OpSecure: A Secure Unidirectional Optical Channel for Implantable Medical Devices

Arsalan Mosenia, *Student Member, IEEE*, and Niraj K. Jha, *Fellow, IEEE*

Abstract—Implantable medical devices (IMDs) are opening up new opportunities for holistic healthcare by enabling continuous monitoring and treatment of various medical conditions, leading to an ever-improving quality of life for patients. Integration of radio frequency (RF) modules in IMDs has provided wireless connectivity and facilitated access to on-device data and post-deployment tuning of essential therapy. However, this has also made IMDs susceptible to various security attacks. Several lightweight encryption mechanisms have been developed to prevent well-known attacks, e.g., integrity attacks that send malicious commands to the device, on IMDs. However, lack of a secure key exchange protocol (that enables the exchange of the encryption key while maintaining its confidentiality) and the immaturity of already-in-use wakeup protocols (that are used to turn on the RF module before an authorized data transmission) are two fundamental challenges that must be addressed to ensure the security of wireless-enabled IMDs.
In this paper, we introduce OpSecure, an optical secure communication channel between an IMD and an external device, e.g., a smartphone. OpSecure enables an intrinsically user-perceptible unidirectional data transmission, suitable for physically-secure communication with minimal size and energy overheads. Based on OpSecure, we design and implement two protocols: (i) a low-power wakeup protocol that is resilient against remote battery-draining attacks, and (ii) a secure key exchange protocol to share the encryption key between the IMD and the external device. We evaluate the two protocols using a human body model.

Index Terms—Battery-draining attack, encryption, healthcare, implantable medical device, key exchange, radio frequency module, security attack, smartphone, wakeup, wireless communication.

This paper can be cited as: A. Mosenia and N. K. Jha, "OpSecure: A Secure Unidirectional Optical Channel for Implantable Medical Devices," in IEEE Trans. Multi-scale Computing Systems (TMSCS).
The latest version of this manuscript is available on IEEE Xplore

1 Introduction

Implantable medical devices (IMDs) are revolutionizing healthcare by offering continuous monitoring, diagnosis, and essential therapies for a variety of medical conditions. They can capture, process, and store various types of physiological signals, and are envisioned as the key to enabling a holistic approach to healthcare [1]. Rapid technological advances in wireless communication, sensing, signal processing, and low-power electronics are transforming the design and development of IMDs. State-of-the-art IMDs, e.g., pacemakers and implantable drug infusion systems, commonly support short-range wireless connectivity, which enables remote diagnosis and/or monitoring of chronic disorders and post-deployment therapy adjustment [2]. Moreover, wireless connectivity allows healthcare professionals to non-intrusively monitor the device status, e.g., physicians can gauge the device battery level without performing any surgery.

Despite the numerous services that wireless connectivity offers, it may make an IMD susceptible to various security attacks. Previous research efforts [2]–[7] have demonstrated how wireless connectivity may be a security loophole that can be exploited by an attacker. For example, Halperin et al. [2] show how an attacker can exploit the security susceptibilities of the wireless protocol utilized in an implantable cardioverter defibrillator (ICD) to perform a battery-draining attack against the device. This is an attack that aims to deplete the device battery by frequently activating/using the RF module. Moreover, they show that it is feasible to exploit these susceptibilities to change on-device data or the current operation of the device. Gollakota et al. [3] explain how an adversary can eavesdrop on an insecure (i.e., unencrypted) communication channel between an IMD and its associated external device to extract sensitive information about the patient, e.g., the patient's electrocardiogram (ECG) readings.

To prevent battery-draining attacks, an attack-resilient wakeup protocol, which activates the RF module before every authorized communication, must be used. Today's IMDs often employ a magnetic switch, which turns on their RF module in the presence of an external magnet. Unfortunately, it has been shown that magnetic switches cannot prevent battery-draining attacks since they can be easily activated by an attacker (without the presence of a nearby magnet) if a magnetic field of sufficient strength is applied [2], [8].

In order to secure the RF wireless channel between the IMD and the external device and avert the risk of eavesdropping on the channel, the use of cryptographic techniques, e.g., data encryption, has been suggested [9], [10]. However, traditional cryptographic techniques are not suitable for IMDs due to limited on-device resources, e.g., limited storage and battery energy. For example, asymmetric encryption mechanisms are not applicable to resource-constrained IMDs since they would significantly decrease the IMD battery lifetime [9], [11]. Several lightweight symmetric encryption mechanisms have been proposed in the last decade to ensure the security of communication protocols utilized in IMDs (see [12] for a survey). While symmetric cryptography may offer a secure lightweight solution, it is

Acknowledgments: This work was supported by NSF under Grant no. CNS-1219570 and CNS-1617628.
Arsalan Mosenia is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (e-mail: arsalan@princeton.edu).
Niraj K. Jha is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (e-mail: jha@princeton.edu).

greatly dependent on a secure key exchange protocol. Such a protocol enables sharing of the encryption key between the IMD and the external device. As extensively described later in Section 2.2, previously-proposed key exchange protocols have various shortcomings since *they either add significant overheads to the IMD or are susceptible to remote eavesdropping.*

In this paper, we present practical **key exchange and wakeup protocols for subcutaneous IMDs**, which complement lightweight symmetric encryption mechanisms, to thwart common security attacks against insecure communication channels. We introduce a secure optical communication channel, which we call OpSecure. We discuss the design and implementation of a low-power wakeup protocol and a secure key exchange protocol based on OpSecure. Our main contributions can be summarized as follows:

1) We introduce OpSecure, an optical secure unidirectional (from the external device to the IMD) communication channel.
2) We present an attack-resilient low-power wakeup protocol for IMDs based on OpSecure.
3) We propose a secure key exchange protocol, which enables sharing of the encryption key between IMDs and their associated external devices.
4) We discuss the design and implementation of a prototype IMD platform that supports the proposed protocols and present evaluation results for the prototype.

The remainder of this article is organized as follows. In Section 2, we explain why wakeup and key exchange protocols are essential for IMDs and briefly discuss the shortcomings of previously-proposed protocols. We present OpSecure and summarize its advantages in Section 3. We also propose a wakeup protocol and a key exchange protocol based on OpSecure. In Section 4, we describe our prototype and experimental setup. We evaluate the prototype implementation that supports both the proposed protocols (wakeup and key exchange) in Section 5. We discuss limitations of the proposed work in Section 6. Finally, we conclude in Section 7.

2 Problem Definition

In this section, we first explain the role of wakeup and key exchange protocols in providing secure communication for IMDs. Then, we present a brief overview of prior related work on these protocols and summarize their shortcomings.

2.1 Wakeup and key exchange protocols

As mentioned earlier, the IMD and its associated external device commonly have an RF channel that is used for bidirectional data communication. We assume that both devices are capable of using symmetric encryption for protecting the data sent over the RF channel. The overall system architecture that we target is illustrated in Fig. 1.

