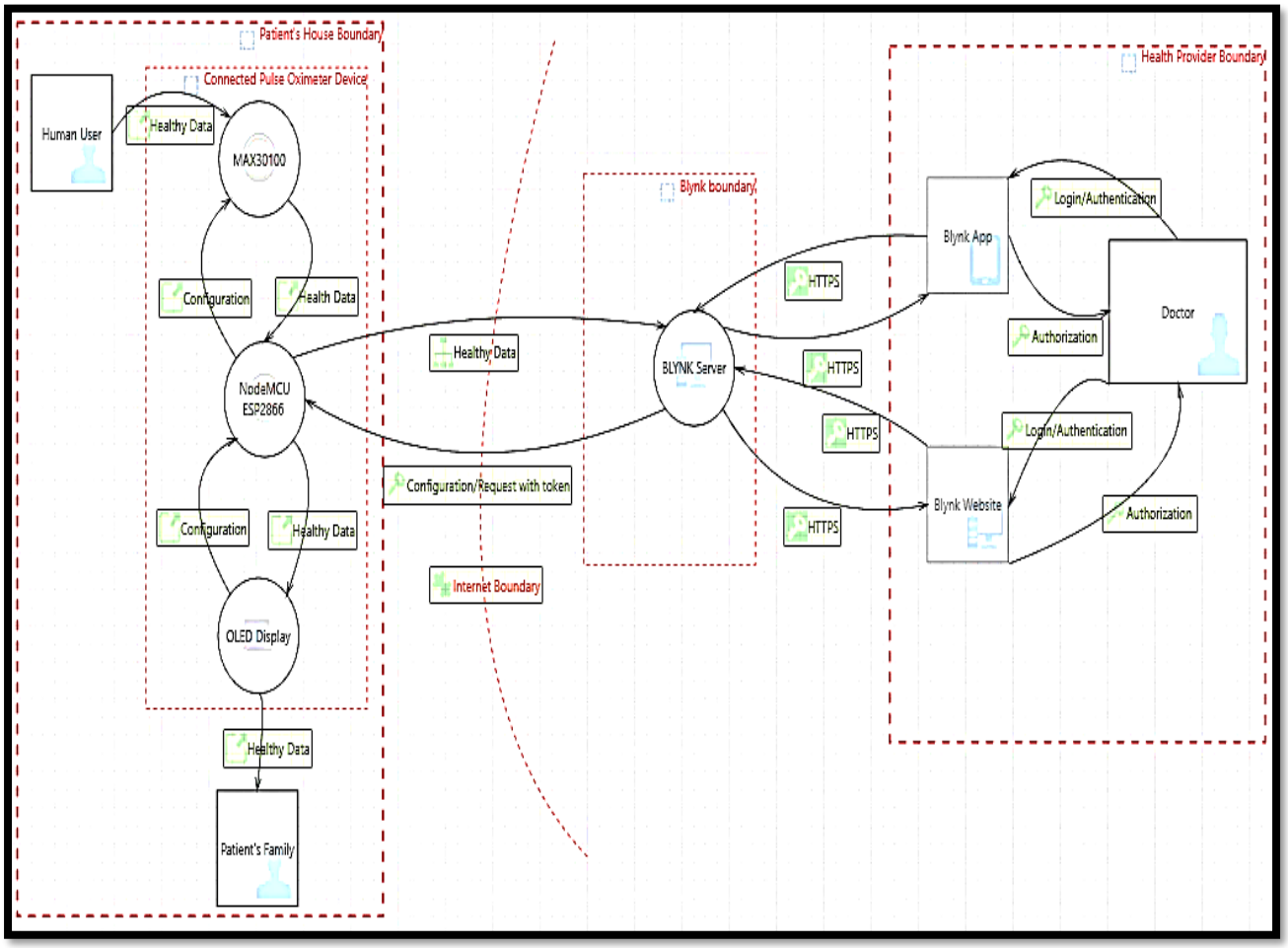
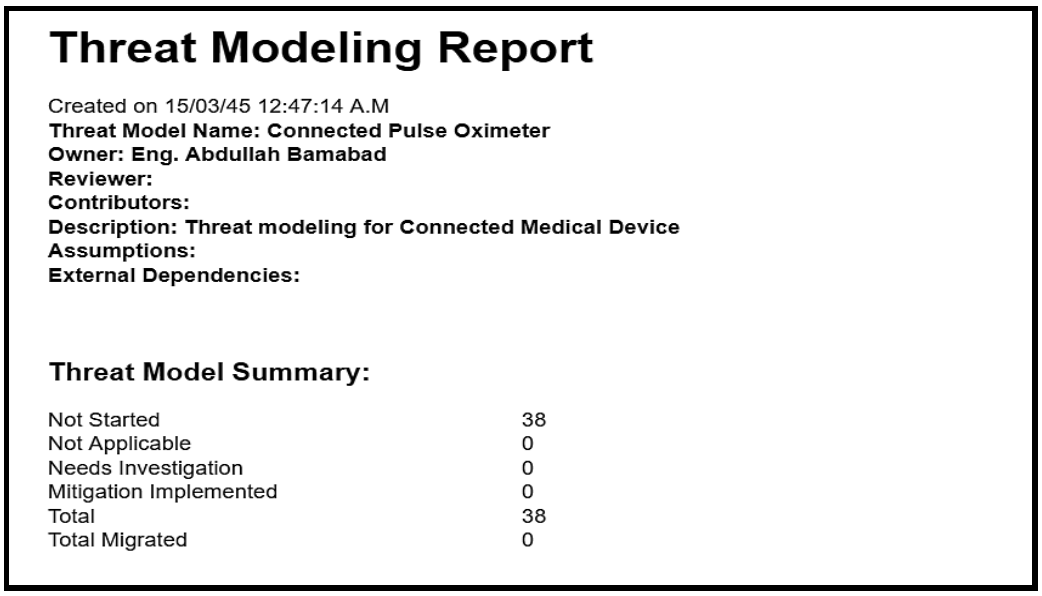


