Securing Wireless Implantable Devices for Healthcare: Ideas and Challenges

Kriangsiri Malasri and Lan Wang, University of Memphis

ABSTRACT

Implantable devices hold great potential for pervasive healthcare, enabling the identification, monitoring, and treatment of patients regardless of their location. To realize this goal, these devices must be able to communicate wirelessly with external devices. However, wireless communication presents many vulnerabilities: an attacker can eavesdrop on transmitted information, use implanted devices to track patients, or spoof an implanted device. An attacker even has the potential to cause direct physical harm to a patient, either by forcibly removing an implanted device from the patient or by maliciously sending commands that affect the operation of an implanted device. Addressing these security threats is crucial for implantable devices due to their permanent nature, but it is difficult because of the severe resource constraints facing such devices. This article details the threats that face wireless implantable devices, surveys the work addressing these threats, and identifies open issues for future research.

INTRODUCTION

Although the term *implantable device* may evoke futuristic images of part-human, part-machine cyborgs, such devices have been used for some time, especially in healthcare. For instance, implantable pacemakers for regulating heart rate were invented in the late 1950s. As technological innovations make implantable devices smaller, safer, and longer-lasting, researchers are developing more applications using these devices to achieve the vision of *pervasive healthcare*. These applications include patient identification, continuous monitoring of patients, and automatic delivery of medications. Implantable devices can potentially outperform their non-implantable counterparts. An implantable insulin pump, for instance, can be placed close to the location of a normal pancreas, enabling more effective absorption of insulin than traditional injections.

Many implantable devices have the ability to communicate wirelessly with other devices. Such a capability can be very useful; for example, an implanted drug delivery device might be reprogrammed remotely to alter its dosage without having to be removed from the patient. However, wireless communication channels are vulnerable to malicious attackers, who might compromise sensitive patient data or even cause physical harm to patients by reprogramming implanted devices. *Security issues deserve particular attention for implantable devices because a person cannot simply remove a device to protect himself or herself from an attack.*

A major challenge in securing implantable devices is the extreme resource constraints facing them. Many devices are completely passive, with no power or computational resources of their own. This makes it difficult to implement traditional security schemes that require them to perform cryptographic operations on data. Even devices that do have computational capabilities are constrained by battery lifetime — their batteries must function for years because changing batteries may require potentially life-threatening surgery. Thus, a practical security scheme must be as efficient as possible.

Similar security issues also exist for many devices with wireless communication capability, including non-implantable medical devices, as well as devices not strictly meant for use in healthcare (e.g., motes in wireless sensor networks). Although there is a wealth of literature on securing such devices, care must be taken when applying this work to implantable devices. Implantable devices are difficult to access directly or remove; this factor might not be considered in a security scheme that is not specifically designed for these devices.

In this article, we classify wireless implantable devices into *identification*, *monitoring*, and *control* devices and present their security issues separately.[1] Figure 1 illustrates these categories and the types of wireless communication that is useful to each.

Implantable identification devices (IIDs) are used strictly for providing personal information. They are not necessarily medical devices, but because of their applications in healthcare, we consider them in this survey. Identification devices must send a patient identifier to an external reader.

Implantable monitoring devices (IMDs) are capable of measuring the physiological characteristics of a patient. Examples include blood glucose sensors and electrocardiogram monitors. Monitoring devices communicate with an external device with their sensed physiological data. In addition, one IMD can send its data to anoth-

[1] *We do not consider devices that are implanted for short durations (e.g., during surgery to monitor a patient) nor devices without any communication capability (e.g., implantable contact lenses).*

er IMD for data aggregation or fusion purposes.

Implantable control devices (ICDs) are capable of altering the physiological characteristics of a patient. Some control devices have integrated monitoring capabilities as well. Examples include artificial pacemakers and drug delivery devices. Control devices *receive* commands from an external device that enable the adjustment of settings on the implanted device. They can also send information on their current status (as well as sensed data, if the control device has integrated monitoring capabilities) to an external device.

In the following sections, we present the security threats and countermeasures relevant for each type of device. Wherever possible, we focus on work that specifically addresses implantable devices. However, because much of the work in this area is nascent, we include some countermeasures that are not proposed specifically for implantable devices but for external devices with similar resource constraints. Finally, this article is not intended to be a complete summary of the relevant literature. Rather, our goal is to identify open issues for future research.

