*International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868*
*Foundation of Computer Science FCS, New York, USA*
*Volume 5– No.6,April 2012 – www.ijais.org*

# IMD-IDS a Specification based Intrusion Detection System for Wireless IMDs

Monika Darji
L.J Institute of Computer Application
Ahmedabad, India

Bhushan Trivedi
GLS Institute of Computer Technology
Ahmedabad, India

## ABSTRACT

Implantable Medical Devices (IMDs) have emerged as a break-through technology for e-healthcare. Healthcare providers use wireless medium of communication to monitor patients, perform diagnostics and download data in hospitals or from homes. This provides great convenience, flexibility, cost effectiveness and timely patient care. These implanted devices contain sensitive personal data and other health related information and are controlled through commands issued by healthcare staff wirelessly. Wireless medium of communication introduces several vulnerabilities which if exploited might have severe implications on the security, privacy and safety of patients using IMDs. In this paper we aim to discuss the security and privacy issues for wireless communication of Implantable Medical Devices and come out with a threat model. We also look into the methods proposed in literature to mitigate them and analyze their suitability. Intrusion Detection has gained importance over the years especially for wireless adhoc networks. Seeing the importance of constantly monitoring the IMD-reader communication in detecting and deterring security attacks, we propose a model called IMD-IDS to be integrated with cellphone or PDA, which people can carry with them. The IMD-IDS manages IMD keys, authenticates IMD readers, and blocks attempted accesses to the patients IMD from unauthorized readers using specification based intrusion detection. It monitors the communication between IMD-reader for detecting malicious activities and help patients to take corrective actions if need be. This research is the first effort to apply specification-based detection techniques to detect attacks in the IMD wireless communication.

## Keywords

***IMDs, security and privacy, threat modeling,IDS***

## 1. INTRODUCTION

Implanted Medical Devices are electronic devices designed to be implanted within the patient's body to monitor chronic illness and provide automatic therapies. IMDs include pacemakers, implantable cardioverter defibrilators (ICDs), neurostimulators, and implantable drug pumps. They can control heart rhythms, monitor hypertension, provide functional electrical stimulation of nerves, operate as glaucoma sensors and monitor bladder and cranial pressure. IMDs generally perform four activities which are Sensing to collect information from the body, Actuating to produce some therapeutic effect, Information processing to perform some computation using collected or communicated information and Communication with other IMDs, external devices or patient [8]. The increased use of wireless technology for communication in medical facilities and the wireless utilization of Medical Devices make it possible for healthcare staff to access medical information from anywhere and provide diagnosis and treatment. But this also makes patients and medical facilities prone to new security and privacy vulnerabilities. According to Health and Human Services (HHS), a major concern to the Healthcare and Public Health (HPH) Sector is exploitation of potential vulnerabilities of medical devices on Medical IT networks (public, private and domestic). These vulnerabilities may result in possible risks to patient safety and theft or loss of medical information. Implantable devices have wireless transmitters and receivers, which enable health-care providers to perform diagnostics, send commands and to download telemetry data using an external reader/programmer. Wireless medium of communication raises privacy and security issues for patients. IMDs if not protected against malicious attacks, may render patients vulnerable to attacks that can disable an IMD or induce a life-threatening condition using it [2 and 3]. Moreover Medical information technology networks are now remotely accessible through the Medical Devices which may be connected to the internet. Therefore it is essential to secure the communication to protect against theft of medical information and malicious intrusion. In this work, we survey the security and privacy challenges arising due to IMDs wireless interfacing and also explore the solution space and provide a comparison of the proposed solutions. From our survey we derive a threat model for IMDs which can be used as for future references. The rest of the paper is organized as follows. Section II discusses the key security objectives and security challenges of IMDs, section III discusses the Vulnerabilities in IMDs, provides threat modeling and surveys methods proposed in literature to achieve Security and Privacy goals, section IV provides proposed specification based IDS to monitor IMD and reader communication, section V concludes the paper by giving some future directions.