Figure 5: Data flow diagram for the CPO device

The platform verifies the reliability of the MCU (ESP8266) first and then receives the health measurements and stores them in the healthcare provider's profile timeline. The platform acts as a third-party intermediary between the patient and the healthcare provider (represented by the doctor). The doctor can monitor the patient's health measurements directly through the platform's website or by installing the BLYNK application on Android or iOS mobiles. The BLYNK platform requests the doctor to

log in to the website or mobile application using his email and password that are registered and trusted on the platform's server.



Threat Modeling Report

Created on 15/03/45 12:47:14 A.M
Threat Model Name: Connected Pulse Oximeter
Owner: Eng. Abdullah Bamabad
Reviewer:
Contributors:
Description: Threat modeling for Connected Medical Device
Assumptions:
External Dependencies:

Threat Model Summary:

Not Started	38
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	38
Total Migrated	0

Figure 6: The cover page of the CPO threat modeling report

In this CMD, the BLYNK platform is primarily used, relying on it as a trusted third party that supports the Public Key Infrastructure (PKI) framework.

After creating and explaining the graphical representation of the data flows using the threat modeling tool, we can create a comprehensive report with just a single click. This report, produced by the Microsoft Threat Modeling tool too, provides a detailed overview of all vulnerabilities found within the data flow diagram of the CPO device design, as well as all the potential threats associated with them.

In this research, seven weakness areas in the design of our CPO model were identified, as shown in the following image:

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (5) May 2024 الإصدار (3)، العدد (5)

