By K.K. Venkatasubramanian,
S.K.S. Gupta, R.P. Jetley, and P. L. Jones

Interoperable Medical Devices

Communication Security Issues

Medical devices are essential for performing modern-day clinical functions. Traditionally, medical devices have been designed to operate in a standalone manner. However, recent years have seen a growth in their ability to communicate information, leading to the emergence of the notion of medical device interoperability. Such interoperable medical devices (IMDs) can afford many advantages in patient care, such as patient context awareness, reduced medical errors, and improved patient safety. However, the potentially sensitive nature of the data being exchanged and increasing use of wireless communication channels demand a security-aware design. This article presents an overview of medical device interoperability, the potential communication-related security threats that manifest as a result of the interoperability, and an overview of the principal approaches to address them.

Consider the following motivation scenario: The year is 2015, a young professional is sitting in an interview for a job. The interview is going really well, and everyone can see her as a good fit for the job. However, unbeknown to the interviewee, one of the interviewers has been eavesdropping on her vital signs the whole time. The idea behind this was to select those candidates who are healthy according to the employer's criteria. The surreptitiously collected data can therefore potentially be used by the employer to influence the eventual hiring decision.

This eavesdropping is possible in many medical devices that use wireless communication, e.g., an insulin infusion pump. As devices begin to interoperate with other devices, the potential for harvesting medical information for nonhealth-care purposes increases.

Unauthorized access to anyone's medical data is a very serious privacy violation. In this case, it can have even more profound consequences as IMDs provide a more detailed view of the patient's health, much more so than any individual device can provide. Moreover, such information can be easily leaked to others (e.g., potential employers and insurance companies) or be used by a malicious entity to remotely actuate a harmful treatment (e.g., deliver high doses of insulin to a diabetic or a shock with implanted defibrillators). We believe that such situations will be realized if the current trend of medical device interoperability and wireless communication continues without appropriate consideration for security.

Digital Object Identifier 10.1109/MPUL.2010.937905

2154-2287/10/$26.00©2010 IEEE

In recent years, health-care providers have been seeking means and methods of aggregating patient data to improve the quality of health care. Today's off-the-shelf technology makes it possible to do much more than just data aggregation. Some in the health-care industry are now considering the notion of medical device interoperation. Many modern medical devices have considerable communication capabilities that can be used to interact with one another. The proliferation of short-distance wireless communication technologies has further opened up the possibility for interdevice communication. Examples of medical devices that are enabled with wireless communication capabilities include oximeters [28], defibrillators, pacemakers [4], and patient monitors [1].

Interoperability models for computing systems [14], [35] have been studied for some time. However, interoperability between medical devices is an emerging topic. Medical device interoperability can be defined as the ability of two or more medical devices to exchange the information they collect with one another and

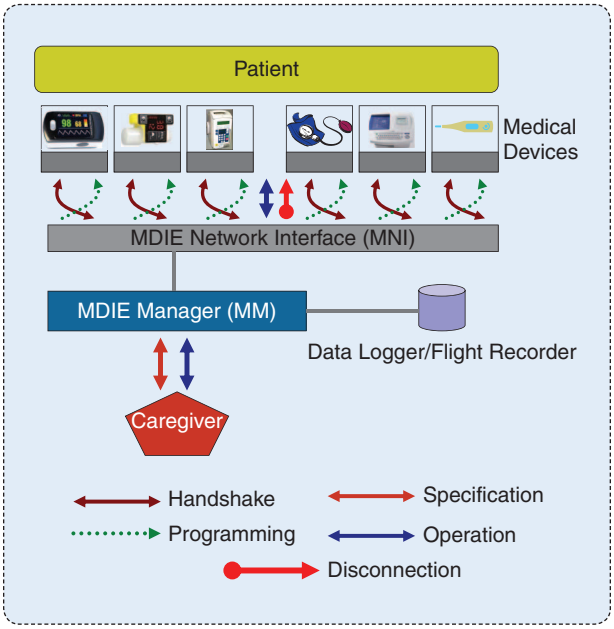

FIGURE 1 MDIE—Functional architecture illustrating the main components and their operation.

to use it for automating processes involved in patient care. Some of the advantages of medical device interoperability in patient care include:

- *Patient Context Awareness*: The ability of medical devices around the patient to exchange information with one another can provide caregivers with a comprehensive view of the current state (context) of a patient's health in a systematic manner.
- *Detailed Patient Health-Record Maintenance*: The ability to aggregate patient information can provide for automatic population and management of electronic health records.
- *Automation of Mundane Tasks*: Devices can coordinate treatment based on rules specified by the caregiver. Such automation has the ability to completely alter the work flow in a hospital environment, allowing a single caregiver to more effectively manage multiple patients at the same time.
- *Error Reduction and Safety*: Medical device interoperability can enable automated enforcement of safety interlocks that can help reduce medical errors.

As IMDs collect and exchange personal health data, assuring security for these devices becomes very important. Lack of security may not only lead to loss of patient privacy but may also cause harm to the patient by allowing attackers to introduce bogus data or modify/suppress legitimate information, resulting in a erroneous diagnosis or treatment. Providing secure communication for IMDs requires preventing attackers from: 1) joining the IMDs around the patient as a legitimate node and introducing bogus health data; 2) accessing confidential health data collected or exchanged between the IMDs; and 3) keeping some or all health data from being reported or modifying actual health data. The Health Insurance Portability and Accountability Act (HIPAA) mandates that all personally identifiable health information be protected [20]. One of the most vulnerable aspects of IMDs is their communication capability, especially when using a wireless interface. Vulnerabilities in the communication interface can allow attackers to monitor and alter the function of medical devices without even being in close proximity to the patient [30]. Case in point: recent demonstration of attacks on implantable cardiac defibrillators by researchers [19] showed the possibility for attackers to surreptitiously read a patient's electrocardiogram data as well as administer an untimely shock. Securing all IMD communication is therefore a very important requirement in IMD design.

There is a growing interest in security issues pertaining to medical information such as data collection, data transfer and processing, and electronic medical health records [12], [17], [33]. However, information security for health-care systems cannot be understood by focusing solely upon the components that comprise the system. Interaction between the components can be more critical than the components themselves [32]. This is the primary reason for studying communication security issues pertaining to interoperability in medical devices. The rest of this article focuses on describing IMD architectures, potential communication security issues in such architectures, and what it takes to secure them. Note that this discussion focuses purely on security issues in IMDs and does not imply Food and Drug Administration (FDA) endorsement of these technologies.

The Health Insurance Portability and Accountability Act mandates that all personally identifiable health information be protected.

The Medical Device Interoperability Environment

Consensus requirements for IMDs are yet to be established. To reason about its security properties, therefore, we need to consider several architectural and operational scenarios. This section explores some of the important characteristics of IMDs, including a functional architecture, communication protocol, operational architecture, operational assumptions, and security requirements.

