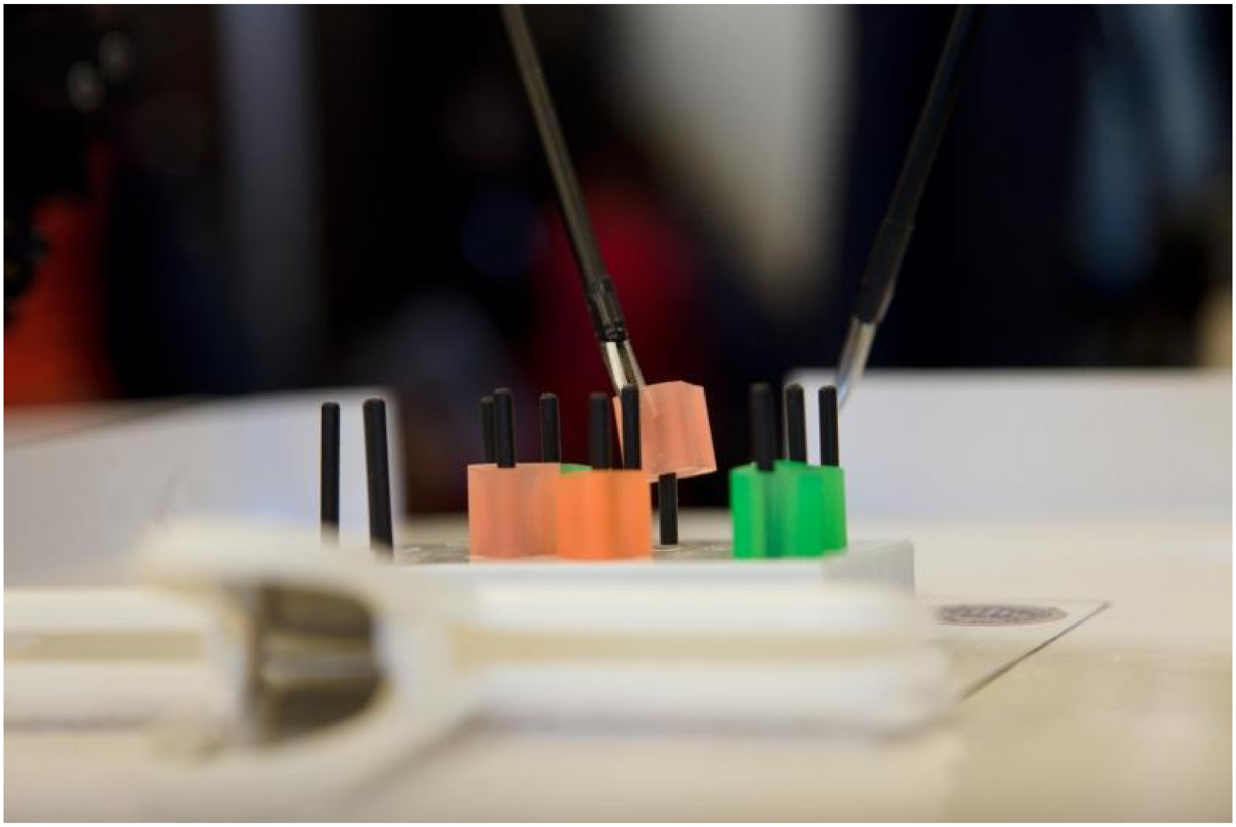
PHYS.ORG

Researchers hack a teleoperated surgical robot to reveal security flaws

May 7 2015, by Jennifer Langston



UW reseachers mounted cyberattacks while study participants used the Raven II surgical robotic system to move rubber blocks on a pegboard. Credit: University of Washington

To make cars as safe as possible, we crash them into walls to pinpoint weaknesses and better protect the people who use them.

That's the idea behind a series of experiments conducted by a University of Washington engineering team who hacked a next generation teleoperated surgical robot—one used only for research purposes—to test how easily a malicious attack could hijack remotely-controlled operations in the future and to make those systems more secure.

Real-world teleoperated robots, which are controlled by a human who may be in another physical location, are expected to become more commonplace as the technology evolves. They're ideal for situations that are dangerous for people: fighting fires in chemical plants, diffusing explosive devices or extricating earthquake victims from collapsed buildings.

