SYNOPSIS

Enrollment Number: 119997493008 Batch: 2011

Branch Name: Computer Science

Name of Research Scholar: Monika Darji

Index

I. Title of the thesis and abstract

Title of Thesis

Two-tier Security Solution for Implantable Medical Devices.

Abstract

The development of MEMS (microelectromechanical systems), SoC (System on Chip) and ultralow power wireless communication technology enabled evolution of Implantable Medical Devices (IMDs). Implantable medical devices (IMDs) diagnose, monitor, and treat a wide range of medical conditions. This has lead to paradigm shift of healthcare industry from doctor centric to patient centric by providing home-based treatment and remote monitoring and hence cost reduction. While these features improve healthcare diagnostics and decision making, security and privacy remain critical design aspects in wireless communication performed by these devices. As compared to previous ones implantable medical devices of current genre are complex embedded systems with networking capabilities that aid in wireless communication amongst IMDs and with other external devices. Due to their unique placement in human body and resource constraints like low power availability, computation and storage capacity, achieving security and privacy for wireless communication is difficult. Security for medical devices has gained attention in the recent years following some well-publicized attacks on Implantable Medical Devices, like pacemakers and insulin pumps. This has resulted in solutions being proposed for securing these devices, which are usually device specific and useful for secure communication with external devices. Multiple IMDs may be implanted on a single patient therefore we argue that securing individual devices will not serve the purpose as these devices will be integrated sooner or later for advance therapeutic implications. Also security solution rather than being device specific should be patient specific to cater to the security needs of IMDs of a patient.

In order to address this issue we are rethinking the way we store, transmit, process and access the telemetry data from IMDs. This will help us to generalize the solution to provide security to a large range of IMDs. In this thesis we study the security challenges in Implantable Medical Devices and then provide an application layer security solution which not only allows secure communication between IMDs and external devices but also allows secure communication between interoperable IMDs for a single patient. Our proposed solution uses an external device called “proxy device” to provide security. The “proxy device” offloads the burden of security related transformations from IMDs thus conserving IMDs energy. We consider extreme resource constraints of IMD and explore the tradeoffs among different cryptographic primitives for use in IMDs to carefully design a light weight protocol optimized for IMDs for mutual authentication and secure communication between the IMD and the proxy device. We also design a secure publish-subscribe communication protocol between the

"proxy device" and external devices. Finally, we provide a proof-of-concept of the proposed two-tier security solution.

II. Brief description on the state of the art of the research topic

Introduction

Implantable Medical Devices are being used in healthcare for various applications. Their applications are primarily grouped into two main categories: physiological parameter monitoring (for diagnostic purposes) and actuation [1]. IMDs are being used for measuring blood pressure [2], blood-glucose concentration [3], gastric pressure [4], tissue bio-impedance [5]. IMDs are also used as electrical stimulators for paralyzed limbs [6], for bladder control [7], for blurred cornea in the eye [8] and as implantable pacemakers [9,10], implantable cardiac defibrillators (ICDs) [11]. Wireless IMDs improve the quality of life by providing high accuracy diagnostics. Almost every aspect of human health can be monitored by an implanted device. An implantable medical device generally works as an isolated standalone device rather than as a connected and coordinated system. But during many critical medical treatment procedures, comprehensive real-time body information is often required for medical decision making. For example, the implanted drug delivery device needs the feedback information from the targeting areas in order to release the right dosage at the right time and in the right place. Recent work has proved that it is feasible to develop implantable body sensor networks (IBSNs) by adding network function to multiple standalone implantable devices [12]. Moreover, in near future implant functionality will heavily rely on software rather than pure, hardwired circuitry. For improvements in quality of monitoring and therapy, IMDs are in fact, becoming increasingly complex with software programmability and network connectivity features.

These devices consist of wireless network interface that are used to communicate with external monitoring or diagnostic equipment called readers or programmers, and for device reprogramming to optimize the delivered therapy. Recently standardized IEEE 802.12.6 [13] is used to connect these devices.

Since transmitted data in medical applications usually contain sensitive information that are either private or critical for the proper operation of the IMD. Moreover, the introduction of interoperability makes medical devices increasingly connected and dependent on each other. Security and privacy are major concerns in IMD communications. However, current research shows that IMDs do not use any of these security mechanisms and these devices are easy accessible for people with the right equipment [14-16]. For cardiac IMDs, it is shown that an adversary of an IMD with the right equipment is able to read, interfere and change the data communication [14].