Due to severe on-sensor energy constraints, the RF module must be enabled only when absolutely needed, e.g., when an authorized physician wants to access on-device data. Thus, prior to each data transmission, the RF module should be activated using a pre-defined wakeup protocol. This protocol must satisfy two main design requirements.

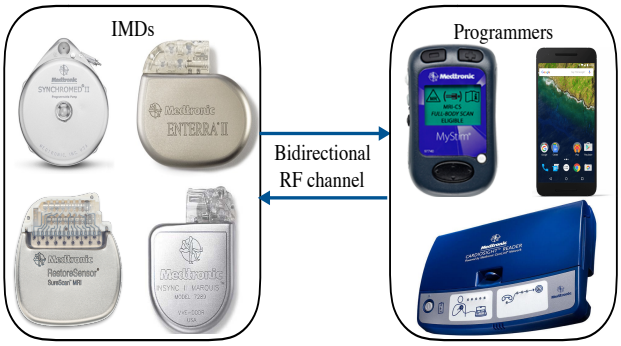

Fig. 1. Overall system architecture: IMD and external device have a bidirectional RF channel that supports symmetric encryption, e.g., Bluetooth Low Energy.

First, it must be resilient against battery-draining attacks so that an attacker cannot activate the RF module. Second, it should add negligible size and energy overheads to the device.

After enabling the RF module by the wakeup protocol, data can be transmitted over the bidirectional communication channel that supports symmetric encryption. Since symmetric encryption is based on an encryption key, an exchange protocol must be used to securely exchange the encryption key between the IMD and the external device. Every practical key exchange protocol must satisfy the following design requirements. First, it must guarantee the confidentiality of the encryption key and be resilient to remote eavesdropping. Second, its size and energy overheads must be minimal. Third, it must ensure that healthcare professionals can access and control the IMD without a notable delay in an emergency situation in which the patient needs immediate medical assistance.

2.2 Related work

Next, we summarize previous research efforts on both wakeup and key exchange protocols and highlight their shortcomings.

2.2.1 *Wakeup protocols*

As mentioned earlier, a magnetic switch is commonly integrated into today's IMDs to turn on the RF module when needed. However, magnetic switches are vulnerable to battery-draining attacks since they can be remotely activated [2]. A few wakeup protocols have recently been presented in the academic literature. For example, the wakeup protocol presented by Halperin et al. [2] relies on an authentication technique in which the IMD harvests the RF energy supplied by the external device itself. The RF module is powered by the battery only after the external device is authenticated. However, the RF energy harvesting subsystem needs an antenna, which imposes a significant size overhead on the IMD. Kim et al. [5] suggest a wakeup scheme in which the IMD activates the RF module when it detects the vibration generated by an external electrical motor. Their scheme adds minimal size and energy overheads to the IMD since it only needs the addition of a low-power accelerometer to the IMD. However, in practice, the patient's regular activities,

e.g., running, may unintentionally and frequently turn on the RF module and, as a result, deplete the device battery.

2.2.2 Key exchange protocols

The use of a pre-defined password, which is stored on the device and known to the user, is a longstanding tradition in the security community. However, a key exchange approach that needs active user involvement, e.g., asking the user to remember a password and give it to authorized physicians upon request, is not suitable for IMDs since the user may not be able to cooperate with healthcare professionals in an emergency, e.g., when the patient is unconscious. In order to minimize user involvement, previous research studies have proposed several user-independent key exchange protocols. Next, we summarize them and discuss their shortcomings.

Ultraviolet tattoos: Schechter [13] presented a scheme in which a fixed user-selected human-readable key is tattooed directly on the patient's body using ultraviolet ink. In this protocol, all devices that need to communicate with the IMD must be equipped with a small, reliable, and inexpensive ultraviolet light-emitting diode (LED) and an input mechanism for key entry. This tattoo-based approach has two limitations. First, the design requires the patient to agree to acquire a tattoo, which significantly limits its applicability [14]. Second, if the password becomes compromised, access by the attacker cannot be prevented easily since the password cannot be changed in a user-convenient manner.

Radio-frequency identification (RFID) and near-field communication (NFC) tags: The use of RFID and NFC tags, which can hold a small data packet (for example, a fixed encryption key) that can be read later by an external reader, have been suggested in previous research studies [15], [16]. They rely on magnetic coupling that offers a short communication range (typically, less than 20cm), minimizing the feasibility of remote eavesdropping. However, it has been mentioned that RFID and NFC are not suitable for IMDs for two reasons. First, NFC/RFID devices create electromagnetic fields that can result in electromagnetic interference with IMDs (in particular, with pacemakers, cardioverter/defibrillators, and neurostimulators). This can lead to several serious consequences, including missing of pacing pulses and generation of asynchronous pulses for pacemakers, inappropriate tachyarrhythmia and delivery of therapy for cardioverter/defibrillators, and inappropriate inhibition of neurostimulators [17]. Second, similar to the tattoo-based approach, if the password becomes compromised, it cannot be changed during the lifetime of the IMD.

Physiological signal-based key generation: A few physiological signal-based key generation protocols have been proposed [18]–[20], which can be used to generate a shared key for the IMD and the external device from synchronized readings of physiological, such as ECG, signals. Unfortunately, the robustness and security properties of keys generated using such techniques have not been well-established [5].

Using acoustic side channel: Halperin et al. presented a key exchange protocol based on acoustic side channels in [2]. Unfortunately, their protocol is susceptible to remote acoustic eavesdropping attacks [21] and, as a result, does not offer a secure key exchange protocol. Moreover, it is not reliable in noisy environments since they utilized a carrier frequency within the audible range. Furthermore, it imposes a significant size overhead [5].

Using vibration side channel: Kim et al. [5] proposed a key exchange protocol that relies on a vibration side channel, i.e., a channel in which the transmitter is a vibration motor, and the receiver is an accelerometer embedded in the IMD. This protocol requires negligible size and energy overheads. However, it has two shortcomings. First, since electrical motors generate capturable electromagnetic and acoustic waves during their normal operation [4], an adversary might be able to extract the key from signals leaked from the vibration motor. Second, since the method uses an accelerometer to detect vibrations, regular physical activities, e.g., running, may be interpreted as key transmission. This can reduce the battery lifetime of the IMD since the device needs to listen to the communication channel even when there is no actual transmission.

In this paper, we aim to address the above-mentioned shortcomings of previously-proposed protocols, *in particular size/energy overheads and vulnerability to eavesdropping*, through a simple low-power, yet secure, key exchange protocol using *visible light*.

3 The Proposed Channel and Protocols

In this section, we first describe OpSecure and highlight its advantages. Then, we discuss the two proposed protocols that are based on OpSecure.