Medical Device Interoperability Environment Functional Architecture

In Figure 1, we depict a functional architecture for IMDs called the medical device interoperability environment (MDIE). The MDIE consists of a patient-centric network of medical devices, an MDIE network interface (MNI), an MDIE manager (MM), and a caregiver. The MNI is used to collect data from the various devices in the MDIE. It provides an interface to which the medical devices in the MDIE connect. Data collected by the MNI is sent to the MM. The MM is responsible for enabling interoperability between the devices. It is used to receive data from the various medical devices in the MDIE, process these data, and initiate action from the medical devices within the MDIE. For example, the MM can receive data from a glucose monitor,

process the data to analyze the level of blood sugar in the patient, and ask the infusion pump to administer a particular dose of insulin to the patient—thus establishing interoperability between the blood sugar monitor and the infusion pump. Table 1 provides a list of abbreviations that are used throughout this article.

The MM can also facilitate other aspects of interoperability, such as safety interlocks, context awareness, and alarm generation within the MDIE. The MM also provides caregivers with an interface that allows them to specify requirements for individual devices in the MDIE. Additionally, the MDIE has the ability to record system data in a system data logger/flight recorder for system maintenance and forensic analysis. We further assume that the devices communicate with the MNI using a wireless interface. The MDIE functional architecture introduces components such as MNI and MM, because the devices available today do not (generally) have the ability to interact with one another and lack standards in this regard. The MNI and MM can be thought of as providing required middleware support to make medical devices interoperate. Architectures depicted in this article suggest a type of centralized control process via the MM. This notion is used merely to simplify discussing security considerations. Many other control processes are possible, and perhaps ultimately more appropriate for meeting interoperability requirements.

TABLE 1. LIST OF ABBREVIATIONS AND DEFINITIONS.

Abbreviation	Full Form	Definition
IMD	Interoperable medical devices	Medical devices that interoperate
MDIE	Medical device interoperability environment	Patient-centric system, setup for enabling medical devices to interoperate
MNI	MDIE network interface	Constituent element of MDIE that provides an interface for communicating with various medical devices
MM	MDIE manager	Constituent element of an MDIE that provides the intelligence to manage the interaction between various medical devices

MDIE Communication Protocol

Interdevice communication in the MDIE is facilitated through a number of interactions between the different components. As there are no standards for IMD communication as yet, we assume a protocol (shown in Figure 1) consisting of the following sequence of events:

- *Handshake:* Each device in the MDIE connects to the MNI and exports its application programming interfaces (APIs) to inform the MM about its capabilities. For example, an infusion pump may inform the MM that the function call `start()` turns it on, `dosage(drug, volume)` specifies the volume per dosage of a particular drug, and so on. The APIs thus received are maintained by the MM.
- *Specification:* A caregiver specifies operational parameters (data collection rates and alarm conditions) for the medical devices in the MDIE through the MM using equipment such as a personal computer (PC) or a handheld device.
- *Programming:* The MM then programs each of the devices in the MDIE with the caregiver's specifications by sending appropriate commands (using the APIs exported during the handshake) through the MNI.
- *Operation:* Once the devices have been programmed, they can perform their respective tasks. The monitoring devices forward their data to the MM through the MNI. The MM stores the raw data in a data logger/flight recorder, analyzes the data received, and controls any actuation by sending a command to the appropriate device. It may also provide data visualization by sending the data to a patient monitor. If any of the vitals go beyond predefined limits (as provided in the specification stage), an alarm is generated by the MM (the MDIE may even have a dedicated device for alarms). The activities of the MDIE can be viewed and controlled by caregivers by connecting to the MM, either directly or over the health-care network. All activities carried out by the MM are stored in the data logger/flight recorder for design improvement, maintenance, and forensic analysis purposes.
- *Disconnection:* If the MDIE needs to be deconfigured (e.g., when the patient is moved to another location or discharged), the MM sends a command (through the MNI) to disconnect each of the devices connected to it.

Health-care providers have been seeking means and methods of aggregating patient data to improve the quality of health care.

Since an MDIE enables the implementation of IMDs, we use the two terms interchangeably.

MDIE Operational Architecture

To evaluate the security issues associated with IMDs based on the MDIE system model, certain assumptions have to be made about how the MDIE functional architecture is implemented. We base our choice of the architecture for MDIE upon the principal requirement of ease of implementation and deployment. There are three prominent architectural choices for implementing the MDIE depicted (for a three-patient scenario) in Figure 2, which are described later:

- *Centralized*: In this architecture, each care-facility ward has a common interoperability box (IBOX), which contains the necessary interfaces and logic for implementing the MNI, data logger/flight recorder, and MM. All devices in the ward (attached to the patients) are connected to the IBOX. Caregivers connect to it using a care-facility network. This is the simplest architecture to implement; however, it is inefficient given the common IBOX for the whole ward. Further, the common IBOX creates a single point of failure whose malfunction will affect interoperability for all patients in the ward.

