Project title: Development of Security mechanisms for Implantable and Wearable Medical Devices (IWMDs)

Project leader: Dr. Carlo Galuzzi **Function**: Assistant professor, DKE, Maastricht University, NL

Collaborators: Prof. Dr. Ralf Peeters and Dr. Katerina Stankova (Maastricht University, NL), Dr. Christos Strydis (Erasmus MC , NL).

Proposal: Over the past years, we have witnessed a tremendous increase in the use of implantable devices, like cardiovascular, sensory, and neurological implants, as well as wearable devices, like electrocardiogram patches, glucose monitoring systems, and smart hearing technology. Due to the nature of the information collected and processed, these systems should be not only reliable but should also provide various level of security as well as privacy. As a result, there is a need for the development of advanced security mechanisms capable of dealing with the critical nature of these devices. Implantable and wearable medical devices (IWMDs) acquire various kind of data. Pre-processing and analysis of the data is usually done locally, whereas post-processing is usually done on different devices (e.g., computer systems and smartphones) which, therefore, requires reliable means to transmit data using mutual authentication mechanisms. At the same time, when a patient is in an emergency situation, sometimes it is vital to be able to access the data, even without a security access, in order to correctly diagnose the nature of the problem. This means that communication should preserve not only the integrity of the data but also its confidentiality via different authentication mechanisms.

The main focus of IWMDs over the past years has been on collection and (pre, post) processing of the data overlooking security. Anyhow, security should be of main concern as today's devices are extremely sophisticated and equipped with many features. Overlooked security leaves space for malicious entities to improperly operate on a device and seriously harm the health and even the life of an individual. We have already witnessed many examples, which show that such harmful behaviors are possible (e.g., blocking of pacemaker activities as well as altering neurological stimulators or hearing devices). As a result, we should develop adequate security features in order to cope with data security in various ways in both software and hardware. Security mechanisms should prevent various malicious attacks like, data theft, side channel attacks, and fault injection attacks. The main goal of this work is the development of various reliable methodologies for medical device systems in order to cope with system and hardware security and bridge the gap that today exists between security research and hardware development.

Requirements candidate: A highly motivated student with good English communication skills, proactive and resolute attitude and with, preferably, a master degree in (applied) mathematics and knowledge in cryptography and game theory. Knowledge on the following subjects is considered an asset: Matlab, Algorithms (Exact and Approximation), and programming in C++.

Keywords: Implantable and wearable medical devices (IWMDs), Security, Game Theory.

Selected publications:

1. Carmen Camara, Pedro Peris-Lopez, Juan E.Tapiador: Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics Volume 55, June 2015, Pages 272-289
2. D. Arney, K.K. Venkatasubramanian, O. Sokolsky, I. Lee: Biomedical devices and systems security, in: Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2011, pp. 2376–2379.
3. D. Halperin, T.S. Heydt-Benjamin, K. Fu, T. Kohno, W.H. Maisel: Security and privacy for implantable medical devices. IEEE Pervasive Comput., 7 (1) (2008), pp. 30-39
4. P.A. Karger, G.S. Kc, D. Toll: Privacy is essential for secure mobile devices. IBM J. Res. Dev., 53 (2) (2009), pp. 5:1-5:17
5. S. Rane, Y. Wang, S.C. Draper, P. Ishwar: Secure biometrics: concepts, authentication architectures, and challenges. IEEE Signal Process. Mag., 30 (5) (2013), pp. 51-64