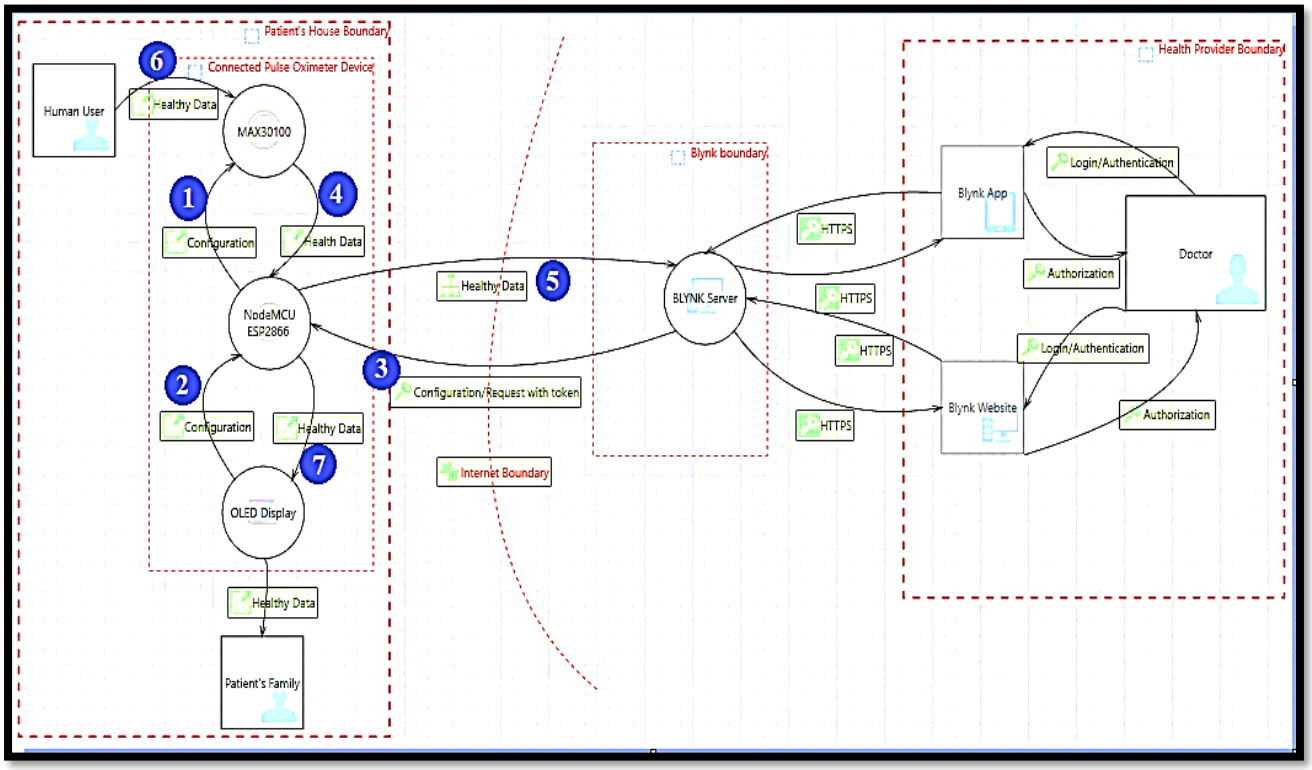


Figure 7: Weakness points for the CPO device

After identifying the vulnerabilities in our device, we notice that each vulnerability is susceptible to various types of threats. We can identify and classify the types of threats that may occur at each vulnerability by using the STRIDE model, which is applied by Microsoft Threat Modeling tool.

Regarding the fourth step of the threat modeling process, which is to evaluate the risks of each type of detected threat and ensure that the mitigation tools and procedures applied to them are effective in mitigating the severity of the threats through the DREAD model, the following tables present the results of the evaluation of the threats that were discovered using the threat modeling tool, where each type

of STRIDE threat was evaluated separately using the DREAD model, then the mean severity score for each type of threat was calculated.

Spoof Vs DREAD

Table (7) shows the severity of tampering threats using the DREAD model. We observe that 10 potential threats of this type have been discovered. Although there are 4 possibilities for different tampering threats on the same component or element, which is the ESP2866MCU, we note that the severity levels of tampering vary between low and medium.

Table 6: severity score of tampering threats

Region No.	Threat	D	R	E	A	D	severity score
1	4. Tampering with MAX30100 configuration	3	0	0	1	3	7
1	5. Tampering with NodeMCU ESP2866 configuration	0	1	1	1	3	6
2	9. Tampering with NodeMCU ESP2866 configuration	1	1	1	1	3	7
3	16. Tampering with NodeMCU ESP2866 configuration	0	0	0	1	3	4
4	18. Tampering with MAX30100 configuration	0	0	0	1	3	4
4	19. Tampering with NodeMCU ESP2866 configuration	3	0	1	1	3	8
5	31. Tampering with NodeMCU ESP2866 configuration	1	1	1	1	3	7
5	37. Healthy Data Tampering	1	1	1	1	3	7
6	44. Tampering with MAX30100 configuration	3	1	1	1	3	9
7	46. Tampering with NodeMCU ESP2866 configuration	1	1	1	1	3	7
	Average of all tampering threats						6.6=7

The reason for this is that the severity level of a tampering threat is determined by the vulnerability area that is affected by the potential attack. Each vulnerability area has a different severity level, which in turn affects the final severity assessment.

