IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 26, 2015, accepted January 20, 2016, date of publication January 26, 2016, date of current version March 23, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2521727

Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices

RIHAM ALTAWY AND AMR M. YOUSSEF, (Senior Member, IEEE)
Concordia Institute for Information Systems Engineering, Concordia University, Montréal, QC H4B 1R6, Canada
Corresponding author: A. Youssef (youssef@ciise.concordia.ca)

This work was supported by the Natural Sciences and Engineering Research Council of Canada.

ABSTRACT The new culture of networked systems that offer everywhere accessible services has given rise to various types of security tradeoffs. In fact, with the evolution of physical systems that keep getting integrated with cyber frameworks, cyber threats have far more critical effects as they get reflected on the physical environment. As a result, the issue of security of cyber physical systems requires a special holistic treatment. In this paper, we study the tradeoff between security, safety, and availability in such systems and demonstrate these concepts on implantable medical devices as a case study. We discuss the challenges and constraints associated with securing such systems and focus on the tradeoff between security measures required for blocking unauthorized access to the device and the safety of the patient in emergency situations where such measures must be dropped to allow access. We analyze the up to date proposed solutions and discuss their strengths and limitations.

INDEX TERMS Access control, cyber physical systems, implantable medical devices, security vs. safety.

I. INTRODUCTION

The vast growth of remotely accessible services has made us unconsciously accept security trade-offs. For instance, on daily basis, people share their information with remote supposedly trusted entities because they seek faster responses to their needs. Also, in the back of the average person's mind, the exchanged information is secured against various sources of threats. Nevertheless, such convenience always comes with a price. In other words, there is always a trade-off between security of entities (individuals or states) and another desired essential property. For example, the trade-off between the privacy of individuals and the convenience of storing/accessing information using multiple devices is evident in cloud computing, where one can seemingly trust a company over a local secondary storage with sensitive information. To gain convenience, people are accepting some risk which could have been easily avoided without the use of the cloud. A second example, is the trade-off between state security and privacy where governments claim the authority to monitor the contents of emails, web searches, social networks accounts, and shared files [1]. Despite its ethical controversial nature, this state mass surveillance mechanisms are arguably gaining acceptance as some people justify the compromise of individual privacies by propagandizing the fear of terrorism.

Yet, another example of security trade-offs is when enforcing security measures aimed to shield individuals from possible threats can affect their safety and wellbeing or vice versa [2]. A recent physical example on the case where security was imposed at the expense of individuals safety is the crash of the Germanwings flight 9525 [3]. The crash was allegedly deliberate and caused by the co-pilot when he took advantage of the post 9/11 aircraft security features and locked the door of the cockpit leaving the pilot outside without any means of getting in. Another case where safety procedures contradicted with security is demonstrated in the increased theft incidents of a European luxury car [2]. After an independent investigation launched by the manufacturer, it was discovered that the designers of the car recently installed a new safety feature which enables the doors to unlock if enough pressure is applied on the roof assuming that the car rolled over in an accident. Accordingly, a car thief needs only to jump on the roof of the car and the doors automatically unlock. A safety feature that is meant to facilitate getting out of the car in the case of a catastrophic event, compromised its security by making it easier to break in when there is

no accident. In the sequel, modern cars are equipped with mechanisms that enable the recording of driving habits such as speed, visited locations, dates and timings of car trips [4]. Such mechanisms include wireless technologies which in the case of an accident, relevant information is transmitted to emergency response centers. These *black box* like features are used as safety and insurance measures, and in the same time they can be considered as surveillance mechanisms that severely violate the privacy of the owners of these cars.

Security trade-offs are visible in systems which are composed of subsystems from different domains [5]. Such systems include Cyber Physical Systems (CPSs) [6], [7] which are physical in nature and their operation requires advanced connectivity and computation. Many CPSs are built from a physical systems that were developed before wireless communication and IT capabilities became an essential part of our daily life [6]. Theses physical systems were usually constructed based on their own proprietary components and communication protocols. Due to the separation of such systems from the external networks and Internet technologies, their requirements focused on performance, reliability and safety. Indeed, there was no need for communication security because these systems were not vulnerable to typical cyber threats. In fact, security for these systems concentrated on physically securing access to the local network and the consoles that controlled the systems [5]. Integrating these physical systems with advanced connectivity and computation capabilities exposed them to new spectrum of cyber threats [7], [8]. Moreover, typical defense mechanisms which are meant to thwart cyber threats can sometimes conflict with another essential requirement of the system. Accordingly, regulatory and standardization bodies such as the National Institute of Standards and Technology (NIST), have specific guidelines regarding integrating cyber security features in industrial control systems [5]. Particularly, these guidelines demonstrate the need for innovative solutions and designs that accommodate security solutions with essential requirements of the physical system such as security and safety.

Security solutions adopted in CPSs respond differently when compromised by an attack. In such case when a system fails as a result of an attack, one of the following failure modes [9] can be activated: (i) Fail stop where the system abruptly stops operating and cannot be restarted easily, (ii) Fail safe mode where the system changes its operation and enters a safe mode to avoid any hazardous effects, (iii) Fail loud where the system sounds an alarm in response to unauthorized alteration of its state, and finally (iv) Fail quiet where the system allows unauthorized access to its information without taking any further actions.

CPSs has computation capabilities to sense data from the domain they are embedded in, process it into valuable information, and act on the physical context parameters in response to the inferred information [7]. In particular, these systems can sense vital information such as congestion, speed, energy consumption or medical condition, perform specific evaluations, and accordingly project the desired control or protection over the surrounding physical environment. In the sequel, in each CPS, there is a physical reaction for every cyber action. Such reaction has an impact on the safety of the physical environmental, and given the criticality of CPSs, the potential consequences of cyber security incidents are of paramount importance when compared to similar incidents in computer systems. Additionally, most CPSs have high availability requirements which renders the possibility of adopting various threat thwarting methods insupportable. For instance, patching is a rarely acceptable mechanism in CPSs because these systems usually lack having a prototype to test the patch on [5]. Accordingly, there is no systematic way to predict the effect of the patch on the system and the safety risks of having the system unavailable for some time is much higher than the risks of having an unpatched system.

The tension between security and safety is manifested in Implantable Medical Devices (IMDs) [10] which are an important class of CPSs. IMDs are inserted into the human body to administer therapies related to a chronic medical condition, monitor the state of some body parts, or to provide the functionality of a malfunction organ [10], [11]. As depicted in Figure 1, examples of IMDs include cardiac pacemakers and defibrillator [12]–[14] which cope with cardiac conditions, infusion pumps such as insulin pumps [15], neurostimulators for brain stimulation [16], body area networks which are composed of bio-sensors to trace various biological functions [17]–[19], cochlear implants that provide hearing to those with extreme deafness [20], and gastric simulators which emit electrical pulses to the nerves and smooth muscle of the lower stomach to decrease nausea and vomiting in patients with gastroparesis [21]. These devices are now designed to communicate wirelessly with their respective programming devices using a shared secret key to authenticate the programmer and protect the communicated data [22], [23]. IMDs may also transfer data about the patients

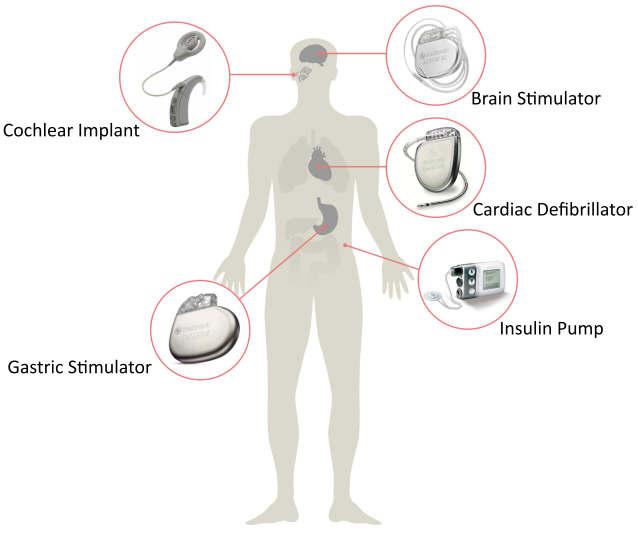

FIGURE 1. Examples for wireless implantable devices.

health and receive information to administer specific therapies. On one hand, the nature of the exchange information makes IMDs critically vulnerable to a wide range of threats that may affect the patient's life [10], [24], [25], and thus the necessity for controlling their access using authentication protocols is absolute. On the other hand, in case of emergency where the patient might be incapacitated, these devices must allow communication with unauthenticated programmers to allow doctors to administer the required treatment which can save the patient's life.

In this survey, we present a tutorial-style introduction to security trade-offs in the context of cyber physical systems. In particular, we investigate the case of implantable medical devices. We discuss the trade-off between securing the device in terms of access rights and the safety of the patient in case of emergency. More precisely, we study how enforcing preset authentication rules in normal situations and enabling on the fly authentication in case of critical situations can be achieved. While other survey results [10], [26] that investigated all security aspects of IMDs, we focus on the analysis of the up to date proposed authentication protocols which address this trade-off and discuss their advantages and limitations. Moreover, we contrast them with respect to the cryptographic and security mechanisms implemented on the implant, and other vulnerabilities and security properties.

The rest of the paper is organized as follows. In the next section, the definition of cyber physical systems is given along with demonstrative examples. In section III, we give an overview of the possible security threats and the challenges involved in securing such systems. Afterwards, in section IV, we investigate the high level non functional requirements of cyber physical systems and demonstrate them in the context of smart grids, IMDs, and drones. In section V, we emphasize on the security trade offs in the context of IMDs as a case study. Primarily, because IMDs have high safety requirements imposed by their critical physical environment where securing the cyber domain of such systems demands a dynamic approach in order to mitigate safety risks. We start by giving and overview on various IMD technologies, communication capabilities and adopted standards. Next, we survey possible attacks and describe the realizable attacks that have been demonstrated in a lab environment. In the sequel, we investigate security research challenges that arise from the critical constrained operation environment of IMDs. To this end, we demonstrate security trade-offs in cyber physical systems by investigation the tension between security and safety in IMDs. We particularly categorize and analyze the security proposals that aim to solve this tension by enforcing access control polices that can be tightened in the normal operation mode and loosened in case of emergency situations. In our analysis, we summarize these proposals and contrast them in terms of their advantages, limitations, and how they address the trade-off between security and safety. Finally, we summarize the main ideas presented in the paper and discuss open problems and future research directions.

II. CYBER PHYSICAL SYSTEMS

Context aware electronic systems that interact with their physical surroundings are known as cyber physical systems [7], [27], [28]. The deployment of such systems has widely increased in the recent years. These systems include smart power grids [29] which are dynamic and interactive infrastructures that combine high speed communication and monitoring technologies with millions of power equipments to provide efficient energy management such as advanced metering [29], and demand and response capabilities [29], [30]. A second example of cyber physical systems are implantable medical devices [10] which are electronic systems embedded in the human body to continuously monitor its health, detect and predict certain conditions, and deliver therapies. Unmanned vehicles [31] are another example of cyber physical systems where they actively interact with the surrounding physical objects to achieve their goals. Such vehicles use cameras and proximity sensors to build a virtual terrains and accordingly can make decisions in terms of speed and direction and ultimately achieve their objective. The common factor between all these examples is their interaction with their physical environment which provides the information required for accomplishing many of their functionalities. CPSs generally use the information acquired from the physical environment, and accordingly they affect the physical environment through their operation. They also rely heavily on information networking infrastructures which makes them a good target to the potential vulnerabilities associated with communications and networking systems [8]. Although the cyber vulnerabilities are similar to those of computer systems, their effect on CPSs may vary according to the nature and criticality of the system. For example, failing to protect the confidentiality of one's email password can lead to revealing her private correspondence and possibly the compromise of other accounts credentials. However, the privacy of the access credentials of a patient's cardiac implantable device is crucial for ensuring the safety of her life especially if the patient is a high value target [32].

