Researchers aim to prevent medical imaging cyberattacks

27 November 2018

Two new studies being presented this week at the annual meeting of the Radiological Society of North America (RSNA) address the potential risk of cyberattacks in medical imaging.

The Internet has been highly beneficial to health care—radiology included—improving access in remote areas, allowing for faster and better diagnoses, and vastly improving the management and transfer of medical records and images. However, increased connectivity can lead to increased vulnerability to outside interference.

Researchers and cybersecurity experts have begun to examine ways to mitigate the risk of cyberattacks in medical imaging before they become a real danger.

Medical imaging devices, such as X-ray, mammography, MRI and CT machines, play a crucial role in diagnosis and treatment. As these devices are typically connected to hospital networks, they can be potentially susceptible to sophisticated cyberattacks, including ransomware attacks that can disable the machines. Due to their critical role in the emergency room, CT devices may face the greatest risk of cyberattack.

In a study presented today, researchers from Ben-Gurion University of the Negev in Beer-Sheva, Israel, identified areas of vulnerability and ways to increase security in CT equipment. They demonstrated how a hacker might bypass security mechanisms of a CT machine in order to manipulate its behavior. Because CT uses ionizing radiation, changes to dose could negatively affect image quality, or—in extreme cases—pose harm to the patient.

"In the current phase of our research, we focus on developing solutions to prevent such attacks in order to protect medical devices," said Tom Mahler, Ph.D. candidate and teaching assistant at Ben-Gurion University of the Negev. "Our solution monitors the outgoing commands from the device before they are executed, and will alert—and possibly halt—if it detects anomalies."

For anomaly detection, the researchers developed a system using various advanced machine learning and deep learning methods, with training data consisting of actual commands recorded from real devices. The model learns to recognize normal commands and to predict if a new, unseen command is legitimate or not. If an attacker sends a malicious command to the device, the system will detect it and alert the operator before the command is executed.

"In cybersecurity, it is best to take the 'onion' model of protection and build the protection in layers," Mahler said. "Previous efforts in this area have focused on securing the hospital network. Our solution is device-oriented, and our goal is to be the last line of defense for medical imaging devices."

He added that it is also important to note that although these types of attacks are theoretically possible, there is no indication that they 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.

A second study, to be presented tomorrow, looked at the potential to tamper with mammogram results.

The researchers trained a cycle-consistent generative adversarial network (CycleGAN), a type of artificial intelligence application, on 680 mammographic images from 334 patients, to convert images showing cancer to healthy ones and to do the same, in reverse, for the normal control images. They wanted to determine if a CycleGAN could insert or remove cancer-specific features into mammograms in a realistic fashion.

"As doctors, it is our moral duty to first protect our patients from harm," said Anton S. Becker, M.D., radiology resident at University Hospital Zurich and ETH Zurich, in Switzerland. "For example, as radiologists we are used to protecting patients from unnecessary radiation. When neural networks or other algorithms inevitably find their way into our clinical routine, we will need to learn how to protect our patients from any unwanted side effects of those as well."

The images were presented to three radiologists, who reviewed the images and indicated whether they thought the images were genuine or modified. None of the radiologists could reliably distinguish between the two.

"Neural networks, such as CycleGAN, are not only able to learn what breast cancer looks like," Dr. Becker said, "we have now shown that they can insert these learned characteristics into mammograms of healthy patients or remove cancerous lesions from the image and replace them with normal looking tissue."

Dr. Becker anticipates that this type of attack won't be feasible for at least five years and said patients shouldn't be concerned right now. Still, he hopes to draw the attention of the medical community, and hardware and software vendors, so that they may make the necessary adjustments to address this issue while it is still theoretical.

Dr. Becker said that artificial intelligence, in general, will greatly enrich radiology, offering faster diagnoses and other advantages. He added that there are positive aspects to these findings as well.

"Neural networks can teach us more about the image characteristics of certain cancers, making us better doctors."

Provided by Radiological Society of North America