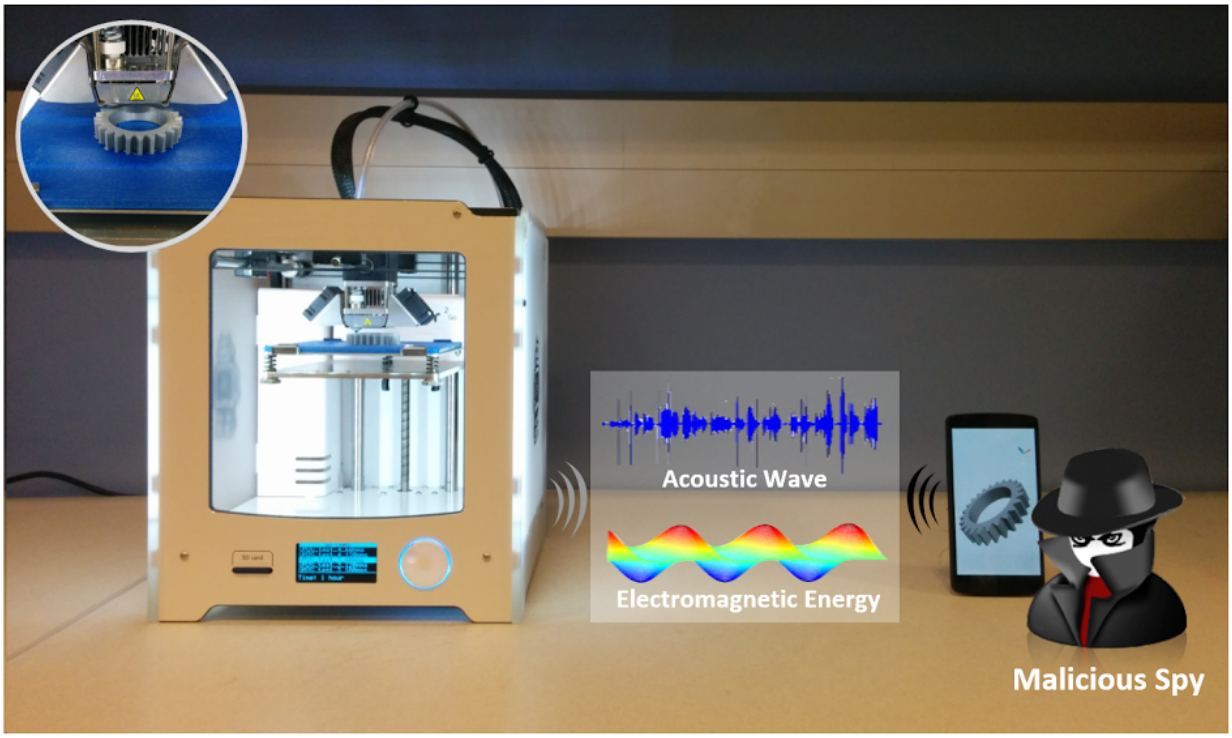
# Smartphone hacks 3-D printer by measuring 'leaked' energy and acoustic waves

September 7 2016, by Cory Nealon




An illustration of a smartphone hacking a 3-D printer. Credit: Wenyao Xu.

The ubiquity of smartphones and their sophisticated gadgetry make them an ideal tool to steal sensitive data from 3-D printers.

That's according to a new University at Buffalo study that explores security vulnerabilities of 3-D printing, also called additive

manufacturing, which analysts say will become a multibillion-dollar industry employed to build everything from rocket engines to heart valves.

"Many companies are betting on 3-D printing to revolutionize their businesses, but there are still security unknowns associated with these machines that leave intellectual property vulnerable," said Wenyao Xu, PhD, assistant professor in UB's Department of Computer Science and Engineering, and the study's lead author.

Xu and collaborators will present the research, "My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks Against 3D Printers," at the Association for Computing Machinery's 23rd annual Conference on Computer and Communications Security in October in Austria.

## Not a cyberattack

Unlike most security hacks, the researchers did not simulate a cyberattack. Many 3-D printers have features, such as encryption and watermarks, designed to foil such incursions.

Instead, the researchers programmed a common smartphone's built-in sensors to measure electromagnetic energy and acoustic waves that emanate from 3-D printers. These sensors can infer the location of the print nozzle as it moves to create the three-dimensional object being printed.

The smartphone, at 20 centimeters away from the printer, gathered enough data to enable the researchers to replicate printing a simple object, such as a door stop, with a 94 percent accuracy rate. For complex objects, such as an automotive part or medical device, the accuracy rate was lower but still above 90 percent.

"The tests show that smartphones are quite capable of retrieving enough data to put sensitive information at risk," says Kui Ren, PhD, professor in UB's Department of Computer Science and Engineering, a co-author of the study.

The richest source of information came from electromagnetic waves, which accounted for about 80 percent of the useful data. The remaining data came from acoustic waves.

Ultimately, the results are eye-opening because they show how anyone with a smartphone—from a disgruntled employee to an industrial spy—might steal intellectual property from an unsuspecting business, especially "mission critical" industries where one breakdown of a system can have a serious impact on the entire organization.

"Smartphones are so common that industries may let their guard down, thus creating a situation where intellectual property is ripe for theft," says Chi Zhou, PhD, assistant professor in UB's Department of Industrial and Systems Engineering, another study co-author.

## Making 3-D printers more secure

The researchers suggests several ways to make 3-D printing more secure. Perhaps the simplest deterrent from such an attack is distance. The ability to obtain accurate data for simple objects diminished to 87 percent at 30 centimeters, and 66 percent at 40 centimeters, according to the study.

Another option is to increase the print speed. The researchers said that emerging materials may allow 3-D printers to work faster, thus making it more difficult for smartphone sensors to determine the print nozzle's movement.

Other ideas include software-based solutions, such as programming the printer to operate at different speeds, and hardware-based ideas, such as acoustic and electromagnetic shields.

**More information:** DOI: 10.1145/2976749.2978300