# Vibration-based Secure Side Channel for Medical Devices

Younghyun Kim[1], Woo Suk Lee[1], Vijay Raghunathan[1], Niraj K. Jha[2], and Anand Raghunathan[1]
[1]School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907
[2]Department of Electrical Engineering, Princeton University, Princeton, NJ 08544
[1]{yhkim1, lee992, vr, raghunathan}@purdue.edu, [2]jha@princeton.edu

## ABSTRACT

Implantable and wearable medical devices are used for monitoring, diagnosis, and treatment of an ever-increasing range of medical conditions, leading to an improved quality of life for patients. The addition of wireless connectivity to medical devices has enabled post-deployment tuning of therapy and access to device data virtually anytime and anywhere but, at the same time, has led to the emergence of security attacks as a critical concern. While cryptography and secure communication protocols may be used to address most known attacks, the lack of a viable secure connection establishment and key exchange mechanism is a fundamental challenge that needs to be addressed. We propose a vibration-based secure side channel between an external device (medical programmer or smartphone) and a medical device. Vibration is an intrinsically short-range, user-perceptible channel that is suitable for realizing physically secure communication at low energy and size/weight overheads. We identify and address key challenges associated with the vibration channel, and propose a vibration-based wakeup and key exchange scheme, named *SecureVibe*, that is resistant to battery drain attacks. We analyze the risk of acoustic eavesdropping attacks and propose an acoustic masking countermeasure. We demonstrate and evaluate vibration-based wakeup and key exchange between a smartphone and a prototype medical device in the context of a realistic human body model.

## 1. INTRODUCTION

Advances in the design of implantable and wearable medical devices (IWMDs) have enabled fundamentally new options for monitoring, diagnosing, and treating a wide range of medical conditions. IWMDs have become increasingly sophisticated over the years and are now commonly equipped with wireless connectivity. In addition to enabling continuous ambulatory monitoring, wireless connectivity in IWMDs also allows healthcare professionals to non-intrusively monitor a patient's health and device status.

Although wireless connectivity in IWMDs enables convenient and timely access to medical data, it can also be a security loophole that allows adversaries to obtain sensitive medical data from IWMDs or even take control of them [1, 2, 3]. Recent research has exposed several security vulnerabilities in wireless-enabled IWMDs [2, 3]. Typically, the radio frequency (RF) channel between two wireless devices is secured through the use of cryptographic techniques. However, traditional cryptographic techniques are not directly applicable to IWMDs due to their unique usage model. Specifically, IWMDs should be protected from unauthorized access and, at the same time, healthcare professionals' access to them should not be hindered or delayed in an emergency when the patient requires immediate medical assistance. Traditional security mechanisms do not address this tension between resistance to adversaries and the need for easy access in an emergency situation.

Specifically, securing the wireless channel between IWMDs and external devices (EDs) involves three main challenges. First, only legitimate EDs should be able to activate the RF module in the IWMD and establish a wireless connection to it. If the IWMD's RF module can be activated by any ED, adversaries can make repeated (possibly invalid) connection requests in order to deplete the batteries in the IWMD, which is referred to as a battery drain attack. Second, for resource-constrained IWMDs, asymmetric cryptography is not suitable since it is significantly more expensive (in terms of computation and memory) than symmetric cryptography [4]. Further, establishing a public-key infrastructure (PKI) for certification of all EDs that an IWMD may interact with is an open and difficult challenge. While symmetric cryptography is a lightweight solution, it requires the secure exchange of a shared secret key between the two devices. Third, even if symmetric cryptography is used, the encryption and decryption algorithms need to be implemented efficiently. While the third challenge has been alleviated by the inclusion of efficient cryptographic hardware accelerators in modern microcontroller platforms, the first and second challenges are yet to be satisfactorily addressed.

In this paper, we propose a *vibration-based secure side channel*[1] to address the aforementioned security challenges. A vibration-based communication channel has the fundamental properties that it is intrinsically short-range, requires direct physical contact, and is highly user-perceptible (*i.e.,* any attempts to communicate over this channel can be easily perceived by the patient). We exploit these advantages and propose a wakeup and key exchange scheme, named *SecureVibe*. Our contributions in this paper can be summarized as follows:

- We propose a vibration-based, ultra-low power wakeup mechanism for IWMDs that is resistant to battery drain attacks. Vibration can be detected by an IWMD only when it is produced at a location close to the IWMD through a direct contact to the body. This property significantly increases the patient's awareness of attempted access to the IWMD and enables the patient to take an evasive action, if necessary.
- We present a new physical-layer signaling technique for the proposed vibration channel. The technique is based on an enhanced on-off keying (OOK) demodulation scheme that uses a combination of amplitude gradients and mean values to achieve communication bit rates of up to 20 bits per second (bps), which is 4× higher than what conventional OOK demodulation can achieve in our scenario.
- We propose a vibration-based, lightweight key exchange protocol that enables an IWMD and ED to securely and reliably exchange a shared cryptographic key for use in cryptographically protecting their RF communication. We perform a security analysis of the proposed protocol and present an acoustic masking countermeasure for thwarting acoustic eavesdropping attacks.
- We have designed a prototype wireless-enabled IWMD platform to evaluate SecureVibe. We have conducted ex vivo experiments using our prototype IWMD and a smartphone as the ED. Experimental results demonstrate that the proposed vibration-based side channel enables cryptographic key exchange between an IWMD and an ED in a reliable and secure manner with minimal energy overheads.