III. SECURITY CHALLENGES IN CYBER PHYSICAL SYSTEMS

Due to the entangled relation between physical and computational infrastructures of CPSs, a comprehensive handling of these systems in terms of security is required. More precisely, the complexity, and diversification of both cyber and physical components make the system vulnerable to a variety of security threats and constraints [27], [28]. For instance, damages and operation interruptions of the physical infrastructure of a nation may be caused by bad weather conditions or crises such as wars or terrorist plots which intentionally target these critical infrastructures [33] to harm and disrupt the lives of the general population. Other types of attacks target the communication capabilities of CPSs. A cluster of such attacks may only affect the system passively by intruding and maliciously listening to the communications to steal sensitive information. Other attacks can be more harmful as they aim to bring

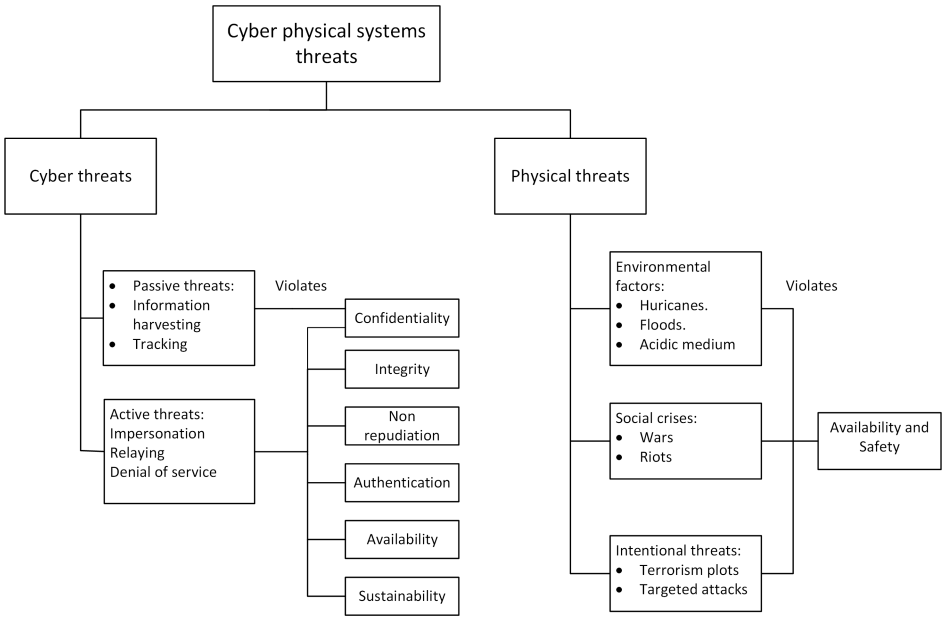

FIGURE 2. Examples of threat sources in CPSs and the properties they violate.

down the IT system by either disrupting the communication altogether, thus halting the activity of the whole system, or by injecting malevolent information with the intention to bypass security policies. The latter type of attacks can be even used to affect the safety of the individuals present in the physical environment of the CPSs through tampering the expected proper interaction between them and the system. Figure 2 depicts some examples for the sources of threats in CPSs and the properties that are violated by them. The continuous monitoring and analysis of data in the system, especially the data required to evaluate the state and the efficiency of the infrastructure, is essential for the evaluation of both its performance and threats [7]. However, in some systems such analysis can only be performed by monitoring the utilization of the system services by its users which raises major issues regarding the violation of their privacies and proprietary information. For example, during the process of efficient power distribution in smart grids, an analysis of the power consumption among residential and industrial areas is performed [29]. This analysis includes classification of the households appliances types and usage timings and average wattage consumption. Though it does not affect the functionality of the infrastructure, such information can be used to determine the valuable contents of a specific property, and to even predict the timings at which it is empty and thus, vulnerable for property theft [29]. Another example is the unmanned vehicles which employ cameras which record the surrounding areas to build terrains for its proper operation [31]. The captured footage can be considered as surveillance material which can be leaked and used against the will of the individuals appearing in this footage [34]. Similarly, in the case of implantable medical devices, information collected by these systems include the device identifier, model, diagnosis, and therapy regimen. Such information, if not handled securely, can be used by malicious adversaries for blackmailing purposes. Although protecting individuals privacy is a major objective of most security policies implemented by CPSs, the mere working of these systems to deliver safe and reliable functionality contradicts such objective.

IV. PROPERTIES OF CYBER PHYSICAL SYSTEMS

Generally, different CPSs operate in various environments to achieve different purposes. However, their operation needs to ensure both cyber and physical securities. From a high level perspective, as depicted in Figure 3, safety, security, and availability are key non functional requirements for the basic working of CPSs [27]. Achieving these three properties in a complex multidisciplinary systems is a challenging objective and requires a careful holistic consideration. Particularly, because of the different nature of the cyber and physical components of the system and the dynamic interaction between the CPS and its physical environment. The continuous alteration of the state of the system given the aggressive diversification of the physical conditions renders optimally achieving the three properties next to impossible [2], [27]. Indeed, there are always trade-offs between one and another and hence, the scope of our survey. As we are aiming to investigate the trade off between security and other properties, in what follows, we describe these properties in details:

- *Safety:* The operation of cyber physical systems relies heavily on their interaction with their dynamic environment and in most cases this environment encompasses or directly affects living beings [27]. Accordingly, the most important requirement for any given CPS is to ensure the safety of the individuals involved in its operation. In other words, CPSs are intelligent context

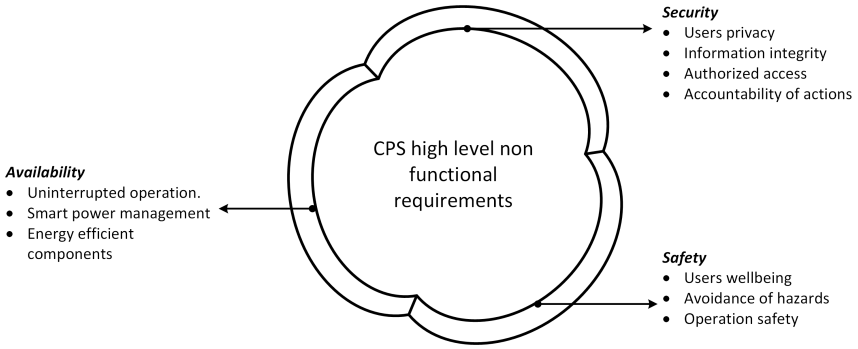

FIGURE 3. High level properties of cyber physical systems.

aware systems [27] that take decisions to influence the state of the surrounding physical and all its constituents. For the safety of concerned individuals, the operation of CPSs should account for all possible scenarios and enumerate the corresponding possible output decisions such that harming living beings is avoided by all means. For example, in smart power grids, there must be mechanisms to ensure that the power is not shut off life sustainable devices and that no over voltage delivery can take place. In unmanned vehicles, incidents which cause malfunctioning of its control and lead to crash and possibly loss of lives should be covered by safety policies.

- *Security:* Both physical and cyber securities should be considered in the comprehensive security framework. In other words, the protection of the physical components of the system from theft, weather conditions, and unauthorized tampering and the confidentiality and integrity of information as well as information access control must be considered. For example, in the case of smart power grids, all the equipment that must be located outdoors should be installed in a weatherproof housing. Also, policies and protocols must be established such that both information and the operational facilities of the system are only accessed with the adequate authorization. Failing to do so may have catastrophic results, especially for those CPSs that are used in critical situations. For instance, an attack on an insulin pump was demonstrated in a lab where a malicious unauthorized adversary took control over it and programmed it to inject an elevated number of insulin units which, if injected in a human body, would directly lead to hypoglycemic coma and possibly death [35], [36]. Confidentiality of sensitive information related to the physical components of CPSs must also be protected. The availability of such information to malicious entities can be exploited in blackmailing acts, discrimination, identity theft, and burglary. For example, the unauthorized acquisition of the footages captured by air drones can be used in stealing sensitive information or for extortion. A main key feature in the security of CPSs is that cyber attacks have a physical impact. Accordingly, computer security solutions that deal with cyber threats only are not enough. There must be a comprehensive approach that considered both the cyber and critical physical processes of the system.
- *Availability:* CPSs are usually used to provide critical functionality, thus it is expected that their operation is available uninterruptedly for a long period of time. Accordingly, implementations of both the cyber and physical components must be coordinated to provide means for such continuous operation. In other words, there should be a reasonable balance between the power/energy required for the computation and that consumed by the actuation especially in resource constrained systems. Indeed, in highly critical systems where downtimes are not acceptable, vulnerabilities patching procedures are avoided as much as possible. This measure is attributed to the fact that patching usually requires rebooting the system. Also, sometimes patches can trigger other actions that may tamper with the system's operation. Because the availability requirements of such systems outweigh the risks of the found vulnerabilities, they remain unpatched [5].

Security trade-offs in CPSs depend on the physical environment of the system, as well as the criticality of its application. In other words, according to the main objectives of the system, operation requirements have a specific priority order. In the sequel, in order to demonstrate the concept of security trade-offs in CPSs, we investigate it in the case of implantable medical devices where the system operation is highly critical as it affects the health and sometimes the life of the patient. Also, the physical environment which is the human tissues is extremely constrained which further limits the options that can be adopted by security solutions.

V. IMPLANTABLE MEDICAL DEVICES

Modern IMDs communicate wirelessly with an external device known as "programmer" to send monitoring data or receive updated therapeutic regimens. Previous generation of IMDs enabled wireless communication with programmers which are at its close proximity within the range of 2m.

In other words, the patient needed to be physically present in the hospital or her treatment facility for her physician to gain access to the IMD. Current IMDs provide advanced computation and communication capability known as telemetry [22] which enables longer range remote wireless access to the IMD usually between 10 to 20 meters. These IMDs have significantly transformed the medical devices industry as they proved to be very useful in monitoring the vital signs of patients, especially the ones with critical conditions. More precisely, a patient can be in her home and the IMD sends the monitored vitals data to an in-house device that communicates the information to the physician. The continuous monitoring helps transfer real time information in the case of life threatening situations which ensures that the patient gets the required medical attention as quickly as possible. In what follows, we briefly describe some of the available communication standards used by different IMDs.

A. TELEMETRY

IMDs are increasingly relying on various networking capabilities for wireless communication. IMDs communicate with external programmers using Radio Frequency (RF) signals utilizing specific frequency spectrum [23]. Telemetry for implantable medical devices is regulated by one or more of the following standards:

- Wireless Medical Telemetry Services (WMTS) specification [22], [37]: This spectrum is a U.S. standard defined by the Federal Communications Commission (FCC). It is used by IMDs withing the United States only as it is not an internationally regulated standard.
- Medical Implant Communication System (MICS) specification [22]: This standard is a radio service that is mainly used for communications between IMDs and programmers. Devices operating using MICS has a small communication range (about 2 meters) and low bandwidth. However, due to the conductive nature of the human body, MICS radio signals can be transmitted between external programmers and IMDs.
- Medical Device Radiocommunications Service (MedRadio) [38]: This standard is a radio band defined to be used by implanted and wearable medical devices. The standard dates back to 1999 but was approved by the FCC in 2009. The communication spectrum of MedRadio is internationally and independently used for IMD communications and it also transmits signals easily through the human body.

