OOBKey: Key Exchange with Implantable Medical Devices Using Out-Of-Band Channels

MO ZHANG, University of Birmingham, UK and University of Melbourne, Australia
EDUARD MARIN, Telefonica Research, Spain
DAVID OSWALD, University of Birmingham, UK
VASSILIS KOSTAKOS, University of Melbourne, Australia
MARK RYAN, University of Birmingham, UK
BENJAMIN TAG, University of Melbourne, Australia
KLEOMENIS KATEVAS, Brave Software, Spain

Implantable Medical Devices (IMDs) are widely deployed today and often use wireless communication. Establishing a secure communication channel to these devices is vital, however, also challenging in practice. To address this issue, numerous researchers have proposed IMD key exchange protocols, in particular ones that leverage an Out-Of-Band (OOB) channel such as audio, vibration and physiological signals. These solutions have advantages over traditional key exchange, e.g., their plug-and-play nature. However, such protocols are often constructed in an ad-hoc manner and lack stringent evaluation of their security, usability and deployability properties. In this paper, we systematize this area and derive a solid theoretical footing to compare different OOB-based approaches. We review related work in that light and show the shortcomings of previous approaches. We then make the core observation that security imperfections in OOB channels can be mitigated by incorporating password-authenticated key agreement. Accordingly, we propose a new construction for OOB key exchange and formalize the security level. We then derive three protocols from it that only require an inertial sensor in the IMD, which is already available in advanced devices. We analyze those protocols with the proposed formalism to highlight shortcomings and advantages depending on specific practical scenarios.

CCS Concepts: • **Security and privacy → Mobile and wireless security**; **Usability in security and privacy**.

Additional Key Words and Phrases: medical device security, implantable medical device, out-of-band channel, key exchange, inertial sensor

ACM Reference Format:
Mo Zhang, Eduard Marin, David Oswald, Vassilis Kostakos, Mark Ryan, Benjamin Tag, and Kleomenis Katevas. 2022. OOBKey: Key Exchange with Implantable Medical Devices Using Out-Of-Band Channels. *ACM Trans. Comput. Healthcare* 0, 0, Article 0 (2022), 24 pages. https://doi.org/XXXXXXX.XXXXXXX

Authors' addresses: Mo Zhang, University of Birmingham, Edgbaston, Birmingham, UK and University of Melbourne, Parkville, Melbourne, Australia, mxz819@cs.bham.ac.uk; Eduard Marin, Telefonica Research, Barcelona, Spain, eduard.marinfabregas@telefonica.com; David Oswald, University of Birmingham, Birmingham, UK, d.f.oswald@cs.bham.ac.uk; Vassilis Kostakos, University of Melbourne, Parkville, Melbourne, Australia, vassilis.kostakos@unimelb.edu.au; Mark Ryan, University of Birmingham, Birmingham, UK, m.d.ryan@cs.bham.ac.uk; Benjamin Tag, University of Melbourne, Parkville, Melbourne, Australia, benjamin.tag@unimelb.edu.au; Kleomenis Katevas, Brave Software, Barcelona, Spain, kkatevas@brave.com.

2637-8051/2022/0-ART0 $15.00
https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

The number of patients with an Implantable Medical Device (IMD), such as a pacemaker, an Implantable Cardioverter Defibrillators (ICD), or a neurostimulator, has been rapidly growing for decades. According to [10], the global active IMD market was USD 15.21 billion in 2017, and is expected to grow to USD 30.42 billion by 2025. Over the last decade, IMDs have evolved significantly both internally and externally. Currently, IMDs are computationally much more complex and interconnected than ever before. Meanwhile, there is an ongoing effort towards reducing their size as much as possible in order to increase the patients' comfort[1].

Unlike old IMD generations, modern IMDs increasingly rely on a wireless interface to communicate with external devices. In particular, we can distinguish between programming devices through which doctors can wirelessly send commands to the IMD (e.g., to change the patient's therapy) and gather telemetry data, and monitoring devices—located in the patient's home—which periodically collect patients' medical data and send it to the hospital, thus enabling remote monitoring of the patient's condition when they are at home. One recent development that will further improve patients' care is the fact that IMDs have started to support standard wireless technologies (e.g., Bluetooth Low Energy (BLE)) [34, 36]. Clearly, such wireless connectivity provides greater convenience to patients and doctors and allows the realization of new use cases. Besides, it has shown great potential to improve the health system in the future [4]. For example, a patient carrying an IMD may undertake medical examinations and receive personalized treatment without the need to leave their houses.

However, wireless channels also introduce new security threats. For example, adversaries who are relatively close to the patient (i.e., a few meters away) may eavesdrop the wireless channel to learn sensitive patient information [48], or even worse, send malicious commands to the IMD to alter its settings. The consequences of these attacks can be very severe for patients, as these commands can allow adversaries to deliver (or disable) a therapy with the goal of causing serious injuries or even death. While no real attack against an IMD is known to date, past research has demonstrated that many IMDs available on the market today lack effective security mechanisms [14, 29–31, 48]. To resolve these issues, it is necessary to first establish a secure wireless communication channel between an IMD and an external device before any sensitive data or commands are transmitted. This can be achieved by running any secure *IMD key exchange* that allows the establishment of a shared cryptographic key between the IMD and the external device. However, establishing a shared key in this context can be a challenging task due to the characteristics of current IMDs: they have strict resource constraints, including limited memory and computational power. Furthermore, most IMDs are operated by a single non-rechargeable and non-replaceable battery. Once the battery is depleted, the patient typically needs to undergo surgery to get a new IMD, which always introduces risks. Additionally, IMDs have no physically accessible input or output interfaces (such as a keyboard or a screen) once they are implanted. Hence, wireless communication with the IMD is "invisible" to the patient and there is no means to physically allow communication (e.g., by pressing a button).

1.1 Related work on IMD key exchange methods

Several classes of solutions have been proposed for secure key exchanges between IMDs and external devices. We introduce them in the following.

Symmetric-key based. One approach to secure the connection between an IMD and an external device is by provisioning them with the same symmetric key during manufacturing. However, this is not compatible with the envisioned use of IMDs, where multiple personal devices, such as the patient's smartphone or the doctor's tablet, will need to be connected to the IMD during its lifetime (e.g., when patients change their smartphone or decide to go to another doctor). Equally, in an emergency situation (e.g., if the patient becomes unconscious or has

[1]For example, MICRA (one of the most advanced Medtronic pacemakers) is only about the size of a large vitamin capsule [38], which is significantly smaller than its predecessors like Medtronic Azure [36].

exacerbated symptoms) the doctor may need to get access to the patient's IMD immediately using a new device programmer. The problem is that this device programmer may not be able to retrieve the correct symmetric key on time (e.g., due to not being able to identify the patient or not having a stable connection with the cloud).

Halperin et al. proposed a key diversification protocol in order to address this issue [15]. In their protocol, external programming devices can derive the IMD's key (pre-installed during manufacturing) by using a key derivation function with a master key and the serial number of the IMD. In this way, secure communication can be established without requiring the external device to store a large number of symmetric keys or have access to the cloud. However, the master key is a single-point-of-failure, because it is shared by many external devices. All IMDs will be at stake if an adversary manages to obtain the master key from one of them (e.g., by stealing an external device and performing hardware attacks). Marin et al. proposed a solution to alleviate this problem by updating the master key periodically [29]. An adversary who obtains one master key can only derive valid symmetric keys of IMDs for a limited period of time. Nevertheless, the security of this method still depends on the assumption that the master key and the external devices are well protected, which is challenging to guarantee in practice. Overall, we conclude that key exchange by installing a symmetric key in the IMD is not a viable secure option in practical scenarios.

Public-key cryptography based. One can also leverage public-key cryptography to realize the key exchange. We provide a simple protocol as an example: the external device first transmits its public key to the IMD. Subsequently, the IMD generates a secret key, encrypts it using the received public key, and transmits the ciphertext to the external device. The security of the secret key is guaranteed because it can only be decrypted using the corresponding private key. However, the biggest challenge of such a public key-based solution is that it is hard for the IMD to verify the legitimacy of the public key, *i.e.*, decide whether it belongs to a legitimate entity instead of a malicious adversary. One can address this issue using digital certificates, which are widely used in e.g., the Transport Layer Security (TLS) protocol. However, a digital certificate system is hard to manage as it requires the establishment of a worldwide robust and costly Public Key Infrastructure (PKI). Moreover, because the external devices can be retired or compromised (e.g., stolen), the PKI must have proper mechanisms to revoke such illicit devices and update this information in the IMD. However, IMDs do not have an Internet connection to receive these updates, so in practice, using public-key solutions also poses a number of challenges.

Distance-bounding protocols. These protocols are built around the principle that an external device—which is physically close enough to the IMD (e.g., a few centimeters)—is legitimate, while any device that exceeds this distance limit is malicious [44, 45]. At the core of such solutions is a method that leverages cryptography in combination with physics to allow both devices to reliably and securely estimate the distance to the other.

Distance measurements can be realized by calculating the Round-Trip Time (RTT) of a signal, *i.e.*, the time interval between sending a challenge and receiving the response. However, it can be very difficult to implement this on resource-constrained IMDs: the IMD must be able to accurately measure the RTT even if the signal travels very fast, e.g., near the speed of light for a typical wireless signal. Moreover, the processing time (including the time to process the challenge and compute the response) of the IMD must be very stable. Otherwise, the external device cannot tell if a long RTT is caused by a distance beyond range, or a software delay occurs in the IMD. Both criteria assume that the IMD is computationally relatively powerful, where in reality it is not.

Rasmussen et al. proposed a concrete solution that uses ultrasound to calculate the distance, relying on the fact that adversaries cannot transmit data on the audio channel using a signal which propagates faster than the speed of sound [45]. A significant advantage is that the speed of sound is relatively low, thus alleviating the computational burden of the IMD to some extent. However, this workaround opens the door for wormhole attacks [53] and requires an ultrasound transceiver in the IMD, which may not be a viable option.