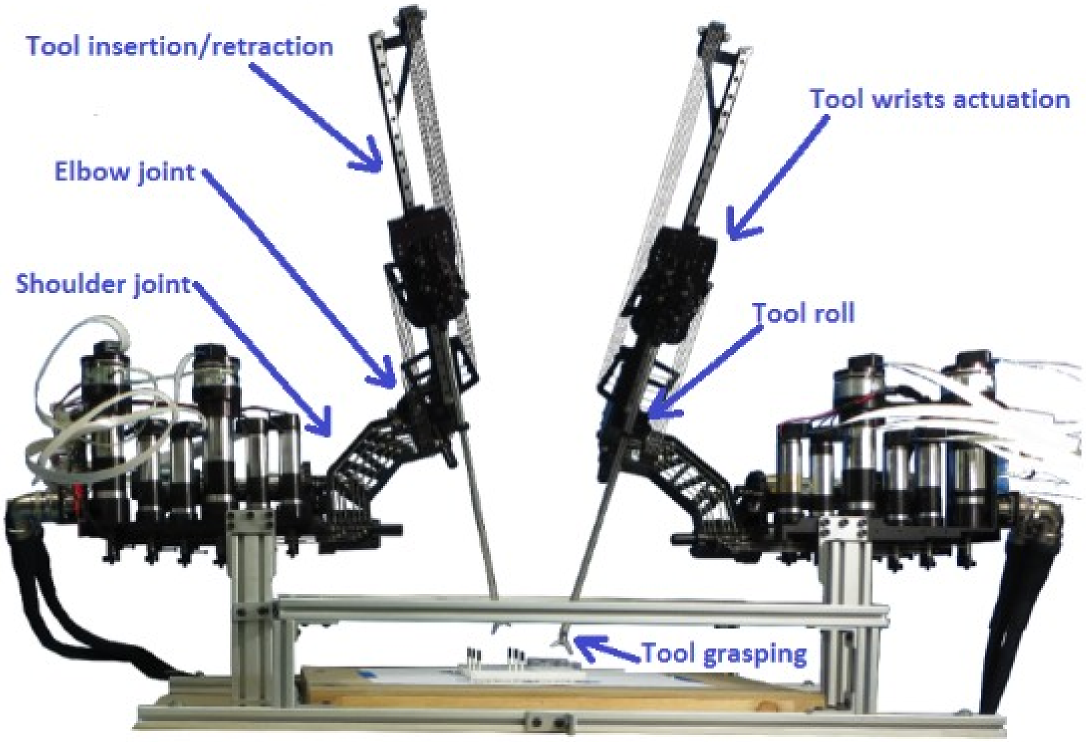
Outside of a handful of experimental surgeries conducted remotely, doctors typically use surgical robots today to operate on a patient in the same room using a secure, hardwired connection. But telerobots may one day routinely provide medical treatment in underdeveloped rural areas, battlefield scenarios, Ebola wards or catastrophic disasters happening half a world away.

In two recent papers, UW BioRobotics Lab researchers demonstrated that next generation teleoperated robots using nonprivate networks—which may be the only option in disasters or in remote locations—can be easily disrupted or derailed by common forms of cyberattacks. Incorporating security measures to foil those attacks, the authors argue, 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," said lead author Tamara Bonaci, a UW doctoral candidate in electrical engineering.

To expose vulnerabilities, 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.

By mounting "man in the middle" attacks, which alter the commands flowing between the operator and robot, the team was able to maliciously disrupt a wide range of the robot's functions—making it hard to grasp objects with the robot's arms—and even to completely override command inputs. During denial-of-service attacks, in which the attacking machine flooded the system with useless data, the robots became jerky and harder to use.



Raven II was developed by UW researchers to explore the boundaries of robotic-assisted surgery. Credit: University of Washington

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—such as surgery or a search and rescue extrication—these types of cyberattacks could have more serious consequences, the researchers believe.

