International Journal of Advances in Computer Science & Its Applications
Volume 6 : Issue 2 *[ISSN 2250-3765]*
Publication Date : 31 August, 2016

A Secure and Investigation-aware Smart Healthcare Cyber Physical System

Nourhene Ellouze, Slim Rekhis, and Noureddine Boudriga

***Abstract*— The aim of this research is to develop a Smart Healthcare Cyber Physical System (CPS) which allows to: a) enhance the responsiveness of implantable medical systems to health abnormalities; b) protect the patients from security threats and attacks from outsiders; c) provide a remote supervision of the patients' health, and of the vital equipment that he/she wears; and d) forensically generate evidentiary data to promote the forensic investigation of healthcare attacks. In this paper, we define the CPS architecture together with the functions it implements. A mutual authentication protocol between the CPS and the remote physician is proposed. A technique for the investigation of healthcare attacks on that CPS using incident response cognitive maps is also described.**

***Keywords*— Cyber Physical Systems, Implantable Medical Devices, Wearable and Embedded Sensors, Security.**

I. Introduction

A Healthcare Cyber Physical System (CPS) is a networked solution that introduces intelligence to the health. It interconnects the physical system to a virtual word, where computation, control, and communication can be provided. Medical sensors, actuators, and clouds are among the technologies that made CPSs popular in healthcare applications. One of the most autonomous devices that can be integrated to CPSs is the Implantable Medical Devices (IMDs). They are miniaturized programmable platforms which have limited computational and energy resources. They are surgically implanted into the patients' bodies to supervise their physiological state, detect anomalies, and deliver therapeutic functions. This kind of CPS is cost effective in improving the patient's life quality, and accelerating the detection and response to chronic disorders.

Recent research works have addressed several concerns about the security of IMD based CPSs. They have identified a set of security weaknesses, which make IMDs subject to attacks threatening the privacy and the life of patients. For instance, an adversary, who gets access to the IMD, modifies the therapy settings in such a way that the device could not react appropriately to future arrhythmias, which could be lethal. To deal with these concerns, several approaches protecting IMDs were proposed in the literature. In [1, 5], a 3-tier architecture, which integrates in addition to the IMDs and the programmers, an Authentication Server, was proposed. This server allows authenticating programmers and distributing credentials (useful for establishing secure communication with the IMD). However, these proposals do not provide a practical solution allowing a secure access to IMDs during emergency situations where the user could not be able to provide the credentials to the physician. To cope with this limitation, some approaches introduced the use of a wearable device (Shield [3], Guardian [7]). Such a device allows enforcing the secrecy of the traffic exchange between the IMD and the programmer. Access during emergency situations is enabled by switching off the device. The limits of these solutions are related to the inefficient protection against battery depletion attacks, and the insecure access during emergency.

Because of their crucial role in improving the quality of life of patients, it becomes essential to not only protect IMDs, but also to improve the functions they implement. In particular, to improve the detection of abnormalities, IMDs need to be complemented with a set of wearable sensors to sense the physical activity of the patients, detect the security threats occurring in their vicinity, and improve the responses to the detected emergency situations. Moreover, IMDs need to be remotely accessible by physicians to respond at time to critical health situations. To guarantee the safety of patients carrying them, IMDs need to be supervised and controlled, so that any potential failure could be detected and corrected.

We provide in this research a Smart Healthcare cyber physical system integrating implantable and wearable sensors to increase the efficiency of IMDs in delivering the required therapy and response to abnormalities, detect security threats and attacks from outsiders, enable a remote surveillance of the whole CPS, and forensically generate evidentiary data to promote the forensic investigation of healthcare attacks on these IMDs. In this proposal, the IMD architecture is extended to enable the powerless and secure exchange of data with remote authenticated programmers and applications through a wearable gateway.

