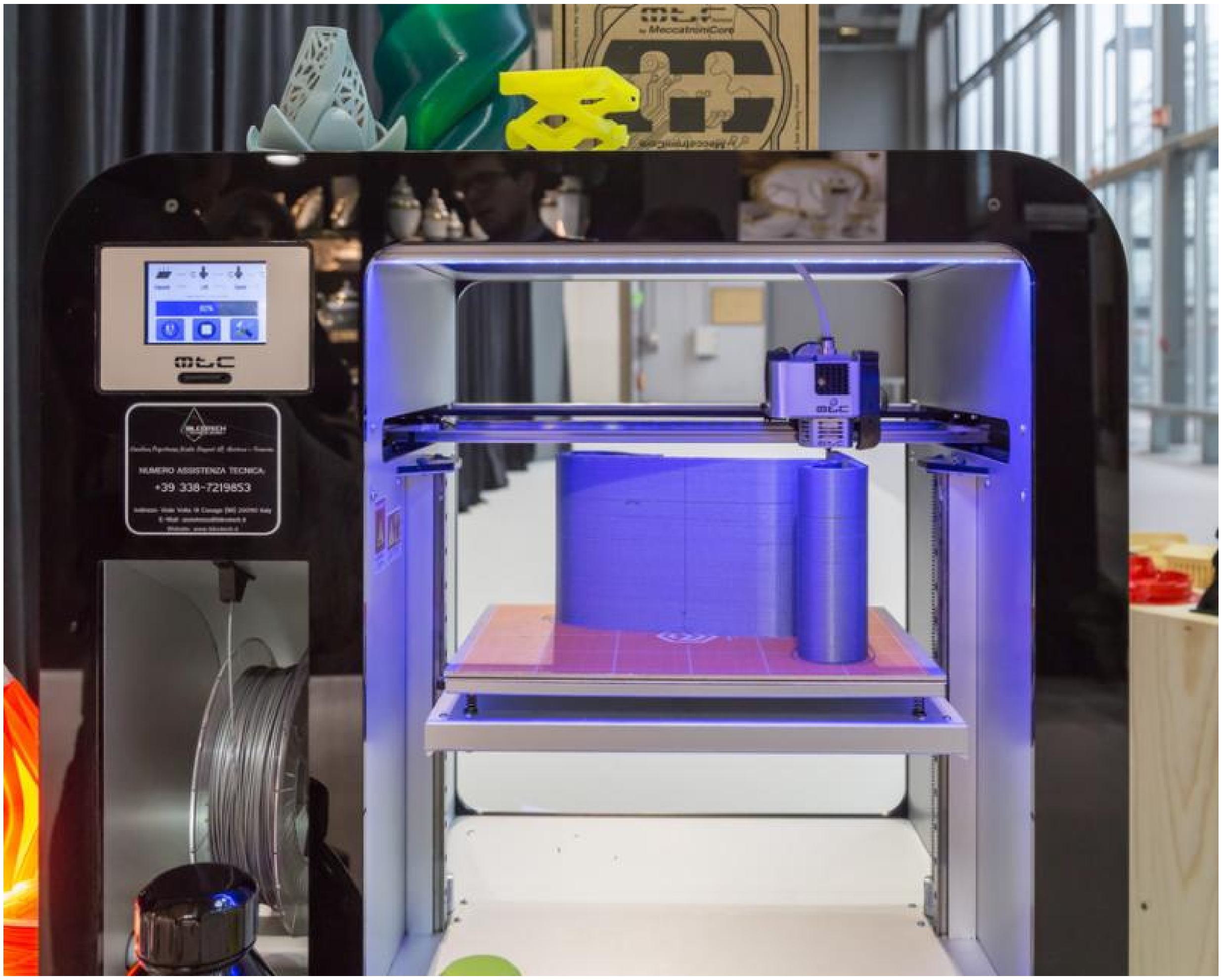
Researchers report cybersecurity risks in 3D printing

July 13 2016



A 3D Printing device layers polymers to build an object by depositing material in very small layers. A new paper by a team of NYU Tandon researchers reports that 3D printing is vulnerable to the insertion of fine defects. Credit: New York University

Additive manufacturing (AM), commonly called 3D printing, is a $4 billion business set to quadruple by 2020. One day, manufacturers may print everything from cars to medicines, disrupting centuries-old production practices. The Federal Aviation Administration recently certified the first 3D-printed part for GE commercial jet engines, and companies like Ford Motor Company are using AM to build products and prototypes.

But the new technology poses some of the same dangers unearthed in the electronics industry, where trusted, partially trusted, and untrusted parties are part of a global supply chain.

That finding, along with initial recommendations for remedies, was reported by a team of cybersecurity and materials engineers at the NYU Tandon School of Engineering in *JOM*, the Journal of the Minerals, Metals & Materials Society.

In the paper, the researchers examined two aspects of 3D printing that have cybersecurity implications: printing orientation and insertion of fine defects. "These are possible foci for attacks that could have a devastating impact on users of the end product, and economic impact in the form of recalls and lawsuits," said Nikhil Gupta, noted materials researcher and an associate professor of mechanical engineering at the New York University Tandon School of Engineering.

Additive manufacturing builds a product from a computer assisted design (CAD) file sent by the designer. The manufacturing software deconstructs the design into slices and orients the printer head. The printer then applies material in ultra-thin layers.

The researchers reported that the orientation of the product during printing could make as much as a 25 percent difference in its strength.

However, since CAD files do not give instructions for printer head orientation, malefactors could deliberately alter the process without detection. Gupta explained that economic concerns also influence how a supplier prints a product. "Minus a clear directive from the design team, the best orientation for the printer is one that minimizes the use of material and maximizes the number of parts you can print in one operation," he said.

The team comprised Gupta; lead author Steven Eric Zeltmann, a graduate student in mechanical engineering; Ramesh Karri, professor of electrical and computer engineering; Michail Maniatakos, professor of electrical and computer engineering at NYU Abu Dhabi; Nektarios Tsoutsos, a doctoral student at NYU Abu Dhabi, and Jeyavijayan Rajendran, an assistant professor at The University of Texas at Dallas and former student of Karri.

Said Karri, a cybersecurity researcher known for improving the trustworthiness of the microchip supply chain: "With the growth of cloud-based and decentralized production environments, it is critical that all entities within the additive manufacturing supply chain be aware of the unique challenges presented to avoid significant risk to the reliability of the product."

He pointed out that an attacker could hack into a printer that is connected to Internet to introduce internal defects as the component is being printed. "New cybersecurity methods and tools are required to protect critical parts from such compromise," he said.

When the researchers introduced sub-millimeter defects between printed layers, they found that the defects were undetectable by common industrial monitoring techniques, such as ultrasonic imaging, which do not require destruction of the sample. Over time, materials can weaken with exposure to fatigue conditions, heat, light, and humidity and become more susceptible to these small defects.

"With 3D printed components, such as metallic molds made for injection molding used in high temperature and pressure conditions, such defects may eventually cause failure," Gupta said.

More information: Steven Eric Zeltmann et al. Manufacturing and Security Challenges in 3D Printing, *JOM* (2016). DOI: 10.1007/s11837-016-1937-7

Provided by New York University

Citation: Researchers report cybersecurity risks in 3D printing (2016, July 13) retrieved 3 May 2024 from https://phys.org/news/2016-07-cybersecurity-3d.html