3.1 OpSecure: The proposed channel

Optical data transmission (also called light-based wireless communication) is a well-known communication type that has attracted increasing attention in recent years due to its potential to offer high-speed wireless communication (as a complement or an alternative to WiFi) for a variety of portable devices, e.g., smartphones and laptops. Previous research studies [22], [23] demonstrate that optical communication channels can enable high-rate data transmission (the transmission rate can vary from several hundred Mb/s to a few Gb/s). In an optical channel, data packets flow from a light source (transmitter) to a light sensor (receiver). Therefore, to establish a bidirectional communication channel between two devices, both devices must have a light source and a light sensor.

There is a basic domain-specific challenge that must be addressed when developing an optical communication scheme for IMDs: integration of light sources into IMDs imposes significant size and energy overheads on these resource-constrained devices. Hence, it is not feasible to transmit data from an IMD to an external device via an optical channel even though such a channel can potentially enable two-way communication. Unlike light sources, state-of-the-art already-in-market light sensors are sufficiently compact and energy-efficient to be embedded in IMDs. Therefore, a one-way communication channel, which transmits data from the external device to the IMD, can be implemented with minimal size and energy overheads. We implement such a channel and call it OpSecure.

OpSecure is intrinsically secure due to its close proximity requirement and high user perceptibility. Visible light

Fig. 2. The IMD (pacemaker) has an embedded light sensor, and the smartphone flashlight acts as a light source.

attenuates fast in the body and, hence, can only be captured within a very close range. As demonstrated later in Section 5, if the light source is in contact with the body and directed at the IMD, it can penetrate deep enough into the body to reach the IMD. However, a passive adversary cannot eavesdrop on OpSecure without an eavesdropping device attached to the body, which is very likely to be noticed by the patient.

As illustrated in Fig. 1, the external device may vary from specialized IMD programmers, i.e., external devices that are specifically designed to query the IMD data or send commands to the IMD, to general-purpose portable devices, e.g., smartphones. As in the case of vibration-based key exchange [5], we implement our prototype using a smartphone used as the external device (see Fig. 2). This has three advantages. First, the component that we need in the external device for establishing OpSecure is already present in smartphones (the flashlight can be used as a light source). Second, smartphones have become the dominant form of base stations for a large number of medical devices since they are ubiquitous and powerful, and incorporate various technologies needed for numerous applications [24]. As a result, they can be used as a base station for collecting and processing several types of physiological data (including data collected by IMDs) [1]. Third, smartphones can easily support highly-secure encrypted transmission, which deters several potential attacks against the IMD [25]. However, OpSecure can also be implemented on other devices that are used to communicate with the IMD, at minimal overheads, if they can be equipped with a small light source and an input mechanism for key entry.

3.2 The proposed protocols

Next, we describe both the wakeup and key exchange protocols that we have developed based on OpSecure.

3.2.1 Wakeup protocol

As mentioned earlier, when the light source is in contact with the human body, visible light can penetrate deep enough into the body to reach the IMD. However, it attenuates very fast in the body. We exploit this fundamental characteristic of visible light to develop a wakeup protocol that works as follows. The smartphone fully turns on its flashlight and the IMD wakes up periodically to check if a light source is on the body, i.e., it checks if the intensity of the light received by the IMD is above a predefined threshold T. The presence of an on-body light source that points to the IMD is interpreted as the presence of a trusted external device.

As shown later in Section 5, the proposed wakeup protocol adds minimal size and energy overheads to the device. Unlike a majority of previously-proposed protocols, it also provides immunity against battery-draining attacks. In fact, an attacker, who wants to wake up the RF module, needs to attach a light source to the patient's body at a location close to the IMD. Such an action can be easily detected by the patient.

3.2.2 Key exchange protocol

Assuming the IMD and the external device use a bidirectional RF communication protocol that supports symmetric encryption, our protocol can be used to transmit a randomly-generated key from the smartphone to the IMD. For each key exchange:

Step 1: The smartphone first generates a random key $K \in \{0,1\}^N = k_1 k_2 ... k_N$ of length N, and prepares a key packet as $Key_{packet} = Pre||K||Post$, where Pre and $Post$ are two fixed binary sequences that are concatenated with the key to mark the beginning and end of a key packet.

Step 2: The physician places the smartphone on the patient's body so that its flashlight is directed at the light sensor of the IMD (IMDs commonly have a fixed location and can be easily detected by the physician).

Step 3: The external device uses on-off keying (OOK) modulation to transmit Key_{packet}: the flashlight is turned on (off) for a fixed period of time (T_{step}) to transmit bit "1" ("0"). *Algorithm* 1 shows a simplified pseudo-code for this step. It first computes $T_{step} = \frac{1000}{R} ms$, where R is the transmission rate given by the user. Then, it calls the $keySegmentation$ procedure, which divides Key_{packet} into smaller segments such that each segment only consists of all "1"s or all "0"s. The $keySegmentation$ procedure outputs an array of integer numbers ($segments[]$) so that: (i) the absolute value of each element in the array represents the length (the number of bits) of each of the above-mentioned segments, and (ii) the sign of the element shows whether bits of the segment are all "1"s or all "0"s, i.e., if all bits in the ith segment are "1", $segments[i] > 0$, otherwise, $segments[i] < 0$ (see Fig. 3 for an example). Finally, *Algorithm* 1 turns on/off the flashlight with respect to the absolute values of the elements of $segments[]$ and T_{step}, i.e., $Abs(segment) * T_{step}$ determines how long the flashlight must be kept on/off.

Step 4: The IMD demodulates the received visible light and recovers Key_{packet}. Then, it extracts K from Key_{packet} by removing Pre and $Post$. Thereafter, it encrypts a fixed pre-defined confirmation message $M_{confirm}$ using K and transmits this message $C = ENC(M_{confirm}, K)$ to the smartphone.

Step 5: The smartphone checks if it can successfully decrypt the received message C using K, i.e., if $DEC(C, K) =$

$M_{confirm}$. If the message can be successfully decrypted, the smartphone knows that the IMD received the key K correctly, and then subsequent RF data transmissions are encrypted using key K.

Algorithm 1: flashlightControl procedure

Given: The key packet (Key_{packet}) and transmission rate (R)

1. $T_{step} \leftarrow 1000/R$
2. $segments[] \leftarrow keySegmentation(Key_{packet})$
3. $For\ each\ segment\ in\ segments[]$
4. $\quad If(segment > 0)$
5. $\quad\quad turnTheLightOn(Abs(segment) * T_{step})$
6. $\quad else$
7. $\quad\quad turnTheLightOff(Abs(segment) * T_{step})$
8. $\quad end$
9. end

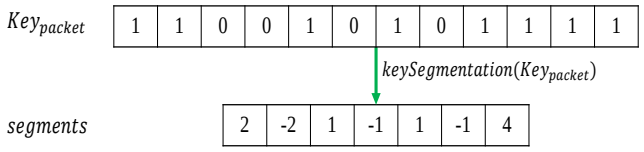

Fig. 3. $keySegmentation$ outputs $segments[]$, given Key_{packet}.