IIDs

IIDs serve strictly to provide identifying information about a person. Thus far, the IIDs we are aware of are implantable, radio-frequency identification (RFID) tags. Such a tag is generally very small (comparable in size to a grain of rice), with no power source of its own. When scanned by an external reader, the tag uses the energy in the reader's signal to emit a unique identifier wirelessly.

The most well-known IID is VeriChip Corp.'s RFID tag (Fig. 2), which was approved for human implantation by the U.S. Food and Drug Administration in 2004. The VeriChip is usually implanted in the upper arm. Authorized medical professionals can use the serial number emitted by a VeriChip to access a person's medical information in a database called VeriMed. This makes it possible to quickly retrieve vital information even if the patient is unresponsive or unconscious, for example, in a medical emergency. According to the company Web site, "thousands" of people have had this chip implanted.

Whereas the VeriChip is intended chiefly for convenient access to medical records, IIDs can have other practical uses in healthcare as well. For example, physicians and other medical professionals can use IIDs to gain access to sensitive hospital areas or to certain patient records. From the patient's perspective, IIDs might be used to verify a patient's identity before performing an operation or administering a drug treatment.

Possible Attacks

The VeriChip and other IIDs have been subject to much controversy, partly due to privacy and security concerns. In principle, such devices are vulnerable to a number of threats.

Harvesting — If an IID is not capable of authenticating the interrogating reader, an attacker may try to illegitimately obtain the information stored in an IID with his own reader. Alternately, an attacker might eavesdrop on the communication between an IID and a valid reader. The harvested information may be used directly or to carry out additional attacks such as *tracking* and *cloning*.

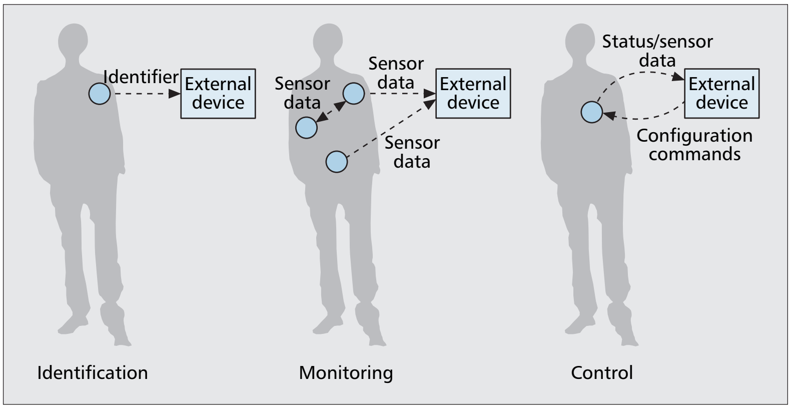


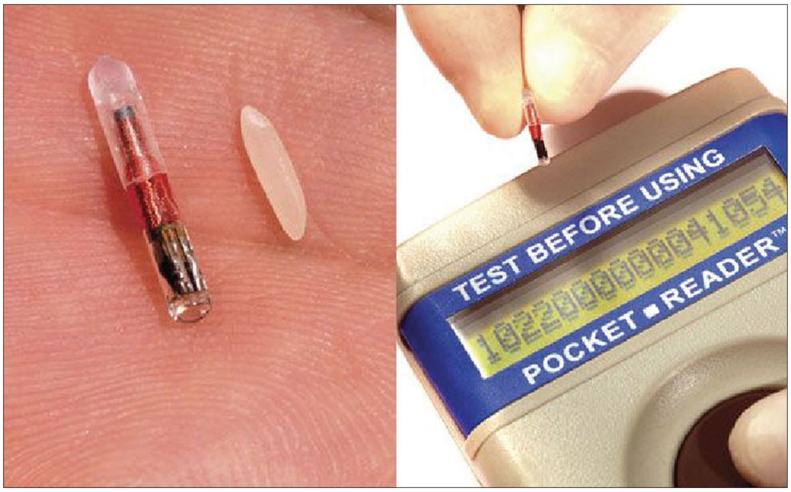
Figure 1. *Types of wireless communication in implantable identification, monitoring, and control devices.*

Tracking — Someone with access to a large number of readers can potentially monitor people's locations as they move within range of different readers. This is possible even if the IID identifier contains no intrinsic private information and/or is encrypted, as long as the identifier is unique and static for each IID. Note that tracking is sometimes mentioned as a *beneficial* application of using RFID devices (e.g., for tracking mentally unstable patients). In general, however, the ability to track an implantable device poses a privacy threat.