Adding security mechanisms even if seems obvious, is a complex task for IMDs due to following reasons:

1. **Resource Constraints:** As mentioned in [17], IMDs are resource constraint devices that are miniaturized to place them in human body. Most of the IMDs are expected to run for 5- 10 years on a limited size battery. If battery is exhausted, replacement requires surgery. Their unique placement and miniaturized size limit places stringent limits on processor capability and memory size. Reported literature and an extensive study [18] on implants have revealed that typical memory sizes inside the implants range from 1 KB to 10 KB. Secure communication [19] in particular require use symmetric-key cryptography to ensure confidentiality of the transmitted data, message authentication for integrity protection and validation of source of origin, and public-key cryptography for peer authentication and key exchange. Such cryptographic translations present higher processing, memory, and energy requirements unless optimized for use with these devices.
2. **Usability Constraints:** During a medical emergency strong authentication and cryptographic measures may prevent emergency responders from communicating with the device
3. **Key Distribution Constraints:** Use of symmetric key cryptosystem require sharing of secret key between legitimate parties and key renewal which is difficult to manage as only non-invasive means of accessing these devices is wireless interface. Well-established public-key cryptosystems such as RSA, Diffie-Hellman, and elliptic curve cryptography (ECC) provide ample flexibility to incorporate the security needs of IMDs but remain prohibitively expensive due to their higher order resource requirements and code size [16].
4. **Environmental Constraints:** IMDs are used in insecure physical environments and are prone to greater exposure to the attackers.
5. **Manageability Constraints:** Devices per user may tend to increase making it impractical for users to manage separate security administration tasks such as security patching and credentials management.

For secure communication under tight power budget, these devices can only support minimalistic security transformation for wireless communication and storage. The key solution to the given resource constraint is use of algorithms that optimize the resource consumption.

Wireless Communication

Implantable Medical Devices use RF-based communications for bidirectional data and command transfer. A wireless medical system consists of one or more implantable medical devices (IMDs) for continuous monitoring of biological parameters, external devices(ED) like base station (BS), external readers(ER), external programmers (EP)). The wireless connection serves one or more of the following purposes:

1. Remote monitoring of vital parameters and querying of IMD status parameters by an external device;

2. Access by an external device for calibration purposes, program adjustments, software maintenance

3. In-body distribution of sensor data between two or more IMDs for control purposes or to form a loop of simulation and actuation.

The IMD and ED communicate through an RF link that operates in industrial, scientific and medical (ISM, at 2.4GHz- 2.48 GHz) or medical implantable communication service (MICS, at 402MHz-405MHz) bands. MICS band has a maximum bandwidth of **300 kHz** and a typical coverage range of **2 m to 3m** [1]. Typically, IMDs are designed using system-on-chip technologies and uses ultralow-power Zarlink MICS transceiver for wireless data transmission. **Zarlink ZL70101 402 MHz MICS transceiver** is world's first ultralow-power RF wireless chip designed specifically for implantable communication [20] at the MICS band. ZL70101 supports a typical **raw data transmission rate of 200 to 800 kb/**s [20]. Zarlink transceiver is commercially available as an implantable-grade bare die [21] and can be stacked on the sensing unit or the actuation unit to build up the implantable network nodes for sensing and actuation. For long-term active implantable biomedical system, **Lithium-ion (LI) batteries** are used [21] which has approximate capacity up to **10 mWh** [20]. The transceiver of an implant is idle most of the time and activates after a large time interval (several hours or even weeks) to save power [7]. Some IMDs receive power through inductive coupling [22] and some completely depend on their battery.

Possible Attacks on IMDs in wireless networking environment

A passive or active adversary may misuse the vulnerability of unprotected wireless channel using standard or custom equipments like off-the-shelf software radio or Universal Software Radio Peripheral (USRP) to pose an attack on IMD [23]. Attacks on IMDs have been described in [10], [23], [14], [24]. Attacks on IMDs can be classified as following types:

Eavesdropping attack: If wireless communication channel is not strongly protected, an eavesdropper may sniff the channel and threaten confidentiality.