B. CYBER ATTACKS ON IMDs

The leisure of providing patients with appreciable autonomy and faster response to their needs comes with the challenge of securing the communicated information as a door to a new source of security and privacy threats for the patient is opened. The majority of such threats [39]–[41] are related to their wireless networking capabilities and similar to the threats available to the different IT systems. In fact, previous in-vitro demonstrations [14], [35], [36], [42] have shown that IMD security is highly compromised and that any adversary with malicious intent can bypass the simple security mechanisms and gain access to this device, which can cause damages ranging from invasion of privacy to the threating the life of the patient with the IMD. In other words, attacks against an IMD can put at risk the safety of the patient who uses it and can be fatal in some scenarios [14], [42]. The deliberate tampering of a critical implant such as cardiac implants or insulin injectors can lead to death as has been demonstrated in the following cases:

- The first case was presented by Halperin *et al* [14] where they demonstrated attacks on an implantable cardioverter defibrillator. In this work, the protocol employed by the implant was reverse engineered and software radio based attacks were used to read the information stored on the IMD and reprogram it to change the prescribed therapy. Moreover, the IMD was made to communicate indefinitely with an unauthenticated external device, thus posing a potential denial of service. The presented attacks were the first to be implemented on a real commercial cardioverter defibrillator and were shocking as they introduced a realizable compromise of the safety and privacy of the patient.
- Another case was demonstrated by Jerome Radcliffe [35] who is a diabetic himself, where utilizing the ID of the device, he took control of his own insulin pump by connecting to it remotely from a distance of 100 feet. Moreover, Radcliffe showed how he can command the pump to inject insulin every three minutes or stop insulin delivery. Afterwards, the attack was improved by Burnaby Jack [36] to enable an adversary to compromise any vulnerable device within 300 feet without the knowledge of its ID. Furthermore, hijacking attacks on insulin pumps have also been investigated by Li *et al.* [15] where utilizing off the shelf software defined radio device, they were able to eavesdrop on the wireless communication and command the devices to alter the prescribed therapy.
- Barnaby Jack demonstrated several ways in which an implantable cardiac devices could be accessed [42]. Additionally, he used a laptop 50 feet away from the IMD to deliver a deadly 830 volt shock.
- Hanna *et al.* presented an attack on a Cardiac Automated External Defibrillator (CAED) [43]. Exploiting the fact that the CAED did not verify the authenticity and freshness of software updates, the attack enabled the successful update of the device by custom firmware. Such update can be used to stop the device from administering life saving electrical pulses or enforce them to deliver shocks of high strength.

Other attacks aim to deplete the battery [44] and render the device useless, thus forcing the patient to undergo an additional surgery to change the implant [12], [45]. Moreover, cardiac implants have a switch that can be turned off by applying a magnetic field at close proximity [46] to protect the implants from electromagnetic fields when the patient

undergoes cardiac surgery using electrocautery devices [47]. This property could be exploited by an attacker and all she has to do is to generate magnetic field and be close to the patient. For that reason, the former U.S. vice president Dick Cheney had his modern implantable cardioverter defibrillator replaced by another one without WiFi capability [32].

IMDs usually adopt security by obscurity [48]. However, the implemented protocols can be sometimes reverse engineered to gain access to the implant [14], [40]. Moreover, the patient with the IMD can be remotely detected and any adversary can listen to insecure communications which enables access to exchanged data. Such data may contain sensitive information such as vital signals, diagnosed conditions, and prescribed therapies [10], [26], [41].

Despite the dangers imposed by cyber attacks, patients seem to be unaware of their effects as they tend to think about the security of their IMDs as a secondary aspect. This fact was investigated by Denning *et al.* [49] where a study with 13 patients with IMDs was carried out. The patients were asked about their understanding of the IMD security and privacy issues and how they feel towards various security mechanisms. Ten patients expressed no concern about an adversary changing their IMD settings without their consent, seven patients were not worried about emergency responders being denied access to their IMDs in the case of an emergency, and only 7 patients agreed that security mechanisms should be adopted to protect future IMDs. Similarly, manufacturers of IMDs often are reluctant to introduce new security mechanisms because of the delay consequences such actions may have on the regulatory approval process [50].

C. CYBER THREATS ON IMDs

A study to investigate how wireless IMDs are protected against information security threats was carried by the U.S. Government Accountability Office (GAO) [51]. In August 2012, the GAO determined that the current threats can indeed affect the security and safety of patients with IMDs and it published a report with a recommendation to the Food and Drug Administration (FDA), urging it to adopt a strategy that focuses on information security risks. In June 2013, the FDA released a safety communication containing guidelines for the industry on the design, testing, and use of wireless medical devices [52]. The released safety communication stressed on the significance of the security of the exchanged wireless information to protect the privacy of the patient, and to prevent unauthorized access to medical devices with built in wireless capabilities. In particular, the FDA communication stated that wireless medical devices must implement cryptographic approaches to protect communications and accesses. The required mechanisms are determined according to the type and probability of expected threats which the device can be vulnerable to, as well as the operating environment and the consequences on the patient in case of a security incident. Generally, IMDs are vulnerable to the following threats:

- ***Information harvesting:*** Recently, the value of electronic personal health information has been rising drastically on the black market. According to a 2012 Healthcare Information and Management Systems Society report, personal health information is more valuable than credit card data [53]. In fact, the value of a patient health record in the black market is estimated to be $50, compared to $3 for a social security number and $1.50 for a credit card. Consequently, if no authentication mechanisms are enforced in IMDs, any adversary may obtain a commercial programmer and command the attacked IMD to illegitimately obtain the private information related to the health of the patient [20], [24], [39]. Alternatively, an eavesdropper can listen to unencrypted communications between IMDs and legitimate programmers. The harvested information can be used to carry out additional attacks.
- ***Tracking the patient:*** A patient with an IMD supporting wireless communication can be easily detected especially when she is in the open [10]. Accordingly, an attacker in possession of a large number of programmers can effectively track the movement of a patient with IMD as long as its communication is covered by the range of the programmers [54]. Although, tracking a person's movement is not harmful by itself and in some cases such as patients with dementia or Alzheimer, it may be a beneficial, it poses a severe violation of privacy.
- ***Impersonation:*** An adversary can impersonate either the IMD or the programmer if the wireless channel is not properly protected [40], [53]. More precisely, the adversary can eavesdrop on legitimate communications and record the IMDs handshake reply to a genuine programmer. Later, when the IMD is interrogated by the programmer, the adversary can replay the recorded messages and convince the programmer that it is talking to the IMD. Such attacks can be used to harvest further information regarding the patient therapies or to feed falsified information to the patient's physician which can delay the response to the needs of the patient and in some cases endanger her life.
- ***Relaying attacks:*** This type of attacks is used to trick the IMD by making it assume that it is taking to a programmer at it close vicinity. More precisely, IMDs using either the telemetric MICS or WMTS bands have limited communication ranges (within 2 meters) [22] which implies that a programmer must be in close proximity to the IMD. However, an attacker can illegitimately convince the IMD that its talking to a programmer within its proximity by adopting a special setting with two devices, called a *ghost* and a *leech* which supports fast long range communication [54]. In this setting, the *ghost* impersonates an IMD to a genuine programmer, and the *leech* pretends to be a programmer to the IMD. In proximity-based authentication protocols [55], the *leach* and *ghost* keep relaying the messages between the IMD and the

programmer to trick the IMD into believing that it is talking to an authorized programmer.

- ***Denial-of-Service (DOS) attacks:*** These attacks aim to tamper with the availability of the IMD to perform its job [54]. DOS attacks can be launched using several approaches, for instance an attacker may try to request power consuming tasks from the IMD, thus leading to a power draining attack [44]. Another method to prevent the IMD from servicing legitimate programmer is to interfere with its communication. Particularly, using a signal jamming device, an adversary can scramble all the responses of the IMD to legitimate requests which renders it meaningless for the requesting programmer [56]. Moreover, by exerting a magnetic field at close proximity to a patient, an IMD with magnetic switch will shut itself off [47].

Addressing the IMD security and privacy issues is a challenging task [54], [57], [58] because of the increased demand for a longer range for the wireless communication which creates new threat models and widens the scope of the existing ones. Another factor is the resource constraints of an IMDs in terms of area required by the processor and memory, and power consumption (i.e., battery). Hence, trade-offs are unavoidable when choosing between various security strategies. Next, we give a brief review on the existing challenges, constraints, and trade-offs in securing IMDs.

D. CHALLENGES AND SECURITY TRADE-OFFS IN IMDs

Although the attacks on the wireless information communication in IMDs are similar to that in computer systems networks which have standard mitigation techniques, adapting the exact protection techniques for IMDs cannot always be feasible. In other words, such techniques must not only be secure in order to be deployable on IMDs, but it must also operate within the constrains imposed by the physical environment. More precisely, there is a number of challenges and constraints in securing IMDs attributed to the operating physical environment that makes protecting it follows a completely different scenario from securing computer networks. In what follows, we cite five challenges (depicted in Figure 4) which face any security solution adopted by IMDs:

1) ***Critical physical environment:*** IMDs are embedded in the human body in direct contact with vital tissues. The casings IMDs are made of biomedical materials such as titanium, silicone, or apatite [59]. Such materials do not react with the surrounding environment and are not affected by the corrosive nature of different bodily fluids. Even though IMDs use biomedical material, there have been reported cases where the patient's body passes through recurrent body rejection episodes which is usually accompanied by inflammation and pain. The volume and weight of the packaged implant device must be small and light so that it does not affect the normal activity of the patient. Adopting a security approach must consider the criticality of the operation environment. In particular, security solutions must consider the safe amount of power dissipation and RF radiation [59]. Since the implant is embedded in the human body usually beneath the skin by 2 to 5 centimeters, it has a limited area and accordingly tiny microprocessor and memory. Accordingly, any set of executed concurrent operations on the device should not cause heat dissipation above certain levels [59]. Also, the increased number of exchanged messages can subject the patient to additional RF radiation. Excessive amounts of power dissipation and RF radiation can lead to damage in the surrounding tissues and may trigger implant induced coagulation and/or allergic foreign body response [59].
2) ***Constrained resources:*** In addition to having a tiny area, IMDs encompass an integrated non rechargeable battery which is supposed to last between 8 to 10 years [60]. Accordingly, power should be manged efficiently by processing and communication elements. These constraints complicate the ability to implement the traditional cryptographic techniques which efficiently satisfy both security and safety. In other words, a typical authentication protocol to control who is granted the right to access the IMD requires multiple executions of a symmetric encryption algorithm, a public key algorithm (usually adopted in key distribution via public key infrastructure), and sometimes a hash function, all of which if implemented, require high processing power which will deplete the battery much sooner than its expected lifetime. Moreover, if the battery is depleted, the whole IMD needs to be replaced via surgery which comes with its associated risks on the patient's health.
3) ***Legacy compatibility:*** Another important challenge is that adopting any new cryptographic solution involves modifying the IMD which means that all the already implanted devices will remain vulnerable to the above mentioned security threats. In fact, there are millions of cardiac implants already in use and about 700,000 are implanted each year [61]. Accordingly, a favorable cryptography-based security solution is the one that can provide an additional mechanism to secure the already implanted IMD as well.
4) ***Bureaucracy:*** The process of adopting a security solution for IMDs is completely inflexible. More precisely, a given security mechanism changes the nature of the IMD and such change must first go through quality and compliance testing by various regulatory bodies. Additionally, in the U.S., it must be approved by the

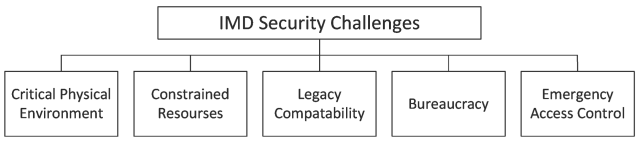

FIGURE 4. Challenges in securing IMDs.

FDA whose process encounters bureaucratic delays that may reach 7 years [50]. During this period, the security system may even become obsolete because of the new emerging generation of IMDs with advanced technologies.

5) ***Emergency authentication:*** The most important challenge, as it directly affects the life of the patients, is how to deal with authentication to access the IMD in case of emergency [40]. More precisely, suppose an incapacitated patient is presented at the emergency room in a hospital different than hers. Health professionals at that hospital should be able access the IMD using their unauthenticated programmers to gain personal and therapy information about the patient. The safety of the patient can be endangered if the IMD implements a rigorous access control protocol that does not consider this scenario. Any acceptable authentication protocol must also provide a way for unauthenticated programmers to communicate with IMDs in the event of an emergency.