In addition to key exchange, the above-mentioned protocol (the first three steps) can be used to transmit data/commands from the smartphone to the IMD without using the RF module. For example, a predefined stream of bits can be reserved for the shutdown command, i.e., a command that entirely disables the device, and sent using this protocol when needed. Note that the IMD cannot provide any feedback via OpSecure since the channel is unidirectional. However, modern IMDs commonly have an embedded beeping component that warn the patient in different scenarios, e.g., when the RF module is activated [2] or when the device's battery level is low [26]. Such a component can also be used to provide feedback when the IMD receives a predefined message over OpSecure, e.g., the beeping component can generate three beeps when the IMD receives the shutdown command via OpSecure.

4 The Prototype Implementation and Body Model

In this section, we first describe the wireless-enabled IMD that we implemented and the smartphone application that we developed. Second, we discuss how we set the appropriate threshold T for the received light intensity, as mentioned in Section 3.2.1. We then describe the human body model, which we used to evaluate the prototype implementation.

4.1 Prototype implementation

As mentioned earlier, OpSecure establishes a unidirectional communication channel between the IMD and the external device. We implemented a wireless-enabled IMD prototype based on ATmega168V [27] (a low-power microprocessor from Atmel), TEMT6000 [28] (an ambient light sensor from Vishay Semiconductors), and RFD77101 [29] (a Bluetooth Low Energy module from Simblee). The prototype does not offer any health monitoring/therapeutic operations. Indeed, it only implements the two proposed protocols. TEMT6000 enables OpSecure by receiving visible light generated by the user's smartphone, and RFD77101 provides the bidirectional RF communication that can be secured using a symmetric encryption mechanism for which the key can be exchanged over OpSecure. We also developed an Android application that can be used to either wake the IMD up or generate and transmit a random key to the IMD using the smartphone flashlight. The application allows the user to set the key length (N) and transmission rate (R). Fig. 4 illustrates the application and the prototype. It also demonstrates how the application turns the flashlight on/off to transmit the key. For the key exchange example shown in Fig. 4, the key length and transmission rate are set to $4b$ (in practice, the N used would be much higher) and $20b/s$, respectively. Thus, the smartphone needs $T_{step} = \frac{1000}{20} ms = 50ms$ for transmitting a single bit. In this implementation, the application uses two 4-bit sequences ("1100" and "1111") to mark the beginning and end of the key.

We hypothesized that the smartphone's specifications, in particular the maximum light intensity generated by its flashlight and maximum blinking frequency (i.e., how fast the flashlight can be turned on and off), may affect the experimental results. Thus, we evaluated our protocols using three different smartphones: Nexus 5s, Nexus 6, and MotoX.

Fig. 4. The smartphone generates a 4-bit key and transmits the key over OpSecure. The application allows the user to control both the key length (N) and transmission rate (R).

4.2 Appropriate Threshold for Light Intensity

As mentioned earlier in Section 3.2.1, in our prototype implementation, we set a predefined threshold T for the received light intensity ($L_{intensity}$) to wake up the IMD's RF module, i.e., if $L_{intensity} > T$, the IMD's RF module

becomes enabled; otherwise it remains disabled. Furthermore, in our implementation, we use the same threshold T to distinguish "0"s from "1"s, i.e., if $L_{intensity} > T$, the transmitted bit is "1"; otherwise it is "0".

Next, we describe how we set the predefined threshold T. We note that it is essential to minimize the effect of other light sources on the protocol. To ensure security, we would like to ensure that $L_{intensity}$ always remains below T when the light beam comes from unauthorized light sources. As discussed in Section 5.5.2, we assume that, without raising suspicion, unauthorized light sources cannot be placed on the human body close to the IMD. We rely on this assumption to set the threshold: the minimum value of T can be determined by the maximum light intensity received by the IMD, which is implanted in the bacon-beef body model, when a powerful light source is present in the environment. To determine T, we first placed a powerful light source (coherent laser beam with the power of $25mW$) pointed toward the light sensor very close to the IMD ($1cm$ away from the surface of the body model). We then measured the received light intensity and used the measured value as our threshold T.

4.3 The bacon-beef body model

The bacon-beef model for the human body has been previously used in several research studies [2], [3], [5]. It consists of a thin layer of bacon on a thick layer of 85% lean ground beef (Fig. 5). In our experiments, the IMD prototype is placed between the bacon and the ground beef, which reflects the typical placement of ICDs [2]. The smartphone is placed on top of the bacon layer above a transparent plastic sealing.

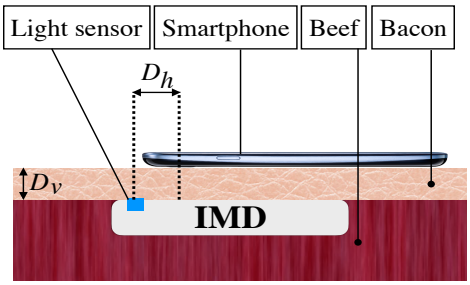

Fig. 5. Experimental setup: The smartphone is placed on top of the bacon layer above a transparent plastic sealing.

5 Evaluation of the Proposed Protocols

In this section, we present evaluation results for the prototype implementation. In particular, we evaluate the transmission range (how far the smartphone can be placed from the IMD and have the visible light still reach it), wakeup/exchange time (the time needed by the wakeup/exchange protocol), protocol overheads (size and energy), and their security.

5.1 Transmission range

We evaluated the prototype using the bacon-beef model for the human body. We varied both the vertical distance and horizontal distance between the IMD and the smartphone (shown as D_v and D_h in Fig. 5, respectively) to evaulate the vertical and horizontal transmission range (maximum D_v and D_h at which the visible light can still reach the IMD). We found that both maximum D_v and D_h are independent of the key length and transmission rate. They mainly depend on the maximum light intensity that the flashlight has to offer.

The flashlight used in the modern smartphones is commonly an LED that emits a white light beam consisting of three fundamental components: red, green, and blue beams. For example, the PLCC6 LED [30], which is a commercialized white LED designed for the camera flash in smartphones, generates a beam with dominant wavelengths of $470nm$ (blue), $530nm$ (green), and $620nm$ (red). We examined the intensity of the white LED embedded in under-experiment smartphones (Nexus 5s, Nexus 6, and MotoX) using Leaton L830 (a handheld lux meter). We noticed that the intensities of light generated by different smartphones are similar (between $70,000lux$ and $80,000lux$).