Proxy device-based protocols. These protocols delegate security to a proxy device which can be carried around by the patient (e.g., a bracelet) [5, 12, 62]. One of their main advantages is that they do not require to modify the IMD, which makes them suitable for legacy devices with no (or limited) security. Unlike IMDs, the

proxy device can have desirable hardware properties (e.g., higher computational power, rechargeable battery, Internet connection and input/output interfaces), which can be utilized to provide a high level of security, e.g., by using public-key cryptography between the proxy and an external device. After a secure connection is established between them, the proxy can distribute a session key to the IMD and the external device to build a secure channel. In emergency situations, a doctor can remove the proxy and connect with the IMD directly using an external device. However, this solution requires that a secure communication between the IMD and the proxy can be established, e.g., based on pre-installed symmetric keys, which again can be challenging in practice. Another drawback is that this method requires 24-hour wearing of the proxy device, which places the security burden on the patient, and also suffers in terms of usability and convenience. In addition, some concrete solutions [5, 12] also protect the IMD by using the proxy to jam the wireless channel, which can be illegal in certain countries.

1.2 Motivation

From the above discussion, it becomes apparent that conventional symmetric/public key based key exchange techniques and other solutions are often unsuitable (or even not viable) in the context of IMDs. Furthermore, some of the current solutions can only be applied in static contexts where the set of external devices the IMD can communicate to is very small and known at initialization time. This shows that there is a need for novel key exchange solutions that are secure, usable and deployable while at the same time being suitable for the new IMD generations.

Over the last decade, the usage of Out-Of-Band (OOB) channels has been proposed as a promising way to bootstrap security between an IMD and an external device that do *not* share any prior secrets beforehand. In this paper, we systematically specify properties of OOB channels, perform an in-depth analysis of existing OOB-based solutions for IMDs and propose a new class of key exchange protocols that leverage inertial sensors embedded within IMDs.

Our contributions

We make the following three key contributions:

- First, we systematize and analyze the use of OOB channels for key exchange with IMDs. In particular, we unify the requirements for an OOB key exchange protocol. Under this formalism, we review the OOB key exchange solutions in previous work and demonstrate that none of the methods proposed so far satisfies all the necessary requirements.
- Second, we identify that any OOB channel-based key exchange can benefit from being coupled with a Password-authenticated Key Agreement (PAKE) method. We formalize the security level of this construction.
- Third, we bring about new insights by proposing a new kind of OOB channel using patient motion as the information carrier. We study the suitability of this channel for secure key exchange and propose three protocols based on inertial sensors that are already available in state-of-the-art IMDs.

Our protocols are applicable to both dedicated, proprietary external devices developed by medical companies and off-the-shelf smartphones, which are of increasing importance in giving patients (some) access to their IMDs. For example, Medtronic has developed a smartphone app that allows the patient to view some basic characteristics of their pacemakers (such as remaining battery power) over a BLE link [35].

Paper Organization

The remainder of this paper is organized as follows. In Section 2, we define our attacker model and make security assumptions. In Section 3, we review the prior use of OOB channels for IMD key exchange. We propose a new construction of OOB key exchange in Section 4, before developing three protocols based on inertial sensors in Section 5. We conclude in Section 6.

2 ATTACKER MODEL AND ASSUMPTIONS

In this section, we define our attacker model and identify two security assumptions for the context of IMD key exchange that are well-accepted by the security community.

2.1 Attacker model

We consider a powerful and sophisticated adversary who has full knowledge of the key exchange protocol itself (but not the involved secrets) and has the following capabilities:

Attacks on the channel/network: We assume that the adversary has full control of the wireless channel. This implies that the adversary can either perform passive attacks by eavesdropping on the communication, or carry out active attacks, e.g., replay signals, modify/jam specific signals, or launch a Man-in-the-middle (MITM) attack. Furthermore, depending on the chosen OOB channel, the adversary might also be able to either eavesdrop or tamper with the data sent over the OOB channel. We elaborate more on this in Section 3.

Physical attacks: We assume that the adversary has the ability to steal relevant hardware, in particular a legitimate external device such as a programmer device from the hospital, or a patient's personal belonging such as a bracelet. We further assume that the adversary can analyze and reverse-engineer such devices, obtaining all firmware and cryptographic keys stored on the device.

Observation: We assume that the adversary can visually observe the complete key exchange process, *i.e.*, watch the patient directly or indirectly through a camera. This means that the adversary may obtain any secret information that is visible. Moreover, some protocols might involve physical actions of the user that are related to security, e.g., Xu et al. [63] proposed a pairing protocol where two wearables derive a key from the carrier's gait. In these cases, the adversary can launch simple or sophisticated mimicry attacks (e.g., computer vision technique-based attacks) with the aim to emulate the pairing operations of the user in order to compromise the protocol.

We acknowledge that the adversary might perform Denial-of-Service (DOS) attacks such as jamming the communication channel or depleting the IMD's battery by continuously sending pairing requests. However, these attacks are independent of the core protocol design and are out-of-scope for this paper. Moreover, they can be prevented by integrating existing solutions [49].

2.2 General assumptions

Touch-to-access access control. We inherit the widely accepted "touch-to-access" security assumption adopted by numerous researchers for IMD key exchange protocols [31, 50]: the adversary can be in proximity to the patient, however, can neither physically touch the patient without the patient noticing nor physically compromise a device worn by the patient. This touch-to-access access control model is widely used by the research community because it achieves a reasonable trade-off between security and availability for emergency situations, *i.e.*, the doctor can get access to the IMD by simply making physical contact with the patient (such as touching the skin for a while). Based on this assumption, we do not consider other attacks that require physical access to the patient, such as power analysis side-channel attacks [22] conducted on the IMD.

Patient awareness. We also point out a reasonable assumption that—outside of emergency situations—the patient has basic abilities to move physically and think properly. Otherwise, there are many more straightforward ways to cause severe impacts on the patient. Because the IMD and the patient are physically inseparable, it is reasonable to require the patient to take part of the responsibility for ensuring the IMD's security: the patient should be aware of environment changes and reject any anomalous touching unless in an emergency situation. Similarly, the patient should notice any abnormal signal indicating the IMD pairing process, such as strong continuous sound or vibration (that appears when the patient is not in hospital and under a routine examination), and react appropriately, e.g., by escaping the scene. We argue that the patient should not be responsible for

anything else. For example, the patient does not need to wear a proxy device to protect themselves or be able to detect a remote adversary who is eavesdropping the communication channel.

3 OUT-OF-BAND CHANNELS FOR IMD KEY EXCHANGE

The main intention of leveraging OOB channels for key exchange is that such channels are believed to be more secure in contrast to long-range wireless channels and thus are suitable for transmitting secret data. For example, our adversary is able to eavesdrop the wireless signals from a few meters away, however, may not be able to easily obtain the information transmitted through an OOB channel, e.g., an audio signal. Furthermore, the use of OOB channels does not rely on any prior shared information, which is especially advantageous in the context of IMD key exchange. Moreover, the use of an OOB channel might also bring about additional benefits. Consider the audio channel as an example again: an audio signal itself is detectable, which further increases the security because the user can perceive the occurrence of the data transmission.

In this section, we first define the (security) properties and types of OOB channels in Section 3.1. We then identify the requirements for OOB-based IMD key exchanges in Section 3.2, introduce existing approaches in previous work in Section 3.3, and provide a systematic assessment of these approaches in Section 3.4.

3.1 Property and type of OOB channels

OOB channels typically have more limited bandwidth compared to wireless channels, and data transmission and reception can be more costly (e.g., in terms of the energy consumption), possibly requiring additional hardware components such as an audio transceiver. Therefore, the OOB channels *cannot* replace wireless channels and are used only for transporting a small amount of data, *i.e.*, a session key (or a secret value from which a shared key can be generated). After a session key is agreed on, the parties can apply any standard encryption techniques and transmit the encrypted data through the wireless channel. In this paper, we view an OOB channel as a *directional channel from one sender to one or more legitimate receivers* that fulfills one or more of the following security properties:

Confidentiality: A confidential OOB channel is an OOB channel where the transmitted data can only be received by the legitimate receiver. It is hence resistant to eavesdropping (from a distance). We define a confidential OOB channel as:

Definition 3.1. Let s be a symbol transmitted over the OOB channel. Let P_c denote the probability that the adversary can correctly infer s by passively observing the channel. Then we call a channel confidential if $P_c < \epsilon_c$, where ϵ_c is the threshold at which P_c is negligible in the given context.

We note that the exact threshold ϵ at which we call P_c negligible depends on the properties of the protocol. For example, if the OOB channel is used to directly transport a long-term secret key, then to achieve 80-bit security, we need $\epsilon_c < 1/2^{80}$ to prevent offline bruteforce attacks. Conversely, if the OOB channel is used to exchange an ephemeral secret used in a PAKE [20], and the adversary only has a single attempt at completing the protocol, a much larger threshold, e.g., $\epsilon_c < 0.01$ might be acceptable. We further discuss these aspects in Section 5. A confidential channel is not necessarily resistant to spoofing or tampering. For example, an adversary might not be able to eavesdrop a low-power electric signal conducted through the patient's skin from a distance but might be able to overpower the signal with a very strong electro-magnetic field.

Authenticity: An authentic OOB channel is an OOB channel where the transmitted data is resistant to spoofing or tampering, but not necessarily resistant to eavesdropping:

Definition 3.2. Let s be a symbol transmitted by the legitimate sender over the OOB channel. Let s' be the symbol transmitted by the adversary. Then P_a denotes the probability that the legitimate receiver receives the

adversary's symbol s'. Then we call a channel authentic if $P_a < \epsilon_a$, where ϵ_a is the threshold at which P_a is negligible in the given context.

For example, the vibration channel from an external device to an IMD is often regarded as an authentic channel (see Section 3.3): only nearby devices can reliably receive such signals. If the attacker was to overpower the signal with a very strong vibration, this could be easily noticed by the patient. Conversely, this channel is not confidential, because vibrations can be picked up from a distance e.g., using suitable microphones or accelerometers, as shown by Halevi et al. [13].

Ideally, we would desire an OOB channel that is both confidential and authentic for an IMD key exchange. However, such a perfect channel does not exist in practice, as we will show in the following sections. Nevertheless, we may still leverage some imperfect OOB channels in combination with certain cryptographic techniques to realize secure IMD key exchanges (cf. Section 5).