This work was supported by the National Science Foundation (NSF) under grants CNS-1219570, CNS-0953468, and CCF-1018358.


*DAC '15,* June 7–11, 2015, San Francisco, CA, USA

http://dx.doi.org/10.1145/2744769.2744928

[1]By *side channel*, we mean an additional *intentional* communication channel and not an unintentional source of information leakage as in side channel attacks [5].

## 2. RELATED WORK

In this section, we present a brief overview of prior related work on the use of vibration for security, wakeup techniques for IWMDs, and cryptographic key exchange protocols.

### 2.1 Vibration for Security

The idea of vibration-based PIN transmission has been proposed for RFID tag authentication [6]. However, using this technique to exchange long cryptographic keys may not be realistic due to the high bit error rate (2.7%) and the low bit rate (5 bps). For example, to exchange a 128-bit key, it would take about 25 s and the probability of a successful key exchange without any error would be only about 3%. In contrast, our proposed demodulation scheme for vibration channels supports a 4× higher bit rate and our key exchange protocol enables bit errors to be tolerated.

Vibration from body motion (*e.g.,* shaking) that is measured simultaneously by two communicating devices has been used for mutual authentication [7, 8]. Gesture-based authentication [9] also exploits body motion, albeit for user-to-device authentication. These approaches rely on the user's motion and, therefore, may not be suitable for sharing a cryptographic key. Also, they may not be applicable to IWMDs because it is not practical to shake the patient's body, especially in a medical emergency. To overcome these limitations, we utilize motor-generated vibration instead of body motion.

### 2.2 RF Module Wakeup Techniques

In today's IWMDs, a magnetic switch is commonly used to turn on the RF module. Magnetic switches are vulnerable to battery drain attacks since they can be easily activated from a fair distance if a magnetic field of sufficient strength is applied [10]. An ED authentication technique in which the IWMD harvests the RF energy supplied by the ED itself to power the authentication can also protect against battery drain attacks [2]. The RF module is powered by the battery only after the ED is authenticated. However, the RF energy harvesting subsystem, including an antenna, represents a significant size overhead for small IWMDs. In contrast, our proposed wakeup scheme provides resistance against battery drain attacks with minimal size and energy overheads by only using a small, low-power accelerometer.

### 2.3 Cryptographic Key Exchange Techniques

Acoustic side channels have been proposed to exchange cryptographic keys [2]. However, they can be breached by an acoustic eavesdropping attack [11] and involve a significant size overhead for embedding a piezo speaker in the IWMD. Further, their performance in a noisy environment may not be reliable since they use a carrier frequency within the audible range so that it may be user-perceptible. On the other hand, exchanging keys via a body-coupled communication (BCC) channel requires the ED to have physical contact with the patient's body [12]. However, remote eavesdropping on a BCC channel is possible with a sensitive antenna [3]. Another approach is to generate a key from synchronized readings of physiological signals, such as an electrocardiogram (ECG), which can be read only with physical contact [13, 14, 15]. However, the robustness and security properties of keys generated using such techniques have not been well-established. In contrast, our proposed vibration-based side channel is tightly distance bounded and requires direct contact with the specific part of the body where the medical device is implanted. Further, since the choice of the key is not limited (*e.g.,* by a physiological signal), the ED can pick a cryptographically strong key, enhancing the security of the subsequent RF communication.

Shield [16] is an external gateway device to protect legacy IWMDs with no cryptographic methods. It relays messages between the IWMD and the ED while jamming any direct communication between them. Only the communication between the Shield and the ED is encrypted. Hence, the burden of key exchange is carried by the Shield. However, this approach requires the patient to carry an additional device for security. Also, the design of a receiver-cum-jammer is more complex than the design of a conventional transceiver.

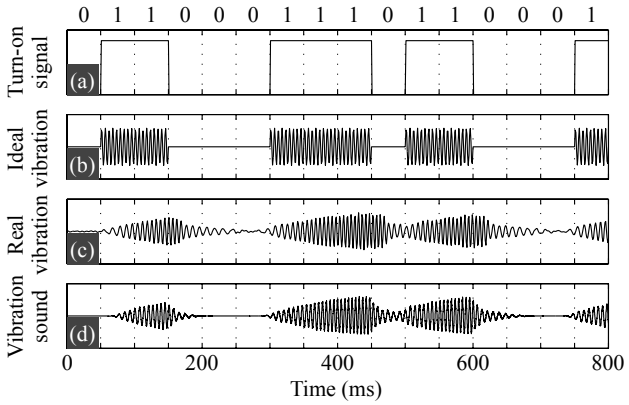


Figure 1: (a) Vibration motor turn-on signal, (b) ideal vibration, (c) real vibration measured from a smartphone, and (d) vibration sound measured at 3-cm distance.

