The Challenges of Balancing Safety and Security in Implantable Medical Devices

Konstantinos KATZIS[a,1], Richard W. JONES[b] and George DESPOTOU[c]
[a] *Department of Computer Science and Engineering, European University Cyprus, CY*
[b] *Department of Computer Science, University of York, UK*
[c] *Institute of Digital Healthcare WMG, University of Warwick, UK*

Abstract. Modern Implantable Medical Devices (IMDs), implement capabilities that have contributed significantly to patient outcomes, as well as quality of life. The ever increasing connectivity of IMD's does raise security concerns though there are instances where implemented security measures might impact on patient safety. The paper discusses challenges of addressing both of these attributes in parallel.

Keywords. Implanted Medical Devices, Security, Safety, Reliability, Lifecycle

Introduction

Implantable medical devices, or IMDs, are widely used to improve patient outcomes in presence of numerous conditions as well as contribute to the quality of life. They also enable authorised medical staff to extract useful data regarding the health of the patient for a given period of time. Modern versions of IMDs increasingly offer many of their functions, based on software implementation (e.g. software control of pacemakers). Use of software has also enabled medical device manufacturers to offer more complex functions, as well as features that increase the usability of the device. For example, wireless control of the device, mobile based interfaces, bluetooth enabled data collection, as well as automated update of the software, without the need for a special procedure. IMDs pose numerous challenges to developers with regard to their safety (i.e. harm to patient) as well as security (i.e. breach of privacy, device malfunction due to malicious attacks etc.). Safety of the devices is an intuitive attribute, as an IMD operating in an unintended way, may cause direct harm to the patient. Furthermore, security attacks to the patient can result in loss of privacy of the patient (e.g. loss of their data) or loss of control of the device, which could effectively lead to unintended operation of the IMD. There are numerous reports from researchers, who have managed to breach the security of an IMD [1]. Although the benefits from using IMDs currently far outweigh security risks the ever-increasing connectivity of IMDs will make them vulnerable to potentially more subtle security attacks. There are still security challenges to be overcome to address contemporary security risks [2] with one of the more complex issues being where the design of security measures might be in conflict with safety requirements to the possible detriment of patient health [3].

[1] Corresponding Author: Department of Computer Science and Engineering, 6 Diogenous Street, Engomi, Nicosia, 2404, Cyprus; email: K.Katzis@euc.ac.cy.

This contribution examines some of the trade-offs between safety and security in IMD's – one of the intentions being to increase awareness where 'design for security' might impact the patient safety. The approach to identifying the challenges included a digital library search, as well as review of the main standards applicable to IMDs. The authors picked a representative sample from the results, based on their experience. The literature used the keywords "implanted + medical + device + security" and "'security + medical device + safety". The papers were reviewed by the authors for examples or discussion on the interaction between security design features.

1. Regulatory Frameworks and Implanted Medical Devices

IMDs fall in Class III type of medical devices as defined in the classification procedure of the Code of Federal Regulations, (usually known as 21 CFR 860) [4] and Council Directive 93/42/EEC on Medical Devices [5]. Class III type of devices are expected to support or sustain human life since they are designed to prevent impairment of human health. As stated in [6], the ability of software to implement complex functionality that cannot be implemented at reasonable cost in hardware, makes new kinds of medical devices possible. IMDs, are becoming increasingly pervasive, with current developments being propelled by the ever-increasing capability of processing power, energy efficiency along with power system optimisations [7]. Furthermore, technological advances in ultra-low-power wireless connectivity [8] and the development of numerous lightweight communication protocols [9] have also helped connecting IMDs with the outside world. All these put together have made it possible to provide real-time monitoring and treatment of patients [10]. With the technology mature enough, it's now necessary to consider safety along with security. FDA has recently called for manufacturers to address cybersecurity issues relevant to medical devices from the initial design phase through deployment and end-of-life [11]. FDA's guidance document, does not establish legally enforceable responsibilities. However it describes FDA's intentions on the matter of security in medical devices. As stated in the document: "The extent to which security controls are needed will depend on the medical device, its environment of use, the type and probability of the risks to which it is exposed, and the probable risks to patients from a security breach". The document points out that devices that are connecting to another medical device, or the internet / network are more vulnerable to cybersecurity. It also defines cybersecurity as "the process of preventing unauthorized modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.". According to FDA, cybersecurity is a shared responsibility between stakeholders and failure to address it could lead to compromised device functionality and loss of data. These calls consist draft guidelines for ensuring appropriate medical device security. Nevertheless there is evidence these guidelines will be used by the FDA as grounds for rejection of premarket medical device submissions [2]. Keven Fu in [12] states that the problems in medical device software result largely from a failure to apply well-known systems engineering techniques thus compromising properties such as safety, effectiveness, usability, dependability, reliability, security, and privacy.

2. IMD Design Trade-offs

IMD design process should be based on well-founded security practices to build trustworthy systems. In order to achieve this, designers must consider security in early design stages aiming at encrypting sensitive data where possible. Furthermore, security should be integrated in such a way to improve safety. Current security threads have been identified as: telemetry interface, software and hardware. The telemetry interface threats, which are typically wireless could be subjected to eavesdropping, jamming, interference etc. Software threats, involve access to sensitive information and modification of the logic of the system to affect its operation. Hardware threats involve physical attacks as well as remote attacks caused by an insecure telemetry interface. E.g. there could be unnecessary triggering of the IMD to constantly transmit its readings, thus depleting its battery. Telemetry interface threats can be addressed by employing advanced radio interference mitigation techniques to prevent accidental or intentional interference with the IMDs. Wireless Medical Telemetry Systems (WMTS) [13] and Medical Device Radio-communications Service (MedRadio) [14] radio bands are shared between various radio systems raising concerns about the consequences on the operation of IMDs or medical devices in general. Issues such as jamming, have been addressed in literature [15] through anti-jamming mechanisms. Software threats can be possibly addressed by employing highly secure encryption mechanisms such IMDGuard [16], OPFKA [17] tested for security flaws in [18] – all aiming at protecting access of personal health information. Fu and Blum in [19] state that poor security design could open the backdoor to malware on network medical devices, resulting in unreliable data or actuation, impacting both the integrity and availability of the systems in question. Using traditional cryptographic techniques and protocols in IMDs may be inappropriate due to the limited capabilities of the devices [20]. Hardware threats (apart from physical abuse) can be addressed in a similar way to the telemetry threats since such threats usually involve remote attacks and alteration of sensor data.