The tension between securing the access to IMDs and the safety of patients in the case of emergencies [40], [54], [57] has been addresses in several proposals, each with its own inherent weaknesses. Next, we survey these techniques and discuss their pros and cons.

E. THREAT MODELS

All the surveyed proposals consider attacks by one or more threat model out of the three following adversarial models:

- An adversary with a commercial programmer which is unauthorized by the IMD. These programmers usually contain no mechanism to restrict their use by only health professionals.
- A passive adversary who has the capability to listen to the communications on the RF channel between IMDs and their respective programmers. It is also assumed that she possesses all the necessary equipments to capture, record, and analyze the acquired RF transmissions.
- An active adversary who possesses the abilities of the passive adversary and can generate RF signals to send commands to the IMD, modify messages in transit before they reach the IMD or the programmer, or just block them so that they never arrive to either parties.

All the authentication protocols that authenticate programmers in emergency situations using readings of physiological values assume that the adversary is present during the IMD and programmer authentication. However, the adversary cannot touch the patient and is usually present within 2m for IMDs using MICS and WMTS and up to 10m if using advanced communication capabilities. The proximity assumption is based on the fact that if an attacker is close enough to touch an unconscious patient, then she might as well inflict harmful actions on the patient without going through the technical complications of attacking the IMD. While the proximity assumption is true, an adversary attacking the IMD has the advantages of both the stealthiness and untraceability.

VI. SECURITY VS. SAFETY: A CASE STUDY ON AUTHENTICATION PROTOCOLS IN IMDs

Cryptographic algorithms are the main building blocks in authentication protocols. Since traditional public key cryptography requires considerably high computation and communication capabilities, it is not well suited for the resource constrained environment of IMDs. Hence, the use symmetric ciphers are better option for such requirements. However, IMDs and their authorized programmers must share a private key which is used for authenticating both devices to each other and for encrypting the exchanged information. Generally, symmetric cryptographic schemes suffer from inefficient key distribution mechanisms and the problem gets worse in the case of IMDs because the solutions do not suit the constrained environment.

Authentication protocols in the case IMDs differs completely than that adopted in computer systems [26]. First because of the resource constraints of IMDs do not allow such protocols to operate efficiently. Second because IMDs require access polices of dynamic nature. More precisely, while IMDs must adopt access control policies to mitigate unauthorized access, they should offer a loosely permissive access control policies when life threatening medical events take place. Health care professionals may need to reprogram IMDs or read the patient's information and diagnosis from them. One proposal [62] has suggested that a preset secret key is to be coded in the IMD and used by any programmer to access this particular IMD. Moreover, the key is stored printed on the patient's skin using ultraviolet pigmentation (invisible tattoo) to be read by special programmers equipped with ultraviolet readers. Another solution proposes that the cryptographic key used by the IMD can be stored on an external wearable bracelet. However, both solutions reveal the IMD secret key to all the programmers and their associated personnels which renders it not a secret after a while. In the case of the wearable bracelet, the key is externally present and can be seen or photographed by attackers. Moreover, if the bracelet is lost or stolen, the IMD becomes unaccessible or only accessible by a malicious adversary.

In what follows we survey the IMD authentication proposals that consider authentication in emergency situations. We first categorize them based on the adopted approach and discuss their main advantages and their constraints. The adopted approaches are: (i) Proximity-based techniques [63]–[65] that authorize only programmers which are close to the patient, (ii) Proxy-based approaches [66]–[69] where another device is employed to handle the authentication process, (iii) Biometric-based approaches [70]–[73] which require the biometric features of the patient to grant access to her IMD, and (iv) Hybrid approaches [74], [75] that propose new techniques and integrate them with other approaches to authenticate programmers. The surveyed

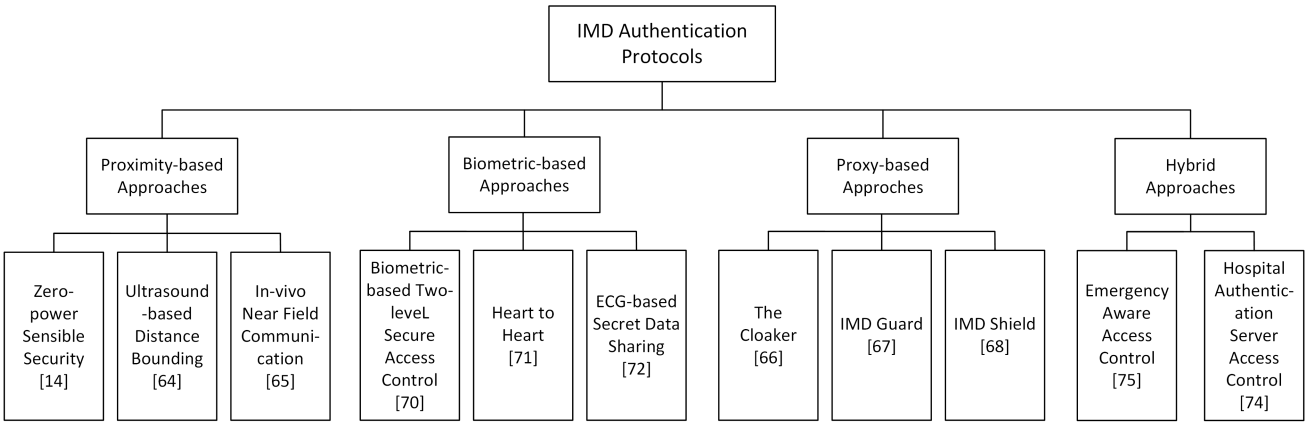

FIGURE 5. Authentication approach categories and their respective protocols.

protocols and the adopted categorization are depicted in Figure 5.

1) PROXIMITY DETECTION APPROACHES

The set of authentication protocols under this category adopts the fact that close proximity [76] and sometimes the concept of *touch-to-access* ensure the awareness and consent of a conscious patient to external authentication attempts [14], [55], [77]. Moreover, in the case of critical situations when the patient is incapacitated, access attempts from programmer devices operated by any emergency responders can always succeed. Mechanisms proposed in [78] have introduces some ideas by which an attacker can hijack the proximity, thus allowing unauthorized authentication.

a: ZERO POWER SENSIBLE SECURITY (ZP SEC)

Halperin *et al.* [14] proposed a set of defenses against unauthorized accesses. Particularly, their approach aimed to mitigate complex cryptographic solutions in order to avoid depleting the battery of the implant. They first presented *zero power* authentication mechanism where a Wireless Identification and Sensing Platform (WISP) and a piezoelectric element circuitry are implanted in the human body. The WISP harvests energy from RF signals generated from programmers, at close proximity of the patient which are trying to connect to the IMD. The harvested energy is used to feed the piezoelectric element so that it emits the secret parameters required to calculate the shared key acoustically such that only programmers with microphones touching the patient can sense these signals. To further enable the detection of unauthorized access attempts, the authors proposed *Zero power* notification where the WISP fails loud [9] by audibly warning the patient of events of cryptographic operations via a combination of auditory and tactile stimulation.

b: STRENGTHS

The main advantage of the *zero-power* scheme is that it is highly aware of the criticality of the context of the physical environment associated with IMDs. More precisely, although the security module is implanted in the human body, it consumes no battery power at all, thus preserving all the available power of the IMD to the more important communication and actuation operations required for the treatment of the patient. All the power needed for both the authentication and notification mechanisms is harvested from the RF signals generated by access attempts from the programmer devices. Another advantage is that the adopted cryptosystem for the key establishments phase is very light. More specifically, this stage requires only a simple four steps challenge-response protocol. Additionally, it is very fast as the embedded security module performs one execution of a symmetric key encryption algorithm only to generate a 128-bit key to be used for encrypting the communication between the IMD and the programmer.

c: WEAKNESSES

A major disadvantage of the *zero-power* authentication scheme is that the authentication module (containing the WISP and the piezoelectric element) must be implanted 1cm beneath the skin so that the released acoustic signals are detectable by the programmer device. This constraint means that the authentication and notification circuitry cannot be incorporated for use with the IMDs that need to be embedded deeper within the human body. Having both the module and the IMD independently implanted in the human body raises the question of how the module can further communicate the established key with the IMD. The scheme also requires that the microphone of the programmer is placed directly above the implanted security module which means that in case that the patient is unconscious, emergency responders will have to find a way to locate it for authentication to take place. A straight forward solution to this problem is to permanently mark (using tattoos) the place of the module on the skin so that it is clearly visible in case of emergencies. However, being permanently visibly marked may not be accepted among patients due to religious or social reasons

(e.g., tattoos may be perceived as a mark of low socioeconomic status or undesirable affiliations) [62]. Additionally, this solution leaves the patients recognizable by adversaries which may later facilitate the ability of being targeted by attackers/blackmailers. Also, the psychological impact on patients from false positive alarms may by itself induce a stress state [10]. An attack by Halevi and Saxena [63] demonstrated that using a general purpose microphone, the secret generated acoustically by the piezo element can be recovered from a distance of 0.9m with success probability of 99.88%.

d: ULTRASOUND-BASED DISTANCE BOUNDING (US-DB)

In this authentication protocol, Rasmussen *et al.* [64] proposed a method to detect the proximity of a programmer device attempting to communicate with the IMD based on the speed of sound. The mechanism adopts the Diffie-Hellman (DH) key agreement protocol [79] to generate the shared private key required for encrypting the communicated information. In this protocol, both the IMD and programmer generate their own partial secret key, known as the DH secret, via modular exponentiation. Then they both exchange their masked DH secrets through two sequential rounds of rapid bit exchanges. In each round, either the IMD or the programmer receives a masked bit from the other party through a radio channel and sends a masked bit of its DH secret contribution utilizing a sound channel. Accordingly, based on the speed of sound and taking into account the expected delays, the receiver can determine the proximity of the other party. At the end of the protocol both the IMD and the programmer have each others secrets and can compute one shared secret key.

e: STRENGTHS

Since the mechanism relies on the speed of sound in determining the proximity of the programmer, it does not require the programmer to touch the skin of the patient which slightly loosens the restriction of the touch-to-access policy. In fact, any programmer, operated by a malicious individual or a legitimate one, can reply via sound signals to the challenges that was sent by the IMD over the radio channel. However, because the speed of sound cannot be altered, only those programmers within the acceptable distance to the patient will be authenticated. A second advantage is that although the protocol adopts a public key scheme that employs modular exponentiation which is a computationally exhaustive task, the IMD executes its part of the algorithm and generates its DH secret only after it determines that the programmer is authenticated (i.e., within close proximity), thus mitigating going through this power consuming operations in the event of an adversary launching a battery draining attack. Unlike the case of [62], the mechanism is not based on specific credentials which could be lost, stolen, or duplicated which renders the implant unaccessible or subjects it to an unauthorized access.

f: WEAKNESSES

It was found that some RF signals could be sent to the IMD and affect the circuitry of the embedded audio receiver by inducing a current in it [64]. More precisely, the protocol measures the distance between the patient and the programmer by detecting the presence of electrical currents in the audio receiver. Accordingly, if an attacker is able to use radio signals from farther distance to induce current in the audio receiver, she will be authenticated by the IMD and authorized to access the device. The solution to such breach is protecting the IMD by an RF shield which further complicates the IMD design. However, if no adequate RF shielding is in place, an attacker with the proper equipment can effectively trick the IMD into assuming it received a sound signal while in fact it received an RF signal.

g: In-vivo NFC

This mechanism is proposed by Kim *et al.* [65] to enable authenticated access to the IMD using Near Field Communication (NFC) enabled smart phones. NFC technology has a communication ranging between 10cm to 1m depending on the type of the adopted NFC standard. Such communication limit suits distance bounding applications such as IMDs. The work in [65] proposes to insert an in-vivo (within the human body) NFC tag in IMDs to communicate with the ex-vivo NFC reader embedded in the patent's smart phone which basically acts as the programmer device. The smart phone in return can relay the information retrieved from the IMD to the appropriate medical personnel via a 3G or a WiFi network. The employed NFC tag adopts NXP proprietary security protocol for authentication and ciphering. This proposal offers no cryptographic solution to the access control problem but rather a system with its own implemented security protocol to enable the IMD to communicate with a specific smart phone within maximum distance of 1m.

h: STRENGTHS

The system adopts two types of NFC tags for the tag in the IMD and the one in the smart phone. Specifically, a passive in-vivo NFC tag is used in the IMD which requires no power from the battery of the implant for its operation and an active NFC tag in the smart phone which provides the power for the in-vivo NFC tag. Such adaptation is very desirable for prolonging the battery life of the IMD. While the heat dissipation by the IMD processing and communication has been a critical issue during their design, mainly because continuous exposure to even slightly elevated temperature can damage the surrounding tissues, operations of the in-vivo NFC tag results in minimum heat dissipation.

i: WEAKNESSES

A major disadvantage of this protocol is the process by which the secret key is shared between the IMD and the patient's smart phone. In particular, the authors assume that a long term predeployed key is shared between the two NFC tags

at the time of the surgical implantation of the IMD. Such key agreement method is limiting as the shared key cannot be changed which makes the protocol arguably unpractical because it raises a huge concern with regards to what happens if the phone is lost, stolen, or even broken. In such cases, the whole protocol becomes useless.