## 3. VIBRATION: A SECURE SIDE CHANNEL

In this section, we discuss the advantages of vibration-based communication and the challenges that need to be addressed in order to implement a reliable and secure side channel based on this communication mechanism.

### 3.1 Advantages of the Vibration Channel

A vibration-based channel is intrinsically secure due to its close proximity requirement and high user perceptibility. Vibration attenuates very fast in the body and, hence, can only be captured within a very close range. For example, if the IWMD is implanted in the chest, a passive adversary (eavesdropper) cannot eavesdrop on the vibration channel without an eavesdropping device attached to the chest, which is very likely to be noticed by the patient. Also, since a vibration motor needs to make a highly perceptible vibration to reach the IWMD, active attacks that inject vibration would be easily noticed by the patient. Therefore, relying on the user's perception and reaction, we assume that the IWMD can trust an ED from which it receives vibration. If required, a more explicit authentication step, *e.g.,* based on a user-supplied PIN, can be added.

Vibration channels can be implemented using simple hardware and minimal overheads. The transmitter in a vibration channel is a vibration source, such as a vibration motor, and the receiver is an accelerometer that detects the vibration. Vibration motors are embedded in almost all modern personal mobile devices such as smartphones and smart watches, which are likely to evolve into personal health hubs. The low power consumption and small footprint of accelerometers play a key role in enabling vibration-based communication channels for IWMDs. State-of-the-art MEMS accelerometers consume very low current (less than a few hundred μA in active mode) and are very small in size (only a few mm along any dimension). Since IWMDs are severely energy-constrained, the low energy overhead and small footprint (leaving more room for the battery) are essential for prolonging their lifetime.

Finally, the vibration channel is inherently a clean channel with very little noise or interference. The frequency of motor vibration is typically higher than 150 Hz, which is a high frequency not typically observed in the ambient environment. Other sources of vibration, *e.g.,* body motion or vehicle vibration, have a much lower frequency. Therefore, a simple high-pass filter is sufficient to eliminate almost all channel noise and the communication is not influenced by ambient vibrations.

### 3.2 Challenges of the Vibration Channel

One of the major challenges of the vibration channel is that the vibration motors found in smartphones exhibit a non-ideal, damped response to excitation. For instance, for the signal in Figure 1(a), where a bit value of 1 turns the motor on and a bit value of 0 turns it off, an

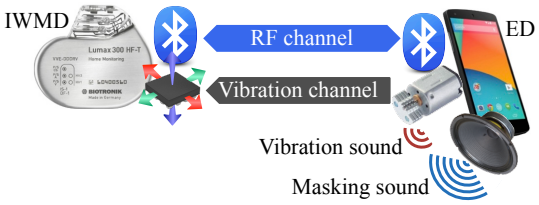


Figure 2: System architecture of SecureVibe.

ideal motor would generate the vibration shown in Figure 1(b). However, the vibration of a real motor is not amplified or attenuated immediately, as shown in Figure 1(c). With such a slow response, a simple OOK scheme that maps bit 0 and bit 1 to zero amplitude and maximum amplitude, respectively, cannot achieve a bit rate of more than a few bps.

Typical implantable medical devices are expected to last 90 months on a battery with 0.5 to 2-Ah capacity [17]. Hence, their average system-level current drain should not exceed 8 to 30 μA. Although a MEMS accelerometer is intrinsically a low-power sensor, the use of an appropriate system-level power management technique, such as duty-cycling, would enable a further decrease in energy consumption. Also, due to the energy and size overheads, it is not practical to embed a vibration motor in the IWMD for a bidirectional vibration channel.

Finally, the vibration motor also leaks an audible acoustic signal, which can be captured using a microphone. As shown in Figure 1(d), the recorded acoustic waveform is highly correlated to the vibration waveform in Figure 1(c). This acoustic signal can potentially lead to an eavesdropping attack and should be effectively blocked while transmitting a cryptographic key. We demonstrate how this acoustic leakage can be masked in Section 4.3.2.

# 4. VIBRATION-BASED WAKEUP AND KEY EXCHANGE SCHEMES

In this section, we present SecureVibe, a secure wakeup and key exchange protocol for IWMDs, which exploits a vibration-based side channel. The overall system architecture that we envision is shown in Figure 2. The IWMD and ED have an RF channel (*e.g.*, Bluetooth Smart) that is used for bi-directional data communication. Both the devices are assumed to be capable of using symmetric encryption and cryptographic hashing for protecting the data sent over the RF channel. The unidirectional vibration channel formed between the vibration generator in the ED and accelerometer in the IWMD is utilized to enable wakeup of the RF channel and key exchange so that the RF channel may be cryptographically protected. Since vibration has an acoustic side-effect, it is necessary to address the possibility of acoustic eavesdropping on the vibration channel. We utilize the speaker in the ED to generate a masking sound as a countermeasure against acoustic eavesdropping. We note that the components that we require in the ED, *viz.*, vibration motor and speaker, are already present in smartphones and most wearable devices. In the following subsections, we first propose a modified OOK scheme that improves the data rate and robustness of the vibration channel, and then describe the proposed schemes for vibration-based secure wakeup and key exchange.

