CHAPTER – 2

Threat Modeling

2.1 Introduction

A literature survey of the existing body of work is essential during the entire process of doctoral work. The first phase of Literature survey was conducted to identify the broad research gap by referring to the research work that emphasizes on securing IMDs and also demonstrated attacks. This chapter is the outcome of the initial literature survey which helped us to derive a threat for IMDs as an outcome.

2.2 Threat Model

Recent security research has provided evidences that IMDs fail to meet the standard expectations of security for critically important systems. Ensuring security of wirelessly communicating IMDs is a critical issue as they perform life-critical or health-critical functions. Careful design of security technique either from scratch or by modifying existing techniques is the need of the hour. But before designing a security technique, the problem should first be clearly defined and the threats against which they will operate identified. A threat model is needed to adequately specify the security requirements. Our goal is to determine the threats that are of concern and should be defended against by proposing a comprehensive threat model for IMDs.

Threat modeling[35, 36] is the process of analyzing a software system for vulnerabilities, by examining the potential targets and sources of attack in the system. It has following benefits:

1. It prioritizes types of attacks to address.
2. It helps mitigating risks more effectively.
3. It helps identifying new potential attack vectors and vulnerabilities.

4. It adequately specifies security requirements

We find a lack of complete threat model for IMDs in literature. To address this gap, in this chapter we provide with a comprehensive threat model for IMDs which unifies previous work and discusses vulnerabilities and threats for wirelessly communicating inter-networked IMDs.

2.3 Related Work

There is a body of work which we referred and which identifies privacy and security vulnerabilities, threats and attacks and also indicates the mitigation steps. Following are the related work which emphasizes on security for IMDs:

In [16] tensions between design goals of wireless IMDs viz. security, safety, and utility is studied and it is stated that security and privacy goals of IMDs should to be in tandem with safety and utility.

In [14] attacks on confidentiality, integrity and availability of Implantable Cardiac Defibrillator (ICDs) are demonstrated and through reverse engineering it is shown that ICD discloses private information like patient name , hospital name and medical condition in plain. IMDs can be made to talk to unauthorized devices and commands may be replayed which may affect the functioning of these devices. These ICDs poses a risk of denial-of-service due to battery depletion when forced to communicate indefinitely with unauthorized party.

In [37] security issues of IMDs are described and major challenge of severe resource constraint is mentioned.

A survey [38] draws attention to technological approaches for improving IMD security and privacy including judicious use of cryptography and limiting unnecessary exposure to attackers. According to them premarket approval for IMDs should explicitly evaluate security and privacy and manufacturers should not rely on security through obscurity.

In [39] it is mentioned that networked IMDs have potential to communicate with other IMDs and establish complex feedback loops, such that attack on one IMD can affect others. It classifies vulnerabilities by their scope, level of access gained if exploited, cause (proximity, IMD activity, and patient state), result of exploitation (component affected, permanence). Also describes the protective, corrective, and detective countermeasures.

In [40] it is stated that along with security and safety, user acceptance, user environment, resource constraints, clinical effectiveness are also important factors for designing a security system. It categorizes security challenge through risk based analysis for Insulin Pump, Glucose Monitor and Continuous Glucose Monitor.

Work in [27] summarizes the recent work on IMD security. It identifies two classes of vulnerabilities. One is control vulnerability which includes unauthorized person gaining access and control of the IMD. Second is privacy vulnerability in which IMDs exposes the patient data to unauthorized person. It classifies the IMDs as open loop, closed loop and biosensors and enlists the threats for these classes. It classifies adversaries as passive having access to listening devices and active with the ability to generate radio transmissions. Such adversary may perform binary analysis by inspecting compiled code.

In [41], an overview of the trend of embedded devices is presented, with a case study of wearable and implantable medical devices and discussion on the vulnerabilities, security challenges and steps towards addressing them.

In [42] it is stated that security and privacy risks of medical device should be addressed at manufacturing phase itself to make them safe and effective. The risk of malware, use of old software versions and upgradability issues may lead to diminished integrity and availability.

