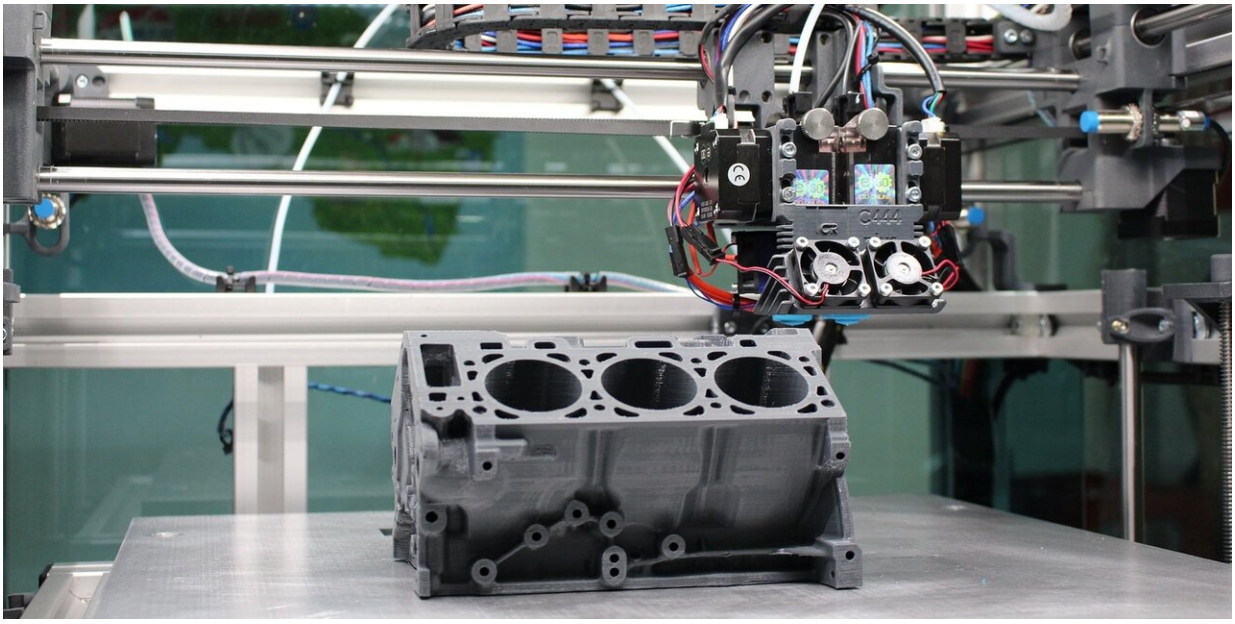
New tool determines threats to networked 3-D printers

October 23 2019, by Miranda Liu



C3PO is composed of two parts. One part identifies the printer's security vulnerabilities, and the other identifies potential attack paths based on the given vulnerabilities and network deployment. Credit: Carnegie Mellon University

In the rising era of industrial Internet of Things (IoT) devices, factories are being upgraded. Devices, such as networked 3-D printers, can now interact with other machines and be controlled remotely to improve efficiency. But connecting these devices to the network makes them more prone to danger. Some cyberattackers might stop them from

working, while others could steal designs or hold them hostage for ransom.

Carnegie Mellon University security researchers are planning ahead. Vyas Sekar and Matthew McCormack have developed a tool with their team to help protect these devices. This tool, named Connected 3-D Printer Observer, or C3PO, is designed to systematically determine potential security risks for individual networked 3-D printers. The work is funded by CMU's Manufacturing Futures Initiative, which supports the digital transformation of manufacturing,

"Many manufacturers care a lot about cybersecurity. They're starting to work on it, but it's very, very nascent," said Sekar an associate professor of electrical and computer engineering. But, there are few tools to provide security for 3-D printers.

C3PO is composed of two parts. One part identifies the printer's security vulnerabilities, and the other identifies potential attack paths based on the given vulnerabilities and network deployment. For example, it can find out whether connecting a web camera to a 3-D printer provides attackers an avenue to steal information.

C3PO functions by following the belief that sometimes the best way to know your enemies is to mimic them. After performing a security audit, C3PO questions what attackers could find if they observe network traffic to the 3-D printer. From there, it can learn more about the 3-D printer's operation and protocol. Armed with this knowledge, it can identify malicious inputs to the printer and potential Denial of Service (DoS) attacks in which attackers can make the printers inaccessible to their intended users.

Sekar's team tested the tool on eight 3-D printers from multiple vendors and manufacturing deployments. They found all of the printers were

vulnerable to DoS attacks. Understanding each devices' vulnerabilities is the first step to protect them.

Sekar's team aims to tailor the protections they have designed to each specific printer based on its problems and how it operates. When that happens, it will strengthen our defenses against future attacks.

"What we want to do next is say, alright, we found these problems, and we have a tool. Can we now create a way to protect them?" said McCormack, a Ph.D. student in electrical and computer engineering. "Can we add on something to the network to protect this printer so someone can't steal that information? Can we use what we learn about the printer itself to bolt-on a defense for the printer?"

More information: CMU's Manufacturing Futures Initiative: engineering.cmu.edu/mfi/index.html

Provided by Carnegie Mellon University