Man-in-the middle attack: An adversary may be present during authentication session between programmer and IMD or when keying material between IMD and reader is exchanged in clear. Recently, two such protocols have been broken as illustrated in [25].

Impersonation and Injection attack: A spoofed reader may declare itself a legitimate one and perform unauthorized communication threatening confidentiality, integrity and availability.

Denial-of-Service Attack: Attacker may continuously send request to exhaust the scarce resources like draining the battery on which the IMD is running. This can pose a severe threat to availability and can lead to a life threatening condition for the patient.

Replay attack: Even if encryption is used**,** the older authorized packets can be trapped and replayed which may compel the IMD to disclose private information or exhibit abnormal behavior. Such an attack threatens integrity and availability.

Related work in securing Implantable Medical Devices

The criticality of security issues related with wireless telemetry of IMDs has attracted many researchers to propose different solutions to this important problem. Confidentiality based approaches includes ultraviolet-ink micro pigmentation to create UV-visible Tattoos [26] and Access Tokens [27]. Access Control Based Approaches include use of proximity-based access control [23] wherein proximity-based device pairing protocol was proposed based on ultrasonic distance bounding allowing access to only those devices which are in close proximity; the utility of this approach relies on implementation ultrasonic distance bounding features on IMD which makes it invasive and also this approach may not work well in case on noisy channels. Another solution is proposed as Patient Notification and Access Control using RFID which provides Zero-power notification by harvesting 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; Sensible key exchange that 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[10]. Some invasive techniques which propose changes in IMD are also mentioned here. A scheme [14] makes use of rolling code cryptography between IMD and reader to provide confidentiality. Scheme [28] presents a lightweight wireless protocol for IMDs that emphasizes on low-energy computation. Scheme [29] explores the use of block ciphers in IMD security. Another set of solution involves used of trusted external device like Communication Cloaker [24], Sheild [30], IMDGuard [31], Amulet [32] and SVM on Mobile Phone [25]. Communication Cloaker [24] provides a defensive countermeasure and controls access to the IMD by making it invisible to all unauthorized queries. It encrypts all communications to and from the IMD and checks them for authenticity and integrity. The shield [30] acts as a jammer-cum-receiver to jam the IMDs messages and unauthorized commands preventing others from decoding them while being able to decode them. The channel between Shield and legitimate programmer uses encryption. IMDGuard [33] utilizes the patient's electrocardiography signals for key extraction. Using the biometric exchange, it pairs with an IMD and use radio jamming to defend against eavesdropping and unauthorized commands. Amulet [32] is a vision which is dedicated to secure communications with wearable Medical Devices. Scheme [25] presents SVM based technique to battle against battery depletion attack. Our solution also uses a similar external proxy

and presents detailed protocols for preventing active attacks in proxy environment. The scheme given in [34] also uses RF signal characteristics for physical anomaly detection by use of a passive monitoring device.

III. Problem Definition

Implantable medical devices (IMDs) are used to monitor and treat physiological conditions within the human body. Such devices include pacemakers, implantable cardiac defibrillators (ICDs), insulin pumps, neurostimulators, hearing aids, biosensors and automated drug delivery systems. They can be used to remotely monitor vital signs or adjust therapy by sending commands to the implanted device. IMDs can help to manage a broad range of ailments such as cardiac arrhythmia, diabetes or Parkinson's disease without hospitalization. Wireless interface is used to give commands from an external device called a programmer or reader. The use of wireless communication for IMDs gives rise to unique security and privacy challenges. Plausible threats are that attackers may compromise the confidentiality of the transmitted data or send unauthorized commands to change the settings of an IMD. The consequences of such attack can be life threatening to the patient. Though computer and network security is a highly matured field, complexity of human body, safety concerns, and some technological bottlenecks like low power, processing, storage capacity poses a challenge in developing security solutions for these devices.

In this thesis, we address the following research question: "How can we define a system that provides confidentiality and integrity, authentication and access control of sensitive information during the communication between a IMD and a legitimate programmer, or between two or more IMDs of a patient while ensuring availability of information in case of an emergency?"