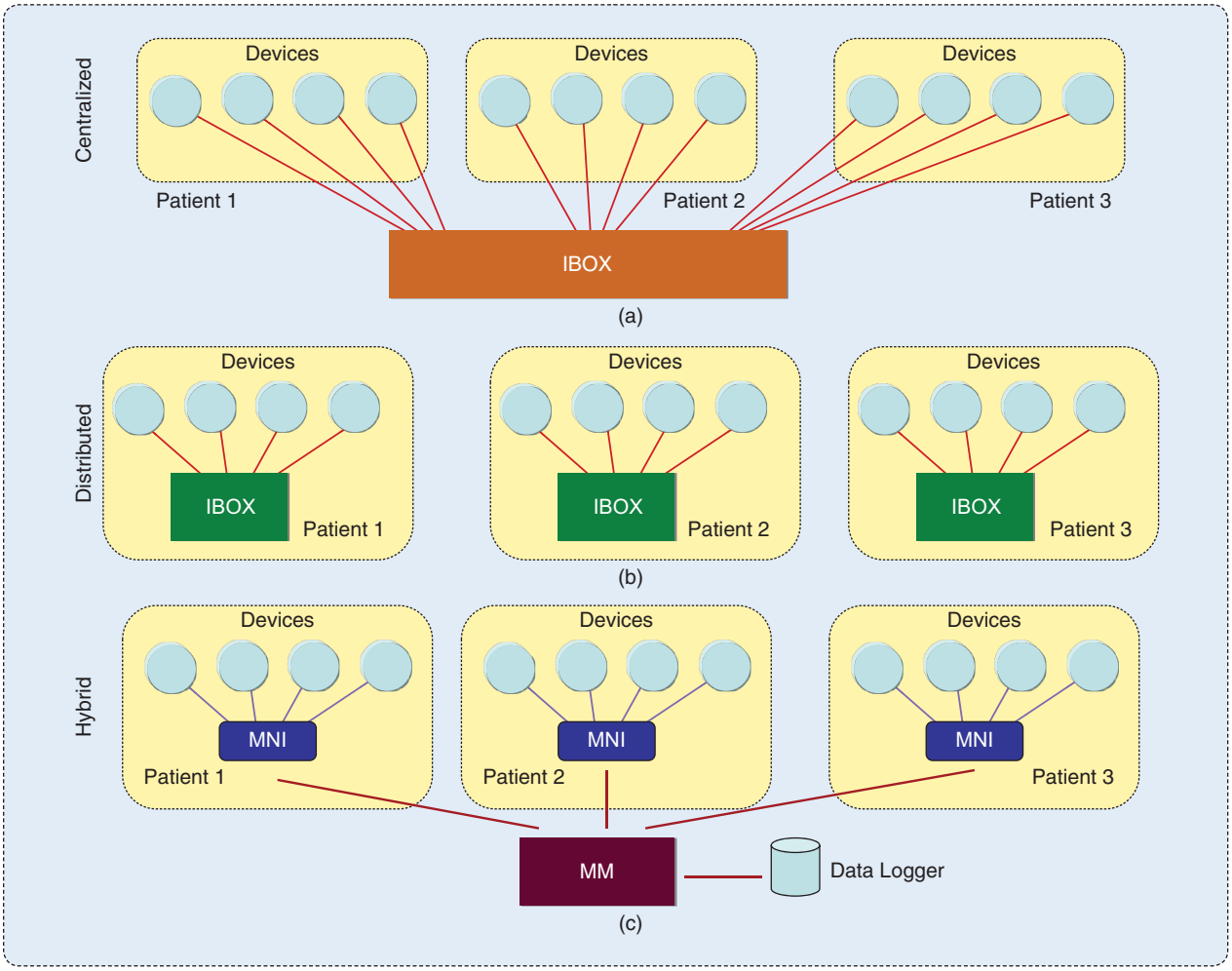

FIGURE 2 Common operational architectures for MDIE, implemented as a part of a multipatient care facility. (a) The centralized case has a common MNI and MM for all patients implemented as part of a common IBOX. (b) The distributed case provides an MNI and MM for each patient as a part of a personal IBOX. (c) The hybrid case provides a personalized MNI for each patient while providing a common MM.

- *Distributed*: This architecture consists of a star-like setup for the MDIE. Each patient has an IBOX that contains the necessary interfaces and logic for implementing the MNI, data logger, and MM. All medical devices attached to the patient connect to this IBOX to perform the handshake and send their data during operation. Caregivers connect to the IBOX to access the devices to provide specifications and obtain patient data. A possible implementation of this architecture is to integrate an IBOX as a part of the patient's bed. The IBOX can be given a unique IP address to allow other caregivers to connect to it using the care-facility network, while all medical devices which are in proximity to it can connect to it directly using a Bluetooth-like low-power short-distance communication technology.
- *Hybrid*: The hybrid architecture combines features of the centralized and distributed architecture schemes. One implementation could be to have one MM and data logger/flight recorder for the entire care-facility ward, with each bed having only an MNI. The devices would connect to the MNI which in turn connects to the MM and forwards commands and data between the two entities. The caregiver would connect to the MM through the care-facility network to provide specifications as well as access patient data and their devices. The advantages of this architecture is that it may require less resources at each bed; however, the amount of communication infrastructure required would be high, given that all MNIs have to connect to the common MM. Further, as in the centralized case, this architecture also suffers from single-point failure issues.

Medical devices are essential for performing modern-day clinical functions.

This is not intended to be an exhaustive list of operational architecture for studying the security concerns of MDIE but just the most common ones. For example, architectural models with each medical device having a local MM and MNI forming a mesh network on the patient are also possible.

Attack Vectors for IMD Communication

Although IMDs are prone to variety of attack vectors, in this article, we focus solely on the communication related ones. In the MDIE model described in the "The Medical Device

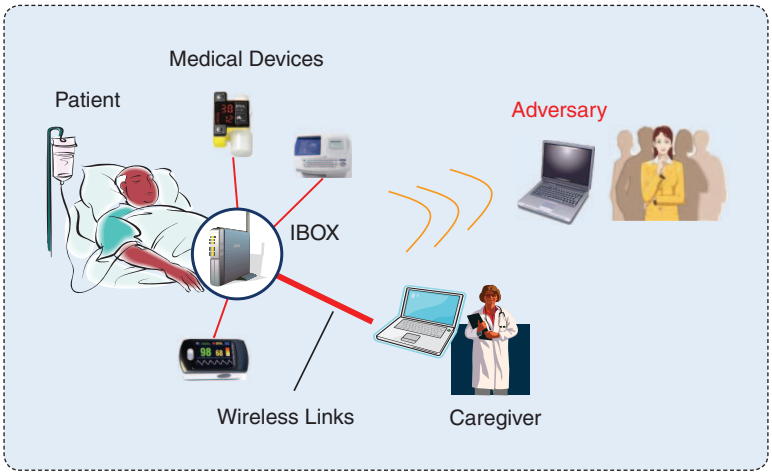

FIGURE 3 Eavesdropping classes of attacks on unsecured MDIE-based interoperating medical devices.

Interoperability Environment" section, each of the five interdevice communication processes (MDIE protocols) is susceptible to attacks from malicious entities. Such attacks can include viewing or altering sensitive patient data, issuing unauthorized commands, and mounting denial of service (DoS) attacks. This section presents the MDIE system model, a model for the attackers, and enumerates some of the security breaches that are possible at each of the five phases of MDIE communication protocol.

System Model

Although we motivated this work with a futuristic example with wearable medical devices, in this article, we consider a hospital-based nonambulatory scenario, without any loss of generality. We assume that a patient is connected to a cart consisting of a set of medical devices. Individual medical devices in the cart have limited communication and control capabilities. To enable interoperability between these different devices, an IBOX is configured as a part of each patient cart. The IBOX comprised the MNI, the MM, and the data logger/flight recorder (we assume the use of the distributed architecture for MDIE here. This decision was made owing to the better reliability and scalability provided by the distributed architecture. Despite the focus on the distributed architecture, the security issues enumerated below apply to the other two architectures as well because of their use of a wireless communication interface). It has the capability to understand each of the medical devices' properties and configurations, to make informed decisions about the data they collect, and to monitor device operation (change in medications, alarms). An IBOX interface permits caregivers to control all of the medical devices on the patient cart. We assume that the IBOX and the equipment used by the caregivers to interface with the IBOX [laptop, PC, or personal digital assistant (PDA)] have the appropriate computation, memory, and communication capabilities. All the devices in the MDIE are assumed to be wireless in nature. Each care facility is assumed to have an administrator who is trusted and is responsible for managing the IBOXs in it.