Besides, we note that there are two types of OOB channels used in IMD key exchange: typically, the sender and receiver roles are held by IMD and external device, or vice versa. The IMD or external device is responsible for generating the secret and transmitting it to another side through an OOB channel. This guarantees the secrecy of the entropy source, *i.e.*, an adversary cannot obtain the original secret without physically accessing the device. However, we note that secret generation on these devices, especially to resource-constrained IMDs, might be a challenging task.

Alternatively, there is also the *shared entropy channel* that mitigates the above restriction: in this situation, both IMD and external device receive a (near) identical signal from a shared entropy source, e.g., some physical or physiological signal measured by both parties simultaneously. Subsequently, they derive a key by eliminating the mismatches on the signals, e.g., using a fuzzy cryptographic primitive [66]. For our work, we abstract this situation as a special case of an OOB channel: the sender is the entropy source while the receivers are the IMD and external device that can accurately measure it. For example, both devices can measure the heart rate of the patient and derive a shared key on this basis. We further detail this approach in Section 3.3. To ensure security, it is necessary that each separated channel (*i.e.*, from the entropy source to each individual party) is both confidential and authentic. Moreover, the entropy source should contain sufficient randomness. Otherwise, it may take a long measurement time to derive a secret from it.

3.2 Requirements

An OOB key exchange protocol for IMDs needs to satisfy a comprehensive set of security, usability, and deployability requirements. In this section, we summarize the core requirements that we identify:

(Sec 1) Channel-independent security. An adversary with full control of the wireless channel and certain control of the OOB channel (in terms of the properties in Section 3.1) must not be able to compromise the security of the protocol (e.g., must not be able to impersonate an IMD to the external device or vice versa). We will discuss the feasibility of the latter in the coming sections.

(Sec 2) Device-independent security. An adversary who can steal and fully analyze hardware involved in the key exchange (e.g., a programmer from hospital) must not be able to compromise the security of the protocol.

(Sec 3) Patient perception. Patients should be able to perceive the occurrence of the key exchange through certain feedback, e.g., vibration or touching the patient's body with the external device. This allows the patient to react to malicious situations. Thus, the adversary must not be able to conceal the feedback to the patient.

(Usa 1) Simplicity. Patients and doctors should be able to easily understand and learn the steps required for the key exchange process.

(Usa 2) Executability. A patient or doctor should be able to execute the steps of the protocol. Furthermore, the protocol should consider physical restrictions that the patient may have, e.g., some patients may be unable to hear certain sounds, especially in crowded places.

(Usa 3) Emergency availability. Medical personnel must be able to access a patient's IMD easily and quickly in emergency situations without relying on Internet connection or other long-range communication links.

(Dep 1) Additional hardware components. If necessary for key exchange, the protocol should only require additional hardware components that are acceptable for IMDs: this is especially in terms of the size of the additional hardware, which will inevitably compete for space with the battery. Furthermore, the additional component must not reduce the reliability or durability of the IMD: replacing the IMD during its lifetime requires unplanned surgery and additional risks to the patient.

(Dep 2) Execution time. The protocol must have a reasonable execution time: a long execution time (e.g., over one minute) can negatively affect the user experience and emergency availability. This is especially if the protocol can fail sometimes due to environmental conditions, e.g., paramedic operational mistakes, which could further increase the total execution time.

(Dep 3) Resource consumption. The protocol must consume acceptable resources on the IMD in terms of hardware (e.g., extra memory) and energy consumption. To ensure this, one should (i) carefully design and test the key exchange program on the IMD to guarantee that the medical functions are not affected, and (ii) minimize both computational and communication overheads to conserve battery. We note that the communication cost is typically dominant compared to the computation cost [56]. Besides, most of the battery energy is reserved for the medical functions and only a small portion can be used for communication and security bootstrapping.

3.3 Previous approaches for OOB key exchange

Using a tattoo or a bracelet (visual channel). One possible way for establishing a key between a device programmer and an IMD—both in normal and emergency situations—is to tattoo the IMD key on the patient's skin or to print it on a bracelet worn by the patient [52]. This solution costs little and places little burden on the IMD, however, the applicability of this idea is debatable. For example, a tattoo can become unreadable after an accident, can disclose the patient's condition to others, or be refused by patients due to the religious, aesthetic, or cultural concerns. Secondly, replacing the secret key on compromise is very difficult and requires tattoo removal. Equally, a bracelet can be damaged, lost, or stolen, which can lead to severe consequences.

Using audio channels. Halperin et al. [15] were the first to propose transmitting a key through an audio channel. One of the main advantages is that due to the nature of audio signals, patients can notice when a key exchange occurs. The main idea behind this solution is that the IMD generates a random session key and broadcasts it as a modulated sound wave (4 kHz signal generated by a piezo element embedded in the IMD) such that only an external device in close proximity (a few centimeters away) to the IMD can demodulate it correctly. However, Halevi and Saxena [13] showed that adversaries can accurately capture the sound using an off-the-shelf microphone from several meters away. By contrast, Siddiqi et al. [55] proposed an IMD key exchange scheme where the secret is transported using MHz-range ultrasound. The security of their solution is based on the assumption that the MHz ultrasound waves (generated by an IMD) can only be received by devices that touch the patient's body. However, the authors only verified this security assumption in an acoustic software simulation but not in a real hardware set-up. Moreover, it is also unclear if a MHz ultrasound transceiver can be miniaturized and embedded inside an IMD.

Using vibration channels. Similar to the audio channel, researchers proposed to use vibration for key exchange between an IMD and an external device. The transmitter device (typically the external device) requires a vibration motor to generate the vibration signal, while the receiver (typically the IMD) uses an accelerometer to receive it. Saxena et al. [51] were the first to propose transmitting a key to an IMD via the vibration channel. Similar to the audio channel solution, the activity of this channel is also perceivable by the patient. Crucially, unlike the audio channel, a strong advantage of this channel is that sending a vibration to an IMD requires the sender device

to directly touch the patient's body. However, the vibration is essentially a low-frequency audio signal, which also inevitably emits acoustic side-channel signals. To defend against an eavesdropping attack, Kim et al. [21] proposed to use Gaussian white noise to conceal the acoustic emanations. Anand and Saxena [2] further proposed to use a masking signal, which better conceals the acoustic emissions. However, whether these solutions are completely secure against eavesdropping attacks remains controversial. Moreover, they can increase the IMD's computational requirements.

Using the human body as a conductive channel. The human body can also be used for secret transmission due to its conductivity. A galvanic coupling technique was often proposed in this scenario. Concretely, the transmitter injects a low alternating current (e.g., 0.5 mA) into the skin/tissue, while the receiver can detect the voltage across two receiving electrodes elsewhere on the body. Wegmueller et al. [60] and Tomlinson et al. [58] proposed two implementations using galvanic coupling on an emulation of human tissue and skin, respectively. Marin et al. [31] also proposed a method where an electrical signal (secret key) is sent from a neurostimulator's case to an external device that touches the human skin. The common assumption of these solutions is that the current is absorbed by the tissue and emits little side-channel signals outside the body. Both [58] and [31] also tried to eavesdrop the emanations around the human body, but did not detect any. However, whether this method can totally defend against eavesdropping attacks is still debatable and requires further research. Moreover, this method generally assumes that injecting a low-enough current is harmless for a patient carrying implants. However, this statement is not based on examinations conducted on real patients, but based on theoretical data for healthy people [60] or doctors' experiences in medical practice [31]. To our knowledge, there is no proof that this method does not cause any side effects on a patient or an IMD. Furthermore, it is difficult to ensure that these solutions are reliable and robust under all circumstances, e.g., in an emergency.

Based on physiological signals. In addition to the aforementioned solutions, where one of the devices is always responsible for generating and transmitting the secret to the other via an OOB channel, there are also solutions that rely on a shared entropy channel like the patient's body. Poon et al. [42] were the first to propose the usage of physiological signals extracted from the patient for establishing a cryptographic key between two devices. As opposed to biometrics, where information is person-specific and to a large extent invariant, physiological signals are random signals that vary over time. For an overview on the security and functional requirements that a physiological signal must satisfy to be used in a cryptographic protocol, we refer the reader to [27]. A standard approach to establish a cryptographic key from the patient's body (acting as a shared entropy source and channel) consists of each device independently and synchronously taking a measurement of a chosen physiological signal. However, these measurements are typically not identical but at best rather similar due to the noise, and not necessarily uniformly distributed. Therefore, one cannot use them directly to establish a shared cryptographic key. Dodis et al. [6] and Linnartz and Tuyls [26] tackled this problem and proposed fuzzy cryptographic mechanisms, which, unlike standard cryptographic mechanisms, can tolerate a small amount of noise without compromising the required level of security. Prior work has mostly focused on the proposal of physiological signal-based solutions using fuzzy cryptographic primitives [28, 66].

As shown by Marin et al. [27], the security of physiological signal-based cryptographic protocols is questionable, with attacks exploiting weaknesses or limitations in the selection of the physiological signal, the design of the protocols, or even their implementation. For example, work by Lin et al. [25] and Rostami et al. [50] proposed to use the Inter-Pulse-Interval (IPI), *i.e.*, the time interval between two consecutive R-peaks of the Electrocardiogram (ECG) signal of the patient, to realize key exchange. However, Ortiz-Martin et al. [39] and Seepers et al. [54] have shown that IPI is not an appropriate selection. In addition, there is currently no known suitable physiological signal that meets all the requirements for being used in combination with fuzzy cryptographic protocols.

3.4 Limitations of previous OOB channel-based solutions

In this section, we evaluate previous OOB channel-based solutions against the requirements that we identified. The results are shown in Table 1 (for security and usability) and Table 2 (for deployability).

	Security			Usability		
	Channel-independent	Device-independent	Patient perception	Simplicity	Executability	Emergency availability
Using visual channels [52]	○	○	○	●	●	●
Using audio channels [15, 55]	○	●	●	●	●	●
Using vibration channels [2, 21, 51]	○	●	●	●	●	●
Using human body [31, 58, 60]	●	●	○	●	●	●
Based on physiological signals [25, 50]	○	●	○	●	●	●

Table 1. Evaluation of security and usability properties. Symbols indicate whether a solution fulfills (●) or does not fulfill (○) a certain evaluation criterion.