## 4.1 Two-Feature On-Off Keying

As described in Section 3, the slow response of the vibration motor and noise are key challenges associated with the vibration channel. With a simple OOK scheme, the bit rate of the vibration channel is limited to a few bps (2 to 3 bps in our experiments, which translates to an unacceptable ∼85 to 128 s for transmitting a 256-bit AES key). To address these challenges and enable bit rates that are more acceptable for key exchange, we propose an enhanced two-feature OOK scheme. In the proposed scheme, modulation is the same as in the basic OOK; the vibration motor is turned on to transmit a bit 1, and turned off to transmit a bit 0. On the other hand, demodulation of the vibration waveform is based on a combination of two features of the waveform, amplitude gradient and amplitude mean. This is in contrast to the basic OOK scheme that uses only the amplitude mean. We note that the sampling rates of commodity accelerometers are in the range of several hundred samples per second (sps), which enables us to estimate the amplitude gradient. Utilizing the amplitude gradient greatly enhances the distinguishability between bit 0 and bit 1 when the mean has an intermediate value, and thereby enables significantly faster bit-rates (over 20 bps in our experiments).

The first step of demodulation is high-pass filtering to eliminate low-frequency noise that is induced by patient movement or internal organs. We apply a high-pass filter with a cutoff of 150 Hz to the samples from the accelerometer. Next, for feature extraction, we derive the signal envelope and segment it into intervals equal to the bit period. We derive the mean and gradient for each segment, and interpret each bit based on low and high thresholds. Steep negative gradients (lower than the low gradient threshold) and steep positive gradients (greater than the high gradient threshold) are interpreted as a bit 0 and a bit 1, respectively. Similarly, amplitudes below the low and high amplitude thresholds are interpreted as a bit 0 and a bit 1, respectively.

Note that the range between the low and high thresholds represents the classification margin. If at least one of the gradient and mean values lies outside the range between the corresponding low and high thresholds, the bit is labeled as a clear bit. When both the mean and gradient values lie between the corresponding low and high thresholds, the bit is labeled as an ambiguous bit. Ambiguous bits are handled by the key exchange protocol that we introduce later in this section.

## 4.2 Battery Drain Resistant Wakeup

As previously mentioned, the vibration channel is intrinsically limited to very close range, and is furthermore easily perceived by patients. An adversary who attempts to wake up the RF module of an IWMD needs to attach a vibrating device to the patient's body at a location close to the IWMD. Thus, evasive action can be easily taken by the patient. Therefore, the presence of vibration can be interpreted as the presence of an ED that is trusted by the patient. By waking up the RF module in the IWMD only upon detecting a vibration signal generated by an ED, remote battery drain attacks on the RF channel can be prevented.

The most critical challenge for vibration-based wakeup is reducing its energy consumption. Without proper power management, the energy consumed for continuous vibration measurement and signal processing for high-pass filtering may unacceptably reduce the battery life of IWMDs. We devise a power management scheme by leveraging two key observations: (i) given that the time required for transmitting a key is likely to be several seconds, it is acceptable for the wakeup scheme to take a few seconds, and (ii) modern low-power accelerometers have a motion-activated wakeup (MAW) mode that generates an interrupt when a vibration greater than a certain threshold is detected. In this mode, accelerometers consume significantly lower power than in the normal measurement mode.

To take advantage of this low-power mode, we devise a two-step wakeup scheme, as illustrated in Figure 3. First, the IWMD periodically wakes up the accelerometer and puts it into the MAW mode for a short time to check if the vibration exceeds a specified threshold. The wakeup threshold is set to be able to detect the vibration generated by an ED, but not to be activated by modest body motions. If no vibration is detected, the accelerometer is returned to the standby mode. When vibration is detected, the accelerometer is placed in the normal measurement mode, where it measures the vibration at the full sampling rate. Next, we extract the high-frequency components from the measured vibration. In this step, we use a simple moving average filter for high-pass filtering. Finally, the RF module is turned on for communication if a high-frequency vibration is observed after the filtering. This two-step wakeup scheme significantly reduces the energy consumed for monitoring of the vibration channel. Our results in Section 5.2 demonstrate that it imposes less than 0.3% energy overhead for an energy budget of 1.5 Ah over 90 months.

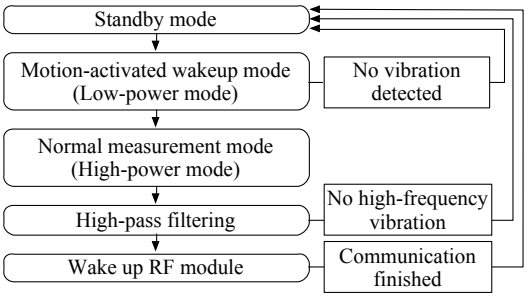


Figure 3: Two-step RF module wakeup.