## 2. KEY SECURITY OBJECTIVES AND SECURITY CHALLENGES OF IMDS

Due to wireless medium of communication, unauthorized person can eavesdrop on medical telemetry data or gain control of IMDs operation and issue commands to disable its therapeutic services which may endanger patient's safety, security and privacy. They may explore privacy vulnerabilities by exposing patient's data to an unauthorized party. Therefore it is essential to secure the communication to protect against theft of medical information and malicious intrusion. Level of impact on Medical Facility or on a patient should there be a breach of Security and privacy is High (FIPS 199) and has drawn immediate attention.

### 2.1 Key Objectives of IMDs Security

The fundamental key objectives of security aligned with IMDs are mentioned below:

**Data Confidentiality and Privacy:** Private or confidential patient data should not made available or disclosed to unauthorized individuals during storage periods or during transmission to-and-fro IMDs. Patients must have control on what information related to them may be collected and stored by the health staff and to whom that information may be disclosed.

**Data and Command Integrity:** Patient related data is vital and modified data would lead to disastrous consequences therefore data must be changed only in specific and authorized manner. Unauthorized manipulation of the data during storage or transmit must be detectable and preventable. Integrity must be ensured in the commands issued to the IMDs by healthcare staff as it dictates the state of IMD.

**Availability:** IMD is not vulnerable to any attack like battery depletion which renders it unusable or attacks which shuts it down. It should perform its functionalities seamlessly.IMD works promptly and access is not denied to authorize healthcare staff as failure to retrieve data may become a life threatening matter for patients.

**Authenticity:** Authentication of the health staff and programmer and assurance that each data or control input is coming from a trusted source.

**Accountability:** Actions of user of programmer can be traced uniquely to support non-repudiation, instill deterrence, fault isolation, intrusion detection and prevention, and legal action.

## 2.2 Challenges in Securing IMDs

IMDs security is complex and difficult to achieve because of the following reasons:

Stringent resource constraints of IMD's battery (power), processor (computation), memory and storage require the security mechanism to be as light weight as possible, ideally drawing no energy from these devices.

The fact that these devices are implanted inside patient's body and replacement require surgery need the security mechanism to be robust and non-interfering with treatment.

Security mechanisms must not be vulnerable causing attacks on security features by exploiting some unexpected weakness.

To ensure legitimate access to patient's data in emergency situations, security mechanism must be context-aware, flexible and possess fail-open access property for patient's safety.

The physical placement of the security mechanism (eg external, internal, wearable, installed on IMD), and logical placement i.e. on which layer of communication protocol, is important for its usability, applicability and acceptability by IMD users.

Security mechanisms typically require creation, distribution, revocation and protection of secret information(keys) which is a huge concern.

The security mechanism should have low false positives and false negatives.

The increasing size and complexity of the software used in IMDs is another key concern in security and privacy research [3]. Software complexity combined with wireless communication can lead to an emergent risk of malware.

As there are many types of implantable devices which have different functionality and way of working, it is difficult to design a security solution that fits all.

# 3. Vulnerabilities in IMDs, Threat Modeling and IMDs Security and Privacy Solutions

## 3.1 Vulnerabilities in IMDs

Security researchers have identified a number of vulnerabilities in IMDs which are mentioned as follows:

Lack of Encryption [2]

Poor access control/lack of authentication [10]

IMD devices are battery powered attacks may target battery consumption [2]

Poor input validation [10]

Wireless Interfaces [1]

## 3.2 Threat Modeling

Security attacks are action of adversaries which compromises the security of the IMDs communication and can be classified as active and passive attacks.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions and are much difficult to detect. Given below are the types of passive attacks:

**Release of Message Contents:** A passive adversary may eavesdrop on the wireless communication sent to the IMD to learn private information by using off the shelf software and hardware. This could compromise medical telemetry data and patient's data privacy [2].

**Traffic Analysis:** Even if the transmission of IMDs is encrypted on radio links, an opponent still might be able to observe the pattern of these messages and determine the location and identity of communicating parties.