Repudiation Vs DREAD

Table (8) shows the severity of repudiation threats using the DREAD model. We note that 8 potential threats of this type have been discovered. All threats were at a low or medium severity level.

Table 7: severity score of repudiation threats

Region No	Threat	D	R	E	A	D	severity score
1	2. MAX30100 - Repudiation	0	0	0	1	3	4
2	7. NodeMCU ESP2866 - Repudiation	0	0	0	1	3	4
3	13. NodeMCU ESP2866 - Repudiation	2	0	0	1	3	6
4	21. NodeMCU ESP2866 - Repudiation	2	0	0	1	3	6
5	28. NodeMCU ESP2866 - Outgoing Auditing	0	0	0	1	3	4
5	29. Potential Data Repudiation by BLYNK Serve	0	0	0	1	3	4
6	41. MAX30100 - Repudiation	3	1	1	1	3	9
7	47. OLED Display - Repudiation	1	0	0	1	3	5
	Average of all repudiation threats						5.25=5

Information Disclosure Vs DREAD

All three potential information disclosure threats, as shown in Table (9), have been rated as low severity in different vulnerability areas. This indicates that information disclosure threats do not pose a risk to our CPO.

Table 8: severity score of information disclosure threats

Region No.	Threat	D	R	E	A	D	severity score
5	27. Physical theft of component communicating via Healthy Data	2	0	1	1	3	7
5	33. Healthy Data Information Disclosure	0	0	0	1	3	4
7	48. OLED Display Usage in Public Spaces	0	0	1	1	3	5
	Average of all information disclosure threats						5.7 = 6

Denial of Service Vs DREAD

Table (10) shows the severity of denial-of-service threats using the DREAD model. We observe that there are four potential threats of this type. Two of these threats were rated as low severity and two of them were rated as medium severity. The severity level of a denial-of-service threat is determined by the number of affected users.

Table 9: severity score of denial-of-service threats

Region No.	Threat	D	R	E	A	D	severity score
3	12. Wireless Connection via Configuration/Request with token to NodeMCU ESP2866	1	1	1	3	3	9
5	24. Wireless Connection via Healthy Data to BLYNK Server	1	0	0	2	3	6
5	25. Data Flow Healthy Data Is Potentially Interrupted	1	0	0	1	3	5
5	26. Potential Process Crash or Stop for BLYNK Server	1	1	1	2	3	8
	Average of all denial-of-service threats						7

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (5) May 2024 الإصدار (3)، العدد (5)

Elevation of privilege Vs DREAD

There are 10 potential elevation of privileges threats for our CPO, as shown in Table (11). The distinctive feature of this type of threat is that the assessment of all of these threats is at the lowest assessment level of (4), with the exception of one potential threat that got an assessment of (5), which is also considered low. The average severity rating of this type of threat is around 4, which means that this type has been well mitigated; because we have implemented a number of security measures to mitigate the risk of these attacks, such as strong passwords and encryption, implement role-based access control (RBAC) to restrict users' access, and use multi-factor authentication (MFA) to require users to provide multiple forms of authentication before accessing to the device. However, the severity level of this threat must be maintained.