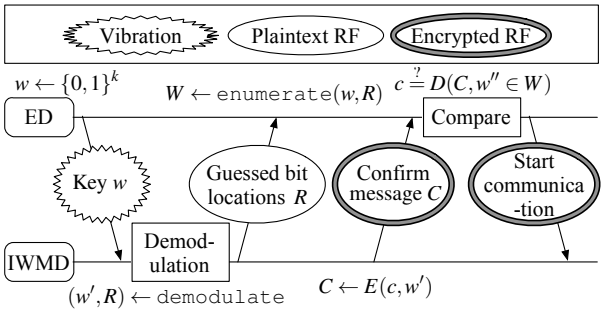


Figure 4: Key exchange protocol.

## 4.3 Cryptographic Key Exchange

After successful wakeup of the RF module in the IWMD, a shared key needs to be exchanged between the IWMD and ED for the symmetric encryption of subsequent wireless communication. In this subsection, we propose a key exchange protocol to make the IWMD and ED agree upon an identical key in the presence of errors introduced by the vibration channel.

### *4.3.1 Key exchange protocol*

In the proposed key exchange protocol, described in Figure 4, the ED first generates a random key $w \in \{0,1\}^k = w_1 w_2 ... w_k$ of length $k$. The key $w$ is modulated into vibration, which is received by the IWMD and converted into a bit string $w'$ using the two-feature OOK demodulation scheme. Note that $w'$ may differ from $w$ due to errors during transmission. The IWMD encrypts a predefined, fixed confirmation message $c$ using $w'$ as the key to get a ciphertext $C = E(c, w')$ and transmits it to the ED through the RF channel. If $C$ is successfully decrypted by the ED with $w$, *i.e.*, if $D(E(c,w'),w) = c$, the ED knows that the IWMD received the key $w$ correctly, and the subsequent wireless communication is encrypted using the key $w$.

As previously mentioned, however, the received vibration signal may contain ambiguous bits, which could lead to bit errors after demodulation ($w' \neq w$). Repeating the entire key exchange process until the IWMD receives $w$ correctly may take significant time and energy. When the number of ambiguous bits is small, a key reconciliation step is performed instead of re-starting the key exchange, since the IWMD and the ED only need to agree upon a random key, not restricted to the original key $w$. For key reconciliation, the IWMD makes random guesses for the values of the ambiguous bits to create $w'$ and sends only the locations of those bits, $R$, to the ED using the RF channel. In addition, as explained above, the IWMD encrypts the fixed message $c$ into $C$ with $w'$ and sends it to the ED. The ED performs an exhaustive enumeration of all possible values for the bits in $R$, and obtains a set of key candidates $W$. If any key $w'' \in W$ can decrypt $C$, the key exchange is successfully completed. For example, consider a case in which $k = 4$ and $w = 1011$. Assume that $w_2$ and $w_3$ are ambiguous, and the IWMD makes guesses that $w_2 = 1$ and $w_3 = 0$, resulting in $w' = 1\underline{1}\underline{0}1$ and $R = \{2,3\}$. Upon receiving $R$, the ED prepares a set of candidate keys $W = \{1\underline{0}\underline{0}1, 1\underline{0}\underline{1}1, 1\underline{1}\underline{0}1, 1\underline{1}\underline{1}1\}$. Since $C$ can be decrypted by one of these keys, *i.e.*, 1101, the IWMD and ED can start encrypted communication with this key. Figure 4 illustrates the overall protocol. If the number of ambiguous bits detected during demodulation exceeds a predefined limit, or if none of $w'' \in W$ is able to decrypt $C$, the key exchange process is restarted with a fresh random key.

Considering the severe asymmetry in energy and computational capability between the IWMD and the ED, this key exchange protocol minimizes the effort expended by the IWMD. The IWMD prepares only one key $w'$, encrypts $c$ with it, and sends $C$ only once. The IWMD is not burdened with any extra computation or communication compared to the case where $w'$ exactly matches $w$. This is achieved at the cost of requiring the ED to perform multiple decryption trials using the various candidate keys, which is acceptable in our scenario since the ED has a much larger energy budget and computation power.

### *4.3.2 Security analysis and attack mitigation*

We discuss various possible attacks on the vibration channel and, where merited, countermeasures against them.

Direct attacks on the vibration channel include passive attacks to eavesdrop on the key exchange using an accelerometer and active attacks to illegitimately wake up the RF module using a vibration motor. Such direct attacks on the vibration channel, however, are not likely to be possible due to the short transmission range, as we demonstrate in Section 5.4.

A more likely attack on the vibration channel is acoustic eavesdropping, which captures the sound generated by the vibration motor and uses suitable signal processing techniques to recover the key. More sophisticated forms of this attack would use multiple microphones and differential analysis to mitigate noise. As described in Section 5, we successfully implemented a countermeasure against both simple and differential acoustic attacks. We exploit the fact that mobile devices typically integrate speakers and propose acoustic masking as a countermeasure to such acoustic attacks. When the ED transmits the key through the vibration channel, it also generates a masking sound pattern from its speaker. To maximize the effectiveness of masking, it utilizes band-limited Gaussian white noise that is restricted to the same frequency range as the acoustic signature of the vibration motor. In our experiments, we found that this also had the desirable side effect of making the masking sound less unpleasant to the user.