For all three smartphones, the maximum vertical (horizontal) transmission range was about $2cm$ ($1.5cm$). Thus, if the physician places the smartphone on the patient's body and keeps the smartphone within $1.5cm$ of the IMD's light sensor ($D_h < 1.5cm$), the visible light can easily reach a depth of $1cm$ (the typical D_v for IMDs, such as ICDs [2]). The IMD location is fixed and easily recognizable by inspecting the patient's skin under which the IMD is implanted. Therefore, ensuring $D_h < 1.5cm$ would be straightforward for a physician.

We noticed that when the authorized smartphone's flashlight is accurately aligned with the light sensor, the intensity of the received light is significantly higher than the predefined threshold T. This intensity becomes closer to the threshold as we increase the distance between the sensor and the flashlight and goes below the threshold when the smartphone is placed outside the horizontal transmission range (D_h).

5.2 Transmission quality

We transmitted 100 different keys from each of the three smartphones to the IMD, with each smartphone placed within the horizontal transmission range of OpSecure ($D_h < 1.5cm$), and with the IMD under a $2cm$ layer of bacon ($2cm$ is the vertical transmission range). We found that all keys were transmitted over OpSecure without any error. Therefore, the bit error rate (the number of received bits that have been altered due to noise, interference, distortion, etc.) was zero in all these transmissions. In order to evaluate the effect of ambient noise (e.g., other light sources in the environment, such as sunlight or a car's headlight) on transmission quality, we placed a powerful (3000-lumen) light source at a close distance ($1m$) from the IMD. We noticed that the intensity of the visible light received by the IMD remained almost the same in the presence of the external light source. Indeed, the external light source did not negatively impact the quality of transmission at all.

5.3 Wakeup/exchange time

Next, we evaluated the wakeup time (the time that the wakeup protocol takes to detect the presence of the external

device and turn on the RF module) and the exchange time (how long the key exchange protocol takes to exchange the encryption key).

Wakeup time: As mentioned in Section 3, the wakeup protocol periodically places the light sensor in the full operating mode, in which the sensor samples the light intensity, to check if the smartphone flashlight is present. The wakeup time depends on two parameters: (i) how long the light sensor is in the full operating mode ($T_{operation}$), and (ii) how long the light sensor remains in the standby mode ($T_{standby}$) in which the sensor is disabled. $T_{operation}$ and $T_{standby}$ should be set with regard to the maximum tolerable wakeup time and energy consumption of the wakeup protocol. For example, if we set $T_{standby} = 1.8s$ and $T_{operation} = 0.2s$, the IMD turns on the light sensor for $0.2s$ and then disables it for $1.8s$. In this case, the worst-case wakeup time will be $T_{standby} + T_{operation} = 2s$. As described later in Section 5.4, the worst-case wakeup time can be traded off against energy consumption by varying either $T_{standby}$ or $T_{operation}$.

Exchange time: The exchange time can be readily calculated as $T_{EX} = N/R$, where N and R are the key length and transmission rate, respectively. N depends on the encryption mechanism and is commonly $64b$ or $128b$. The transmission rate generally depends on two parameters: (i) the blinking frequency, and (ii) how fast the light sensor can sample the visible light. In our experiments, the maximum blinking frequency offered by the smartphones was within a 20-30Hz range, and the light sensor was able to sample visible light with a sampling rate of a few hundred Hz (a sampling rate of $60Hz$ is sufficient to recover the key when the blinking frequency is $30Hz$). Therefore, the maximum blinking frequency of the smartphone flashlight limited the transmission rate. In fact, the maximum transmission rate was within the range of $20b/s$ (for MotoX) to $30b/s$ (for Nexus 6). As a result, the minimum time needed for exchanging a packet, that includes a key of length $64b$ ($128b$) and both Pre and $Post$, was within the range of $2.4s$ to $3.6s$ ($4.5s$ to $6.8s$).

Note that different smartphones may offer different maximum transmission rates. However, the IMD does not need to know the transmission rate R beforehand since R can be computed based on the binary sequence Pre, which is known to the IMD. In our prototype implementation, where the first two bits of Pre are always "11" (as mentioned in Section 4, Pre="1100"), R can be computed as follows: $R = \frac{1000}{T_{step}} ms$, where $\frac{1000}{T_{step}} ms$ is half of the duration of the time frame in which the IMD observes the Pre sequence.

5.4 Size and energy overheads

Next, we examine the size and energy overheads that the proposed protocols add to the IMD.

Light sensors commonly consist of a phototransistor in series with a small resistor that converts received light to a voltage. Light sensors typically also have an analog-to-digital converter (ADC) that converts this voltage to a digital number. Thus, a light sensor consists of simple circuitry that can be implemented in a very small area. To save more area on the chip, manufacturers may also use an ADC already incorporated into the IMD and just add a phototransistor/resistor. In both cases, the size overhead is negligible.

The energy overhead is the additional energy consumed by the light sensor, which is added to the IMD to enable transmission over OpSecure. The energy consumption of a light sensor (even one with a built-in ADC) is typically very small, and thus results in negligible energy overhead on the IMD. We investigate the energy overheads for each protocol using a realistic example next.

Consider a typical ICD with a 1.5-Ah battery and 90-month lifetime (it consumes about 23.14 μA current on an average). We can either use a light sensor with a built-in ADC such as MAX44007 [27] or a light sensor without an ADC such as TEMT6000 [28] (used in our prototype). Next, we discuss the energy overheads of wakeup and key exchange protocols for the ICD in both cases.

Wakeup protocol: We configure the IMD so that the light sensor is in the full operating mode for $T_{operation} = 0.2s$ after being in the standby mode for $T_{standby} = 1.8s$. Thus, the light sensor only spends 10% of the time in the full operating mode. MAX44007 drains $0.65\mu A$ ($100pA$) from the battery in the full operating (standby) mode, thus draining 65.09 nA on an average. In this case, the energy overhead of the wakeup protocol is less than 0.3% of the total energy consumption. If we use TEMT6000, the phototransistor in series with the resistor and the built-in ADC, when operating in the full operating mode, drain a few nA [28] and tens of nA [1] from the battery, respectively. Therefore, their energy overheads are negligible in comparison to the total energy consumption of the ICD. Reducing $\frac{T_{operation}}{T_{operation}+T_{standby}}$ makes the energy overhead even smaller.

Key exchange protocol: After waking up the RF module, the physician can use the smartphone to initiate the key exchange procedure in which the IMD configures the light sensor to sense light in the full operating mode for a few seconds. However, key exchange is a very rare event for two reasons. First, a key that is exchanged once can typically be used for a long period of time unless the user suspects that the key is compromised. Second, the communication between the IMD and the external device is very sporadic (e.g., the number of transmissions varies from a few times per day to a few times per year). Thus, even if the external device transmits a new key for each communication session, the timeframe in which the light sensor operates in the full operating mode to exchange the key is negligible in comparison to the device lifetime. Consequently, the key exchange protocol adds almost-zero energy overhead to the IMD.

