Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey

Carmen Camara[a,b], Pedro Peris-Lopez[a,*], Juan E. Tapiador[a]

[a] *Department of Computer Science, Universidad Carlos III de Madrid, Avda. Universidad 30, 28911 Leganés, Madrid, Spain.*
[b] *Center for Biomedical Technology, Technical University of Madrid (UPM), Campus Montegancedo, 28223 Pozuelo de Alarcón, Madrid, Spain.*

Abstract

Bioengineering is a field in expansion. New technologies are appearing to provide a more efficient treatment of diseases or human deficiencies. Implantable Medical Devices (IMDs) constitute one example, these being devices with more computing, decision making and communication capabilities. Several research works in the computer security field have identified serious security and privacy risks in IMDs that could compromise the implant and even the health of the patient who carries it. This article surveys the main security goals for the next generation of IMDs and analyzes the most relevant protection mechanisms proposed so far. On the one hand, the security proposals must have into consideration the inherent constraints of these small and implanted devices: energy, storage and computing power. On the other hand, the proposed solutions must achieve a balance between the safety of the patient and the security level offered, with the battery lifetime being another critical parameter in the design phase.

Keywords: Implantable Medical Devices, Security, Privacy, m-Health, Survey

1. Introduction

Implantable Medical Devices (IMDs) are electronic devices implanted within the body to treat a medical condition, monitor the state or improve the functioning of some body part, or just to provide the patient with a capability that he did not possess before [47]. Current examples of IMDs include pacemakers and defibrillators to monitor and treat cardiac conditions; neurostimulators for deep brain stimulation in cases such as epilepsy or Parkinson; drug delivery systems in the form of infusion pumps; and a variety of biosensors to acquire and process different biosignals.

*Corresponding author
Email addresses: carmen.camara@ctb.upm.es (Carmen Camara), pperis@inf.uc3m.es (Pedro Peris-Lopez), jestevez@inf.uc3m.es (Juan E. Tapiador)

Some of the newest IMDs have started to incorporate numerous communication and networking functions—usually known as "telemetry"—, as well as increasingly more sophisticated computing capabilities. This has provided implants with more intelligence and patients with more autonomy, as medical personnel can access data and reconfigure the implant remotely (i.e., without the patient being physically present in medical facilities). Apart from a significant cost reduction, telemetry and computing capabilities also allow healthcare providers to constantly monitor the patient's condition and to develop new diagnostic techniques based on an Intra Body Network (IBN) of medical devices [9, 10, 105].

Evolving from a mere electromechanical IMD to one with more advanced computing and communication capabilities has many benefits but also entails numerous security and privacy risks for the patient. The majority of such risks are relatively well known in classical computing scenarios, though in many respects their repercussions are far more critical in the case of implants. Attacks against an IMD can put at risk the safety of the patient who carries it, with fatal consequences in certain cases. Causing an intentional malfunction of an implant can lead to death and, as recognized by the U.S. Food and Drug Administration (FDA), such deliberate attacks could be far more difficult to detect than accidental ones [30]. Furthermore, these devices store and transmit very sensitive medical information that requires protection, as dictated by European (e.g., Directive 95/46/ECC) and U.S. (e.g., CFR 164.312) Directives [54, 106].

The wireless communication capabilities present in many modern IMDs are a major source of security risks, particularly while the patient is in open (i.e., non-medical) environments. To begin with, the implant becomes no longer "invisible", as its presence could be remotely detected [20]. Furthermore, it facilitates the access to transmitted data by eavesdroppers who simply listen to the (insecure) channel [44]. This could result in a major privacy breach, as IMDs store sensitive information such as vital signals, diagnosed conditions, therapies, and a variety of personal data (e.g., birth date, name, and other medically relevant identifiers). A vulnerable communication channel also makes it easier to attack the implant in ways similar to those used against more common computing devices [65, 69, 83], i.e., by forging, altering, or replying previously captured messages [43]. This could potentially allow an adversary to monitor and modify the implant without necessarily being close to the victim [85]. In this regard, the concerns of former U.S. vice-president Dick Cheney constitute an excellent example: he had his Implantable Cardioverter Defibrillator (ICD) replaced by another without WiFi capability [114].

While there are still no known real-world incidents, several attacks on IMDs have been successfully demonstrated in the lab [44, 73]. These attacks have shown how an adversary can disable or reprogram therapies on an ICD with wireless connectivity, and even inducing a shock state to the patient [33]. Other attacks deplete the battery and render the device inoperative [52], which often implies that the patient must undergo a surgical procedure to have the IMD replaced. Moreover, in the case of cardiac implants, they have a switch that can be turned off merely by applying a magnetic field [79]. The existence of this

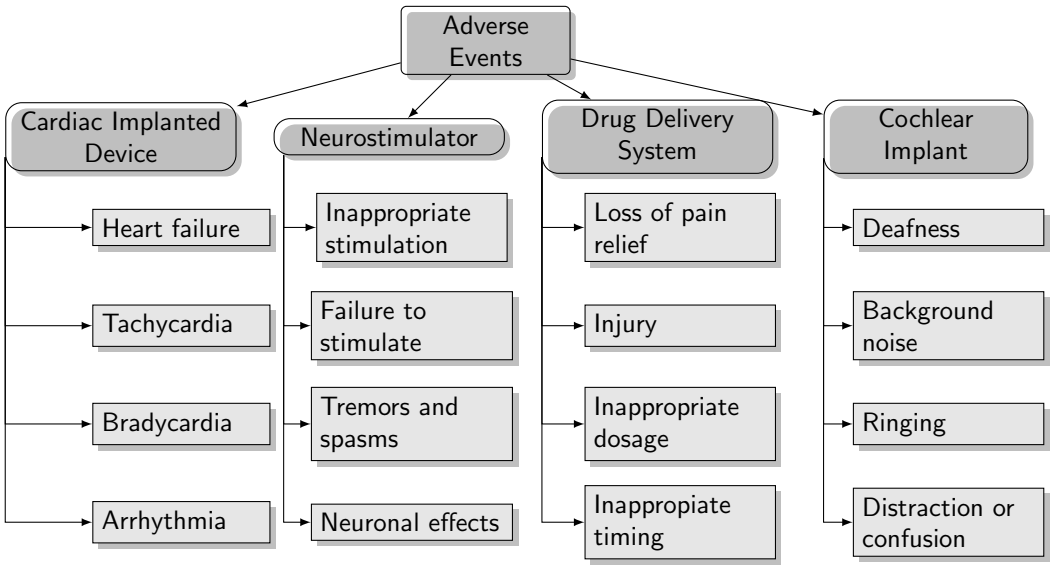

Figure 1: Adverse events for four representative IMD types.

mechanism is motivated by the need to shield ICDs to electromagnetic fields, for instance when the patient undergoes cardiac surgery using electrocautery devices [19]. However, this could be easily exploited by an attacker, since activating such a primitive mechanism does not require any kind of authentication.

The exploitation of a vulnerability in the IMD by an attacker can cause negative medical effects to the patient. Such effects are commonly known as "adverse events". Since each type of implant is devoted to treat a particular medical condition, the adverse effects that can be originated if the attacker succeeds are very varied [47]. In Fig. 1 we enumerate some of the damages an adversary could cause on a patient for the most commonly used IMDs. Attacks and their associated adverse events can be studied from both their extent and persistence point of view. The former measures the number of affected entities in the overall system, such as the IMD, the patient, other implants within the patient's IBN, and other devices outside it. The latter distinguishes whether the effects of the attack are temporary or permanent.

In order to prevent attacks, it is imperative that the new generation of IMDs will be equipped with strong mechanisms guaranteeing basic security properties such as confidentiality, integrity, and availability. For example, mutual authentication between the IMD and medical personnel is essential, as both parties must be confident that the other end is who claims to be. In the case of the IMD, only commands coming from authenticated parties should be considered, while medical personnel should not trust any message claiming to come from the IMD unless sufficient guarantees are given.

Preserving the confidentiality of the information stored in and transmitted by the IMD is another mandatory aspect. The device must implement appropriate

security policies that restrict what entities can reconfigure the IMD or get access to the information stored in it, ensuring that only authorized operations are executed. Similarly, security mechanisms have to be implemented to protect the content of messages exchanged through an insecure wireless channel.

Integrity protection is equally important to ensure that information has not been modified in transit. For example, if the information sent by the implant to the Programmer is altered, the doctor might make a wrong decision. Conversely, if a command sent to the implant is forged, modified, or simply contains errors, its execution could result in a compromise of the patient's physical integrity.

Technical security mechanisms should be incorporated in the design phase and complemented with appropriate legal and administrative measures. Current legislation is rather permissive in this regard, allowing the use of implants like ICDs that do not incorporate any security mechanisms. Regulatory authorities like the FDA in the U.S or the EMA (European Medicines Agency) in Europe should promote metrics and frameworks for assessing the security of IMDs. These assessments should be mandatory by law, requiring an adequate security level for an implant before approving its use. Moreover, both the security measures supported on each IMD and the security assessment results should be made public.

Prudent engineering practices well known in the safety and security domains should be followed in the design of IMDs. If hardware errors are detected, it often entails a replacement of the implant, with the associated risks linked to a surgery. One of the main sources of failure when treating or monitoring a patient is precisely malfunctions of the device itself. These failures are known as "recalls" or "advisories", and it is estimated that they affect around 2.6% of patients carrying an implant. Furthermore, the software running on the device should strictly support the functionalities required to perform the medical and operational tasks for what it was designed, and no more [34, 72, 112].

Overview and Organization: In this paper, we present a survey of security and privacy issues in IMDs, discuss the most relevant mechanisms proposed to address these challenges, and analyze their suitability, advantages, and main drawbacks. Throughout this work, we will find typical security issues such as eavesdropping, spoofing, or man-in-the-middle attacks, as well as classical problems like how to appropriately distribute cryptographic keys or how to control accesses in a secure but flexible manner.

We start by providing an overview of current IMD technology in Section 2, including current standards for telemetry. Then, in Section 3 we discuss typical usage scenarios for patients carrying IMDs and the associated threat model, paying special attention to the various adverse events that could arise as a consequence of attacks against the implant. Subsequently in Section 4 we describe various trade-offs that should be taken into account when designing mechanisms to preserve security and privacy in IMDs. Such trade-offs are intimately related to the scarcity of resources in the implant and to the need to guarantee the patient's safety even if this means that security mechanisms should be bypassed in some circumstances. Section 5 describes and analyzes a variety of security and privacy solutions specifically proposed for IMDs, ranging from mechanisms

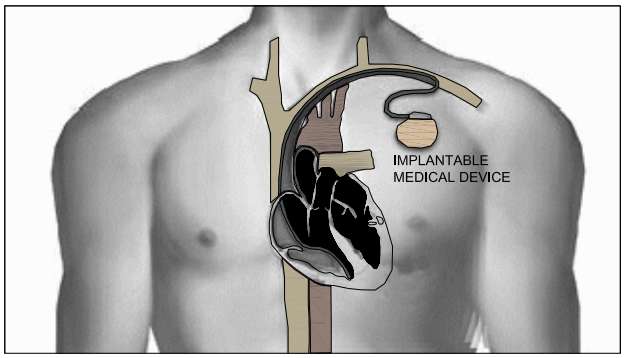

Figure 2: Implantable Medical Device: Pacemaker

to protect the communication channel to access control models tailored for this domain. Finally, Section 6 summarizes the main issues introduced in this paper and discusses open problems and avenues for future research.

2. Implantable Medical Devices

An IMD is often defined as an electronic device that is permanently or semi-permanently implanted on a patient with the purpose of treating a medical condition, improving the functioning of some body part, or providing the user with a capability that he did not possess before [47]. These devices are often implanted around 2-3 cm under the patient's skin and connected to the organ that needs treatment or monitoring. Cardiac implants (see Fig. 2) are possibly the most widely known example of IMDs, but many others are increasingly being used to deal with different medical conditions more efficiently than by traditional methods. The most common types include:

Cardiac Implanted Devices These include devices such as Implantable Cardioverter Defibrillators (ICD) and Pacemakers. They are designed to treat cardiac conditions by monitoring the heart's electrical activity and applying electrical impulses of suitable intensity and location in order to make the heart pump at the desired speed [122]. New models are equipped with pressure sensors capable of actively monitoring changes that could lead to a heart failure. This allows to alert the patient or the medical personnel if a pressure increment in the ventricle is detected, as this represents a hazard condition for the patient.

Cardiac implants may also be equipped with accelerometers to measure the patient's physical activity level. This can be set as an input parameter to the IMD controller, allowing to adjust the cardiac stimulation frequency to the one that best suits each moment [109].

Neurostimulators These devices transmit low-amplitude electrical signals through one or more electrodes placed in different locations of the brain. These

electrodes are implanted in very specific areas depending on the patient's condition. The process is known as Deep Brain Stimulation (DBS) and allows to treat a variety of pathologies such as Parkinson, dystonia, epilepsy, or even depression that, in some cases, are resistant to medication after several years of treatment [75].

