This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

Threat Modeling and Risk Analysis for Miniaturized Wireless Biomedical Devices

Vladimir Vakhter, *Member, IEEE*, Betul Soysal, *Member, IEEE*, Patrick Schaumont, *Senior Member, IEEE*, and Ulkuhan Guler, *Senior Member, IEEE*

***Abstract*— The landscape of miniaturized wireless biomedical devices (MWBDs), including various injectables, ingestibles, implantables, and wearables, is rapidly expanding as proactive mobile healthcare proliferates. While the growth of MWBDs increases the flexibility of medical services, the adoption of these technologies poses privacy and security risks to their users. As a result, while being restricted in resources (size, power, processing, and storage), these devices require trust and must be at least minimally secure in the face of evolving threats. Making MWBDs secure begins with threat modeling. Therefore, this research reviews and summarizes the information on threat modeling applicable to MWBDs. Then, we propose a domain-specific qualitative-quantitative threat model that aims to help the designers and manufacturers of MWBDs to identify threats and embed security in their designs in the pre-market phase of the lifecycle of an MWBD. This model is tailored to a wide range of MWBDs. Among the different stakeholders, this model focuses on the user. It also prioritizes non-invasive direct attacks against telemetry interfaces. To discuss the advantages and disadvantages of the proposed model, it is compared to some other threat models. To illustrate how the model can be adopted by a threat-modeling team, it is then applied to representative case studies from each category of MWBDs. The outcomes of the performed risk analysis reveal that the model is easy to apply and sufficient to disclose threats.**

***Index Terms*—Security, privacy, threat modeling, risk assessment, miniaturized wireless biomedical devices, injectables, implantables, ingestibles, wearables, the Internet of Things (IoT).**

I. Introduction

Rising interest in remote health monitoring and treatment stimulates an increase in the variety and the volume of miniaturized wireless biomedical devices (MWBDs) [1]–[4]. The need for these smart-and-connected health technologies is foreseen to continue rising globally as their share in the reduction of healthcare costs grows [5]. Being convenient, low-cost, and easy-access, MWBDs support a transition from traditional reactive medicine to the proactive, personalized precision healthcare model [6], [7]. There has been a raise in interactive communication between patients and healthcare providers with the help of remote monitoring devices, including MWBDs, especially after the global crisis of the public health system caused by the COVID-19 pandemic [8], [9]. This trend is expected to create even more demand for MWBDs among patients and healthcare providers [10], [11].

V. Vakhter, P. Schaumont, and U. Guler are with the Electrical and Computer Engineering Department, Worcester Polytechnic Institute, 100 Institute Rd., Worcester, MA 01609, USA (e-mail: {vvvakhter, pschaumont, uguler}@wpi.edu).

B. Soysal is a security software engineer, 1600 Amphitheatre Pkwy, Mountain View, CA 94043 (e-mail: betuls@ieee.org).

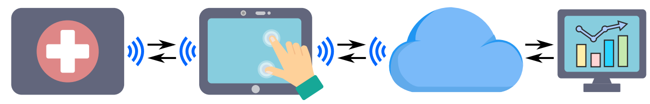

Fig. 1: A typical biomedical system. Adapted from [20].

While novel designs are regularly presented, more applications and use scenarios are envisioned for MWBDs. Therefore, they are still considered emerging devices. MWBDs may be divided into four main categories: (1) injectables, injected underneath the human tissue; (2) implantables, implanted into the human body during a surgery; (3) ingestibles, ingested by the patient in the form of a regular pill; and (4) wearables, worn on the human body.

MWBDs are capable of collecting and transmitting sensitive, private information, like bio-electrical activity [12], [13] and vital signs [14], [15], and affecting the human body through stimulation [16], [17] and drug delivery [18], [19]. Therefore, while being convenient, they produce privacy and security risks for their users [20]–[23]. Traditionally, designers and manufacturers of MWBDs tend to prioritize functionality and user experience over security [21]–[23]. As a result, protection mechanisms are missing at the architectural level for most of MWBDs [13]–[19]. Multiple attacks for the misuse of sensitive medical information and the malfunctioning of MWBDs may be implemented, for example, forging, alternating, or replaying previously captured messages, depleting the battery, or unauthorized reprogramming [24]. Professionals are now tasked with defeating well-funded attacks that, in some cases, can cause immediate physical harm for the user. For instance, the first security issues with pacemakers were identified over a decade ago [25]. Nevertheless, additional hacks on pacemaker devices were announced as of 2018 [26]–[28], indicating that the problem is far from being resolved. Another example is the malicious use of an insulin pump that could cause hypoglycemia for its user [22]. Attackers may also be attracted by the assets belonging to other primary stakeholders of MWBDs, as described in Table I.

To formulate security objectives efficiently, it is necessary to have a perspective on the whole system. A typical next-generation biomedical system, outlined in Fig. 1, consists of an MWBD wirelessly connected to an external controller. An MWBD usually has limited functionality: (1) it may serve as a controllable actuator, capable of processing a small set of external instructions from the controller; or (2) it can operate as a smart sensor, which transmits the collected medical data to the controller. The controller typically acts as a gateway and transfers the user health-related data to a cloud service

TABLE I
Examples of Potential Risks for Stakeholders of MWBDs

Stakeholder	Potential Risk
User	(1) The corruption of medical data may lead to wrong diagnoses, and therefore wrong therapies. (2) Privacy leakage may result in stolen identities and electronic fraud. (3) Denial of service (DoS) may harm the patient or even cause their death.
Manufacturer	(1) The leakage of intellectual property (IP) may be used by competitors to increase their market share. (2) The leakage of IP may also lead to an increase in the number of counterfeits and attacks. (3) If an attack harms the patient, it may damage the manufacturer's reputation. (4) Additionally, lawsuits may be filed against the manufacturer.
Hospital	If hospitals deal with corrupted MWBDs or counterfeits, they could (1) lose their professional reputation and trust, (2) be involved in lawsuits, or (3) lose their accreditation.

for post-processing. The data processed in the cloud is then sent to a dashboard for the authorized users [20]. The current biomedical systems implement protection mechanisms mainly beginning from the gateway [29]. The lack of security in the MWBD puts the whole system in danger. Therefore, security should be built into MWBDs to protect their users [30].

The MWBDs in the scope of this work typically have at least one network interface (wireless telemetry) and at least one transducer (sensor or actuator). These capabilities allow categorizing MWBDs as the Internet of Things (IoT) devices [7]. The National Institute of Standards and Technology (NIST) maintains a cybersecurity program dedicated to IoT [31], reflecting the high demand for security for these devices. Some NIST standards applicable to MWBDs include NISTIR8200 [7], NISTIR8228 [32], NISTIR8259 [4], and NISTIR8259A [33]. The developers of MWBDs should also be aware of the drafts from NIST [34]–[37], which will eventually be turned into standards.

A. Motivation

While the manufacturers and designers of MWBDs may often not have direct experience with cybersecurity-related technologies [36], implementing these mechanisms is of high importance and must be systematic. Accordingly, a standardized approach to profile potential attackers and to catalog potential threats is needed for the diverse architectures of emerging MWBDs, as the US Food and Drug Administration (FDA) announced recently [38]. The process of understanding, documenting, and evaluating system vulnerabilities, followed by addressing the protective measures, is known as threat modeling [39]. Threat modeling can play a critical role in addressing the weaknesses of a system against specific adversary scenarios, especially when conducted in the early stages of the device lifecycle [40]. This work proposes a methodology for modeling and semi-quantitatively assessing potential threats for the next-generation MWBDs.

B. Contributions

The contributions of this work are summarized as follows:

1) We proposed a novel qualitative-quantitative threat modeling and risk assessment methodology designed specifically for next-generation MWBDs. The proposed framework analyzes these devices at the architectural level and considers their constraints. We examined the recent literature on IoT devices and available threat modeling and risk assessment for MWBDs and did not find concrete competitors.
2) We applied our risk assessment methodology to representative case studies from each category of MWBDs to illustrate how it can be adopted by a threat-modeling team.
3) We performed an extensive literature review on threat modeling procedures applicable to MWBDs. Furthermore, we summarized the relevant information to educate and assist medical device designers in integrating threat modeling into their design and manufacturing processes.
4) We discussed various security challenges for emerging MWBDs to raise awareness about associated risks among the key stakeholders and stimulate interest in proactive risk mitigation.

C. Organization of the Paper

The remainder of this publication is organized as follows. Section II provides the background on the security challenges in MWBDs. Section III presents some general considerations for the threat modeling process. In Section IV we review some existing threat modeling frameworks. Section V describes the proposed threat model for MWBDs. Section VI compares the proposed model with some existing threat models. Section VII presents an application of the proposed model to real case studies of the four primary categories of MWBDs. Section VIII discusses the results and makes suggestions for future work. Section IX concludes the work.

II. Security Challenges for Emerging MWBDs

This section discusses various security challenges for emerging MWBDs. Some of these challenges have already been detected and require immediate attention. Other challenges are only anticipated in the future. However, both of these categories of challenges illustrate the importance of security for MWBDs.

A. Limited Resources

Multiple designs of emerging MWBDs are known to have reduced area, weight, power, storage, network interfaces, and computing resources [30]. Therefore, they stand apart from classical IT devices (for example, smartphones, servers, or laptops), which have been used to define device cybersecurity capabilities [4]. The limited resources available to MWBDs constrain the range of security mechanisms applicable to these devices. Such as, the limited area excludes the integration of complex security units occupying a lot of silicone on the chip. Constraints on power exclude complex cryptographic computations and reduces the bandwidth and range of communications. Memory and performance limitations prevent the use of sophisticated cryptographic algorithms [24]. Therefore, even though multiple modern cryptographic algorithms are reliable, the simplicity of MWBDs makes them unavailable for these devices [4]. Correspondingly, lightweight cryptographic algorithms, suitable for constrained environments, need to be developed and standardized [24], [41], [42].