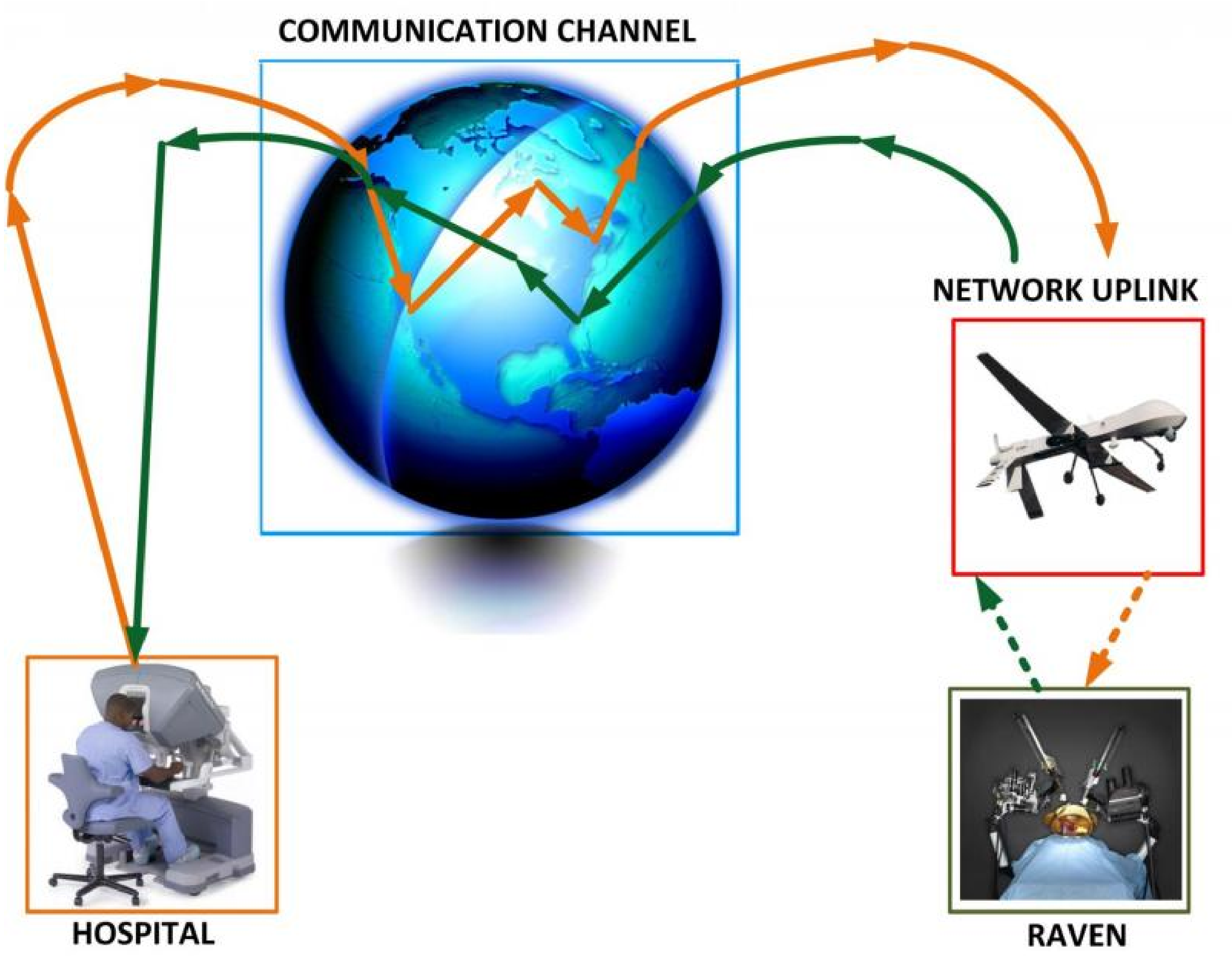
With a single packet of bad data, for instance, the team was able to maliciously trigger the robot's emergency stop mechanism, rendering it useless.

The tests were conducted with the Raven II, an open source teleoperated robotic system developed by UW electrical engineering professor Blake Hannaford and former UW professor Jacob Rosen, along with their students. Raven II, currently manufactured and sold by Seattle-based Applied Dexterity Inc., a UW spin-out, is a next generation 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.

The surgical robots that are FDA-approved for clinical use today, which typically allow a surgeon to remove tumors, repair heart valves or perform other procedures in a less invasive way, use a different communication channel and typically do not rely on publicly available networks, which would make the cyberattacks the UW team tested much harder to mount.

But if teleoperated robots will be used in locations where there's no secure alternative to networks or other communication channels that are easy to hack, it's important to begin designing and incorporating additional security features now, the researchers argue.

"If there's been a disaster, the network has probably been damaged too. So you might have to fly a drone and put a router on it and send signals up to it," said Howard Chizeck, UW professor of electrical engineering and co-director of the UW BioRobotics Lab.



In future telerobotic procedures, the last communication link may a wireless uplink (dotted lines) to a drone or satellite that is more easily hacked than pre-established network connections (solid lines.) Credit: University of Washington

"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."

Encrypting data packets that flow between the robot and human operator would help prevent certain types of cyberattacks. But it isn't 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 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.

Moreover, monitoring those actions and reactions during a telerobotic procedure could give early warning that someone else has hijacked that process.

"Just as everyone signs something a little bit differently and you can identify people from the way they write different letters, different surgeons move the robotic system differently," Chizeck said. "This would allow us to detect and raise the alarm if all of a sudden someone who doesn't seem to be operator A is maliciously controlling or interfering with the procedure."

More information: brl.ee.washington.edu/teleoper … eoperationsecurity/

Provided by University of Washington

Citation: Researchers hack a teleoperated surgical robot to reveal security flaws (2015, May 7) retrieved 24 April 2024 from https://phys.org/news/2015-05-hack-teleoperated-surgical-robot-reveal.html