Drug Delivery Systems (DDS) A DDS consists of a pump and a catheter that are surgically implanted under the skin. Their function is to supply medication in a controlled, localized, and prolonged way. Since the medication goes directly to the target area, an infusion pump provides a considerable degree of control, which allows to use a lower dose than that required with oral medication. For instance, this type of implants have been successfully used to mitigate pain in cases of cancer where traditional medication does not have good results [68].

Biosensors The implant consists of a sensor or a set of sensors placed inside the human body to monitor any part of it. They are capable of measuring certain physiological parameters and use such measures to make decisions. In this sort of implants there exists a special device that acts as a control node, communicating with the sensors and with other external entities (e.g., a programmer). The set of sensors and the control node are often regarded as a wireless biosensor network [13, 24, 116].

2.1. The New Generation of IMDs with Telemetry

Healthcare systems incorporating numerous communication and networking functions have proliferated over the last years. This has made possible to develop medical sensor networks that, for instance, can monitor patients in their own homes [98, 87, 124, 107]. Doctors, caregivers, or even the patient himself can thus conduct a continuous and more flexible control of his state, as well as access medical data remotely, communicate during an emergency, and even command various household appliances. This also promotes the autonomy of patients who, in many situations, are elderly people or individuals with reduced mobility.

Similar communication and networking capabilities are increasingly being embedded into IMDs. Equipped with a radio transmitter, the IMD can communicate with an external device—generally known as "Programmer" or "Reader"—and send it physiological data such as electrocardiogram (ECG) signals in the case of pacemakers and ICDs, that the doctor can use to track the patient's pathology. Apart from querying sensed data, the Programmer can also command the IMD to adjust or disable therapies, perform software updates, etc.

Augmenting IMDs with wireless communication and networking capabilities has significant advantages, including:

- It allows to constantly monitor the patient's physiological parameters and other symptomatology captured by the device, which reduces the time needed to regularly tracking medical conditions and, furthermore, causes less disruptions in the patient's daily activities.

- Enhanced supervision and management of the IMD operation, which allows to address any problem that might arise and apply adequate correction measures in a shorter time.

- The two previous items also imply a reduction in the overall costs involved in tracking the patient's condition and managing the operation of the IMD.

- In the case of future IntraBody Networks (IBN) [9, 10, 105], computation and analysis tasks could be shared among different networked devices, which will contribute to the development of new diagnostic techniques.

In their current generation, not all types of IMDs support access to all their available functions through the wireless communication channel. The vast majority of IMDs can be reprogrammed remotely, which allows the doctor to modify therapies as required. The reverse link (i.e., from the IMD to the Programmer) is not present in all of them. For instance, while pacemakers and ICDs can communicate in both directions, current neurostimulators can only receive reprogramming commands but they do not provide any information (e.g., sensed data) back to the Programmer. This fact has caused that most research works on advanced computational and networking issues related to IMDs, including the security and privacy problems addressed in this paper, are commonly focused on cardiac implants. Nevertheless, new IMD designs are computationally more complex and are increasingly basing part of their functionality in the ability to communicate externally to perform diagnostic and therapy tasks.

The main standards regulating telemetry for medical devices are:

- Many non-implantable medical devices are compliant with the Wireless Medical Telemetry Services (WMTS) specification, which sets three operating frequency bands: 608-614 MHz, 1395-1400 MHz, and 1427-1432 MHz [12, 46]. This is a U.S. standard defined by the Federal Communications Commission (FCC) in 2000 that is not internationally agreed, hence that its use is often restricted to the U.S. only.

- IMDs operate under the Medical Implant Communication System (MICS) specification, which operates in the 402-405 MHz band. MICS is a low-power (25 microwatt), unlicensed mobile radio service that facilitates data communications between the IMD and an external programmer. The communication range is about 2 m and the bandwidth is very low when compared with wireless communication technologies such as bluetooth or WiFi. The radio signals can go through and be transmitted within the human body due to its conductive characteristics. The purpose of these communications can be accessing the measures taken by the implant or reconfiguring it to, for example, adjust the treatment. MICS compliant IMDs have proliferated in the last years, including pacemakers, ICDs, neurostimulators, hearing aids, and DDSs [11, 26, 100].

- Similarly to the WMTS specification, the Medical Device Radiocommunications Service (MedRadio) defines communication services for both im-

planted and wearable medical devices. The specification, which was approved by the FCC in 2009 [85], extends the MICS spectrum 1 MHz in both sides, covering a frequency band from 401 to 406 MHz. The use of these frequencies in IMDs is well justified [16]: 1) At those frequencies, radio signals can easily propagate within the human body; and 2) The 401-406 MHz band is compatible with international regulations and does not interfere with other radio operations in the same band.

Incorporating a wireless communication capability into an implant involves some special requirements that affect their design. One of the most important is that the radio frequency module must consume very little power (e.g., 10 mW and up to 100 mW for a glucose and ECG monitor, respectively [48]) in order to save the implant battery life. Additional design factors include the required communication range (typically from 1 up to 5 meters [118]), the data transfer rate (e.g. 0.1 bps and up to 10 Kbps for a glucose and ECG monitor, respectively [48]), the environmental conditions in which the IMD will operate, and its size and cost [55, 56, 127].

Recently, the FDA has published guidelines for the industry on the design, testing, and use of wireless medical devices [27]. As stated, the security of wireless signals and data is an important issue in order to protect access to patient's data and hospital networks, and to prevent unauthorized communications with medical devices like IMDs or Programmers. Wireless medical devices must use cryptographic techniques (ive., encryption, authentication, secure key storage) to protect communications and accesses. The necessary security level is determined by the sort of threats, and their probability, to which the device is exposed, as well as the operating environment and the consequences/damages on the patient in case of a security incident. For the design of secure solutions, the FDA suggests that wireless medical devices include security measures to protect communications and accesses but also include software protections. Nowadays, the FDA is currently working on the design of recommendations for the management of cybersecurity in medical devices [28]. Apart from the FDA, other organizations are contributing to the elaboration of standards (e.g., X.1120 and X.1139), including tele-biometrics, mobile secure transmissions, secure transmission of personal health information, etc. [62].

3. Security Assumptions

In this section we first present the system model and then describe the usage scenarios. After that, the threat model is explained and finally the different types of adversaries are introduced.

3.1. System Model and Usage Scenarios

Fig. 3 presents the main entities involved in the system and shows the possible communication interactions (linked to the usage scenarios) between these devices. The IMD will communicate with a Programmer, which will be any entity/device authorized to interact with the implant (e.g., medical personnel).

In normal operation (i.e., while the implant has not detected an emergency situation [100]), the Programmer has to initiate the communication with the IMD as stated by the FCC regulations. Since the radio channel is a shared communication medium, the programmer will listen to the channel until it detects that is not busy to establish the communication. The goal of this communication is either requesting data (e.g., ECG signals or insulin levels) or sending commands (e.g., treatment modifications). In the case of secure solutions, the IMD and the Programmer are authenticated and sensitive data is passed encrypted on the channel.

Apart from the direct communication between the IMD and the Programmer, some authors have introduced the idea of using an external device (e.g, cloaker [22], shield [37], IMDGuard [125], etc.), which acts as a proxy. In this case, rather than establishing a direct connection with the Programmer, the IMD can delegate this task to an external device that authenticates the Programmer—initially there is a secure pairing between the IMD and the external device. Once the Programmer is authenticated (normal mode operation), this can communicate with the IMD using an encrypted channel via the external device. In emergency mode, the IMD has to answer even if the authentication fails—and, in some cases, the medical personnel must be able to disable the device easily.

As the patient will generally move about different locations and may visit several doctors and hospitals, IMDs will not always communicate with the same, previously known device. Furthermore, the entities authorized to communicate with the implant can vary [43]. Potential attackers must be also considered, as not all signals received by the IMD will actually come from an authorized Programmer and, in many cases, their purpose could be malicious. Under these conditions, guaranteeing the security and privacy of the IMD and its data is essential to protect the safety of the patient.

As described above, an IMD must operate under two different modes: normal and emergency. One major objective is to find a sensible trade-off between these two possible situations:

A. **Security in normal operation mode**. The patient controls what entities can interact with his IMD. In this case, it is necessary to implement both a strong access control mechanism and cryptographic protocols in the communication link to thwart malicious and unauthorized accesses. The IMD must ignore indiscriminate data requests or device reprogramming commands. Ideally, the implant should be undetectable to unauthorized parties. Security mechanisms might be similar to those used in constrained devices like RFID tags or smart sensors (e.g., lightweight hash functions [4, 5, 41] or tiny block ciphers [60, 66, 67]).
B. **Security in emergency mode**. As important as offering strong access control, secure communications, and even undetectability, is the ability of being accessible under an emergency condition. Consider a patient who enters an emergency room in a hospital different to the one he often visits. To further complicate matters, assume that the patient is visiting a

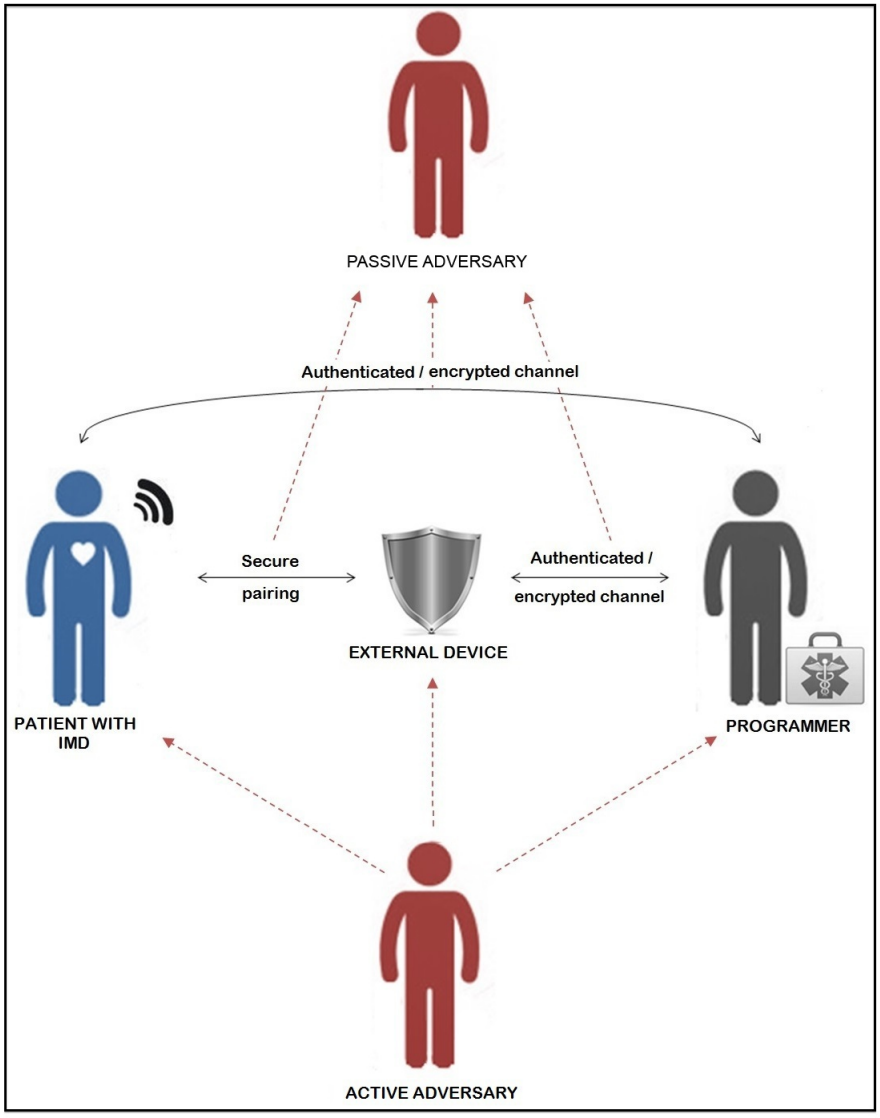

Figure 3: Typical usage scenario for IMDs

foreign county. Even under these circumstances, the healthcare staff must be able to communicate with the implant, determine its type (e.g., model and brand), extract physiological data or information about the treatment, and even update its configuration if required. Even in a secure scheme, under an emergency situation such as an urgent surgery of a patient who holds an ICD, in which it is mandatory to deactivate the implant, the IMD should always respond before deactivation.