B. Multiple Attack Channels

There are two primary ways to access an MWBD. It may be accessed physically or wirelessly. For these two types of access, there are multiple underlying interfaces. MWBDs are often equipped with diverse transducers (sensors and actuators) and employ various wireless communication and power delivery schemes. All these interfaces may be considered as potential channels which can be used by an intruder to maliciously interact with the device [43]. For a typical MWBD, five such channels may be identified. Three input channels include the control channel, the sensing channel, and the power delivering channel. Two output channels include the user data transferring channel and the actuating channel. Apart from the attacks on these five external interfaces, additional internal attacks include the ones on the memory and on the digital hardware. An attacker model covering mentioned channels was presented in [44].

C. Patient's Safety

Given the limited resources and multiple attack channels, MWBDs should employ protective schemes that would not endanger a patient's life in an emergency [24]. Therefore, while these devices require server-side authentication to ensure that commands are authorized, critical care services must be able to access the device even when the normal authentication method is unavailable. Hence, including the patient in authentication schemes, such as that proposed in [45], is potentially dangerous. Also, a direct disregarding of authentication and authorization in an emergency might introduce many potential threats. Because of that, authentication in medical devices remains an open problem [24].

In general, for MWBDs, security and privacy requirements of a device should not affect its safety, reliability, and resilience [32]. Traditional IT security prioritizes confidentiality, integrity, and availability. The ability of MWBDs to interact with the physical world through sensors and actuators requires addressing threats to patients and their environments. Depending on the functionality of a particular biomedical device and its vital necessity for the patient, availability or integrity may be the highest priority, followed by privacy and finally confidentiality [7].

D. Distributed Supply Chain

The manufacturing of MWBDs relies on a complex and distributed supply chain. This chain includes multiple entities, distribution channels, technologies, and different laws and practices. This multifariousness affects the design, fabrication, distribution, deployment, usage, and maintenance of MWBDs. Therefore, whether intentionally or unintentionally, the final users of MWBDs are at risk of supply chain attacks. Supply chain risks for MWBDs may include the insertion of malicious logic blocks, the use of unauthorized components and counterfeits, tampering, poor manufacturing and design practices, etc [46]. Component suppliers often have poor cyber hygiene, and these vulnerabilities are more of an issue than the ingenuity of the attackers [47].

E. Lack of Incentives

There is a lack of incentives to build security and privacy into IoT devices. Cybersecurity has been often an afterthought to getting to market, with price and features prioritized. There is also a general lack of consumer education, leading to a lack of demand for better cybersecurity and privacy. There are guidelines available to help manufacturers mitigate risks, but a lack of incentives to adhere to them [47], [48].

F. Oncoming Challenges

IT innovation is outpacing the development of supporting standards. With the changing threat environment, the cybersecurity needs of the future should be considered [7]. One such challenge for cryptography as a whole is that if large-scale quantum computers are ever built, many current public-key cryptosystems will be broken [46]. That would compromise the information security of digital communication. Therefore, NIST initiated a process of post-quantum cryptography standardization, including quantum-resistant lightweight algorithms for resource-restricted devices [49], [50].

The list of challenges for MWBDs is not limited by the preceding examples. Any influx of new technologies will introduce new security challenges [51], and new countermeasures should be proposed accordingly. Security requires resources and places demands on the device (e.g., exceeding a tight power budget, increasing time delays, or causing extra memory usage, etc.) [24]. Considering all the limitations, it might be adequate to talk about the compromises between security and other parameters, when these biomedical devices contain, at least, some basic protective mechanisms against the most possible attacks. Lightweight security does not mean weak security. However, the lightweight security properties may be different from those desired for general use: it may be less robust, less misuse resistant, and have fewer features [52].

However, if developers follow well-articulated and transparent principles and practices, adding secure mechanisms into devices is repeatable [53]. Therefore, developers should have a guidance of the threat modeling process, allowing them to estimate and mitigate threats in the early stages of the device lifecycle. In the following section, general considerations on the threat modeling process will be provided.

III. Threat Modeling Methodology

Considering the potential effects of cyberattacks against the emerging MWBDs, it is necessary to plan for these intrusions and to take steps to prevent them [54]. Therefore, a high-level method aimed to reveal, document, and address the security flaws of a system is demanded for these devices. This method is called threat modeling. Threat modeling uses special security terms, the main of which are assets, vulnerabilities, threats, attacks, risk, and risk assessment. Interconnection of these terms is shown in Fig. 2.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

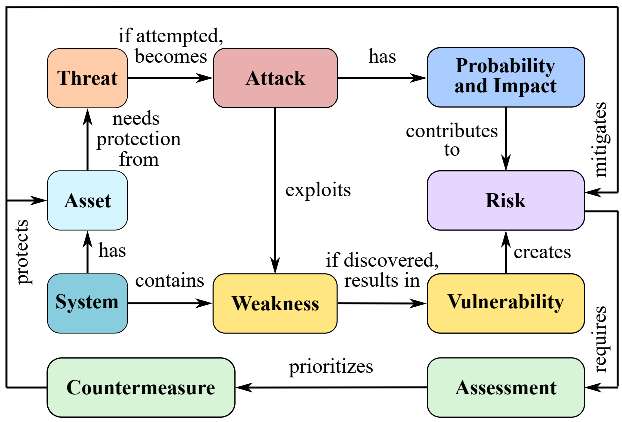

Fig. 2: Interconnection of terms in threat modeling and risk assessment. Adapted from [55].

An asset is any item of value present in the system that must be kept secure and that an adversary aims to steal, modify, or disrupt [39], [44]. A vulnerability is a weakness in a system caused by a bad design or implementation. A threat is a circumstance or an event with the potential to have a malicious effect on assets, individuals, or organizations [56]. An attack is a malicious activity that attempts to threaten an asset by exploiting a vulnerability [40]. Risk is a measure of the extent to which an entity is threatened by a potential circumstance or an event, and typically is a function of (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence [56]. Risk assessment is the process of identifying, estimating, and prioritizing risks to assets, individuals, or organizations [56]. In particular, qualitative-quantitative risk assessment is a set of methods, principles, or rules for assessing risk based on the use of qualitative terms and assigning them numerical ratings [56].

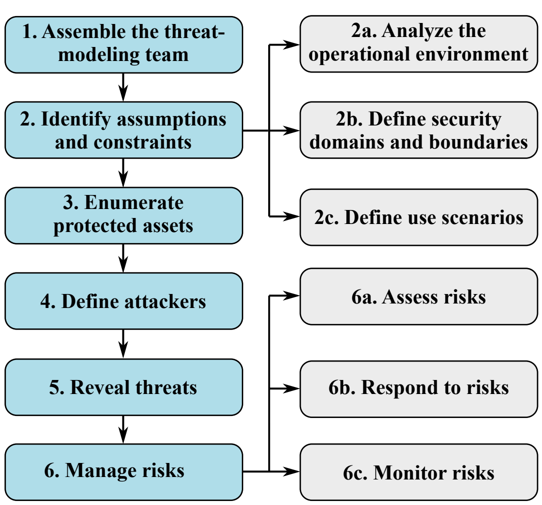

Fig. 3: Six primary steps of the threat modeling process. Adapted from [39], [40], [56].

Threat modeling is a multistage iterative process that provides insights on the assets that adversaries may be attracted by and detects the most probable attack vectors [40], [57], [58]. The ultimate goal of threat modeling is to reduce the overall threat risk to an acceptable level. During threat modeling, all its steps should be collected and organized into a threat-model document [39], [58], [59]. This document should be kept current, reflecting new threats and mitigations as they originate [39]. Threat modeling should be included in the overall development-and-documentation lifecycle [58]. Setting it apart from the overall design lifecycle may decrease the number of developers recognizing its importance [39].

The following subsections provide a high-level description of the primary phases of the threat modeling process, shown in Fig. 3. Activities highlighted for each phase build on the outcomes of prior activities. The steps provided for each phase are meant as a starting point and do not entirely define each activity.

A. Assemble the Threat-Modeling Team

A team that will perform threat modeling should be assembled first. A threat modeling team should consist of at least one member from each engineering group (hardware, wireless link, software, and others) to guarantee a complete understanding of underlying technologies [40].

B. Identify Assumptions and Constraints

The next step in the process is to identify security assumptions and constraints under which the threat modeling is performed. It allows capturing the information at an appropriate level of abstraction. These assumptions must be verified later [39]. This step includes three substeps:

1) Analyze the Operational Environment: the team captures the information about the infrastructure and describes the environment in which risk-based decisions are made. It helps to understand how different objects and elements in the system (an MWBD, a controller, a user, medical personnel, and other participants) interact with each other.

2) Define Security Domains and Boundaries: in this step, the primary logical components (for example, the analog front-end, the power management module, the data link, etc.) in the system are identified. Each logical component may be composed of several physical components and have different entry points and threats [39], [43]. Later, these logical components may be decomposed or merged to achieve a manageable level of granularity. For example, it may be appropriate to talk about the analog front-end of a device as a whole, or it may be essential to analyze the individual functional blocks that form this front-end.

No components are completely trusted, but rather various trust levels may be assigned to them (for example, high and low trusted components). After the high and low trusted logical components in the system are identified, the boundaries and interfaces between them should be determined [40]. After assumptions about the trust boundaries are made, threat analysis is usually performed for the data crossing these boundaries. The analysis must consider the direction of the data moving between trusted and untrusted components.

3) Define Use Scenarios: security measures are application-dependent [60]. For each system component, use scenarios provide a high-level description of how it will be implemented, deployed, and used. In order to better

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

understand the system behavior, it may also be useful to list "anti-scenarios", which are the settings or the usage scenarios that are known to be vulnerable or restricted [39], [60].

