Georgia Tech News Center

Print No Evil: Three-Layer Technique Helps Secure Additive Manufacturing

By John Toon | August 16, 2017 • Atlanta, GA

Additive manufacturing, also known as 3-D printing, is replacing conventional fabrication processes in critical areas ranging from aerospace components to medical implants. But because the process relies on software to control the 3-D printer, additive manufacturing could become a target for malicious attacks – as well as for unscrupulous operators who may cut corners.

Researchers from the Georgia Institute of Technology and Rutgers University have developed a three-layer system to verify that components produced using additive manufacturing have not been compromised. Their system uses acoustic and other physical techniques to confirm that the printer is operating as expected, and nondestructive inspection techniques to verify the correct location of tiny gold nanorods buried in the parts. The validation technique is independent of printer firmware and software in the controlling computer.

The verification and intrusion detection research will be described August 18 at the 26th USENIX Security Symposium in Vancouver, British Columbia. The two institutions recently received a grant from the National Science Foundation to further develop the process described at the symposium.

"These 3-D printed components will be going into people, aircraft and critical infrastructure systems," said Raheem Beyah, the Motorola Foundation Professor and associate chair in Georgia Tech's School of Electrical and Computer Engineering. "Malicious software installed in the printer or control computer could compromise the production process. We need to make sure that these components are produced to specification and not affected by malicious actors or unscrupulous producers."

Click image to enlarge

Raheem Beyah, the Motorola Foundation Professor and associate chair in Georgia Tech's School of Electrical and Computer Engineering, is shown in a 3-D printing lab at the Woodruff School of Mechanical Engineering. (Credit: Christopher Moore, Georgia Tech)

MORE PHOTOS

The three components of the new system include:

- **Acoustic measurement of the 3-D printer in operation**. When compared to a reference recording of a correct print, this acoustic monitoring – done with an inexpensive microphone and filtering software – can detect changes in the printer's sound that may indicate installation of malicious software.
- **Physical tracking of printer components**. To create the desired object, the printer's extruder and other components should follow a consistent mechanical path that can be observed with inexpensive sensors. Variations from the expected path could indicate an attack.
- **Detection of nanorods in finished components**. Using Raman Spectroscopy and computed tomography (CT), the researchers were able to detect the location of gold nanorods that had been mixed with the filament material used in the 3-D printer. Variations from the expected location of those particles could indicate a quality problem with the component. The variations could result from malicious activity, or from efforts to conserve printer materials.

The researchers tested their technique on three different types of 3-D printers and a computer numerical control (CNC) machine using a polyethylene tibial knee prosthesis as a test case. Beyond detecting malicious activity or quality problems, the technique could stop inadvertent production problems, reducing materials waste.

In their technique to detect flaws in 3-D printed components, the researchers were inspired to apply the same kind of contrast agents used in medical imaging techniques for detecting tumors, said Mehdi Javanmard, assistant professor in the Department of Electrical and Computer Engineering at Rutgers University.

The gold contrast materials were tested to make sure they wouldn't compromise the structural integrity of the printed components.

Now that they've demonstrated the feasibility of the techniques, the researchers plan to use the NSF funding awarded August 1 to improve the validation methods and move them closer to application. "Our focus now will be on testing the resilience of this technology and its resistance to intrusion and malicious attacks," Javanmard said.

Among the challenges ahead will be obtaining good acoustic data in the noisy environments in which 3-D printers typically operate. In the research reported by the researchers, operation of other 3-D printers near the one being observed cut the accuracy significantly, but Beyah believes that challenge can be addressed with additional signal processing. The technique will also be applied to additional types of printers, and to different materials.

With the capabilities of 3-D printers growing and their cost declining, Beyah believes the use of additive manufacturing techniques will continue to expand. The validation and intrusion detection system will therefore become more critical.

"The idea that additive manufacturing processes could be compromised to intentionally hurt someone hasn't really been considered with some of these applications," he said. "There is a good bit of room to improve the security of 3-D printers, and we think that will start with applications that are closest to humans, such as implants and medical devices."

In addition to those already mentioned, the research included Christian Bayens from Georgia Tech, and Saman Zonouz, Tuan Le, and Luis Garcia from Rutgers University.

CITATION: Christian Bayens, Tuan Le, Luis Garcia, Raheem Beyah, Mehdi Javanmard and Saman Zonouz, "See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Patterns Detection in Additive Manufacturing," (26th USENIX Security Symposium, August 18, 2017). https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/bayens

Research described in this news release is being funded under award 1739259 from the National Science Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Research News
Georgia Institute of Technology
177 North Avenue
Atlanta, Georgia 30332-0181 USA

Media Relations Contacts: John Toon (jtoon@gatech.edu) (404-894-6986) or Josh Brown (josh.brown@comm.gatech.edu) (404-385-0500).

Writer: John Toon

Additional Photos

Raheem Beyah in 3-D Printing Lab

Raheem Beyah, the Motorola Foundation Professor and associate chair in Georgia Tech's School of Electrical and Computer Engineering, is shown in a 3-D printing lab at the Woodruff School of Mechanical Engineering. (Credit: Christopher Moore, Georgia Tech)

Contact Information

John Toon

Research News

(404) 894-6986

Categories

Science and Technology