The last possible attack is to eavesdrop on the RF channel. If an attacker eavesdrops on the RF channel during the key exchange, he may obtain the locations of the guessed bits, $R$, and the encrypted confirmation message $C$. From $R$, the adversary gets to know which bits of the key are randomly guessed by the IWMD. However, this information about the locations of random bits does not provide any information about the actual values of those bits. Note that the key reconciliation is equivalent to generating a key by combining $k - |R|$ random bits from the ED and $|R|$ random bits from the IWMD. Also, since $c$ is encrypted only once by the IWMD and only a single $C$ is sent over to the ED, related-key attacks[2] are not feasible.

We discuss further details of our security evaluation and countermeasures for acoustic eavesdropping attacks in the next section.

# 5. IMPLEMENTATION AND EVALUATION

In this section, an ex vivo evaluation of SecureVibe is presented by implementing it on an IWMD prototype embedded in a realistic human body model.

## 5.1 Prototype Design and Experimental Setup

Figure 5 presents the prototype IWMD platform that we developed and the experimental setup used to evaluate it. The IWMD platform is based on the nRF51822 RF SoC, which has an ARM Cortex M0 core and a 2.4-GHz transceiver for Bluetooth Smart, and supports two different accelerometers with distinct power and sampling rate specifications. The ADXL362 accelerometer consumes very low power (3 μA

[2]Cryptanalysis where the adversary can observe multiple ciphertexts that are encrypted with slightly different keys.

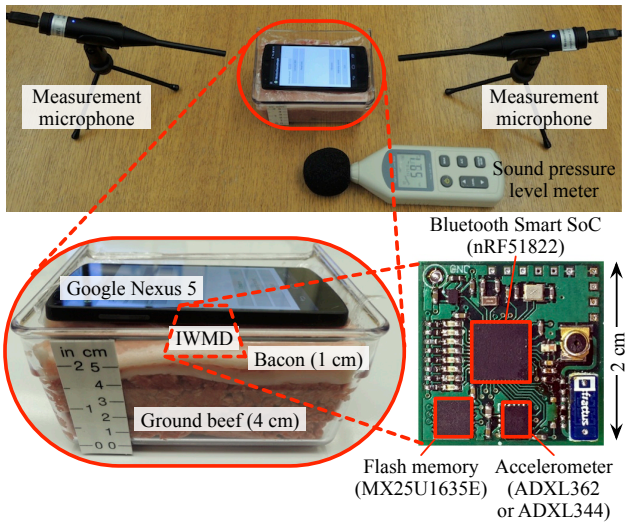


Figure 5: SecureVibe prototype and experimental setup.

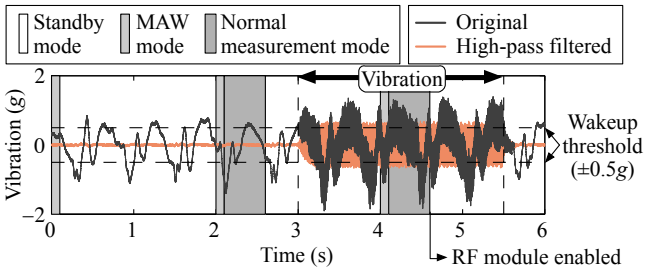


Figure 6: Wakeup vibration generated while the patient is walking.

in active mode, 270 nA in MAW mode, and 10 nA in standby mode), which is suitable for persistent motion detection, but its sampling rate is limited to 400 sps. On the other hand, the ADXL344 accelerometer has a higher sampling rate of up to 3200 sps, but due to its high power consumption (140 μA in active mode), it is more suitable for an occasional high sampling rate measurement. We used the Google Nexus 5 smartphone as the ED. We developed an Android application that generates a random cryptographic key, and executes the proposed wakeup scheme and key exchange protocol, while concurrently playing the masking sound.

Figure 5 (bottom left) shows the experimental setup used to evaluate the performance of vibration-based wakeup and key exchange in an emulated human body model that consists of a 1-cm layer of bacon on a 4-cm layer of 85% lean ground beef. The IWMD prototype is placed between the bacon and the ground beef, which reflects the typical implementation of implantable cardioverter defibrillators (ICDs) [2]. The ED is placed directly on the bacon layer with a thin plastic sealing.

The setup used to implement acoustic eavesdropping attacks and evaluate the proposed countermeasure is also shown in Figure 5 (top). We use precision measurement microphones, the Dayton Audio UMM-6, for sound measurement and analysis and a sound pressure level meter from Koolertron for measuring the ambient noise level.