C. Enumerate Protected Assets

At this stage, assets that will be protected should be identified and listed for the investigated design. Assets may be tangible (such as user's personal information, therapies, or encryption keys) and intangible (for example, data consistency, data secrecy, data integrity, or data availability) [61]. The list of protected assets is later used in the risk analysis. This list for a particular design must be made considering the perspective of different stakeholders [44].

D. Define Attackers

Understanding the attacker type is important to understand the resources and capabilities that they have at their disposal [61]. While real attackers rarely fit into one category, at a high level, they can be classified based on: (1) their position relative to the system (external or internal adversaries), (2) their ability to intervene into the system (passive or active adversaries), (3) their number (a single entity or a coordinated group), and (4) the level of their expertise and equipment (sophisticated or unsophisticated) [24], [60], [62].

An external intruder is an outside entity that is not a part of the system and does not have an authorized access [60]. An internal intruder may be: (a) a malicious user who performs attacks to learn the secrets of the manufacturer or to get access to restricted functionality, and (b) a malicious manufacturer who has the ability to exploit the technology to collect information about the user or other devices [60]. A passive eavesdropper is capable only to listen to the communication channel and to get access to the exchanged messages. These attackers are able to compromise the patient's privacy. They can determine if a person has a biomedical device; discover the type of device, its model, and serial number; capture the information about the patient, such as the identifier (ID) of their health records, name, age, diagnosis, therapy, and so forth [24]. An active adversary is not only capable to listen to the channel, but also to send or replay commands to the device and to modify or block messages. The motivation for the active attacks may be, for example, to cause malfunctioning or DoS to the device [24].

E. Reveal Threats

In the next step, threats will be revealed using systematic analysis. For example, threats can be identified by defining participants (like the user, the attacker, etc.), their actions, and the consequences of those actions [39]. The objective is to enumerate the ways by which an attacker can compromise the system [40].

Threat modeling appears to be more productive when people have an understanding of how to attack systems [40]. For example, a kill-chain model [63] studies intrusions from the adversaries' perspectives by incorporating the analysis of adversaries, their capabilities, objectives, attitudes, and limitations. In a kill-chain model, intrusions are described not as singular events but as phased progressions. This model illustrates that, in fact, the adversary must successfully move through each stage of the chain to achieve the desired goal. Therefore, just one mitigation breaks the chain and stops the adversary [63].

F. Manage Risks

Once the risks for a system have been defined, the risk management process should include three steps:

1) Assess Risks: risk assessment is a crucial part of effective risk management. It is used to identify, estimate, and prioritize risks. The purpose of risk assessment is to inform decision-makers and to plan for risk responses. The result of risk assessment is a ranked list of threats that reflects the impact of attacks and the likelihood that harm will occur [56].

Risk and its contributing factors can be assessed in a variety of ways, including quantitatively, qualitatively, or semi-quantitatively [56]. While both quantitative and qualitative assessments have their limitations, the semi-quantitative assessment provides the benefits of both these approaches. This method typically employs bins, scales, or representative numbers. Bins or scales translate easily into qualitative terms and also allow relative comparisons between values. The role of expert judgment in assigning values is more evident than in a purely quantitative approach. Also, when scales or sets of bins provide enough granularity, relative prioritization among results is better supported than in a purely qualitative approach [56].

2) Respond to Risks: in this step, the corresponding techniques and technologies should be chosen to respond to the discovered threats. Depending on the threat model, customers, and expected use cases, various countermeasures may be proposed [33], [64]. As a starting point for MWBDs, the model for the lightweight implementation of data security may be applied [44]. While providing a guideline on how to start protecting MWBDs, this model primarily focuses on data security. Therefore, other interfaces (sensing channel, power delivery channel, and actuating channel) require a separate analysis of available protective mechanisms. In general, engineers should weigh the value of each security countermeasure for MWBDs to reach a trade-off between safety, reliability, resilience, security, and privacy risks.

3) Monitor Risks: risk assessment is not simply a one-time activity that provides permanent and definitive information for decision-makers. Monitoring risk factors (threats, vulnerabilities, capabilities and intent of adversaries, etc.) over time can provide critical information on changing conditions that could potentially affect the security of systems. Information derived from the ongoing risk monitoring can be used to refresh risk assessments [56].

In the next section, we will review and discuss some existing threat modeling frameworks.

IV. Existing Threat Modeling Frameworks

Multiple threat modeling frameworks have been developed in IT. Twelve of them, including STRIDE, PASTA, LINDDUN, CVSS, Attack Trees, Persona non Grata (PnG), Security Cards, Hybrid Threat Modeling Method (hTMM), Quantitative Threat Modeling Method (QTMM), Trike, VAST, and OCTAVE, were

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

summarized in [65]. Four more threat modeling frameworks (Attack Graph, Privilege Graph, Probabilistic Logic Modeling (PLM), and Insecurity Flow) have been reviewed in [43]. While all of these frameworks are most useful in their application areas, they have mainly been developed for pure software systems and networking systems. However, emerging MWBDs are predominantly hardware systems, which differ from classical IT devices [4], and these existing threat modeling techniques may be less efficient for them. Di et al. [43] also proposed a hardware threat modeling methodology. However, this work was preliminary, did not include any detailed threats/attack severity analysis mechanism, and did not involve any real-life assessment. ISO/IEC 15408 "Evaluation Criteria for IT Security" [66] defines the general methodology for threat modeling and a quantitative attack potential calculation, but it is a general framework that requires IT security expertise and an extended time to be applied to a product area. Section VI of this work will also introduce more threat models that are dedicated to the IoT devices, including the health IoT.

In the next section, a specific threat model for emerging MWBDs will be introduced. According to the described threat modeling methodology, assumptions about the operational environment, security boundaries, and use scenarios will be identified first. Then, suggestions about protected assets and attackers will be provided. Finally, a risk assessment methodology will be proposed.

V. Proposed Threat Model for MWBDs

Generic models, such as the one proposed in [44], may be a good starting point for implementing security in MWBDs. However, each particular device would require a separate threat analysis. Security expertise is needed to develop a threat model. Once the threat model is defined, the threat analysis becomes an engineering task that can be performed by non-experts in security [40].

We propose a domain-specific qualitative-quantitative threat model that aims to help the designers and manufacturers of MWBDs to identify threats and embed security in their designs in the pre-market phase of the lifecycle of an MWBD. Although some elements of the proposed threat modeling process may or may not be applicable to a specific MWBD, the overall process is valid for a wide range of devices.

A. Assumptions

1) Operational Environment: this model considers a single victim using an MWBD in a public space, accessible to multiple people, including but not limited to adversaries. Being in a public space, attackers can neither have physical access to the user (device) nor utilize large high-end equipment. For each particular case study of MWBDs, additional assumptions about its operational environment may be required.

2) Security Domains and Boundaries: in general, an MWBD controls and monitors some physical process (a health condition) in the human body. A set of sensors report the state of this health condition to the processor. Based on the information received from sensors, the processor defines the control signals to actuators to maintain the desired state. The processor often communicates with an external controller that monitors

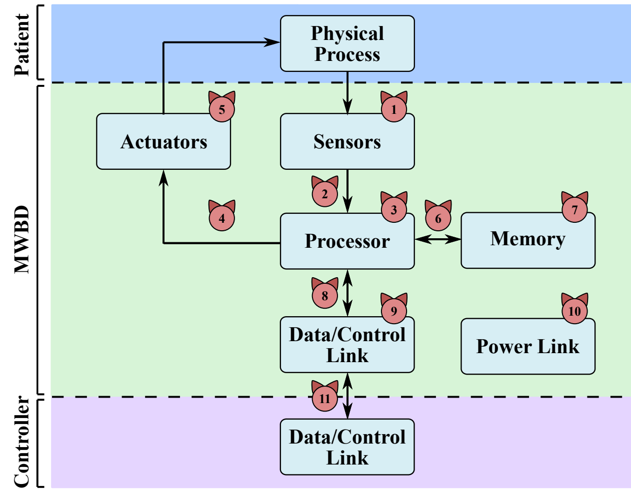

Fig. 4: General architecture of an MWBD. Attack points are shown in red. Adapted from [48].

or configures the device. This communication is performed via a wireless telemetry interface (data/control link). The power is typically also delivered wirelessly, except in more complex battery-powered wearables or implantables, like pacemakers. The processor may store various sensitive data (end users' private data, the chip ID, etc.) in the off-chip memory. This general architecture, presented in Fig. 4, considers eleven attack points, for which examples are provided in Table II.

TABLE II
Attack Points - Examples of Attacks

Attack point	Attack example
1	Fault injection attack [67].
2, 4, 6, 8	Probing [68].
3	Hardware trojans [69].
5	Control spoofing [70].
7	Microprobing [71].
9	Shielding / cutting the antenna.
10	Denial of sleep [72]. Power Analysis [73].
11	Man-in-the-middle (MIM) [74].

This work focuses on non-invasive direct attacks because the direct channels, missing security mechanisms, should be protected in the first place. Among the eleven defined attack points, direct interfaces include sensors (attack point 1), actuators (attack point 5), and telemetry (attack points 9, 10, and 11). For MWBDs, sensors and actuators are mainly located on/in the body. Therefore, it is hard to access them once they are deployed. Also, before deployment, there is a rigorous calibration for MWBDs, which makes it harder to deploy a tampered device. Therefore, for direct channels, attacks against telemetry (wireless data and power transfer) are prioritized in this work. Attack points 2 - 4 and 6 - 8 are out of scope for this model. Securing the remaining elements of the biomedical system (the physical process, the controller, the cloud, and the dashboard) needs separate analysis and is out of scope for this study.