Cloning — An attacker can replay a harvested identifier to a valid reader and attempt to pass herself off as someone else — in effect, the attacker has *cloned* another person's identifier. This has been performed successfully on the VeriChip [1]. In a variant called *existential cloning* [1], the attacker can try to generate a valid identifier by guessing or analyzing known identifiers. This could be used, for example, to illegitimately gain privileges granted by an IID.

Relay Attack — IIDs typically have limited communication ranges, on the order of inches. Thus, a reader must be in close proximity to an IID. However, an attacker can greatly extend this range by using two devices, called a *ghost* and a *leech*, capable of fast long-range communication (e.g., Wi-Fi) [2]. The ghost pretends to be an IID to a valid reader *R*, while the leech pretends to be a reader to a valid IID *D*. By relaying the messages between *R* and *D*, the leech and ghost can trick *R* and *D* into believing that they are communicating normally while harvesting useful information from the messages. Such a relay attack might be used to overcome *distance-measurement* countermeasures.

Physical Compromise — If an IID grants its bearer privileges, an attacker may be motivated to illegitimately obtain these privileges by coercing a person or even forcibly removing the IID. There have been reports of similar incidents



■ **Figure 2.** *(Left) The VeriChip implantable RFID tag, with a grain of rice for size comparison. (Right) The handheld reader used to scan the VeriChip. (Source: VeriChip Corp., used with permission).*

with biometric security tools; for instance, in 2005 Malaysian car thieves severed a victim's finger to steal his Mercedes, which was equipped with a fingerprint recognition system.

COUNTERMEASURES

Although security issues regarding IIDs such as the VeriChip have been mentioned widely in the literature, few countermeasures have been proposed specifically for IIDs. However, extensive research has been performed for securing general RFID devices. Here we outline some proposed solutions that are applicable to IIDs and identify which of the above threats they address.

The most straightforward way of discouraging harvesting is to *limit the amount of information* contained in the IID. VeriChip seems to have adopted this approach; the IID simply contains a serial number without any personal information such as medical history. To gain such information, the attacker must also have access to the VeriMed database. If the database is sufficiently secure, no patient information is at risk of being compromised. However, this approach alone does not prevent other attacks such as cloning or tracking.

Distance measurement [3] attempts to control the information emitted from an RFID tag based on its distance from the reader. Fishkin, Roy, and Jiang [3] note that the signal-to-noise ratio of the reader's signal can be used to estimate the distance between the reader and the tag. They propose that with some added circuitry, a tag could compute this distance and release tag-specific information, such as an identifier, only to readers within a certain range. An attacker thus must be in close proximity to the tag to harvest its identifier; this also makes tracking an IID difficult. However, it still allows harvesting in close quarters and relay attacks.

In *blocking* approaches [4], an RFID tag relies on a second tag called a blocker to prevent itself from being scanned by readers. The blocker transmits certain identifiers to collide with the blocked tag's transmission, making it impossible for the reader to obtain a clear reading. We note, however, that the particular blocking approach outlined in [4] works only for readers that use a tree-walking singulation protocol. The blocker can be turned on or off at will, allowing the tag's owner to control when it can be read. In the context of IIDs, this might be accomplished by incorporating blocker tags into common devices such as cell phones. Blocking addresses the threats of harvesting, tracking, and cloning but also prevents the tag's functionality when it is turned on.

To prevent harvesting by arbitrary readers, as well as tracking and cloning, an IID can *authenticate readers using shared secrets*. These secrets can be used to assure that only valid readers can identify the tag correctly. Weis *et al*. [5], for instance, suggest that each time a tag is interrogated, it generates a random number r and emits a message of the form (r, $d \oplus f_k(r)$), where f_k is a pseudo-random function computed using secret key k, and d is the tag's identifier. Under this scheme, a valid reader with knowledge of k can easily determine d, whereas a random reader sees a different number every time the tag is queried. An attacker without the correct secret information cannot use his own reader to collect identifiers. However, the IID must be capable of cryptographic operations, which is usually not the case with the IIDs available today (such as the VeriChip). Furthermore, the idea of using shared secrets for authentication poses an interesting dilemma due to the fact that a reader can store different secrets for multiple tags. How does the reader know which secret to use when receiving a message from an IID if the identifier is hidden? Researchers have proposed a procedure called *key search* to address this issue (see Sections III-A and III-B of [6]). Briefly, the concept is for a reader to cycle through the set of secrets until it finds one that works for the current tag. Finally, as discussed later, if the shared key is compromised, it is a challenge to securely update the key, given that the device is implanted in the body.