IV. Objective and Scope of work

The major objectives of this research are:

- Understanding the security and privacy implications of future implantable medical devices that provide an unprecedented view into the inner workings of the human body.
- To perform threat modeling for a network of IMDs and external devices.
- To explore design alternatives that effectively provide a single security solution for a system involving heterogeneous IMDs of a patient and which communicate with each other and with external devices by wireless means.
- To propose an application layer security solution which is patient specific rather than device specific.

- To greately reduce overhead of security related processing on IMDs
- To propose a two-tier model which can allows secure communication between resources constrained IMDs and resource rich external devises simultaneously.
- To understand energy issues, including power depletion and replay attacks that exploit the lightweight nature of the IMDs and propose a solution model that offload security related processing from IMDs .
- To impose security policies on IMDs as well as external devices for fine-grained access control.

Scope of Work

We define our scope as:

- Developing a detailed threat model for wireless communication of implantable medical devices.
- Developing a secure two-tier communication protocol for Implantable Medical Devices. We may assume typical IMD for our case. The assumption might not be exact in terms of some typical IMD. The proposed protocol will work at an application layer which assumes a specific transport layers services present. The protocol also assumes a key exchange and renewal technique to be in place.
- Providing a proof of concept.

V. Original contribution by the thesis

The thesis first discusses the insufficiencies of current solutions for securing implantable medical devices in providing security to multiple IMDs of a patient time and proposes a suitable defense framework for resource constrained IMDs. The frameworks include light weight secure communication protocol for IMDs for which components have been carefully selected to reduce the overhead on IMDs.

The thesis proposes a novel proxy-based two-tier solution to achieve secure data transmission in wireless IMDs. The proposal combines, for the first time, a request response protocol for IMDs with publish-subscribe protocol, a powerful and general approach for asynchronised unicast and multicast communication , which allows usage of security mechanism based on the requirement and constraint of communicating party.

The thesis thereafter presents a novel countermeasure against replay attacks on IMDs by use of nonces which are generated using Physiological Values that are sensed by IMDs therefore not needing any pseudo random number generator (PRNG).

The communication protocol provides authentication, encryption and integrity checking of the communicated data along with fine-grained access control for IMDs by defining topics and controlling who is allowed to publish and to subscribe to which topic. Our theoretical analysis demonstrates that the proposed system can meet the requirements of these devices.

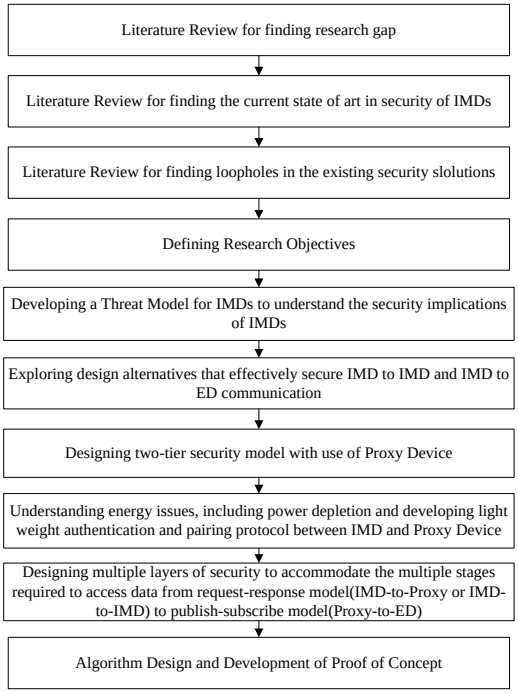
We also implement the proposed system for a proof of concept. Evaluation results show the feasibility of the system in practice.

The thesis also proposes security for emergency conditions. Finally the thesis also discusses a buddy system for securing wireless IMDs which runs authentication and access control protocols on behalf of IMDs allowing controlled access to the external devices. We also propose a Session Key generation scheme on IMD which harvests Physiological Values (PVs) randomness and therefore shuns the need of a Pseudo Random Number Generator (PRNG). Finally we propose friendly jamming scheme for secure transmission of thus generated one time session key from IMD to authenticated external device. Proposed scheme is lightweight and adaptable as it is applicable to wide range of devices and saves IMD critical resources like memory, computation and communication.

VI. Methodology of Research, Results / Comparisons

Methodology of Research

The data for the study has been collected mainly from secondary sources comprising various books, periodicals, journals. Our Research is:



Qualitative since we continuously strive to maintain optimal balance between safety and security without compromising any of the performance measures.