Security. Solutions based on the use of a visual, audio[2], vibration channel, or physiological signal have in common that they assume that the OOB channel is confidential. However, this assumption is hard to satisfy under a realistic adversary (e.g., who can steal personal belongings or perform an eavesdropping attack from several meters away), thus violating *Sec 1*. Besides, almost all methods (except for the visual channel-based one) satisfy *Sec 2* as they do not require the protection of relevant hardware to ensure security. As for *Sec 3*, we note that only the audio and vibration channel-based solutions are naturally perceivable by the patient.

Usability. All considered solutions are simple and executable by doctors and patients. The visual channel-based solution requires the user to manually retrieve the secret from a patient's tattoo or personal item, while other solutions merely require the user to hold the external device near the patient or attach it to the patient's skin. Moreover, all methods are plug-and-play and the key exchange process in emergency situations is identical to the one employed in hospitals.

Deployability. The deployability of a solution highly depends on the requirements and limitations of a specific application scenario. For example, a pacemaker is expected to have stricter size limitations than an insulin pump. Therefore, we do not make strict judgment on this criterion, but only provide the data from prior work as a reference in Table 2. Note that this data is not always complete, e.g., only a few work provided an estimated energy consumption value. Additionally, the visual channel-based method is presented more conceptually, rather than giving a concrete implementation. Furthermore, it only requires a symmetric key to be pre-installed, thus placing little burden on the IMD. Therefore, we omit it in the following.

For *Dep 1*, all protocols require additional hardware components in the IMD. In particular, the audio-based solutions require a piezo element [15] or a MHz-ultrasound transceiver [55]. The applicability of embedding

[2]Here, we only refer to the use of a low-frequency audio signal, as in [15]. A MHz-ultrasound channel is claimed to be a confidential channel in [55]. However, we argue that verifying this claim requires further testing.

Category	Additional components	Execution time	Energy consumption
Using audio channels	piezo element [15]; MHz-ultrasound transceiver [55]	0.4 s [15]; 2.56 ms (under theoretical 50 kbps) [55]	claimed negligible [15]; < 15 mJ [55]
Using vibration channels	accelerometer	85.3 s (zero error rate mode) [51]; 6.4 s [21]	< 4.5 mAh (over IMD's 90-month lifetime) [21]
Using human body	a pair of electrodes	1.5 s [31]; 2.56 ms [58]; 26.7 ms [60]	≤ 2.75 mJ [58]
Based on physiological signals	biosensor (e.g., ECG sensor)	40 s [25]; 24 - 32 s [28, 50]	≤ 19.68 mJ [25]

Table 2. Evaluation of deployability properties in terms of required additional hardware components, execution time, and energy consumption.

these components inside an IMD remains controversial. By contrast, the vibration and physiological signal-based solutions only require a sensor inside the IMD, *i.e.*, an accelerometer and biosensor (such as an ECG sensor), respectively. Such sensors have been highly miniaturized and extensively used in small-size Internet of Things (IoT) devices. The solution based on current transmission through the body requires a pair of electrodes or wires inside the IMD to receive the current, which can be easily embedded.

The execution time in Table 2 refers to the time used by the protocol to exchange a 128-bit secret key, which is typically sufficient for a body area network scenario[3]. For the physiological signal-based solution, this value is the total measurement time (we omit the time for other steps such as pre-processing, as it is trivial compared to the measurement time); while for the rest of the solutions, it is the time of secret transmission through an OOB channel, which only depends on the signal's data rate. We observe that the solutions based on audio channel and human body require little time to transmit a 128-bit key. By contrast, the vibration and physiological signal-based methods take significantly more time, which potentially violate *Dep 2*. We show how this can be mitigated to a large extent in Section 4.

We also show some energy consumption values in prior work. Among them, the physiological signal-based method consumes the most energy with 19.68 mJ per execution. To evaluate this value, we first estimate an IMD's battery capacity using state-of-the-art pacemakers as an example: The energy density of a pacemaker's Li/I_2 battery can reach 210 Wh/kg [1]. Hence, the energy contained in the pacemaker is approximate 4 Wh (14400 J) if the battery weighs 20 g—here estimated using the Medtronic Azure pacemaker [36] as an example and assuming the battery accounts for 80% of the total weight. Therefore, the energy consumption of prior work should generally satisfy *Dep 3*. Again, we emphasis that it is vital to test the energy consumption carefully on the resource-constrained IMDs.

Overall, we find that the prior IMD key exchange solutions based on an OOB channel lack comprehensive security considerations. Many OOB channels are not confidential channels as the authors expected. The requirement for patient perception is typically neglected. Conversely, all solutions perform well in terms of usability. Furthermore, the deployability of these solutions deserves more testing. Note that the comparison between existing solutions in terms of reliability is out of the scope of this paper. However, this should be considered before deploying any of these solutions in real devices.

4 A NEW CONSTRUCTION FOR IMD KEY EXCHANGE

Based on our requirements and analysis so far, we find that a new approach is needed for secure bootstrapping between an IMD and an external device. We propose some designs in Section 5. Before that, we first provide an insight that any OOB channel-based key exchange can benefit from being coupled with a PAKE (Password-authenticated Key Agreement) [20].

[3]Some protocols were not designed to transmit 128-bit secret—we thus estimate the theoretical execution time based on the data rate.

4.1 Usage of a PAKE

A PAKE aims to exchange a (high entropy) Long-Term Key (LTK) between parties who have already shared a (short, low-entropy) Short-Term Key (STK), and provides forward secrecy. A specific example of PAKE is Diffie-Hellman Encrypted Key Exchange (DH-EKE) [3]. Figure 1 shows our main idea: first, the external device and IMD initiate an STK exchange via an OOB channel. Subsequently and instantly, they execute a PAKE method and exchange a LTK. The prerequisite for successful PAKE execution is that both parties share the exact same STK; otherwise, the legitimate devices can detect a failure, thus abandon the current session and require a restart (*i.e.*, a new STK exchange).

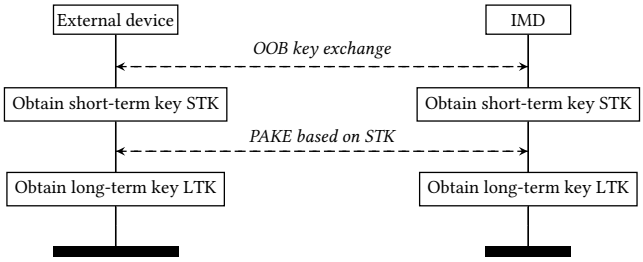

Fig. 1. PAKE coupled with OOB channel-based key exchange

The involvement of a PAKE has two major advantages. First, the protocol execution time can be reduced: the aim of a key exchange protocol is to establish a secure key of a certain length (most likely 128-bit); however, this can be slow over an OOB channel with low data rate. Therefore, one can exchange a short STK via the OOB channel first, and afterwards apply a PAKE protocol where STK is used to authenticate a LTK. The PAKE uses the normal wireless channel and is thus usually fast compared to the OOB exchange.

Second, the PAKE can also significantly reduce the threat by restricting the time window during which an adversary can conduct attacks. The STK agreed via an OOB channel is short-lived and only valid until the start of the PAKE. This means that the adversary must obtain the STK in a usually short timeframe, ruling out e.g., attacks with substantial exhaustive search components.

Only if the adversary successfully obtains the full STK during the limited time window, they can actively perform a MITM attack to impersonate the IMD and/or external device. However, the adversary still cannot obtain the LTK through passive observation. For example, assume DH-EKE is used as the PAKE, then the underlying Diffie-Hellman scheme naturally prevent the adversary from obtaining the exchanged key. Apart from this, we note that this construction also defends against offline brute-force attacks, where the adversary collects all information related to the key exchange process (e.g., communication traffic or video recording) and performs offline analysis to recover the LTK.

In this paper, we quantify the success probability of the adversary (*i.e.*, to conduct a successful MITM attack) against a PAKE construction, denoted as P_{adv}. We first define two types of MITM attacks that an adversary can conduct, and then identify possible adversary strategies and their corresponding P_{adv}. For simplicity, we assume that the adversary aims to impersonate the external device and connects with the IMD (which is normally the worst case) in the following, but note that the situation is similar if the target is the external device.

4.2 Attack types

An adversary can conduct two types of attacks during one protocol execution.

Attack 1: sniff STK. The external device exchanges an STK with IMD over an OOB channel and tries to complete PAKE on it, while the adversary in parallel sniffs the STK and tries to execute the PAKE concurrently. Let P_c (defined in Section 3.1) be the probability that the adversary succeeds in obtaining the STK. We assume that if the adversary can eavesdrop the STK, they can use it to complete the PAKE, and thus, the adversary's success probability is also P_c. Let Q_c be the probability that the legitimate external device succeeds in completing the PAKE with its exchanged STK. Given this, the probability that neither of them obtains STK (and hence the exchange fails) is denoted by $1 - P_c - Q_c$.

Attack 2: inject STK. Both external device and adversary try to actively exchange an STK with the IMD, each of them competing for the IMD to accept its STK and execute the PAKE. Let P_a (defined in Section 3.1) be the probability that IMD successfully exchanges with adversary's STK and completes PAKE with the adversary. Similarly, we assume that if the adversary is able to exchange an STK with the IMD, a PAKE can be completed between them. Q_a is the probability that the IMD successfully exchanges with the legitimate external device's STK and completes the PAKE with it; similarly, as before, $1 - P_a - Q_a$ denotes the probability that it fails to exchange an STK with either party.

The adversary's success probability of *Attack 1* and *Attack 2* depends on the confidentiality and authenticity of the OOB channel, respectively. As in Section 3.1, we use the criterion for a confidential OOB channel that $P_c < \epsilon_c$, where P_c is the probability that the adversary infers the full STK and we set $\epsilon_c < 0.01$ when a PAKE is used. In this case, the lower bound on the required STK entropy is 7 bit. However, this only holds if the adversary cannot obtain any side-channel information on the OOB channel and is purely limited to guessing STK. Hence, in practice longer STKs are required, where the length depends on the specific OOB channel.