Below we describe two more methods to vary the identifier emitted from a device. In *minimalist cryptography* [7], the basic idea is for a tag to have a set of identifiers and choose one from the set to send each time it receives a reader signal. A valid reader has access to the entire list of identifiers. Although this scheme makes it more difficult for an attacker to clone or track a tag, a naive implementation is vulnerable to brute-force interrogation by an attacker in order to harvest all possible identifiers of a tag. To address this weakness, Juels [7] suggests that tags limit their responses when rapidly interrogated. Juels also proposes a protocol to enable valid readers to update the list of identifiers stored in the tag, using a mutual authentication scheme. However, the protocol assumes that attackers cannot eavesdrop on the communication from readers to tags for an extended period of time.

In *re-encryption* schemes [1] (Fig. 3), a tag identifier is encrypted using the reader's public key (*PK*), producing a ciphertext. Whenever the tag is interrogated, the current ciphertext is *randomly* re-encrypted using *PK* to produce a different ciphertext. The crucial requirement is that a reader possessing the correct private key *SK* is able to decrypt any of the derived ciphertexts into the original plaintext. Moreover, the derived ciphertexts must be *unlinkable* — without knowledge of *SK*, it must be infeasible to determine if two ciphertexts are re-encryptions of the same plaintext or just random strings. Both of these properties can be assured by using a *homomorphic* public-key scheme such as El Gamal. With such a re-encryption system, an attacker receives a constantly changing identifier each time she queries a tag, making tracking difficult. Cloning, however, can still be performed easily: an attacker simply must obtain one valid ciphertext and use *PK* to repeatedly re-encrypt the ciphertext herself. Kinoshita *et al*. [8] propose several variants of re-encryption that avoid public-key operations, including common key encryption and hash-chaining.

A number of countermeasures for relay attacks have been proposed in the context of RFID systems — for example, for contactless smart cards [9] — but not specifically for IIDs. These techniques include measuring the time delay of messages and using triangulation to estimate the location of a communicating party. However, Hancke [9] concludes that such schemes are unreliable and/or impractical and computationally expensive.

Physical attacks have not been well addressed in the literature. Interestingly, Halamka *et al*. [1] argue that to reduce the incentive for coercion or forced removal of an IID, an IID should be able to be easily cloned *by design*. Furthermore, Halamka *et al*. suggest that IIDs be applied only for identification (as in the intended use case of the VeriChip) and not for authorization or access control.

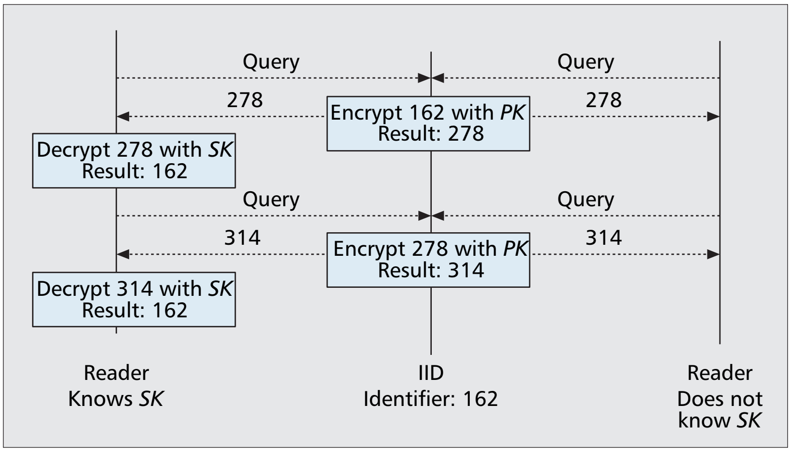


Figure 3. *Illustration of a re-encryption scheme for RFID tags. A reader without knowledge of the private key SK receives constantly changing identifiers.*

Figure 4. *Implantable radiation sensor developed by Dr. Babak Ziaie's group at Purdue University. (Source: Babak Ziaie, used with permission).*

IMDs

We define IMDs as those that are capable of measuring physiological characteristics of the patient but cannot directly affect the patient. IMDs are often developed with wireless communication capability because the data collected by an IMD must be transferred to some external collection device to be of any practical use. An IMD might also send data to another IMD for data aggregation or fusion purposes. As an example of recent IMD research, Purdue University has developed an implantable radiation sensor [10] that will help doctors more accurately deliver radiation treatments to cancer patients (Fig. 4).