2) PROXY-BASED PROTOCOLS

The set of protocols surveyed under this category employ an external device to mediate the communication between the programmer and the IMD. These external devices implement access control procedures and accordingly are responsible for determining who communicates with the IMD, thus removing the burden of establishing secure communication from the IMD. While approaches that operate under this category offer an active solution to the problem of IMD access in the event of emergency by providing fail open access [9] to the IMD, they suffer from security issues in the case when the proxy device is lost or broken which leaves the IMD with no security protection. Nevertheless, this category is the most desired by medical providers when given the chance to choose between different approaches [80]. Particularly, because of its fail open guaranteed access in the case of emergency.

a: THE Cloaker

In this proposal, Denning *et al.* [66] describe the Cloaker as an externally worn device that protects the security of the IMD as long as it is worn and provides open access when removed. The IMD ignores all access attempt as long as it detects the presence of the clocker. In the case of emergency, emergency responders can remove the Cloaker and the IMD responds to any access requests. The Cloaker shares a long term master key with the IMD which authenticates and encrypts all the data communication between them. Since the Cloaker is an external device with more computational and power capabilities, public key protocols can be used to authenticate legitimate programmers and to establish a shared session key. Then all communication between the programmer and the IMD can either go through the Clocker, or the shared key can be handed by the Clocker to both the programmer and the IMD to communicate separately. The scheme encompasses two approaches by which the IMD can detect the presence of the Cloaker. Firstly, the IMD pings the Cloaker only when it detects an access request so that the Cloaker takes over the authentication procedure if present. Secondly, the IMD sends periodic keep-alive messages and updates its state according to the response from the Cloaker. In both cases, the IMD assumes an emergency mode if it receives no response from the Cloaker after a prespecified waiting period.

b: STRENGTHS

This solution highly prioritizes the safety of patients in emergency situations. In fact, it offers a very fast response time from the IMD during emergency situations. More specifically, no security measures or authentication procedures are applied in such time sensitive scenarios and the functionality of the IMD is completely dedicated to respond to the requested commands. This approach can be seen as an adoption from a framework of solutions known as *Breaking the Glass* [81], [82] which enables overriding of access control requirements in critical situations for the system. Moreover, if the Cloaker is lost, broken, or out of batteries, it can still be accessed in the event of an emergency. Also, since the Cloaker can be set to mediate all communication between the programmer and the IMD, it can create a log record which allows forensic analysis if required.

c: WEAKNESSES

The two ways by which the IMD detects the presence of the Cloaker are not efficient in terms of power consumption. More precisely, according to the FCC regulations [22], IMDs must not initiate any communication unless a life threatening condition is detected. Additionally, wireless communication is the most power consuming operation in IMDs. Accordingly, forcing IMDs to periodically send messages to detect the presence of the Cloaker is not an efficient approach. Also, the response of the Cloaker in both cases can be jammed by an active adversary which forces the IMD to grant access to any requesting programmers. Lastly, the Cloaker shares a predeployed long term key with the IMD which we assume is set in the IMD at the time of implantation. Nevertheless, the proposal does not address the situation when the Cloaker is lost or broken and how a new Cloaker may share the secret key with already implanted medical devices.

d: IMD GUARD

This protocol [67] proposes that an external device, called the Guardian, employs electrocardiogram (ECG) signals to extract long term secret key to be shared between the IMD and its Guardian. The protocol first defines a key establishment phase by which the IMD and the Guardian can share a secret key. In this phase, both parties commence by synchronously reading the ECG and taking the least significant 4 bits of 43 consecutive intra pulse intervals (IPI_4). ECG is considered a time varying physiological value which makes it well suited for this purpose [83]. Studies in [83] have shown that these bits are independent and identically distributed. Also, the analysis presented in [71] and [83] have confirmed that these bits have the maximal entropy and are completely uncorrelated. Additionally, discrepancies between different readings of an ECG signal have been investigated in [19]. In the sequel, both the IMD and the programmer enters the first round of key confirmation where they exchange the parity of each 4 bits from the 43 IPI_4, and if the parities match, the first bit is dropped because the parity leaks one bit of information, but if the parities differ, then the IPI block is dropped and subsequent IPI are read to complete a 129 bit key. Then the 2 parties exchange the hashes of the keys and if they do not match, another round of parity checking on the 3 bit blocks that survived in the first round is performed. The protocol supports two modes of operation. First, a normal

mode where the Guardian is worn. In this mode, when a programmer requests access, the IMD replies with a session ID and a fresh nonce, and waits for a specific time T_1 for the Guardian to authenticate the programmer and distribute a session key for the IMD and the programmer. In the case that the IMD receives no reply from the Guardian, it enters emergency mode assuming that the Guardian is physically removed and sends a nonce to the programmer, waits a time period T_2, then sends a second nonce. Finally, the programmer replies to the IMD with a message containing the hash of the nonces. On the other hand, if the Guardian is physically available, it authenticates the programmer employing a public key scheme and sends the generated one time session key to the IMD so that it can communicate with the programmer securely before the first waiting time has elapsed.

e: STRENGTHS

The most important feature in this protocol is that the shared key between the Guardian and the IMD can be changed. In other words, there is no need for any predeployed secret in the IMD. Accordingly, it is easy to rekey the IMD when the Guardian is lost or malfunctioning. Another advantage is that the two nonces that the IMD sends to the programmer when it receives no response from the Guardian are separated by T_2 seconds. This step prevents an adversary from convincing the IMD that the Guardian is absent by jamming its response after T_1. In other words, the Guardian can be calibrated to the parameters of its own IMD, thus if it detects the first nonce being sent by the IMD to the programmer, then it knows that its first response did not reach the IMD because it has been jammed. Because the guardian knows that the IMD will send another nonce after T_2 time, it jams the IMDs transmissions to prevent it from reaching the programmer.

f: WEAKNESSES

This protocol relies on the fact that ECG signals can only be measured with skin contact. Nevertheless, analysis in [84] has demonstrated that by video recording the face of a person over a period of time, movement and change in the color of the face with each heart beat pulse can be traced. Moreover, the resulted set of IPI_4 calculated by analyzing the video recording slightly differs than the one obtained by recording the ECG by touching the body. This results suggests that a remote adversary can produce a valid set of IPI_4, send it to the IMD to make it assume it is in a critical situation and authorize access. Similar results were validated using a smart phone camera in [85]. Accordingly, a remote adversary can convince the IMD that it is its Guardian and successfully establish a secure channel with it. Additionally, a man-in-the-middle attack on the method by which the IMD and the Guardian confirm the key bits extracted from the *IPI* block was presented in [86]. In this attack, at the end of round one of the parity check, the adversary interrupts the response of the IMD and sends the Guardian a random hash value, thus prompting the Guardian to send a reject message and enter round two. Moreover, the adversary can change the reject to accept and consequently, the IMD terminates the protocol and keeps three bits from each *IPI* block as secret key material. On the other side, The adversary keeps communicating with the Guardian through round two where she knows one bit of information from each consecutive 3 bits of the key used by the IMD from the leaked parity bit. It should be noted that IMD Guard use the hash function in the emergency mode protocol in an unjustified manner. More precisely, when the programmer receives the two challenges from the IMD, it replies with a message containing the hash of their xor which we find no reason for using this unkeyed hash function as anyone can evaluate it.

g: IMD SHIELD

This solution offers a non cryptographic communication between the IMD and the external device which is called the shield [68]. The shield is an externally worn device responsible for authenticating and authorizing programmers which can establish a cryptographically secure channel with it. It is also responsible for relaying the responses of the IMD to commands issued by authorized programmers. The shield accomplishes its task by adopting a full duplex radio device which acts as a jammer and receiver. In other words, it employs a jamming antenna and a receive antenna where the jamming antenna transmits a random signal to scramble the IMDs transmissions. The receive antenna is simultaneously connected to both a transmit and a receive chain where the transmit chain sends an antidote signal that cancels the jamming signal at the receive antenna, enabling it to receive the IMDs scrambled signal and decode it. Because, only the shield can generate the antidote signal, it is the only party that can decode the IMD's jammed signal. The shield also jams any communication from unauthorized programmers so that their transmissions cannot be decoded by the IMD and hence it will not respond to them. If the shield is absent, the IMD replies to all commands because all its transmissions are sent unscrambled. Another scheme called BodyDouble [69] adopts a similar approach but employs a spoofing mechanism by which the external device pretends to be the IMD and communicates with adversaries. Such technique thwarts the vulnerability of the IMD to battery draining attacks.

h: STRENGTHS

The most important feature of the Shield which distinguishes it from other protocols is its support to the already implanted device. Particularly, with millions of patients who already have wireless IMDs, the shield can be used to provide security to such devices as it requires no additional modification. It is also very considerate to the battery life of the implant as it requires no special effort in terms of communication or computation from the IMD's side. Unlike other wearable devices where the IMD has to detect their presence in case of emergencies and sometimes has to wait and/or issue additional messages to them, the response time of the IMD to all commands is the same whether the Shield is present or not. Also, because jamming consumes power

and the Shield should jam the IMD's transmission effectively, it can detect the timing when the IMD is expected to respond and then start jamming. More precisely, according to the MICS band regulations for IMD communication, IMDs transmit only in a response to commands from programmers without sensing the medium so the shield listens for programmers transmissions and can predict when the IMD may start transmitting and bound the duration of its responses.

i: WEAKNESSES

Jamming is the adopted approach by this proposal to thwart both passive and active adversarial attacks. However, operating jamming devices has legal consequences because it can interfere with other RF devices and potentially lead to legal complications. Also, commercial devices that operate in the MICS band have to adhere to the FCC power limitations. However, an adversary that transmits at high power can not be jammed by the Shield and the IMD will respond to such communications. Such transmissions can be detected by the Shield which raises an alarm to inform the patient and also jams the IMD responses, but still, such adversary can easily launch a battery draining attack because the IMD always responds to its commands. The effect of friendly jamming where a jamming device is used to protect the confidentiality of communications was undermined in [56]. More precisely, it has been demonstrated in [56] that an attacker with multiple receiving antennas can recover information from the protected jammed signals.