To understand the importance of emergency conditions, it would be useful to know the frequency of occurrence of these events. Unlikely, there are not public reports about emergency conditions for patients holding an IMD. Nevertheless we can take a look inside the statistics of pacemakers, which are one the most popular IMDs, in order to shed some light on this matter. For instance, lead complications are one of the principal causes of re-intervention in patients with heart diseases. In a recent retrospective study [119] Walker et al. reported 1.4 events per 100 patient years of follow-up for lead-related complications (e.g, vein thrombosis, acute perforation or dislodgement) –this figure doubles whether the population under study are children [84]. For the pocket-related complications (e.g, infection, erosion or migration of the pacemaker), which is the other main cause of complications for pacemakers [40], the values are a bit higher (1.9 events for 100 patient years) in comparison to the lead complications. Furthermore the probability of re-intervention increases with every consecutive replacement [6]. We concur with the notion that re-intervention due to lead or pocket complications is not strictly an emergency condition since in the majority of the occasions the surgery is planned. Nevertheless, and due to the lack of any published report at least to the best of our knowledge, we propose to use this number as an upper threshold for the emergency events. Under this assumption, we can expect that the number of emergency conditions for IMDs may be less than 1-5 events per 100 patients. In the face of such emergency situations it is the job of manufacturers, engineers and physicians to evaluate the importance of that events. For that, long-term studies on the matter are required to address a rigorous risk analysis.

A straightforward solution for emergency conditions that provides the necessary safety to the patient is to force the IMD to disregard authentication and authorization mechanisms and process all incoming commands. Any requester thus becomes an authorized user, possibly with full privileges. This would not be possible if security protocols and strong access control mechanisms are not deactivated, which in turn leaves the implant fully exposed to attackers. Unfortunately, telling apart normal from emergency scenarios is far from trivial for the IMD, and nowadays the best way to provide an adequate security for IMDs is still an open problem. Security tensions between these two conflicting goals are thus created, hence the importance of finding solutions that balance the security requirements to provide security in normal mode while guaranteeing safety during emergencies [96]. Several works (see, e.g., [17, 10, 55]) have proposed schemes in which the IMD can only be accessed by authorized entities and remain invisible for the remaining ones. The prevailing philosophy in most

works is that in case of doubt about the patient's safety, security mechanisms should be relaxed and access must be granted. We will discuss in detail the most relevant proposals in this field later in Section 5.

3.2. Threat Modeling

Security threats against the IMD can be categorized using the STRIDE methodology. The acronym stands for six general categories of attacks: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. Table 1 relates each category with the security property attacked in each case and provides some examples. Generally it is assumed the following set of relations (i.e., security property - threat): spoofing – authentication, integrity – tampering, non-repudiation – repudiation, confidentiality – information disclosure, availability – denial of service, authorization - elevation of privileges. Apart from these one-to-one connections, it should be noted that some threats may address various properties simultaneously, or that a single attack can be decomposed into individual threats.

The six security properties addressed above have their usual meanings, although focused on the IMD domain:

Authentication The identity of parties must be correctly established before performing any other operation. Within the domain of implantable medical devices, any device in the system (IMDs, Programmer or External device) can be impersonated. For instance, if the identity of the Programmer is supplanted it might be the starting point for an elevation of privileges attack.

Integrity Data, either stored in the device or being communicated through the wireless link, can only be modified by authorized parties. If there is not integrity checking mechanism on the IMD, data could be altered during the transmission over the insecure radio channel. Furthermore the IMD could accept malicious inputs, which could be employed to run a code injection attack [94]. On the other hand the lack of integrity checking would facilitate that the manipulation of the data stored on the IMD memory might be not detected –or be detected in a distant future.

Non-repudiation Operations performed by/on the IMD are kept securely in an access log. The attacker could focus on delete these inputs in order to cover her traces. On the other hand no all IMDs are equipped with a log system. If this were the case the adversary could repeatability try to gain access to the IMD without leaving any trail. Even if a log system is present the events would be logged but no alarm would be triggered to alert the IMD holder in case of a malicious event.

Confidentiality Data, either stored in the device or being communicated through the wireless link, can only be read by authorized parties. In particular, IMDs and the Programmer communicate through the radio channel (401-406 MHz) and these communications are exposed to eavesdroppers. If

Table 1: STRIDE categories and examples in the IMD domain.

Security Property	**Threats**	
Authentication	Impersonate the Programmer Impersonate the IMD Impersonate the external device	Spoofing
Integrity	Patient data tampering Malicious inputs Modify communications	Tampering
Non-repudiation	Delete access logs Repeated access attempts	Repudiation
Confidentiality	Disclose medical information Determine the type of IMD Disclose the existence of the IMD Track the IMD	Information Disclosure
Availability	Drain the battery of the IMD Interfere with the IMD communication capabilities Flood the IMD with data	Denial of Service
Authorization	Reprogram the IMD Update the therapy of the patient Switch-off the IMD	Elevation of privileges

communications are not encrypted, an adversary could disclose private information such as the IMD model or even medical information of the patient. This would compromise the privacy (data) of the implant holder. Even if communications are encrypted, an attacker could detect the presence of the implant or, even worse, track the movements of its holder. In this case the privacy location would be put at risk.

Availability The services offered by the IMD should be available to authorized parties at all times. Availability is crucial for IMDs since these devices are devoted to treat medical conditions of their holders. Unfortunately, an IMD could be rendered inaccessible through the blockage of the radio channel (active jamming). Alternatively the device might be overloaded by flooding the IMD with network traffic over the radio channel. This could be used to block the access to the device or to drain its battery. If the battery runs out of power, the device would become permanently

inaccessible and the patient's health could be at risk.

Authorization An operation must be executed only if the requester has sufficient privileges to order it. For instance, therapy parameters (e.g., voltage, current, thresholds, operation mode, etc.), cannot be updated by the patient and only doctors should be able to modify these. In this regard, re-programming the IMD must be done under the joint supervision of the doctor and a technician (typically from the manufacturing company of the IMD). On the other hand, the IMD must be kept running at all times and only be switched off under special circumstances that may threat the patient's life (e.g., cardiac surgery with electrocautery devices). In the case of pacemakers, a magnetic field has to be applied near the device (over the patient chest) and this procedure must be authorized by the cardiologist.

3.2.1. Types of Attackers

At high level, attackers can be grouped into two main categories: *active* and *passive* (see Fig. 4):

Passive Eavesdropper A passive attack can only listen to the channel and, therefore, getting access to the messages exchanged between the IMD and the Programmer. Assuming an insecure radio channel, a passive attacker is a direct threat to confidentiality and may threaten authentication. By just reading messages a passive attacker may determine whether a person carries an implant or not; find out what type of implant and other data such as its model, serial number, etc.; capture telemetry data and disclose private information about the patient, such as the ID of his health records, name, age, conditions, etc. In all cases, the overall result is a serious compromise of the patient's privacy.

Active Adversary In this case, the adversary is not only capable of capturing messages exchanged over the radio channel, but also to send commands to the IMD, modify messages in transit before they reach the IMD or the Programmer, or just block them so that they never arrive. Attacks may involve a sequence of interceptions, interruptions, modifications, and generation of messages. The goals pursued by an active attacker are diverse. For example, he could indiscriminately request information from the IMD with the purpose of draining its battery. He could also attempt to modify the configuration of the device, disable therapies, or even induce a shock state to the patient [44].

It must be noted that it is not essential for the attacker (active or passive) to be physically close to the patient to conduct the attack [31]. Depending on the specific communication technology used for the radio link, the IMD could be reachable from a few meters (typically 1-2 meters for MICS and WMTS [86, 118] or even up to 10 meters in case of using advanced communication techniques [49]). Furthermore, communication devices can be acquired very easily nowadays; e.g., certain smartphones can perform this task.

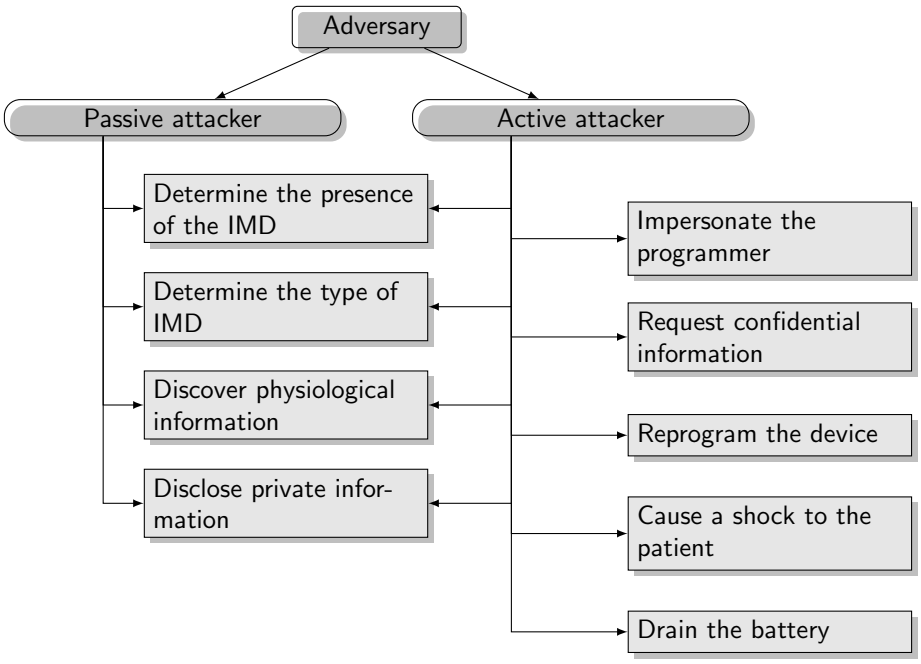

Figure 4: Passive vs active adversaries.

In summary, the technical means needed to carry out most attacks against IMDs are cheap and easy to acquire and use. As a consequence, passive attackers can easily eavesdrop sensitive information about an implant holder without much difficulty. Even if the attacker is not someone who attempts to threaten the patient's safety, the data stored on it might be very valuable for many individuals and organizations.

It is worth mentioning that the attacker could be the patient himself in a deliberate or involuntary attempt to sabotage his own implant. An example of this was reported in [89], where it is described how a patient who sent unauthorized commands to his insulin pump in order to gain unsupervised use of it ended up with a medical condition as his manipulation resulted in the ingestion of a very high dose of medication.

Finally, apart from general system and channel vulnerabilities, attackers can exploit a number of IMD-specific features to achieve their goals [1, 47]:

- *Exploiting proximity*, where proximity refers to the distance between the attacker and the IMD. Many current proposals have some form of distance-based access control, allowing access to the IMD only if the Programmer is in short range. The rationale here is to force the attacker to be physically very close to the patient to conduct the attack. In practice, however, the attacker may use a compromised device in the proximity of the patient to launch the attack, including those used in medical facilities.

- *Exploiting the IMD functions.* IMDs are programmed to perform various activities such as sensing biomedical parameters in the body area where they are implanted, treat a medical condition (actuating), processing gathered data, and communicate with other devices, either external or those in the IBN [129]. These functions can be misused by an attacker, for example by inducing an incorrect sensing to trigger a particular response in the implant.

- *Exploiting the patient's status.* As we will discuss later, the patient's status plays a key role in the design of many countermeasures. For instance, an implanted biosensor can trigger an alarm if certain parameters fall out of the safety range. In some cases, such an alarm puts the IMD in emergency mode and automatically disables access control mechanisms.

4. Limitations and Trade-offs

In this Section, we first introduce a number of technological limitations of current IMDs that restrict the sort of security mechanisms that can be implemented on them. We next describe various trade-offs that arise when designing security measures for IMDs and that originate as a consequence of the IMD's computational limitations, the criticality of some of its functions, and the need to support an emergency mode of operation.

4.1. Limitations

IMDs have restricted capabilities in three separate dimensions: energy, storage, and computing power. All three of them have security implications, either because they can be misused or because they limit the security mechanisms that can be afforded. We next discuss them in more detail.

Energy IMDs are powered by an integrated battery that supplies energy to all functions incorporated in the device (i.e., monitoring, treatment, communication, etc.). Once the IMD is implanted, the battery can last from 8 years in the case of neurostimulators [81] up to 10 years in the case of pacemakers [76]. Battery usage has a direct impact over the implant lifetime. Once exhausted, it has to be replaced, which requires a surgical procedure with its associated risks. Some designs support batteries that can be charged wirelessly using magnetic fields, but organs close to the implant could be damaged. Some recent advances in this area can be found in [63, 108, 126].

Storage Storage is quite limited in current IMDs. The memory available in the device is used to store historical data from different events and episodes that arise related with the patient's pathology. For instance, pacemakers and ICDs store ECG signals that occurred when the device decided to apply stimulation. The RAM memory of these device varies from 2 KB to 36 KB for the former, and from 128 KB to 1024 KB for the latter. In the

case of ICDs, around 75% of this memory is devoted to store ECG signals [61]. Devices with low sensing rate like a Biostator Glucose Controller demand 8 Kb for data storage [111]. One consequence of incorporating a reduced memory on-chip is that security mechanisms have to consume as little memory as possible in order to save it for the potential storage requirements required by the medical functions of the device.