Experimental since our proposed model follows hybrid approach for deployment, which we have used for proof of concept.

Exploratory as we are combining two popular communication models to find the right balance for securing IMD to IMD as well as IMD to External Device communication.

Comparisons

Comparison Parameters	H2H	Cloaker	IMD Shield	IMD Guard	Medmon	Our Solution
Design Approach	Use of PVs	Trusted External Device	Trusted External Device	Trusted External Device (PVs)	Trusted External Device	Trusted External Device
Invasive Approach	Y	Y	N	Y	N	Y
Confidentiality	Y	Y	Y	Y	N	Y
Data Integrity	Y	Y	Y	Y	N	Y
Authentication	Y	Y	Y	Y	Y (anomaly detection)	Y
Message Freshness	N	N	N	N	N	Y
Replay Resilience	N	N	N	N	N	Y
Access Control	N	N	N		Y	Y
Fail-open system?	N(Physical Proximity)	Y	Y	Y	N	N
Secure IMD-IMD communication?	N	N	N	N	N	Y
Secure IMD-ED communication?	Y	Y	Y	Y	Y(passive monitoring)	Y

VII. Achievements with respect to objectives

- Performed threat modeling for a network of IMDs and external devices.
- Proposed an application layer security solution which reduces overhead of security related processing on IMDs by use of an external proxy device.
- Proxy device is based on a two-tier model which can allows secure communication between resources constrained IMDs and resource rich external devises simultaneously.

- Proxy device imposes security policies on IMDs as well as external devices for fine-grained access control.
- Designed secure communication protocol for IMD-proxy communication and proxy-external device communication.
- Designed a Mapping engine for secure mapping of request-response protocol to publish-subscribe protocol.
- Designed a security solution for emergency situation where a patient is incapacitated and a controlled access is provided for accessing IMDs.
- Designed a **Buddy system which runs authentication and access control protocols on behalf of IMDs allowing controlled access to the external devices by use of friendly jamming scheme for secure transmission of thus generated one time session key from IMD to authenticated external device.**

VIII. Conclusion

Implantable medical devices are likely to include more storage, more complex signal processing, integrated software control, and use of multiple intercommunicating sensors, all of which will complicate security and privacy issues. In this thesis we provide solutions for securing heterogeneous IMDs while considering their resource constraints. The thesis first discusses the insufficiencies of current solutions for securing implantable medical devices in providing security to multiple IMDs of a patient time and proposes a suitable defense framework for resource constrained IMDs. The frameworks include light weight secure communication protocol for IMDs for which components have been carefully selected to reduce the overhead on IMDs.

The thesis proposes a novel proxy-based two-tier solution to achieve secure data transmission in wireless IMDs. The proposal combines, for the first time, a request response protocol for IMDs with publish-subscribe protocol, a powerful and general approach for asynchronised unicast and multicast communication , which allows usage of security mechanism based on the requirement and constraint of communicating party.

The thesis thereafter presents a novel countermeasure against replay attacks on IMDs by use of nonces which are generated using Physiological Values that are sensed by IMDs therefore not needing any pseudo random number generator (PRNG).

The communication protocol provides authentication, encryption and integrity checking of the communicated data along with fine-grained access control for IMDs by defining topics and controlling who is allowed to publish and to subscribe to which topic. Our theoretical analysis demonstrates that the proposed system can meet the requirements of these devices.

We also implement the proposed system for a proof of concept. Evaluation results show the feasibility of the system in practice.

The thesis also proposes security for emergency conditions. Finally the thesis also discusses a buddy system for securing wireless IMDs which runs authentication and access control protocols on behalf of IMDs allowing controlled access to the external devices. We also propose a Session Key generation scheme on IMD which harvests Physiological Values (PVs) randomness and therefore shuns the need of a Pseudo Random Number Generator (PRNG). Finally we propose friendly jamming scheme for secure transmission of thus generated one time session key from IMD to authenticated external device. Proposed scheme is lightweight and adaptable as it is applicable to wide range of devices and saves IMD critical resources like memory, computation and communication.

