Implantable Medical Devices - Cyber Risks and Mitigation Approaches

Sarbari Gupta
Electrosoft Services
Reston, Virginia USA
sarbari@electrosoft-inc.com

***Abstract*—Over the past decade, there has been an explosion in the deployment of implantable medical devices (IMDs) to facilitate the management and treatment of a wide variety of human health conditions. While functionality and patient safety requirements have driven new generation IMDs to be increasingly accessible through wireless communication channels, these changes cause significant concern in terms of increased risk from cyber threats whether malicious or unintentional. This paper investigates the risks associated with such devices from the cyber environment and proposes approaches to support decisions regarding the integration of adequate security and privacy measures to mitigate these risks.**

Keywords-medical devices; security, privacy, cyber, risks

I. INTRODUCTION

Deployment rates for implantable medical devices (IMDs) have skyrocketed over the past decade. Devices such as pacemakers, cardiac defibrillators, heart monitors, cochlear implants, insulin pumps, infusion pumps and other similar devices are routinely used to monitor and treat a plethora of medical conditions. These IMDs have been increasingly accessible through wireless channels to support functions such as emergency extraction of patient health history, remote monitoring of health status, firmware updates and local as well as remote therapy reprogramming. As with all things connected to the cyber world, there are known and unknown threats lurking that threaten the reliability and safety of these devices as well the privacy of patients who depends on them.

II. REGULATION OF IMPLANTABLE MEDICAL DEVICES

Within the United States, the Food and Drug Administration (FDA) regulates the manufacturers, importers and resellers of these devices through the Center for Devices and Radiological Health (CDRH). A review of a sampling of FDA testing guidance (e.g. for implantable cardiac pacemakers) reveals that the "tests are designed to reasonably assure safe and effective functioning of the pacemaker in the patient, according to written specifications of performance, and its survival under expected environmental conditions in the body and during storage, shipping and handling" [1]. FDA testing guidelines do not appear to address the resistance and resilience of these devices in the face of cyber attacks.

III. REVIEW OF RECENT RESEARCH

Halperin et al have shown that a recent (2003) model of implantable cardioverter defibrillator (ICD), designed to communicate wirelessly with an external programmer in the 175 kHz frequency range, is vulnerable to several radio-based attacks that threaten patient safety and privacy [2]. Several other research papers have pointed out similar vulnerabilities to cyber threats and possible mitigation mechanisms [3, 4, 5, 6].

IV. SECURITY ANALYSIS OF IMDS

IMDs are tiny computing platforms that run firmware in extremely power constrained environments. They offer data storage for static data (such as device information), relatively static data (such as patient identification, medical condition, therapy configuration) and dynamic data (such as recent patient readings and audit logs). IMDs offer wireless access for read and write operations to the data on the IMD (including the firmware) to a variety of stakeholders and roles.

A. Threats, Vulnerabilities and Risks

Some of the threats to wireless IMDs include device reprogramming, data extraction, data tampering, repeated access attempts and data flooding. Vulnerabilities include unsecured communication channels, inadequate authentication and access control, weak audit mechanisms and meager storage. The resulting risks include patient safety compromise resulting from firmware malfunction or therapy misconfiguration, device unavailability due to battery power depletion, patient privacy loss due to data leakage to unauthorized parties, and inappropriate medical follow-up due to tampering of patient readings. While some cyber threats may be unintentional, various motivations exist for deliberate cyber attacks, such as patient information gathering, negative impact to patient health status, ego satisfaction of the attacker, as well as gaining competitive advantage over another vendor through negative press.

B. Impact of Security Compromise

Identification of the various data types within an IMD is an essential step in analyzing the security and privacy risks of such devices. Possible data types include firmware (though technically not "data"), device identification data, patient identification and health condition data, therapy configuration data, patient readings, audit log data, and other data.

Following identification of the different data types within the IMD, it is useful to conduct a security categorization using the approach described in FIPS 199 [7]. For each data type, the security analyst asks the question: "What is the impact (High, Moderate or Low) of a compromise to the confidentiality, integrity and availability of this type of data?" It is useful to collect the results of this analysis in a table format.

