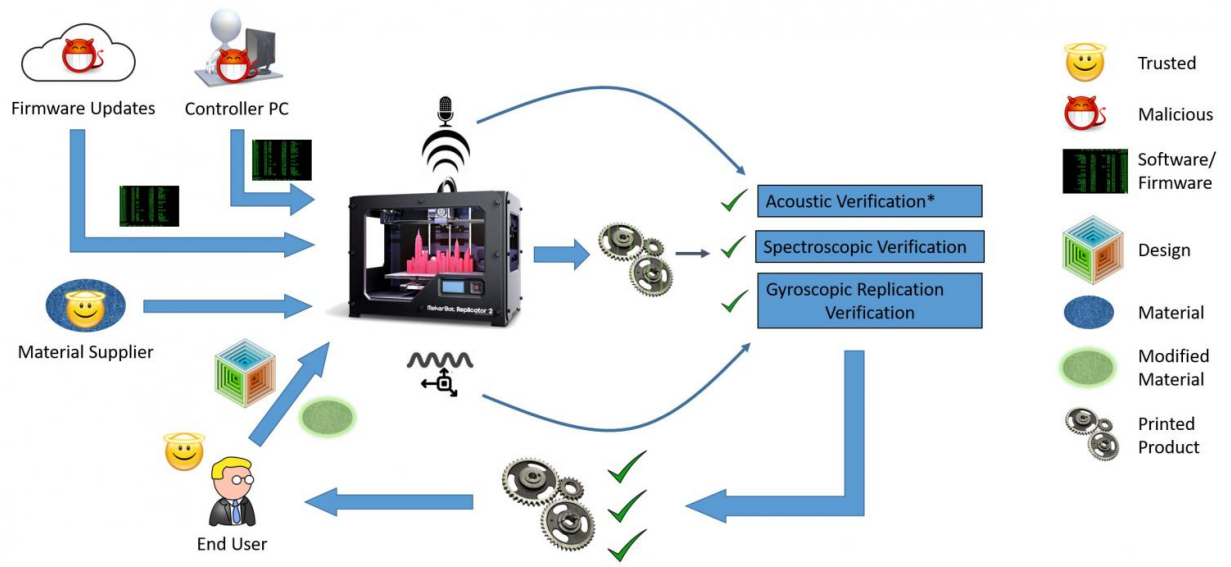
Defeating cyberattacks on 3-D printers

August 16 2017



Rutgers University-New Brunswick and Georgia Tech engineers have devised three ways to combat cyberattacks on 3-D printers: monitoring printer motion and sounds and using tiny gold nanoparticles. Credit: Christian Bayens/Georgia Institute of Technology

With cyberattacks on 3D printers likely to threaten health and safety, researchers at Rutgers University-New Brunswick and Georgia Institute of Technology have developed novel methods to combat them, according to a groundbreaking study.

"They will be attractive targets because 3D-printed objects and parts are used in critical infrastructures around the world, and cyberattacks may

cause failures in health care, transportation, robotics, aviation and space," said Saman Aliari Zonouz, an associate professor in the Department of Electrical and Computer Engineering at Rutgers University-New Brunswick.

He co-authored a peer-reviewed study - "See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Pattern Detection in Additive Manufacturing" - that was published today at the 26th USENIX Security Symposium in Vancouver, Canada. It's the security community's flagship event, highlighting the latest advances in protecting computer systems and networks. Among several unique techniques, the Rutgers and Georgia Tech researchers are using cancer imaging techniques to detect intrusions and hacking of 3D printer controllers.

"Imagine outsourcing the manufacturing of an object to a 3D printing facility and you have no access to their printers and no way of verifying whether small defects, invisible to the naked eye, have been inserted into your object," said Mehdi Javanmard, study co-author and assistant professor in the Department of Electrical and Computer Engineering at Rutgers University-New Brunswick. "The results could be devastating and you would have no way of tracing where the problem came from."

3D printing, also called additive manufacturing, plays an increasingly important role in industrial manufacturing. But health- and safety-related products such as medical prostheses and aerospace and auto parts are being printed with no standard way to verify them for accuracy, the study says. Even houses and buildings are being manufactured by 3D printers, noted Javanmard.

Instead of spending up to $100,000 or more to buy a 3D printer, many companies and organizations send software-designed products to outside facilities for printing, Zonouz said. But the firmware in printers may be hacked.

For their study, the researchers bought several 3D printers and showed that it's possible to hack into a computer's firmware and print defective objects. The defects were undetectable on the outside but the objects had holes or fractures inside them.

Other researchers have shown in a YouTube video how hacking can lead to a defective propeller in a drone, causing it to crash, Zonouz noted.

While anti-hacking software is essential, it's never 100 percent safe against cyberattacks. So the Rutgers and Georgia Tech researchers looked at the physical aspects of 3D printers.

In 3D printing, the software controls the printer, which fulfills the virtual design of an object. The physical part includes an extruder or "arm" through which filament (plastic, metal wire or other material) is pushed to form an object.

The researchers observed the motion of the extruder, using sensors, and monitored sounds made by the printer via microphones.

"Just looking at the noise and the extruder's motion, we can figure out if the print process is following the design or a malicious defect is being introduced," Zonouz said.

A third method they developed is examining an object to see if it was printed correctly. Tiny gold nanoparticles, acting as contrast agents, are injected into the filament and sent with the 3D print design to the printing facility. Once the object is printed and shipped back, high-tech scanning reveals whether the nanoparticles - a few microns in diameter - have shifted in the object or have holes or other defects.

"This idea is kind of similar to the way contrast agents or dyes are used for more accurate imaging of tumors as we see in MRIs or CT scans,"

Javanmard said.

The next steps in their research include investigating other possible ways to attack 3D printers, proposing defenses and transferring methods to industry, Zonouz said.

"You'll see more types of attacks as well as proposed defenses in the 3D printing industry within about five years," he said.

More information: See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Pattern Detection in Additive Manufacturing, www.usenix.org/biblio-123

Provided by Rutgers University