Possible Attacks

Since IMDs collect medical data that must be transmitted wirelessly, they are subject to many of the same threats facing IIDs. An attacker may attempt to illegitimately obtain patient data directly (the equivalent of harvesting identifiers in IIDs). Patient data conceivably also could be used to track patients if the data can uniquely identify patients. Finally, an attacker may try to pass one patient's data off as another patient's data or generate falsified patient data [11]. This is the IMD equivalent of cloning an IID.

In addition to the above threats, IMDs are subject to denial-of-service (DoS) attacks.[2] An attacker might flood the wireless channel with meaningless transmissions, rendering the IMD unable to send data. This type of attack is difficult to defend against. Misic and Misic [12] have compared the DoS resilience of two technologies (Bluetooth and IEEE 802.15.4) for wireless transmission of patient sensor data; they conclude that Bluetooth is superior.

Countermeasures

Addressing security in IMDs can be reduced to three main goals:

- Preventing attackers from harvesting patient information through eavesdropping
- Preventing unauthorized devices or personnel from accessing patient information
- Enabling receivers to authenticate patient data to prevent data falsification

As for DoS attacks, we are not aware of any relevant studies specifically targeting IMDs. However, work has been done on addressing DoS in resource-constrained, wireless sensor networks; Raymond and Midkiff [13] provide a survey.

[2] *We note that DoS attacks may apply to IIDs as well. However, they are more relevant to IMDs, as unlike IIDs, IMDs may require continuous data transmission to operate as intended.*

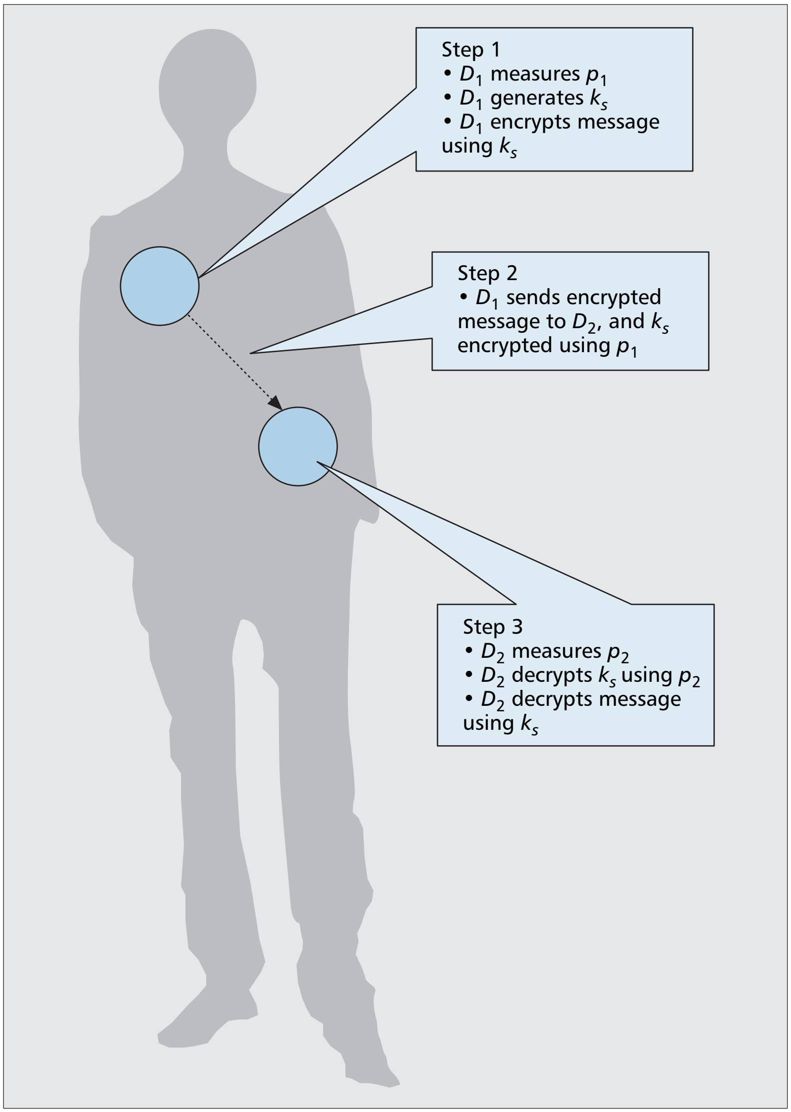

Step 1
• D_1 measures p_1
• D_1 generates k_s
• D_1 encrypts message using k_s
Step 2
• D_1 sends encrypted message to D_2, and k_s encrypted using p_1
Step 3
• D_2 measures p_2
• D_2 decrypts k_s using p_2
• D_2 decrypts message using k_s