The paper contribution is four-fold. First, to improve the efficiency of IMDs in identifying the patients' physical activity and sensing sensitive events crucial for the automated update of the delivered therapy and response, we design a healthcare CPS promoting the communication of IMDs with wearable sensors. Second, we integrate the use of a wearable gateway for protecting IMDs. Such a gateway implements complex security mechanisms that require a lot of computational resources and high energy consumption, including the provision of secure remote access, the detection of attacks, the collection of digital traces, and the forensic investigation of healthcare attacks. Third, a mutual authentication protocol between the gateway and the physician allowing the secure sharing of a session key is also proposed. An Authentication and Authorization Server is involved to alleviate the authentication burden, by taking the responsibility of searching an available physician, checking its authenticity, and ensuring the secure generation and sharing of a session key between himself and the patient's gateway. Fourth, the framework of Incident Response Cognitive Maps is used for the investigation of lethal attacks on IMD based CPS.

The remaining part of the paper is organized as follows. Section II presents the healthcare CPS architecture. In Section III, we detail the security functions implemented within the CPS. Section IV presents the proposed security

N. Ellouze, S. Rekhis and N. Boudriga
Communication Networks and Security Research Laboratory, Tunisia.

approach to secure communication between the CPS, the remote physicians, and the Storage Server. In Section 5, we propose a formal investigation approach of healthcare attacks on cardiac CPS. Section 6 concludes the paper.

II. A smart Healthcare CPS Architecture

Despite the crucial role of IMDs in saving the human life and their importance in the healthcare industry, several limitations can be observed. First, IMDs operate in autonomous manner and poorly interact with the external world (e.g., physicians, hospital) to send alerts, and help remotely handling emergency situations, or even to receive configuration updates from remote physicians. Second, no solutions were developed to remotely and continuously supervise IMDs, detect their unavailability, and predict their potential failure. Third, even if these equipment are able to collect sensitive medical information, they are not linked to any Electronic Healthcare System and therefore they are unable to automatically store the collected data to the patients' medical records. Fourth, a physician, who accesses to the IMD using an external programmer during a consultation, will only be able to examine short-term information due to the resource storage constraints within the IMD. Fifth, even if the IMDs are endowed with embedded sensors (e.g., sinoatrial node rate, blood temperature, posture), the latter are showing some limitations in recognizing the exact activity, motion, and metabolism of the patients to adapt the therapy (one of the pacemakers' issues is how to avoid any mismatch between the patient activity and the delivered pacing rate). This limitation is due to the fact that all the sensors are embedded in the same device and deployed in one location of the body.

The proposed architecture is detailed in Figure 1. A networked implantable and sensors system is deployed inside and around the patient's body to: a) increase the efficiency of the IMD response to the detected health anomalies through the supervision of some parameters and the exchange of the collected data. These parameters include physiological state, body activity, posture, motions, and respiratory activity; b) protect the IMD activity against the external threats through the sensing of events related to the existence of electromagnetic interference and high radiation emission; and c) collect the patients' positions to promote the development of emergency services, to check whether the patient is located in special environments susceptible to generate a high electromagnetic radiation (hospitals, airports, operators' base stations). A Proxy gateway is also designed to be worn by the patient. A healthcare professional, using a programmer or a remote application, cannot communicate directly with the IMD, but needs to communicate with the Proxy gateway, which relays data to the IMD (using a short-range transmission). The gateway communicates also with the wearable sensors to collect the afore cited sensory data, analyze them to detect sensitive events, and generate and deliver notifications to the IMD and the datacenter. Examples of alerts sent toward the IMD are related to modification of the patient's activity or posture, localization in the vicinity of high threat environments, and detection of external physical threats. Upon reception of those data, the IMD can adjust the delivered therapy, or even change its pulsing mode in the case where the patients is behind a strong magnetic signal. In the case where the notification is not related to therapy adjustment, the gateway generates a sound alert together with the notification sent to healthcare professionals.