Computing and Communication Both computing and communication capabilities are extremely limited in IMDs due to power restrictions. Communication is the most energetically expensive task for the IMD. Hence, if communications are minimized, the battery life can be extended [99, 102]. As for computation, these are generally supported by a tiny microcontroller. For instance, the micro of a neurostimulator consumes an area of around $5mm^2$, which is around forty times smaller than the area used for a general purpose microcontroller [58]. In general, the whole chip of the implant occupies an area of around several hundreds squared millimetres.

4.2. Tensions and Trade-offs

As described in Section 3, and IMD can work in two operation modes: normal and emergency. Mechanisms designed to preserve security and privacy properties in both modes must consider various tensions:

Security vs Safety Nowadays in a real scenario it is common to assume that all the actors, both the legitimate (new generation of IMDs, external devices and programmers) and the illegitimate ones (active and passive adversary) count with connectivity. This should lead to the inclusion of solid security solutions due to the possible security threats. In normal mode the IMD is vulnerable to a variety of attacks. Attackers could be physically situated at a long distance from the IMD and use its wireless communication capabilities—perhaps relying on a nearby proxy device—to receive data requests and perform update operations. Any proposed solution must guarantee basic security and privacy properties in this case. Nevertheless, during an emergency, the medical personnel must be able to access the implant rapidly and without restrictions. Thus, while the use of strong security measures could provide a high level of protection, it can also put at risk the patient's safety during an emergency situation. The trade-off between safety and security is one of the most critical aspects in the design of security mechanisms for IMDs. Nevertheless,

Battery Lifetime vs IMD Capabilities As discussed above, IMDs have severe restrictions in terms of energy consumption since extending the battery lifetime is an essential requirement. In turn, this also restricts the amount of computations and communications involved in security functions. This motivates the design of new security and privacy mechanisms that are not very demanding in terms of computation, communications, and storage. An interesting fact in this regard was pointed out in [85]:

power consumption increases drastically if the data transfer rate increases. Thus, although it may seem counterintuitive, it is preferable to rely on long transmissions at very low bit rate than on short data exchanges at high speed.

Several solutions have addressed the problem of saving or recharging the battery of IMDs to postpone as much as possible its replacement. For example, in [123] Warwick et al. present an innovative solution to provide higher intelligence to neurostimulators. The idea is to provide the implant with the capability to predict tremor conditions in Parkinsons' activity, so that only in that precise moment an stimulation on the sub-thalamus is triggered. Once the tremor has diminished, the implant stops the stimulation. Intelligent solutions like these could prolong the lifetime of the battery.

Other approaches have suggested techniques to recharge the battery wirelessly. In [117], Arx and Najafi propose to provide the implant with receiver (planar spiral) coils and accompanying circuitry that are capable of receiving transmitted power from a few centimetres away. Another example can be found in [109], where an inductor with a parallel chip capacitor is proposed. In this system, the inductor radiates energy by coupling a signal at the resonant frequency (300 Mhz in this proposal). These systems would allow the IMDs to work without any battery, which would be highly desirable since the battery replacement procedure would be avoided [130].

Using a different approach, Wang and Song proposed to transform mechanical energy obtained from the movement of the patient's muscles into electrical energy [120]. Using this technology, the IMD could be automatically and continuously recharged by the patient's physical activity.

Unfortunately, neither these solutions nor others recently proposed (e.g., [63, 108, 126]) can be nowadays found implemented in commercial IMDs. Therefore, any security measure for implants must take into account existing energy restrictions and potential impacts on the battery life. Furthermore, as there are attacks that pursue to waste the battery of the IMD, security functions should not make this easier (e.g., by allowing the attacker to drain the battery by misusing security mechanisms).

Answering Time If the interaction with the implant takes too much time because of the overhead imposed by security controls, the patient's safety could be put at risk. Such controls should be analyzed to guarantee that their worst-case latency is within a reasonable range.

In summary, tensions between safety (i.e., guaranteeing access in critical conditions) and security (allowing access only to authorized entities), coupled with the restrictions present in current IMD platforms, introduce unique challenges in the development of adequate security mechanisms for IMDs. Adapting solutions proposed for other similar environments (e.g., wireless sensor networks) is not

straightforward, since questions such as how security mechanisms should behave in emergency mode—and, most importantly, guaranteeing that the existence of this mode is not abused by an attacker—are still open problems.

5. Protection Measures

In this section, we discuss different security mechanisms that have been proposed to thwart security threats in IMDs. Many of these proposals explicitly address the trade-offs and tensions previously discussed, while others simply focus on counteracting specific attacks. The majority are preventive and attempt to stop attacks from happening in the first place, although detection and correction mechanisms have been also suggested.

Ideally, the inclusion of security measures should not require any modification of the IMD, as this would imply its replacement and, therefore, a surgical procedure. The alternative would be implementing security functions in external devices or independent modules of the IMD chip. Under this approach, the software running on the implant would be exclusively used to treat the patient's medical condition.

As discussed above, a major problem with most security measures is that they could put at risk the patient's safety in emergency situations if they cannot be easily disabled. The use of some form of "backdoor" to bypass security could be a straightforward solution, though it is too easily manipulable by an attacker.

Fig. 5 provides a classification of the security mechanisms that will be discussed throughout this section.

5.1. No Security

Many IMDs, particularly the older generations without wireless communication capabilities, have no security mechanisms at all [78, 80]. This is unacceptable for the newest generations of IMDs in which the presence of communication capabilities may jeopardize the patient's safety.

5.2. Auditing

One of the simplest security mechanisms consists of constantly registering all accesses—authorized or not—together with the patient's status. This is a measure amied at facilitating the detection of non-permitted actions and constitutes a valuable source of evidences to take subsequent actions. Therefore, auditing helps to combat threats against non-repudiation. Unlikely, it does not prevent the occurrence of attacks, but may act as a deterrent element if appropriately implemented, i.e., if it is not possible for an attacker to compromise the audit log and if it facilitates attribution of the attack. As a consequence of this, this sort of solutions should be be complemented with appropriate mechanisms to detect and block such attacks, as well as measures to prevent them from happening in the first place (e.g., cryptographic or access control solutions).

The main problem that auditing proposals face is the limited amount of memory available in IMDs. For instance, the whole memory of an ICD is less

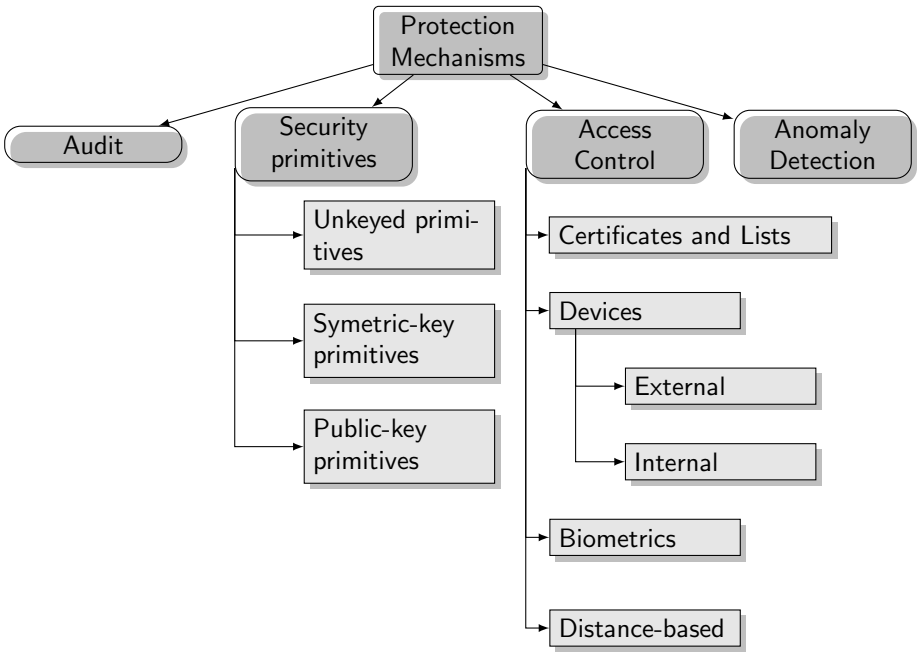

Figure 5: Protection mechanisms proposed for IMDs.

than 1 MB and around 75% of this memory is used for medical functions. In that a case, only a few hundreds kilobytes could be used for logging events, which is extermely restricted. An additional memory could be added to the chip, but this would increase the size of the IMD, which is not recommendable.

To avoid increasing the memory of IMDs, the logging task can rely on an external device without memory and computation limitations. One example in the context of RFID systems is "RFID Guardian" [93], which collects and analyzes evidences of all events that occur in a predetermined range. A similar approach, called MedMon, has been recently proposed for IMDs and e-Health applications [128]. The authors propose the use of an external device that works as a security monitor snooping and analyzing all communications to and from the IMD. The events are locally stored in the external device and an alarm could be raised to alert the patient. A more drastic solution can include blocking the communication channel if a dangerous communication is detected.

5.3. Cryptographic Measures

Cryptography-based security solutions strongly depend on cryptographic primitives, which can be categorized in three main groups [82], as shown in Figure 5. Unkeyed primitives, such as hash functions or one-way permutations, are cryptographic tools that do not use any key. Within the keyed cryptographic tools we can distinguish between symmetric-key and public-key primitives. In symmetric-key primitives a secret key is shared between the trusted entities.

The type of primitives in this category is varied including symmetric key ciphers (block and stream ciphers), message authentication codes (MACs), pseudorandom sequences and identification primitives. On the other hand, public-key ciphers and signatures are two examples of asymmetric-key primitives. In this type of algorithms two keys are used, one of them is public and the other one must be kept secret.

In the context of IMDs, cryptographic measures are effective mechanisms to protect the wireless communication channel and the records stored in the device against tampering and information disclosure. Additionally, cryptographic protocols also provide a means to control and manage accesses to the IMD, thus providing protection against spoofing and, in some cases, elevation of privilege attacks. Both symmetric [44, 55] and public-key [25, 110] schemes have been proposed for these applications, although the latter are considerably more expensive in terms of communication, computation, and power consumption. Protocols based on public-key cryptographic schemes often exchange a high number of messages, which makes them quite energy demanding since sending and receiving messages consume power. Furthermore, public-key ciphers result in complex circuits that consume excessive resources (hardware and memory) and are inefficient in terms of power consumption [35, 71]. Due to the resource limitations discussed above for the current generation of implants, solutions based on symmetric-key approaches are the preferred option. Standardized protocols like the one proposed in ISO/IEC 9798 rely on the use of symmetric primitives (i.e., symmetric encryption or keyed hash function) and the encrypted tokens include random numbers (a PRNG is often used for its generation) to guarantee freshness between sessions [59].

Symmetric cryptographic schemes suffer from the key distribution problem. In general, the IMD and other authorized devices such as the programmer need to share a key (or a set of keys) that is used to generate authentication tokens for gaining access to the IMD, and to encrypt communications. The suitability of a particular key distribution scheme depends on the type of IMD, the expected interactions with other parties, and other assumptions about the operational environment. For example, if the programmer and the IMD will have a lasting relationship, a pre-set key can be used. This solution could be valid when the programmer is always a device belonging to the patient or the physician. In these cases, a first approach consists of pre-loading a factor key on the authorized devices. This factor might be renegotiated between the legitimate parties during the first communication session to update the key. We emphasize here that is crucial to protect these keys and guarantee that only authorized entities (i.e., the patient and healthcare staff) have access to the them [104]. Such keys will be used to build various cryptographic tokens (e.g., an authenticated token or an encrypted message) used in the transactions between legitimate entities in the system.

Other solutions suggest that the cryptographic keys used by the IMD can be stored in an external wearable device such as a smart bracelet. Externalizing the key storage incurs a significant risk, as the loss of such a device (e.g., if the patient losses the bracelet or it gets damaged) would render the IMD inaccessible

and/or will facilitate access to unauthorized users [32]. Some authors propose to print the key into the patient's skin using ultraviolet pigmentation (i.e., invisible tattoos) that can be read by medical personnel in case of emergency [101]. Note, however, that the keys might be read by an attacker who has physical access to the patient—its presence may be detected due to its proximity.

In the case of sporadic communications with authorized devices that nonetheless do not know the access key, a key agreement protocol must be supported (e.g., RSA-based [110] or using physiological signals [115]).

Providing a confidential channel between the IMD and the programmer is another major goal when using cryptographic solutions. Some approaches suggest to exploit the limited coverage of the physical layer during the initialization phase [74]. Most proposals are based on symmetric ciphers [44], and some of them incorporate a key updating mechanism (e.g, a hash-chain based updating scheme [50]). Recently, Kaadan and Refai have proposed in [64] a novel cryptographic system with claimed military-grade security level that combines a one time pad cipher with a novel key distribution and authentication scheme. Other approaches, like the one discussed in [55], focus on hardware efficiency and propose the use of lightweight ciphers that offer tiny footprints with low power consumption. Recently, a new IMD architecture, evaluated on an artificial pancreas implant, has been proposed. In this case, the implant includes two separates cores (illness treatment and security tasks), and the overhead for the security module in terms of hardware and energy consumption is minimal [111].