Figure 5. *Biometric-based keying. Communicating IMDs* D_1 *and* D_2 *measure the same physiological quantity, producing readings* p_1 *and* p_2*.* p_1 *and* p_2 *are used to secure an encryption key* k_s *generated by the sending IMD.*

Data Encryption — To prevent harvesting through eavesdropping, patient data must be *encrypted* before transmission. Two options exist for encryption: secret-key or symmetric encryption and public-key or asymmetric encryption. Symmetric encryption is attractive in IMDs for its efficiency. However, it presents the challenge of key management: how to securely generate, store, and update secret keys between a sender and a receiver. The most straightforward approach is to pre-configure secret keys in communicating devices before implantation. If the key is compromised by an attacker, however, a device requiring a new key must be physically removed from the patient and manually reconfigured. As this is not a practical solution, we require efficient key management schemes.

There has been extensive work on key management in wireless networks in general, but not specifically for implantable devices. We provide two examples below that illustrate requirements that are similar to what is required in implantable devices: one for communication between an IMD and an external collection device and the other for communication between two IMDs.

We propose an elliptic curve cryptography (ECC)-based key-management protocol [11] to securely derive and update symmetric keys between medical sensors and collection devices. ECC consumes fewer resources than the popular Rivest Shamir Adelman (RSA), while providing comparable security. Our protocol enables symmetric keys to be derived without the existence of any prior shared secrets, making it scalable to large systems where individually configuring devices with secret information would be prohibitive. This is especially desirable for implantable devices, as they cannot simply be removed from a patient to reconfigure shared secret information. Our work was originally intended for use with non-implanted medical sensors attached to *wireless motes*, which also have severe resource constraints.

Biometric-based keying, proposed by Cherukuri, Venkatasubramanian, and Gupta [14], allows two IMDs to secure shared-secret keys (Fig. 5). Under this scheme, two IMDs that wish to communicate measure the same physiological quantity of the patient and use it to secure an encryption key generated by the sender. For this to work, both devices must be able to measure the same quantity, and the two readings must be able to handle slight deviations from each other. To address the latter issue, Cherukuri *et al*. suggest using error correction schemes such as majority encoding.

Data Access Control — The schemes presented above address the mechanics of symmetric key management. Once the encryption mechanisms are established, the main concern becomes not *how* the data is encrypted, but rather *who* should have access to it. One issue is how an IMD can authenticate an external device to ensure that it is valid. To do this, many of the same mechanisms outlined for IIDs could be used (e.g., using shared secrets); we do not reiterate them here.

At a higher level, there must be some system of determining which entities (such as personnel) should have access to patient data. The simplest approach is for each patient record to have an *access control list* indicating the entities who have the right to view it. However, this is not scalable; for an environment like a large hospital, it becomes tedious to maintain a long list of authorized entities. In response, researchers devised the idea of role-based access control (RBAC). In RBAC, users are categorized into *roles*, each of which has its own set of access privileges. For example, a patient record can simply indicate "allow access from *doctors*," rather than "allow access from Dr. Jane Smith, Dr. Joe Smith, and Dr. John Doe." Several variants of RBAC have been proposed for the health-care industry, including schemes that provide deny-lists and schemes for providing rapid access in emergencies; Venkatasubramanian and Gupta [15] survey a number of these.

Addressing Data Spoofing — A receiver of patient data must be able to verify that the data actually belongs to the patient it claims to be from. We present a two-tier authentication scheme [11] for a collection device to verify the source of incoming patient data. At the first tier, a biometric signature from the patient — for example, a fingerprint — is sent to the collection device. Data from that patient is accepted only if the signature belongs to a valid patient in the system. At the second tier, incoming physiological data is continually passed to a filter that assesses whether the data is consistent with prior data from that patient. The filter uses statistical or machine-learning techniques to *learn* a patient's profile and then raises an alarm if incoming data deviates from that profile. An alarm could be triggered by falsified patient data or an acute change in the patient's medical condition; either case warrants checking on the patient. We implemented this filter using neural networks on electrocardiogram signals with promising results. This scheme is designed for non-implanted sensors under tight resource constraints, but it could easily be applied to implanted devices because the computational burden of the filter lies with the collection device.