3) BIOMETRIC-BASED PROTOCOLS

Biometric techniques employ information extracted from the physical or physiological features of the patient [17], [87]. Adopting such information to form access credentials avoids the key distribution problem between the IMD and programmers. Accordingly, it is considered more feasible than that solutions based on shared keys. Also, because they require being physically in contact with the patient which implies her consent to the requested access to the IMD. In case of critical situations where the patient is unconscious, medical personnels can acquire such features and use them to access the IMD.

a: BIOMETRIC-BASED TWO-LEVEL SECURE ACCESS CONTROL (BBS-AC)

In [70], Hei and Du propose a solution that enforces access control procedure using two levels of authentication. More precisely, BBS-AC requires programmers to provide biometric features from the patient in two consecutive levels. At the first level of authentication, the scheme requires basic biometric information, such as fingerprints pattern, height, and eye color. If a programmer is authenticated through the first level, the second level of authentication takes place where the patient's iris snap shot is required to determine whether the programmer is authorized to access the IMD or not.

b: STRENGTHS

The adopted two levels method takes the limited battery life in consideration. More precisely, the first level of authentication is light weight as it involves comparing numeric values which represent fingerprints pattern, height, and eye color to the ones stored on the IMD. The second level calls for a more computationally exhaustive procedure required for iris recognition. Thus, in the case of an adversary, who has no knowledge of the required biometric values, tries to connect to the IMD, only the first lightweight level of authentication is executed and the request is rejected, which saves the power required for the iris recognition and hence the power of the IMD. It is also expected that the features required in the first level can be acquired if someone is at close proximity of the patient but obtaining a high quality snapshot of the iris requires an infrared camera [70] at a distance of between fifty and seventy centimeters. Such snapshot can only be taken of the iris of either a consenting patient or an unconscious one. The proposal also proposes a method to perform the iris verification step by matching partial iris data rather than the entire iris data which significantly reduces the computation overhead of this step, thus saving the limited power of IMDs.

c: WEAKNESSES

BBS-AC requires data related to the biometric features of the patient to be pre-stored in the IMD prior to implantation which is equivalent to setting a predeployed master key. Accordingly, because this data is not supposed to change with time, all the medical personnels who use it can know the secret as well. In other words, the secret after multiple uses will not be a secret anymore and it cannot be changed either. Biometrics in general including dynamic ECG signals bind access to IMDs to the physical presence of the patient which may not be convenient for the case where IMD remote monitoring is required. Also, biometric measurements are rarely perfect, especially in case of an incapacitated or seizuring patient, taking her iris snapshot may be impossible as iris cannot be fully visible. Additionally, measurements taken using two different reading devices, could generate different results. Accordingly, these scenarios result in credentials that prevents the desired critical access to the IMD even if the programmer is legitimate.

d: HEART-TO-HEART (H2H)

Proposed by Rostami *et al.* [71], this scheme is a cryptographic authentication protocol that uses ECG signals to ensure proximity. This protocol proposes that both the IMD and the programmer which is requesting access to measure the heart activities by recording the ECG signal at the same time. Afterwards, both the IMD and the programmer extract the least significant four bits from a consecutive set of intra pulse timing intervals (IPI_4). In the sequel, the programmer sends its recorded set of IPI_4 to the IMD. This reading can be different than what is read by the IMD due to recording errors. To decide whether to accept the reading as genuine

or reject the session, the IMD first evaluates the error by comparing the received reading to the one it recorded. Then, using Neyman-Pearson hypothesis testing [71] where the hypothesis is that the calculated error is drawn from the error probability distribution of an honest programmer, access decision is established. The cryptographic protocol starts by first setting up a secure channel using TLS [88] where the programmer sends its certificate to the IMD which acts as the client. The output of this stage is a shared master key and a random value. Next the authentication stage takes place where each party commits to its set of IPI_4 after binding it to the shared random number generated from the TLS session. Then commitments are exchanged and based on the output of the Neyman-Pearson test on the difference between the two readings, the IMD accepts or rejects the programmer's access request.

e: STRENGTHS

In the secure channel setup, TLS is employed where the programmer send it certificate to the IMD. However, the certificate is used by the IMD to extract the public key of the programmer only, thus the procedure involves no verification via Public Key Infrastructure (PKI) which saves the battery power. Another advantage is that during the authentication stage and after exchanging the commitment, the programmer reveals its reading to the IMD only after accepting the received reading from the IMD. The order of revealing the commitments prevents the reuse of the programmer's reading by an adversary in a man-in-the-middle attack. Also the authors propose that in the case of heart failure or other life threatening conditions where the ECG signal of the IMD has no pulse, all access control procedures are dropped.

f: WEAKNESSES

The protocol assumes that ECG readings and thus the sequence of IPI_4 can only be evaluated by a device touching the body of the patient. However, the protocols suffers from the limitation of ECG signals discussed in the *IMD Guard* protocol. Another weakness of this protocol is that the TLS session takes place where the IMD performs a modular exponentiation operation (RSA encryption) before checking if the programmer is legitimate or not. Although in the event of the IMD rejecting an authentication attempt it waits one reading cycle before accepting any requests, the system is vulnerable to battery draining attacks given the modular exponentiation computational requirements.

g: ECG-BASED SECRET DATA SHARING (ESDS)

Zheng *et al.* [72] proposed this technique by which a programmer can establish a secure channel and authenticate itself to the IMD using ECG signals. First, the IMD and the programmer measure ECG signals synchronously. Then, both parties generate a secret key bit string by concatenating the five least significant bits from consecutive sets of *IPIs*. Next, all the data that needs to be shared privately is first encoded using an Error Correcting Code (ECC) technique. ECC adds redundant check bits to the transfered data which can be used by the receiver to correct bit errors via a decoding procedure. In the sequel, the coded data is then xored by the ECG *IPI* bit string to encrypt it. Typically, ECC schemes are used to correct system noise but because ECG data is xored to the coded data, it can be used to correct difference between the ECG readings by both the IMD and programmer.

h: STRENGTHS

The algorithm is straightforward and simple. Encryption and authentication involve no public key primitives. Moreover, encryption is performed via xor which makes the algorithm very light in terms of power consumption.

i: WEAKNESSES

This proposal suffers from the challenges of ECG-based schemes. Particularly, if an adversary is able to remotely measure ECG signals by observing changes in skin color or movements induced by heart pulses, then she would be able to remotely authenticate herself and gain access to the IMD. Moreover, since ECG signal is used to derive the encryption key, an eavesdropper observing the pairing process between a legitimate programmer and the IMD may be able reproduce the shared key and decrypt the exchanged information.

4) HYBRID APPROACHES

Techniques in this category [74], [75] utilize one of the previously discussed categories to provide access to IMDs in the case of emergency.

a: EMERGENCY AWARE ACCESS CONTROL (EA-AC)

This protocol [75] assumes that a proxy device is worn by the patient and that it shares a long term key with the IMD. It also proposes that the state of emergency (e.g., heart failure, hypoglycemic attacks, or high blood pressure) is solely determined by the IMD, in which case the protocol does not provide fail open access but alerts the proxy device. Upon receiving an emergency signal, the proxy device accesses a virtual space using a web service, specifies the required medical service and the location of the IMD. In response to the proxy's request, the web service provides a list of doctors who are available in close proximity of the patient and with a doctor's consent, the proxy allows access to the IMD for a limited period only to this doctor. More precisely, the device provides the chosen doctor with temporary constrained access credentials for the IMD.

b: STRENGTHS

The algorithm pays a great attention to access control in case of emergency. While one may argue that fail open access is the preferred method to deal with emergency situations, EAAC emphasizes on the fact that attacks can take place even in such scenario and that role-based access [89], [90] to a given physician must be decided by the criticality of the medical condition which is determined by the IMD.

Also, all the security procedure is carried out by the proxy device which saves the battery of the IMD.

c: WEAKNESSES

In addition to having a predeployed key shared between the IMD and the proxy, EAAC adds to the weaknesses of proxy devices protocols. Particularly, if the proxy is lost or stolen, the IMD is inaccessible in the event of an emergency. Also the protocol relies heavily on the fact that physicians must regularly sign in to the virtual space and provide their availability and location which may not be easily accepted by all medical staff. The protocol also runs a lot of procedures to provide emergency response to the patient's condition requiring network access, waiting times, and most shockingly the availability of a consenting physician in the vicinity of the patient. Alternatively, it is more reasonable to alert emergency responders and provide fail open access.

d: HOSPITAL AUTHENTICATION SERVER ACCESS CONTROL (HAS-AC)

This authentication mechanism [74] proposes the use of a three tier architecture for access control. It assumes that patients with IMDs that are treated within a given hospital share a long term key with a hospital server. Also, physicians in the hospital share a long term key with the authentication server. When an incapacitated patient is present at the hospital, a general purpose programmer can be customized using the physician and the IMD keys which they share with the hospital sever to access the IMD. More precisely, the physician inserts a smart card containing her long term key and signing key. In the sequel, the programmer verifies the identity of the physician from the hospital server and requests the ID of the patient's IMD. Afterwards, the programmer sends an authorization request to the server which subsequently provides both the IMD and the programmer with a session key to continue their communication. In the event that the patient is admitted to a hospital different than hers, the protocol assumes that the patient wears a medical bracelet with an access key to disable the IMD.

e: STRENGTHS

The protocol addresses the problem of having a specific programmer for each IMD that can be operated by any individual in the case of a non consenting patient. In other words, it provides a means for general purpose programmers to be personalized according to an authenticated physician and IMD. Accordingly, only authorized physicians can operate programmers and any programmer can be used with any IMD.

f: WEAKNESSES

This proposal does not provide a solution for the problem of emergency authentication when the patient is outside her usual treatment facility. In fact, the protocol proposes that the patient wears a medical bracelet with an access key for that purpose. Accordingly, the IMD can become inaccessible in the event of an emergency if the bracelet is forgotten or lost.

Trade-offs between the applicability of the provided security features and the safety of the patient are very evident in the previously surveyed proposals. In fact, each one of these access control proposals offer a specific balance between security and safety. Some are completely leaned towards the safety of the patient especially in emergency situations, which consequently comes on the expense of the other factor. Examples of such schemes include the Cloaker where once the wearable device is taken off, no additional communication from the IMD is required to allow open access. On the other hand, it requires the IMD to either continuously update the state of the Cloaker or to check it upon receiving access request. The first case affects the battery life and the second case makes the IMD vulnerable to denial of service attacks. On the other hand, protocols such as Heart-to-Heart enforce active security measures at the time of emergency. In fact, this protocol first establishes a TLS secure channel and uses an ECG fresh reading to prove the proximity of the emergency personnel. However, the TLS step involves modular addition and it is carried out before authenticating the requesting programmer which makes the IMD vulnerable to a battery draining attack. All the above protocols do not solve the problem of backward compatibility, except the Shield which does not require any alteration of the firmware of the IMD and it does not enforces any cryptographic solution that burdens the battery of the IMD. However, its use on a wide scale is questionable, mainly because it is a jamming device and its operation may affect other communication leading to further legal restrictions.

Table 1 provides a comparison of the surveyed authentication proposals in terms of keys used by the IMD communications where predeployed key refers to a key that is used throughout the lifetime of the IMD and dynamic key refers to a key that is newly generated for each session. In the case of proxy based and three tier approaches, the intended key refer to the key shared between the IMD and the external device or the third party. Also, we contrast the surveyed protocols with respect to the cryptographic methods implemented in the IMD. Moreover, we indicate how fast the IMD responds to the programmer request in the case of emergency. Also, merits including their vulnerability to battery draining attacks (BDA), whether the established key can be acquired by an adversary, if access is always guaranteed, the need for additional devices other than the IMD, and the probability of detecting an emergency when there is none (false alarm) are addressed.

VII. FUTURE RESEARCH DIRECTIONS

Unlike information security of computer systems, cyber security of IMDs is a relatively new area. Particularly because people only started realizing the urgent need for protecting these critical systems when the actual attacks on IMDs which directly affect the patient's wellbeing were realized in-vitro [14], [35], [42]. Most of the efforts from the security community are focused on the design and analysis of access protocols for IMDs. Indeed, the required dynamic

TABLE 1. Comparison of IMD authentication protocols. BDAs: battery draining attacks, N/A means that the information was not available in the original publication.

