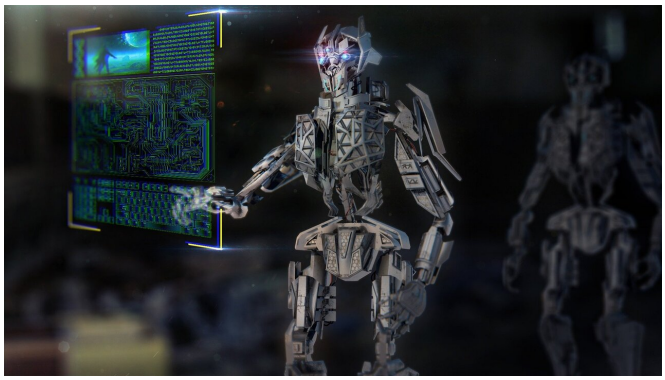
New technique to prevent imaging cyberthreats proposed by researchers

25 August 2020



Credit: Pixabay/CC0 Public Domain

Researchers at Ben-Gurion University of the Negev have developed a new artificial intelligence technique that will protect medical devices from malicious operating instructions in a cyberattack as well as other human and system errors.

BGU researcher Tom Mahler will present his research, "A Dual-Layer Architecture for the Protection of Medical Devices from Anomalous Instructions" on August 26 at the 2020 International Conference on Artificial Intelligence in Medicine (AIME 2020). Mahler is a Ph.D. candidate under the supervision of BGU Profs. Yuval Elovici and Prof. Yuval Shahar in the BGU Department of Software and Information Systems Engineering (SISE).

Complex medical devices such as CT (computed tomography), MRI (magnetic resonance imaging) and ultrasound machines are controlled by instructions sent from a host PC. Abnormal or anomalous instructions introduce many potentially harmful threats to patients, such as radiation overexposure, manipulation of device components or functional manipulation of medical images. Threats can occur due to cyberattacks, human errors such as a technician's configuration mistake or host PC software bugs.

As part of his Ph.D. research, Mahler has developed a technique using artificial intelligence that analyzes the instructions sent from the PC to the physical components using a new architecture for the detection of anomalous instructions.

"We developed a dual-layer architecture for the protection of medical devices from anomalous instructions," Mahler says. "The architecture focuses on detecting two types of anomalous instructions: (1) context-free (CF) anomalous instructions which are unlikely values or instructions such as giving 100x more radiation than typical, and (2) context-sensitive (CS) anomalous instructions, which are normal values or combinations of values, of instruction parameters, but are considered anomalous relative to a particular context, such as mismatching the intended scan type, or mismatching the patient's age, weight, or potential diagnosis.

"For example, a normal instruction intended for an adult might be dangerous [anomalous] if applied to an infant. Such instructions may be misclassified when using only the first, CF, layer; however, by adding the second, CS, layer, they can now be detected."

The research team evaluated the new architecture in the computed tomography (CT) domain, using 8,277 recorded CT instructions and evaluated the CF layer using 14 different unsupervised anomaly detection algorithms. Then they evaluated the CS layer for four different types of clinical objective contexts, using five supervised classification algorithms for each context.

Adding the second CS layer to the architecture improved the overall anomaly detection performance from an F1 score of 71.6%, using only the CF layer, to between 82% and 99%, depending

on the clinical objective or the body part.
Furthermore, the CS layer enables the detection of CS anomalies, using the semantics of the device's procedure, an anomaly type that cannot be detected using only the CF layer.

Provided by American Associates, Ben-Gurion University of the Negev