Moreover, we emphasize that both P_c and P_a also depend on the precise attacker model. For example, while eavesdropping a low-power signal from a large distance might be infeasible (and hence a negligible P_c), if we admit an attacker in closer proximity to the victim/have a higher ability to observe on the OOB channel, P_c might increase drastically. We thus argue that the definition of a precise and realistic attacker model is of utmost importance to accurately assess the security of a given construction.

4.3 Adversary strategies

The key exchange protocol might fail under some circumstances, thus, should tolerate a certain number of restarts. Correspondingly, an adversary can conduct one of the above two MITM attacks during each protocol instance. The maximum number of restarts can be fixed by design. We denote by n the maximum tolerable number of protocol restarts. The adversary can choose multiple strategies depending on the precise attacker model, e.g., his prior knowledge of the security properties of the OOB channel, or his personal ability/cost to conduct an attack. In the following, we define three most likely strategies and calculate the corresponding P_{adv} values.

Strategy 1^n. In this case, the adversary keeps performing *Attack 1* for n times. The adversary succeeds if they succeed in the first attempt; or both (adversary and the external device) fail in the first attempt, and the adversary succeeds in the second attempt; etc.

Proposition 4.1. Given an adversary adopting *Strategy* 1^n,

$$P_{adv} = P_c + \phi P_c + \cdots + \phi^{n-1} P_c = \frac{P_c(1-\phi^n)}{1-\phi}, \text{ where } \phi = 1 - P_c - Q_c.$$

Proof. The first term corresponds to the case that the adversary succeeds in the first attempt; the second term corresponds to the case that the adversary succeeds in the second attempt; and so on. Note that these cases are

exclusive, and therefore can be summed. The adversary succeeds in the nth attempt if they fail in the first $n-1$ attempts (with probability ϕ^{n-1}) and succeed in the attempt after that (with probability P_c). □

Strategy 2^n. In this case, the adversary keeps performing *Attack 2* for n times.

Proposition 4.2. This case is similar with *Strategy* 1^n, with P_a and Q_a in place of P_c and Q_c respectively. Formally, given an adversary adopting *Strategy* 2^n,

$$P_{adv} = P_a + \psi P_a + \cdots + \psi^{n-1} P_a = \frac{P_a(1-\psi^n)}{1-\psi}, \text{ where } \psi = 1 - P_a - Q_a.$$

Strategy $(12)^{\frac{n}{2}}$. Alternatively, if an adversary has the ability to conduct both *Attack 1* and *Attack 2*, they can try combinations of these two attacks, hoping something will work. For example, an adversary may choose an obvious strategy such as $(12)^{\frac{n}{2}}$, *i.e.*, alternating between the two attacks.

Proposition 4.3. Given an adversary adopting *Strategy* $(12)^{\frac{n}{2}}$,

$$P_{adv} = P_c + \phi P_a + \phi\psi(P_c + \phi P_a) + \cdots + (\phi\psi)^{\frac{n}{2}-1}(P_c + \phi P_a) = \frac{(P_c+\phi P_a)(1-(\phi\psi)^{\frac{n}{2}})}{1-\phi\psi},$$
$$\text{where } \phi = 1 - P_c - Q_c \text{ and } \psi = 1 - P_a - Q_a.$$

Proof. The term $P_c + \phi P_a$ indicates the adversary's success probability after the first (12) attempt, and $\phi\psi(P_c + \phi P_a)$ indicates the success probability after the second (12), etc. The adversary succeeds in the $\frac{n}{2}$th attempt if they fail in the first $\frac{n}{2} - 1$ attempts (with probability $(\phi\psi)^{\frac{n}{2}-1}$) and succeed in the attempt after that (with probability $(P_c + \phi P_a)$). □

The optimal strategy of the adversary can vary under different circumstances. For example, if the adversary knows that P_c is much larger than P_a, they may try more *Attack 1* and not bother with *Attack 2*. Regardless, we note that P_{adv} is easy to calculate given another specific strategy. Furthermore, we can prove that P_{adv} is always less than some constant multiple of P_c or P_a.

Proposition 4.4. There is a constant k independent of P_c or P_a, such that:

- For Strategy 1^n, we have $P_{adv} \leq k \cdot P_c$.
- For Strategy 2^n, we have $P_{adv} \leq k \cdot P_a$.
- For Strategy $(12)^{\frac{1}{2}}$, we have $P_{adv} \leq k \cdot (P_c + \phi P_a)$.

Proof. Consider Strategy 1^n as an example. Since $1 - (1 - P_c - Q_c)^n \leq 1$ (remember that these are probabilities, hence in the interval $[0, 1]$), we have $P_c(1 - (1 - P_c - Q_c)^n) \leq P_c$; also $P_c + Q_c \geq Q_c$, and therefore

$$P_{adv} = \frac{P_c(1 - (1 - P_c - Q_c)^n)}{P_c + Q_c} \leq \frac{P_c}{Q_c} = k \cdot P_c$$

when we put $k = \frac{1}{Q_c}$. The argument for Strategies 2^n and $(12)^{\frac{n}{2}}$ is similar. □

To understand this proposition, let us assume for example an adversary who is adopting *Strategy* 1^n. Suppose the legitimate external device usually succeeds ($Q_c > 0.5$), and the adversary usually fails ($P_c < 0.1$), although the adversary has a substantial probability of causing the protocol to fail and have to be restarted. In this case, we see that $P_{adv} < 0.2$. The situation improves if the legitimate external device is more likely to succeed, e.g., if $Q_c = 0.9$ and $P_c < 0.1$, then we have $P_{adv} < 0.11$. These results show that the advantage the adversary gets of being able to force a restart of the protocol is fundamentally limited.

5 NEW PROTOCOLS FOR IMD KEY EXCHANGE

In this section, we explore the possibility of using existing or new OOB channels to realize secure, usable and deployable IMD key exchange. We start by reiterating two major pain points in previous approaches that we want to address in our work.

First, we aim to design a key exchange scheme to be compatible with either a conventional external device or an off-the-shelf consumer device (e.g., a smartphone), following the trend of modern IMD designs. However, this can be challenging because the smartphone is only designed for general tasks, unlike a dedicated programmer device that can be highly customized by medical device companies. Considering this, we want to leverage existing components on the smartphone and note that modern smartphones are equipped with various sensors, including inertial sensors (e.g., accelerometer and gyroscope). While being able to accurately measure motion-related data, the inertial sensors are becoming more miniaturized and energy efficient, which makes them appropriate for state-of-the-art IMDs. For example, the latest Medtronic pacemakers and ICDs already contain accelerometers for medical use[4] [33, 37, 43].

Second, we highly focus on patient perception (*Sec 3*) that is of great importance in the context of IMD key exchange. This can be introduced into a protocol in two general ways: by involving non-cancelable and perceivable signals such as vibration or audio; or by requiring mandatory and perceivable human behaviors. We argue that the latter might also benefit from the usage of inertial sensors (*i.e.*, the inertial sensors can measure certain behaviors).

5.1 OOB channels as building blocks

We outline several instances of OOB channels with different security properties in the context of IMD-smartphone key exchange.

Vibration channel. Based on prior work, the vibration channel from a smartphone to an IMD can always be regarded as an authentic channel [21, 51] in practice when an adversary is at (some) distance to the user. We inherit this assumption in our paper. Conversely, the vibration channel is not resistant to eavesdropping in proximity according to the literature [2, 13]. To ensure security, we assume $P_c = 1$, *i.e.*, this channel is not confidential and can be fully observed by an adversary.

Motion channel. Although inertial sensors were considered as components of some OOB channels (e.g., an accelerometer is used as a receiver in a vibration channel), the ability of such sensors to measure human body motion, which is one of the major functions of the inertial sensors in smartphones or smartwatches, has been largely ignored. By leveraging this ability, a new OOB channel can be constructed, where the sender is the patient and the receiver is a device carried by the patient (whether implanted or held in the hand). Human physical motion is the data carrier of this channel, measured by the inertial sensors embedded in the patient's devices. For our work, we abstract motion as a signal and call the corresponding channel that transmits the motion signal the *motion channel*.

First, we argue that the motion channel is authentic: a property of this channel is that its sender can only be the patient himself, thus the signal cannot be spoofed or tampered (assuming that the patient cannot be forced or fooled); while for the receiver side, the inertial sensor measurements of patient's devices should only depend on the patient (*i.e.*, cannot be remotely modified).

Next, we discuss the confidentiality of this channel. Consider the following scenario as an example: a patient performs a sequence of N motion events, where each event represents a fraction of the STK. The recipient device (e.g., the patient's pacemaker) measures the motions, derives the information embedded in each event, and

[4]An accelerometer is used to enable Medtronic's Rate Response feature, *i.e.*, adapt the pacemaker's pacing rate to changes in the patient's physical activity.

concatenates them together to reveal the original STK. An adversary can obtain STK if they can reveal each motion event by a mimicry attack. Suppose P_{mim} is the probability that a motion event is fully revealed in this way, and that motions are independent. Then, the probability that the adversary can reveal the whole STK is $P_c = (P_{mim})^N$. Note that the above is an upper bound: the adversary needs to control a camera or similar that has a clear view of the patient. However, this can be very challenging to launch especially in private places such as the patient's home or a consultation room in hospital.

The adversary can conduct a mimicry attack on a motion channel in two ways. First, by mimicking the patient themselves—first emulate the patient's environment (*i.e.*, by equipping the same inertial sensors attached to the same body location), then mimic the patient's motions simultaneously, trying to obtain sufficiently similar measurements (compared to the counterpart obtained on the patient's body). We expect P_{mim} to be relatively small in this case: due to the usage of a PAKE, the adversary only has *one* shot and thus must act accurately without any delays. This is expected to be very challenging considering the human reaction time [18]. The experimental results of mimicry attacks in [23, 24] confirm our expectations to a certain extent. Second, a more realistic way is to leverage computer vision techniques. In particular, an adversary can run a *real-time* machine learning model on camera-captured video to recognize the motion events. P_{mim} then may depend on various factors, such as the type of motion, type of camera (e.g., visible/depth/infrared thermal), and the camera's viewpoint [64]. We can roughly estimate P_{mim} from start-of-the-art Convolutional Neural Network (CNN) real-time motion recognition models [65]: the reported recognition accuracy varies between 61.5% and 86.4% on various datasets, which generally consist of over 100 motion classes and offer a large diversity in terms of people, camera type/viewpoint, etc. [19, 57].