To have a manageable level of complexity in the model,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

we consider that integrated circuits (ICs) are trustable after fabrication and testing, which means that malicious logic blocks are not inserted into the design and a chip manufacturer is trustable. After deployment, the IC design is fixed, in other words, there are no dynamic attacks on hardware. Semi-invasive (chip imaging, laser probing, voltage contrast, photo-emission, etc.) and invasive (reverse engineering, laser fault injection, etc.) hardware attacks are out of scope for this work.

3) Use Scenarios: use scenarios are unique for each device, and therefore cannot be generalized. Each specific MWBD would require listing its use scenarios. To give the readers a clearer picture through examples, Section VII of this work provides case studies for injectables, implantables, ingestibles, and wearables.

B. Protected Assets

Among various stakeholders of MWBDs, this model focuses on the user. This perspective requires balancing safety, service availability, resilience, and privacy. Safety protects from hazards, risks, or injury caused by the operation of the device. Service availability protects against denial of device service. Resilience means security against most attacks and the ability to return to a safe state in case of a successful attack. Privacy means protecting the confidentiality and integrity of personally identifiable information (PII). Privacy goals include: (1) device-existence privacy; (2) device-type privacy; (3) unique device ID privacy; (4) measurement and log privacy; (5) patient privacy; and (6) patient location privacy [62]. Confidentiality prevents the improper disclosure of information, and data integrity prevents the improper modification of information.

Assets are unique for each MWBD. Therefore, each case study of MWBDs would require specific analysis. After the assets are listed, attacks for each of them should be defined.

C. Attackers

This model considers sophisticated attackers, who have the intent and capabilities to attack the MWBD. The attacker may be either an individual (outsider, insider, trusted insider, or privileged insider) or an established group. The attacker may be both passive and active. The adversary, however, does not have physical access to the user of the MWBD, and as such all attacks are remote. For this reason, attacks on the physical process are not considered in the proposed model. However, for the smartwatch-like wearables, the attacker may manipulate the device for a limited period of time before the user begins to use it, for example, if the device was left unattended after deployment. Large high-end equipment is excluded from consideration in this paper since an attacker is not able to bring it to a public place.

D. Risk Assessment

The smartcard community introduced the guidance metrics to calculate the total effort required by an attacker to perform a successful attack. This guidance is described in the CCDB-2009-03-001, Common Criteria "Application of Attack Potential to Smartcards" [75]. In the proposed model, based on some recommendations from [75], six relevant characteristics of threats are selected to assess risks for an MWBD (see Table III):

1. *Expertise of the attacker* reflects the extent to which related knowledge is necessary for the adversary to perform a successful attack.
2. *Equipment required to carry out the attack* describes the tools that an adversary needs to use to carry out an attack.
3. *Physical proximity to the attacked device* shows how close the adversary should be to the user of an MWBD to mount a successful attack.
4. *Device access time* evaluates how long the attacker can access the attacked device.
5. *Device information* evaluates the need for the particular information assisting the attack, which cannot be substituted by a related combination of time and expertise [75].
6. *Severity of the attack* estimates the loss caused by its occurrence. In this model, severity corresponds to the physical harm for the user caused by a successful attack.

Further, the scoring system and the technique that is used to represent the final results of risk assessment will be described.

1) Scoring System: For each characteristic $C_1 - C_6$ in Table III, a three-tiered qualitative-quantitative scale is assigned. While this scale may provide limited granularity, it makes the first iteration of the proposed model less complex and easier to apply. Additional tiers may be added when required.

Characteristics $C_1 - C_5$ in Table III define the probability of an attack. The quantitative values for these categories are assigned in the reverse order: the fewer efforts are needed to perform an attack, the higher its likelihood, and therefore the higher the corresponding score. The total probability P of an attack equals to the sum of the values for $C_1 - C_5$. The impact of an attack I equals the value of the characteristic C_6 in Table III, for which the highest score corresponds to the highest severity. In the current scoring system, we differ three levels of severity. Attacks with low severity have a limited adverse effect on the user. Attacks with moderate severity temporarily impact the health of the user. Attacks with high severity lead to constant damage or a loss of human life. Since the impact reflects the effect on the patient's health condition, adding more levels to the impact would require an expertise of physicians who could define a finer border between different levels of severity.

To illustrate how these characteristics can be applied and scored, a case study of concrete MWBDs will be presented in Section VII. Since this scoring system is done by human judgement, the values do not have a formal basis. However, the relative values of the selected characteristics appear to be correct, based on the further provided analysis of case studies and the performed literature review. Our scoring system makes threat analysis systematic since it quantifies the relevant characteristics of threats. Therefore, it allows relative comparison between values and supports prioritization among results. It was noted by the authors that the proposed risk assessment method, which establishes a global conclusion by analyzing contributing individual factors, is similar to what has been adopted in other domains that face complex evaluation and decision making. A known example is the Building Security in Maturity Model (BSIMM) method [76], which is used by software developers to measure the quality of the internal development process towards creating secure software.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

TABLE III
Risk Assessment - Characteristics and Scales

	Characteristic	QLV	QNV	Description
Probability	**C1: Expertise of the attacker**	Expert	1	The attacker has broad expertise in cybersecurity, familiar with the target device at the developer level, and experienced with / equipped by sophisticated tools, for which the expertise in using is difficult to obtain.
		Proficient	2	The attacker is familiar with security behavior, classical attacks [75], and related disciplines (electrical engineering, software development, etc.).
		Layman	3	The attacker has no particular expertise.
	C2: Equipment required to carry out the attack	Custom	1	The attacker can use bespoke equipment.
		Specialized	2	The attacker can use expensive commercially available equipment, for which sales are controlled by manufacturers. The expertise in using the equipment is difficult to obtain, for example, the type of expensive equipment which universities have in their possession [75].
		Standard	3	The attacker can use only mass-market commercially available equipment, for example, smartphones or laptops. The expertise in using the equipment may be acquired from publicly available resources.
	C3: Physical proximity to the attacked device	Nearby	1	The attacker is in the vicinity (the same room) of the victim and is immediately visible. No physical obstacles, like walls and doors, exist between the attacker and the victim (device).
		Moderate	2	The attacker is in the same space with the victim, there are no physical obstacles between the attacker and the victim, but the distance between the attacker and the victim does not allow the victim to see the attacker.
		Remote	3	The attacker is capable to mount an attack while in a different location than the victim.
	C4: Device access time	Long	1	The attacker is able to access the device continuously.
		Moderate	2	The attacker is able to access the device multiple times.
		Short	3	The attacker is able to access the device once in real time.
	C5: Device information	Critical	1	Low-level information about hardware design or source code is available for the attacker [75].
		Restricted	2	Proprietary confidential developer's information, such as specifications or guidances, is available for the attacker [75].
		Public	3	Public domain information is available for the attacker.
Impact	**C6: Severity of the attack**	Low	1	Attacks have a limited adverse effect on the user (pose surmountable problems for the victim). For example, under certain context, loss of personal information does not prevent the MWBD from its correct functioning.
		Moderate	2	Attacks have a moderate adverse effect on the user. For example, alternating the sensor data may cause wrong commands to actuators, directly impacting the health of the victim, but the malicious effect is temporary.
		High	3	Attacks have a severe or catastrophic adverse effect on the user. In some circumstances, DoS attacks may lead to an irreparable harm, such as stroke, or even a loss of human life.

Note: QLV and QNV stand for a qualitative value and a quantitative value accordingly.

The BSIMM uses a ranking mechanism that combines many different factors - similar to the one proposed in this work - to measure the overall quality of secure software development. The BSIMM is an industry standard that has been adopted by multiple companies in several different sectors.

2) Representation of Final Results: After potential threats are identified, and their principal characteristics are captured, the total risk R for each of them may be defined based on their impact I and probability P. In risk management, the risk matrix approach is a typical qualitative-quantitative tool to evaluate various risks. Even though it is not mathematically rigorous, its visibility and ease of application make it well-received in various industries [77].

TABLE IV
Risk matrix

Probability (P)	**Impact (I)**		
	Low (1)	**Moderate (2)**	**High (3)**
Low (5-7)	Very Low	Moderate	High
Moderate (8-12)	Low	Moderate	High
High (13-15)	Moderate	High	Very High

For this model, the risk matrix shown in Table IV is used to assess risks, where different colors code different levels of risk. Since our model focuses on users, prioritizing their safety, between the total probability of an attack and its impact, the impact is more important as it corresponds to the physical harm for the user caused by a successful attack. After the risk assessment is completed for each threat and the data are filled in the risk matrix, the results appear sorted according to their risk levels. While these results suggest which threats are perilous and require more attention, designers should decide which threat to address first, based on their abilities and specific requirements for the design.

VI. Comparison of Threat Model Features

This section presents a comparison between the proposed threat model and four existing models [57], [60], [78], [79]. Out of four of these models, two models are dedicated to the general IoT devices [60], [78]. The other two models are designed for the health IoT devices [57], [79]. We will first discuss how these models perform risk assessment and if they may be efficiently applied to MWBDs. Then, we will present the results of comparison between our proposed model and these models in Table V.

The model proposed by Atamli et al. [60], while emphasizing the importance of careful consideration of the impact and likelihood of potential hazards, does not provide a scoring system to assess them. Aydos et al.'s model [78] evaluates the impacts of possible threats on IoT platforms and their likelihoods using a three-level system. This model is qualitative and does not provide any numerical levels for their nonnumerical categories. Therefore, using these models, different experts could produce significantly different assessment results relying on their individual experiences [56].