Unauthorized access to anyone's medical data is a very serious privacy violation.

Threat Model

The broadcast nature of the wireless medium used for communication makes the MDIE vulnerable to many threats. We assume that threats can originate from two sources: active and passive attackers. Active attackers have the capability to eavesdrop on all traffic within the MDIE, inject messages, replay old messages, spoof, and compromise medical devices to become part of the MDIE. Such a compromise can involve modifying legitimate medical devices to behave maliciously or replace a legitimate medical device with a malicious version. Active attackers, if successful, can not only invade a patient's privacy but can also suppress legitimate data or insert bogus data into the network leading to unwanted actions (drug delivery) or prevent legitimate actions (notifying doctor in case of an emergency). On the other hand, passive attackers are attackers who eavesdrop on the messages exchanged during medical device interoperation and use off-line cryptanalytic attacks to access confidential data being communicated (invading a patient's privacy). This type of attack does not try to interfere with the interoperability of the medical devices.

Attack Classes

Some of the main classes of attacks for such a system setup include:

- *Eavesdropping and Traffic Analysis*: The attacker (both passive and active) can overhear (e.g., using a hand-held device) the communication taking place between the devices and the IBOX. This eavesdropping can allow an attacker to learn about the devices connected to the patient, the capabilities of the device through the model type communicated during the handshaking process, instructions given to the IBOX by the caregiver (specification), the settings to which individual devices are programmed (programming), and patient health information (operation). Using this information, an attacker can infer detailed information about the current status of the patient's ailments and track the patient throughout the

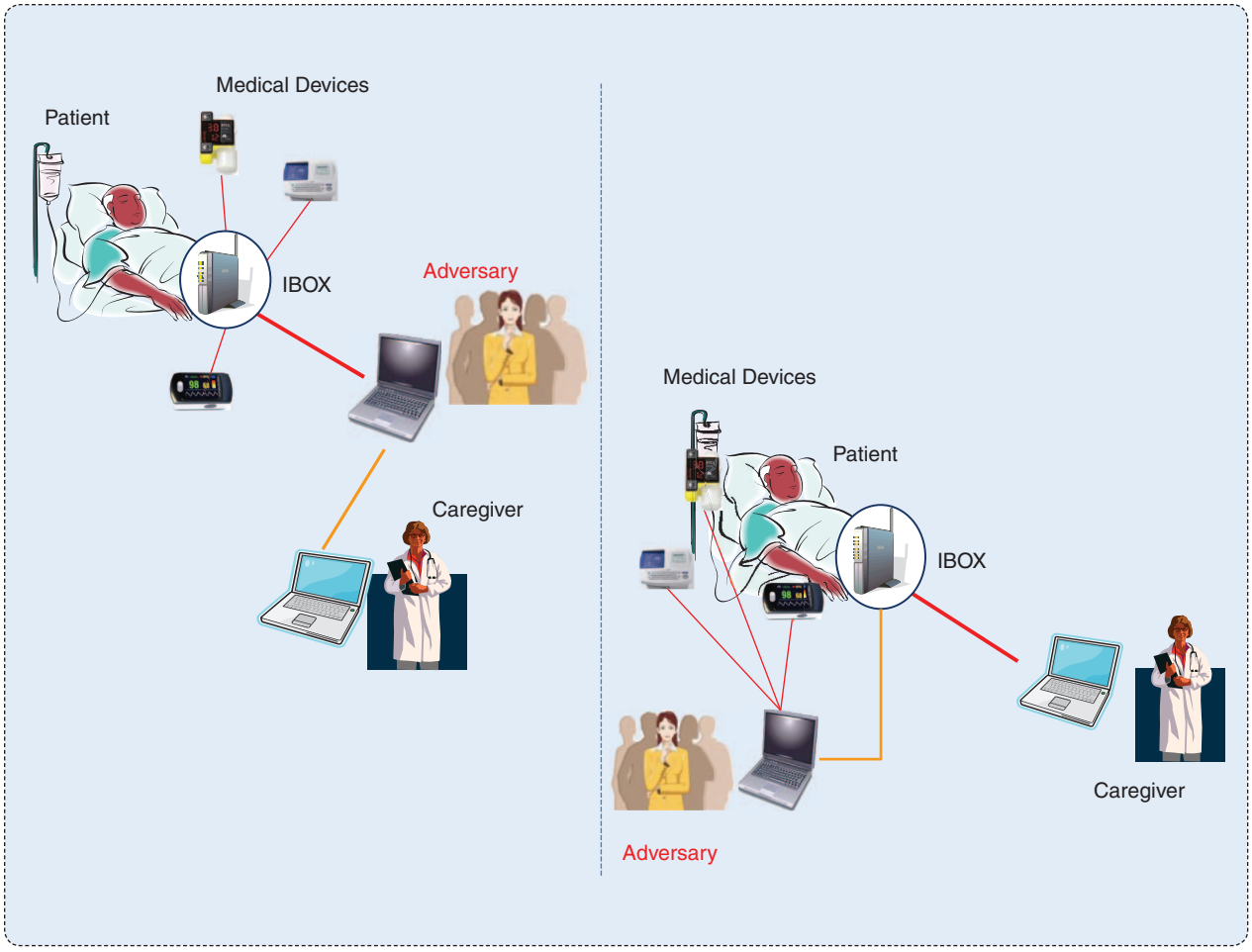

FIGURE 4 MIM class of attacks on unsecured MDIE-based interoperating medical devices.

care facility, including discharge (disconnection), without even approaching the patient. Figure 3 shows an attacker eavesdropping on the wireless communication between the devices and the IBOX and the IBOX and the caregiver.

- *Man-in-the-Middle*: An (active) attacker can mount man-in-the-middle (MIM) attacks by inserting itself between a device and the IBOX or the IBOX and caregiver and passing data between them, making them believe that they are communicating directly. For example, in a wireless environment, such an attack can be mounted by jamming the signal from the IBOX while providing a clear signal to the medical devices on another channel [11]. This allows an attacker to access patient data in an unauthorized manner, know the status of the patient's health, and manipulate any data being sent to the IBOX or caregiver (operation). It also enables attackers to manipulate commands issued by the caregiver (specification) or IBOX (programming) through message insertion and modification that can result in the wrong diagnosis, treatment, and device actuation. Figure 4 shows two places where MIM can be mounted in the MDIE architecture, i.e., between devices and IBOX and the IBOX and the caregiver. An important consequence of MIM attack vectors described earlier is that they can be easily extended to mount DoS attacks on the medical devices. For example, the attacker between the medical devices and the IBOX can easily exhaust the medical devices by simply discarding the patient health information they provide (during operation), leading to continuous repeated retransmissions, or by ensuring that the disconnection command issued by the IBOX is never sent to the medical devices forcing them to be in operation longer than required.
- *Spoofing*: A more generic version of the MIM attack involves an active attacker posing as a legitimate entity (caregiver, IBOX, or device) and taking part in the patient-to-cart operation. This attack does not require the attacker to be in between any two entities and is therefore relatively easier to mount. Another important difference between MIM and spoofing is that an attacker performing spoofing for the first time may not have any information about the protocol used between the device and the IBOX and has to learn these protocols. The most common technique used while spoofing is a replay attack. Replaying an old message exchanged between two legitimate entities can easily fool the receiver into believing the legitimacy of the attacker. Once the connection is established, the attacker can have unauthorized access to the patient data and corrupts data as well as commands. The attacker can