IX. Copies of papers published and a list of all publications arising from the thesis

Title	ISSN/ISBN number	Detail
Survey of Intrusion Detection and Prevention System in MANETs based on Data Gathering Techniques	ISBN: 978-93-65823-02-5	Darji, Monika, and Bhushan Trivedi. "Survey of intrusion detection and prevention system in MANETs based on data gathering techniques." *IJAIS* 1 (2012): 38-43.
IMD-IDS a Specification based Intrusion Detection System for Wireless IMDs	ISBN: 978-93-65823-44-2	Darji, Monika, and Bhushan Trivedi. "Imd-ids a specification based intrusion detection system for wireless imds." *International Journal of Applied Information Systems* 5.6 (2013): 19-23.
Detection of Active Attacks on wireless IMDs using Proxy Device and Localization Information	ISBN: 978-3-662-44966-0	Darji, Monika, and Bhushan H. Trivedi. "Detection of active attacks on wireless imds using proxy device and localization information." *Security in Computing and Communications*. Springer Berlin Heidelberg, 2014. 353-362.
Emergency Aware , Non-invasive, Personalized Access Control Framework for IMDs	ISBN: 978-3-642-54525-2	Darji, Monika, and Bhushan H. Trivedi. "Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs." *Recent Trends in Computer Networks and Distributed Systems Security*. Springer Berlin

		Heidelberg, 2014. 370-381.
Secure Leader Election Algorithm Optimized for Power Saving using Mobile Agents for Intrusion Detection in MANET	ISBN: 978-3-642-34135-9	Darji, Monika, and Bhushan Trivedi. "Secure leader election algorithm optimized for power saving using mobile agents for intrusion detection in MANET." *Recent Trends in Computer Networks and Distributed Systems Security*. Springer Berlin Heidelberg, 2012. 54-63.

X. Patents

Filed complete specification for Patent application for our invention entitled "An Improved System for Securing Implantable Medical Devices" application numbered 92/MUM/2015 filed on 07th January 2016. The supporting document is attached herewith.

XI. References

[1] Strydis, C., Gaydadjiev, G., and Vassiliadis, S. Implantable microelectronic devices: A comprehensive review. CE-TR-2006-01, Computer Engineering, Delft University of Technology, December 2006.

[2] Flick, B., and Orglmeister, R. A portable microsystem-based telemetric pressure and temperature measurement unit. In IEEE Transactions on Biomedical Engineering (Jan. 2000), vol. 47, p. 12–16.

[3] Shults, M.C.; Rhodes, R.K.; Updike, Stuart J.; Gilligan, B.J.; Reining, W.N., "A telemetry-instrumentation system for monitoring multiple subcutaneously implanted glucose sensors," in Biomedical Engineering, IEEE Transactions on , vol.41, no.10, pp.937-942, Oct. 1994

[4] Valdastri, P.; Menciassi, A.; Arena, A.; Caccamo, C.; Dario, P., "An implantable telemetry platform system for in vivo monitoring of physiological parameters," in Information Technology in Biomedicine, IEEE Transactions on , vol.8, no.3, pp.271-278, Sept. 2004

[5] Min, M., Parve, T., Kukk, V., and Kuhlberg, A. An implantable analyzer of bio-impedance dynamics - mixed signal approach. In IEEE Instrumentation and Measurement (Budapest, Hungary, 21-23 May 2001), p. 38–43.

[6] Smith, B., Tang, Z., Johnson, M., Pourmehdi, S., Gazdik, M., Buckett, J., and Peckham, P. An externally powered, multichannel, implantable stimulator-telemeter for control of paralyzed muscle. In IEEE Transactions on Biomedical Engineering (1998), vol. 45, p. 463–475.

[7] Sawan, M., Robin, S., Provost, B., Eid, Y., and Arabi, K. A wireless implantable electrical stimulator based on two FPGAs. In Proceedings of the IEEE International Conference on Electronic Circuits and Systems (ICECS) (Piscataway, New Jersey, USA, 1996), vol. 2, p. 1092–1095.

[8] Schwarz, M., Ewe, L., Hauschild, R., Hosticka, B., Huppertz, J., Kolnsberg, S., Mokwa, W., and Trieu, H. Single chip CMOS imagers and flexible microelectronic stimulators for a retina implant system. In Sensors and Actuators A: Physical (22 May 2000), vol. 83, p. 40–46.

