Up close and personal: cybersecurity in medical IoT devices

Stefano Zanero, *Senior Member, IEEE*; Eric Evenchick, *Member, IEEE*

***Abstract*— The growing field of cybersecurity encompasses a wide range of challenges, but we argue that none is more pressing and timely than the rising issue of securing devices in the so-called Internet of Things. In particular, we review the challenges in securing IoT devices designed to interact in a highly intimate and personal relationship with the human body, e.g. medical devices. Their unique features, conjoined to a very high potential impact of any security issue, pose specific challenges and require novel approaches and research efforts to be solved.**

I. Extended Abstract

The field of cybersecurity has rapidly risen in status, thanks to the growing perception of the value of the assets that are managed, connected and empowered by computer systems and networks, as well as the growing prevalence of cyber threats (as shown, for instance, in [1]).

One of the emerging fields of ICT, the so-called Internet of Things, is gathering a lot of attention from researchers. In a recent report [2], 70% of the tested systems were found to be vulnerable to different types of attacks.

Among the so-called IoT devices, a class which particularly deserves attention is the category of medical devices, in particular implantable ones. These are growing in prevalence, thanks also to the increasing efficiency and low cost of small scale, sense-actuate embedded systems: In 2001, the estimated number of patients in the United States with an implantable medical device exceeded 25 million [3]. Thanks to ultra-low-power wireless connectivity, and the development of a number of lightweight communication protocols, such systems belong to a so-called Body Area Network (BAN) [4] and can collect a number of physiological values and provide actuation or treatment based on the measurements.

A seminal work exploring the security issues in Implantable Medical Devices (IMDs) is [5], and a good review of the state of the art of medical device security is offered in [6]. While the details vary across different types of devices and architectures, we can easily identify a number of challenges in securing this peculiar class of IoT devices:

- They are designed to interact in a highly intimate and personal relationship with the human body. They require high precision and an impeccable safety record.
- They are often necessarily small in scale, and constrained in power consumption and heat generation.
- They may need to connect wirelessly to be effective, and at the same time require appropriate segmentation and insulation from the public Internet
- Firmware updates might be unfeasible, or risky.

There are also challenges with the mindset of designers and engineers. Safety-critical systems, as well as medical devices, are most often tested according to standards and regulatory specifications: Unfortunately, it is well known that this type of testing is inapplicable, as of our current understanding, to security engineering, where most testing is negative (i.e. conducted by trying to break the system). Also, security assessment and design needs a systemic approach, whereby all components of a system are tested together, observing their interactions.

One of the main challenges in several IoT domains (including, for instance, automotive security) is the lack of a perceived threat level to justify the investment of significant resources. While it seems relatively straightforward to point out the potentially dire consequences of an attack, security investment is a risk-based decision, factoring in the likelihood of an event. The perception of the industry is perhaps shifting, but until now it has been a major factor in slowing down the development and adoption of secure solutions and approaches.

Partially funded by the European Union's H2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement n. 690972.

S. Zanero is with the Politecnico di Milano, Milan, Italy (phone: +39 02 2399 4017; fax: +39 02 2399 3411; e-mail: stefano.zanero@polimi.it).

E. Evenchick is with Linklayer Labs, Toronto, Canada (e-mail: eric@evenchick.com).

Acknowledgment

We would like to recognize and remember the unique, seminal contributions of Barnaby "Barnes" Jack (1977–2013). An inspiration to many, his bright mind and unique skills will always be missed by the security community.

References

[1] "Internet security threat report," Symantec Corporation, Tech. Rep. Vol. 21, April 2016. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[2] "Internet of things research study," HP Fortify, Tech. Rep., 2014. [Online]. Available: http://go.saas.hpe.com/fod/internet-of-things

[3] A. Pope, F. J. Manning, P. Bouxsein, K. E. Hanna *et al.*, *Innovation and Invention in Medical Devices: Workshop Summary*. National Academies Press, 2001.

[4] 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," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[5] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *2008 IEEE Symposium on Security and Privacy*, May 2008, pp. 129–142.

[6] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "Sok: Security and privacy in implantable medical devices and body area networks," in *2014 IEEE Symposium on Security and Privacy*, May 2014, pp. 524–539.