Pacemakers with Internet connection, a not-so-distant goal

January 28 2015

A pacemaker. Credit: UPV/EHU

The healthcare sector is not escaping from the revolution in information and communications technologies. Thanks to the latest advances in microelectronics and communications technologies, it is not difficult to imagine a future with medical sensors connected to the Internet. Thanks to the Ladon security protocol developed by the UPV/EHU researcher Jasone Astorga in the 12T research group, a little more progress has been made in the area of the remote monitoring of patients by means of implanted sensors.

The ageing of society needs new, more cost-effective solutions to improve the life quality of patients and cut the burden that is placed on the social welfare system. In modern western societies the fitting of pacemakers and implantable cardioverter defibrillators (ICDs) is growing rapidly. Devices of this type control heart rhythm and, if necessary, send an appropriate response to make the heart beat at the right rhythm. They also record heart activity patterns when abnormal heart rhythm is detected. This information is periodically checked and monitored by a doctor to plan future treatment. To do this, the information is transmitted in wireless mode to an external device. At the moment this communication is carried out in hospitals.

The main manufacturers of pacemakers and DCIs have started to market remote management devices. The remote monitoring of implantable, wireless medical sensors is a constantly advancing field which nevertheless still has clear shortcomings. The direct connection of medical sensors to the Internet is the next natural step in this evolution, and will enable doctors to obtain the information stored by the sensors at any moment and from any device connected to the Internet. Despite its great potential, the success of a monitoring system of this type is determined, among other things, by the protection of the privacy of the information transmitted. A researcher in the UPV/EHU's Department of Communications Engineering has developed the Ladon security protocol, an efficient mechanism to authenticate, authorise and establish the end-to-end keys (keys for communication between the terminal used by the doctor and the patient's device), which offers revolutionary features for sensors of this type.

Energy efficiency, memory space and latency

There are three key parameters in the development of new solutions for implantable medical sensors: energy consumption, memory space and latency. Energy efficiency is the most important design parameter for

any protocol that has to work in these devices, since replacing the batteries used in them means opening up a wound in the patient's chest. As the UPV/EHU researcher Jasone Astorga explained, it has been found that "the energy consumption of this Ladon protocol is negligible in comparison with the usual consumption of a pacemaker or ICD when applying its therapy (stimulating or defibrillating), and has no significant impact on how long the batteries last". On the other hand, they have found that the deployment of this security application in the sensors has led to very little memory consumption. And finally, the latency incorporated by the protocol in the setting up of a secure communication is also less. All this turns it into a protocol suited to deploying functionalities to authenticate and control access in the sensors and for the setting up of a secret key that can be used to protect the confidentiality and integrity of the medical information transmitted over the wireless network.

Apart from its application in the remote monitoring of medical sensors, all the checks carried out in relation to the protocol lead to the conclusion that this is a protocol to authenticate, authorise and set up the keys that is right for use even in the securization of critical applications from the point of view of delay, like remote surgery, for example. In any case, the possibility of marketing this protocol for these purposes is still a long way off, as validations would have to be conducted on real pacemakers. "We have carried out our validation on a commercial sensor, not on a real pacemaker," said the researcher. In other words, "one would have to conduct studies using real medical sensors and real patients," explained Astorga. "In any case, we believe that it is a step forward down the road along which the remote monitoring of patients using implanted medical sensors can go on advancing."

More information: J. Astorga, J. C. Astorga, E. Jacob, N. Toledo, M. Higuero (2014). "Securing access to next generation IP-enabled pacemakers and ICDs using Ladon", Journal of Ambient Intelligence and

Smart Environments, ISSN: 1876-1364, vol. 6, nº 2, 157-177.

J. Astorga, E. Jacob, N. Toledo, M. Aguado (2014). "Analytical Evaluation of a Time- and Energy-Efficient Security Protocol for IP-enabled Sensors", Computers and Electrical Engineering, ISSN: 0045-7906, vol. 40, nº 2, 539-550.

J. Astorga, E. Jacob, M. Huarte, M. Higuero (2012). "Ladon: End-to-end Authorization Support for Resource-Deprived Environments", IET Information Security, ISSN: 1751-8709, vol. 6, nº 2, 93-101.

Provided by University of the Basque Country