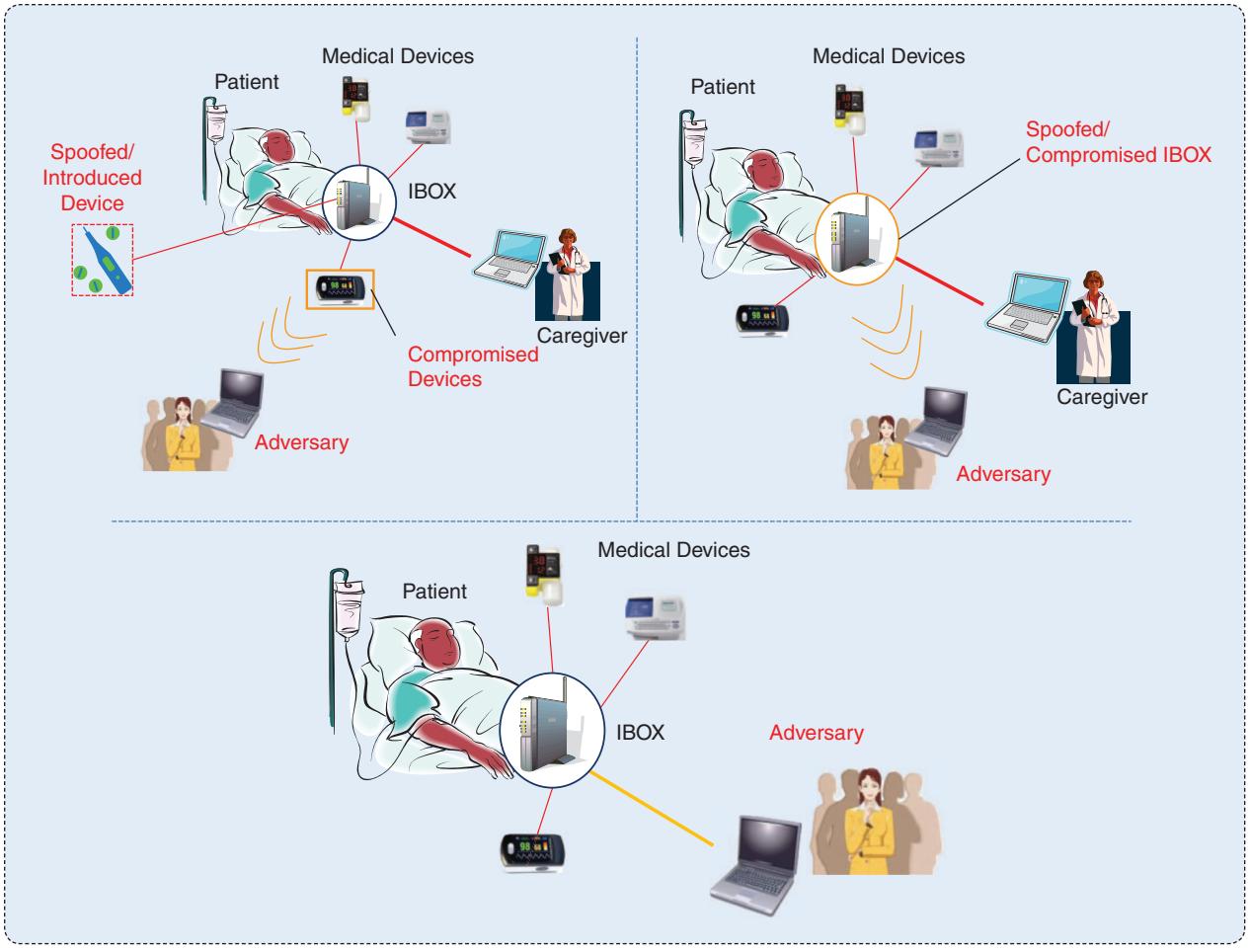

FIGURE 5 Spoofing/physical compromise class of attacks on unsecured MDIE-based interoperating medical devices.

then form sinkholes [25] by pretending to be an IBOX, try to associate itself with devices belonging to multiple patients, or try to associate itself with MDIEs of one of more patients. As in the case of MIM, most of these attack vectors can be easily modified to mount DoS. Figure 5 shows attackers spoofing the identities of all the main players in the MDIE architecture—the medical devices, the IBOX, and the caregiver.

- *Physical Attacks*: One of the most potent forms of attack possible, a physical attack, may involve modifying the functions of the devices and/or IBOX, introducing a new device into the patient cart configuration, replacing existing devices and/or IBOX with malicious versions, and modifying the data and activity logs in the IBOX making nonrepudiation difficult. Each of these attack vectors allows the attacker to become a part of the patient monitoring infrastructure and engage in misinformation and DoS without even being detected. Figure 5 is also used to represent these physical attacks. This is because, in terms of representation, physical attacks are similar to spoofing attacks—except instead of malicious devices pretending to be legitimate ones, the legitimate devices are compromised.

Proposed Approaches

The security attacks presented earlier are possible because entities in the MDIE implicitly assume that any message received is from a legitimate entity within the MDIE itself. This assumption is problematic, because it allows an attacker to eavesdrop and potentially manipulate information by posing as a legitimate entity.

Maintaining security for IMDs is not very different from traditional systems and depends on the maintenance of four basic properties:

1) *Data Integrity*: All information generated and exchanged during the interoperation of the medical devices is accurate and complete without any alterations.

2) *Data Confidentiality*: All information generated during the use of medical devices is only disclosed to those who are authorized to see it.