The use of standard cryptographic solutions to provide security services in IMDs has been criticized, both for usability reasons and for the lack of rigour in the analysis of many proposals [96]. The main drawbacks that would entail the exclusive use of these solutions are [36]:

Inalterability Incorporating cryptographic mechanisms in the device implies that current implants must be re-designed and replaced. This will force patients to undergo a surgery procedure only to get a more secure device, as the treatment functions do not present any problem.

Patient's safety The use of cryptographic measures embedded in the device introduces some challenges for emergency situations in which the communication with the IMD is necessary even for unauthorized parties (i.e., programmers who does not know the access key). This problem is not present in solutions based on external devices such as those discussed later in Section 5.4.2.

Maintenance As security measures are implemented in the device, there is an increment in the amount of software embedded in the implant, which also implies a higher likelihood of errors. Many authors support the idea of restricting as much as possible the software running on the device, keeping just those functionalities needed to treat the medical condition for what it was designed.

5.4. Access Control

Access control mechanisms prevent unauthorized and inappropriate uses of the IMD functions. Prior to proceed with a particular action (e.g., access, reading, reprogramming, etc.), the privileges of the requester are evaluated with the aim of assessing whether it is authorized to execute that particular action or not. In particular, permitted and forbidden operations are governed through access control policies that establish who can do what, possibly depending on the context in which the access request takes place. Note that access control is fully compatible with other security measures such as cryptographic protocols to protect the communication channel. Furthermore, access control generally requires previous authentication, as decisions on whether an operation is permitted or not are made on the basis on the identity of the requester, who must be previously established.

We next describe a number of access control models suggested for IMDs and discuss their main advantages and limitations.

5.4.1. Certificates and Lists based solutions

In [32], the authors present two classical authentication mechanisms adapted for IMDs. One is based on Access Control Lists (ACLs)—an implementation of discretionary access control models based on the access matrix—, while the second relies on a Public Key Infrastructure (PKI). The ACL defines which operations an authenticated reader is authorized to execute. Such permissions are permanent once the ACL is programmed. Thus, although it can be reprogrammed in the future, it is intended for providing permanent access to certain readers. Contrarily, in PKI-based solutions the relationship between the IMD and the reader is transitory. In particular, the reader will have to repeat the procedure for obtaining its certificate to authenticate with the IMD in each new session.

In order to optimize the energy consumption in those cases where the reader communicates frequently with the IMD, the PKI and ACL approaches can be combined. For instance, the first time the reader is authenticated with the IMD, it will use its certificate. After that, this particular reader is registered in the ACL, since using this approach is more efficient in terms of energy consumption than PKI-based solutions.

One critical point is that the PKI and the certificate directories should be publicly—and permanently—accessible through the Internet. Consider, for example, a patient suffering an emergency condition while visiting a foreign country or just a different hospital. The medical personnel should be able to obtain the required credentials. Connectivity or authentication problems with the PKI may prevent them from gaining the required credentials to modify or disable the IMD, which in some cases may threaten the patient's safety. Therefore, the needed PKI is very demanding in the sense that is global and must be accessible by all the authorized actors in all possible locations at any time.

5.4.2. Delegation in External Devices

Some authors have suggested to make use of an external device to control accesses to the IMD. Such devices would not be implanted in the patient's body, and part or all of the security functions would be delegated to them. This presents several benefits. On the one hand, the IMD would save battery life since security-related computations are performed externally. On the other hand, a single device can integrate a number of security capabilities, such as auditing, key management, authentication, and access control. Furthermore, as most of these capabilities operate at the physical layer, other sort of solutions can be used at higher layers.

Generally, the role of the external device is to act as a mediator between the programmer and the IMD. When the programmer needs to access the IMD, it first gains access to the external device and then communicates with the IMD. In [22], the authors present a solution based on external devices named "Cloaker". The IMD periodically checks the presence of the Cloaker. While it is detected, the IMD remains silent. Therefore, the Cloaker will provide security to the patient while he holds it. Otherwise, the communications with the IMD are fully open to all readers. Using this approach, in an emergency condition it would suffice to remove the Cloaker from the patient to get full access to the device.

The authors of [22] provide a number of ideas about the role that such an external device could play. Two different possibilities are identified:

- The Cloaker would mediate in all exchanges until the IMD and the programmer successfully finish a key exchange. After that, both parties directly communicate with each other over a secure channel built using the shared key. The external device does not participate in such communications.

- A different possibility is having the Cloaker involved in all communications between the IMD and the programmer. In this case, all packets pass through it, which would allow to record them (for example, for a subsequent forensic analysis) and even implement filtering and attack detection functions. Note, however, that in this setting the Cloaker becomes a single point of failure, so any malfunction or degradation in performance will affect the availability of the IMD.

Solutions based on external devices such as the one presented in [22] attempt to balance the security tensions described in Section 4. Security mechanisms are offered only in normal operation and the safety of the patient is guaranteed in emergency conditions. Nevertheless, there are still some open questions that have not been definitely addressed, including:

- The constant detection of the Cloaker by the IMD is not trivial. The authors proposed two ways to do this. In the first case, the IMD sends a "hello" message to the Cloaker whenever an incoming message is detected. Another, more restrictive way consists of the IMD periodically sending

"hello" messages to the Cloaker to check its presence. The result is stored in just one bit that indicates whether the Cloaker is present or not.

- Both schemes discussed above are inefficient in terms of energy consumption as a consequence of the messages exchanged to check the presence of the external device. The first solution avoids a continuous flow of requests to the Cloaker, but renders the system more vulnerable since the adversary knows the exact time when the Cloaker would be interrogated. Thus, the attacker could send a fake request to the Cloaker and then impersonate it. Contrarily, the second approach is much more secure but requires the IMD to continuously check the presence of the Cloaker.

- The authors do not address the problem of how deal with an attack that causes interferences in the communication channel between the IMD and the Cloaker.

- Finally, it is worth mentioning that [22] is not a definite solutions and the authors do not recommend its immediate adoption.

Another solution based on external devices is "RFID Guardian", proposed in [93]. RFID Guardian registers all devices in its range, manages keys, authenticates programmers that request access to the IMD, and blocks all unauthorized entities. Using this approach, all the devices in the neighbourhood of the Guardian (i.e., about 1 or 2 meters according to [93]) are detected and corrective measures could be enforced if needed. Although the solution was originally proposed in the context of RFID systems, the approach can be easily adapted to IMDs. The authors propose to integrate the Guardian into a device that the user (patient) always holds, such as a smartphone or a smart wearable device (e.g., a watch, a bracelet, etc.).

Other approaches are based on the use of hardware tokens. There is a wide variety of these devices, including disconnected and connected tokens, smart cards, bluetooth tokens, etc. In this case, the device stores a password shared with the IMD. The medical personnel would use this key to access the implant. The main drawback is the same as in other solutions based on external devices: if the token is lost or the patient forgets to carry it under an emergency condition, the IMD would be inaccessible [3].

Gollakota et al. proposed the use of an external device, named "shield" [39, 38], that acts as an intermediary so that all communications between the IMD and the programmer pass through it. The shield protects the communication channel by jamming messages sent to and from the IMD in such a way that no other entity can decode them. Similarly, it protects the IMD from unauthorized devices by jamming all messages coming from them. Fraudulent messages are rendered unusable after the jamming and the IMD would discard them simply by its inability to interpret them, thus preventing the execution of malicious actions.

In summary, the main advantage of solutions based on external devices is that they offer a high protection level against unauthorized commands. The

IMD will not respond to malicious re-programming commands or attacks to drain the battery. Their main drawbacks include:

- If the patient forgets the external device, the IMD would respond to all incoming (authorized or not) requests, which is only necessary in emergency mode.
- These solutions do not generally consider scenarios in which the external device is replaced by a malicious one. In this case, the security and privacy of the IMD would be highly compromised.
- The external device is fully visible to external entities, which can reveal sensitive information about the patient's medical condition. Moreover, some authors have pointed out that it is a constant reminder to the patient about his medical condition.
- These proposals often assume that the external device is a trusted entity. Nevertheless, this entity can be compromised or act maliciously. For instance, packets can be altered (e.g., flipping certain bits), dropped out, or blocked, which would render inoperative the communication with the IMD.

5.4.3. Trusting other Implantable Devices

In [47] it is proposed the idea of using a subcutaneous button that opens access to the IMD only after being pressed. This approach would protect the implant from all incoming communications until the patient deliberately presses the button, which can be done only in controlled environments. Note, however, that this would fail to protect the IMD if the adversary has physical contact with the victim and can press the button, or leave an attacking device in the proximity of the patient waiting for the IMD to be accessible.

The same authors also present the notion of an "IMD Hub", this being an implantable device that works as a network switch for all the devices in the IBN and also plays the role of and authentication center. This approach suffers from an excessive trust on a unique central device, so the use of more connected hubs could be a more interesting approach both for security and performance reasons.

5.4.4. Proximity-based Access Control

These solutions base the access decisions on the distance between the programmer and the IMD, allowing only communications with devices located at a short distance from the IMD [93]. In certain applications, it has been suggested that this can be achieved by having the IMD equipped with a magnetic switch. This is just a magnetic sensor that detects the magnetic field generated by programmers in its proximity. Only after this switch has been activated the IMD will become available. After this, the IMD would send to the programmer the key to be used for subsequent communications during this session. Unfortunately, apart from security issues, it is unclear whether these solutions are

safe enough, since having a magnetic field close to the implant might alter its functioning [70].

Other solutions are based on classical distance bounding protocols, these being schemes that compute an upper bound for the distance between two devices. In [91], Rasmussen et al. propose a device paring protocol in which the IMD and the programmer obtain a shared key. Messages are sent through an ultrasonic channel and the response times—i.e., the time between sending a request and receiving an answer—are used to estimate the distance between the devices. This process can be repeated several times to upper bound the estimation. If the computed distance is less than a fixed threshold, the communication with the IMD continues; otherwise, it is interrupted. It is also worth mentioning that some authors consider that response times in the protocol could serve as a deterrent against replay attacks [32], as the device could detect old request being replayed and reject them.

Normal and emergency operation modes are considered in [91]. While in normal model, the paring protocol is executed and a session key is established. This process is carried out assuming that the IMD and the programmer initially share a secret key. When in emergency mode, the shared key established above, which is probably stored in an authorization token but the patient could have forgotten it, may be unknown. To address this, the authors propose a mechanism to deal with this contingency. In detail, they propose a scheme to generate a temporary secret key so that the paring protocol can be executed. This is an alternative to the use of the magnetic switch previously described. In this case, the programmer has to be within the emergency range, which is shorter than in normal operation mode.

Distance-based solutions assume that a reader that is close to the IMD is not an adversary. It can be a legitimate programmer with the required credentials and within permitted range for normal mode. Alternatively, it could be a legitimate reader but without the authorization tokens in an emergency condition and located very close (i.e., in emergency range) to the IMD. This leads to two major disadvantages that have not being considered by this sort of protocols:

- The IMD can be compromised if the adversary is within the defined range. It would be desirable to guarantee the security of the patient independently of the distance an attacker can be. There are many daily situations in which the attacker can get very close to the IMD, such as in a public transport vehicle, at the office, etc. In other cases, the attacker can plant a programmer device close enough to the patient's body and use it as a proxy for conducting his activities. Moreover, the attacker can be the patient himself trying to deliberately manipulate the IMD.

- There are techniques that allow an adversary to simulate being within the permitted range when in reality he is at a longer distance. This is a key limitation for any protocol based exclusively on the computed distance.

5.4.5. Biometric Measures

Biometrics refers to a number of identification techniques based on the patient's physical characteristics, such as his fingerprint, iris pattern, voice, hand, etc. [8, 90]. Interested readers can find in [77] more details about the use of biometrics in the healthcare context.

In [51], Hei and Du propose a solution that restricts access to authorized entities and deals with emergency situations where the patient can be unconscious or not holding his credentials (e.g., an external authorization token). The scheme uses biometric features from the patient in two separate steps or levels. Level 1 employs basic biometric information, such as fingerprints, iris color, the patient's weight, etc. Once level 1 is passed, level-2 authentication must be passed too in order to finally get access to the device. For that, biometric information extracted from the patient's iris must be provided. That information is pre-stored as a key in the memory of the IMD. Iris-based authentication has a high accuracy and is very efficient. Furthermore, to obtain a good snapshot of the iris a near infrared camera is needed, and the user has to be at a distance of between fifty and seventy centimetres, which is a very short range. As consequence of this, the patient would easily detect an attacker due to his proximity in many situations.