[9] R. Pallas-Areny, J.G. Webster, "AC instrumentation amplifier for bioimpedance measurements," Biomedical Engineering, IEEE Trans., vol.40, no.8, pp.830-833, Aug. 1993.

[10] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,” in Proc. IEEE Symp. Security and Privacy, May 2008, pp.129–142.

[11] ICD

[12] Qiang Fang; Shuenn-Yuh Lee; Permana, H.; Ghorbani, K.; Cosic, I., "Developing a Wireless Implantable Body Sensor Network in MICS Band," in Information Technology in Biomedicine, IEEE Transactions on , vol.15, no.4, pp.567-576, July 2011

[13] “Body Area Network,” http://www.ieee802.org/15/pub/TG6.html/.

[14] C. Li, A. Raghunathan, and N. K. Jha, “Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system,” in Proc.IEEE Int. Conf. e-Health Networking, Applications and Services, Jun.2011.

[15] C. Purvis, “Implantable Medical Devices: Hacks and Countermeasures,” Aug. 2011, http://www.securitymanagement.com/news/

[16] K. Carollo, “Can Your Insulin Pump Be Hacked?” Apr. 2012,http://abcnews.go.com/blogs/health/2012/04/10/can-your-insulin-pumpbe-hacked/.

[17] P. Gerrish, E. Herrmann, L. Tyler, and K. Walsh, "Challenges and constraints in designing implantable medical ICs," Device and Materials Reliability, IEEE Trans., vol.5, no.3, pp. 435-444, Sep. 2005.

[18] C. Strydis et al., “Implantable microelectronic devices: A comprehensive review,” Computer Engineering, TU Delft, CE-TR-2006-01, Dec. 2006.

[19] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). New York, NY: John Wiley & Sons, Inc., 1995

[20] Quallion LLC [Online]. Available: http://www.quallion.com

[21] Zarlink Semiconductor [Online]. Available: http://www.zarlink.com

[22] S. Carrara, S. Ghoreishizadeh, J. Olivo, I. Taurino, C. Baj-Rossi,A. Cavallini, M. Op de Beeck, C. Dehollain, W. Burleson, F. Moussy,A. Guiseppi-Elie, and G. De Micheli, “Fully Integrated Biochip Platforms for Advanced Healthcare,” Sensors, vol. 12, pp. 11 013–11 060,2012

[23] K. B. Rasmussen, C. Castelluccia, T. S.Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In CCS ’09: Proceedings of the 16th ACM conference on Computer and communications security, pages 410–419, New York, NY, USA, 2009. ACM.

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

[25] Hei, Xiali, et al. "Defending resource depletion attacks on implantable medical devices." Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. IEEE, 2010.

[26] 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).

[27] 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.

[28] S. Hosseini-Khayat. A lightweight security protocol for ultra-low power ASIC implementation for wirelessimplantable medical devices. In Proceedings of the 5th International Symposium on Medical Information Communication Technology, ISMICT ’11, pages 6–9, March 2011.

[29] C. Beck, D. Masny, W. Geiselmann, and G. Bretthauer.Block cipher based security for severely resource-constrained implantable medical devices. In Proceedings of 4th International Symposium on Applied

Sciences in Biomedical and Communication Technologies, ISABEL ’11, pages 62:1–62:5. ACM, October 2011.

[30] 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)

[31] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li. IMDGuard: Securing implantable medical devices with the external wearable guardian. In Proceedings of the 30th IEEE International Conference on Computer Communications, INFOCOM ’11, pages 1862–1870, April 2011.

[32] Jacob Sorber, Minho Shin, Ronald Peterson, Cory Cornelius, Shrirang Mare, Aarathi Prasad, Zachary Marois, Emma Smithayer, and David Kotz., “An amulet for trustworthy wearable mHealth,” In Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications (HotMobile '12). ACM, New York, NY, USA(2012).

[33] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li. IMDGuard: Securing implantable medical devices with the external wearable guardian. In Proceedings of the 30th IEEE International Conference on Computer Communications, INFOCOM ’11, pages 1862–1870, April 2011.

[34] M. Zhang, A. Raghunathan, and N. K. Jha, ―MedMon: Securing medical devices through wireless monitoring and anomaly detection," IEEE Trans. Biomedical Circuits and Systems, 2013.