ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Review on Security of Medical Devices

Pooja S. Band, Archana B. Kanwade

PG Student [VLSI & Embedded System], Dept. of ECE, Sinhgad Institute of Technology & Science, Narhe, Pune, Maharashtra, India[1]

Assistant Professor, Dept. of ECE, Sinhgad Institute of Technology & Science, Narhe, Pune, Maharashtra, India[2]

ABSTRACT: Implantable Medical Devices (IMDs) allow to use various new therapies to patients by which patients' lives can be improved. Therefore they are day-by-day becoming more and more popular in medical field. IMDs can also be used for monitoring and control applications. To use IMDs for monitoring and control, wireless interfaces need to be used. But while using wireless communication, there are chances of malicious attacks to IMDs. These attacks can raise a question on patients' privacy. This can also make patients' lives in danger. Therefore, there is a great need to secure medical devices. This can protect patients from theft. Also, we can connect medical technology to other systems through wireless communications. The aim of this paper is to survey various papers to find the best method for providing security to implantable medical devices.

KEYWORDS: Attacks, Control, Implantable Medical Devices **(**IMDs), Monitoring, Wireless Interfaces**.**

I.INTRODUCTION

The articles used in hospitals to treat various health related issues e.g., a disease in humans or in animals, having the purpose to cure them from the problem are known as medical devices. These medical devices are important for modern medicine because they can be used for number of purposes like patient monitoring, to perform management functions, etc. If this medical device can be placed on the surface of the human body or it can be either partially or completely introduced into the body, it can be called as implantable. There have been many developments in science and engineering field which has made advancements in implantable medical devices in recent years.

Implantable Medical Devices (IMDs) are generally used to monitor the medical conditions and provide treatment on them. Examples of such IMDs include implantable cardiac defibrillators (ICDs), pacemakers, neuro stimulators, and drug delivery systems. These IMDs are used to manage number of diseases that occurs because of today's lifestyle [1]. The vision for the future of healthcare can be achieved using IMDs. The future of healthcare includes monitoring and treating the patients. To achieve this, medical devices are implanted in human body. For monitoring purpose, IMDs' use will be grown in near future. IMDs help patients to improve their lives through surgical operations. The number of patients using insulin pumps was approximately 245,000 in the year 2005 and for the insulin pump market, the growing rate is expected to be 9% from the year 2009 to next seven years i.e., 2016 [2]. As per the report by Hanna et al. in only U.S., near about 25 million patients make use of IMDs and nearly 300,000 more devices are implanted every year [3]. In 2004, more than two million drug-eluting stents were implanted [4]. Again, operations for hip replacement were near about 152,000, i.e., a 33% increase compared to hip replacement operations in 1990 and 50% of expected number of operations in 2030 [5].

II.IMPORTANCE OF SECURITY

Implantable medical devices must be secured as they are used in number of medical therapies. To connect medical technology with other systems, wireless communication is used and for achieving wireless communication, wireless interfaces are implemented. IMDs use such wireless interfaces for monitoring as well as controlling purpose. To connect IMDs to body area networks (BANs), wireless interfaces are used. This forms personal healthcare system (PHS). Connection of IMDs to BANs forms many wireless health applications. Wireless interfaces use wireless medical devices. Such medical devices consists of large number of sensors and because of this only, they have become susceptible to various security attacks. Also, personal healthcare systems and IMDs improve the effectiveness of health care by performing complex system analysis. IMDs and PHSs communicate wirelessly. These functionalities can be used to improve the quality of healthcare. But IMDs get easily affected by malicious attacks [6]. This is a very serious issue. Other issues include sending unauthorized commands, for example, if we have used a pacemaker to transmit commands wirelessly, there are chances that an attacker can give a command by which shocks will be sent to patients. This can be very severe and even cause patient's death.

Since use of implantable medical devices creates number of risks, patients are not able to use IMDs safely. Therefore, security is very important in implantable medical devices [7].

III.SECURITY ISSUES

Modern implantable medical devices (IMDs) use wireless communication. Wireless interfaces are needed to use IMDs for various applications because they make controlling and monitoring of IMDs conveniently. To achieve this, a control device is used, which can be called as a "programmer." But, according to the recent work done in this field, if we use IMDs for wireless communication, it affects confidentiality of the data transmitted by IMDs. Also, unauthorized commands are sent to IMDs. To overcome these issues, it is necessary to modify the IMDs or to replace them and this is the main challenge in achieving security in IMDs.

There have been many experiments performed by researchers, where they have considered these issues. Some experiments were performed remotely and those provided unauthorized access to IMDs. Examples include insulin pumps [8] and cardiac defibrillators. The attacks have shown interrupts on communication of IMDs as well as modified the therapies applied by IMDs. This affects patients' privacy and also patients' health.