Similarly, in [125] Xu et al. propose the use of ECG (electrocardiograms) signals to generate the patient's secret key. By using this the scheme avoids the need for pre-stored keys and the associated key distribution problem. Access control is guaranteed by a cryptographic protocol that employs this ECG-based key. On the other hand, communications between the IMD and the reader are coordinated by an external device named IMDGuard that is very similar to the RFID Guardian proposed in [93]. The presence of the IMDGuard means that the IMD works under normal mode and ECG-based access control is used. When the IMDGuard is absent, communications are not protected and access control is not enforced, which would allow anyone (e.g., medical personnel in an emergency situation, but also an adversary) to interact with the implant. A recent and detailed study about the use of ECG signals for key generation can be found in [97].

In certain cases, biometric techniques can be easier to apply than solutions based on shared keys, since the key distribution problem is avoided and it is harder for the attacker to disclose the keys. In principle, the adversary could not impersonate the programmer or the IMDGuard unless he has physical contact with the patient. Despite this, biometric-based approaches have two main drawbacks:

- Firstly, the physical presence of the patient is needed. This is certainly not a disadvantage in an emergency situation, where the patient is physically located in the emergency room or equivalent. Unfortunately, this is not the case when medical personnel will attempt to access the IMD remotely.

- Secondly, biometric features are never perfect. Two measures taken at different times, or even acquired simultaneously but using two reading de-

vices, could generate different results. A straightforward use of such measures might generate wrong keys, when in reality the user is authorized. Error correction techniques are used to avoid this [2, 14]. This problem is known as truth rejection rate and implies that not all biometric data can be used for key generation (or authentication). Thus, the measure has to be gathered from body parts so that the differences between measures are within a acceptable range and can be corrected [13].

5.5. Anomaly Detection

The availability of the IMD functions is crucial since the treatment—and even the patient's life—can be compromised otherwise. If an attack is detected, the patient can be informed (e.g., by a notification mechanism) or the device can be rendered inaccessible via switching off the communications (or jamming the channel) while the medical functions are kept running. The difficulty to prevent this sort of attacks mainly arises from the use of the wireless communication channel. Communication between the IMD and the reader starts with the IMD authenticating the reader. If the reader does not pass the authentication step, the communication is interrupted. This consumes resources in the IMD and, therefore, can be exploited by an adversary who, for example, repeatedly attempts to communicate with the IMD. The result would be a classical Denial-of-Service (DoS) attack in which the battery level could be drastically reduced and memory/storage could be also affected—in each authentication, some registers are used to store security values such as session tokens and logs. In general, this sort of attacks are known as Resource Depletion (RD) attacks and focus on wasting the resources of the IMD [57]. They are very easy to implement and their consequences can be very harmful as the battery life of the IMD could be shortened from several yeas to a few weeks just by sending dummy requests.

Standard cryptographic solutions do not prevent these attacks, and existing studies about RD attacks in sensors networks [92] are not directly applicable to IMDs since implants have more severe resource restrictions. Moreover, there is an extra difficultly for adding new resources—the implant is within the body, which is not the case of sensor networks. This motivates the need for designing solutions that take into account the fact that these devices will be used within a human body.

In the context of IMDs, the combined use of pattern/behaviour analysis and notification systems is the most widely used solution to counter RD attacks. Notification systems inform the patient through an alarm signal (e.g., a sound or vibration) when particular events happen, such as when the IMD establishes communication with a external device [43] or when certain biomedical parameters fall out of the normal range [23]. Such alarms are only informative. Thus, notification does not prevent attacks from happening, although alerting the patient may be valuable to make him aware of unexpected ongoing communication activity. One major drawback of these approaches is that they do not work properly in acoustically noisy environments. Besides, alarms have an associated energy consumption that should not be underestimated. As in the

case of auditing, notification mechanisms alone are insufficient and should be complemented with other solutions.

By leveraging the fact that the wireless communications between an IMD and a reader follow a set of observable patterns (e.g., frequency, localization, patient conditions, etc.), Hei et al. propose in [52] a mechanism against RD attacks with an average detection rate over 90%. The scheme uses a Support Vector Machine (SVM), which is assumed to run in the patient's phone. In detail, the authors consider five kinds of input data to carry out detection: reader action type (i.e., the action(s) the reader can execute on the IMD, where the set of actions depends on the type of implant); the time interval of the same reader action; the location (e.g., home or hospital); the time; and the day (e.g., weekly or weekend). Once trained, the classifier will determine whether a pattern is valid or not. For instance, if a particular type of request is always sent from the doctor office, an attempt of the same request from a different location would raise an alarm. The overall system works as follows. Each time the reader attempts to contact with the IMD, the latter sends a message to the mobile phone of the patient with the access pattern. The phone executes the classification algorithm and returns an output that is sent back to the IMD. Depending on that output, three actions are possible: (1) the input vector is considered legitimate. In this case the mobile sends a "1" (true) to the IMD and the communication with the reader continues; (2) the input vector does not correspond with any of the allowed patterns, in which case the phone sends a "0" (false). The request may come from an attacker and the IMD turns into sleep mode to avoid RD attacks; (3) If it is unclear whether the input vector is legitimate or an attack, an alarm is triggered (e.g., an audible alarm) to inform the patient, who must decide if the communication is permitted.

The proposal in [52] has three main drawbacks. Firstly, the scheme assumes that the IMD is always running in normal mode and does not consider emergency conditions in which legitimate access patterns could be certainly anomalous. If that is the case, access to the IMD would be rejected, which could result in severe consequences for the patient's safety. Secondly, the proposal inherits some disadvantages from schemes that base its security on an external device—the mobile phone, in this case—, as discussed in Section 5.4.2. Finally, but not less important, the patient has the responsibility of making a decision in case the SVM cannot classify the input data.

Instead of using patterns, Henry et al. have recently proposed in [53] a system to detect malicious/anomalous use of an insulin pump. In particular, the administration of insulin dosages is detected by tracking the acoustic bowel sounds. The events are logged and then used for checking the proper system operation. The proposal is a passive solution and does not offer protection in real-time. Moreover, as in [52], the system is based on the use of an external device needed to measure abdominal sounds.

A new defense method for IMDs based on wireless monitoring and anomaly detection is proposed in [128]. The authors propose the use of a medical security monitor, named MedMon, which eavesdrops communications to and from the IMD. Captured traffic is then passed for analysis to a multi-layer anomaly de-

tection system. If a malicious transaction is detected, the user can be informed (passive response) or alternatively the system can render the IMD inaccessible via active jamming (active response). Jamming refers to the transmission of radio signals with the purpose of impeding communications in the channel by reducing the signal-to-noise ratio. In this case, jamming is used to protect the IMD from being accessible to the adversary. The main drawback of this proposal is that the whole security resides on an external device, but it has the advantage of being applicable on existing devices without any modification. In line with MedMon, Darji and Trivedi have recently proposed a system for detecting active attacks [18]. They propose the use of an external proxy device equipped with several antennas that builds a signature of authorized readers/programmers based on their position. Positions are estimated through triangulation techniques. The proposal seems effective for static scenarios but not for dynamic ones.

5.6. Overriding Access Control

Although strictly speaking overriding access control mechanisms is not a protection measure, we have included these solutions here for completeness. Furthermore, in an emergency situation keeping the patient alive is more crucial than maintaining the IMD security protections fully functioning.

Access control models are often too inflexible. The access policy is generally established at the design phase, setting what actions are allowed, by which entities and under what circumstances. However, during the system life it is possible that unexpected and unanticipated situations may arise in which access to the implant is vital. For instance, in the context of IMDs and under an emergency condition the usage scenarios are unpredictable. Since guaranteeing the patient's safety is a priority, it is mandatory that access requirements can be removed if it becomes necessary. This type of situations give rise to a family of solutions collectively known as "Breaking-the-Glass" (BTG) that allows to switch the access control requirements off in critical or unknown situations for the system. This would facilitate the access to the implant under a emergency condition, although it also opens the door to a number of security vulnerabilities.

A typical proposal of a BTG policy can be found in [29]. Even though this work is not focused on IMDs, it can be adapted easily. In this case, the access controls requirements can be suppressed even if the entity previously did not have privileges to do that. The BTG is complemented with a non-repudiation mechanism that facilitates a subsequent analysis of the accesses carried out. The authors define a series of steps that must be executed in a precise order to override access control. First, when a user requests access, the system checks if he has the required privileges. If the answer is negative, the system may give him access under the BTG modality provided that the user accepts that all the actions will be recorded. If so, he gets access to the system and assume all responsibilities.

In [95], Rissanen et al. propose a model that distinguishes between allowed actions, forbidden actions, and all those that can be executed (possible actions).

The intersection between the sets of possible and forbidden actions represents the actions that can be allowed when overriding the access control policy.

The classical Clark-Wilson access control model for data integrity [15] also provides a reference framework for BTG policies. In this case, the basic steps needed in a BTG system are reduced to [7]:

1. Pre-staging break-glass accounts: emergency accounts are created in advance, so users and passwords are generated for these special cases.
2. Distributing accounts: pres-stages accounts are efficiently managed to guarantee that the required access data is available in appropriate and reasonable manner in case of emergency.
3. Monitoring the usage of the accounts: the system must be audited while being accessed during an emergency condition.
4. Cleaning up: once access in the emergency mode concludes, new access accounts are generated and the old ones are revoked, thus avoiding temporary-authorized users have a permanent access to the system.

Obviously, a set of measures to ensure the proper functioning of the system are required as consequence of bypassing the access control in a BTG system [42, 88, 103]:

1. Users must accept their new privileges, warning them of the possible consequences of their acts.
2. The system must record the actions performed by each user. A posterior analysis will determine if the access was legitimate or not. For that, access requests can be stored together with the system status, which could help to conclude whether the access was justified by the circumstances or not. As in the case of the auditing mechanisms described in Section 5.2, this can be considered as a deterrence measure.
3. In an emergency condition, all access operations must be monitored in real time to grant those privileges needed for them to be executed. Furthermore, the system has to be in emergency mode only while the emergency lasts, returning to the previous access policy as soon as possible.
4. The privileges granted in such situations must be kept to the minimum required to perform the task, but not more.
5. Some proposals like [88] go one step beyond and consider whether the requested action is reversible or not. Thus, actions executed by a user with enhanced privileges due to an emergency condition should be reversible, in such a way that unjustified actions can be undone.

As a practical implementation, the work presented in [7] by Brucker and Petritsch describes the integration of a standard access control model with a BTG policy and discusses the improvements in the architecture. Similarly, a context-based access control mechanism is proposed in [45], which depends on four factors: time, location, identity, and history of events.

In summary, BTG policies extend access control policies to critical situations, dynamically grating privileges to users who require them to execute an essential

Measure		Type	Safety	Security	Battery Life	Security Properties Addressed
No security		$*$	$-$	$-$	$*$	None
Auditing		Detection	$-$	$-$	$+$	Non-Repudiation
Cryptographic Measures		Protection	$-$	$+$	$\pm$	Authentication, Confidentiality, Integrity
AC	**Certificates & Lists**	Protection	$-$	$+$	$\pm$	Authorization (+Authentication)
	External Devices	Protection	$+$	$\pm$	$+$	
	Internal Devices	Protection	$+$	$+$	$*$	
	Proximity	Protection	$+$	$\pm$	$*$	
	Biometrics	Protection	$+$	$+$	$*$	
Anomaly Detection		Protection	$-$	$+$	$+$	Authorization, Availability
BTG Policies		Protection	$+$	$-$	$*$	Authorization during emergencies

Legend: $+$ Positive; $-$ Negative; $\pm$ Both positive and negative effects; $*$ No influence.

Table 2: Security Solutions for IMDs

action. This type of policies are very important since it is unrealistic to assume that all possible situations will be considered at design time. In fact, in the case of IMDs the situations in which an emergency can appear are unpredictable and, in the majority of the cases, a successful management of the emergency situation depends on the access being granted in time. As for the proposals discussed above, some of its properties are difficult to guarantee a priori, such as for example ensuring that the system can recover from the BTG policy by allowing only reversible actions (in most emergency situations the required actions are clearly irreversible). Therefore, although these measures aim at solving the tension between security and patient's safety, its usage can be risky. In general, it would be necessary to carefully define what an emergency situation is and providing the IMD with the means necessary to recognize it. However, as this would have to be done at the design phase, it somehow contradicts the basic BTG motivation, namely that critical situations are unpredictable and must be detected at execution time.

5.7. Summary

Table 2 provides an overview of the proposals discussed throughout this section, detailing for each one of them its main purposes and how it affects three main goals: security, patient's safety, and battery life. Furthermore, in relation with STRIDE methodology, we show the security properties addressed.

6. Conclusions

Implantable Medical Devices improve the quality life of patients and, in some cases, play an important role in keeping them alive. The new generation of IMDs are increasingly incorporating more computing and communication capabilities. In this article, we argued that advances on novel and smarter IMD designs must incorporate security solutions by design in order to provide the user with both safety and security guarantees. We have provided a comprehensive overview of the main security problems associated to the newest IMDs and have discussed how, in some cases, the patient's health can be seriously threatened by a malicious adversary. It is therefore evident that security mechanisms have

to be incorporated into these devices. Further cooperation among researchers coming from manufacturing technologies, bioengineering, and computer security are necessary to guarantee both the patient's safety and the privacy and security of the data and communications.