Cagnazzo et al.'s model [57] uses the STRIDE model and the DREAD model to classify and evaluate threats. Both STRIDE and DREAD are described in [40]. The STRIDE model appears to be one of the most known models [65] to help people remember the types of threats to which system

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

TABLE V
Comparison of Threat Models

Features \ Models	This work	[60] 2014	[78] 2019	[57] 2018	[79] 2020
MWBD-specific	✓	✗	✗	✓	✓
Applicable to various types of MWBDs	✓	✗	✗	✓	✗
Qualitative-quantitative	✓	✗	✗	✓	✓
Visualizes results using risk matrices	✓	✗	✓	✗	✓
Considers a device deployed in a public space	✓	✗	✗	✗	✓
Prioritizes the patient	✓	✗	✗	✗	✗
Prioritizes attacks against the wireless link	✓	✗	✗	✗	✓
Classifies threats according to IoT layers	✗	✗	✓	✗	✗
Evaluates the expertise of the attacker	✓	✗	✗	✓	✗
Evaluates the equipment of the attacker	✓	✗	✗	✗	✓
Evaluates the proximity to the device	✓	✗	✗	✗	✗
Evaluates the device access time	✓	✗	✗	✗	✓
Evaluates the need for the device information	✓	✗	✗	✗	✗
Evaluates the impact of an attack	✓	✓	✓	✓	✓
Evaluates the overall likelihood of an attack	✓	✓	✓	✓	✓
Analyzes risks for other system elements (Fig. 1)	✗	✓	✓	✗	✓
Applied to real devices (case studies)	✓	✗	✗	✗	✗
Proposes possible risk mitigation strategies	✗	✓	✗	✓	✓

✓: the model supports that feature; ✗: the model does not support that feature.

components might be exposed. STRIDE is an abbreviation for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege [40]. In [57], Cagnazzo et al. use STRIDE to analyze the security and privacy of data flows across networks. STRIDE was developed for software systems whereas MWBDs are predominantly hardware systems. Therefore, the application of STRIDE to MWBDs to analyze threats at the device level seems less effective. DREAD is an acronym for damage potential, reproducibility, exploitability, affected users, and discoverability. DREAD was initially designed to rank errors, flaws, or faults in software [40]. Since MWBDs are predominantly hardware systems, DREAD is not entirely suitable for them. For example, in the case of MWBDs, there is only one user and, as such, the criteria of the affected users would not contribute to the final decision. The category of discoverability also does not seem to be informative as it is difficult to estimate and is usually set equal to the maximum possible value [40].

Ngamboé et al.'s model [79] carries out risk assessment according to the ISO/IEC 27005 [80] standard and the NIST SP 800-30 guide [56]. This work focuses solely on cardiac implantable electronic devices. The authors proposed to extend their study to other implantables. However, other categories of MWBDs, such as ingestibles, injectables, and wearables, are missing in their research.

As presented in Table V, the model proposed in this manuscript appears to be efficient for MWBDs when compared to [57], [60], [78], [79], and therefore would eventually provide better security for these devices. As it can also be observed in Table V, our model is applicable to a wide range of MWBDs and provides a qualitative-quantitative scoring system for risk assessment. This system makes the role of expert judgement in assigning values more evident and also allows better prioritizing results than in purely quantitative approach [56].

We also examined the recent literature in IEEE IoT Journal and did not find concrete competitors for our threat modeling and risk assessment methodology. For example, in the specific area of medical devices, Masud et al. [81] introduced a lightweight security protocol to provide mutual authentication and secret key establishment between a physician and a sensor node. Wu et al. [82] surveyed access control schemes to prevent unauthorized access to implantable medical devices. Rahman et al. [83] examined nine COVID-19 diagnostic methods, involving medical IoT devices and relying on deep learning, with adversarial examples. Gatouillat et al. [84] reviewed recent contributions, dealing with robustness, security, reliability, verification, and validation for cyber-physical systems in medicine. Sun et al. [85] proposed a mutual authentication scheme for the device-to-server communication in the Internet of Medical Things. None of these authors propose threat modeling and risk assessment for miniaturized wireless medical devices, which is a specific novelty claim in our work.

In the next section, we will apply the proposed model to representative injectables, ingestibles, implantables, and wearables. Our goal is to cover enough information to illustrate how the proposed model can be applied, but also to keep it less complex, so that non-experts in security could add threat modeling in their design and manufacturing processes. Moreover, the proposed model is intended to be used in the pre-market phase of the lifecycle of an MWBD. While applying our model to already existing devices appears to be beneficial, the case studies are used only to illustrate the threat modeling process.

VII. Case Studies for Emerging MWBDs

This chapter aims to provide meaningful examples of MWBDs (see Table VI) and their associated threats (see Table VII), which are disclosed and prioritized with the application of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

TABLE VI
Case Studies - Devices and Assets

Number	Name	Category	Purpose	Status	Assets	Ref.
D1	BioMote	Injectable	A wireless sensor node for continuous monitoring of the blood alcohol content (ethanol, background, and pH).	In-vitro tests.	1. Backscattered user sensor data (blood alcohol content).	[14]
D2	Wireless Capsule Endoscope	Ingestible	A wireless spherical endoscopic capsule for ColoRectal Cancer (CRC) screening with a locomotion control.	In-vitro tests.	1. User data (cancer information, video frames). 2. Control signals from an external device.	[86]
D3	Trimodal wireless implantable neural interface System-on-Chip (SoC)	Implantable	A wireless trimodal neural interface SoC, providing optical/electrical stimulation capabilities and neural recordings.	In-vivo tests in freely behaving animals.	1. Recording/stimulation parameters (BLE and on-off-keying (OOK) signals at 13.56 MHz). 2. Evoked neural activities (OOK RF signals at 433 MHz).	[87]
D4	An integrated readout circuit for a transcutaneous oxygen sensing wearable device	Wearable	A fluorescence-based readout dedicated to sensing transcutaneous oxygen diffusing through the skin.	Ex-vivo tests.	1. User data (partial pressure of transcutaneous O_2). 2. Control signals from an external controller.	[88]

TABLE VII
Case Studies - Threats

Number	Threat	Threat violates	Device	Probability						Impact
				C1	C2	C3	C4	C5	Total	C6
T1	The attacker uses a counterfeit wearable controller to power up the device and to collect the sensitive private health data. As a result, the confidentiality of the patient's personal information is violated.	Confidentiality Authenticity	D1	3	3	2	3	3	14 (High)	1 (Low)
T2	The attacker conducts a MIM attack using special equipment to tamper with the data / control signals, producing a false report about the health condition / a false command, causing a false treatment or therapy. This may result in temporary or permanent health damage. Even if the device does not have actuators, a physician working with the corrupted sensor data can prescribe a wrong treatment or therapy.	Integrity	D1 D3	1	2	2	3	3	11 (Moderate)	3 (High)
T3	The attacker jams the wireless data link. Sensor data cannot be collected accurately, and stimulation cannot be applied correctly. This may result in permanent health damage due to the incorrect or missing treatment.	Availability	D1 D3	1	2	3	2	3	11 (Moderate)	3 (High)
T4	The attacker uses a software-defined radio or an external hub to collect the data about the evoked neural activities of the user. This leads to a leak of the patient's personal confidential information.	Confidentiality Authenticity	D3	2	3	2	3	3	13 (High)	1 (Low)
T5	The attacker eavesdrops the data, using the standard Bluetooth equipment. This leads to a leak of the patient's confidential information.	Confidentiality Authenticity	D2 D4	2	2	2	3	3	12 (Moderate)	1 (Low)
T6	The attacker interferes with the communication channel and substitutes the user data by some counterfeit data. This may result in permanent health damage due to a wrong or missing therapy.	Authenticity	D2 D4	1	2	2	3	3	11 (Moderate)	3 (High)
T7	The attacker replays a command to decrease the illumination or to switch the Bluetooth module off to decrease the amount of information that can be extracted from video frames. This would require to repeat the measurements with a different device.	Availability	D2	2	2	2	3	3	12 (Moderate)	1 (Low)
T8	The attacker sends a high-volume radio traffic to deplete the battery. Even if the device supports authentication, the process of commands' and data validation would consume extra power, which could lead eventually to denial of service.	Availability	D2 D4	2	2	2	3	3	12 (Moderate)	1 (low) 3 (High)

Note: for D2 and D4, T8 has different impacts. D2 is used for short-term monitoring of the digestive tract. Measurements are performed in a laboratory under the supervision of a physician. In this case, the denial of service may be quickly resolved and the procedure may be repeated with another device. However, D4 can be used outside the hospital. In the event of DoS, it may not be quickly replaced with another device. Therefore, the impact of T8 is higher for D4.

our proposed threat model. The values in Table VII were assigned based on the scales presented in Table III and the available information about selected example devices. For each category of MWBDs, one representative device was selected. At the time of writing this paper, most MWBDs were either in the proof-of-concept stage or in the stage of pre-clinical trials in freely-behaving animals. Nevertheless, since they have a potential for large-scale manufacturing and are intended to be ultimately used in humans, it is of interest to analyze threats for them using the proposed threat model.

Since the primary purpose of this section is to illustrate the application of the designed model, but not to perform a comprehensive threat modeling for the selected devices, it does not guarantee to include all potential threats for the selected case studies. Another reason why a more in-depth threat analysis has not been performed is that these devices are not commercially available and widely accessible; moreover, we have learned about them from the available academic

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

publications, which we used as datasheets. The following subsections will provide brief overviews of these case studies, including information about their purposes, internal structure, and operational environments. For each of them, risk assessment results will be presented in the form of risk matrices.

A. Case study 1 - Injectable

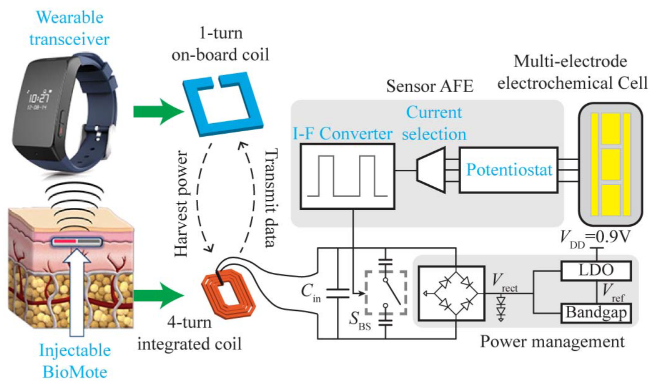

Fig. 5: Device 1: block diagram. Adapted from [14].