It [43] shows possibility of subtle eavesdropping and injection attacks on sensor inputs which form the primary source of data for IMDs for making actuation decisions.

In [44] authors observed that poor security design can result in real vulnerabilities impacting the privacy, integrity and availability of the device.

In [45], author discusses the trustworthiness of medical devices and categorizes the solutions available for radio attacks as: (i) those proposing close-range communication to authorized devices, (ii) the introducing cryptography in IMDs and (iii) the use of external devices to support security processing for IMDs. [46] is a survey of security techniques relevant for IMDs.

A recent survey [47] enlists three categories viz. telemetry interface, software, and sensor interface layers in which security threats needs to be addressed.

In [48] author examines privacy related threats, and classifies them as identity threats (misuse of patient's identity), access threats (unauthorized access of patient health information) and disclosure threat (unauthorized disclosure of patient private health

information).Such is the seriousness of the issue that The U.S. Federal Drug Administration (FDA) has recently called for manufacturers to address cyber security issues relevant to medical devices [49].

In [50] access control approaches for IMD and three intra-body secret keys exchange techniques viz. acoustic, electric, and electromagnetic signals are surveyed.

2.4 Vulnerability and Threats in Existing IMDs

In absence of security association between IMD and external devices, we found multiple vulnerabilities that IMDs become exposed to. These vulnerabilities of IMDs are susceptible to exploitation by attackers leading to threats of different impact. A comprehensive list of vulnerabilities and resulting threats and demonstrated attacks by security researchers are presented in Table II.

TABLE 2.1 Vulnerabilities and Threats in IMDs

Vulnerability	Threat	Justification
Magnetic switch based access	Tampering with device settings;Unauthorized changing or disabling of therapies, continous wake-up calls to device	Attack on authentication using out-of band channels like audio, video or tactile is presented in [51]
Wireless mode of communication	Loss or disclosure of sensitive information; Traffic Analysis; Wireless Jamming ;Replay of older commands	An attack against an ICD using a software radio can deliver untimely defibrillation (shock) [14].
Networked IMDs	A compromise on one IMD may affect others; Distributed Denial of Service attack	Demonstrated theoritically in [41]
Limited or nonexistent authentication	Unauthorized telemetry access and commands; Denial of Service	Use of USB device to control the insulin pump's operations by intercepting wireless signals sent between the sensor device and the display device on BG monitors and to display inaccurate readings by knowing just the serial number [52].
Limited battery, storage and processing capacity	Battery Depletion; Inability of performing security related processing	Battery depletion demontrated in [48]
Wirelessly Programmable	Sophisticated attacks; Zero day attacks; reprogramming attacks without close proximity	Reprogramming attack demonstrated in [38]
Software and	Buffer overflow attack, Side Channel	Singnal injecton attack demontrated in

firmware design without considering security	Attack, Malwares ;Binary Analysis, Device Malfunction; Injection attacks	[43]
Telemetry without encryption	Harvesting Privacy Information	Eavesdropping demostrated in [28]
Granting access without authentication and authorization	Tampering with device settings;Unauthorized changing or disabling of therapies; MITM	Fatal attacks on Insulin Pump System like disabling the device alarm and delivering of a lethal dose were also demonstrated[52].
Tradeoff between security and safety	Inability to enforce stringent security measures to cater to immediate access during emergency.	Consequences demonstrated in [53][27[80]
Remote accessibility	Masquerade, MITM, DOS; Repudiation	Man-in-the-middle attack was demonstrated on a Bluetooth-enabled pulse-oximeter system in [54]

2.5 A Hypothetical Attack Scenario

To help visualize the security attacks on IMDs, we are taking a hypothetical scenario as shown on Fig 2.1.