	Predeployed key	Dynamic key	Public key crypto	Symmetric key primitives	Response time in emergency	Vulnerability to BDAs	Protection can be bypassed	Guaranteed access in emergency	Requires additional devices	Legacy compatibility	False positive alarms
ZP Sec [14]		✓		✓	fast	low	✓	✓	✓		✓
US-DB [64]		✓	✓	✓	moderate	moderate	✓	✓			
in-vivo NFC [65]	✓		N/A	N/A	moderate	low	N/A		✓		
The Cloaker [66]	✓			✓	fast	low		✓	✓		
IMD Guard [67]		✓		✓	slow	moderate	✓	✓	✓		
The shield [68]					fast	high	✓	✓	✓	✓	
BBS-AC [70]	✓			✓	moderate	low		✓			
H2H [71]		✓	✓	✓	slow	high	✓	✓	✓		
ESDS [72]		✓		✓	moderate	moderate	✓	✓			
EA-AC [75]	✓			✓	slow	moderate			✓		✓
HAS-AC [74]	✓			✓	slow	low			✓		

nature of such procedures which distinguishes them from the standard methods used in computer systems makes realizing both security and safety a challenging task. In fact, among all the dozen surveyed emergency authentication solutions, none achieves the required levels of security and safety which makes this direction remain as an open problem. Most of the surveyed authentication proposals provide informal proofs to justify how the cryptographic protocol achieves both security and safety requirements. However, using only this approach makes it easy to overlook an essential assumption which can lead to contradictory situation between security and safety. Verifying that both the security and safety requirements are satisfied simultaneously can be achieved by formal methods [2], [91], [92]. Accordingly, an interesting research direction is to attempt to apply formal verification techniques on the IMD authentication protocols in order to validate the claims of their designers and accordingly, gain the confidence of the security community. Despite the criticality of managing authorized access of IMDs, some areas such as secure control [93], [94] of IMDs are essentially as important and the existing work addressing them is very limited. In what follows, we highlight some challenging areas in the hope of having our discussion serve as first steps for future research directions:

- *IMD Forensic Investigation:* Auditing is usually a standard tool for forensic investigation in computer systems. Particularly, accountability of actions can be determined if an audit log is utilized. Such log records system activities in a chronological order and subsequently enables the reconstruction of the sequence of events and changes in the state of the system. Accordingly, in the case of a security breach, audit logs are essential components required for forensic investigation. For IMDs, security incidents can lead to the patient's death as has been demonstrated in-vitro in [14], [35], [36], and [42] which makes auditing essential in IMDs. Unfortunately, audit logs require memory which is a scarce resource in IMDs. For example, the average memory of a modern cardiac defibrillator is around 1 MB and nearly 75% of it is consumed by its basic functions which leaves very small memory for logging purposes [10]. Accordingly, with such small memory, audit logs can be easily overflown and thus bypassed. Even though there has been no reported cases on death resulting from a security attacks on IMDs, there is no definitive way to differentiation between whether death is caused by an intentional tampering of the implant or from natural causes. The little work in this area is mainly attributed to the diversification of required expertise. For instance, when a deceased patient with an IMD arrives at the morgue, without the knowledge of biomedical engineering, the corner cannot determine if the cause of death is a result of natural circumstances, a malfunction of the IMD, or an intentional sabotage of the working of the IMD. On the other side, in order to be able to design auditing methods for forensic investigation in IMDs, biomedical engineers need to understand how medical investigators work. A recent effort in this area is presented by Ellouze *et al.* [95] where they developed an inference system that uses evidence from technical investigators and medical deductions from pathologists to determine the probability of a given attack scenario being the source of the patient's death. With millions of IMDs implanted in the U.S. and given the fact that some of them can be high value targets [32], killing without leaving a trace must not be that easy. It is crucially urgent for researchers from all the concerned disciplines to work together and find systematic ways to distinguish crime from fate.

- *Intrusion Detection (ID) in IMDs:* A computer system uses an ID system to try to identify if the system activity is a result of genuine or malicious communication. It usually monitors the network traffic and performs some analysis using either anomaly or signature identification. Anomaly-based ID systems monitors incoming traffic and compares it to an established pattern for the normal behavior of the system. Such pattern is usually identified by the ID system during a training stage where various parameters of normal communication are observed by the system for an extended period of time. On the other hand, signature based ID systems compare the monitored communication with a preset repository of attributes from previously known threats. Both systems are usually employed together to perform intrusion detection in computer systems because each of them has its own limitations that the other can solve. Particularly, anomaly-based ID systems suffer from the high false positive detections and signature-based ID systems cannot spot new threats.

  There are only few works covering the area of intrusion detection in IMDs. Existing proposals [44], [96], [97] adopt an anomaly-based approach to try detecting battery depletion resulting from malicious communication. Training parameters include physiological changes that accompany therapy administration following genuine IMD operations [96], information related to the commands which are usually issued by a legitimate programmer [44], and certain characteristics of the radio signals generated in authorized communication [97]. Most of the available proposals suggest the use of an external device to carryout the work of the ID system [44], [97] to protect the battery of the IMD from over consumption. No proposals have considered signature-based ID and with the limitations of anomaly detection techniques, there is a need for further investigation in the area of intrusion detection.
- *Software and Hardware Vulnerabilities in IMDs:* Software plays a fundamental role in the safe operation of IMDs. In 2010, the FDA recalled 23 defective cardiac pacemakers [98]. At least six of the defective pacemakers were recalled due to software defects. Following the trend of security by obscurity [5], manufactures of IMDs employ proprietary software which might be more beneficial from financial perspective. However, from security perspective open source software is arguably more secure as it becomes subjected to continuous international auditing which improves its reliability and security through the identification and patching of the discovered vulnerabilities. Accordingly, the challenge for future research is how to balance both the financial interests of IMD manufacturers and the desirable security benefits that come with the open software especially that such benefits directly affect the safety of patients with IMDs. Also, hardware Trojans [99], [100] that may be intentionally designed in IMDs to disable security mechanisms when triggered can have catastrophic consequences. Testing IMDs for hardware Trojans is a very challenging task and requires further attention from the security community.

VIII. CONCLUSION

In this paper, we have briefly visited security trade-offs in cyber physical systems. We have identified the threats, and challenges facing the adoption of a given risk mitigation mechanism. Also, we have discussed the effects of cyber security and how it has an effect on the safety of the surrounding environment of the system. As a case study, we have surveyed the case of IMDs. Particularly, we categorized and contrasted different proposals targeting the concept of emergency authentication. Such proposals try to balance the trade off between providing security measures for the IMD and the safety of the patient at the time of emergency. Moreover, we have identified a number of security advantages and vulnerabilities in our analysis for each protocol. Given the tension between how each protocol handles both security and safety requirements in a power constrained environment, we conclude that the topic of emergency authentication is still an open area for further research. Moreover, we have cited a number of challenges that face IMD security mechanisms along with some possible research directions.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that helped improve the quality of the paper. This work is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

REFERENCES

[1] D. J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven, CT, USA: Yale Univ. Press, 2011.
[2] M. Sun, S. Mohan, L. Sha, and C. Gunter, "Addressing safety and security contradictions in cyber-physical systems," in *Proc. 1st Workshop Future Directions Cyber-Phys. Syst. Secur. (CPSSW)*, 2009, pp. 1–5.
[3] Wikipedia. (2015). *Germanwings Flight 9525*. [Online]. Available: https://en.wikipedia.org/wiki/Germanwings_Flight_9525
[4] W. D. Jones, "Black boxes get green light [car crash data recorders]," *IEEE Spectr.*, vol. 41, no. 12, pp. 14–16, Dec. 2004.
[5] K. Stouffer, J. Falco, and K. Scarfone. (2011). *Guide to Industrial Control Systems (ICS) Security*. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
[6] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," *IEEE Syst. J.*, vol. 9, no. 2, pp. 350–365, Jun. 2015.
[7] S. K. Das, K. Kant, and N. Zhang, *Handbook on Securing Cyber-Physical Critical Infrastructure*. San Mateo, CA, USA: Morgan Kaufmann, 2012.
[8] A. Cárdenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Proc. Workshop Future Directions Cyber-Phys. Syst. Secur.*, 2009, pp. 1–7.
[9] E. Y. Vasserman, K. K. Venkatasubramanian, O. Sokolsky, and I. Lee, "Security and interoperable-medical-device systems, part 2: Failures, consequences, and classification," *IEEE Security Privacy*, vol. 10, no. 6, pp. 70–73, Nov./Dec. 2012.
[10] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Inform.*, vol. 55, pp. 272–289, Jun. 2015.
[11] J. A. Hansen and N. M. Hansen, "A taxonomy of vulnerabilities in implantable medical devices," in *Proc. 2nd Annu. Workshop Secur. Privacy Med. Home-Care Syst. (SPIMACS)*, 2010, pp. 13–20.

[12] V. S. Mallela, V. Ilankumaran, and N. S. Rao, "Trends in cardiac pacemaker batteries," *Indian Pacing Electrophysiol. J.*, vol. 4, no. 4, pp. 201–212, 2004.

[13] J. G. Webster, *Design of Cardiac Pacemakers*. New York, NY, USA: IEEE Press, 1995.

[14] D. Halperin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy*, May 2008, pp. 129–142.

[15] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Services (Healthcom)*, Jun. 2011, pp. 150–156.

[16] T. R. Lukins, S. Tisch, and B. Jonker, "The latest evidence on target selection in deep brain stimulation for Parkinson's disease.," *J. Clin. Neurosci.*, vol. 21, no. 1, pp. 22–27, 2014.

[17] K. Cho and D. H. Lee, "Biometric based secure communications without pre-deployed key for biosensor implanted in body sensor networks," in *Information Security Applications* (Lecture Notes in Computer Science), vol. 7115, S. Jung and M. Yung, Eds. Heidelberg, Germany: Springer, 2012, pp. 203–218.

[18] 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," in *Proc. Int. Conf. Parallel Process. Workshops*, Oct. 2003, pp. 432–439.

[19] 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 *Proc. USENIX Conf. Health Secur. Privacy*, 2012, p. 5.

[20] D. Bodmer and S. Capkun, "On the security and privacy risks in cochlear implants," Dept. Comput. Sci., ETH, Zürich, Switzerland, 2010.

[21] Professional.medtronic.com. (2015). *About Gastric Electrical Stimulation: Medtronic*. [Online]. Available: http://professional.medtronic.com/pt/gastro/ges/edu/about/#.Vk6qq3arTIU

[22] Federal Communications Commission. *Report and Order: FCC 00-211*. [Online]. Available: http://transition.fcc.gov/Bureaus/Engineering_Technology/Orders/2000/fcc00211.pdf

[23] 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.

[24] S. S. Clark and K. Fu, "Recent results in computer security for medical devices," in *Wireless Mobile Communication and Healthcare* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 83, K. S. Nikita, J. C. Lin, D. I. Fotiadis, and M.-T. A. Waldmeyer, Eds. Berlin, Germany: Springer, 2012.

[25] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.

[26] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 524–539.

[27] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 283–299, Jan. 2012.

[28] K. Wan and V. Alagar, "Context-aware security solutions for cyber-physical systems," *Mobile Netw. Appl.*, vol. 19, no. 2, pp. 212–226, 2014.

[29] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[30] P. Jokar, N. Arianpoo, and V. C. Leung, "A survey on security issues in smart grids," *Secur. Commun. Netw.*, vol. 9, no. 3, pp. 262–273, 2012.

[31] J. Wan, H. Suo, H. Yan, and J. Liu, "A general test platform for cyber-physical systems: Unmanned vehicle with wireless sensor network navigation," *Procedia Eng.*, vol. 24, pp. 123–127, 2011.

[32] G. Kolata. (2015). *Of Fact, Fiction and Cheneys Defibrillator*. [Online]. Available: http://www.nytimes.com/2013/10/29/science/of-fact-fiction-and-defibrillators.html?_r=0

[33] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Comput. Secur.*, vol. 49, pp. 70–94, Mar. 2015.

[34] W. Hu, T. Tan, L. Wang, and S. Maybank, "A survey on visual surveillance of object motion and behaviors," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 34, no. 3, pp. 334–352, Aug. 2004.

[35] *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System*. [Online]. Available: http://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf, accessed Oct. 15, 2015.