## 5.2 Wakeup Vibration Detection

We first demonstrate the vibration-based wakeup scheme using the ADXL362 accelerometer and estimate its power consumption. To evaluate the scheme in the presence of motion-induced noise, we perform the experiment while a human is walking with the IWMD prototype, and the results are shown in Figure 6. The period and duration of the MAW mode are 2 s and 100 ms, respectively, and the duration of the normal measurement mode is 500 ms. Figure 6 shows the original vibration signal and the high-pass filtered vibration using a moving

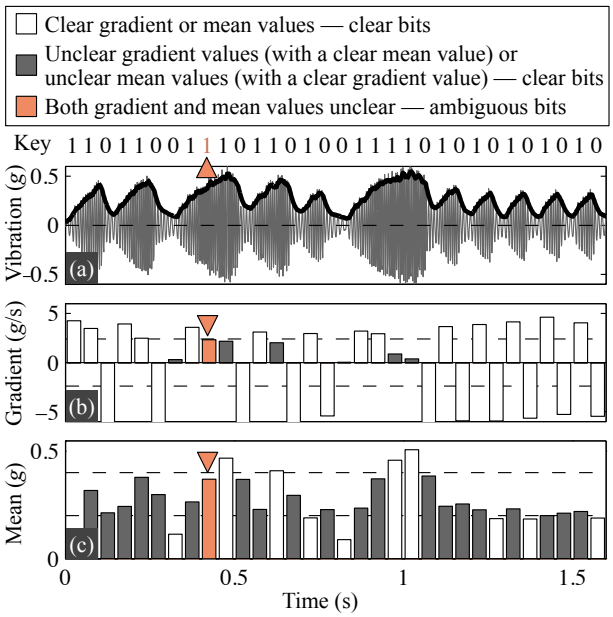


Figure 7: Modulation and demodulation for 32-bit key exchange at 20 bps. (a) Vibration waveform, (b) amplitude gradient, and (c) amplitude mean. In (b) and (c), the dashed lines indicate the gradient and mean thresholds, respectively.

average filter. The accelerometer did not detect any significant vibration in the first MAW period and, hence, returned to the standby mode immediately. In the next MAW period, the large vibration due to the motion of walking made the accelerometer enter the normal measurement mode for 500 ms for full-rate sampling. However, as no vibration was detected after high-pass filtering (false-positive), it returned to the standby mode without enabling the RF module. In the third MAW period, the accelerometer again entered the normal measurement mode. This time, the residual vibration after high-pass filtering was accepted as a wakeup signal, and the RF module was enabled. For the settings used in our experiments, the worst-case wakeup time was 2.5 s (1.8 s in the standby mode in the worst case, 200 ms in the MAW mode, and 500 ms in the normal measurement mode).

In practice, the worst-case wakeup time can be traded off against energy consumption by varying the time spent in the standby mode. Let us conservatively assume that the false-positive vibration detection rate is 10% (*i.e.*, 2.4 hours of active movement per day). We set the period for which the accelerometer enters the MAW mode to be 5 s (*i.e.*, the worst-case wakeup time is 5.5 s). For an IWMD with a 1.5-Ah battery and 90-month lifetime, the estimated energy overhead of the accelerometer and the microcontroller is only 0.3% of the total energy budget.

## 5.3 Key Exchange

We demonstrate cryptographic key exchange using our prototype platform with the bit rate set to 20 bps. This bit rate enables the exchange of a 256-bit key in 12.8 s. For illustration, we show the measured waveforms for a shorter 32-bit key exchange in Figure 7. The bit string at the top is modulated into a vibration waveform, as shown in Figure 7(a). The gray waveform is the vibration measured by the IWMD platform, and the thick black curve is its envelope. The amplitude gradient and the amplitude mean of each segment are displayed in Figures 7(b) and (c), respectively. The dashed lines denote the thresholds, and gray bars indicate the values that lie between the two thresholds. Out of 32 bits, 31 bits could be demodulated clearly, but the 9-th bit, which is highlighted with triangular markers, was an ambiguous bit. Therefore, the ED receives $R = \{9\}$ from the IWMD, and could find $w'$ within two trials to decrypt $C$.

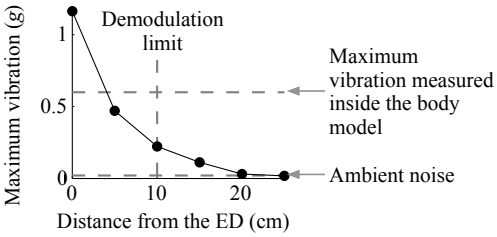


Figure 8: Maximum vibration amplitude measured at different distances from the ED on the chest surface.

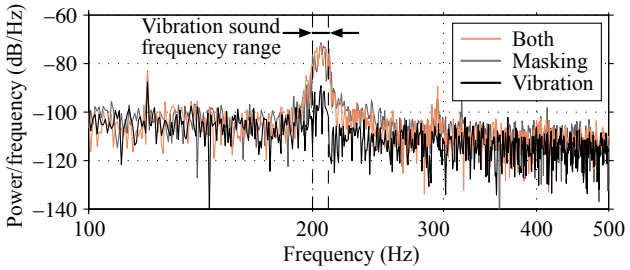


Figure 9: Power spectral density of the vibration sound, the masking sound, and both, measured 30 cm away from the ED.

## 5.4 Security Evaluation

In this subsection, we evaluate various security attacks on the vibration channel. First, in order to see the feasible range of direct attacks on the vibration channel, we placed the ED on the chest of a human subject, measured the vibration at the body surface at varying distances from the ED, and attempted to recover the key. Figure 8 shows the vibration amplitude measured at distances of 0 to 25 cm from the vibrating ED. As shown in Figure 8, the vibration exponentially attenuates with distance. The key exchange was successful only within 10 cm. Therefore, an eavesdropping device to pick up the vibration should be placed on the body surface within 10 cm of the IWMD, which is not likely to be possible without the patient noticing.