C. Authentication and Access Control Mechanisms

For each type of data identified, the authentication and access control mechanisms applicable for extracting or updating the data type need to be reviewed to determine adequacy of the protection mechanisms while balancing the needs of patient safety in emergency situations and the utility of the IMD within a patient's environment. This is a non-trivial exercise since the security and privacy requirements for IMDs frequently conflict with the requirements stemming from emergency access to patient data and device utility in hospital and home settings. Creative approaches may be devised to decouple data essential for patient safety in emergency conditions from patient personally identifiable information/data to allow different authentication and access control mechanisms to apply to each group of data. Alternately, identifying different modes of operation (such as home health setting versus open environment versus emergency situation) to allow the IMD to apply different authentication and access control mechanisms in different modes.

D. Cryptographic Techniques

Cryptographic techniques are potentially very useful to improve the security and privacy properties of IMDs through stronger authentication protocols and (confidentiality and integrity) protected communications over wireless channels. However, since IMDs operate in very constrained environments (such as device size, cost, and power availability,) traditional cryptographic techniques and protocols may be inappropriate. More compatible cryptographic suites and protocols need to be devised for use on IMDs and applied in a very selective manner to optimize the security protection from these power intensive operations. The body of research conducted for cryptography for sensor networks are directly applicable [8] to applying cryptographic techniques to IMDs.

E. Audit Mechanisms

Audit logs are essential for tracking patient history and IMD behavior over a period of time. The audit records provide information needed for adequate patient care as well as updates to patient therapy delivered through the IMD. Given the limited storage capabilities of IMDs, it is possible to overflow the audit logs through certain types of attacks on the IMD. Creative techniques for selective overwriting of audit records based on significance of each type of audit record may be useful. Alert mechanisms when audit log storage space nears depletion may also be useful for alerting the patient or the remote monitoring facility so that appropriate steps can be taken in a timely manner prior to audit space exhaustion.

V. SUMMARY AND NEXT STEPS

Implantable medical devices pose a number of security and privacy risks even while providing essential medical support functions such as patient monitoring and treatment delivery. With the proliferation of IMDs of various types, it is essential to understand the risks from cyber threats, and integrate sufficient protections and controls to balance patient safety and device utility with security and privacy risks.

Some of the possible next steps in this area include (i) applying risk assessment methods to better understand the threat model and risks applicable to each type of IMD, (ii) performing security categorization analyses to various data types to guide optimal grouping of data to better protect each data group and apply appropriate cryptographic techniques when appropriate, (iii) development of guidelines for development, delivery, configuration, and monitoring of IMDs, and (iv) targeted regulation of IMDs by the FDA CDRH (in the United States) to improve protection against cyber risks. .

REFERENCES

[1] "Implantable Pacemaker Testing Guidance," found at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM081382.pdf.

[2] D. Halperin, et al, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," Proceedings of the 2008 IEEE Symposium on Security and Privacy, Oakland, CA, 2008.

[3] D. Halperin et al, "Security and Privacy for Implantable Medical Devices," in Pervasive Computing, Vol. 7, No. 1, January–March 2008.

[4] S. Capkun, "On Secure Access to Medical Implants," Workshop on Security and Privacy in Implantable Medical Devices, Lausanne, Switzerland, April, 2011.

[5] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body," Proc. Int'l Conf. Parallel Processing (ICPP)Workshops, IEEE CS Press, 2003, pp. 432–439.

[6] T. Denning, et al "Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices," Proceedings of the 28th international conference on Human factors in computing systems, ACM New York, NY, USA, 2010, pp 917-926.

[7] National Institute of Standards and Technology "FIPS Pub 199: Standards for Security Categorization of Federal Information and Information Systems," FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, February 2004.

[8] S. Fischer and M. Zitterbart, "Security in Sensor Networks," Information Technology: Vol. 52, No. 6, 2010, pp. 311-312.