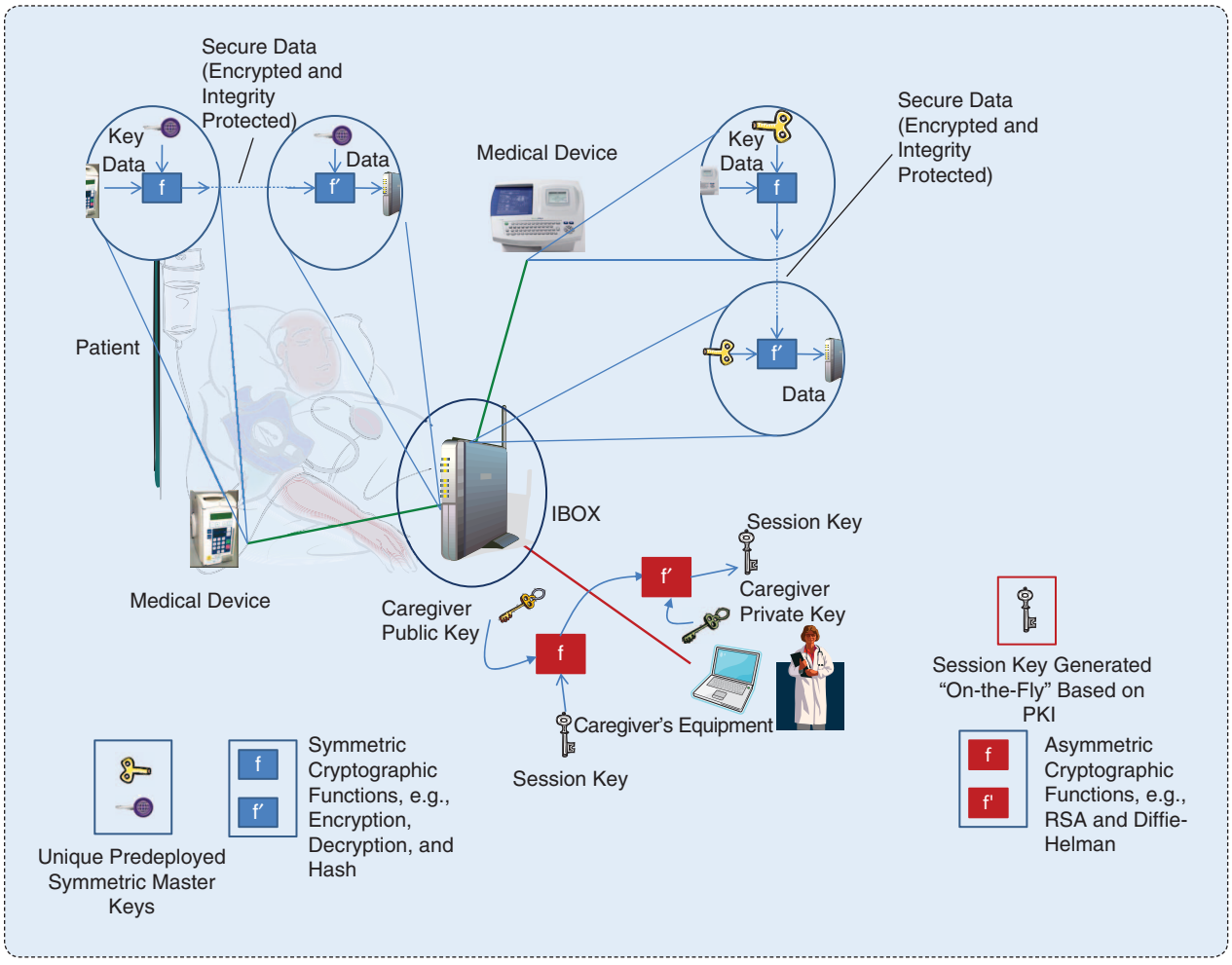

FIGURE 6 Secure channel establishment for MDIE-based interoperating medical devices.

3) *Authentication*: All devices involved in the interoperability process know about all other entities with whom they are interacting.
4) *Physical/Administrative Security*: All medical devices and associated equipment used by caregivers and others should be protected from tampering. Further, work flow of the organization should allow only authorized physical access to equipment.

Based on the threat descriptions in the earlier section, we present a broad overview of communication security approaches for mitigating them by satisfying the four security properties. The approaches can be divided into three parts—secure channel establishment, physical security, and access control.

As IMDs collect and exchange personal health data, assuring security for these devices becomes very important.

Secure Channel Establishment

Secure channel establishment essentially deals with establishing a secure channel between the entities in MDIE by distributing cryptographic keys between them. The presence of such a channel prevents: 1) eavesdropping and traffic analysis by providing confidentiality (encryption) and 2) MIM or spoofing attacks through a combination of confidentiality, data integrity (message authentication codes), and transaction freshness (nonce or monotonically increasing counters).

Specifically, a secure channel has to be established between the medical devices in the MDIE and the IBOX and the communication between the IBOX and caregivers. We make this distinction between the two types of communication because the security solutions for each may be different. Medical devices, being simple entities, may have limited computing resources compared with the IBOX and the caregiver (i.e., the equipment they use to access the MDIE). Thus, the solutions for the device-to-IBOX security pairing may need to be less computational and less communication and memory-intensive than the IBOX-to-caregiver security pairing. Much work has been done with regard to cryptographic security solutions for securing wireless communication, and these solutions can be easily adapted to this environment (see Figure 6 that illustrates the basic idea).

1) *Device–IBOX Communication:* One way for establishing secure channel between the medical device and the IBOX is to establish a unique pair-wise symmetric master key between them. The master key can then be used to establish a secure

(confidential and integrity protected) communication channel between the entities and thwart the attacks presented in the earlier section. Several existing solutions [31], [40] provide simple but secure communication between two entities with limited resources that can be adapted to work here. However, an important question that needs to be answered is how the master key is deployed. For communication between devices and the IBOX, the master key can be predeployed by the administrator when the device is added to the patient-cart configuration. Some of the techniques that can be used for this purpose include: Faraday cages [26], side-channels [34], and features derived from physiological signals [5], [36]–[38]. During the handshake phase, the device and IBOX can verify the presence of the master key with each other and use it for secure communication during all the other phases of operation.

Securing all IMD communication is a very important requirement in IMD design.

2) *IBOX–Caregiver Communication:* For communication between the IBOX and the caregivers, a session key can be established in an authenticated manner using asymmetric key cryptographic techniques such as public key infrastructure (PKI). Here, instead of predeploying symmetric keys, a public/private key pair and a protocol such as Rivest-Shami Adleman (RSA) or Diffie-Hellman (and its variants) can be used to distribute the keys [29]. Using asymmetric key cryptography allows easy authentication (e.g., with PKI using digital certificates signed by a certification authority within the hospital) and more flexibility by changing the session key on-the-fly. This is ideal for interactions between the IBOX and the caregivers that are ephemeral in nature unlike device–IBOX associations that might last a long time.

Physical Security

Secure channel establishment is not always sufficient. As mentioned in the "Attack Vectors for IMD Communication" section, unauthorized compromise to entities in the MDIE can compromise security of the system as well. Physical security can be achieved in one of the two ways: controlling physical access to areas around the patient and tamper proofing. Controlling physical access is the simplest way to ensure that physical security is maintained. However, this may not always be possible. Tamper-proofing techniques could include the placement of seals on individual devices, IBOX, and caregiver equipment. If a tamper-proofed entity is compromised without authorization, it could be prohibited from communicating with other entities in the MDIE and a suitable warning message issued. A combination of these techniques may need to be used to ensure that the physical security of entities in the MDIE is maintained.