Furthermore, we notice that an authentic and confidential motion channel has the potential to construct a shared entropy channel with the patient being the entropy source. Unlike solutions based on physiological signals, the randomness originates from the motions performed by the patient.

Smartphone-patient visual channel. When we consider the scenario of key exchange between a smartphone and an IMD, the smartphone can display information on the screen, which can be read by humans. We regard the visual channel from the smartphone screen to its owner, *i.e.*, the patient, as an authentic channel, assuming that the smartphone held by the patient is legitimate and not compromised. Note that this assumption is necessary, otherwise, there is no guarantee to exchange a key securely between the IMD and a smartphone.

So far we have several OOB channels with different security properties. Based on these building blocks, we next discuss three case studies in terms of using a confidential, authentic, and shared entropy OOB channel to build an IMD key exchange in our proposed formalism (cf. Section 3.2). We assume the IMD is a pacemaker and the external device is a smartphone, but note that the type of devices can be easily varied. As mentioned, the following OOB key exchanges only aim to exchange an STK. Afterwards, two devices apply a PAKE to agree on a LTK. We omit the latter step when we describe each instantiation for simplicity.

5.2 Key exchange based on a confidential channel

We first discuss if we can use a confidential OOB channel to realize IMD key exchange. Here we adopt a motion channel from the patient to the IMD and assume for the moment that it is confidential. This way, the patient can leverage this channel to actively pass a secret to their IMD by performing a series of motions, which can be identified by an inertial sensor.

There is one challenge: *How does the patient know what they need to do to transmit this secret?* We show our design in Figure 2. Here, we assign the task of secret generation to the patient's smartphone. Next, the smartphone truncates and maps the secret into a sequence of motions. The type of motions, as well as the mapping between each motion and a bitstring, should be previously defined by the IMD and smartphone. We do not assume that the mapping mechanism is secret—an adversary can easily obtain it by e.g., reverse engineering the mobile app.

Subsequently, the smartphone illustrates the motions on the screen in the form of an animation (authentic to the patient[5]). This way, the secret is translated from a bitstring into visual orders that can be easily understood by the patient. On the other hand, the protocol relies on the inertial sensor embedded in the IMD to recognize certain user motions, as has long been used reliably in smartphones and wearables [11, 46]. After obtaining a series of patient motions, the IMD concatenates them and reveals the original secret.

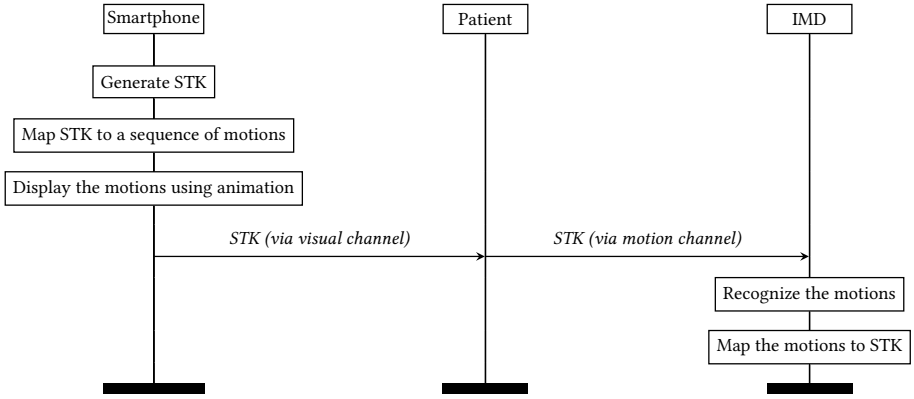

Fig. 2. Key exchange based on a confidential motion channel.

Now we study the feasibility of this instantiation. The protocol must meet the following core requirements at once:

- To ensure security, we require $P_c = (P_{mim})^N < \epsilon_c$. Thus, the number of motions $N > \log_{P_{mim}}(0.01)$.
- For usability, the motion must be executable for the patient. For example, complex motions may be hard to perform and strenuous motions may cause dizziness.
- For deployability, the motions cannot pose too long execution time (denoted as T).

We make a reasonable design decision that each motion is required to be completed in three seconds (taking into account the patient's physical conditions). Then we have $T > 3 \cdot \log_{P_{mim}}(0.01)$. Suppose P_{mim} is correlated with the complexity of the motion, *i.e.*, a more complex motion brings about a smaller P_{mim} and vice versa [59]. This way, the instantiation requires a trade-off between usability and deployability. For example, suppose we select a complex enough motion type with $P_{mim} = 61.5\%$ (the lower bound from previous work, cf. Section 5.1), then we have $T > 28.4$ seconds. If the motion is 'simpler' (and hence larger P_{mim}), T increases accordingly. In the following, we propose a potentially feasible construction in the context of IMDs. We highlight that one needs to empirically determine the value of P_{mim} under a specific attacker model.

Construction 5.1. The type of motion that the user must carry out can be "rotate your body towards a certain direction", e.g., rotate 30 degrees to the right. To better assist the patient with doing this, the animation can be designed as a compass, *i.e.*, change the direction of the pointer as the patient moves, and give positive feedback

[5]However, the animation is not necessarily confidential. This is similar to entering a PIN at an ATM machine. In this way, the patient can be advised that they need to be careful of "shoulder surfing" [9].

(e.g., a sound or vibration) when reaching the target position. Additionally, the rotating angle and direction can be accurately recognized using a gyroscope inside the IMD and smartphone [41].

5.3 Key exchange based on an authentic channel

We next discuss the possibility of using authentic channels for key exchange. As mentioned before, a vibration or motion channel can be regarded as authentic (at a distance) in the IMD context.

We propose to combine an authentic channel with a public key cryptosystem to circumvent the limitations of the latter (see Section 1.1). The main idea is shown in Figure 3: a smartphone sends its Public Key (PK) to the IMD via an authentic channel. Subsequently, the IMD generates an STK, encrypts it using PK, and sends the ciphertext to the smartphone through a wireless channel. Finally, the smartphone reveals the STK using its Private Key (SK). In this scheme, an adversary will not learn any secret even if they can eavesdrop on the OOB channel or wireless channel. The adversary may tamper with the wireless signal, however, this can at most result in a failure of key exchange and can be noticed in a subsequent key confirmation process.

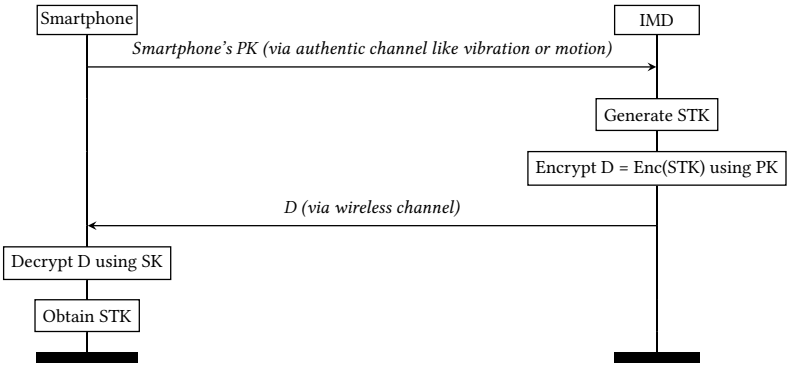

Fig. 3. Key exchange based on an authentic channel.

The PK transmission can be time-consuming due to the relatively slow data rate of OOB channels. We base the public key size to 160-bit that comes from the advanced Elliptic Curve-based public key schemes that provide 80-bit security [8]. Accordingly, we can estimate the time cost on a vibration channel based on [21], where a smartphone is able to transmit 20 bps to an IMD through a vibration. This way, we expect to transmit the PK in 8 seconds. For the motion channel, the transmission speed depends on the entropy of the selected motion. We show this can be troublesome: suppose we use the rotation motion in Construction 5.1, and we limit the maximum rotation angle per motion to 90 degrees and set every ten degrees as an interval (*i.e.*, the required rotation angle can be ten, twenty degrees, etc.), we have in total 18 combinations—about 4-bit entropy per motion only. Inheriting the previous design where each motion takes three seconds, the PK transmission takes 120 seconds, which is much longer than the counterpart of vibration channel. Thus, the vibration channel may be a better choice.

Additionally, Figure 3 is vulnerable to a MITM attack. If the adversary can eavesdrop the PK, they can do the same thing as the IMD does, *i.e.*, generate a fake secret, encrypt it using the PK and send it to the legitimate smartphone. Precisely, this attack can be performed by sending the signal (D) faster than the IMD (with the help

of a much more powerful device than the IMD), or by intercepting the IMD's D and sending their own. This can trick the smartphone to pair the adversary's device, causing e.g., the IMD to not receive important commands from the legit device.

To address this, IMD needs to prove its identity to the smartphone. This forms an *entity authentication* [67] problem, which is often resolved by the claimant showing the possession of the same (or sufficiently similar) secret (named *evidence* in the following) shared with the verifier. Because the IMD and the smartphone do not share any prior secrets beforehand, we need a shared entropy channel here to generate a short and ephemeral evidence for authentication. For the moment, we assume that the chest area can make a qualified shared entropy source where the IMD and smartphone can derive a similar evidence by simultaneously measuring the accelerometer[6] data. Based on this assumption, we propose the following construction.

Construction 5.2. We present the idea in Figure 4. After PK is transmitted, the smartphone and IMD synchronize with each other, measure the accelerometer data for a period of time and derive an evidence (denoted by E_s and E_i, respectively) from the measurements. The evidences might vary slightly due to the noise introduced by the measuring process. Subsequently, the IMD encrypts both STK and E_i using PK, then sends the ciphertext to the smartphone. The smartphone verifies the identity of the received message based on a pre-defined similarity threshold, and accepts STK if the condition is met.