Active Attacks unlike passive attacks involve modification of the data stream or creation of a false stream and are of following types:

**Masquerade:** A programmer/reader pretends to be an authorized entity and gains extra privileges by impersonation and can steal, modify patient data from IMDs or issue undesirable commands.

**Replay:** Involves passive capture of radio transmissions and replaying the recorded control commands later on to control or disable therapies.

**Modification of Messages:** An adversary may reverse engineer the communication protocol to understand its operation and send malicious data and instructions to it.

**Denial of Service:** An attack which drains IMD's battery may lead to its malfunctioning and lead to replacement by surgeries.

## 3.3 IMD security and privacy solutions

Some security approaches that were proposed in literature to meet the security and privacy goals of IMDs are given below:

### *3.3.1 Confidentiality Based Approaches*

**Access Token based approach** [11]: Medical staff accesses the IMD using the access token which can be a USB stick or bracelet configured with secret key, to establish a secure link to download data and send programming commands. These access tokens needs to be protected from theft, if lost or stolen or forgotten, it creates a safety problem by rendering the IMD inaccessible.

**UV-visible Tattoos** [6]: Password was proposed to be tattooed as ultraviolet-ink micropigmentation, adjacent to the point of implantation as a UV-visible 2D barcode which are invisible under normal light. Devices that interact with IMD must be equipped with ultraviolet light emitting diode (UV LED) and an input mechanism for key entry. This technique mentions the risk of infection for patients from micropigmentation and the risk that a tattoo could be rendered unreadable when needed.

### *3.3.2 Access Control Approaches*

**Use of proximity-based access control** [4]: This scheme uses proximity-based device pairing protocol based on ultrasonic distance bounding which allows access to only those devices which are in close proximity. This technique enables the IMDs to predefine an exact range for granting access and prevents the attacker from accessing the IMD from distance regardless of the type of transceiver he has. IMD can operate in two different modes, in normal mode, the reader needs to be in possession of a shared key to access the IMD and in emergency mode reader just needs to be within certain security range. The drawbacks are that it requires and assumes ultrasonic distance bounding features to be implemented on IMD, ultrasonic distance bounding is vulnerable to RF wormhole attacks, further in case of noisy channels, for the reader to interpret the received bits before replying to the device may cause long processing delays. Impersonators may make the device run this protocol by repeatedly sending 'hello' message and thus denying access to the actual reader.

**Patient Notification and Access Control using Batteryless Proxy** [2]: This security system consists of an external device (battery less proxy) that is used by medical staff and does not involve patient participation. When placed in contact with the patient, the device negotiates a temporary key with the IMD through the patient's body by acoustic signaling thereby gaining permission to access the IMD. Zero-power notification harvests induced RF energy to wirelessly power a piezo-element that audibly alerts the patient of security-sensitive events at no cost to the battery. Zero-power authentication that uses symmetric cryptographic techniques to prevent unauthorized access; it aims to protect against adversaries who have custom equipment. Sensible key exchange combines techniques from both zero-power notification and zero-power authentication for vibration-based key distribution that a patient can sense through audible and tactile feedback. This technique does not address the problem of key management, renewal and revocation and key exchange may be susceptible to eavesdropping.

### *3.3.3 External Devices Based Approaches*

No modification is done in the IMD device therefore more feasible for already implanted IMDs.

**Using Communication Cloaker** [9]: A removable device called communication cloaker, defensive countermeasure that controls access to the IMD by making it invisible to all unauthorized queries. This device provides security when worn by the patient, makes IMD acts on commands sent by only authorized medical staff, encrypts all communications to and from the IMD and checks them for authenticity and integrity. When the cloaker is removed, it provides fail open access to all external programmers. In this way emergency medical staff can access a patient's IMD even if the wristband is lost or destroyed in an accident. It shifts power-intensive computation and some of the protection mechanisms to a cloaker outside the patient's body and thus reduces battery consumption.

**Physical layer Solution using Shield** [7]: This scheme delegated the security of an IMD to a personal base station called the shield. The shield act as a jammer-cum-receiver to jam the IMDs messages and unauthorized commands preventing others from decoding them while being able to decode them. Selective radio Jamming has a number of problems. First, its use is legally questionable, since it is conceivably a form of signal war-fare. Secondly, malicious readers can abuse Selective Jamming by repeatedly performing unauthorized queries. This Denial of Service attack would cause both a furry of jamming signals, and a major drain on the battery of the Sheild.