BioMote [14], shown in Fig. 5 and further referred to as device 1 (D1), is a wireless sensor node intended for continuous monitoring of the blood alcohol content. D1 is routinely used outside of a clinical laboratory. D1 is subcutaneously injected into the interstitial fluid and wirelessly paired with an external wearable controller. The D1's electrochemical sensor array measures alcohol and pH. These measurements are unidirectionally transmitted to the controller through backscatter using a current-to-frequency converter. D1 is wirelessly powered by the controller via an inductive link.

TABLE VIII
Risk matrix - Device 1

Probability (*P*)	**Impact (*I*)**		
	Low	**Moderate**	**High**
Low	–	–	–
Moderate	–	–	T2, T3
High	T1	–	–

For D1, the risk matrix is presented in Table VIII. It shows that T1 has a moderate risk while T2 and T3 have high risks.

B. Case study 2 - Ingestible

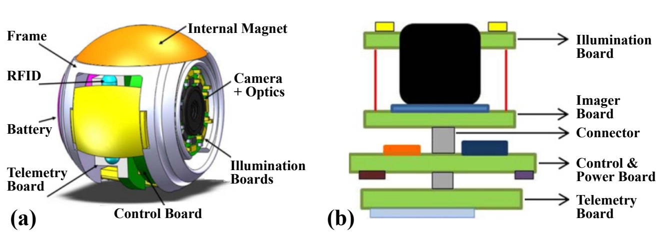

Fig. 6: Device 2: (a) 3D design. (b) Block diagram. Adapted from [86].

A wireless capsule endoscope [86], shown in Fig. 6 and further referred to as device 2 (D2), is intended for ColoRectal Cancer (CRC) screening with locomotion control. The primary modules of D2 include an image sensor with optics, an illumination board, a control unit, a telemetry board, an actuation system, a localization unit, and a battery with a recharging circuit. D2 is used in a clinical laboratory and swallowed by the patient. The image sensor of D2 captures the condition of the patient's digestive tract. The collected images are streamed via Bluetooth to the external controller.

TABLE IX
Risk matrix - Device 2

Probability (*P*)	**Impact (*I*)**		
	Low	**Moderate**	**High**
Low	–	–	–
Moderate	T5, T7, T8	–	T6
High	–	–	–

For D2, the risk matrix is presented in Table IX. It demonstrates that, among four detected threats, T6 has a high risk and T5, T7, and T8 have low risks.

C. Case study 3 - Implantable

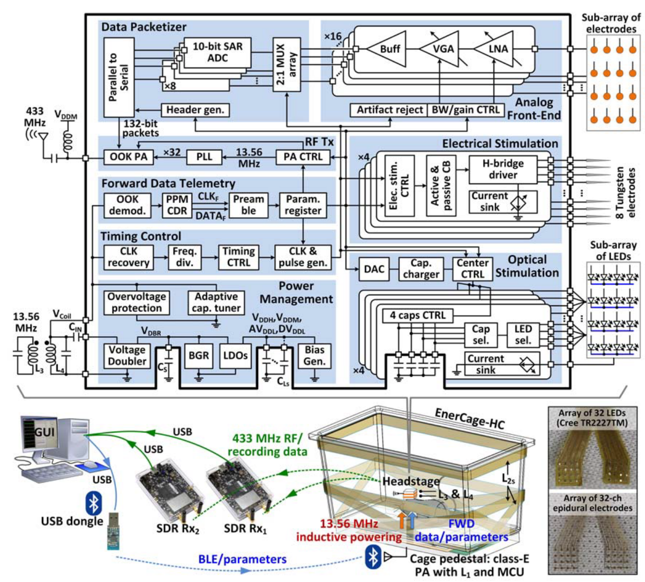

Fig. 7: Device 3: block diagram. Adapted from [87].

A trimodal wireless implantable neural interface system on chip (SoC) [87], shown in Fig. 7 and further referred to as device 3 (D3), provides optical/electrical stimulation capabilities and neural recordings. D3 consists of optical and electrical stimulation blocks, an analog front-end, a data packetizer, telemetry blocks, a timing control unit, and a power management module. D3 is used in a clinical laboratory. D3 is implanted into the brain and wirelessly paired with a control arena. The recording/stimulation parameters are sent to the arena via Bluetooth Low Energy (BLE) from an external terminal (computer). The arena relays the BLE parameters to D3 by on-off-keying (OOK) of a 13.56 MHz power carrier via inductive coils. D3 generates optical/electrical stimulation pulses based on the received parameters. The evoked neural

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3144130, IEEE Internet of Things Journal

activities are sensed, processed, and transmitted by D3 to the terminal by OOK at 433 MHz. The terminal receives the data by a pair of software-defined radios (SDRs). D3 is not currently used in humans but for scientific experiments in freely behaving animals (rodents). However, it was selected as a case study since its functionality is similar to that of commercial products like [89]. In addition, the commercial products themselves are proprietary, which makes them unavailable for the analysis based on public data.

TABLE X
Risk matrix - Device 3

Probability (P)	Impact (I)		
	Low	Moderate	High
Low	–	–	–
Moderate	–	–	T2, T3
High	T4	–	–

For D3, the risk matrix is presented in Table X. It shows that T2 and T3 have high risks, whereas T4 has a moderate risk.

D. Case study 4 - Wearable

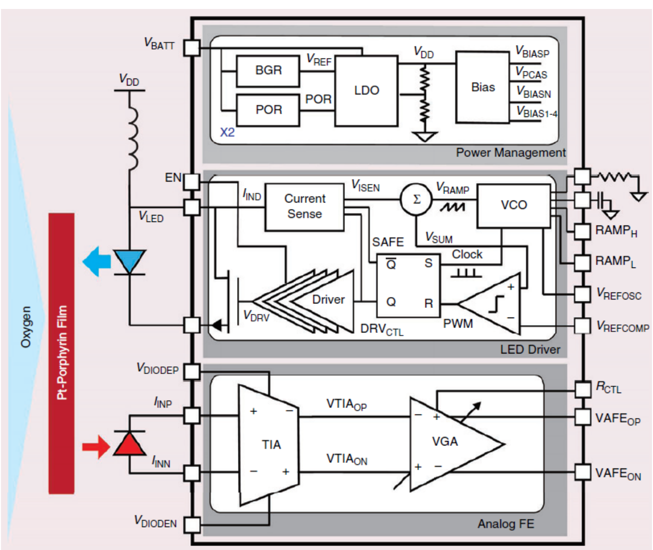

Fig. 8: Device 4: block diagram of the readout IC. Adapted from [9].

An integrated readout circuit [88], shown in Fig. 8 and further referred to as device 4 (D4), is used for non-invasive transcutaneous oxygen sensing, which correlates with the blood oxygen level. D4 primary blocks include an analog front-end, a light-emitting diode (LED) driver, and a power management block. D4 is routinely used both in a home setting and in a clinical environment. D4 is intended to be used with dry electrodes in the form of a smart watch or a smart patch. D4 is projected to be a battery-powered device transmitting the sensor data to the external controller via BLE.

For D4, the risk matrix is presented in Table XI. It reveals that T6 and T8 have high risks while T5 has a low risk.

TABLE XI
Risk matrix - Device 4

Probability (P)	Impact (I)		
	Low	Moderate	High
Low	–	–	–
Moderate	T5	–	T6, T8
High	–	–	–

VIII. Discussion and Future Work

The use of the proposed model revealed and prioritized threats for the case studies of injectables, ingestibles, implantables, and wearables, showing that the model is applicable for a wide range of devices. However, the proposed threat model enables performing further validation, which would involve additional case studies. This validation may be done by investigating known vulnerabilities in devices and comparing the results of the analysis with the outcome of other models. It would also be of interest to include more commercial devices. However, being proprietary and closed source, these devices are challenging to be analyzed based on the public domain information [62]. Based on the results of these additional investigations, it may become apparent if separate threat models for each category of MWBDs may provide more information for designers and manufacturers. In addition, as discussed in Section V, more levels for selected characteristics of threats would provide higher granularity and more comprehensive threat analysis. Another suggestion for future work is to design threat models focused on other primary stakeholders of MWBDs, including manufacturers and hospitals.

IX. Conclusion

This work discussed the importance of security for the emerging miniaturized wireless biomedical devices. The combination of valuable assets belonging to different stakeholders and multiple attack surfaces makes MWBDs a target for cybercriminals. Since MWBDs pose significant risks for their stakeholders, security should be embedded into MWBDs in a structured and repeatable way during the pre-market phase.

The initial step in embedding security into a design is to perform threat modeling. However, it has been shown that MWBDs are distinct from conventional IT devices and require a unique threat model. Therefore, first, this work described the threat modeling process for MWBDs. Then, a domain-specific qualitative-quantitative threat model, suitable for a wide range of MWBDs, was proposed. ISO/IEC 15408 ”Evaluation Criteria for IT Security” [66] defines the general methodology for threat modeling and a quantitative attack potential calculation, but it is a general framework that requires IT security expertise and an extended time to be applied to a product area.

The model suggested using six relevant characteristics of attacks to assess their probability and impact. For each characteristic, a three-tiered qualitative-quantitative scale was assigned. This approach makes the role of expert judgement in assigning values more evident than in purely quantitative and purely qualitative models. The three-tiered scale makes the first iteration of our model less complex, but still provides enough granularity and supports relative prioritization among results. The rationale behind this decision was to motivate more medical device creators, including those who do not have adequete expertise in cyber security, to integrate threat modeling into their designs. The total risk of an attack was defined using the risk matrix approach. While this approach is not mathematically rigorous, its intuitive graphic form, ease of understanding, and ease of application make it common in various industries [77].