5.5 Security analysis

In this section, we first discuss our threat model. We then examine the resiliency of OpSecure against various security attacks.

5.5.1 Threat model

An attacker can be any unauthorized person who has a short-term proximity to the subject. He might attempt to (i) target the wakeup protocol to launch a battery-draining attack, (ii) inject his arbitrary encryption key into OpSecure, or (iii) eavesdrop on OpSecure to extract the encryption key. The first two attacks against OpSecure are *active attacks* in which the attacker interferes with the wakeup or key

exchange protocol and sends unauthorized messages to the IMD, whereas the third attack is a *passive attack*, in which the attacker only monitors the ongoing communications.

If the attacker is able to extract the encryption key (either passively or actively), he can steal sensitive medical information from the patient and/or send unauthorized commands to the IMD, causing the device to malfunction. Potential attackers might be criminal groups that want to sell sensitive medical data to the highest bidder [31] or launch life-threatening attacks against a person of interest, political operatives who intend to exploit medical issues of the subject for their political advantage [4], or employers who discriminate against a group of ill employees.

5.5.2 Resiliency against security attacks

Next, we consider both active and passive attacks.

Active attacks: We discuss the feasibility of two active attacks against OpSecure: remote activation of the RF module and key injection.

As mentioned earlier, the horizontal transmission range is about $1.5cm$ and the physician should keep the smartphone within this range to wake up the IMD or transfer the key. Due to this proximity requirement, the attacker cannot place an unauthorized smartphone on the patient's body within the horizontal transmission range without raising suspicion.

Moreover, as mentioned in Section 5.2, the presence of an external powerful light source, which is not attached to the body, does not affect the intensity of the light received by the in-body light sensor. Thus, it cannot be used to launch an active attack against the IMD. To further examine the feasibility of active attacks using external light sources, we replaced the external light source with a laser generating coherent light (with the power of $25mW$). In this scenario, the laser was located $1m$ away from the IMD and pointed toward the light sensor of the IMD. The sensor used in the prototype is sensitive to the ambient light within the wavelength range of 400 to 1100nm. The light sensor has the highest sensitivity around the wavelength of green light [28]. For this reason, we used a green light laser, which generates a coherent light beam with wavelength of 532nm, in our experiment.

We observed that the coherent light is not able to sufficiently penetrate the bacon layer used in our experimental setup (Fig. 5) to reach the IMD and, therefore, it cannot be used by the attacker to activate the wakeup protocol or inject the encryption key.

Can the attacker arbitrarily increase the laser power and eventually succeed? Since we assume that the attacker aims to inject his arbitrary key/data without raising suspicion, we suppose that he uses a laser beam that does not cause skin damage. This limits the maximum power of the laser that can be used for key injection. Considering this limitation, the most powerful laser, that has no skin burn hazard from a $1m$ distance, is a $5mW$ green laser [32]. Our empirical results demonstrate that even a $5\times$ more powerful laser beam cannot reach the IMD.

To sum up, the attacker can neither attach a device to the patient's body without raising suspicion nor remotely (i.e., without physical contact) attack the device.

Passive attack: We examined the possibility of eavesdropping using two different experimental scenarios, as described next.

1. Near-IMD attack: We first placed the smartphone on the chest of a human subject and placed a light sensor close to the smartphone to measure the light intensity on the body surface at varying distances from the smartphone flashlight. As expected, the visible light attenuated very fast and the light sensor was not able to detect the light from the flashlight as the distance between them became greater than $2cm$. Thus, an eavesdropping device to pick up the light and extract the key would need to be placed on the body surface within $2cm$ of the IMD, which is not likely to be feasible since the patient can easily detect such a device.

2. Remote attack: We next investigated the feasibility of launching remote eavesdropping (without an on-body sensor). We noticed that the smartphone flashlight creates a red circular area on the user's chest when it is on. We investigated if an attacker may be able to use a camera to capture a video from the user's chest and process the video to extract the key.

In order to examine the feasibility of such an attack, we asked a subject to hold the smartphone over his chest. Then, we placed a 12-megapixel camera at a distance of $1m$ (a reasonable distance for remote eavesdropping) from the user's chest, and captured two videos in a dark room: one video when the smartphone flashlight was on and one when the flashlight was off. We captured the videos in a dark room to simulate the worst-case scenario since the effect of ambient light sources is minimized and, as a result, the red spot created by the flashlight becomes more visible. We stabilized the camera on a tripod, and, for each frame, cropped a small area around the camera's flashlight (a $3cm \times 3cm$ area).

We created two sets of frames, each including 100 frames ($S_{baseline}$ and S_{on}) extracted from the first video in which the flashlight was on. We then extracted 100 frames from the second video in which the flashlight was off (S_{off}). After creating the three above-mentioned sets of frames, we first computed the RGB Euclidean distance [1] between the frames of $S_{baseline}$ and frames of S_{on} (the frames that were captured when the flashlight was on). We then computed the RGB Euclidean distance between the frames of $S_{baseline}$ and the frames of S_{off} (the frames that were captured when the flashlight was off). The RGB Euclidean distance is a metric that represents the color difference between two frames. The computed values of the RGB Euclidean distance in these two cases were similar, indicating that the frames of S_{on} were not distinguishable from the frames of S_{off}. In other words, the attacker cannot detect the red spot created by the smartphone flashlight when the smartphone is placed on the user's chest.

Furthermore, for a more comprehensive analysis, we performed similar experiments with a thermal camera (FLIR One [33]) and observed similar results. We believe that the thermal camera was not able to pick up the thermal signature of the flashlight since the activities of the other

1. The RGB Euclidean distance between two frames is computed as follows: $D = \sum_{n=1}^{\#pixels} \sqrt{(R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2}$ where R, G, and B denote red, green, and blue components of a pixel, respectively and $\#pixels$ is the number of pixels in the frame

smartphone components (in particular, its display) conceal the activity of the flashlight.

Both experiments indicate that the attacker cannot distinguish bit "1"s from "0"s when the key exchange protocol is sending the key.

6 Discussion

In this section, we briefly discuss four items not yet explained in detail. First, we discuss limitations of the proposed mechanism for deeply-implanted IMDs. Second, we describe shortcomings of the bacon-beef body model. We then discuss how embedding a light sensor in an IMD may also enable wireless charging in addition to providing a communication channel. Finally, we discuss why we chose OOK modulation in our implementation.

6.1 Limited vertical transmission range

As mentioned earlier, the idea of using visible light to wake up the IMD or transfer encryption keys is motivated by the observation that visible light penetrates deep enough through the human body to reach an IMD if a powerful light source is placed on the body. OpSecure enables a secure communication channel for subcutaneous implants. However, it may not be suitable for deeper implants for two reasons. First, as demonstrated in Section 5.1, OpSecure offers a vertical transmission range (shown as D_v in Fig. 5) of $2cm$ that may not be sufficient for all IMDs. Second, it may be difficult for physicians to locate deep IMDs with non-invasive procedures. To sum up, the rapid attenuation of visible light within the human body ensures the security of the proposed communication channel, however, it may also limit the applicability of the channel to deeply-implanted IMDs.