Table 10: severity score of elevation of privilege threats

Region No.	Threat	D	R	E	A	D	severity score
1	1. Non-production modes for MAX30100	0	0	0	1	3	4
2	6. Non-production modes for NodeMCU ESP2866 NodeMCU	0	0	0	1	3	4
3	10. Trusted Wireless Connection via Configuration/Request with token to NodeMCU ESP2866	0	0	1	1	3	5
4	11. Non-production modes for NodeMCU ESP2866	0	0	0	1	3	4
5	22. Non-production modes for NodeMCU ESP2866	0	0	0	1	3	4
6	23. BLYNK Server May be Subject to Elevation of Privilege Using Remote Code Execution	0	0	0	1	3	4
7	34. Elevation by Changing the Execution Flow in BLYNK Server	0	0	0	1	3	4
8	35. Trusted Wireless Connection via Healthy Data to BLYNK Server	0	0	0	1	3	4
9	40. Non-production modes for MAX30100	0	0	0	1	3	4
10	49. Non-production modes for OLED Display	0	0	0	1	3	4
	Average of all elevation of privilege threats						4.2=4

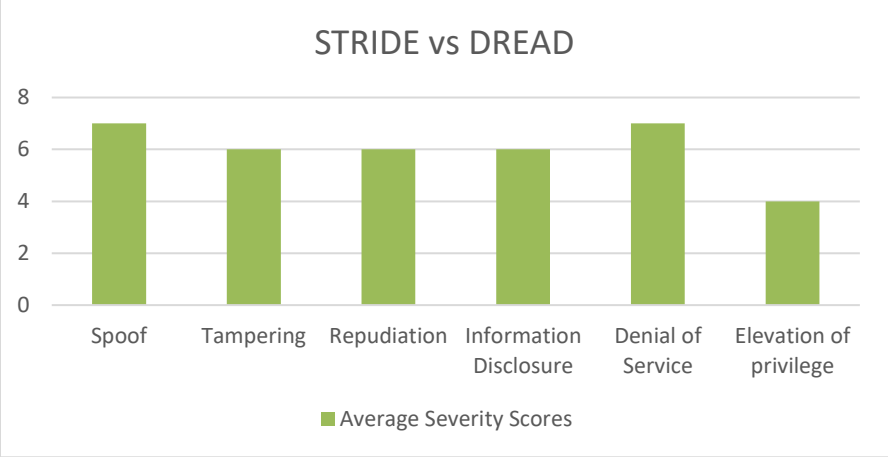


Figure 8: Average Severity Scores for all types of potential threats

Based on the previous results of measuring the severity of threats, we believe that it is not enough to rely only on the average severity of threats in general. Rather, all potential threats for all types of threats that have been discovered for each component and for all stages of sending and receiving data must be evaluated. We have noticed that threat modeling tools such as STRIDE model and DREAD model do these tasks effectively and distinctively, with logical results. This makes us feel comfortable recommending the CMD's manufacturers to use STRIDE model to detect potential threats of their devices and then use the DREAD model to assess these risks.

By comparing our threat modeling method and our results with another threat modeling method in the research paper, "Medical Device Safety Management Using Cybersecurity Risk Analysis," [11] in which the researchers applied a different threat modeling method (later referred to as Method B) on the same type of our connected device (Pulse Oximeter). Our method was compared with Method B with regard to the concepts, steps, difficulty of implementation and results, and we arrived at some points, which are as follows:

First: In our method, the tool was tested with specific components of the pulse oximeter and with known security properties for each component. While in Method B, the tool was tested with the general components of the pulse oximeter (see Fig 13) and without knowing the security properties of each component.

