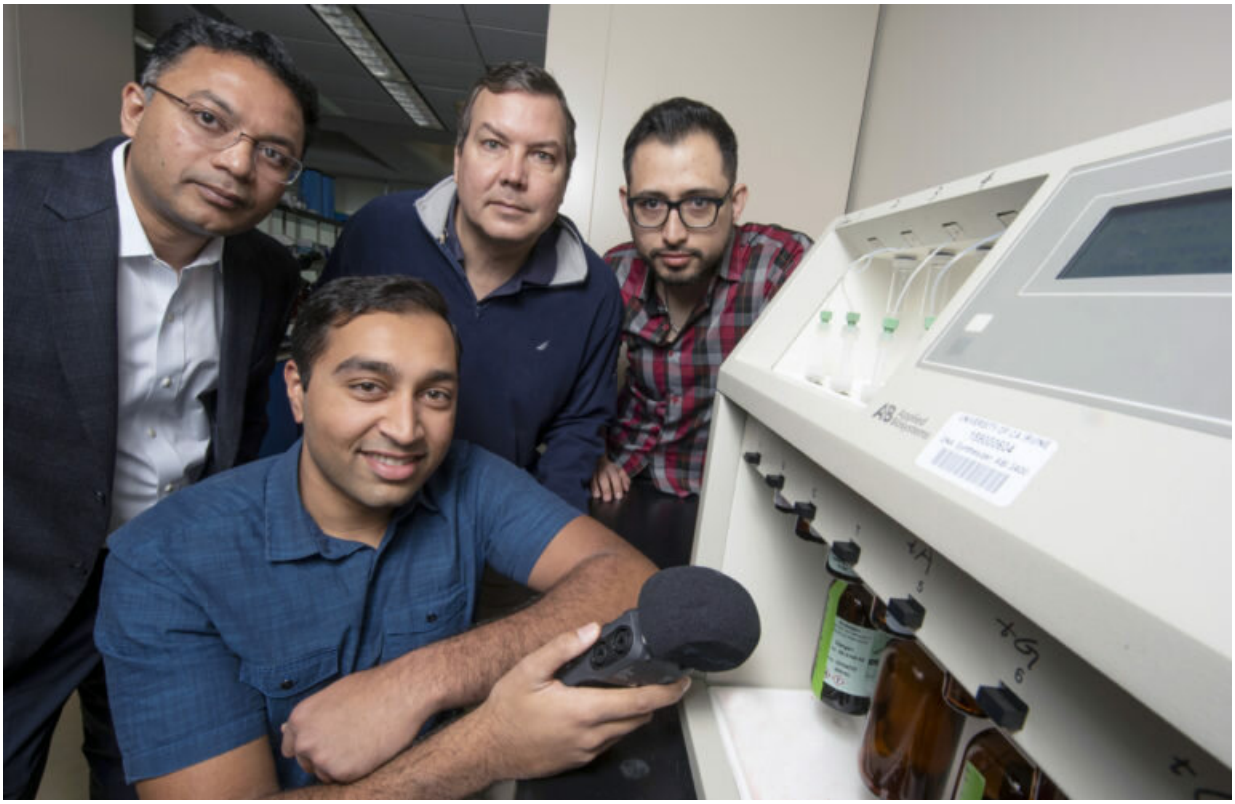
Scientists eavesdrop on DNA synthesizer to steal genetic blueprint

February 25 2019, by Brian Bell



UCI researchers who helped discover that hackers can steal genetic blueprints by interpreting the sounds emitted by a DNA synthesizer are (from left) Mohammad Al Faruque, associate professor of electrical engineering & computer science; Arnav Malawade, a graduate student in Al Faruque's lab; John Chaput, professor of pharmaceutical sciences; and Sina Faezi, also a graduate student in Al Faruque's lab. Credit: Steven Zylius / UCI

During the DNA synthesis process in a laboratory, recordings can be made of the subtle, telltale noises made by synthesis machines. And those captured sounds can be used to reverse-engineer valuable, custom-designed genetic materials used in pharmaceuticals, agriculture and other bioengineering fields.