## 4. PROPOSED SOLUTION: IDS FOR IMDs

In this paper, we suggest a new approach for personal security management of IMDs called the IMD-IDS. The IMD-IDS is integrated into Personal Digital Assistants (PDAs) or cellphones, to manage and control the security of IMD.

### 4.1 The need for IDS

It is apparent from the above discussion that lack of security between IMD and IMD readers may lead to undesirable situations like unauthorized data collection, where attackers gather illicit information by either actively issuing queries to IMD or passively eavesdropping on existing IMD-reader communications. They may also issue commands to an IMD to make it shut down. Moreover, it has been reported in a recent work that even using encryption is insufficient to protect the confidentiality of patient telemetry [2]. Data packet timing information and headers distinguish the types of medical and monitoring devices even if traditional cryptographic mechanisms are used. Data compression technology further exposes encrypted telemetry to cryptanalysis. The techniques to mitigate these security and privacy risks in wireless telemetry between IMD and reader/programmer require extra energy, computation and bandwidth from the medical device. Preventive measures like encryption and authentication while providing security still falls under prey of a an attack if the reader itself is compromised.

Intrusion Detection System identifies malicious activity and acts as a second line of defense[13]. It can continuously monitor the IMD-reader communication for unusual activity, and take preventive measures which may involve issuing alerts or blocking a suspected connection by using jamming techniques. Intrusion detection can be classified into three broad categories: anomaly detection, signature or misuse detection, and specification-based detection. Anomaly detection recognizes deviations from normalcy by building models of normal behavior. Any deviation from normal is identified as an attack. Misuse detection use patterns of

known attacks to recognize intrusions. Specification based detection detects attacks with use of a set of constraints (rules) that define the correct operation of a program or a protocol. Misuse detection has high detection accuracy and low false alarm rate for known attacks, but it is unable to detect novel attacks whose signatures are unknown. Anomaly detection is able to detect unknown attacks. However, anomaly detection techniques also produce a high degree of false alarms. Specification-based detection engines share the advantages of signature-based and anomaly-based detection, since they can detect unknown attacks, without the side effects of high rates of false positives.

## 4.2 Intrusion Detection

**Specification-based detection:** The proposed light-weight detection engine is deployed as IMD-IDS running on a cellphone/PDA and performs detection using a set of specifications, which describe the correct operation of the communication protocol between IMD and reader. The proposed engine introduces a number of significant advantages since it can effectively detect both known and unknown attacks in real time and with minimum overhead. Moreover, its deployment requires no modifications in IMD, Reader or communication protocol. Specification-based engine relies on a set of constrains which specifies the correct operation of communication protocols and monitor the execution of IMD-Reader communication with respect to these constraints. Specification-based engines can detect both known and unknown attacks. Moreover, they avoid high rates of false alarms, since they do not rely on normal profiles, as in case of anomaly detection.

**Assumption:** The proposed technique assumes that readers are authenticated by IMD during communication and includes its ID and authentication information which cannot be forged. The communication between IMD-Reader is encrypted.

## 4.3 IMD-IDS

The IMD-IDS runs on patient's cell phone/PDA and IMD store reader's IMD access pattern, such as reading frequency and the previous time of each action. IMD-IDS is meant to be used for non-emergency condition.

During the non-emergency condition, most actions should have a pre-determined frequency and this information can be used to develop specifications.

The engine performs detections using a set of specifications, which describe the correct operation of the IMD-Reader communication protocol. These specifications are expressed through the use of a Finite State Machine (FSM). Each state of FSM corresponds to either a legitimate or malicious behavior of the monitored reader and a transition from one state to another is triggered by the readers's operations and actions. The proposed engine introduces a number of significant advantages since it can effectively detect all the types of attacks (both known and unknown) that occur at real time and with minimum overhead. Specification based detection are similar to anomaly detection as they detect attack as a deviation from normal and are based on manually developed specifications that capture legitimate system behavior. In general, development of detailed specifications can be time consuming. But as the communication between predefined and follow a fixed pattern, it is not the case here.