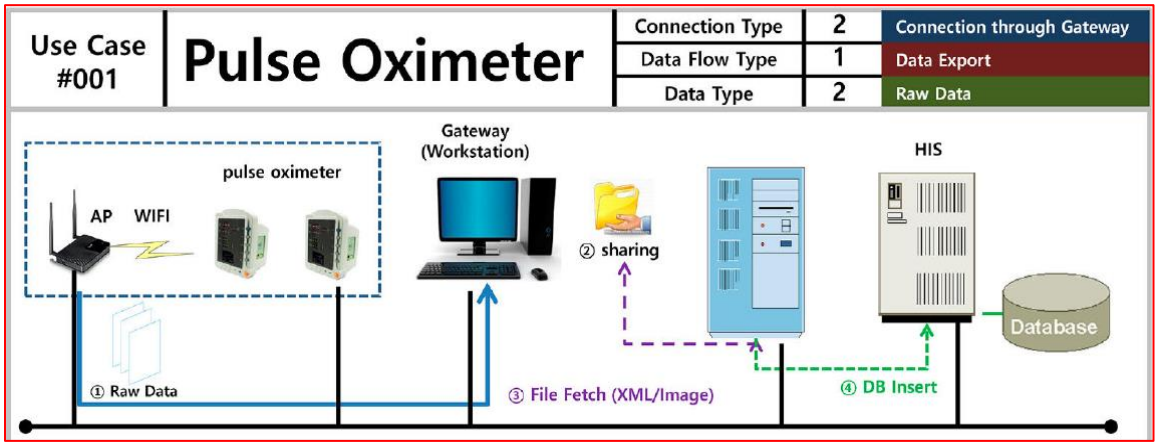


Figure 9: CPO components for Method B [11]

Second: Our method can be applied by anyone with minimal experience in the field of cybersecurity. But the researchers mentioned that the B method requires high-level experts in cybersecurity to implement it and obtain correct results [11].

Third: The results change significantly in Method B if it is applied by different cybersecurity experts based on their experiences. While in our method, it is not expected that the results will differ if applied by different cybersecurity experts because they are not needed in the first place and because the results depend on the values of the average level of risk against cyberattacks.

Fourth: It is easy for the FDA to rely on the results of our method to decide whether to issue a sale and use license for CMDs or not, because the results and steps that were applied to obtain them are consistent and more realistic. While in Method B it is difficult to rely on the result because it is not always the same among experts

Fifth: One of the most important features of our method is that the steps of our method can be integrated into the life cycle of cybersecurity development for CMDs, but in Method B, all steps must be re-executed from the beginning if any modification or development occurs in the components of the CMDs.

5- Conclusion and Future Work

Healthcare providers and patients are often considered the weakest link in the security chain due to their lack of awareness and experience in the safe and correct use of the CMDs. It must be taken into account that the use of IoT technology in medical devices requires strict controls, because medical devices connected to the Internet are at risk of cyber-attacks. This is because it contains codes and software components that can be hacked and controlled remotely, causing harm to the patient that may lead to death, and then the medical device loses its purpose. The process of adopting a specific system or threat model that can be used by non-security professionals to evaluate the security of CMD against cyber-attacks requires certain controls in order for its results to be approved by the FDA, such that this methodology is applicable to most types of CMDs and repeatable throughout the CMDs life cycle with realistic results. These controls can be achieved through a threat modeling tool that detects all potential threats to the connected medical device and the mitigation methods used to reduce or completely eliminate the severity of these threats, and then assess the severity level of these threats after applying the mitigation tools on it. After completing the CMD threat modeling, we are ready to analyze the results of the severity assessment of the detected threats and then develop special instructions and recommendations to mitigate their severity so that the device is always maintained at the lowest acceptable risk level.

Security is a sequential and interconnected process, where each mitigation and protection tool relies on those before it to defend against cyberattacks. There are many threat models that evaluate CMD security against cyberattacks such as PASTA

or OCTAVE, but they may need highly experienced professionals or powerful equipment such as penetration testing machines with advanced software and tools. We chose DREAD and STRIDE over OCTAVE or similar models, because of their capability to help any developer or biomedical engineer to analyze the internal design of CMD components, detect potential security threats, and manage the process of assessing and mitigating security risks at an early stage, which is one of the most important advantages of our threat modeling method.

The proposed threat model was applied to a CPO device and detected 38 potential threats, which were divided into 6 threat types using the STRIDE model: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. The severity of all these threats was then assessed individually, and the average severity of each type was evaluated through the DREAD model categories after taking into account the mitigation tools used in the device. The threat modeling tool showed satisfactory and realistic results, which we were able to determine that the severity level of using the CPO device is low and it is valid for use. We also compared our method of threat modeling with another method of threat modeling, as our method proved the ease of application and its feasibility in obtaining more realistic results, in addition to the ease of adding it to the security development life cycle of CMDs and ensuring the ability of CMDs to confront cyber threats and reduce their seriousness and effects or mitigate them. The tool also helped us identify instructions and recommendations that all stakeholders should be implement to maintain the security of their CMD against cyber-attacks.