To demonstrate utility of this model, we compared it to some other existing models in Section VI and applied it to representative case studies in Section VII. The primary intent of case studies was to detect several threats to show how the model may be adopted by a threat modeling team. The model appeared to be easy to apply and sufficient to describe threats for selected case studies. This paper also made suggestions for future work.

REFERENCES

[1] C. J. Bettinger, "Advances in materials and structures for ingestible electromechanical medical devices," *Angewandte Chemie International Edition*, vol. 57(52), pp. 16 946–16 958, Dec. 2018.

[2] H. C. Koydemir and A. Ozcan, "Wearable and implantable sensors for biomedical applications," *Annual Review of Analytical Chemistry*, vol. 11, pp. 127–146, Jun. 2018.

[3] J. Dunn, R. Runge, and M. Snyder, "Wearables and the medical revolution," *Personalized medicine*, vol. 15(5), pp. 429–448, Sep. 2018.

[4] *Foundational cybersecurity activities for IoT device manufacturers*, NISTIR 8259, 2020.

[5] A. Meola, "IoT healthcare in 2021: companies, medical devices, and use cases," *Business Insider*, Feb. 2021. [Online]. Available: https://www.businessinsider.com/iot-healthcare. [Accessed Apr.22, 2021].

[6] A. Kiourti and K. S. Nikita, "A review of in-body biotelemetry devices: Implantables, ingestibles, and injectables," *IEEE Transactions on Biomedical Engineering*, vol. 64(7), pp. 1422–1430, Feb. 2017.

[7] *Interagency report on the status of international cybersecurity standardization for IoT*, NISTIR 8200, 2018.

[8] T. Weil and S. Murugesan, "IT risk and resilience – cybersecurity response to COVID-19," *IT Professional*, vol. 22(3), May 2020.

[9] U. Guler, I. Costanzo, and D. Sen, "Emerging blood gas monitors: how they can help with COVID-19," *IEEE Solid-State Circuits Magazine*, vol. 12(4), pp. 33–47, Nov. 2020.

[10] S. Allen, "2020 US and global health care outlook," *Deloitte*, 2020. [Online]. Available: https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/global-health-care-sector-outlook.html#. [Accessed Apr.22, 2021].

[11] J. E. Hollander and B. G. Carr, "Virtually perfect? Telemedicine for COVID-19," *New England Journal of Medicine*, vol. 382(18), pp. 1679–1681, Apr. 2020.

[12] S. Song et al., "A 769μW battery-powered single-chip SoC with BLE for multi-modal vital sign monitoring health patches," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 13(6), pp. 1506–1517, Oct. 2019.

[13] M. Li, W. Xiong, and Y. Li, "Wearable measurement of ECG signals based on smart clothing," *International Journal of Telemedicine and Applications*, vol. 2020, Jan. 2020.

[14] H. Jiang et al., "A sub-1μW multiparameter injectable BioMote for continuous alcohol monitoring," in *2018 IEEE Custom Integrated Circuits Conference (CICC)*, Apr. 2018, pp. 1–4.

[15] M. Mimee et al., "An ingestible bacterial-electronic system to monitor gastrointestinal health," *Science*, vol. 360, no. 6391, pp. 915–918, May 2018.

[16] J. Charthad et al., "A mm-sized wireless implantable device for electrical stimulation of peripheral nerves," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 12(2), pp. 257–270, Mar. 2018.

[17] B. C. Johnson et al., "StimDust: a 6.5mm^3, wireless ultrasonic peripheral nerve stimulator with 82% peak chip efficiency," in *2018 IEEE Custom Integrated Circuits Conference (CICC)*, 2018, pp. 1–4.

[18] B. Yan et al., "Battery-free implantable insulin micropump operating at transcutaneously radio frequency-transmittable power," *Medical Devices & Sensors*, vol. 2(5-6), p. e10055, Oct. 2019.

[19] X. Guo et al., "A novel and reproducible release mechanism for a drug-delivery system in the gastrointestinal tract," *Biomedical microdevices*, vol. 21(1), pp. 1–9, Mar. 2019.

[20] G. Selimis, "A healthy approach to medical security," *Electronics Europe News*, pp. 30–31, Jan. 2020.

[21] W. Sun et al., "Security and privacy in the medical internet of things: a review," *Security and Communication Networks*, vol. 2018, Mar. 2018.

[22] B. Alexander, S. Haseeb, and A. Baranchuk, "Are implanted electronic devices hackable?" *Trends in cardiovascular medicine*, vol. 29, no. 8, pp. 476–480, Nov. 2019.

[23] D. Kotz et al., "Privacy and security in mobile health: a research agenda," *Computer*, vol. 49(6), pp. 22–30, Jun. 2016.

[24] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: a comprehensive survey," *Journal of biomedical informatics*, vol. 55, pp. 272–289, Jun. 2015.

[25] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, May 2008, pp. 129–142.

[26] L. H. Newman, "A new pacemaker hack puts malware directly on the devices," *Wired*, Aug. 2018. [Online]. Available: https://www.wired.com/story/pacemaker-hack-malware-black-hat/. [Accessed Apr.22, 2021].

[27] S. Shin and J. Lipton, "Security researchers say they can hack Medtronic pacemakers," *CNBC*, Aug. 2018. [Online]. Available: https://www.cnbc.com/2018/08/17/security-researchers-say-they-can-hack-medtronic-pacemakers.html. [Accessed Apr.22, 2021].

[28] F. Donovan, "Medtronic Criticized for Lax Medical Device Security Response," *Health IT Security*, Aug. 2018. [Online]. Available: https://healthitsecurity.com/news/medtronic-criticized-for-lax-medical-device-security-response. [Accessed Apr.22, 2021].

[29] S. Tuli et al., "Next generation technologies for smart healthcare: challenges, vision, model, trends and future directions," *Internet Technology Letters*, p. e145, Mar. 2019.

[30] P. A. Williams and V. McCauley, "Always connected: the security challenges of the healthcare Internet of Things," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Dec. 2016, pp. 30–35.

[31] *NIST cybersecurity for IoT program*, 2016. [Online]. Available: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program. [Accessed Jan.17, 2021].

[32] *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*, NISTIR 8228, 2019.

[33] *IoT device cybersecurity capability core baseline*, NISTIR 8259A, 2020.

[34] *IoT device cybersecurity guidance for the federal government: establishing IoT device cybersecurity requirements*, NIST SP 800-213 (Draft), 2020.

[35] *IoT non-technical supporting capability core baseline*, NISTIR 8259B (Draft), 2020.

[36] *Creating a profile using the IoT core baseline and non-technical baseline*, NISTIR 8259C (Draft), 2020.

[37] *Profile using the IoT core baseline and non-technical baseline for the federal government*, NISTIR 8259D (Draft), 2020.

[38] M. K. McGee, "FDA's Kevin Fu on threat modeling for medical devices," *Careers Info Security*, 2020. [Online]. Available: https://www.careersinfosecurity.com/interviews/fdas-kevin-fu-on-threat-modeling-for-medical-devices-i-4869. [Accessed Apr.22, 2021].

[39] P. Torr, "Demystifying the threat modeling process," *IEEE Security & Privacy*, vol. 3(5), pp. 66–70, Oct. 2005.

[40] M. Howard and D. Leblanc, *Writing Secure Code*, 2nd ed., Redmond, WA, Microsoft Press, 2002.

[41] M. Alioto and S. Taneja, "Enabling ubiquitous hardware security via energy-efficient primitives and systems," in *2019 IEEE Custom Integrated Circuits Conference (CICC)*, Apr. 2019, pp. 1–8.

[42] *NIST Lightweight Cryptography Project*, 2016. [Online]. Available: https://csrc.nist.gov/Projects/lightweight-cryptography. [Accessed Jan.17, 2021].

[43] J. Di and S. Smith, "A hardware threat modeling concept for trustable integrated circuits," in *2007 IEEE Region 5 Technical Conference*. IEEE, Apr. 2007, pp. 354–357.

[44] V. Vakhter et al., "Minimum on-the-node data security for the next-generation miniaturized wireless biomedical devices," in *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug. 2020, pp. 1068–1071.

[45] S. Maji et al., "A low-power dual-factor authentication unit for secure implantable devices," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*, Mar. 2020, pp. 1–4.

[46] *2019 NIST/ITL cybersecurity program annual report*, SP 800-211, 2020.