We further discuss the possibility of constructing a shared entropy channel in the chest area in Section 5.4. Note that even if this is not viable, our initial instantiation still has value because it protects STK and eliminates the possibility that an adversary pairs with the IMD (which is the worst case).

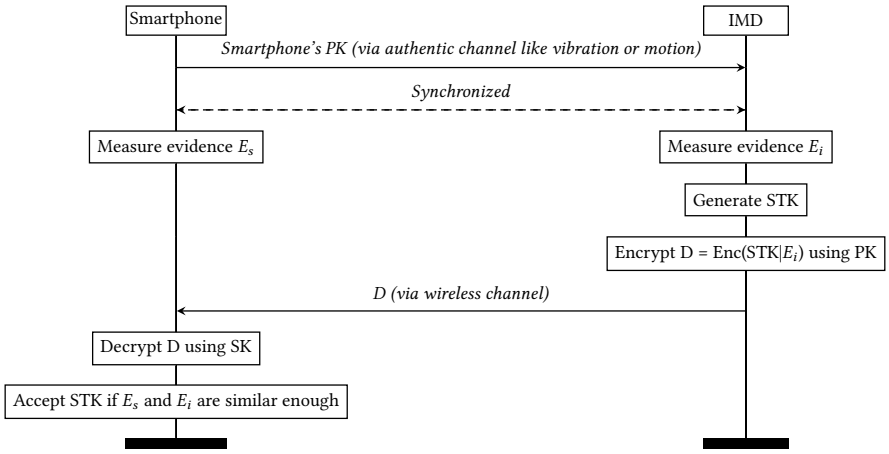

Fig. 4. Key exchange based on an authentic channel (enhanced)

[6]We exclusively use accelerometers here because the IMD also requires an accelerometer to receive the vibration signal, *i.e.*, PK.

5.4 Key exchange based on shared entropy channel

Finally, we study the use of the patient themselves as a shared entropy source for IMD key exchange. Relevant research exist that explore this approach for pairing between IoT/wearable devices. We show the work that only require an inertial sensor in the following. In general, we observe that the entropy can originate from two main sources.

Entropy originates from random human motions. Specifically designed for wearables, Xu et al. [63] and Revadigar et al. [47] realized key exchange based on simultaneous accelerometer measurements while the user is walking (the randomness is extracted from user's gait). Mayrhofer and Gellersen [32] and Hinckley [17] proposed key exchange between two IoT devices by holding them together in the hand and shaking them. Li et al. [24] proposed a key exchange method between an IoT device that contains a button/knob/tangible screen and a smartphone, where both the IoT device and the smartphone measure the timing information (e.g., the time of pressing a button) of a series of motions (e.g., randomly press and release the button) and extract a secret from it. The timing information can be obtained from accelerometer or gyroscope measurements.

However, all these solutions are not directly transferable to the IMDs because they generally require physical contact with IoT devices, while the IMDs are inaccessible once implanted. Besides, they do not take into account the emergency situation. We then propose a construction viable for the IMD context.

Construction 5.3. To exchange a key between an IMD and a smartphone, the patient or doctor is required to randomly tap the patient's chest with a smartphone over a certain period. The entropy comes from the timing information of the tapping, which can be measured using inertial sensors embedded in both devices.

One major concern is that the timing information of the taps is potentially exploitable to an adversary using a camera or microphone in proximity, a point also mentioned in [23, 24]. We can roughly estimate the eavesdropping capability of the adversary from state-of-the-art video-based periodic motion detection models (not real-time) [7, 40]. These models are able to detect the occurrence of certain periodic motions from long videos, which is exactly applicable to our scenario. In [7, 40], the model recall value (the ratio of successfully recognized motions to all motions appearing in the video) reaches up to 85.9%. This indicates that at least 30 taps are required to ensure $P_{mim} < \epsilon_c$. Again, it is worthy of further research to study the impact of a real-time camera/microphone based attack.

Entropy originates from unique physical properties of body. Wei et al. [61] proposed a secret exchange between an IoT device and a wearable that contains a vibration motor. By having the user (with a wearable worn) touch the IoT device and the motor release a vibration, both devices can derive a common secret from accelerometer measurements that embody the resonance properties of the hand area. The authors claimed that the resonance properties are variable both within and between subjects, and that this construction emits little side-channel information of the secret.

Note that [61] is not based on a vibration channel. The vibration is merely used to excite the human body so that the resonance properties can be captured using off-the-shelf accelerometers. We argue that their work is potentially transplantable to our context by changing the location from hand to chest.

5.5 Usability Analysis

We analyze our proposed constructions in terms of usability. All three constructions generally satisfy the requirements on simplicity (*Usa 1*) and executability (*Usa 2*). In particular, Construction 5.2 (based on a vibration channel) is the simplest and easiest to execute from the perspective of a patient or doctor, followed by Construction 5.3 (based on taps) and Construction 5.1 (based on rotations). The former one only requires the smartphone to be attached to the patient's chest area. Besides, this protocol promises to be appropriate to execute for a patient because a smartphone vibration is normal in daily life. By contrast, Construction 5.3 can be harder to perform as it

requires random taps. Construction 5.1 is relatively more challenging for a patient as it involves body movement and interactions with animated instructions, like a game or exercise.

In terms of requirement on emergency availability (*Usa 3*), Construction 5.3 and Construction 5.2 can work in emergencies because the motions (tapping or attaching) can also be performed by doctors. Conversely, Construction 5.1 does not really work in emergencies. Nevertheless, we note that this solution may be potentially applied in special treatments, e.g., when the patient needs certain physical entertainment to improve memory, concentration and mental health [16].

6 CONCLUSION

In this paper, we systematically and fairly analyze previous approaches of IMD key exchange, and specifically focus on the use of OOB channels. We identify the necessary security, usability and deployability requirements that an IMD key exchange needs to satisfy, and show that none of the prior solutions satisfies all requirements at once. Subsequently, we present the insight that an OOB key exchange benefits from being combined with a PAKE, and provide security evaluations of this construction. Finally, we propose a new OOB channel that uses patient motion as the information carrier, and develop three protocols based on this channel using inertial sensors. The ubiquity of inertial sensors in today's commercial smart devices and IMDs maximizes the chance of widespread acceptance of our designs. We analyze our protocols in the proposed formalism and discuss their advantages and disadvantages depending on the application scenario and attacker model. Overall, we hope that our work will serve as a reference to more systematically reason about the use of OOB channels together with cryptographic protocols for key exchange in body area networks.

REFERENCES

[1] Achraf Ben Amar, Ammar B Kouki, and Hung Cao. 2015. Power approaches for implantable medical devices. *sensors* 15, 11 (2015), 28889–28914.

[2] S Abhishek Anand and Nitesh Saxena. 2017. Coresident evil: Noisy vibrational pairing in the face of co-located acoustic eavesdropping. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 173–183.

[3] Steven Michael Bellovin and Michael Merritt. 1992. Encrypted key exchange: Password-based protocols secure against dictionary attacks. (1992).

[4] Michele De Santis and Ilaria Cacciotti. 2020. Wireless implantable and biodegradable sensors for postsurgery monitoring: Current status and future perspectives. *Nanotechnology* 31, 25 (2020), 252001.

[5] Tamara Denning, Kevin Fu, and Tadayoshi Kohno. 2008. Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security.. In *HotSec*.

[6] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. 2004. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *Advances in Cryptology - EUROCRYPT*. 523–540.

[7] Debidatta Dwibedi, Yusuf Aytar, Jonathan Tompson, Pierre Sermanet, and Andrew Zisserman. 2020. Counting out time: Class agnostic video repetition counting in the wild. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 10387–10396.

[8] ECRYPT-CSA. 2018. Algorithms, key size and protocols report. (2018). https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

[9] Malin Eiband, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 4254–4265.

[10] GlobeNewswire. 2019. Global Active Implantable Medical Devices Market is Expected to Reach USD 30.42 Billion by 2025. https://www.globenewswire.com/news-release/2019/08/08/1898922/0/en/Global-Active-Implantable-Medical-Devices-Market-is-Expected-to-Reach-USD-30-42-Billion-by-2025-Fior-Markets.html.

[11] Alan Godfrey, AK Bourke, GM Olaighin, P Van De Ven, and J Nelson. 2011. Activity classification using a single chest mounted tri-axial accelerometer. *Medical engineering & physics* 33, 9 (2011), 1127–1135.

[12] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. 2011. They can hear your heartbeats: non-invasive security for implantable medical devices. In *Proceedings of the ACM SIGCOMM 2011 conference*. 2–13.

[13] Tzipora Halevi and Nitesh Saxena. 2010. On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping. In *Proceedings of the 17th ACM conference on Computer and communications security*. 97–108.

