HealthManagement
Promoting Management and Leadership

Hacking the AI to protect imaging devices

Radiology and medical imaging is continuously experiencing rapid enhancements including quality of patient care as a result of uncovering new aspects of the vast potential of artificial intelligence implementation in clinical practice. As more hospital medical imaging equipment connects to the internet, cyberattacks and malicious software vulnerabilities present a clear and present danger.

Tom Mahler Ph.D. candidate and researcher at the Ben-Gurion University of the Negev (BGU) Cyber@BGU, and his team have been developing solutions using AI in a proactive approach to get ahead of any potential future threats.

"In the current phase of our research, we focus on developing an anomaly detection system using advanced AI methods to train the system with actual commands recorded from actual equipment," said Tom Mahler. "Our solution monitors the outgoing commands from the device before they are executed, and will alert—and possibly halt—if it detects anomalies."

You may also like: Facebook and NYU fastMRI project: largest-ever open source dataset using AI for 10X faster MRI's

Contrary to how others approach this, by creating shields and protocols to protect an entire hospital network, Mahler and his team of colleagues wanted to focus on the device as they see it to be the last line of defence to prevent as many potential attacks as possible for medical imaging devices. As AI rapidly increases the potential of solutions and applications, hackers lurking behind the scenes are constantly challenging the resolve of systems.

In his wittingly themed presentation "CTrl-Alt-Radiate?" at the Radiological Society of North America (RSNA) annual meeting, Mahler showed a captive audience how a CT machine's security can be breached and the device be manipulated by a hacker. Changing ionizing radiation doses on a CT could alter the image itself and possibly harm the patient as well. As with every effort to create protection from hacking, the first step is to hack the system you want to protect to find where it's vulnerable and find a way to eliminate that risk.

Connecting devices to the internet has opened a whole new dimension to healthcare and radiology is one of the fields that has benefited the most, being able to access better diagnosis faster, optimising the management and transfer of medical images and patients records. X-ray, mammography, MRI and CT medical imaging devices are the centre of diagnosis and treatment. When a machine is connected this usually happens by way of the hospital networks, which can and have been hacked as massive data breaches and cyberattacks in recent years have caught gatekeepers unprepared.

"The medical information device development process, from concept to market, takes three to seven years. Cyber threats can change significantly over that period, which leave medical imaging devices highly vulnerable," Mahler says. "If health care manufacturers and hospitals take a proactive approach, we can prevent such attacks from happening in the first place."

To detect anomalies, the researchers created a system using advanced machine learning and deep learning methods, with training data coming from actual commands recorded from real devices. The system learns to recognise normal commands and to predict whether a new command is legitimate or not. In case an attacker sends a malicious command the system will detect and alert the device operator before the command is executed.

Mahler noted that although these types of attacks are theoretically possible, there is no indication that they have ever actually occurred.

"If health care manufacturers and hospitals will take a proactive approach, we could prevent such attacks from happening in the first place," he said.

In the future the researchers plan to expand this process by collecting more scans from different devices and sites to develop a more accurate model.

Sources: Radiological Society of North America (RSNA), AMERICAN ASSOCIATES, BEN-GURION UNIVERSITY OF THE NEGEV, CSRC - Cyber Security Research Center @ Ben-Gurion University
Image Credit: iStock

Published on : Tue, 4 Dec 2018