The first step is to develop specifications of IMDs and readers in terms of packets received or transmitted by them. An IMD comprises a wireless receiver configured to communicate wirelessly with an external transmitter of an external reader or programmer via a plurality of communication channel having different frequency within a frequency band. IDS monitor the RF communication between IMD and reader.

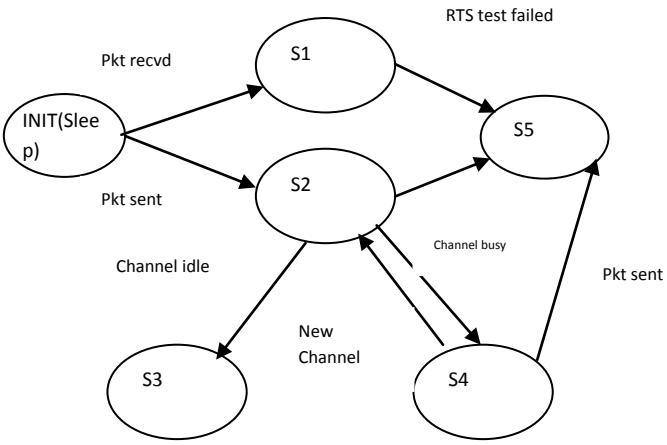


**Fig 1: Architecture of the proposed specification engine**

### *4.3.1 Finite State Machine Language*

We use an FSM. Formally, specifications are defined as a tuple (S, NO, S0, δ, F), where S is the set of all possible states; NO is the set of reader operations; S0 is the initial state; δ is a function that maps node operations from a previous state to the current state; and F is the set of final states that correspond to malicious behaviors. We divide the specifications into three set according to the IMD-Reader communication condition: (a) idle, (b) transmitting, or (c) receiving data. Figure 1 shows the architecture of the proposed specification engine with different states.

### *4.3.2 Sleep State Specification*

These specifications describe the operation of the IMD is in sleep state (i.e IMD is not receiving or transmitting any packet). The engine initializes at state S0 and begins monitoring the IMD for any new packets that is transmitted to and from IMD. If the monitored IMD receives a communication request, then the engine moves to S1. On the other hand, if IMD initiates transmission, the engine moves to S2.

### *4.3.3 Receiving Specification*

If the monitored IMD receives a communication request, then the engine moves to S1.The IMD performs authentication to verify the reader before transmitting data or taking commands.If an unauthorized reader repeatedly tries to connect with an IMD, it would cause the IMD perform multiple authentications and hence waste a lot of battery power. In battery depletion attack, several packets will be sent by reader to IMD, IDS engine will track Number of packets relayed by reader to IMD in last T seconds and use this statistics to detect attack and raise alarm.

To defend against the DOS attacks, we use random assessment delay (RAD) technique and a simple packet dropping mechanism which is used in literature to curb DOS attacks which occur by flooding the network with RREQs.

Upon sniffing a new connection request packet for IMD, IMD-IDS keeps track of redundant packets received over a short period of time, ≤ 200 milliseconds. If the number of redundant requests exceeds a preset count, then connection/ authentication request is jammed and/or an alarm is raised. The proposed technique uses statistical analysis to detect misbehaving readers and reduces their impact on IMD performance.IMD-IDS monitors the connection/authentication request issued by reader to IMD and maintains a count for each reader during a preset time period ($\delta\tau$ ). At the end of the time period, the IMD-IDS compute the rate at which it has been receiving connection/authentication requests from each reader using (1)

$$rate_i = CREQCount_i / \delta\tau \quad (1)$$

If rate is beyond a preset threshold, engine moves to S5 which designates a malicious behavior an alarm is raised.

