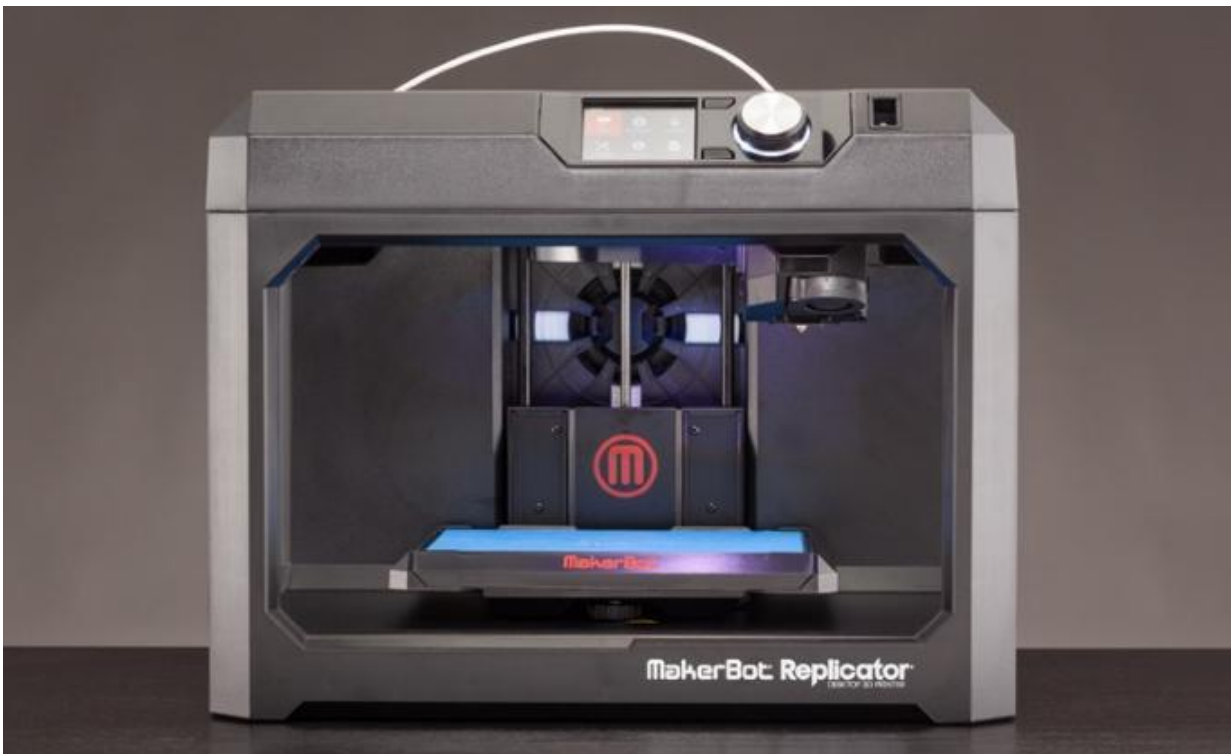# Researchers find security breach in 3-D printing process

March 2 2016

With findings that could have been taken from the pages of a spy novel, researchers at the University of California, Irvine have demonstrated that they can purloin intellectual property by recording and processing sounds emitted by a 3-D printer.

The team, led by Mohammad Al Faruque, director of UCI's Advanced Integrated Cyber-Physical Systems Lab, showed that a device as ordinary and ubiquitous as a smartphone can be placed next to a machine and capture [acoustic signals](#) that carry information about the precise movements of the printer's nozzle. The recording can then be used to reverse engineer the object being printed and re-create it elsewhere. Detailed processes may be deciphered through this new kind of cyberattack, presenting significant security risks.

"In many manufacturing plants, people who work on a shift basis don't get monitored for their smartphones, for example," Al Faruque said. "If process and product information is stolen during the prototyping phases, companies stand to incur large financial losses. There's no way to protect these systems from such an attack today, but possibly there will be in the future."

Al Faruque's team achieved nearly 90 percent accuracy using the sound copying process to duplicate a key-shaped object in the lab. They will present their results at April's International Conference on Cyber-Physical Systems in Vienna.

State-of-the-art 3-D printing systems convert digital information embedded in source code to build layer upon layer of material until a solid object takes shape. That source file, referred to as G-code, can be protected from cyberthievery with strong encryption, but once the creation process has begun, the printer emits sounds that can give up the secrets buried in the software.

"My group basically stumbled upon this finding last summer as we were doing work to try to understand the relationship between information and energy flows," said Al Faruque, an electrical engineer and computer scientist. "According to the fundamental laws of physics, energy is not consumed; it's converted from one form to another - electromagnetic to

kinetic, for example. Some forms of energy are translated in meaningful and useful ways; others become emissions, which may unintentionally disclose secret information."

The emissions produced by 3-D printers are acoustic signals that contain a lot of information, he said, adding: "Initially, we weren't interested in the security angle, but we realized we were onto something, and we're seeing interest from other departments at UCI and from various U.S. government agencies."

"President Obama has spoken about returning manufacturing to the United States, and I think 3-D printing will play a major role because of the creation of highly intellectual objects, in many cases in our homes," Al Faruque said. But he cautioned that with the convenience of these new technologies come opportunities for industrial espionage.

He suggested that engineers begin to think about ways to jam the acoustic signals emanating from 3-D printers, possibly via a white-noise device to introduce intentional acoustic randomness or by deploying algorithmic solutions. At a minimum, Al Faruque said, a fundamental precaution would be to prevent people from carrying smartphones near the rapid prototyping areas when sensitive objects are being printed. Today's smartphones, he noted, have sensors that can capture a range of analog emissions.

Provided by University of California, Irvine

provided for information purposes only.