Reasrach article of the issue

Light-Weight and Effective Security Schemes for Wireless Medical Devices (NPRP No.: 8-408-2-172)

By Prof. Mohsen Guizani

Wireless medical devices have been widely used to treat various diseases and to help patients overcome difficulties. There are many different types of these wireless medical devices, such as wireless insulin pumps, pacemakers, cardiac defibrillators, neuro stimulators and various drug delivery systems. The US FDA reported that about 375,000 adults used insulin pumps in 2007. The market is expected to grow exponentially. The use of such devices can have many benefits and some risks. Using these devices should increase the patient mobility by eliminating wires that bind a patient to a medical bed, provide health care professionals the ability to remotely program devices, and give physicians remote access and monitoring of patient's data regardless of the physical location. They can also access patients' real-time data without being physically in the hospital and allowing device adjustment and patient treatment. Remote monitoring can detect problems with senior citizens and/or chronic disease patients before more serious consequences occur. Since this technology continues to evolve, it is important to keep in mind its potential for interference with pacemakers, implantable cardioverter defibrillators (ICDs), and implantable medical devices (MDs). Therefore, health care facilities should pay attention to the selection of the wireless technology used, quality of service (QoS), electromagnetic compatibility (EMC), coexistence, and security.

Unfortunately, most existing wireless medical devices lack sufficient security mechanisms to protect patients from malicious attacks. With the rise of using such devices, security becomes so critical due to the fact that such attacks may hurt or even kill patients. An attacker may launch several different kinds of attacks on wireless medical devices. For instance, an adversary may activate a magnetic switch within a pacemaker or implantable cardioverter defibrillator (ICDs) by using a sufficiently strong magnetic field. The current access is based on a magnetic switch but it does not require any authentication, which is a serious security concern. The medical device vulnerabilities provide opportunities for an adversary to monitor or even change the parameters/function of a medical device remotely. Without sufficient security protection on medical devices, the consequences could be fatal.

Therefore, it is essential to find solutions to fully secure these devices. First, securing such tiny devices can pose many challenges due to their very limited resources. These limitations include, but are not limited to energy supply, processing power, and storage space. For example, an implantable medical device (IMD) with a small battery is expected to operate for several weeks, months or even years. A PRIZM 2 ICD typically lasts 4 to 6 years. Furthermore, because an IMD is embedded in the human body, it may need surgery to change the battery (not practical in many cases). In addition, most medical devices have very limited storage. For example, a medical device manufactured in 2002 (which is still being used today) contains only 8 KB of RAM/ROM**Error!**