6.2 Imperfection of the bacon-beef body model

The bacon-beef body model has been widely used for testing IMDs by researchers due to the difficulties associated with more realistic experiments, e.g., laws that permit and control the use of animals for scientific experimentation [34]. We acknowledge the fact that the physical characteristics of this model (for example, how much it absorbs, reflects, refracts, and scatters the visible light) may differ from those of the human body. We have reviewed several related publications that used the bacon-beef model and realized that the validity of this model has not been experimentally confirmed for electromagnetic waves (even for lower radio frequencies). A comprehensive analysis of physical characteristics of this model is beyond the scope of this paper; however, we have performed a simple experiment to demonstrate that the attenuation of visible light in this model is similar to that of the human body. We first asked a subject to place his fingertip on a smartphone's flashlight, and measured the intensity of light that penetrated through the fingertip and was received on the other side. Second, we slightly modified our bacon-beef body model so that the height of the bacon layer (D_v) becomes almost the same as the height of the subject's fingertip. We placed the same smartphone's flashlight on the bacon layer and measured the intensity of the light that penetrated through the model and was captured by the sensor in the IMD. We found that the intensity of the received light in the first scenario was slightly higher than the intensity of light measured in the second scenario (5% higher), indicating that visible light can penetrate slightly deeper into the human body.

6.3 Light-based energy harvesting

Several wireless energy harvesting approaches for IMDs have been discussed in the literature. These approaches aim to increase the lifetime of IMDs, preventing the risks associated with their replacement. Among them, light-based energy harvesting techniques, where a light sensor harvests the energy provided by an external light source, have shown promising results [35]–[37]. However, there are two challenges that limit the applicability of light-based techniques. First, considering the attenuation of light in the body, the surface of the energy-harvesting cells should be large (for example, a $20mm \times 28mm$ array of sensors is proposed in [36]). Second, the power of the external light source must be limited to avoid skin overheating. Despite these challenges, the integration of a light sensor into an IMD can potentially increase its battery lifetime (Ref. [37] demonstrates how the battery lifetime of an implantable pacemaker can be increased significantly), and, at the same time, enable a secure communication channel, as discussed in this paper.

6.4 The rationale behind choosing OOK modulation

In general, any type of digital modulation scheme can be used to transmit data (for example, commands and encryption keys) over the proposed optical communication channel. However, in already-in-market smartphones, the frequency and phase of the light generated by the smartphone's flashlight cannot be controlled through the application programming interfaces provided for application development. Therefore, frequency-/phase-based modulation techniques (for example, frequency-shift keying and phase-shift keying) cannot be reliably implemented using smartphone flashlights. Thus, our options are limited to amplitude-shift keying techniques in which data are represented as variations in the amplitude of a carrier signal (the intensity of visible light signal in OpSecure). Furthermore, we noticed that the intensity of light generated by the flashlight is not adjustable in many smartphone models. However, in almost all modern smartphones, an application can turn on/off the flashlight. Therefore, we used the simplest form of amplitude-shift keying modulation, called OOK, which can be implemented by turning the flashlight on/off. In addition to compatibility with almost all in-market smartphones, the simplicity of the algorithm imposes minimal design/computation overheads on the IMD.

7 Conclusion

We described why attack-resilient wakeup and secure key exchange protocols are essential for establishing a secure RF-based communication link between the IMD and the external device. We discussed the shortcomings of previously-proposed protocols. We presented OpSecure, an optical secure communication channel between an IMD and an external device, e.g., smartphone, that enables an intrinsically

short-range, user-perceptible one-way data transmission (from the external device to the IMD). Based on OpSecure, we proposed a wakeup and a key exchange protocol. In order to evaluate the proposed protocols, we implemented an IMD prototype and developed an Android application that can be used to wake up the IMD and transmit the encryption key from the smartphone to the IMD. We evaluated our prototype implementation using a human body model. The experimental results demonstrated that OpSecure can provide a secure approach for implementing both wakeup and key exchange protocols for IMDs, with minimal size and energy overheads.

REFERENCES

[1] A. M. Nia, M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Energy-efficient long-term continuous personal health monitoring," *IEEE Trans. Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 85–98, 2015.

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

[3] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 2–13, 2011.

[4] A. M. Nia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Physiological information leakage: A new frontier in health information security," *IEEE Trans. Emerging Topics in Computing*, vol. 4, no. 3, pp. 321–334, 2016.

[5] Y. Kim, W. S. Lee, V. Raghunathan, N. K. Jha, and A. Raghunathan, "Vibration-based secure side channel for medical devices," in *Proc. IEEE Design Automation Conference*, 2015, pp. 1–6.

[6] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE Int. Conf. e-Health Networking Applications and Services*, 2011, pp. 150–156.

[7] M. Zhang, A. Raghunathan, and N. K. Jha, "Medmon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomedical Circuits and Systems*, vol. 7, no. 6, pp. 871–881, 2013.

[8] S. Lee, K. Fu, T. Kohno, B. Ransford, and W. H. Maisel, "Clinically significant magnetic interference of implanted cardiac devices by portable headphones," *Heart Rhythm*, vol. 6, no. 10, pp. 1432–1436, 2009.

[9] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in *Proc. ACM Wkshp. Hot Topics on Wireless Network Security and Privacy*, 2013, pp. 31–36.

[10] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, 2014.

[11] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Trans. Mobile Computing*, vol. 5, no. 2, pp. 128–143, Feb. 2006.

[12] C. Strydis, D. Zhu, and G. N. Gaydadjiev, "Profiling of symmetric-encryption algorithms for a novel biomedical-implant architecture," in *Proc. ACM Conf. Computing Frontiers*, 2008, pp. 231–240.

[13] S. Schechter, "Security that is meant to be skin deep," Microsoft Research, Tech. Rep., Apr. 2010.

[14] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel, "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices," in *Proc. ACM SIGCHI Conf. Human Factors in Computing Systems*, 2010, pp. 917–926.

[15] R. A. Stevenson, "RFID detection and identification system for implantable medical devices," Mar. 29 2011, US Patent 7,916,013.

[16] E. Freudenthal, D. Herrera, F. Kautz, C. Natividad, A. Ogrey, J. Sipla, A. Sosa, C. Betancourt, and L. Estevez, "Suitability of NFC for medical device communication and power delivery," in *Proc. IEEE Engineering in Medicine and Biology Wkshp.*, 2007, pp. 51–54.

