World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Cyber-Med: Practical Detection Methodology of Cyber-Attacks Aimed at Medical Devices Eco-Systems

Authors : Nir Nissim, Erez Shalom, Tomer Lancewiki, Yuval Elovici, Yuval Shahar

Abstract : Background: A Medical Device (MD) is an instrument, machine, implant, or similar device that includes a component intended for the purpose of the diagnosis, cure, treatment, or prevention of disease in humans or animals. Medical devices play increasingly important roles in health services eco-systems, including: (1) Patient Diagnostics and Monitoring; Medical Treatment and Surgery; and Patient Life Support Devices and Stabilizers. MDs are part of the medical device eco-system and are connected to the network, sending vital information to the internal medical information systems of medical centers that manage this data. Wireless components (e.g. Wi-Fi) are often embedded within medical devices, enabling doctors and technicians to control and configure them remotely. All these functionalities, roles, and uses of MDs make them attractive targets of cyber-attacks launched for many malicious goals; this trend is likely to significantly increase over the next several years, with increased awareness regarding MD vulnerabilities, the enhancement of potential attackers' skills, and expanded use of medical devices. Significance: We propose to develop and implement Cyber-Med, a unique collaborative project of Ben-Gurion University of the Negev and the Clalit Health Services Health Maintenance Organization. Cyber-Med focuses on the development of a comprehensive detection framework that relies on a critical attack repository that we aim to create. Cyber-Med will allow researchers and companies to better understand the vulnerabilities and attacks associated with medical devices as well as providing a comprehensive platform for developing detection solutions. Methodology: 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. The establishment and maintenance of Cyber-Med's up-to-date attack repository will strengthen the capabilities of Cyber-Med's detection framework. Major Findings: Based on our initial survey, we have already found more than 15 types of vulnerabilities and possible attacks aimed at MDs and their eco-system. Many of these attacks target individual patients who use devices such pacemakers and insulin pumps. In addition, such attacks are also aimed at MDs that are widely used by medical centers such as MRIs, CTs, and dialysis engines; the information systems that store patient information; protocols such as DICOM; standards such as HL7; and medical information systems such as PACS. However, current detection tools, techniques, and solutions generally fail to detect both the known and unknown attacks launched against MDs. Very little research has been conducted in order to protect these devices from cyber-attacks, since most of the development and engineering efforts are aimed at the devices' core medical functionality, the contribution to patients' healthcare, and the business aspects associated with the medical device.

Keywords : medical device, cyber security, attack, detection, machine learning
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020