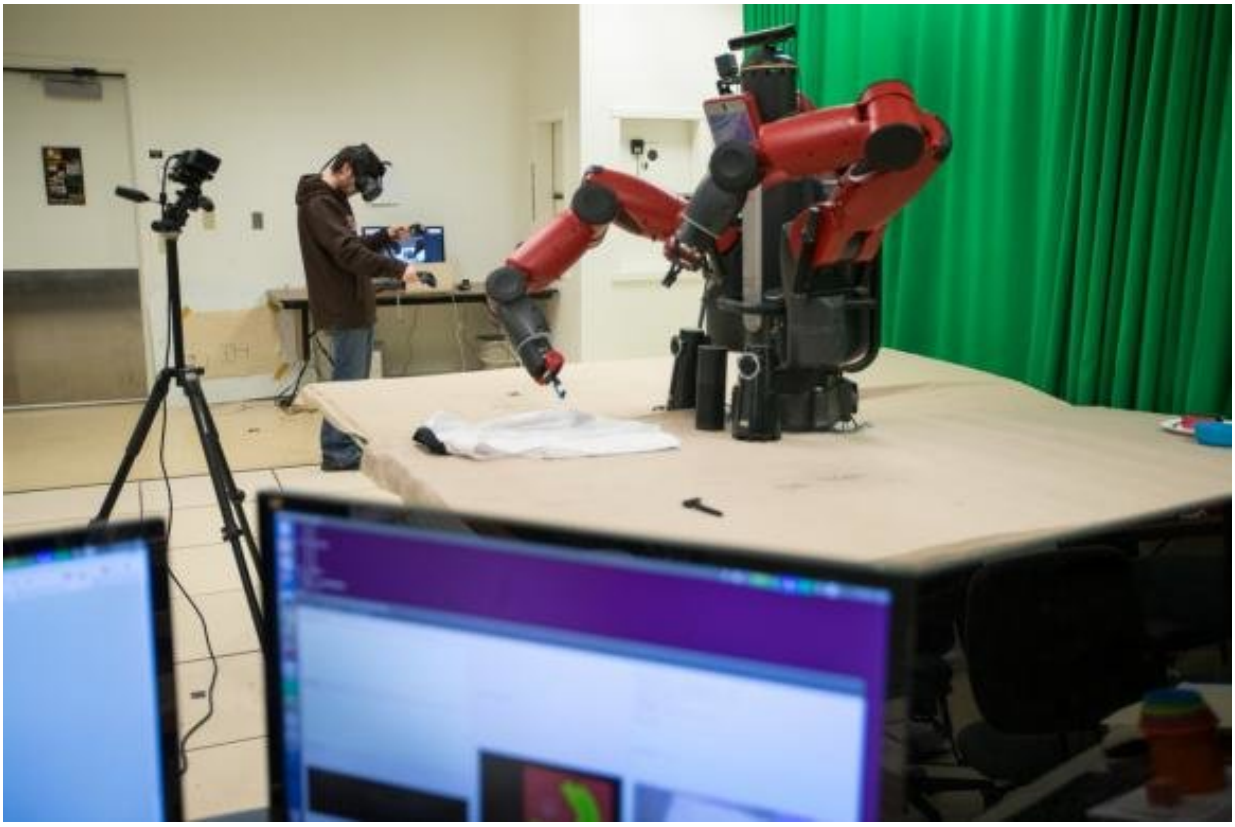
Research robots sometimes left unsecured on the internet, study finds

July 25 2018, by Kevin Stacey



Research finds that robots, like this one in the lab of Brown's Stefanie Tellex, can be accessed over the internet unless researchers take steps to lock them down. Credit: Nick Dentamaro

Robotics researchers wouldn't dream of leaving the door unlocked when they leave the lab for night, but a new study shows that research robots

are often left exposed in another way: unsecured on the internet.

A team of Brown University researchers recently ran a worldwide scan in search of hosts running the Robot Operating System (ROS), a popular research robotics platform. During the scans, which were performed over three different periods in 2017 and 2018, they found as many as 100 exposed systems running ROS, up to 19 of which were considered to be fully operational robots. The researchers showed that it's possible to control these robots remotely—to spy on camera feeds and even send commands to move the robots around.