Access Control

An additional level of security can be provided by building authorization primitives based on access control constructs for the IBOX-to-caregiver pairing. A prominent example of an access control construct is role-based access control (RBAC) [16]. RBAC executing on the IBOX can specify what privileges (with respect to patient data and device access) caregivers may have when they connect to the IBOX. If needed, the access control model can be allowed to dynamically vary the privileges of caregivers to enable appropriate delivery of health care in the event of emergencies, as in [18] and [39].

It should be noted that the attack vectors discussed in the earlier section are generally well known and can threaten any communication link between devices, wireless in particular. Therefore, they are equally applicable for the centralized and hybrid architectures. As a result, the solutions proposed in this section can be used as a guideline for securing these architectures as well. Further, each deployment of IMD may require its own custom, situation-dependent solutions.

Larger Picture

In the earlier sections, we focused solely on the communication aspect of IMD security. However, IMDs have additional aspects that need security consideration as well. Further, any solution developed needs to be evaluated to ensure that it is functioning as expected. In this section, we list all the principal security requirements for MDIE and also present a set of evaluation metrics for MDIE.

Security Requirements

Building MDIE requires the satisfaction of the following seven principal security requirements:

- *Data Access Security*: This protects against unauthorized access to data/logs collected by devices and IBOX with or without physical compromise.
- *Code Execution Security:* This protects against unauthorized changes to device function, i.e., programming devices with code that forces them to perform malicious or unauthorized tasks.
- *Device Association Security:* This protects against integration of malicious devices into the MDIE.
- *Device Presence Privacy:* This protects information establishing the association between devices and patients.
- *Physical Security:* This protects the physical integrity of IBOX, medical devices, and caregiver equipment. This may also include protecting against jamming and electromagnetic interference, presence of administrative security measures such as specifically designed work flows (e.g., measures to deter writing passwords on post-its or leaving sessions open), and user awareness programs.
- *Accountability and Nonrepudiation:* This ensures that all activities within the system are recorded, in a manner that their validity cannot be refuted or repudiated, for accountability reasons.
- *Secure Information Exchange:* This protects the confidentiality and integrity of messages exchanged during each of the five phases of MDIE communication protocol (outlined in the "The Medical Device Interoperability Environment: MDIE Communication Protocol" section).

Evaluation Metrics

It is important to evaluate whether security solutions for MDIE meet the aforementioned requirements. In this regard, we have identified the following four evaluation metrics:

- *Correctness*: We have to be able to formally verify whether the solutions proposed meet the requirements or not [6]. Formal approaches such as [7], [9], [13], [15], and [27] could be used here.
- *Usability*: We have to ensure that security protocols do not adversely affect the basic function of health-care practices. Studying the usability of secure medical device interoperability is very essential to its eventual adoption in the medical domain. Traditionally, usability has been studied in both medical and nonmedical environments from an accessibility and safety perspective [8], [21], [22]. The methodologies proposed in these studies need to be extended to incorporate security as well.
- *Safety*: Safety has always been a primary concern for medical devices. As wireless technology is embraced by the health-care industry, security decisions will become a greater concern in the context of safety. Issues of particular concern include the consequences of security failure and interference in device operation. Fortunately, formal modeling techniques that are used for evaluating medical device safety such as [10], [23], and [24] can be extended to address security requirements as well.
- *Efficiency*: Security always adds an overhead to a system. In an ideal world, there is no need for security, and this overhead can be eliminated. In the real-world, one needs to be able to provide security while minimizing the associated overhead. Security solutions that are very expensive are seldom implemented. Therefore, one of the evaluation criteria for security solutions has to be the cost of a security solution on the device in terms of energy efficiency, additional computation, memory, and communication requirements. Care should be taken that the overhead imposed by security solutions does not affect MDIE performance. An interesting metric here might be a measure of security overhead on device availability and performance.

Regulatory Aspect

As health-care technology evolves to include more sophisticated communication interfaces and with device interoperability on the horizon, federal regulators such as the FDA face new challenges. There are several approaches being considered to enable IMDs' security. For instance, manufacturers may need to provide the user with appropriate device interface information and information to adequately configure communication systems with regard to managing security issues. Further, it could be the user's responsibility to address physical security issues, such as device tampering. The FDA has issued a cyber security guidance document that addresses some of the security issues raised in this article [2]. Work is also being done to look at security from a medical device safety and risk management perspective. The draft International Electrotechnical Commission (IEC) 80001 standard (http://www.iec.ch) on risk management includes security considerations but again from a security administration and software design perspective. Communication security in medical devices, however, has not been formally addressed to date.

Conclusions

Medical device capabilities are increasing at a rapid pace, but they are still operating in a relatively isolated manner. In recent years, much effort has been spent in promoting interoperability between medical devices [3]. Although these efforts look at many aspects of enabling interoperability, one of the aspects conspicuously missing is securing the communication exchange between the devices. Security is very important with respect to device interoperation. Its properties and requirements need to be carefully considered as interoperability standards are established. By looking at security issues early in the evolutionary process, we can help ensure that the issue is considered as an integral part of designing IMDs.

Acknowledgments

This work was done when the primary author was volunteering at the FDA. The work is partly funded by NSF grant CNS-0617671.

K.K. Venkatasubramanian *(vkris@cis.upenn.edu) is currently with the Department of Computer and Information Science, University of Pennsylvania, Philadelphia. This work was done when this author was with the IMPACT Lab at Arizona State University, Tempe.*

S.K.S. Gupta *(sandeep.gupta@asu.edu) is a professor and the director of IMPACT Lab, School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe.*

R.P. Jetley *(raoul.jetley@fda.hhs.gov) is with the Division of Electrical and Software Engineering, Center for Devices and Radiological Health, Food and Drug Administration, Silver Spring, Maryland.*

P.L. Jones *(paull.jones@fda.hhs.gov) is with the Division of Electrical and Software Engineering, Center for Devices and Radiological Health, Food and Drug Administration, Silver Spring, Maryland.*

References

[1] BodyMedia [Online]. Available: http://www.bodymedia.com/

[2] Cybersecurity for networked medical devices containing off-the-shelf (OTS) software [Online]. Available: http://www.fda.gov/cdrh/comp/guidance/1553.html

[3] Medical devices "plug-n-play" interoperability program [Online]. Available: http://mdpnp.org/

[4] Medtronics Inc. [Online]. Available: http://www.medtronic.com/your-health/bradycardia/device/

[5] A. Banerjee, K. Venkatasubramanian, and S. K. S. Gupta, "Challenges of implementing cyber-physical security solutions in body area networks," in *Proc. Int. Conf. Body Area Networks (BodyNets 2009)*, Apr. 2009, pp. 1–8.