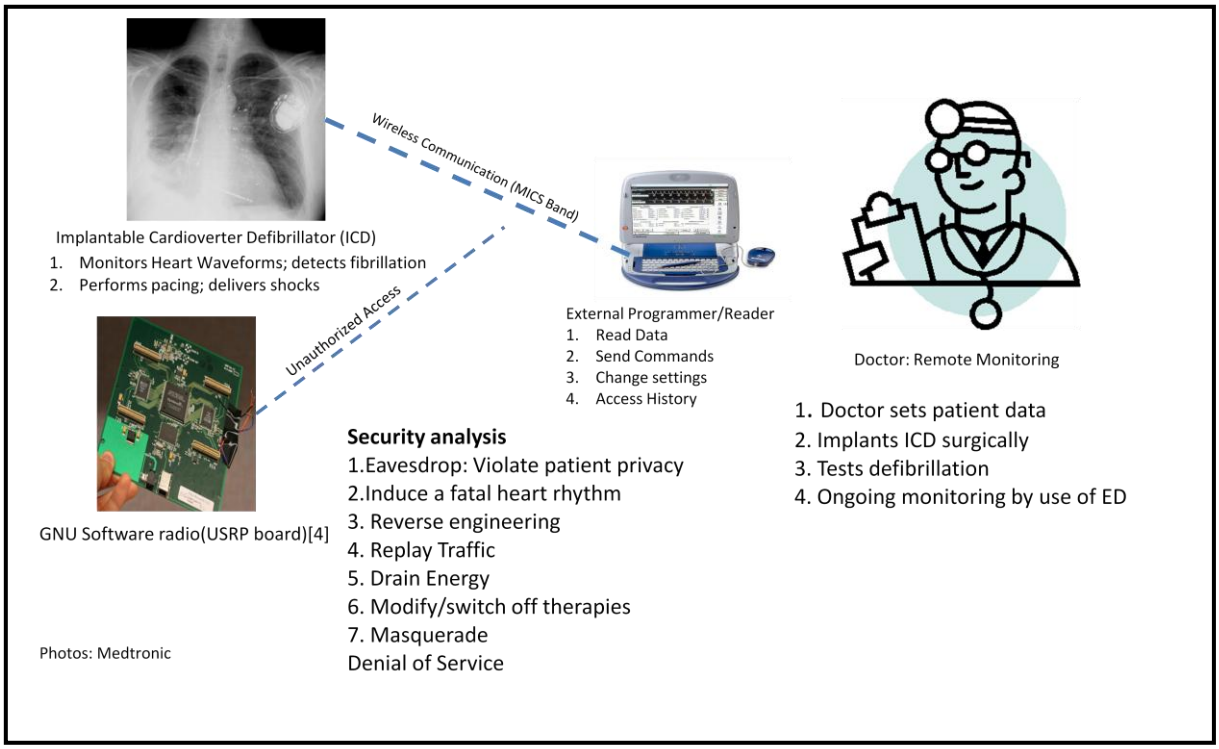

FIGURE 2.1 A Hypothetical Attack Scenario

A doctor sets patient data in the ICD during surgerical implantation into human body. He tests defibrillation to ensure that the device is working properly. Now onwards doctor performs monitoring by means of wireless channel by using an external programmer or reader. The external device reads data, sends commands to the device, changes settings to modify therapy and may also access the patient's history. An attacker may use GNU software radio or other off-the-shelf devices to perform unauthorized actions like eavesdropping to violate patient privacy. From the captured packets, attacker may reverse engineer the device ID and other information pertaining to patient [14], induce a fatal heart rhythm, replay recorded commands, drain energy of IMD battery, modify or switch off IMD therapies, masquerade or pose denial-of-service.

2.6 Adversarial Model

Threat modeling for IMDs presents significant challenges due to unavailability of these devices for security researchers to conduct experiments. In this section, we mention the attack sources, specify our assumptions, and present the threats that arise due to the insecure wireless communication and networking of IMDs. We provide a comprehensive listing of vulnerabilities and threats and then make use of Microsoft's threat modeling tool to generate threat model analysis report. As shown in Fig 2.2, adversaries are mainly classified as passive that perform a passive attack like eavesdropping or traffic analysis or active that has the capability of performing one or more active attacks.