Next, we evaluate the potential of acoustic eavesdropping attacks. We measured the sound, which includes the vibration sound and the masking sound, at 30 cm distance from the ED, and tried to obtain the key from the recorded sound waveform instead of the vibration waveform, using the same demodulation scheme. We assume that the attacker also has access to the RF channel and is able to know from $R$ which bits are guessed by the IWMD, and is able to accurately find the beginning of the vibration. Even after making such assumptions favorable to the attacker, we could not successfully demodulate the vibration into the correct key due to the strong masking sound. Figure 9 compares the power spectral densities of three sounds: vibration sound only, masking sound only, and vibration sound with masking sound. These measurements were taken in a room with an ambient noise level of 40 dB. The vibration sound is significant in the frequency range of 200 to 210 Hz, and the masking sound is stronger than the vibration sound in this range by at least 15 dB. This explains the effectiveness of the masking scheme.

If an attacker is capable of recording the sound at multiple locations, differential attacks may be performed. The independent component analysis (ICA) technique separates a signal into additive subcomponents, and can be used to separate two sound sources measured from two different locations. Since the vibration sound and the masking sound are generated from different sources (the vibration motor and the speaker, respectively), the attacker may try to separate them using the ICA technique. We placed two identical microphones each at a distance of 1 m (a reasonable distance for acoustic eavesdropping), but on opposite sides of the ED, and used them to eavesdrop on a key exchange in the presence of acoustic masking. Running the FastICA algorithm [18] produced two waveforms, one of which is expected to be the vibration sound, and the other one to be the masking sound. However, neither of the two separated waveforms could be demodulated successfully. This is because the two sound sources are too close to each other for the channel difference to be recognized by the two microphones.

# 6. CONCLUSION

We proposed a secure side channel based on vibration to enable secure wireless communication with IWMDs. Vibration has unique advantages for realizing a secure side channel, such as close proximity requirement, user perceptibility, and low power consumption. Based on the vibration channel, we proposed SecureVibe, which incorporates (i) a low-power wakeup scheme for IWMDs to prevent battery drain attacks, and (ii) a key exchange scheme for sharing a secret key that can be used for subsequent protection of the RF channel. To enable acceptable key exchange times, we devised a two-feature OOK scheme to increase the bit rate achievable using the vibration channel. We implemented a prototype IWMD with the proposed schemes and presented ex vivo evaluations in a realistic human body model to demonstrate their effectiveness. The ubiquitous availability of the requisite capabilities in mobile and wearable devices makes vibration-based wakeup and key exchange a viable approach in a broad range of scenarios.

# 7. REFERENCES


[1] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proceedings of the IEEE*, vol. 102, no. 8, 2014.

[2] D. Halperin, T. 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 *Proceedings of the Symposium on Security and Privacy*, 2008.

[3] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proceedings of the International Conference on e-Health Networking Applications and Services (HealthCom)*, 2011.

[4] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the energy consumption of security protocols," in *Proceedings of the International Symposium on Low Power Electronics and Design (ISLPED)*, 2003.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology*, ser. Lecture Notes in Computer Science, 1999, vol. 1666.

[6] N. Saxena, M. Uddin, J. Voris, and N. Asokan, "Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags," in *Proceedings of the International Conference on Pervasive Computing and Communications (PerCom)*, 2011.

[7] J. Lester, B. Hannaford, and G. Borriello, "Are you with me? – using accelerometers to determine if two devices are carried by the same person," in *Proceedings of the International Conference on Pervasive Computing and Communications (PerCom)*, 2004.

[8] D. Kirovski, M. Sinclair, and D. Wilson, "The martini synch: Device pairing via joint quantization," in *Proceedings of the International Symposium on Information Theory (ISIT)*, 2007.

[9] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan, "User evaluation of lightweight user authentication with a single tri-axis accelerometer," in *Proceedings of the International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI)*, 2009.

[10] 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, 2009.

[11] T. Halevi and N. Saxena, "Acoustic eavesdropping attacks on constrained wireless device pairing," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, 2013.

[12] S.-Y. Chang, Y.-C. Hu, H. Anderson, T. Fu, and E. Y. L. Huang, "Body area network security: Robust key establishment using human body channel," in *Proceedings of the Conference on Health Security and Privacy (HealthSec)*, 2012.

[13] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proceedings of the Conference on Computer Communications (INFOCOM)*, 2008.

[14] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proceedings of the Conference on Computer Communications (INFOCOM)*, 2011.

[15] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proceedings of the Conference on Computer & Communications Security (CCS)*, 2013.

[16] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM Conference*, 2011.

[17] M. Rushanan, C. Swanson, D. F. Kune, and A. D. Rubin, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proceedings of the Symposium on Security and Privacy*, 2014.

[18] A. Hyvärinen and E. Oja, "Independent component analysis: Algorithms and applications," *Neural Networks*, vol. 13, no. 4–5, 2000.