The gateway has at least two communication interfaces. The first allows it to communicate with a programmer which can be used by the physician during a surgery or consultation to diagnose the equipment or adjust the therapy. The second allows the IMD to remotely communicate with applications and services, so that the CPS can be remotely supervised, critical alerts generated by the gateway can be delivered to remote actors, and instantaneous sensory data can be remotely collected by physicians during emergency. Since several IMDs can be connected to the same gateway to deliver different therapies, the gateway schedules the incoming and outgoing traffic depending on the priority of the source application. The remote requests for diagnosis in emergency situation are granted the highest priority.

III. Securing the healthcare CPS

Recent research in the literature has witnessed security and privacy issues related to the use of IMDs [4], including: the use of weak authentication techniques, the plaintext exchange of sensitive data, the inefficient protection against denial of service attacks, and the lack of secure accounting techniques to promote forensic analysis. Therefore, a patient can be threatened by several adverse events that could potentially lead to fatal heart failures, or even death. Faced to the importance of these security issues, we propose the following security techniques. First, we design a low energy and secure mutual authentication between the programmer and the IMD though the wearable gateway, and a secure pairing of the two equipment. A biometric authentication and key generation protocol based on the use of the patient's electrocardiogram (ECG) signal, is used between the gateway and the IMD. Another type of mutual authentication is used between the gateway and the remote physicians or programmers, which uses public key certificates to authenticate the remote actor. For this, an Authentication and Authorization Server (AAS) is used.

The second security function is related to the powerless exchange of sensitive data between the programmer and the IMD. A Wireless Identification and Sensing Platform (WISP), which allows the powerless execution of computational functions using the harvested energy (from the signal sent by the RFID reader integrated within the gateway), is deployed inside the IMD. The WISP is equipped with a dual access memory, which can be read by the IMD controller, or by the gateway using its RFID reader. This memory allows the IMD and the programmer to powerlessly exchange data and reduce the energy overhead.

The third security function is related to the design of the CPS forensic techniques, so that a further investigation on healthcare attacks would be conclusive. In this context, the gateway securely generates evidence related to sensitive events received from physicians (e.g., therapy modification), and potentially detected external threats. In the other side, the IMD is extended to periodically generate medical records (e.g., EMG data) and digital evidence, and write them to the dual access memory, to be powerlessly retrieved by the gateway. These evidences allows determining how and when the patient's health was deteriorated, the history of

responses taken by the IMD when it detected an arrhythmia, and also sensitive activities (e.g., authentication).

FIGURE 1. SMART CPS ARCHITECTURE

The fourth security function is related to the investigation of healthcare attacks. The proposed system enables the collection of several types of evidence including medical and technical records. A formal technique based on the correlation of the collected evidence, the identification of potential scenarios, and the assessment of their plausibility, is proposed. A library of correlation rules is used to correlate the two types of scenarios to prove whether the health damages are induced by security attack scenarios.

A contextual-aware intrusion detection system capable of linking changes in the patient's environment to the types of detected events is also implemented with the gateway.

IV. Securing communication

We propose an authentication protocol allowing the secure sharing of a session key between the gateway and a remote physician, so that data can be securely exchanged between the IMD and the remote physician via the gateway. We consider two modes: a) emergency mode which is executed when the gateway notices the deterioration of the patient health status and detects that such a health status needs a physician intervention; and b) remote consultation mode which is periodically initiated by the physician to remotely monitor and diagnose the patients' health status.

To prevent security attacks on IMDs, we implement the authentication protocol proposed in [2] between the IMD and the gateway. This protocol allows the secure generation and sharing of a biometric key, which is computed based on the patient's ECG. Thanks to the use of RFID, this protocol is executed without drawing energy from the IMD battery. It is initiated by the gateway, via a synchronization request, for the purpose of secure pairing with the IMD. Upon request reception, the IMD and the gateway simultaneously sample the ECG signal for a predefined period of time, and then generate a set of features from the sample signal using Fast Fourier Transform. Then, the IMD generates and sends the vault (includes a set of chaff points in addition to the computed features which are randomly permuted) to the gateway. After agreeing on the common generated features, a biometric key K_{bio} is computed at both sides. Such a key has a limited lifetime, for that reason this protocol needs to be periodically executed. Once this protocol is executed under the WISP, the IMD starts listening to signal sent over the MICS band by the gateway. This solution prevents battery depletion attacks, as all potential tentative brute-force requests will be executed over the RFID circuitry.