[47] *IoT cybersecurity colloquium: a NIST workshop proceedings*, NISTIR 8201, 2017.
[48] A. Cardenas, "Cyber-physical systems security knowledge area," London, UK, CyBOK, 2019.
[49] *NIST post-quantum cryptography project*, 2017. [Online]. Available: https://content.csrc.e1a.nist.gov/Projects/Post-Quantum-Cryptography. [Accessed Apr.2, 2021].
[50] *NIST reveals 26 algorithms advancing to the post-quantum crypto 'semifinals'*, May 2019. [Online]. Available: https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals. [Accessed Apr.22, 2021].
[51] J. M. Franklin et al., "Security analysis of first responder mobile and wearable devices," *NIST*, May 2020. [Online]. Available: https://www.nist.gov/publications/security-analysis-first-responder-mobile-and-wearable-devices. [Accessed Feb.2, 2021].
[52] K. McKay, "Introduction to cryptographic work at NIST," Worcester Polytechnic Institute - WPI, Cybercorps. Jan. 30, 2020.
[53] G. Hunt, G. Letey, and E. Nightingale, "The seven properties of highly secure devices," Tech. Report MSR-TR-2017-16, Mar. 2017.
[54] C. Martin, "Cybersecurity and COVID-19," *Computing Edge*, vol. 6(10), 2020.
[55] B. Sanz et al., "A threat model approach to attacks and countermeasures in on-line social networks," in *11th Reunion Espanola de Criptografia y Seguridad de la Información (RECSI)*, Aug. 2011, pp. 343–348.
[56] *Guide for conducting risk assessments*, NIST SP 800-30 Rev.1, 2012.
[57] Cagnazzo, Matteo et al., "Threat modeling for mobile health systems," in *2018 IEEE Wireless Communications & Networking Conference Workshops*, Apr. 2018, pp. 314–319.
[58] Seeam, Amar et al., "Threat modeling and security issues for the Internet of Things," in *2019 Conference on Next Generation Computing Applications (NextComp)*, Sep. 2019, pp. 1–8.
[59] "Five steps to successful threat modelling," *ARM Community*, Jan. 2019. [Online]. Available: https://community.arm.com/iot/b/internet-of-things/posts/five-steps-to-successful-threat-modelling?utm_source=google&utm_medium=cpc&utm_campaign=2019_ebg-security_mk01-1_na_na_bol&utm_term=five-steps-to-successful-threat-modelling&utm_content=blog&gclid=CjwKCAiAjrXxBRAPEiwAiM3DQnNOCgiKA2GuopshH_wYsalX1aa-Ekarmn5jvSSUlWZQj8GrTav_choCeroQAvD_BwE. [Accessed Apr.22, 2021].
[60] A. W. Atamli and A. Martin, "Threat-based security analysis for the internet of things," in *2014 International Workshop on Secure Internet of Things*. IEEE, 2014, pp. 35–43.
[61] R. Hasan et al., "Toward a threat model for storage systems," in *Proceedings of the 2005 ACM workshop on Storage security and survivability*, Nov. 2005, pp. 94–102.
[62] M. Rushanan et al., "Sok: security and privacy in implantable medical devices and body area networks," in *2014 IEEE Symposium on Security and Privacy*, May 2014, pp. 524–539.
[63] E. Hutchins et al., "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1(1), p. 80, Apr. 2011.
[64] I. Verbauwhede, "Hardware security," Bristol, UK, University of Bristol, CyBOK, 2019.
[65] N. Shevchenko et al., "Threat modeling: a summary of available methods," Carnegie Mellon University Software Engineering Institute Pittsburgh United States, Tech. Rep., Jul. 2018.
[66] *Evaluation Criteria for IT Security*, ISO/IEC 15408-1:2009.
[67] O. Salem et al., "Sensor fault and patient anomaly detection and classification in medical wireless sensor networks," in *2013 IEEE International Conference on Communications (ICC)*, Jun. 2013, pp. 4373–4378.
[68] S. Aga and S. Narayanasamy, "InvisiMem: smart memory defenses for memory bus side channel," *ACM SIGARCH Computer Architecture News*, vol. 45(2), pp. 94–106, Jun. 2017.
[69] A. Syed and R. M. Lourde, "Hardware security threats to DSP applications in an IoT network," in *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, Dec. 2016, pp. 62–66.
[70] M. Hasan and S. Mohan, "Protecting actuators in safety-critical IoT systems from control spoofing attacks," in *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, Dec. 2019, pp. 8–14.
[71] S. Skorobogatov, "How microprobing can attack encrypted memory," in *2017 Euromicro Conference on Digital System Design (DSD)*, Aug. 2017, pp. 244–251.
[72] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, Jun. 2005, pp. 356–364.
[73] J. Zhang et al., "Power analysis attack on a lightweight block cipher GIFT," in *Proceedings of the 9th International Conference on Computer Engineering and Networks*, 2021, pp. 565–574.
[74] A. Lahmadi et al., "MitM attack detection in BLE networks using reconstruction and classification machine learning techniques," in *MLCS 2020-2nd Workshop on Machine Learning for Cybersecurity*, Sep. 2020, pp. 1–16.
[75] *Application of attack potential to smartcards*, CCDB-2009-03-001 - Common Criteria, 2009.
[76] *The Building Security in Maturity Model (BSIMM)*, 2021. [Online]. Available: https://www.bsimm.com/. [Accessed Sept.27, 2021].
[77] H. Ni, A. Chen, and N. Chen, "Some extensions on risk matrix approach," *Safety Science*, vol. 48(10), pp. 1269–1278, Dec. 2010.
[78] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Measurement and Control*, vol. 52, no. 5-6, pp. 338–353, Jun. 2019.
[79] M. Ngamboé et al., "Risk assessment of cyber attacks on telemetry enabled cardiac implantable electronic devices (CIED)," *arXiv preprint arXiv:1904.11908*, 2020.
[80] *Information technology — Security techniques — Information security risk management*, ISO/IEC 27005:2018(E), 2018.
[81] M. Masud et al., "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," *IEEE Internet of Things Journal*, pp. 1–1, 2020.
[82] L. Wu et al., "Access Control Schemes for Implantable Medical Devices: A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1272–1283, Oct. 2017, conference Name: IEEE Internet of Things Journal.
[83] A. Rahman et al., "Adversarial Examples—Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9603–9610, Jun. 2021.
[84] A. Gatouillat et al., "Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018.
[85] J. Sun et al., "Mutual Authentication Scheme for the Device-to-Server Communication in the Internet of Medical Things," *IEEE Internet of Things Journal*, pp. 1–1, 2021.
[86] R. Fontana et al., "An innovative wireless endoscopic capsule with spherical shape," *IEEE transactions on biomedical circuits and systems*, vol. 11(1), pp. 143–152, Jun. 2016.
[87] Y. Jia et al., "A trimodal wireless implantable neural interface system-on-chip," in *2020 International Solid-State Circuits Conference (ISSCC), Session 26 / Biomedical Innovations*, Nov. 2020, pp. 414–415.
[88] I. Costanzo, D. Sen, and U. Guler, "An integrated readout circuit for a transcutaneous oxygen sensing wearable device," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*, Mar. 2020, pp. 1–4.
[89] "Percept™ PC Neurostimulator," *Medtronic*, 2020. [Online]. Available: https://www.medtronic.com/us-en/healthcare-professionals/products/neurological/deep-brain-stimulation-systems/percept-pc.html. [Accessed Apr.24, 2021].

VLADIMIR VAKHTER (Member, IEEE) received his Specialist (an equivalent to a combined Bachelor and M.S.) degree (with honors) in Electronics and Automation of Physical Machines from the Ural Federal University (UrFU), Russia in 2016. Being awarded by a Fulbright grant, he received his M.S. degree in Electrical and Computer Engineering from Worcester Polytechnic Institute (WPI), the U.S. in 2021. For two and a half years, Vladimir conducted research of luminescent and scintillation materials at UrFU. Thereafter for two years, he developed a special magneto-optical system for the analysis of ferromagnetic materials at the Russian Academy of Sciences. Vladimir's 4+ year professional experience includes working as an Electronics Engineer and as a Software Developer. Vladimir completed two short-term scientific internships in the Superconducting Quantum Circuits group at the Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany in 2014 and 2015. His Master's research at the Integrated Circuits and Systems Lab (ICAS) at WPI was focused on the security for wireless injectable, implantable, ingestible, and wearable resource-restricted biomedical devices.

BETUL SOYSAL (Member, IEEE) received her B.Sc. (with honors) degree in Electrical and Electronics Engineering from Middle East Technical University, Turkey in 2006 and the M.S. degree from Bogazici University, Turkey in 2010. She started her career as an IT Security Researcher in TUBITAK, the Scientific Research Council of Turkey. Betul was with TUBITAK from 2007 to 2016. She studied Cryptography, Embedded Device Security and ASIC Security; performed security evaluations for various product types, conducted side channel analysis and fault cryptanalysis for crypto devices and ICs; and performed threat modeling and risk analysis for large scale systems. Between 2017 and 2019, Betul was with HP Inc., where she started to work on a new topic, software security for low-level systems, secure boot, and recovery. Betul has been with Google since February 2019, focusing on Chromebooks and Chrome OS security. Her current research interests include run time user data protection and she has special interest in resource-restricted biomedical devices and connecting with these devices securely.

PATRICK SCHAUMONT (Senior Member, IEEE) is a Professor in Computer Engineering at WPI. He received the Ph.D. degree in Electrical Engineering from UCLA in 2004 and the MS degree in Computer Science from Ghent University in 1990. He was a staff researcher at IMEC, Belgium from 1992 to 2000. He was a graduate student and postdoc at UCLA from 2001 to 2005. He was a faculty member with Virginia Tech from 2005 to 2019. He joined WPI in 2020. He was a visiting researcher at the National Institute of Information and Telecommunications Technology (NICT), Japan in 2014. He was a visiting researcher at Laboratoire d'Informatique de Paris 6 in Paris, France in 2018. He is a Radboud Excellence Initiative Visiting Faculty with Radboud University, Netherlands from 2020. His research interests are in design and design methods of secure, efficient, and real-time embedded computing systems. He served as program co-chair for several conferences in cryptographic and secure engineering, including CHES, HOST, ASHES, and FDTC. He received the National Science Foundation CAREER Award in 2007.

ULKUHAN GULER (Senior Member, IEEE) is an assistant professor of Electrical and Computer Engineering at Worcester Polytechnic Institute (WPI), MA, USA. She was a postdoctoral researcher at Georgia Tech, GA, USA. She received the B.Sc. degree in Electronics and Telecommunication Engineering from the Istanbul Technical University, Istanbul, Turkey, the M.E degree, in Electronics Engineering from the University of Tokyo, Tokyo, Japan, and the Ph.D. degree in Bogazici University, Istanbul, Turkey. Her research interests lie in the broad area of circuits and systems, and her primary area of interest is analog/mixed-signal integrated circuits. More specifically, she is interested in the circuit design of sensing interfaces, energy harvesting and wireless power transmission systems, and security for applications in healthcare. She is the recipient of the 2020 outstanding presentation award sponsored by the Interstellar Initiative. She is a member of CICC and BioCAS TPC and co-chair of the outreach committee of CICC'21.