[17] E. Mattei, E. Lucano, F. Censi, M. Triventi, and G. Calcagnini, "Provocative testing for the assessment of the electromagnetic interference of RFID and NFC readers on implantable pacemaker," *IEEE Trans. Electromagnetic Compatibility*, vol. 58, no. 1, pp. 314–322, 2016.

[18] K. K. Venkatasubramanian, A. Banerjee, and S. K. Gupta, "EKG-based key agreement in body sensor networks," in *Proc. IEEE Int. Conf. Computer Communications*, 2008, pp. 1–6.

[19] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE Int. Conf. Computer Communications*, 2011, pp. 1862–1870.

[20] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Computer & Communications Security*, 2013, pp. 1099–1112.

[21] T. Halevi and N. Saxena, "Acoustic eavesdropping attacks on constrained wireless device pairing," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 3, pp. 563–577, 2013.

[22] J. Vučić, C. Kottke, S. Nerreter, K.-D. Langer, and J. W. Walewski, "513 Mbit/s visible light communications link based on DMT-modulation of a white LED," *J. Lightwave Technology*, vol. 28, no. 24, pp. 3512–3518, 2010.

[23] F.-M. Wu, C.-T. Lin, C.-C. Wei, C.-W. Chen, H.-T. Huang, and C.-H. Ho, "1.1-Gb/s white-LED-based visible light communication employing carrier-less amplitude and phase modulation," *IEEE Photonics Technology Letters*, vol. 24, no. 19, pp. 1730–1732, 2012.

[24] K. Patrick, W. G. Griswold, F. Raab, and S. S. Intille, "Health and the mobile phone," *American J. Preventive Medicine*, vol. 35, no. 2, p. 177, 2008.

[25] A. Mosenia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "CABA: Continuous authentication based on BioAura," *accepted for publication in IEEE Trans. Computers*, 2016.

[26] "Is your defibrillator beeping?" https://keepyourhearthealthy.wordpress.com/2011/01/02/is-your-defibrillator-beeping/, accessed: 10-9-2016.

[27] "ATmega168," http://www.atmel.com/devices/atmega168.aspx, accessed: 10-9-2016.

[28] "Light sensor," https://www.sparkfun.com/datasheets/Sensors/, accessed: 10-9-2016.

[29] "Simblee," https://www.simblee.com/index.html, accessed: 10-9-2016.

[30] "PLCC6 LED," http://www.farnell.com/datasheets/9258.pdf, accessed: 2017-10-10.

[31] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, vol. 7, no. 1, 2008.

[32] "How divergence affects hazard distances," http://www.lasersafetyfacts.com/resources/Laser-hazard-distance-chart.pdf, accessed: 2017-10-10.

[33] "FLIR ONE," http://www.flir.com/flirone/, accessed: 2017-10-10.

[34] S. S. Clark and K. Fu, "Recent results in computer security for medical devices," in *Proc. Int. Conf. Wireless Mobile Communication and Healthcare*, 2011, pp. 111–118.

[35] K. Murakawa, M. Kobayashi, O. Nakamura, and S. Kawata, "A wireless near-infrared energy system for medical implants," *IEEE Engineering in Medicine and Biology Magazine*, vol. 18, no. 6, pp. 70–72, 1999.

[36] K. Goto, T. Nakagawa, O. Nakamura, and S. Kawata, "An implantable power supply with an optically rechargeable lithium battery," *IEEE Trans. Biomedical Engineering*, vol. 48, no. 7, pp. 830–833, 2001.

[37] C. Algora and R. Peña, "Recharging the battery of implantable biomedical devices by light," *Artificial Organs*, vol. 33, no. 10, pp. 855–860, 2009.

Arsalan Mosenia received his B.S. degree in Computer Engineering from Sharif University of Technology, Tehran, Iran, in 2012, and M.A. degree in Electrical Engineering from Princeton, NJ, in 2014. He is currently pursuing a Ph.D. degree in Electrical Engineering at Princeton University, NJ. His research interests include wireless sensor networks, Internet of things, computer security, distributed computing, mobile computing, and machine learning.

Niraj K. Jha (S'85-M'85-SM'93-F'98) received his B.Tech. degree in Electronics and Electrical Communication Engineering from Indian Institute of Technology, Kharagpur, India in 1981, M.S. degree in Electrical Engineering from S.U.N.Y. at Stony Brook, NY in 1982, and Ph.D. degree in Electrical Engineering from University of Illinois at Urbana-Champaign, IL in 1985. He is a Professor of Electrical Engineering at Princeton University.

He has served as the Editor-in-Chief of IEEE Transactions on VLSI Systems and an Associate Editor of IEEE Transactions on Circuits and Systems I and II, IEEE Transactions on VLSI Systems, IEEE Transactions on Computer-Aided Design, IEEE Transactions on Computers, Journal of Electronic Testing: Theory and Applications, and Journal of Nanotechnology. He is currently serving as an Associate Editor of IEEE Transactions on Multi-Scale Computing Systems and Journal of Low Power Electronics. He has served as the Program Chairman of the 1992 Workshop on Fault-Tolerant Parallel and Distributed Systems, the 2004 International Conference on Embedded and Ubiquitous Computing, and the 2010 International Conference on VLSI Design. He has served as the Director of the Center for Embedded System-on-a-chip Design funded by New Jersey Commission on Science and Technology and the Associate Director of the Andlinger Center for Energy and the Environment.

He is the recipient of the AT&T Foundation Award and NEC Preceptorship Award for research excellence, NCR Award for teaching excellence, Princeton University Graduate Mentoring Award, and six Commendations for Outstanding Teaching by the School of Engineering and Applied Sciences. He is a Fellow of IEEE and ACM. He received the Distinguished Alumnus Award from I.I.T., Kharagpur in 2014.

He has co-authored or co-edited five books titled Testing and Reliable Design of CMOS Circuits (Kluwer, 1990), High-Level Power Analysis and Optimization (Kluwer, 1998), Testing of Digital Systems (Cambridge University Press, 2003), Switching and Finite Automata Theory, 3rd edition (Cambridge University Press, 2009), and Nanoelectronic Circuit Design (Springer, 2010). He has also authored 15 book chapters. He has authored or co-authored more than 430 technical papers. He has coauthored 14 papers, which have won various awards. These include the Best Paper Award at ICCD'93, FTCS'97, ICVLSID'98, DAC'99, PDCS'02, ICVLSID'03, CODES'06, ICCD'09, and CLOUD'10. A paper of his was selected for "The Best of ICCAD: A collection of the best IEEE International Conference on Computer-Aided Design papers of the past 20 years," two papers by IEEE Micro Magazine as one of the top picks from the 2005 and 2007 Computer Architecture conferences, and two others as being among the most influential papers of the last 10 years at IEEE Design Automation and Test in Europe Conference. He has co-authored another six papers that have been nominated for best paper awards. He has received 17 U.S. patents. He has given several keynote speeches on nanoelectronic design/test and smart healthcare.