In the sequel, we assume that gateways, prescribing physicians, and the Authentication and Authorization Server (AAS) have each one a private key and an X509 certificate obtained from a trusted authority. The AAS has to manage the access rules associating physicians to patients.

A. Authentication in Emergency Mode

The gateway initiates the authentication protocol to benefit from emergency assistance (remote supervision of the cardiac activity, immediate therapy reconfiguration). As depicted in Figure 2, the gateway sends a signed request to the AAS, that includes crt_G, N_G, and K_{Pub}^{AAS} which are the gateway certificate, a nonce useful to ensure the messages freshness, and the AAS public key, respectively. We denote by $\{\text{-}\}_K$, |, and $Sig_{Priv}(\text{-})$ an asymmetric cryptographic function, a concatenation operator, and a signature function, respectively. Upon request reception, the AAS starts by searching for an authorized physician that can remotely diagnoses the patients' health status (the physician selection considers a set of parameters including the IMD type and the physician availability). After that, it sends to the selected physician a signed authentication request that includes the AAS certificate crt_{AAS}, the physician identity ID_{Ph}, and a nonce N_{S1} encrypted using the physician public key K_{Pub}^{Ph}. The physician responds with a signed message that includes its certificate crt_{Ph} and N_{S1} encrypted. When receiving this response, the AAS authenticates the physician and generates a nonce N_{S2} and a session key $K_{Session}$, which are useful to establish a secure communication between the physician and the gateway that guarantees their anonymity. To share $K_{Session}$ between the gateway and the physician, the AAS sends two signed messages. The first message is directed to the physician and contains the gateway identity ID_G, N_{S2}, and $K_{Session}$ encrypted using the K_{Pub}^{Ph}. The second message is directed to the gateway and includes crt_{AAS}, ID_{Ph}, N_{S2}, and $K_{Session}$ encrypted using the gateway public key K_{Pub}^{G}. Upon the messages reception, the gateway and the physician identify N_{S2} and $K_{Session}$. To initiate a secure communication, the physician sends a request that contains N_{S2} in plaintext followed by ID_{Ph}, ID_G, and N_{S2} encrypted using $K_{Session}$. The gateway authenticates the received request and acknowledges the physician. N_{S2} has to be included in plaintext in exchanged messages to ensure the anonymity of the gateway and the physician. It is used as a session identity that replaces the exchange of ID_{Ph} and ID_G in plaintext.

B. Consultation Mode Authentication

The physician periodically establishes a secure data exchange with the gateway to remotely control the patients' health status. He should authenticate himself to the AAS to share a session key with the gateway. To do so, as depicted in Figure 3, he sends a signed and fresh request to the AAS, which authenticates the physician, identifies the gateway identity, and sends a signed request to the gateway. The latter responds with a signed message. Upon reception of this response, the AAS generates a session key $K_{Session}$ and a nonce N_{S2}, and sends two messages (one to the physician and another to the gateway) to share them. The physician and the gateway identify the received $K_{Session}$ and N_{S2}. To initiate the communication, the physician sends an authentic request to the gateway and waits for acknowledgement.

