Cyber-Med: Risk Assessment and Practical Detection Methodology of Cyber Attacks Aimed at Medical Device Ecosystems

Researchers

Dr. Nir Nissim
nirni.n@gmail.com

Erez Shalom
erezsh@post.bgu.ac.il

Prof. Yuval Shahar
yshahar@bgu.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

N. Nissim, T. Mahler, E. Shalom, I. Goldenberg, G. Hasman, A. Makori, I. Kochav, Y. Elovici, and Y. Shahar, "Know Your Enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices," RSNA Conference, Chicago, 2017.

N. Nissim, E. Shalom, Y. Shahar, and Y. Elovici, "Cyber-Med: Risk Assessment and Practical Detection Methodology of Cyber-Attacks Aimed at Medical Device Eco-Systems, " 18th International Conference on Big Data in Biomedicine (ICBDB), Buenos Aires, 2016.

Goals

In an initial survey, we found more than 15 types of vulnerabilities and possible attacks aimed at medical devices and their eco-system. Many of these attacks target individual patients who use devices such as pacemakers and insulin pumps. In addition, such attacks are also aimed at additional medical devices that are widely used by medical centers, such as MRIs, CTs, and dialysis engines; at the information systems that store patient information, including diagnoses (clinical images, test results, etc.), and are used as the basis for decisions related to patient care; at the information systems that store patient information, including diagnoses, and are used as the basis of decisions relating to patient care; at protocols such as DICOM; at standards such as HL7; and at medical information systems such as PACS.

Current detection tools, techniques, and solutions generally fail to detect both the known and unknown attacks launched against medical devices. Very little research has been conducted to protect these devices from cyber-attacks, since most of the development and engineering efforts are focused on core medical functionality, contribution to patient care, and associated business aspects.

We propose to develop and implement Cyber-Med, a unique collaborative project of Ben-Gurion University of the Negev and Clalit Health Services' Health Maintenance Organization.

Description

Cyber-Med focuses on a thorough risk analysis of the vulnerabilities associated with medical devices and the development of a comprehensive detection framework that relies on a critical attack repository that we that aim to create. The Cyber-Med detection framework will consist of two independent, but complementary detection approaches: one for known attacks, and the other for unknown attacks. These modules incorporate novel ideas and algorithms inspired by our team's domains of expertise, including cyber security, biomedical informatics, and advanced machine learning, and temporal data mining techniques. Establishment and maintenance of Cyber-Med's attack repository will strengthen Cyber-Med's detection framework. The attack repository's infrastructure will enable researchers to record, document, create, and simulate existing and new attacks on MDs, which, in turn, will maintain the detection framework's capabilities by incorporating up-to-date knowledge regarding new attacks.