Researchers from the University of California, Irvine and the University of California, Riverside have uncovered the possibility of an acoustic side-channel attack on the DNA synthesis process, a vulnerability that could present a serious risk to biotechnology and pharmaceutical companies and academic research institutions.

"A few years ago, we published a study on a similar method for stealing blueprints of objects being fabricated in 3-D printers, but this attack on DNA synthesizers is potentially much more serious," said Mohammad Al Faruque, UCI associate professor of electrical engineering & computer science. "In the wrong hands, DNA synthesis capability could result in bioterrorists synthesizing, at will, harmful pathogens such as anthrax."

Al Faruque said his lab's discovery might also be used for a good cause: "Government agencies can employ the same technique as a monitoring tool to nullify the possibility of such activities."

A DNA synthesizer is a complex machine with meandering pipes, fluid reservoirs, solenoid valves and electrical circuitry. Chemicals—which have their own unique acoustic signatures due to their varying densities—flow through tubes, creating distinct noises punctuated by the clicking of valves and the whirring of pressure pump motors.

"All of these inner workings of a DNA synthesizer result in the emission of subtle but distinguishable sound signatures that can give clues as to the specific genetic material being generated," said Sina Faezi, a UCI

graduate student in electrical engineering & computer science, who will present a paper on the potential threat of an acoustic side attack on DNA synthesizers at the Network & Distributed System Security Symposium taking place Feb. 24-27 in San Diego.

He said that in many cases, variances in the sounds produced are so tiny that people can't distinguish them. "But through careful feature engineering and a bespoke machine learning algorithm written in [Al Faruque's] lab, we were able to pinpoint those differences," he said.

Another factor that enables DNA synthesis information to be stolen is the design of the synthesizers themselves, according to Faezi. "Solenoid valves are placed asymmetrically inside the housing, so when a valve is working in one corner of the box, it makes a completely difference noise than one that's working in the middle," he said.

If hackers know which device model is in use, they'll have one more piece of the puzzle in place.

"Any active machine emits a trace of some form: physical residue, electromagnetic radiation, acoustic noise, etc.," said study collaborator Philip Brisk, UC Riverside associate professor of computer science & engineering. "The amount of information in these traces is immense, and we have only hit the tip of the iceberg in terms of what we can learn and reverse-engineer from it."

Al Faruque, head of UCI's Advanced Integrated Cyber-Physical Systems Lab, added that the ubiquity of recording devices, such as smartphones, makes the problem even more pervasive.

"Let's say you're a good person who works in a lab. I can hack into your phone and essentially hijack it to record sound that I can eventually retrieve," he said. "Furthermore, some biological labs have acoustic

sensors mounted on the walls, and more people are adopting technologies like Google Home or Alexa—all of these can be used to pilfer sounds."

With their side-channel attack methodology, the researchers said, they can predict each base in a DNA sequence with about 88 percent accuracy, and they're able to reconstruct short sequences with complete reliability. Their technique functions best when a recording device is placed within a couple feet of a DNA sequencing machine, they said, but the algorithm works even in the presence of noise from an air conditioner or peoples' voices.

Al Faruque stressed that this sort of attack is too sophisticated for a small-time criminal or terrorist to pull off but is not beyond the capability of state actors. The stakes are high: The global market for synthetic biological products is expected to reach almost $40 billion by 2020. And that market share is expected to grow, particularly in the area of DNA data storage, an application being pursued by heavy-hitting technology companies.

Faezi noted that there are some ways to prevent snooping attacks. Machine designers could arrange the pipes and valves in a way that mitigates the emission of distinct sounds, and the DNA synthesis process can be scrambled and randomized to block hackers from piecing together the intellectual property.

More information: www.ndss-symposium.org/wp-cont … 5B-1_Faezi_paper.pdf

Provided by University of California, Irvine