The traces generated by the gateway, which are related to the sensitive events executed by physician and the IMD responses, need to be stored in a trusted Storage Server (SS)

that ensures the trustworthy, the integrity, and the long-term storage to these traces. To this end, we propose a secure communication protocol between the gateway and SS (See Figure 4). This protocol is initiated by the gateway when there is a secure communication established between the physician and the gateway or/and when receiving sensitive data from the IMDs and wearable sensors. To initiate this protocol, the gateway sends a request to the AAS that contains the SS identity IDSS. Upon reception of this request, the AAS sends a fresh signed message to the corresponding SS and wait for response. After authenticating SS, the AAS generates a session key $K_{Session}$ together with a nonce NS2 and sends them encrypted to both sides (the gateway and SS). The storage server responds with an authentic message that includes the sequence number seq1. Upon message reception, the gateway starts sending data to the SS side. Data are encrypted together with seq_1 and N_{S2} using $K_{session}$. Each time the gateway sends a new message, it increments the sequence number.

Our security solution guarantees the patients privacy. It ensures the confidentiality of the exchanged data, since they are encrypted using an unpredictable session key that has a limited validity period over time. Moreover, due to the use of public key cryptography, this session key is securely generated and shared between the communicating entities. The proposed solution ensures also the patients' anonymity as neither the gateway identity nor the patient identity are transported in plaintext. Those identities are replaced by a session nonce which is securely distributed by the AAS and used to match the traffic to the patient and the physician. The proposed protocols are also resilient to replay attacks, since they implement the use of nonce. In fact, each message integrates the last received nonce to prove its freshness. We also associate a new nonce to every generated session key, so that their freshness could be guaranteed.

In the proposed CPS, the IMD is secured against battery depletion attack (this attack aims to exhaust the IMD battery, so that it will be unable to react to the occurred arrhythmia), since the authentication protocol is powerlessly executed. However, this attack on the gateway side could succeed, by sending successive authentication requests encrypted using forged keys to force the gateway to decrypt those requests and consume intensive energy. We assume that such a behavior could be controlled using threshold-based signatures and reaction rules (e.g., after three false requests, remote access to the gateway can be prevented for a short period of time). This does not introduce a risk to the patient safety or the system availability, as the gateway could be simply replaced and attached to the implanted device using the authentication protocol proposed in [2].

V. Cyber investigation of healthcare crimes on IMDs

Below, we propose a formal investigation technique of lethal attacks on healthcare CPSs aiming to: a) detect occurred suspicious events and executed actions, and generate alerts; b) correlate events and alerts and build a knowledge about the scenario that targeted the CPS; c) extract healthcare scenarios; d) compare these scenarios and assess their impact; e) identify the attack source; and f) generate the suitable reactions and assess their effectiveness.

The evidence collected at the gateway side are: a) EMG anomalies, which include the description of all forms of arrhythmia observed over the generated EMG at the IMD side, together with the timestamp of occurrence; b) Remote supervision actions, which include the event records related to actions executed by the supervision servers or by the physicians; c) Alerts, which represent suspicious events that occur over the environment where the patient is located. These events (e.g., jamming, electromagnetic radiation) may affect the IMD functioning and/or prevent the well supervision of healthcare CPS; and d) IMD reactions which describe the actions taken by the IMD (e.g., defibrillation, cardioversion shock) in response to a non-lethal arrhythmia.

A. *IRPCM based investigation*

We propose to use the Incident Response Cognitive Maps (IRPCM) [6] to investigate healthcare attacks on the proposed CPS. The IRPCM is a framework provided with a graph-based technique for the reassembly of the collected evidence and the identification of the executed events, together with mathematic tools to extract potential scenarios and compare them. The proposed IRPCM allows pathologists and digital investigators to aggregate their experience-based view regarding the investigation of an executed healthcare attack on IMD-based CPS. The reconstructed IRPCM will be composed of nodes (called concepts) and edges that link them. A concept represents one of the different forms of evidence (an EMG anomaly, a remote supervision action, an alert, or an IMD reaction). An edge in the graph, which links two concepts together, has a probability of occurrence and a label describing the relation type, which can be one of the following: a) *p and q are remote supervision actions*: The relation is "< " (temporal precedence), meaning that the remote action p precedes the remote action q ; b) *p is a remote supervision action and q is an IMD reaction*: The relation is "Impact", meaning that the execution of a remote supervision action p has a direct impact on the reaction q taken by the IMD in response to an arrhythmia; c) *p is an ECG anomaly and q is an IMD reaction*: The relation is "lead to", meaning that the occurrence of an arrhythmia p in the EMG, leads the IMD to take action q; or d) *p is an IMD reaction and q is an ECG anomaly*: The relation is "prepare for", meaning that the reaction p taken by the IMD instigated the occurrence of another arrhythmia q. Typically, in such a situation the IMD action is unsuitable, due to a wrong therapy configuration.