3. Systematising safety and security analysis

Future IMDs, are expected to provide numerous functions that will contribute to patient outcomes, such as their safety as well as quality of life. Safety and security (as well as other attributes) can be in conflict. Reconciling these conflicts requires making trade-offs, by identifying the optimum balance in terms of relative security and safety risk. Integrating security in the product development / safety lifecycle is imperative for making future networked type of IMDs safe and secure. According to [11], the manufacturer's approach should appropriately address the following elements: Identification of assets, threats, and vulnerabilities; assessment of the impact of threats and vulnerabilities on device functionality and end users/patients; Assessment of the likelihood of a threat and of a vulnerability being exploited; Determination of risk levels and suitable mitigation strategies and finally Assessment of residual risk and risk acceptance criteria. Although safety and security are two distinct attributes, realising that they can be interdependent, has resulted in unified approaches for, analysing and designing them as well as reconciling conflicts amongst them [21].

4. Conclusions

IMDs implement capabilities that have contributed significantly to patient outcomes, as well as quality of life. Some of these capabilities such as wireless connectivity, pose a possible security threat. This work has highlighted the fact that safety and security (as well as other attributes) can be in conflict. With numerous reports on bridge of security on various IMDs, it is imperative that IMDs address safety as well as security requirements, by employing unified approaches for, analysing and designing them as well as reconciling conflicts amongst them.

References

[1] J. Kirk (2012). Pacemaker hack can deliver deadly 830-volt jolt. Computer World. [cited 20/04/2016], Available from http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver- deadly-830-volt-jolt.htmlA.N. Author, Article title, *Journal Title* **66** (1993), 856–890.

[2] M. Rushanan, A.D. Rubin, D.F. Kune, and C.M. Swanson. 2014. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP '14). IEEE Computer Society, Washington, DC, USA, 524-539.

[3] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, Security and Privacy for Implantable Medical Devices, IEEE Persuasive Computing, Vol. 7, No. 1 January–March 2008

[4] CFR - Code of Federal Regulations Title 21, Part 860 Medical Device Classification Procedure

[5] Guidelines relating to the application of the council directive 93/42/EEC on medical devices, June 2010

[6] NRC. Software for Dependable Systems: Sufficient Evidence? The National Academies Press. 2007

[7] G. Asada, M. Dong, T. S. Lin, F. Newberg, G. Pottie, W. J. Kaiser, and H. O. Marcy, "Wireless integrated network sensors: Low power systems on a chip," in Proc. 24th European Solid-State Circuits Conference (ESSCIRC '98), 1998, pp. 9– 16.

[8] J. Zheng and M. J. Lee, "Will IEEE 802.15.4 make ubiquitous networking a reality?: A discussion on a potential low power, low bit rate standard," IEEE Commun. Mag., vol. 42, no. 6, pp. 140–146, Jun. 2004.

[9] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks," J. Med. Syst., vol. 36, no. 3, pp. 1065–1094, Jun. 2012.

[10] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," Wireless Commun., vol. 17, no. 1, pp. 80–88, Feb. 2010

[11] Content of premarket submissions for management of cybersecurity in medical devices: Draft guidance for industry and Food and Drug Administration staff. 2013 [cited 30/04/2016]

[12] K.Fu, Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report.

[13] Wireless Medical Telemetry Service (WMTS) [cited 20/04/2016], Available from https://www.fcc.gov/general/wireless-medical-telemetry-service-wmts

[14] Medical Device Radiocommunications Service (MedRadio) , FCC, [cited 20/04/2016] Available from https://www.fcc.gov/general/medical-device-radiocommunications-service-medradio

[15] W.Shen, P. Ning, X. He, and H. Dai,"Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in IEEE Symp. on Security and Privacy, 2013.

[16] F.Xu, Z.Qin, C.Tan, B.Wang, and Q.Li,"IMDGuard: Securing implantable medical devices with the external wearable guardian," in Proc. of IEEE INFOCOM, pp. 1862–1870, 2011

[17] C.Hu, X. Cheng, F. Zhangand, D. Wuand, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in Proc. of IEEE INFOCOM, To Appear, 2013.

[18] M. Rostami, W. Burleson, A. Juels and F. Koushanfar, "Balancing security and utility in Medical Devices?," Design Automation Conference (DAC), 2013 50th ACM/EDAC/IEEE, Austin, TX, 2013, pp. 1-6. doi: 10.1145/2463209.2488750

[19] K. Fu and J. Blum, "Inside risks: Controlling for cybersecurity risks of medical device software," Communications of the ACM, vol. 56, no. 10, pp. 21–23, Oct. 2013.

[20] S. Gupta, Implantable Medical Devices - Cyber Risks and Mitigation Approaches, CPS Workshop,

[21] G. Despotou, Managing the Evolution of Dependability Cases for Systems of Systems, PhD Thesis, 2007, University of York, UK