Given the tensions among the different security objectives and the solutions proposed so far, it is unclear what the optimal choice would be. The question still remains an open problem. Many proposals provide a reasonably high security level but require too many resources (e.g., memory or computation), which is infeasible taking into consideration the need to save battery life. Alternatively, lightweight solutions are often vulnerable to attacks as a consequence of their weak designs.

Apart from purely engineering solutions, the procedures that both the medical personnel and the patients follow when interacting with the implants have to be considered, and existing regulations and standards should be also reviewed. However, nowadays these aspects are essentially ignored [113]. Devices must be used responsibly, and users must know various details about its functioning and the possible threats in order to raise security awareness.

Although some existing security solutions can be effective from a theoretical point of view, patients are very likely to reject them. The IMD is a computer system that is embedded into the human body. This is nowadays a special and delicate situation and the user opinion should be taken into account as far as possible. Interested readers can find in [21] some guidelines for designing security systems for IMDs considering the patient's point of view.

Looking even further ahead, medical implants open the door to other types of devices to improve human abilities, such as memory or perception, or even integrate our physiology with silicon-based components to improve our body. This looks certainly far ahead nowadays, but perhaps pacemakers and neurostimulators were also considered a remote possibility before they were introduced [121]. The field of computer security has to be ready to adapt and incorporate solutions for this new setting at the design phases, avoiding the develop-then-patch approach that has provided disastrous results for the Internet.

Acknowledgements

This work was supported by the MINECO grant TIN2013-46469-R (SPINY: Security and Privacy in the Internet of You).

References

[1] D. Arney, K. K. Venkatasubramanian, O. Sokolsky, and I. Lee. Biomedical devices and systems security. In *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 2376–2379, 2011.

[2] S.-D. Bao, C. C. Y. Poon, Z. Yuan-Ting, and L.-F. Shen. Using the timing information of heartbeats as an entity identifier to secure body sensor

network. *IEEE Transactions on Information Technology in Biomedicine*, 12(6):772–779, 2008.

[3] S. Bergamasco, M. Bon, and P. Inchingolo. Medical data protection with a new generation of hardware authentication tokens. 2001.

[4] T. P. Berger, J. DHayer, K. Marquet, M. Minier, and G. Thomas. The gluon family: A lightweight hash function family based on fcsrs. In *Progress in Cryptology - AFRICACRYPT 2012*, volume 7374 of *Lecture Notes in Computer Science*, pages 306–323. Springer Berlin Heidelberg, 2012.

[5] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varc, and I. Verbauwhede. spongent: A lightweight hash function. In *Proc. of Cryptographic Hardware and Embedded Systems*, volume 6917 of *Lecture Notes in Computer Science*, pages 312–325. Springer Berlin Heidelberg, 2011.

[6] C. J. Borleffs, J. Thijssen, M. K. de Bie, J. B van Rees, G. H. van Welsenes, L. van Erven, J. J. Bax, S. C. Cannegieter, and M. J. Schalij. Recurrent implantable cardioverter-defibrillator replacement is associated with an increasing risk of pocket-related complications. *Pacing and Clinical Electrophysiology*, 33(8):1013–1019, 2010.

[7] A. D. Brucker and H. Petritsch. Extending access control models with break-glass. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, pages 197–206. ACM, 2009.

[8] I. Buhan, E. Kelkboom, and K. Simoens. A survey of the security and privacy measures for anonymous biometric authentication systems. In *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pages 346–351, Oct 2010.

[9] M. A. Callejon, D. Naranjo-Hernandez, J. Reina-Tosina, and L. M. Roa. A comprehensive study into intrabody communication measurements. *IEEE Transactions on Instrumentation and Measurement,*, 62(9):2446–2455, 2013.

[10] M. A. Callejon, L. M. Roa, J. Reina-Tosina, and D. Naranjo-Hernandez. Study of attenuation and dispersion through the skin in intrabody communications systems. *IEEE Transactions on Information Technology in Biomedicine*, 16(1):159–165, 2012.

[11] Industry Canada. Medical devices operating in the 401-406 mhz frequency band. `http://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/rss243.pdf/$FILE/rss243.pdf`, 2010.

[12] P.E. Chadwick. Regulations and standards for wireless applications in ehealth. In *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*, pages 6170–6173, 2007.

[13] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta. Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In *Proc. of International Conference on Parallel Processing Workshops*, pages 432–439, 2003.

[14] K. Cho and D. Lee. Biometric based secure communications without predeployed key for biosensor implanted in body sensor networks. In *Information Security Applications*, volume 7115 of *Lecture Notes in Computer Science*, pages 203–218. Springer Berlin Heidelberg, 2012.

[15] D. D. Clark and D. R. Wilson. A comparison of commercial and military computer security policies. In *IEEE Symposium on Security and Privacy*, pages 184–195. IEEE Computer Society, 1987.

[16] Federal Communications Commission. About medical device radiocommunications service. `http://wireless.fcc.gov/services/index.htm?job=service_bandplan&id=medical_implant`, 2009.

[17] K. Daniluk and E. Niewiadomska-Szynkiewicz. Energy-efficient security in implantable medical devices. In *Computer Science and Information Systems (FedCSIS), 2012 Federated Conference on*, pages 773–778, 2012.

[18] M. Darji and B. Trivedi. Detection of active attacks on wireless imds using proxy device and localization information. In *Security in Computing and Communications*, volume 467 of *Communications in Computer and Information Science*, pages 353–362. Springer Berlin Heidelberg, 2014.

[19] M. de Sousa, G. Klein, T. Korte, and M. Niehaus. Electromagnetic interference in patients with implanted cardioverter-defibrillators and implantable loop recorders. *Indian Pacing Electrophysiol Journal*, 2(3):79–84, 2002.

[20] B. Defend, M. Salajegheh, K. Fu, and S. Inoue. Protecting global medical telemetry infrastructure. Technical report, Institute of Information Infrastructure Protection (I3P), 2008.

[21] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 917–926. ACM, 2010.

[22] T. Denning, K. Fu, and T. Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *Proceedings of the 3rd Conference on Hot Topics in Security*, HOTSEC'08, pages 5:1–5:7. USENIX Association, 2008.

[23] Dexcom. Seven plus cgm system. `http://www.dexcom.com/seven-plus`, Consulted on Feburary 2014.

[24] T. Drew and M. Gini. Implantable medical devices as agents and part of multiagent systems. In *Proc. of the fifth international joint conference on Autonomous agents and multiagent systems*, AAMAS '06, pages 1534–1541. ACM, 2006.

[25] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar. A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. In *2010 International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID)*, pages 1–6, 2010.

[26] Carl Falcon. Wireless medical devices: Satisfying radio requirements. *Medical Device & Diagnostic Industry*, page 80, 2004.

[27] FDA. Radio frequency wireless technology in medical devices - guidance for industry and food and drug administration staff. `http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf`, 2013.

[28] FDA. Content of premarket submissions for management of cybersecurity in medical devices. `http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf`, 2014.

[29] A. Ferreira, R. Cruz-Correia, L. Antunes, P. Farinha, E. Oliveira-Palhares, D. W. Chadwick, and A. Costa-Pereira. How to break access control in a controlled manner. In *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems*, pages 847–854. IEEE Computer Society, 2006.

[30] U.S. Food and Drug Administration (FDA). Medical device safety. `http://wireless.fcc.gov/services/index.htm?job=service_bandplan&id=medical_implant`, Consulted on Nov. of 2013.

[31] K. Fotopoulou and B.W. Flynn. Optimum antenna coil structure for inductive powering of passive rfid tags. In *IEEE International Conference on RFID*, pages 71–77, 2007.

[32] E. Freudenthal, R. Spring, and L. Estevez. Practical techniques for limiting disclosure of rf-equipped medical devices. In *IEEE Engineering in Medicine and Biology Workshop,*, pages 82–85, 2007.

[33] K. Fu. Inside risks: Reducing risks of implantable medical devices. *ACM Communications*, 52(6):25–27, 2009.

[34] K. Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*, 2011.

[35] F. Furbass and J. Wolkerstorfer. Ecc processor with low die size for rfid applications. In *IEEE International Symposium on Circuits and Systems*, pages 1835–1838, 2007.

[36] S. Gollakota, H. Al Hassanieh, B. Ransford, D. Katabi, and K. Fu. Imd shield: Secure implantable medical devices. `http://groups.csail.mit.edu/netmit/IMDShield/`, 2011.

[37] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implantable medical devices. *SIGCOMM Comput. Commun. Rev.*, 41(4):2–13, August 2011.

[38] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implantable medical devices. *SIGCOMM Comput. Commun. Rev.*, 41(4):2–13, 2011.

[39] S. Gollakota, H. A. Hassanieh, B. Ransford, D. Katabi, and K. Fu. Imd shield: Securing implantable medical devices (poster). USENIX Association, 2011.

[40] E. E. Gul and M. Kayrak. Common pacemaker problems: Lead and pocket complications. In Mithilesh R. Das, editor, *Modern Pacemakers - Present and Future*. InTech, 2011.

[41] J. Guo, T. Peyrin, and A. Poschmann. The photon family of lightweight hash functions. In *Advances in Cryptology CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239. Springer Berlin Heidelberg, 2011.

[42] S. K. S Gupta, T. Mukherjee, and K. Venkatasubramanian. Criticality aware access control model for pervasive applications. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 257–261, March 2006.

[43] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, 7(1):30–39, 2008.

[44] 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 *Proc. of the 29th Annual IEEE Symposium on Security and Privacy*, pages 129–142, 2008.

[45] W. Han, J. Zhang, and X. Yao. Context-sensitive access control model and implementation. In *The Fifth International Conference on Computer and Information Technology*, pages 757–763, 2005.

[46] S. Hanna. Regulations and standards for wireless medical applications. In *Third International Symposium on Medical Information & Communication Technology*, pages 1–5, 2009.

[47] J. A. Hansen and N. M. Hansen. A taxonomy of vulnerabilities in implantable medical devices. In *Proc. of the second annual workshop on Security and privacy in medical and home-care systems*, SPIMACS '10, pages 13–20, New York, USA, 2010. ACM.

[48] M.A. Hanson, H.C. Powell, A.T. Barth, K. Ringgenberg, B.H. Calhoun, J.H. Aylor, and J. Lach. Body area sensor networks: Challenges and opportunities. *Computer*, 42(1):58–65, Jan 2009.

[49] G.J. Haubrich, L.D. Twetan, and G.C. Rosar. Multiple band communications for an implantable medical device, July 27 2006. WO Patent App. PCT/US2006/000,961.

[50] D. He, S. Chan, and S. Tang. A novel and lightweight system to secure wireless medical sensor networks. *IEEE Journal of Biomedical and Health Informatics*, 18(1):316–326, Jan 2014.

[51] X. Hei and X. Du. Biometric-based two-level secure access control for implantable medical devices during emergencies. In *Proceedings IEEE INFOCOM*, pages 346–350, 2011.

[52] X. Hei, X. Du, J. Wu, and F. Hu. Defending resource depletion attacks on implantable medical devices. In *Proc. of IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, 2010.

[53] N. Henry, N. Paul, and N. McFarlane. Using bowel sounds to create a forensically-aware insulin pump system. In *Workshop on Health Information Technologies, HealthTech, USENIX*, pages 1–10, 2013.

[54] HIPPA. Security standards: Technical safeguards. 2(4):1–17, 2007.

[55] S. Hosseini-Khayat. A lightweight security protocol for ultra-low power asic implementation for wireless implantable medical devices. In *5th International Symposium on Medical Information Communication Technology (ISMICT)*, pages 6–9, March 2011.

[56] F. Hu, Q. Hao, M. Lukowiak, Q. Sun, K. Wilhelm, S. Radziszowski, and Yao Wu. Trustworthy data collection from implantable medical devices via high-speed security implementation based on ieee 1363. *IEEE Transactions on Information Technology in Biomedicine*, 14(6):1397–1404, 2010.

[57] F. Hu, Q. Sun, Y. Wu, M. Guo, J. Lu, J. Li, D. J. Gay, J. K. Garner, and A. L. Poellnitz. Implantable medical devices: Architectureand design. In *Telehealthcare Computing and Engineering: Principles and Design*, chapter 14, pages 359–406. 1 edition, 2013.

[58] Texas Instruments. Msp430f156, 16-bit ultra-low-power mcu. http://www.ti.com/lit/ds/symlink/msp430f156.pdf.

[59] ISO. Information technology – security techniques – entity authentication – part 2: Mechanisms using symmetric encipherment algorithms, iso/iec 9798-2:2008. International Standard, 2nd ed., 1999.

[60] T. Isobe and K. Shibutani. Security analysis of the lightweight block ciphers xtea, led and piccolo. In *Information Security and Privacy*, volume 7372 of *Lecture Notes in Computer Science*, pages 71–86. Springer Berlin Heidelberg, 2012.

