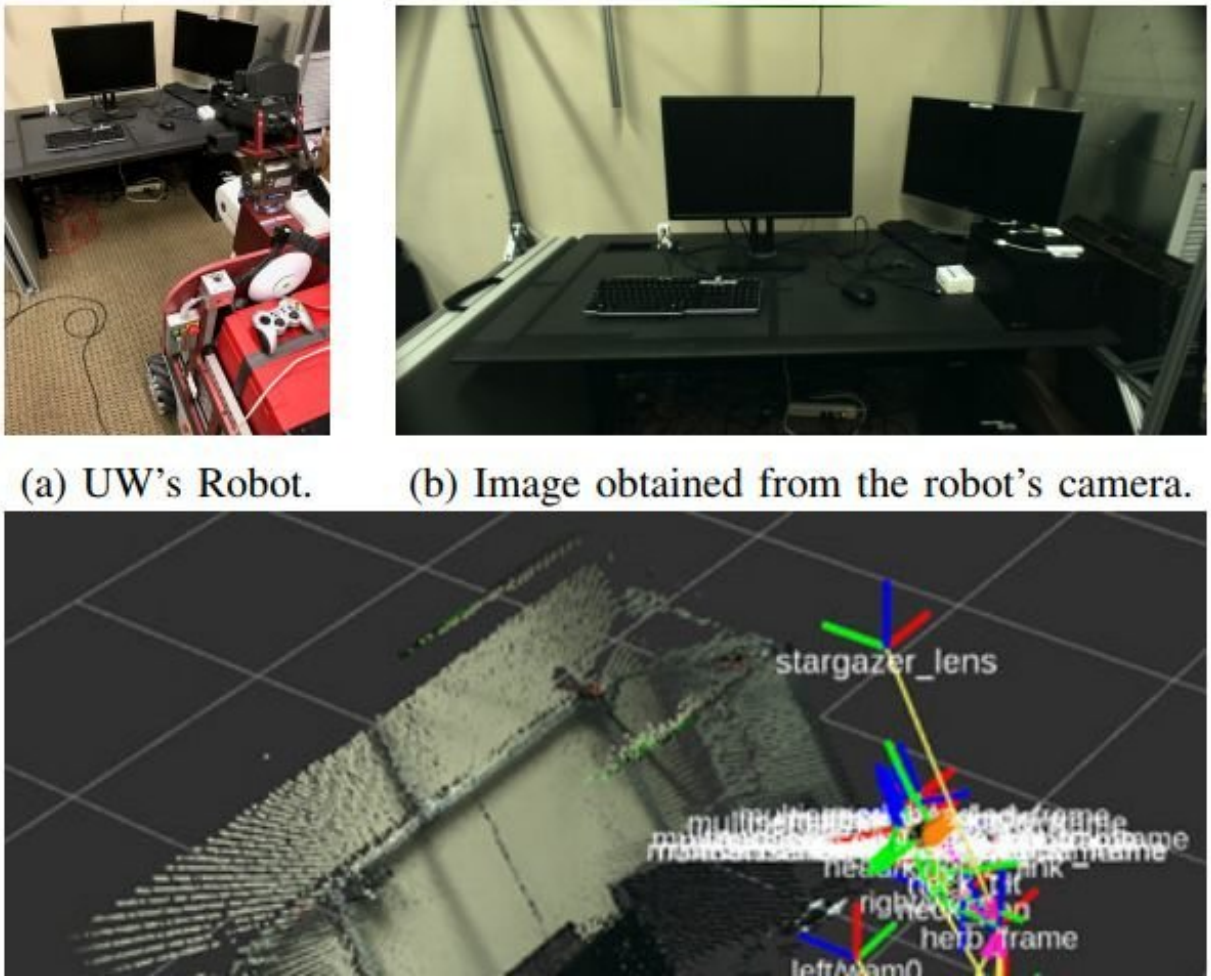
No sweat on Brown University team trying to hack a robot

August 28 2018, by Nancy Owano



Images obtained from the robot's camera. Credit: arXiv:1808.03322 [cs.CR]

As we heat up to the ideas of having assistive robots in our homes and in industry, we also feel the chill of sci-fi imaginations that obsess over robots turning rogue.

Should we travel toward some kind of warm spot in the middle? We can celebrate robotics designs but work out policies and practices to prevent mayhem?

A team of researchers at Brown discovered what could happen when you connect your ROS-loaded robot to the internet.

SCENE (For real) Herb2 is a robot that was built by researchers at the University of Washington. It is at home in its lab at the University of Washington. It speaks. "Hello from the hackers."

The people directing the robot to talk were off and away at Brown University. A simple recap of their work was provided in the *Wired* article by Matt Simon. "We could read the camera, essentially spying," said roboticist Stefanie Tellex. "We could see where its arms were and they were moving. There was a text-to-speak API so we could have the robot mysteriously talk to you."

The point of all this was that hacking the robot was possible and it was not difficult. Researchers scanned for internet-connected research robots in labs and then took command.

Their research is described in detail in "Scanning the Internet for ROS: A View of Security in Robotics Research," which is now on arXiv.

The authors said, "As a proof of concept, and with consent, we were able to read image sensor information and move the robot of a research group in a US university."

Why was it easy? The answer involves ROS (stands for Robot Operating System).

Daniel Starkey, *Geek.com*, had this to say about ROS: "Essentially, designing robots is hard, and many use an open-source collection of software called Robot Operating System, or ROS."

Starkey also noted that "this system lacks basic security features, is widely used, and the source code is free to probe." Kristin Houser in *Futurism* called it "the perfect target" for the Brown team.

It's an open-source collection of software libraries and tools useful for building robots. But the phrase "operating system" calls for further clarification. Simon said in *Wired* that "it's more middleware that runs on top of something like Linux. But if you've got something like a Baxter research robot, you can use ROS to get the thing to do science."

Nonetheless, the researchers' goal was not to belittle ROS. The authors said in their paper, that "Our goal is not to single out any researchers or robot platforms, but to promote security as an important consideration—not just in production systems, but in research settings as well."

How they carried out their research: They scanned the internet—they asked, which robots are running ROS? On finding robots that were vulnerable, they told the robots' owners the robots were vulnerable but they made a special case of Herb2. Instead, they asked the owners if they could please prove they could hack it.

Houser's verdict was that "if we don't want them suddenly acting as puppets for malicious actors, we're going to need to pay a lot more attention to their security."

At *Wired*, meanwhile, the article offered user advice. "If you are going to hook up your robot to the internet, maybe consider a firewall or VPN."

More information: Scanning the Internet for ROS: A View of Security in Robotics Research, arXiv:1808.03322 [cs.CR] arxiv.org/abs/1808.03322

Abstract

Because robots can directly perceive and affect the physical world, security issues take on particular importance. In this paper, we describe the results of our work on scanning the entire IPv4 address space of the Internet for instances of the Robot Operating System (ROS), a widely used robotics platform for research. Our results identified that a number of hosts supporting ROS are exposed to the public Internet, thereby allowing anyone to access robotic sensors and actuators. As a proof of concept, and with consent, we were able to read image sensor information and move the robot of a research group in a US university. This paper gives an overview of our findings, including the geographic distribution of publicly-accessible platforms, the sorts of sensor and actuator data that is available, as well as the different kinds of robots and sensors that our scan uncovered. Additionally, we offer recommendations on best practices to mitigate these security issues in the future.