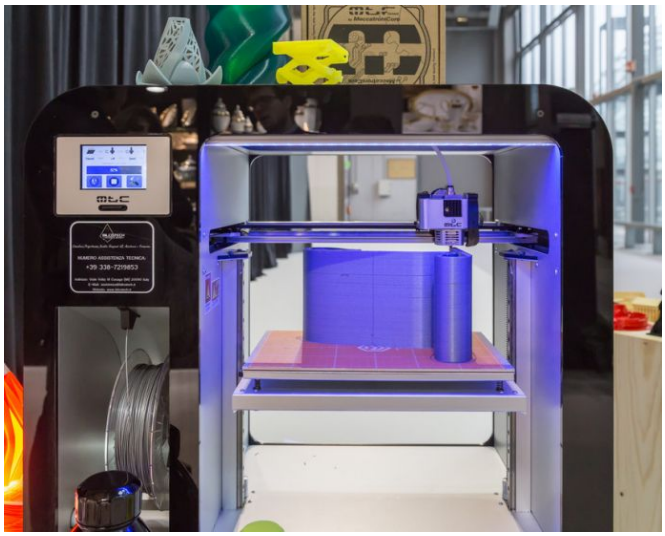
How to prevent 3-D printing hacks? Install secret flaws and share the decoder ring

23 May 2017



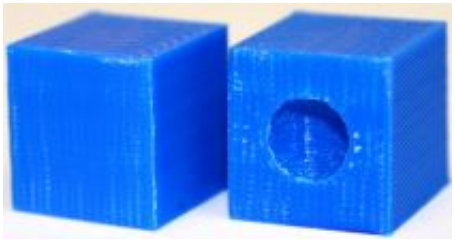
Additive manufacturing, or 3D-printing, involves sending CAD files via email or the cloud. This gives thieves and malefactors opportunities to steal designs to produce counterfeit parts. Researchers at NYU Tandon School of Engineering have found a way to embed flaws so that only trusted parties print the part correctly. Credit: NYU Tandon School of Engineering

Additive manufacturing (AM), also called 3D printing, is growing fast. Worldwide, the AM market grew nearly 26 percent to more than $5 billion last year, versus 2015, and another 17.4 percent this year versus last. The rapid prototyping market alone is expected to reach $5 billion by 2020.

But since the global supply chain for AM requires companies to share computer aided design (CAD) files within the organization or with outside parties via email or cloud, intellectual-property thieves and malefactors have many opportunities to filch a manufacturer's design files to produce counterfeit parts.

A group of researchers at NYU Tandon School of Engineering has discovered ways for manufacturers to turn the tables on thieves by deliberately embedding hidden flaws in CAD files to thwart intellectual property theft. In a new study published in *Materials and Design*, noted materials researcher Nikhil Gupta, an associate professor of mechanical engineering, his doctoral student Fei Chen and former student Gary Mac show how certain intentionally induced defects can disappear when the part is printed under a very specific set of conditions. Those without the information needed to process the files correctly—such as parties with stolen CAD models—would print a part with undesired defects and, consequently, lower quality.

The AM process involves several steps from CAD file to printed product. One step involves translating the CAD design into a stereo-lithography (STL) file format, which maps objects and their internal and external features as triangles and vectors. The researchers explored how this and other aspects of CAD-to-printer processing, such as STL file resolution, printing direction and printer resolution activated or neutralized the intentionally embedded flaws. The team developed security features that can range from the induction of voids in a part that is supposed to be solid to features that make the part print in sections that break off easily.



In the CAD model on the left, the deliberately embedded sphere disappears showing that the part is printed as high quality solid block when the right conditions are used. In the block on the right, the embedded sphere prints as a void if the required printing conditions are not used, giving that part lower strength. Credit: NYU Tandon School of Engineering

"The range of security feature designs demonstrated in this work can provide great flexibility to application engineers in terms of how to disguise these flaws easily in a complex shaped part," said Chen. "Most industrial components manufactured using 3D printing have complex designs to justify the use of 3D printing, which further helps in embedding these features without detection."

The purposeful manufacturing flaws demonstrated in this work range from two-dimensional features to three-dimensional shapes that can be hidden inside the part. One CAD model appears to have a sphere inside a rectangular block. However, the block prints without the spherical feature if the processing is conducted under the correct set of parameters, while incorrect processing creates a void in the block.

Gupta and other researchers at NYU, in a study in the May 2016 issue of *JOM*, The Journal of The Minerals, Metals & Materials Society, demonstrated that defects inserted in 3D printed components can be so small that they can avoid detection by commonly used imaging techniques but can nonetheless affect the performance. Among publisher Springer's portfolio of over 245 engineering journals, the article was the most cited, downloaded and shared last year.

So far, the main ways designers have secured CAD files is with cybersecurity tools such as encryption and password protection and by limiting access to important files. Gupta explained that "cybersecurity tools can be applied as usual to make the files and cloud secure; however, in case the design files are stolen, there is nothing in the designs to deter printing a high-quality component. The new approach is designed to provide an advantage in this scenario and to make printing high-quality parts from stolen files difficult."

The study, which will appear in print in the journal *Materials & Design*.

More information: Fei Chen et al, Security features embedded in computer aided design (CAD) solid models for additive manufacturing, *Materials & Design* (2017). DOI: 10.1016/j.matdes.2017.04.078

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

Provided by NYU Tandon School of Engineering