Poon, Zhang, and Bao [16] propose a scheme for verifying the source of sensor data in communications among different sensors. For two sensors to communicate, they must first demonstrate that they belong to the same patient by measuring a certain physiological value. Communication can proceed only if this value matches in both sensors; Poon, Zhang, and Bao suggest the time between heartbeats as the biometric of choice. Under this scheme, an attacker trying to spoof data and send it to genuine sensors would fail because he would not have access to the correct biometric. Like the scheme proposed by Cherukuri *et al*. [14], this scheme assumes that different sensors are able to measure the same quantity. However, it differs slightly from the one proposed by Cherukuri *et al*. because the biometric is not used as a key.

ICDs

We define ICDs as those that are capable of directly affecting the physiological characteristics of the patient. Examples include artificial pacemakers and drug-administration systems. Pacemakers regulate cardiac rhythm by delivering electrical impulses to the heart. Within the past decade, brain implants also are being used increasingly. These so-called *brain pacemakers* emit electrical signals to the brain and have been successfully applied to treat neurological disorders such as epilepsy, Parkinson's disease, and even clinical depression. Other types of ICDs are in experimental stages. An implantable insulin pump, for instance, is currently under development at Medtronic, Inc. Some ICDs can double as IMDs (i.e., they have monitoring capabilities). For example, many modern pacemakers can measure electrocardiogram (ECG) signals.

Many ICDs are developed with the capability to communicate wirelessly with external devices to make it easier to configure the ICDs after implantation. Some pacemakers, for example, can receive configuration commands through a magnetic *programming head* that is held close to the pacemaker.

Possible Attacks

Clearly, the ability for an ICD to interact with external devices poses some risks. If ICDs also serve as IMDs, they are subject to the same privacy threats present in IIDs and IMDs (e.g., data harvesting). We do not reiterate those threats here. The unique threat faced by ICDs lies in their *wireless reprogramming* capability. A malicious attacker could conceivably cause direct physical harm to a patient by altering commands sent from an external device to change the electrical current emitted by a pacemaker or the dosage of an implanted drug-administration device.

The unique threat faced by ICDs lies in their wireless reprogramming capability. A malicious attacker could conceivably cause direct physical harm to a patient by altering commands sent from an external device.

Countermeasures

The goal of a countermeasure to the wireless reprogramming vulnerability in ICDs is to allow the ICD to respond only to requests from a valid external device. We are not aware of any academic studies that specifically address this vulnerability in ICDs. With current products, limiting the communication range of the device seems to be the primary defense. ICD security can also be approached through access control at the external level: the patient is secure if only authorized personnel can access external devices capable of communicating with the ICD. However, this cannot be enforced if the attacker possesses her own external device or when the access control mechanism fails.

Despite the lack of academic attention, several patents relevant to securing ICDs exist in industry. In U.S. Patent 6,880,085 [17], Balczewski and Lent propose a password-based method to prevent arbitrary reprogramming of ICDs. Before implantation in a patient, the ICD is configured with a password that must be used on subsequent reprogramming attempts. An attacker without knowledge of the password would be unable to affect the ICD. However, Balczewski and Lent are not specific about how to secure the transmission of the password to the ICD.

In U.S. Patent 7,155,290 [18], von Arx, Koshiol, and Bange present a scheme to enable an ICD to securely communicate with an external device. Here, before communication between an ICD and an external device can occur:

- The external device must transmit an `unlock` command to the ICD through short-range communication
- The ICD and the external device must authenticate themselves to each other, by proving the possession of a shared secret (note that this differs from the prior password scheme because the secret is not transmitted directly).

Hence, to successfully reprogram an ICD, an attacker must be in close proximity, as well as know the secret.

Future Research Directions

We have surveyed the security threats facing implantable devices, from the perspectives of identification, monitoring, and control devices. Some threats have not yet been sufficiently

Future efforts to develop implantable devices should continue to prioritize security due to the permanent nature of these devices. Equally important, future work must also focus on addressing security issues from a systems-level viewpoint.

addressed, such as relay and physical attacks in IIDs, DoS in IMDs, and ICD security in general. Moreover, the existing literature has been largely devoted to specific solutions to specific problems (e.g., minimalist cryptography to address tracking in IIDs). It remains an engineering challenge to integrate multiple aspects of previous work into a comprehensive security solution to address the many potential threats. Designers of implantable medical devices have a responsibility to ensure that these security threats have been thoroughly considered.

In addition, a practical security system for implantable devices must be feasibly implementable under severe resource constraints. This has certainly been a consideration in some existing work; however, the need for resource efficiency will become even more crucial after multiple security schemes are combined into a comprehensive solution.