[14] Daniel Halperin, Thomas S Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H Maisel. 2008. Security and privacy for implantable medical devices. *IEEE pervasive computing* 7, 1 (2008), 30–39.
[15] Daniel Halperin, Thomas S Heydt-Benjamin, Benjamin Ransford, Shane S Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H Maisel. 2008. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 129–142.
[16] Maryam Hedayati, Shima Sum, Seyed Reza Hosseini, Mahbobeh Faramarzi, and Samaneh Pourhadi. 2019. Investigating the effect of physical games on the memory and attention of the elderly in adult day-care centers in Babol and Amol. *Clinical interventions in aging* 14 (2019), 859.
[17] Ken Hinckley. 2003. Synchronous gestures for multiple persons and computers. In *Proceedings of the 16th annual ACM symposium on User interface software and technology*. 149–158.
[18] Aditya Jain, Ramta Bansal, Avnish Kumar, and KD Singh. 2015. A comparative study of visual and auditory reaction times on the basis of gender and physical activity levels of medical first year students. *International Journal of Applied and Basic Medical Research* 5, 2 (2015), 124.
[19] Y.-G. Jiang, J. Liu, A. Roshan Zamir, G. Toderici, I. Laptev, M. Shah, and R. Sukthankar. 2014. THUMOS Challenge: Action Recognition with a Large Number of Classes. http://crcv.ucf.edu/THUMOS14/.
[20] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. 2002. Forward secrecy in password-only key exchange protocols. In *International Conference on Security in Communication Networks*. Springer, 29–44.
[21] Younghyun Kim, Woo Suk Lee, Vijay Raghunathan, Niraj K Jha, and Anand Raghunathan. 2015. Vibration-based secure side channel for medical devices. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 1–6.
[22] Paul Kocher, Joshua Jaffe, Benjamin Jun, et al. 1998. Introduction to differential power analysis and related attacks.
[23] Xiaopeng Li, Fengyao Yan, Fei Zuo, Qiang Zeng, and Lannan Luo. 2019. Touch well before use: Intuitive and secure authentication for iot devices. In *The 25th annual international conference on mobile computing and networking*. 1–17.
[24] Xiaopeng Li, Qiang Zeng, Lannan Luo, and Tongbo Luo. 2020. T2Pair: Secure and Usable Pairing for Heterogeneous IoT Devices. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 309–323.
[25] Qi Lin, Weitao Xu, Jun Liu, Abdelwahed Khamis, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. 2019. H2B: Heartbeat-based secret key generation using piezo vibration sensors. In *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*. 265–276.
[26] Jean-Paul Linnartz and Pim Tuyls. 2003. New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. In *Proceedings of the 4th International Conference on Audio- and Video-Based Biometric Person Authentication* (Guildford, UK) *(AVBPA'03)*. Springer-Verlag, Berlin, Heidelberg, 393–402.
[27] Eduard Marin, Enrique Argones Rúa, Dave Singelée, and Bart Preneel. 2019. On the Difficulty of Using Patient's Physiological Signals in Cryptographic Protocols. In *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*. 113–122.
[28] Eduard Marin, Mustafa A Mustafa, Dave Singelée, and Bart Preneel. 2016. A privacy-preserving remote healthcare system offering end-to-end security. In *International Conference on Ad-Hoc Networks and Wireless*. Springer, 237–250.
[29] Eduard Marin, Dave Singelée, Flavio D Garcia, Tom Chothia, Rik Willems, and Bart Preneel. 2016. On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them. In *Proceedings of the 32nd annual conference on computer security applications*. 226–236.
[30] Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede, and Bart Preneel. 2016. On the feasibility of cryptography for a wireless insulin pump system. In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*. 113–120.
[31] Eduard Marin, Dave Singelée, Bohan Yang, Vladimir Volski, Guy A. E. Vandenbosch, Bart Nuttin, and Bart Preneel. 2018. Securing Wireless Neurostimulators. In *Proceedings of Conference on Data and Application Security and Privacy (CODASPY)* (Tempe, AZ, USA). 287–298.
[32] Rene Mayrhofer and Hans Gellersen. 2007. Shake well before use: Authentication based on accelerometer data. In *International Conference on Pervasive Computing*. Springer, 144–161.
[33] Medtronic. 2016. Rate Response (RR) Feature. https://www.medtronicacademy.com/features/rate-response-rr-feature.
[34] Medtronic. 2021. Insulin pump systems. https://www.medtronic.com/us-en/healthcare-professionals/products/diabetes/insulin-pump-systems.html.
[35] Medtronic. 2021. MyCarelink heart mobile app. https://global.medtronic.com/xg-en/mobileapps/patient-caregiver/cardiac-monitoring/mycarelink-heart-app.html.
[36] Medtronic. n.d.. Medtronic Azure XT SR MRI Surescan model W2SR01. https://europe.medtronic.com/content/dam/medtronic-com/xd-en/hcp/documents/azure-specsheet-model-w2sr01.pdf.
[37] Medtronic. n.d.. Medtronic Sensor. https://www.cardiocases.com/en/pacingdefibrillation/specificities/programming-exercise/medtronic/medtronic-sensor.
[38] Medtronic. n.d.. MICRA: the leadless pacemaker. https://www.medtronic.com/uk-en/c/emea/cardiac-rhythm/micra-leadless-pacemaker.html.

[39] Lara Ortiz-Martin, Pablo Picazo-Sanchez, Pedro Peris-Lopez, and Juan Tapiador. 2018. Heartbeats do not make good pseudo-random number generators: An analysis of the randomness of inter-pulse intervals. *Entropy* 20, 2 (2018), 94.
[40] Costas Panagiotakis, Giorgos Karvounas, and Antonis Argyros. 2018. Unsupervised detection of periodic segments in videos. In *2018 25th IEEE International Conference on Image Processing (ICIP)*. IEEE, 923–927.
[41] Damrongrit Piyabongkarn, Rajesh Rajamani, and Michael Greminger. 2005. The development of a MEMS gyroscope for absolute angle measurement. *IEEE transactions on control systems technology* 13, 2 (2005), 185–195.
[42] C.C.Y. Poon, Yuan-Ting Zhang, and Shu-Di Bao. 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine* 44, 4 (2006), 73–81. https://doi.org/10.1109/MCOM.2006.1632652
[43] Venkata K Puppala, Benjamin C Hofeld, Amberly Anger, Sudhi Tyagi, Scott J Strath, Judith Fox, Marcie G Berger, Kwang Woo Ahn, and Michael E Widlansky. 2020. Pacemaker detected active minutes are superior to pedometer-based step counts in measuring the response to physical activity counseling in sedentary older adults. *BMC geriatrics* 20, 1 (2020), 1–11.
[44] Kasper Bonne Rasmussen and Srdjan Capkun. 2010. Realization of RF Distance Bounding.. In *USENIX Security Symposium*. 389–402.
[45] Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S Heydt-Benjamin, and Srdjan Capkun. 2009. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM conference on Computer and communications security*. 410–419.
[46] Nishkam Ravi, Nikhil Dandekar, Preetham Mysore, and Michael L Littman. 2005. Activity recognition from accelerometer data. In *Aaai*, Vol. 5. Pittsburgh, PA, 1541–1546.
[47] Girish Revadigar, Chitra Javali, Weitao Xu, Athanasios V Vasilakos, Wen Hu, and Sanjay Jha. 2017. Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. *IEEE Transactions on Information Forensics and Security* 12, 10 (2017), 2467–2482.
[48] Luca Reverberi and David Oswald. 2017. Breaking (and fixing) a widely used continuous glucose monitoring system. In *11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17)*.
[49] Melanie R Rieback, Bruno Crispo, and Andrew S Tanenbaum. 2005. RFID Guardian: A battery-powered mobile device for RFID privacy management. In *Australasian Conference on Information Security and Privacy*. Springer, 184–194.
[50] Masoud Rostami, Ari Juels, and Farinaz Koushanfar. 2013. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. In *Proceedings of Conference on Computer and Communications Security (CCS)*. 1099–1112. https://doi.org/10.1145/2508859.2516658
[51] Nitesh Saxena, Md Borhan Uddin, Jonathan Voris, and N Asokan. 2011. Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags. In *2011 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 181–188.
[52] Stuart Schechter. 2010. Security that is meant to be skin deep using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices. (2010).
[53] S Sedihpour, Srdjan Capkun, Saurabh Ganeriwal, and Mani Srivastava. 2005. Implementation of attacks on ultrasonic ranging systems. In *Demo at the ACM Conference on Networked Sensor Systems (SenSys)*, Vol. 10. 1098918–1098977.
[54] Robert Mark Seepers, Wenjin Wang, Gerard De Haan, Ioannis Sourdis, and Christos Strydis. 2017. Attacks on heartbeat-based security using remote photoplethysmography. *IEEE journal of biomedical and health informatics* 22, 3 (2017), 714–721.
[55] Muhammad Ali Siddiqi, Robert HSH Beurskens, Pieter Kruizinga, Chris I De Zeeuw, and Christos Strydis. 2021. Securing Implantable Medical Devices Using Ultrasound Waves. *IEEE Access* (2021).
[56] Dave Singelée, Stefaan Seys, Lejla Batina, and Ingrid Verbauwhede. 2015. The energy budget for wireless security: Extended version. (2015).
[57] K. Soomro, A. Roshan Zamir, and M. Shah. 2012. UCF101: A Dataset of 101 Human Actions Classes From Videos in The Wild. In *CRCV-TR-12-01*.
[58] William J Tomlinson, Stella Banou, Christopher Yu, Michele Nogueira, and Kaushik R Chowdhury. 2019. Secure on-skin biometric signal transmission using galvanic coupling. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 1135–1143.
[59] LiMin Wang, Yu Qiao, and Xiaoou Tang. 2013. Mining motion atoms and phrases for complex action recognition. In *Proceedings of the IEEE international conference on computer vision*. 2680–2687.
[60] Marc Simon Wegmueller, Sonja Huclova, Juerg Froehlich, Michael Oberle, Norbert Felber, Niels Kuster, and Wolfgang Fichtner. 2009. Galvanic coupling enabling wireless implant communications. *IEEE Transactions on Instrumentation and Measurement* 58, 8 (2009), 2618–2625.
[61] Wang Wei, Lin Yang, and Qian Zhang. 2018. Resonance-based secure pairing for wearables. *IEEE Transactions on Mobile Computing* 17, 11 (2018), 2607–2618.
[62] Fengyuan Xu, Zhengrui Qin, Chiu C Tan, Baosheng Wang, and Qun Li. 2011. IMDGuard: Securing implantable medical devices with the external wearable guardian. In *2011 Proceedings IEEE INFOCOM*. IEEE, 1862–1870.
[63] Weitao Xu, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. 2016. Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication. In *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 1–12.

[64] Guangle Yao, Tao Lei, and Jiandan Zhong. 2019. A review of Convolutional-Neural-Network-based action recognition. *Pattern Recognition Letters* 118 (2019), 14–22. https://doi.org/10.1016/j.patrec.2018.05.018 Cooperative and Social Robots: Understanding Human Activities and Intentions.

[65] Bowen Zhang, Limin Wang, Zhe Wang, Yu Qiao, and Hanli Wang. 2016. Real-time action recognition with enhanced motion vector CNNs. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2718–2726.

[66] Mo Zhang, Eduard Marin, David Oswald, and Dave Singelée. 2021. FuzzyKey: Comparing Fuzzy Cryptographic Primitives on Resource-Constrained Devices. (2021).

[67] Robert Zuccherato. 2005. *Entity Authentication*. Springer US, Boston, MA, 203–203. https://doi.org/10.1007/0-387-23483-7_144