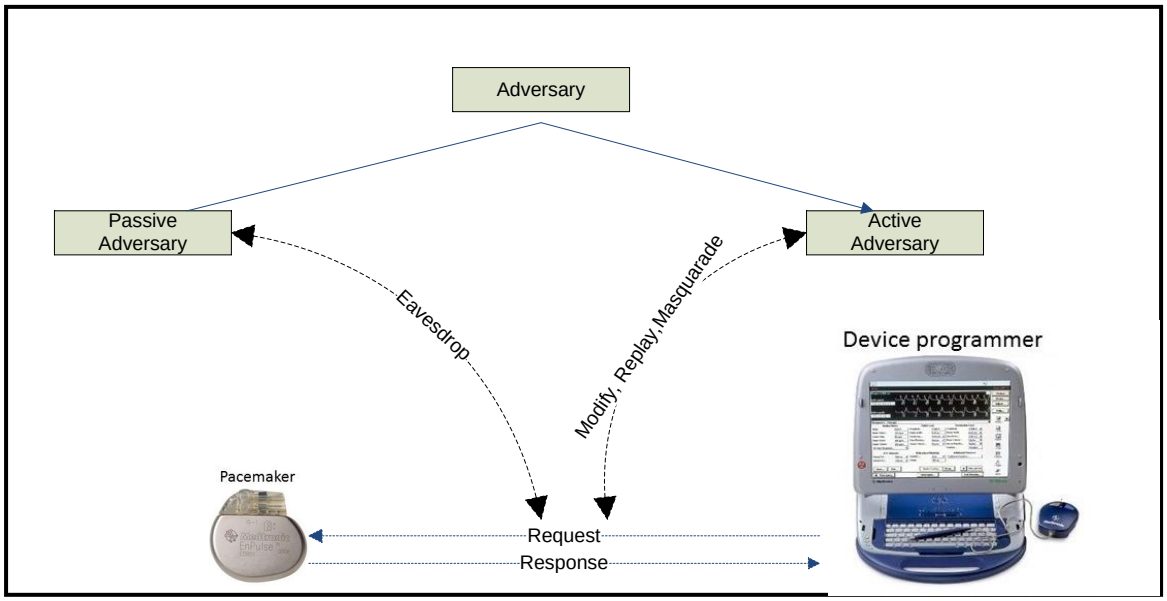

FIGURE 2.2 Types of Attackers

Different classes of Adversary that can be a passive or an active attacker and can harm the system are:

1. Insider: Such an adversary is a legitimate part of the system and therefore most difficult to identify. A patient himself my tamper with the data to fool insurance agencies.
2. Software Cracker: Such an adversary may gain control of IMD of similar make and reverse engineer the firmware to gain a lot of details.
3. Jammer: Such an adversary may perform jamming to hamper the wireless communication.
4. Rouge Device Owner: Such as adversary may own similar devices which communicate in MICS band and make the rouge device part of the network.

Table 2.2 Classification of Adversary

Adversary Type	Action	Equipments Used	Impact	Security Service
Passive	Eavesdrops radio communication	Oscilloscope, software radio, directional antenna	Compromises Confidentiality	Data confidentiality
Active	Generates false radio transmission or manipulates, replays stale commands	Programmable Radios	Disabling of therapies, injecting excessive dosage, changing interpretation , shutting down or changing IMD behavior	Integrity Assurance, Authentication, Replay Resilience
Insider	Part of the system and holds legitimate information	Legitimate devices	Manipulation and tampering	Access Control
Software Cracker	Binary analysis	Source Code inspection and Analysis Tools	Analysis of the underlying cipher and protocol	Use of publicly studied cryptographic primitives
Jammer	Physical Jamming of communication	Jammer equipment	Communication is hampered	Anti-jamming Techniques
Rouge Device owner	A rouge sensor or rouge external device is	IMDs, Universal Software Radio Peripheral (USRP) [14] and external devices available in market	MITM attack, result manipulation	Continuous Authentication

Apart from simple passive and active attacks, more sophisticated attacks are possible. Some of them are given below:

1. **Binary Analysis:** By doing a binary analysis on the software of IMD an adversary may understand its operations and may also reverse engineer the communication protocol to break it.
2. **Reprogramming Attack:** By analyzing bugs in the software program of IMD, this attack forces the device to behave in an unpredictable manner. Attacks like buffer overflow or injection are also possible.
3. **Insecure software update:** The software in the IMDs are upgradable by patches to enhance functionality. An attacker may update the IMD software to make it behave in an unpredictable manner.
4. **Malware based Attack:** A malware is a program which masquerades or embeds itself in another program to get activated later to carry out harmful actions like erasing the device memory.
5. **Denial-of-Service:** Posing Denial-of-service (DOS) by blocking the communication between IMD and the external device or forcing IMD to communicate continuously thereby depleting its battery.
6. **Networking related Attack:** Multiple IMDs on a human body may be networked in an IWBAN. Security compromise on one device may adversely affect the other devices also leading to false diagnosis, treatment and actuation.
7. **Repudiation:** An attacker especially an insider may tamper the device or perform action that he may deny later.
8. **Elevation of Privilege:** Medical staffs who access the IMD may indulge in supplying commands of higher privilege and due to lack of access control may be successful in doing so.
9. **Spoofing:** A rouge device may be used to masquerade as another authorized device and gain illegitimate access.

The threats arising are by and large interrelated and interdependent on each other and need to be considered together for mitigation. For example if software does not implement proper input validation, forged packets can be injected through wireless medium [4].

2.7 Threat Modeling using SDL Tool

As a popular and free tool for threat enumeration we make use of Microsoft SDL Threat Modeling Tool [55] to perform threat modeling using a four-step process which helps in

identifying security objectives, creating the application overview, decomposing application to uncover threats, threat identification and vulnerability identification.

Step1: Creation of data flow diagrams that represents the flow of data through the system that is being modeled for threats. Fig. 2.3 shows the context level DFD for IMDs performing wireless communication with external devices.

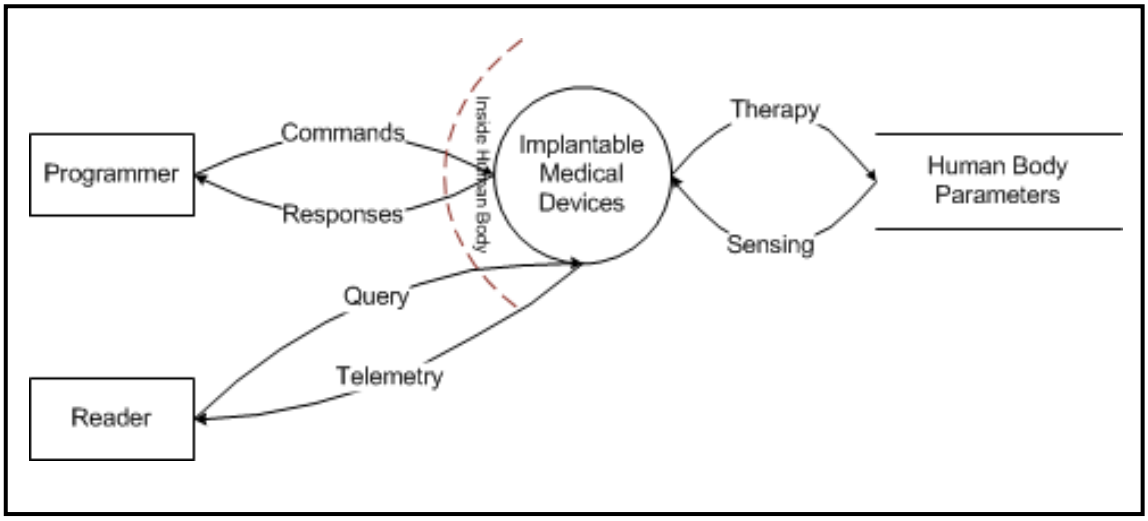

FIGURE 2.3 Context Level DFD for IMDs

In the next step, level one DFD is shown in FIGURE 2.4.It shows the IMDs which are networked using wireless medium to perform sensing and actuation.