Regardless of the exact security scheme that an IID, IMD, or ICD uses, if it is based on a configured secret key or a configured public key, the problem still exists as to how to update the key when it is compromised. As mentioned previously, an implantable device must be removed from the human body to be reconfigured in this case, which is very inconvenient and may be life threatening for the patient. It seems that this is one of the most difficult challenges in addressing the security of implantable devices.

CONCLUSION

Implantable medical devices will play a major role in pervasive healthcare, enabling applications ranging from patient identification to remote administration of drug treatments. Considerable work has been done to date to counter the security threats in implantable devices. For IIDs, the threats of harvesting, tracking, and cloning have been addressed by numerous techniques that restrict or vary the information emitted by the device. For IMDs, the problem of keeping patient data private has been approached by using symmetric encryption with various key-management schemes, in addition to variants of role-based access control. Meanwhile, falsification of patient data has been addressed by schemes that use patient biometric data for authentication.

Even so, open issues still exist. Relay and physical attacks in IIDs, DoS in IMDs, and the wireless reprogramming ability of ICDs have not been well addressed in the literature. Future efforts to develop implantable devices should continue to prioritize security due to the permanent nature of these devices. Equally important, future work must also focus on addressing security issues from a systems-level viewpoint.

REFERENCES

[1] J. Halamka *et al.*, "The Security Implications of VeriChip Cloning," J. American Medical Informatics Association, vol. 13, no. 6, Aug. 2006, pp. 601–7.

[2] Z. Kfir and A. Wool, "Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems," *Cryptology ePrint Archive*, 2005; http://eprint.iacr.org/2005/052.pdf

[3] K. P. Fishkin, S. Roy, and B. Jiang, "Some Methods for Privacy in RFID Communication," *Proc. 1st Euro. Wksp. Security Ad Hoc Sensor Net.*, 2004.

[4] A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *8th ACM CCS '03*, Oct. 2003.

[5] S. A. Weis *et al.*, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Security Pervasive Comp.*, vol. 2802, 2004, pp. 201–12.

[6] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE JSAC*, vol. 24, no. 2, Feb. 2006, pp. 381–94.

[7] A. Juels, "Minimalist Cryptography for Low-Cost RFID Tags," *Proc. 4th Conf. Security Commun. Net.*, 2004.

[8] S. Kinoshita *et al.*, "Privacy Enhanced Active RFID Tag," *ECHISE 2005*, May 2005.

[9] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," *Proc. IEEE SecureComm*, 2005.

[10] S. Upson, "Radiation Sensor Fine-Tunes Cancer Treatments," *IEEE Spectrum*, June 2008.

[11] K. Malasri and L. Wang, "Design and Implementation of a Secure Wireless Mote-Based Medical Sensor Network," *Proc. 10th Int'l. Conf. Ubiquitous Computing*, Sept. 2008.

[12] J. Misic and V. B. Misic, "Implementation of Security Policy for Clinical Information Systems over Wireless Sensor Networks," *Ad Hoc Net.*, 2007, pp. 134–44.

[13] D. Raymond and S. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," *IEEE Pervasive Comp.*, Jan.–Mar. 2008, pp. 74–81.

[14] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body," *Proc. IEEE Int'l. Conf. Parallel Processing Wksp.*, 2003.

[15] K. K. Venkatasubramanian and S. K. S. Gupta, "Security Solutions for Pervasive Healthcare," in *Security in Distrib., Grid, Mobile, and Pervasive Computing*, Y. Xiao, Ed., 2007.

[16] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health," *IEEE Commun. Mag.*, Apr. 2006, pp. 73–81.

[17] R. A. Balczewski and K. Lent, "Security System for Implantable Medical Devices," U.S. Patent 6,880,085, Apr. 12, 2005.

[18] J. A. von Arx, A. T. Koshiol, and J. E. Bange, "Secure Long-Range Telemetry for Implantable Medical Device," U.S. Patent 7,155,290, Dec. 26, 2006.

BIOGRAPHIES

KRIANGSIRI MALASRI (kmalasri@memphis.edu) earned his M.S. (2007) in computer science from the University of Memphis. He is an instructor in the Computer Science Department at the University of Memphis. His research has focused on security issues in wireless sensor networks, with an emphasis on healthcare applications.

LAN WANG (lanwang@memphis.edu) holds a B.S. (1997) in computer science from Peking University, China, and a Ph.D. (2004) in computer science from the University of California, Los Angeles. She is an assistant professor in the Computer Science Department at the University of Memphis. Her research interests include network security, Internet routing, network performance measurement, and sensor networks. More information about her research can be found at http://www.cs.memphis.edu/˜lanwang/.