[36] P. Roberts, M. Mimoso, C. Brook, and M. Mimoso. (2011). *Blind Attack on Wireless Insulin Pumps Could Deliver Lethal Dose*. [Online]. Available: https://threatpost.com/blind-attack-wireless-insulin-pumps-could-deliver-lethal-dose-102711/75808/

[37] P. E. Chadwick, "Regulations and standards for wireless applications in eHealth," in *Proc. 29th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2007, pp. 6170–6173.

[38] Wireless.fcc.gov. (2015). *FCC: Wireless Services: Medical Device Radiocommunications Service: About: Band Plan*. [Online]. Available: http://wireless.fcc.gov/services/index.htm?job=service_bandplan&id=medical_implant

[39] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices, Evidence Res.*, vol. 8, pp. 305–316, Jul. 2015.

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

[41] W. Burleson and S. Carrara, Eds., *Security and Privacy for Implantable Medical Devices*. New York, NY, USA: Springer, 2014.

[42] Go.bloomberg.com. (2015). *Hacker Shows Off Lethal Attack by Controlling Wireless Medical Device—Bloomberg*. [Online]. Available: http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/

[43] S. Hanna, R. Rolles, A. Molina-Markham, P. Poosankam, K. Fu, and D. Song, "Take two software updates and see me in the morning: The case for software security evaluations of medical devices," in *Proc. 2nd USENIX Conf. Health Security Privacy (HealthSec)*, Berkeley, CA, USA, 2011, p. 6.

[44] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.

[45] D. C. Bock, A. C. Marschilok, K. J. Takeuchi, and E. S. Takeuchi, "Batteries used to power implantable biomedical devices," *Electrochim. Acta*, vol. 84, pp. 155–164, Dec. 2012.

[46] R. Krishnan, E. John, and M. Panday, "Towards security policy and architecture for managing implantable medical devices," in *Proc. Int. Conf. Secur. Manage. (SAM), Steering Committee World Congr. Comput. Sci., Comput. Eng. Appl. Comput. (WorldComp)*, 2012, p. 1.

[47] M. de Sousa, G. Klein, T. Korte, and M. Niehaus, "Electromagnetic interference in patients with implanted cardioverter-defibrillators and implantable loop recorders," *Indian Pacing Electrophysiol. J.*, vol. 2, no. 3, pp. 79–84, 2002.

[48] S. Gupta, "Implantable medical devices-cyber risks and mitigation approaches," in *Proc. Cybersecur. Cyber-Phys. Syst. Workshop (NISTIR)*, 2012, pp. 15–30.

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

[50] Medscape. (2013). *FDA Approval Process for Medical Devices*. [Online]. Available: http://www.medscape.com/viewarticle/807243_2

[51] U.S. Government Accountability Office. (2012). *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices*. [Online]. Available: http://gao.gov/products/GAO-12-816

[52] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. USA: Food and Drug Administration, 2014.

[53] D. Stoker. (2014). *Medical Devices Safe, But are They Secure?* [Online]. Available: https://hipaacentral.com/Documents/Perspectives/Medical-Device-Security_PerspectivePaper_0314.aspx

[54] K. Malasri and L. Wang, "Securing wireless implantable devices for healthcare: Ideas and challenges," *IEEE Commun. Mag.*, vol. 47, no. 7, pp. 74–80, Jul. 2009.

[55] S. Brands and D. Chaum, "Distance-bounding protocols," in *Advances in Cryptology*. Berlin, Germany: Springer, 1994, pp. 344–359.

[56] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 160–173.

[57] I. Lee *et al.*, "Challenges and research directions in medical cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 75–90, Jan. 2012.
[58] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, "Design challenges for secure implantable medical devices," in *Proc. 49th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2012, pp. 12–17.
[59] Y.-H. Joung, "Development of implantable medical devices: From an engineering perspective," *Int. Neurourol. J.*, vol. 17, no. 3, pp. 98–106, 2013.
[60] R. K. Shepard and K. A. Ellenbogen, "Leads and longevity: How long will your pacemaker last?" *Europace*, vol. 11, no. 2, pp. 142–143, 2009.
[61] C. Zhan, W. B. Baine, A. Sedrakyan, and C. Steiner, "Cardiac device implantation in the united states from 1997 through 2004: A population-based analysis," *J. General Internal Med.*, vol. 23, no. 1, pp. 13–19, 2008.
[62] S. Schechter, "Security that is meant to be skin deep: Using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices," in *USENIX HealthSec*. Albuquerque, NM, USA: Microsoft, Aug. 2010. [Online]. Available: http://research.microsoft.com/apps/pubs/default.aspx?id=135291
[63] T. Halevi and N. Saxena, "On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping," in *Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS)*, 2010, pp. 97–108.
[64] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, 2009, pp. 410–419.
[65] B. Kim, J. Yu, and H. Kim, "*In-vivo* NFC: Remote monitoring of implanted medical devices with improved privacy," in *Proc. 10th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, 2012, pp. 327–328.
[66] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *Proc. 3rd Conf. Hot Topics Secur. (HOTSEC)*, 2008, pp. 5:1–5:7.
[67] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.
[68] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, Aug. 2011.
[69] G. Zheng, G. Fang, M. A. Orgun, and R. Shankaran, "A non-key based security scheme supporting emergency treatment of wireless implants," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 647–652.
[70] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 346–350.
[71] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1099–1112.
[72] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, and E. Dutkiewicz, "An ECG-based secret data sharing scheme supporting emergency treatment of implantable medical devices," in *Proc. Int. Symp. Wireless Pers. Multimedia Commun.*, Sep. 2014, pp. 624–628.
[73] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2274–2282.
[74] C.-S. Park, "Security mechanism based on hospital authentication server for secure application of implantable medical devices," *BioMed Res. Int.*, vol. 2014, Jul. 2014, Art. ID 543051.
[75] M. Darji and B. H. Trivedi, "Emergency aware, non-invasive, personalized access control framework for IMDs," in *Recent Trends in Computer Networks and Distributed Systems Security* (Communications in Computer and Information Science), vol. 420, G. M. Pérez, S. Thampi, R. Ko, and L. Shu, Eds. Berlin, Germany: Springer, 2014, pp. 370–381.
[76] J. E. Bardram, R. E. Kjær, and M. Ø. Pedersen, "Context-aware user authentication—Supporting proximity-based login in pervasive computing," in *UbiComp 2003: Ubiquitous Computing*. Berlin, Germany: Springer, 2003, pp. 107–123.
[77] S. K. S. Gupta, T. Mukheriee, K. Venkatasubramanian, and T. B. Taylor, "Proximity based access control in smart-emergency departments," in *Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2006, pp. 515–516.
[78] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 113–127.
[79] A. J. Menezes, S. A. Vanstone, and P. C. van Oorschot, *Handbook of Applied Cryptography*, 1st ed. Boca Raton, FL, USA: CRC Press, 1996.
[80] T. Denning, D. B. Kramer, B. Friedman, M. R. Reynolds, B. Gill, and T. Kohno, "CPS: Beyond usability: Applying value sensitive design based methods to investigate domain characteristics for security for implantable cardiac devices," in *Proc. 30th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, 2014, pp. 426–435.
[81] A. Ferreira *et al.*, "How to break access control in a controlled manner," in *Proc. 19th IEEE Symp. Comput.-Based Med. Syst.*, Jun. 2006, pp. 847–854.
[82] A. D. Brucker and H. Petritsch, "Extending access control models with break-glass," in *Proc. 14th ACM Symp. Access Control Models Technol.*, 2009, pp. 197–206.
[83] 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.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.
[84] M.-Z. Poh, D. J. McDuff, and R. W. Picard, "Advancements in noncontact, multiparameter physiological measurements using a webcam," *IEEE Trans. Biomed. Eng.*, vol. 58, no. 1, pp. 7–11, Jan. 2011.
[85] S. Kwon, H. Kim, and K. S. Park, "Validation of heart rate extraction using video imaging on a built-in camera system of a smartphone," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug./Sep. 2012, pp. 2174–2177.
[86] M. Rostami, W. Burleson, A. Juels, and F. Koushanfar, "Balancing security and utility in medical devices?" in *Proc. 50th ACM/EDAC/IEEE Design Autom. Conf.*, May/Jun. 2013, pp. 1–6.
[87] 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," presented at the 3rd USENIX Workshop Health Secur. Privacy, Bellevue, WA, USA, 2012. [Online]. Available: https://www.usenix.org/conference/healthsec12/workshop-program/presentation/Chang
[88] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. [Online]. Available: https://tools.ietf.org/rfc/rfc5246.txt
[89] S. K. S. Gupta, T. Mukherjee, and K. Venkatasubramanian, "Criticality aware access control model for pervasive applications," in *Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun.*, Mar. 2006, pp. 253–257.
[90] D. Goel, E. Kher, S. Joag, V. Mujumdar, M. Griss, and A. K. Dey, "Context-aware authentication framework," in *Mobile Computing, Applications, and Services*. Berlin, Germany: Springer, 2010, pp. 26–41.
[91] G. Elahi and E. Yu, "A goal oriented approach for modeling and analyzing security trade-offs," in *Conceptual Modeling* (Lecture Notes in Computer Science), vol. 4801, C. Parent, K.-D. Schewe, V. C. Storey, and B. Thalheim, Eds. Heidelberg, Germany: Springer, 2007, pp. 375–390.
[92] G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in *Complex Systems Design & Management Asia*, M.-A. Cardin, D. Krob, P. C. Lui, Y. H. Tan, and K. Wood, Eds. Cham, Switzerland: Springer, 2015, pp. 41–53.
[93] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 495–500.
[94] S. McLaughlin, "Securing control systems from the inside: A case for mediating physical behaviors," *IEEE Security Privacy*, vol. 11, no. 4, pp. 82–84, Jul./Aug. 2013.
[95] N. Ellouze, S. Rekhis, M. Allouche, and N. Boudriga, "Digital investigation of security attacks on cardiac implantable medical devices," *Electron. Proc. Theoretical Comput. Sci.*, vol. 165, pp. 15–30, Oct. 2014.
[96] N. L. Henry, N. R. Paul, and N. McFarlane, "Using bowel sounds to create a forensically-aware insulin pump system," in *Proc. USENIX Conf. Safety, Secur., Privacy Interoperability Health Inf. Technol. (HealthTech)*, Berkeley, CA, USA, 2013, p. 8.
[97] M. Zhang, A. Raghunathan, and N. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 7, no. 6, pp. 871–881, Dec. 2013.
[98] Fda.gov. (2015). *Patients Alerted to Pacemaker Recall*. [Online]. Available: http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm165619.htm
[99] D. Mukhopadhyay and R. S. Chakraborty, *Hardware Security: Design, Threats, and Safeguards*, 1st ed. Boca Raton, FL, USA: CRC Press, 2014.

[100] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2008, pp. 15–19.

RIHAM ALTAWY is currently pursuing the Ph.D. degree with the Concordia Institute for Information Systems Engineering, Concordia University, Canada. She is supported by the Ph.D. Scholarship from the Natural Sciences and Engineering Research Council of Canada. Her work on the analysis of the Russian cryptographic hashing standard STREEBOG has won an international research competition by the Russian Federation Standardization Body (TC26). Her research interests focus on the analysis of symmetric key primitives, cryptographic protocols, and cyber security of critical infrastructures.

AMR M. YOUSSEF (SM'06) received the B.Sc. and M.Sc. degrees from Cairo University, Cairo, Egypt, in 1990 and 1993, respectively, and the Ph.D. degree from Queens University, Kingston, ON, Canada, in 1997. He was with Nortel Networks, the Center for Applied Cryptographic Research, University of Waterloo, IBM, and Cairo University. He is currently a Professor with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada. His research interests include cryptology, malware analysis, and secure hardware implementations of cryptographic algorithms. He served as the Co-Chair of Africacrypt 2013 and the Selected Areas in Cryptography (SAC 2014, SAC 2006, and SAC 2001) Conference.