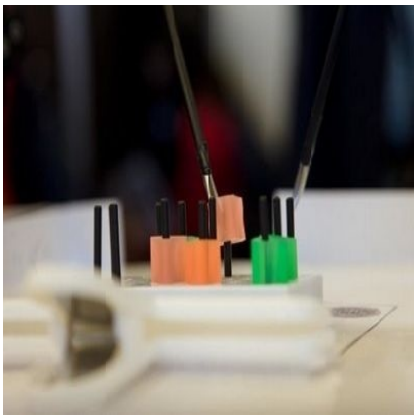
HealthManagement.org
Promoting Management and Leadership

How Safe is That Robot Doing Your Surgery?



Researchers at University of Washington have conducted a series of experiments revealing vulnerabilities of next generation teleoperated surgical robots. The aim was to test how some forms of cyberattacks could hijack remotely-controlled operations in the future and to make those systems more secure.

Use of teleoperated robots, which are controlled by a human who may be in another physical location, is expected to increase as the technology evolves. Outside of a handful of experimental surgeries performed remotely, doctors typically use surgical robots today to operate on a patient in the same room using a secure, hardwired connection. However, telerobots may one day routinely provide medical treatment in underdeveloped rural areas, battlefield scenarios, Ebola wards or catastrophic disasters happening half a world away.

In two recent papers, UW BioRobotics Lab researchers showed that next generation teleoperated robots using nonprivate networks -- which may be the only option in disasters or in remote areas -- can be easily hacked or disrupted by common forms of cyberattacks. Incorporating security measures to prevent those attacks, the researchers note, will be critical to their safe adoption and use.

"We want to make the next generation of telerobots resilient to some of the threats we've detected without putting an operator or patient or any other person in the physical world in danger," says lead author Tamara Bonaci, a UW doctoral candidate in electrical engineering.

For their research, the UW team mounted common types of cyberattacks as study participants used a teleoperated surgical robot developed at the UW for research purposes to move rubber blocks between pegs on a pegboard. For example, during denial-of-service attacks -- in which the attacking machine flooded the system with useless data -- the robots became jerky and harder to use. Using a single packet of bad data, the team also was able to maliciously trigger the robot's emergency stop mechanism, rendering it useless.

In some cases, the human operators were eventually able to compensate for those disruptions, given the relatively simple task of moving blocks. In situations where precise movements can mean the difference between life and death (eg, surgery), such malicious attacks could have more serious consequences, according to researchers.

The tests were conducted with the Raven II, an open source teleoperated robotic system designed to support research in advanced techniques of robotic-assisted surgery. The system is not currently in clinical use and is not approved by the FDA.

"In an ideal world, you'd always have a private network and everything could be controlled, but that's not always

going to be the case. We need to design for and test additional security measures now, before the next generation of telerobots are deployed," says Howard Chizeck, UW professor of electrical engineering and co-director of the UW BioRobotics Lab.

Encrypting data packets that flow between the robot and human operator would help prevent certain types of cyberattacks. This, however, is not effective against denial-of-service attacks that bog down the system with extraneous data. With video, encryption also runs the risk of causing unacceptable delays in delicate operations, the researchers explain.

To enhance security of robotic systems, the UW team is also developing the concept of "operator signatures," which leverage the ways in which a particular surgeon or other teleoperator interacts with a robot to create a unique biometric signature. By tracking the forces and torques that a particular operator applies to the console instruments and his or her interactions with the robot's tools, the researchers have developed a novel way to validate that person's identity and authenticate that the operator is the person he or she claims to be.

Source and image source: University of Washington

Published on : Mon, 11 May 2015