The investigator role is to collect the evidence-based concepts from the gateway, and identify the different relations forms that can be appended to link them. For each added edge in the graph, a probability describing the certitude degree of the related relation is appended. Each evidence-based concept appended to the graph will have an activation degree (a probabilistic value describing the certitude of the concept) equal to 1, as it is retrieved from a trusted equipment. As some events occurred on the IMD could be unobservable or undetectable, the investigator can hypothetically append new concepts starting from the previously known attack scenarios, and link them to the graph. These concepts will have an activation degree lower than 1. As evidence-based and hypothetical concepts are directly or indirectly linked through probabilistic relations, the algorithm described in [6] is used to iteratively update the activation degrees. Once the graph is updated, an investigator starts checking if there is a scenario starting

from a concept related to an alert and ending at a concept related to a fatal EMG anomaly. When several scenarios are identified, the investigator can retain the scenario showing the highest degrees of activation of concepts.

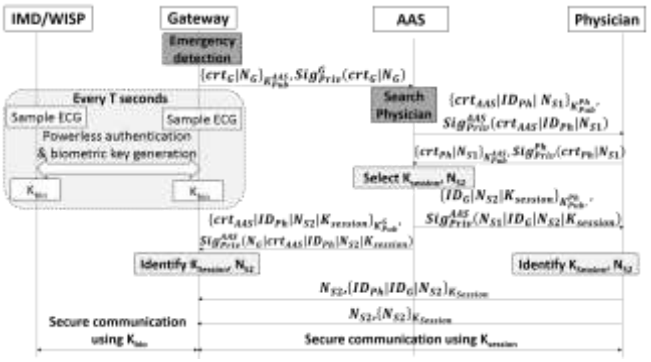

FIGURE 2. AUTHENTICATION IN EMERGENCY MODE

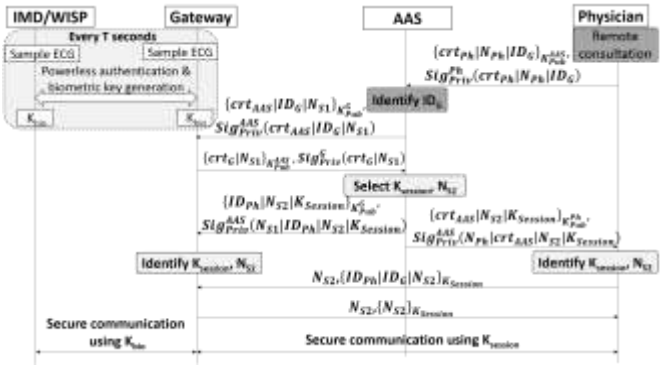

FIGURE 3. AUTHENTICATION IN REMOTE CONSULTATION MODE

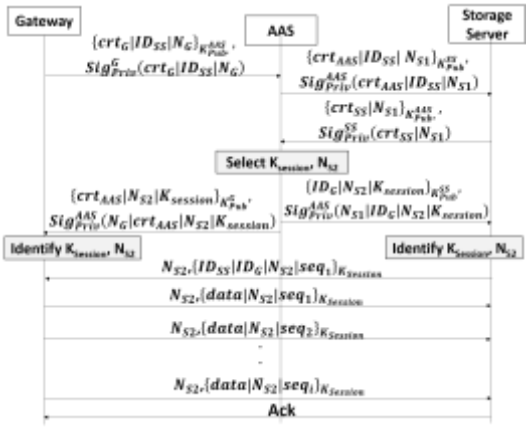

FIGURE 4. DATA STORAGE PROTOCOL

B. *Example of investigation*

We describe in Figure 5 an IRPCM based forensic investigation of a healthcare attack. In this investigation, three ECG anomalies (ventricular tachycardia, ventricular fibrillation, fatal heart), one IMD reaction (cardioversion choc), two remote supervision actions (successful connection, therapy reconfiguration), and one alert (online brute-force) were extracted from the gateway as evidence. After identifying the potential relations between the appended concepts, the following scenario was identified. First, a remote attacker executes an online brute-force attack on the authentication protocol and succeeds authenticating himself to the gateway. After that, he/she reconfigures the IMD by updating the therapy. Later, a cardiac arrhythmia in the form of a ventricular tachycardia happens. The IMD, which detects it, responds by a cardioversion choc. The investigator has realized that such a response is inappropriate due to the previous modification applied on the therapy configuration by the same user. Further to such an inappropriate response, the cardiac arrhythmia was amplified, leading to a Ventricular Fibrillation (VF) to which the IMD does not respond. Few seconds later, the VF induces the death. In this example, the root cause of the death can be attributed to a successful brute-force attack.