"Though a few unsecured robots might not seem like a critical issue, our study has shown that a number of research robots is accessible and controllable from the public Internet," writes the research team. "It is likely these robots can be remotely actuated in ways [that are] dangerous to both the robot and the human operators."

The findings are a reminder, the researchers say, that everyone needs to be mindful of security in an increasingly connected digital world.

The research was presented in June as part of the Adversarial Robotics Workshop at the "2018 Robotics: Science and Systems" conference in Pittsburgh.

ROS is the dominant platform used in research robotics. It can be thought of like a robot's central nervous system. The platform aggregates all of a robot's various components—its cameras, sensors and actuators—and ties them to a central computing node. Through an external computer and a network connection, an operator connects to the central node to give commands to the robot.

"ROS is a great tool for robotics research, but the designers explicitly left security to the end users," said Stefanie Tellex, a roboticist at Brown

and a study co-author. "It doesn't require any authentication to connect to a ROS master, which means if you're running ROS and it's not behind a firewall, anyone can connect to your robot."

That got Tellex and her Brown robotics colleague George Konidaris wondering how many robots running ROS might be out there and accessible via the internet. To find out, they turned to two other Brown colleagues, security expert Vasileios Kemerlis and network expert Rodrigo Fonseca.

"Our group has the ability to basically do a worldwide scan of the internet," Fonseca said. "So we started thinking about ways we could scan for ROS devices in a way that wouldn't be disruptive, but would give us an idea what's out there."

“These robots can potentially be moved in ways endangers to the robot, as well as to the people operating the robot.”—Brown University roboticist Stefanie Tellex . Credit: Mike Cohea

Nicholas DeMarinis, a graduate student who works with Fonseca, led the scanning procedure. The researchers sent queries to more than four billion IP addresses worldwide, looking for programs running on the TCP (transfer communication protocol) port that ROS normally uses. Once they had a list of IP addresses that responded on that port, they sent passive ROS commands to determine if the program on the other end was indeed ROS.

The researchers performed the scan on three different occasions and found around 100 exposed systems running ROS. Since ROS is also used for virtual robots in simulated environments and other applications that aren't necessarily complete robots, the researchers looked at each ROS instance to determine which ones were likely to be real robots. They found 19 robots on their first scan and around a dozen each on the next two scans. The team contacted the owners of all the detected robots and other ROS instances to let the researchers and network administrators know their systems were exposed..

One of the robots detected turned out to be in the lab of one of Tellex's collaborators, Siddhartha Srinivasa, a computer science professor at the University of Washington. To find out if it were actually possible to take control of a robot remotely, Tellex contacted Srinivasa and asked his team to leave some of the robot's functions online for a test. Tellex showed that she could indeed access the robot's camera, move its neck and even make the robot speak using a ROS speech function.

That kind of access can be dangerous, the researchers say.

"These robots can potentially be moved in ways endangers to the robot, as well as to the people operating the robot," Tellex said.

"This is very timely and important work by Stefanie and her team, and we are honored to collaborate," Srinivasa said. "As scientists, we are deeply committed to understand and mitigate the security risks of emerging technologies we create. At U.W., we have been working together with security experts to create safe artificial intelligence, and this work further emphasizes the need for such interdisciplinary collaborations."

The researchers say they performed the study not to point the finger at any individual labs, but to underscore the fact that the security holes in ROS can easily be overlooked. In fact, one of the robots found during the scans was on Tellex's own lab. They had put it on the internet for an external demonstration and simply forgot to lock it back down.

The good news is that securing these robots isn't particularly difficult. They just need to be running behind a firewall or on a virtual private network. But that requires users to be mindful of security, and the researchers hope this study will encourage people to be just that. They also hope the work might encourage security monitoring services like Shodan to start doing their own scans for ROS.

"When you have software written without security in mind coupled with people not thinking about security, that's a dangerous combination," Fonseca said. "We can think of this in the larger context of the Internet of Things, where we need to think about security in all stages of a product, from the development and upgrade cycle to the way in which users deploy the devices."

TechXplore

Provided by Brown University

Citation: Research robots sometimes left unsecured on the internet, study finds (2018, July 25) retrieved 25 April 2024 from https://techxplore.com/news/2018-07-robots-left-unsecured-internet.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.