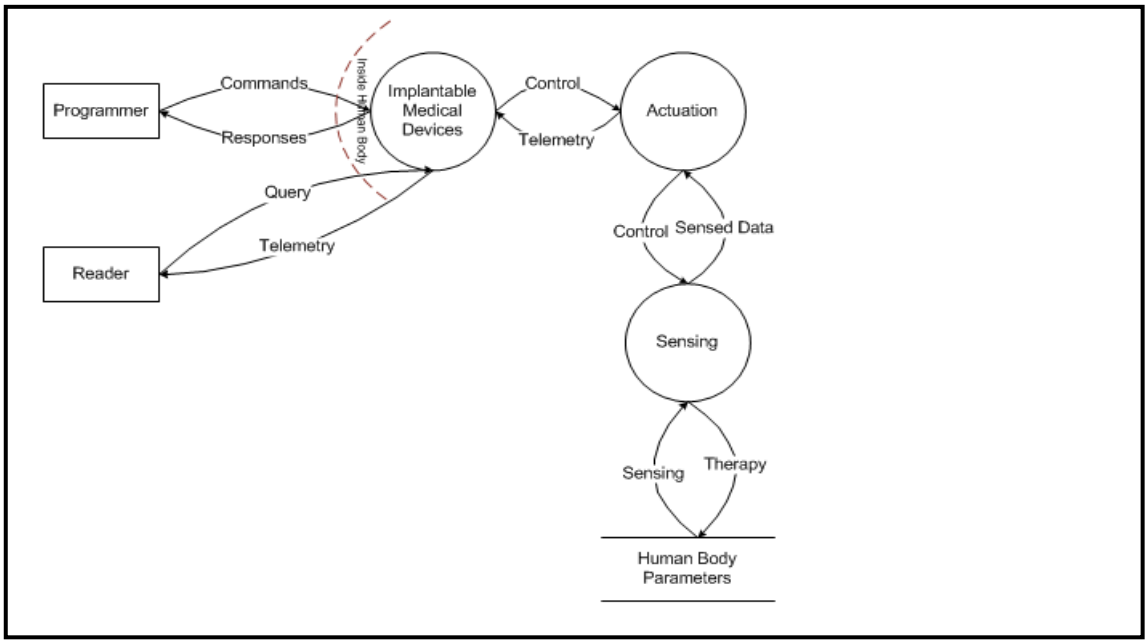

FIGURE 2.4 Level One DFD for IMDs

Step 2: Generation of a list of threats by running the tool. Table 2.3 shows the threat analysis report.

Step 3: Description of the environment in which the software will run. For example Wireless Environment and Implanted in Human Body.

Step 4: Report Generation. Finally we generate the threat model analysis report as shown in Figure 4 which shows a plethora of threats.

Table 2.3 : Threat Analysis Report

Threat Model Analysis Report:

Empty Threats

The following threats have no threat description:

Element Name	Threat Type
Commands	Tampering
Commands	InformationDisclosure
Commands	DenialOfService
Query	Tampering
Query	InformationDisclosure
Query	DenialOfService
Responses	Tampering
Responses	InformationDisclosure
Responses	DenialOfService
Sensing	Tampering
Sensing	InformationDisclosure
Sensing	DenialOfService
Telemetry	Tampering
Telemetry	InformationDisclosure
Telemetry	DenialOfService
Therapy	Tampering
Therapy	InformationDisclosure
Therapy	DenialOfService
Human Body Parameters	Tampering
Human Body Parameters	Repudiation
Human Body Parameters	InformationDisclosure
Human Body Parameters	DenialOfService
Programmer	Spoofing
Programmer	Repudiation
Reader	Spoofing
Reader	Repudiation
Implantable Medical Devices	Spoofing
Implantable Medical Devices	Tampering
Implantable Medical Devices	Repudiation
Implantable Medical Devices	InformationDisclosure
Implantable Medical Devices	DenialOfService
Implantable Medical Devices	ElevationOfPrivilege

2.8. Conclusion

The threat model shows it is necessary for IMDs to have an effective protection and/or detection mechanism for fighting against these attacks. Security services needs to be selected judiciously for securing such devices.