[6] G. Bella, *Formal Correctness of Security Protocols (Information Security and Cryptography)*. New York: Springer-Verlag, 2007.

[7] G. Bella and E. Riccobene, "A realistic environment for crypto-protocol analyses," in *Proc. 5th Int. Workshop Abstract State Machines*, 1998, pp. 127–138.

[8] S. Braun, "Usability for medical devices," in *Proc. 2005 IEEE Symp. Product Safety Engineering*, Oct. 2005, pp. 16–22.

[9] M. Burrows and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[10] V. Cehlot and E. B. Sloane, "Ensuring patient safety in wireless medical device networks," *Computer*, vol. 39, no. 4, pp. 54–60, Apr. 2006.

[11] Z. Chen, S. Guo, K. Zheng, and Y. Yang, "Modeling of man-in-the-middle attack in the wireless networks," in *Proc. Int. Conf. Wireless Communications, Networking and Mobile Computing, 2007 (WiCom'07)*, Sept. 2007, pp. 2255–2258.

[12] T. Cohen, "Medical and information technologies converge," *IEEE Eng. Med. Biol. Mag.*, vol. 23, no. 3, pp. 59-65, May–June 2004.

[13] R. Corin and A. Saptawijaya, "A logic for constraint-based security protocol analysis," in *Proc. IEEE Symp. Security and Privacy*, May 2006, pp. 155–168.

[14] E. Morris, L. Levine, C. Meyers, D. Plakosh, and P. Place, "Systems of systems interoperability," Carnegie-Mellon Univ., Pittsburgh, PA, CMU/SEI-2004-TR-004 (ESC-TR-2004-004), Apr. 2004.

[15] F. J. T. Fabrega, J. C. Herzog, and J. D. Guttman, "Strand spaces: Why is a security protocol correct?," in *Proc. 17th IEEE Symp. Security and Privacy*, 1998, pp. 1–12.

[16] D. F. Ferraiolo, J. F. Barkley, and R. Chandramouli, "Comparing authorization management cost for identity-based and role-based access control," National Institute of Standards and Technology White Paper, 1999.

[17] S. L. Grimes, "Security: A new clinical engineering paradigm," *IEEE Eng. Med. Biol. Mag.*, vol. 23, no. 4, pp. 80–82, July–Aug. 2004.

[18] S. K. S. Gupta, T. Mukherjee, and K. Venkatasubramanian, "Criticality aware access control model for pervasive applications," in *Proc. 4th IEEE Conf. Pervasive Computing (PerCom)*, Mar. 2006, pp. 257–261.

[19] D. Halperin, T. Heydt-Benjamin, K. Fu, T. Kohno, and W. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, 2008.

[20] P. P. Gunn, A. M. Fremont, M. Bottrell, L. R. Shugarman, J. Galegher, and T. Bikson, "The Health Insurance Portability and Accountability Act privacy rule: A practical guide for researchers," *Med. Care*, vol. 42, no. 4, pp. 321–327.

[21] R. Hubert, "Accessibility and usability guidelines for mobile devices in home health monitoring," *SIGACCESS Access. Comput.*, no. 84, pp. 26–29, Jan. 2006.

[22] J. Zhang, T. R. Johnson, V. L. Patel, D. L. Paigec, and T. Kubose, "Using usability heuristics to evaluate patient safety of medical devices," *J. Biomed. Inform.*, vol. 36, no. 12, pp. 23–30, Feb.–Apr. 2003.

[23] R. Jetley, S. P. Iyer, P. L. Jones, and W. Spees, "A formal approach to pre-market review for medical device software," in *Proc. 30th Annu. Int. Computer Software and Applications Conf. (COMPSAC'06)*, Washington, DC, 2006, pp. 169–177.

[24] R. P. Jetley, P. L. Jones, and P. Anderson, "Static analysis of medical device software using codesonar," in *Proc. 2008 Workshop Static Analysis (SAW'08)*, 2008, pp. 22–29.

[25] C. Karlofand D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. IEEE 38th Int. Conf. Communication*, May 2003, pp. 113–127.

[26] C. Kuo, M. Luk, R. Negi, and A. Perrig, "Message-in-a-bottle: User-friendly and secure key deployment for sensor nodes," in *Proc. ACM Conf. Embedded Networked Sensor System (SenSys'07)*, Oct. 2007, pp. 233–246.

[27] X. Li and Q. Wang, "An improvement of authentication test for security protocol analysis," in *Proc. Int. Conf. Computational Intelligence and Security Workshops 2007 (CISW'07)*, Dec. 2007, pp. 745–748.

[28] K. McCarthy, "NONIN Avant 4000 Bluetooth wireless oximetry: Increased safety and accuracy when administering the six-minute walk test," White Paper, Feb. 2008.

[29] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, Oct. 1996.

[30] D. Panescu, "Emerging technologies [wireless communication systems for implantable medical devices]," *IEEE Eng. Med. Biol. Mag.*, vol. 27, no. 2, pp. 96–101, Mar.–Apr. 2008.

[31] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security protocol for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, Sept. 2002.

[32] C. D. Schou, J. Frost, and W. V. Maconachy, "Information assurance in biomedical informatics systems," *IEEE Eng. Med. Biol. Mag.*, vol. 23, no. 1, pp. 110–118, Jan.–Feb. 2004.

[33] N. L. Sneeand K. A. McCormick, "The case for integrating public health informatics networks," *IEEE Eng. Med. Biol. Mag.*, vol. 23, no. 1, pp. 81–88, Jan.–Feb. 2004.

[34] F. Stajanoand R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proc. 7th Int. Workshop Security Protocols*, 1999, pp. 172–194.

[35] A. Tolkand J. A. Muguria, "The levels of conceptual interoperability model," in *Proc. Simulation Interoperability Workshop*, 2003, pp. 1–10.

[36] K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proc. IEEE Military Communications Conf.*, Nov. 2008, pp. 1–7.

[37] K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inform. Technol. Biomed. (Special Issue on Wireless Health)*, vol. 14, no. 1, pp. 60–68, Jan. 2010.

[38] K. Venkatasubramanian and S. K. S. Gupta, "Physiological value based efficient usable security solutions for body sensor networks," *ACM Trans. Sensor Networks*, vol. 6, no. 4, pp. 1–36, 2010.

[39] K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Caac—An adaptive and proactive access control approach for emergencies for smart infrastructures," *ACM Trans. Autonom. Adaptive Syst. (Special Issue on Adaptive Security)*, to be published.

[40] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sensor Networks*, vol. 2, no. 4, pp. 500–528, Nov. 2006.