RAD is simple to implement and redundant broadcast count can be checked at the MAC layer level prior to transmitting

### *4.3.4 Transmitting Specification*

When monitored IMD attempts to transmit telemetry data to reader, the engine moves to S2. At this state, the engine checks if the communication channel is idle or busy. If the channel is idle, then the engine moves to S3; otherwise, if the channel is busy, the engine moves to S4. In S3, the expected behavior of the protocol is to transmitting an Telemetry packet, while in S4 the protocol must change the channel. An attempt to transmit any data when the channel is busy leads to the final state S5, which designates a malicious behavior.

### *4.3.5 Response*

IDS will observe the readers probes, will identify them as suspicious, may actively block the attacker's access to the IMD by jamming the communication between IMD-Reader, and will alert/place a phone call security personnel who can then take appropriate actions to block subsequent access by the attacker.

## 5. CONCLUSIONS AND FUTURE DIRECTIONS

We described the IMDs security and privacy concerns and derived a threat model for future references. We also explored the solution space for mechanisms based on encryption, access control, trusted external devices and compared these techniques. We found a lack of effective protection and detection mechanisms for security in IMDs which can be provided using Intrusion Detection Systems and Firewalls. We proposed Specification based Intrusion Detection System that can be used as a second line of defense to detect and prevent attacks and perform risk assessment by monitoring for suspicious activity on IMDs. The future direction that we would like to explore is introduction of context sensitiveness in developing specifications for Intrusion Detection for IMDs.

## 6. REFERENCES

[1] Halperin, D., Heydt-Benjamin, T.S., Fu, K., Kohno, T., Maisel, W.H. , "Security and Privacy for Implantable Medical Devices," in IEEE Pervasive Computing, vol. 7, pp. 30–39 (2008)

[2] Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W.H. , "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in IEEE Symposium on Security and Privacy (2008)

[3] Israel, C.W., Barold, S.S. , "Pacemaker Systems as Implantable Cardiac Rhythm Monitors," in American Journal of Cardiology (2001)

[4] Rasmussen, K.B., Castelluccia, C., Heydt-Benjamin, T.S., Capkun, S. , "Proximity-Based Access Control for Implantable Medical Devices," in ACM Conference on Computer and Communications Security (2009)

[5] Fu, K. , "Inside Risks, Reducing the Risks of Implantable Medical Devices: A Prescription to Improve Security and Privacy of Pervasive Health Care. ," in Communications of the ACM, vol. 52(6), pp. 25–2` (2009)

[6] Schechter, S. , "Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices," in USENIX Workshop on Health Security and Privacy (2010)

[7] Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu, K. , "They Can Hear Your Heartbeats: Non-Invasive Security for Implanted Medical Devices," in ACM SIGCOMM (2011)

[8] Jeremy A. Hansen and Nicole M. Hansen. , "A taxonomy of vulnerabilities in implantable medical devices. In Proceedings of the second annual workshop on Security and privacy in medical and home-care systems," in (SPIMACS '10). ACM, New York, NY, USA, 13-20.

[9] T. Denning, K. Fu, and T. Kohno. , "Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security," in HotSec, 2008.

[10] Steven J. Templeton. , "Security aspects of cyber-physical device safety in assistive environments," in proceedings of the 4th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '11). ACM, New York, NY, USA.

[11] S. Bergamasco, M. Bon, and P. Inchingolo. , "Medical data protection with a new generation of hardware authentication tokens," in Mediterranean Conference on Medical and Biological Engineering and Computing (MEDICON), pages 82–85, Pula, Croatia, 2001.

[12] S. Schechter. , "Security that is meant to be skin deep:Using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices," in Technical Report MSR-TR-2010-33, Microsoft

[13] Panos, Christoforos; Kotzias, P.; Xenakis, C.; Stavrakakis, I., "Securing the 802.11 MAC in MANETs: A specification-based intrusion detection engine," Wireless On-demand Network Systems and Services (WONS), 2012 9th Annual Conference on , vol., no., pp.16,22, 9-11 Jan. 2012

[14] Desilva, S.; Boppana, R.V., "Mitigating malicious control packet floods in ad hoc networks," Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp.2112,2117 Vol. 4, 13-17 March 2005