Therefore, it is clear that wireless communication is immune to adversarial attacks. Thus IMDs become susceptible to various threats including eavesdropping as well as unauthorized access and control.

IV.SURVEY OF WORK DONE

As per the study done in 2001[9] by Barold and Israel, pacemaker systems were considered as implantable cardiac defibrillators. In this study, they assumed a channel between medical devices and controllers. This channel was based on radio frequency identification (RFID). But here the drawback was if antenna of the attacker is of high gain then there were chances that wireless channel can be easily attacked. Again, a study done in 2007[10] by Flynn and Fotopoulou and in 2008[11] by Centre and Hancke has proved that attacker can easily access the patient data, if it is within ten meters of distance from IMD.

T. Kohno, K. Fu and T. Denning [12] in 2008 discovered a class of new techniques. They called them as Communication Cloackers. Patients have to worn these cloackers externally. The interactions taking place between IMDs and the doctor are co-ordinated by cloackers. When the patient wears the cloacker, unauthorized programmers are not able to see the IMDs. So, patient's data cannot be accessed by an attacker. In emergency, medical staff can access the IMD by removing the cloacker. But, if patient is not wearing the cloacker, it is lost or damaged, external programmer can access the IMD.

A new concept of human-centric connectivity was introduced by Corroy et al. in June 2009 [13]. They used body coupled communication (BCC) technology where human body is used as a transmission medium. For BCC, a small electric field is induced in human body. The devices which are very near to the human body play important role in BCC. Signal propagates between these devices only. Thus, range of the communication is limited very close to the human body.

An access control scheme was developed for implantable medical devices in November 2009 [14] by Rasmussen, et al. This scheme used a message authentication protocol. The protocol used the concept of ultrasonic distance bounding. In this protocol, messages are encrypted beyond the distance measured by the IMD i.e., distance near to the IMD. By this concept, IMDs are accessible to the devices which are very closer to them. There are chances that an attacker can make the physical contact with patient by approaching him.

In 2010, Schechter [15] proposed a method in which a key is used. This key gives patient data of body parameters. The key has to be printed into patient's skin with the help of ultraviolet- ink micropigmentation. The key is placed near the point of IMD implantation. The ultraviolet-ink micropigmentation were called invisible tattoos. The devices which are used for communication with IMDs consist of a reliable, inexpensive and a small ultraviolet light emitting diode (UV LED) and to enter the key, it has a device like a keypad or any other mechanism. Multiple devices may use a single key. No daily effort is required for UV micropigmentation except the use of sunscreen.

F. Xu et al. introduced a scheme for securing cardiac devices which are implantable. They called this scheme as IMDGuard [16]. IMDGuard is used for implantable cardiac devices like pacemaker, implantable cardioverter-defibrillator etc. It uses a Guardian, a wearable device which plays a role of mediator between doctor and IMD. In this case, to extract the key, electrocardiography (ECG) signals of the patient are used. When Guardian is lost by the patient or it does not function properly, it can be easily rekeyed as nothing is required except ECG signal of patient. In case, if attacker could make physical contact with patient, he can extract the key.

In August 2011, another device was developed by Ransford, et al. This was called the Shield [17]. They called this shield as a personal base station. Patients have to wear this shield on the body near the IMD. Messages were co-ordinated between programmer and IMDs using shield. Shield provides secured communication of IMDs with programmer. Shield encrypts the messages sent by IMDs and sends them to the programmer. Considering the reverse case, the commands from the programmer to be send to IMDs by the shield are not encrypted. Therefore, commands do not remain confidential.

In 2013, Zhang et al. proposed a device. They called it as Medmon, meaning medical security monitor [18]. Medmon provides security by two ways. First is through wireless monitoring and second is through anomaly detection. Anomalies include physical and behavioral. Physical anomalies are of three types. These are time of arrival (TOA), differential time of arrival (DTOA) and received signal strength indicator (RSSI). Behavioral anomalies consist of the two, i.e., data anomaly and command anomaly. Medmon keeps a record of previous data and commands. If new data or command arrives, it is compared with the previous record to decide if new data or command is a behavioral anomaly or not. Medmon performs all its functions without being affected by changes in its environment, but has a drawback that data being communicated through the channel does not remain confidential.

V. CONCLUSION

Implantable medical devices monitor medical conditions of patients and also used in applying medical therapies to them to improve their lives. IMDs make use of wireless transceivers due to which they become susceptible to RF wireless attacks. These attacks make hazardous effect on patient's health. Hence, there is a key need to secure medical devices to have no malicious attacks. Various devices have been developed as well as methodologies have been presented to secure IMDs. A comparison of all these devices and the methods is shown in TABLE I.