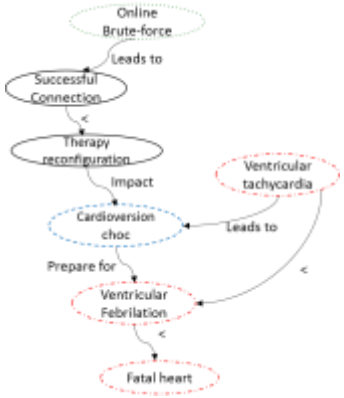

FIGURE 5. EXAMPLE OF AN IRPCM BASED FORENSIC INVESTIGATION OF A HEALTHCARE ATTACK

VI. Conclusion

In this paper, we proposed a Smart Healthcare cyber physical system. A description of the Healthcare CPS system architecture and the implemented security and investigation functions was provided. The proposed authentication protocol between the gateway and the physician allows the secure sharing of session keys and the guarantee of the patients' privacy. We also showed the use of the framework of Incident Response Cognitive Maps for the investigation of lethal attacks on healthcare CPSs.

References

[1] Astorga, J., Astorga, J. C., Jacob, E., Toledo, N., and Higuero, M, Securing access to next generation IP-enabled pacemakers and ICDs using Ladon. Journal of ambient intelligence and smart environments, Vol 6, Issue 2, pp. 157-177, 2014.

[2] Ellouze, N., Allouche, M., Ben Ahmed, H., Rekhis, S., Boudriga, N., Securing Implantable Cardiac Medical Devices: Usee of Radio frequency energy harvesting. In Proceedings of the 3rd international workshop on Trustworthy embedded devices, pp. 35-42, November 2013.

[3] Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu, K, They can hear your heartbeats: non-invasive security for Implantable Medical Devices. In Proceedings of the ACM SIGCOMM 2011 conference, Toronto,ON, Canada, August 2011.

[4] M. Rostami, A. Juels, F. Koushanfar, Heart-to-heart: authentication for implanted medical devices, ACM SIGSAC conference on Computer & communications security, Berlin, Germany, 2013.

[5] Park, C. S., Security mechanism based on hospital authentication server for secure application of implantable medical devices. BioMed research international, vol. 2014, Article ID 543051, 12 pages, 2014.

[6] S. Rekhis, J. Krichene, N. Boudriga. Cognitive-Maps based Investigation of Digital Security Incidents. 3rd International Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE/SADFE2008), Oakland, CA, May 22, 2008.

[7] Xu, F., Qin, Z., Tan, C. C., Wang, B., Li, Q, IMDGuard: Securing Implantable Medical Devices with the external wearable guardian. In Proceedings of the 2011 IEEE, INFOCOM, China, April 2011.