Based on our results in testing the threat modeling tool on the CPO, we have proven that companies developing CMDs can apply this tool on their devices through their developers. Also, we advocate for the integration of threat modeling tool training into the curricula of biomedical engineering programs and within internal training initiatives of CMD manufacturers. This strategic intervention would equip future

engineers with the knowledge and skills needed to design CMDs that are more secure against cyber-security threats. Consequently, the SFDA would be able to expedite the licensing prosses for these medical devices, facilitating their wider adoption by healthcare providers. This broadened access to CMDs would enhance the capacity of healthcare providers, allowing a greater number of patients to be treated. Ultimately, this initiative would positively impact the quality and well-being of patients who rely on these critical medical devices.

In our future work, we will also verify the applicability of the STRIDE and DREAD threat modeling to other more CMDs such as insulin pumps or pacemakers.

References

[1] M. N. Alam , B. Kaur and M. S. Kabir, "Tracing the Historical Progression and Analyzing the Broader Implications of IoT: Opportunities and Challenges with Two Case Studies," *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)*, vol. 12, no. 04, April 2023.

[2] T. TSENG, T. C. Wu and F. Lai, "Threat analysis for wearable health devices and environment monitoring internet of things integration system," *IEEE Access*, vol. 7, p. 144983–144994, 2019.

[3] V. Vakhter, B. Soysal, P. Schaumont and U. Guler , "Security for Emerging Miniaturized Wireless Biomedical Devices: Threat modeling with Applications to Case Studies," *IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS,* 2020.

[4] M. Ghazal, "Piracy of wearable and implanted medical devices," *International Arab Journal of Information,* vol. 5, no. 9, 2017.

[5] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health," *International Journal for Quality in Health Care,* vol. 133, no. 1, 2020.

[6] S. Anderson and T. Williams, "Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?," *Computer Standards & Interfaces,* vol. 56, pp. 134-143, February 2018.

[7] M. Siddiqi and A. Tsintzira, "Adding Security to Implantable Medical Devices: Can We Afford It," *Association for Computing Machinery,* 28 April 2021.

[8] Lechner, N. Hrgarek, Z. Stapić and V. Strahonja, "Threat modeling methods in the medical device industry: An integrative literature review," *Central European Conference on Information and Intelligent Systems. Faculty of Organization and Informatics Varazdin,* 2022.

[9] M. Cagnazzo, M. Hertlein, T. Holz and N. Pohlmann, "Threat modeling for Mobile Health Systems,"

IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2018.

[10] A. Omotosho, B. A. Haruna and O. M. Olaniyi , "Threat Modeling of Internet of Things Health Devices," *Journal of Applied Security Research.*, 2019.

[11] D.-w. Kim, J.-y. Choi and K.-h. Han2, "Medical Device Safety Management Using Cybersecurity Risk Analysis," *IEEE Access*, 2022.

[12] "Saudi Food and Drug Administration," 2019. [Online]. Available: https://www.sfda.gov.sa/sites/default/files/2020-03/MDS-G36.pdf..

[13] P. Williams and A. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices: Evidence and Research*, 2015.

[14] D. Revar, H. Nayak and D. Jhalac, "Design and Implementation of Pulse oximeter to monitor and predict Patient's health," *Compliance Engineering Journal*, p. 18, 2020.

[15] A. Onubeze, "Developing a Wireless Heart Rate Monitor with MAX30100 and nRF51822," *theseus*, p. 42, 2016.

[16] Y. S. Parihar, "Internet of Things and Nodemcu: A review of use of Nodemcu ESP8266 in IoT products," *Journal of Emerging Technologies and Innovative Research*, p. 4, 2019.

[17] "Blynk Platform Security," Blynk, [Online]. Available: https://docs.blynk.io/en/blynk.cloud/security.

[18] S. Sarkar, A. Ghosh, M. Chakraborty and A. Mondal, "Design, Hardware Implementation of a Domestic Pulse Oximeter Using IOT for COVID – 19 Patient," *International Journal of Microsystems and IoT*, p. 8, 2023.

[19] A. Shostack, "Experiences Threat Modeling at Microsoft," p. 11.