[61] C. W. Israel and S. S. Barold. Pacemaker systems as implantable cardiac rhythm monitors. *The American Journal of Cardiology*, 88(4):442 – 445, 2001.

[62] ITU-T. E-health standards and interoperability. http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000170001PDFE.pdf, 2012.

[63] H. Jiang, J. Zhang, D. Lan, K. K. Chao, S. Liou, H. Shahnasser, R. Fechter, S. Hirose, M. Harrison, and S. Roy. A low-frequency versatile wireless power transfer technology for biomedical implants. *Biomedical Circuits and Systems, IEEE Transactions on*, 7(4):526–535, 2013.

[64] A. Kaadan and H.H. Refai. Securing wireless medical devices. In *IEEE Global Communications Conference (GLOBECOM)*, pages 942–948, 2012.

[65] P.A. Karger, G. S. Kc, and D. Toll. Privacy is essential for secure mobile devices. *IBM Journal of Research and Development*, 53(2):5:1–5:17, 2009.

[66] P. Kitsos, N. Sklavos, M. Parousi, and A. N. Skodras. A comparative study of hardware architectures for lightweight block ciphers. *Computers & Electrical Engineering*, 38(1):148 – 160, 2012.

[67] L. Knudsen, G. Leander, A. Poschmann, and M. Robshaw. Printcipher: A block cipher for ic-printing. In *Cryptographic Hardware and Embedded Systems*, volume 6225 of *Lecture Notes in Computer Science*, pages 16–32. Springer Berlin Heidelberg, 2010.

[68] T. J. Lamer. Treatment of cancer-related pain: When orally administered medications fail. *Mayo Clinic Proceedings*, 69(5):473–480, 1994.

[69] N. Leavitt. Mobile phones: the next frontier for hackers? *Computer*, 38(4):20–23, 2005.

[70] S. Lee, K. Fu, T. Kohno, B. Ransford, and W. H. Maisel. Clinically significant magnetic interference of implanted cardiac devices by portable headphones. *Heart rhythm*, 6(10):1432–1436, 2009.

[71] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede. Elliptic-curve-based security processor for rfid. *IEEE Transactions on Computers*, 57(11):1514–1527, Nov 2008.

[72] C. Li, A. Raghunathan, and N. K. Jha. Improving the trustworthiness of medical device software with formal verification methods. *IEEE Embedded Systems Letters*, 5(3):50–53, 2013.

[73] C. Li, A. Raghunathan, and N.K. Jha. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*, pages 150–156, June 2011.

[74] J. Lindqvist, S. Liimatainen, and T. Katajamaki. Secure pairing architecture for wireless mobile devices. In *IEEE 63rd Vehicular Technology Conference*, volume 2, pages 823–827, May 2006.

[75] R. T. Lukins, S. Tisch, and B. Jonker. The latest evidence on target selection in deep brain stimulation for parkinsons disease. *Journal of Clinical Neuroscience*, 21(1):22 – 27, 2014.

[76] V. S Mallela, V. Ilankumaran, and N. S. Rao. Trends in cardiac pacemaker batteries. *Journal Indian Pacing Electrophysiol*, 4(4):201–212, 2004.

[77] D. Marohn. Biometrics in healthcare. *Biometric Technology Today*, 14(9):9 –11, 2006.

[78] ST. Jude Medical. Cardiac rhythm management products. `http://professional-intl.sjm.com/products/crm/pacemakers/dual-and-single-chamber`, Consulted on February 2014.

[79] Medtronic. Implantable pacemaker and defibrillator information. *Patient Services*, 1(800):551–5544, x41835, 2006.

[80] Medtronic. Cardiac rhythm products - pacemakers. `http://www.medtronic.com/for-healthcare-professionals/products-therapies/cardiac-rhythm/pacemakers/index.htm`, Consulted on February 2014.

[81] Medtronic. Parkison's disease. `http://www.medtronic.eu/your-health/parkinsons-disease/device/our-dbs-therapy-products/activaRC/index.htm`, Consulted on Feburary 2014.

[82] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., 1st edition, 1996.

[83] C. Miller. Mobile attacks and defense. *IEEE Security Privacy*, 9(4):68–70, 2011.

[84] N. Noiseux, P. Khairy, A. Fournier, and S. J. Vobecky. Thirty years of experience with epicardial pacing in children. *Cardiology in the Young*, 14:512–519, 2004.

[85] D. Panescu. Emerging technologies [wireless communication systems for implantable medical devices]. *IEEE Engineering in Medicine and Biology Magazine*, 27(2):96–101, 2008.

[86] C.-S. Park. Mechanism based on hospital authentication server for secure application of implantable medical device. *BioMed Research International*, 2014:1–14, 2014.

[87] S. Patel, K. Lorincz, R. Hughes, N. Huggins, J.H. Growdon, M. Welsh, and P. Bonato. Analysis of feature space for monitoring persons with parkinson's disease with application to a wireless wearable sensor system. In *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*, pages 6290–6293, 2007.

[88] D. Povey. Optimistic security: A new access control paradigm. In *Proceedings of the 1999 Workshop on New Security Paradigms*, pages 40–45. ACM, 2000.

[89] J. Radcliffe. Hacking medical devices for fun and insulin: Breaking the human. scada system. In *Black Hat. Technical Security Conference*, 2011.

[90] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar. Secure biometrics: Concepts, authentication architectures, and challenges. *IEEE Signal Processing Magazine*, 30(5):51–64, 2013.

[91] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pages 410–419. ACM, 2009.

[92] R. Raymond, D and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1):74–81, 2008.

[93] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. Rfid guardian: A battery-powered mobile device for rfid privacy management. In *Information Security and Privacy*, volume 3574 of *Lecture Notes in Computer Science*, pages 184–194. Springer Berlin Heidelberg, 2005.

[94] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. Is your cat infected with a computer virus? In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 179–189, March 2006.

[95] E. Rissanen, B. Firozabadi, and M. Sergot. Towards a mechanism for discretionary overriding of access control. In *Security Protocols*, volume 3957 of *Lecture Notes in Computer Science*, pages 312–319. Springer Berlin Heidelberg, 2006.

[96] M. Rostami, W. Burleson, F. Koushanfar, and A. Juels. Balancing security and utility in medical devices? In *Proceedings of the 50th Annual Design Automation Conference*, DAC '13, pages 13:1–13:6. ACM, 2013.

[97] M. Rostami, A. Juels, and F. Koushanfar. Heart-to-heart (h2h): authentication for implanted medical devices. In *ACM Conference on Computer and Communications Security*, pages 1099–1112. ACM, 2013.

[98] M. Salajegheh, A. Molina, and K. Fu. Privacy of home telemedicine: Encryption is not enough. *Journal of Medical Devices*, 3(2), 2009.

[99] C. Sandner and R. Amirtharajah. Power management. In *IEEE Custom Integrated Circuits Conference*, pages 1–1, Sept 2013.

[100] H.S. Savci, A. Sula, Z. Wang, N.S. Dogan, and E. Arvas. Mics transceivers: regulatory standards and applications [medical implant communications service]. In *IEEE Proceedings SoutheastCon*, pages 179–182, April 2005.

[101] S. Schechter. Security that is meant to be skin deep: Using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices. `http://research.microsoft.com/apps/pubs/default.aspx?id=12213`, 2004.

[102] J.H. Schulman. Stimulating and sensing network inside the human body. In *International Workshop on Wearable and Implantable Body Sensor Networks*, pages 95–98, April 2006.

[103] NEMA/COCIR/JIRA Security and Privacy Committee (SPC). Breakglass: An approach to granting emergency access to healthcare systems, 2004.

[104] L. Seltzer. Securing your private keys as best practice for code signing certificates. `https://www.symantec.com/content/en/us/enterprise/white_papers/b-securing-your-private-keys-csc-wp.pdf`, 2013.

[105] M. Seyedi, B. Kibret, D. T. H. Lai, and M. Faulkner. A survey on intrabody communications for body area network applications. *IEEE Transactions on Biomedical Engineering*, 60(8):2067–2079, 2013.

[106] S. Shivshankar and K. Summerhayes. *Challenges of Conducting Medical Device Studies*. Institute of Clinical Research, 2007.

[107] V. Shnayder, B.-r. Chen, K. Lorincz, T. R. F. Fulford Jones, and M. Welsh. Sensor networks for medical care. In *Proceedings of the 3rd international conference on Embedded networked sensor systems*, SenSys '05, pages 314–314. ACM, 2005.

[108] K. M. Silay, C. Dehollain, and M. Declercq. A closed-loop remote powering link for wireless cortical implants. *IEEE Sensors Journal*, 13(9):3226–3235, 2013.

[109] R. N. Simons, D. G. Hall, and F. A. Miranda. Rf telheidu2011emetry system for an implantable bio-mems sensor. In *IEEE MTT-S International Microwave Symposium Digest*, volume 3, pages 1433–1436, 2004.

[110] K. Singh and V. Muthukkumarasamy. Authenticated key establishment protocols for a home health care system. In *3rd International Conference on Intelligent Sensors, Sensor Networks and Information*, pages 353–358, 2007.

[111] C. Strydis, R. M. Seepers, P. Peris-Lopez, D. Siskos, and I. Sourdis. A system architecture, processor, and communication protocol for secure implants. *ACM Trans. Archit. Code Optim.*, 10(4):57:1–57:23, 2013.

[112] R. Sullivan and A. Ferriter. Prevent life-threatening communication breakdowns. *Nursing*, 38(2):17, 2008.

[113] BBC News Technology. Medical device hack attacks may kill, researchers warn. `http://www.bbc.co.uk/news/technology-17631838`, 2012.

[114] TheVerge. Dick cheney had the wireless disabled on his pacemaker to avoid risk of terrorist tampering. `http://www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007`, 2013.

[115] K. K. Venkatasubramanian, A. Banerjee, and S. K S Gupta. Pska: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 14(1):60–68, 2010.

[116] K. K. Venkatasubramanian and S. K. S. Gupta. Security for pervasive health monitoring sensor applications. In *In Proceedings of 4th International Conference on Intelligent Sensing and Information Processing (ICISIP)*, pages 197–202, 2006.

[117] J. A. Von Arx and K. Najafi. On-chip coils with integrated cores for remote inductive powering of integrated microsystems. In *International Conference on Solid State Sensors and Actuators*, volume 2, pages 999–1002 vol.2, Jun 1997.

[118] D. Vouyioukas and A. Karagiannis. *Telemedicine Techniques and Applications*. Intech, 2011.

[119] F. Walker, S. C. Siu, S. Woods, D. A. Cameron, G. D. Webb, and L. Harris. Long-term outcomes of cardiac pacing in adults with congenital heart disease. *Journal of the American College of Cardiology*, 43(10):1894 – 1901, 2004.

[120] Z. L. Wang and J. Song. Piezoelectric nanogenerators based on zinc oxide nanowire arrays. *Science*, 312(57771):242–246, 2006.

[121] K. Warwick. Upgrading humans via implants - why not? `http://www.19.bbk.ac.uk/index.php/19/article/view/488`, 2008.

[122] J. G. Webster. *Design of cardiac pacemakers.* IEEE Press, 1995.

[123] D. Wu, K. Warwick, Z. Ma, M.N. Gasson, Burgess J. G., S. Pan, and T.Z Aziz. Prediction of parkinson's disease tremor onset using a radial basis function neural network based on particle swarm optimization. *International Journal of Neural Systems*, 20(02):109–116, 2010.

[124] S. Xiao, A. Dhamdhere, V. Sivaraman, and A. Burdett. Transmission power control in body area sensor networks for healthcare monitoring. *IEEE Journal on Selected Areas in Communications*, 27(1):37–48, 2009.

[125] F. Xu, Z. Qin, C.C. Tan, B. Wang, and Q. Li. Imdguard: Securing implantable medical devices with the external wearable guardian. In *Proceedings IEEE INFOCOM*, pages 1862–1870, 2011.

[126] R.-F. Xue, K.-W. Cheng, and M. Je. High-efficiency wireless power transfer for biomedical implants by optimal resonant load transformation. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 60(4):867–874, 2013.

[127] A. Yakovlev, S. Kim, and A. Poon. Implantable biomedical devices: Wireless powering and communication. *IEEE Communications Magazine*, 50(4):152–159, 2012.

[128] M. Zhang, A. Raghunathan, and N. K. Jha. Medmon: Securing medical devices through wireless monitoring and anomaly detection. *IEEE Transactions on Biomedical Circuits and Systems*, 7(6):871–881, 2013.

[129] H. Zhu, Xu. R., and Yuan. J. High speed intra-body communication for personal health care. In *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 709–712, Sept 2009.

[130] B. Ziaie, M. Nardin, J. Von Arx, and K. Najafi. A single channel implantable microstimulator for functional neuromuscular stimulation. In *Proceedings 7th International Conference on Solid State Sensors and Actuators*, pages 266–269, 1993.