TABLE I
COMPARISON OF IMD SECURITY METHODS

Sr. No.	Ref. No.	Methodology (Device) used	Limitation
1.	9	RFID-based channel	Attacker having a strong transmitter and antenna with high gain can easily attack the channel
2.	12	Communication Cloacker	External programmers can easily access the patient's data when patient does not wear the cloacker
3.	13	Body Coupled Communication (BCC)	Limited only to a specific distance from human body
4.	14	Ultrasonic-distance bounding	Attacker is able to make physical contact with patient by approaching very close to the patient

5.	15	Ultraviolet-ink micropigmentation (tattoos)	Protects the patient to some extent from close-range attacks
6.	16	IMDGuard	Attacker can make physical contact with the patient and extract the key
7.	17	Shield	Needs to make changes in all programmers
8.	18	Medmon	Does not provide secured communication channel

From TABLE I, it has been observed that many of the researchers have developed a device to provide security to IMDs and others have proposed a scheme or a mechanism. The devices play a role of mediator between the programmer and the IMD. Only Meng et al. developed a device which provides security to IMDs by wireless monitoring as well as by detecting anomalies. Lot of scope is there to secure IMDs by other concepts related to wireless monitoring.

REFERENCES

[1] Halperin, Daniel, et al. “Pacemakers and implantable cardiac defibril-lators: Software radio attacks and zero-power defenses”, IEEE Symposium on Security and Privacy, 2008.

[2] Insulin pumps - global pipeline analysis, opportunity assessment andmarket forecasts to 2016, globaldata. Global Data (2010).

[3] K. Hanna, Innovation and invention in medical devices: workshop summary. National Academies Press (2001).

[4] G. E. Park and T. J. Webster, “A review of nanotechnology for the development of better orthopedic implants”, Journal of Biomedical Nanotechnology, Vol. 1, Issue 1, pp. 18-29, 2005.

[5] E. Gultepe, D. Nagesha, S. Sridhar, M. Amiji, “Nanoporous inorganic membranes or coatings for sustained drug delivery in implantable devices”, Adv. Drug Deliv. Rev. 62:305-315.

[6] Fu, Kevin, “Inside risks: Reducing risks of implantable medical de-vices”, Communications of the ACM, Vol. 52, Issue 6, pp. 25-27, 2009.

[7] Maisel, William H., and Tadayoshi Kohno, “Improving the security and privacy of implantable medical devices,” New England journal of medicine, Vol. 362, Issue 13, pp.1164-1166, 2010.

[8] Li, A. Raghunathan, and N. K. Jha, “Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system,” IEEE Int. Conf. on e-Health Networking Applications and Services, pp. 150–156, 2011.

[9] Israel and S. Barold, “Pacemaker systems as implantable cardiac rhythm monitors”, American Journal of Cardiology, Vol. 88, Issue 4, pp. 442-445, 2001.

[10] K. Fotopoulou and B. Flynn, “Optimum antenna coil structure for inductive powering of passive RFID tags,” in Proc. IEEE Int. Conf. Radio Frequency Identification, 2007, pp. 71–77.

[11] G. P. Hancke and S. C. Centre, “Eavesdropping attacks on high-frequency RFID tokens,” in Proc. Workshop Radio Frequency Identification Security, 2008, pp. 100–113.

[12] T. Denning, K. Fu, and T. Kohno, “Absence makes the heart grow fonder: New directions for implantable medical device security,” in Proc. Conf. Hot Topics in Security, 2008, pp. 1–7.

[13] H. Baldus, S. Corroy, A. Fazzi, K. Klabunde, and T. Schenk, “Humancentric connectivity enabled by body-coupled communications,” IEEE Commun. Magzine., Vol. 47, Issue 6, pp. 172–178, 2009.

[14] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, “Proximity-based access control for implantable medical devices,” in Proc. ACM Conf. Computer and Communications Security, 2009, pp. 410–419.

[15] S. Schechter, “Security That is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices”, Microsoft Research, Tech. Rep. MSR-TR-2010-33, 2010.

[16] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, “IMDGuard: Securing implantable medical devices with the external wearable guardian,” in Proc. IEEE Int. Conf. Computer Communications, pp. 1862–1870, 2011.

[17] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, “They can hear your heartbeats: Non-invasive security for implantable medical devices,” in Proc. ACM Conf. Special Interest Group on Data Communication, 2011.

[18] Zhang, Meng, Anand Raghunathan, and Niraj K. Jha, “MedMon: Securing medical devices through wireless monitoring and anomaly detection”, IEEE Transactions on Biomedical Circuits and Systems, Vol. 7, Issue 6, pp. 871-881, 2013.