Machines whisper our secrets: Spies can learn what a machine is making from the sounds it makes

February 25 2019, by Holly Ober

Credit: CC0 Public Domain

Lab instruments are important tools throughout research and health care. But what if those instruments are leaking valuable information?

When it comes to biosecurity, this could be a very real threat, according to a group of researchers at the University of California, Irvine, and the University of California, Riverside. By simply recording the sounds of a common lab instrument, the team members could reconstruct what a researcher was doing with that instrument.

"Any active machine emits a trace of some form: physical residue, electromagnetic radiation, acoustic noise, etc. 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 about the machine that generated them," said Philip Brisk, a UC Riverside associate professor of computer science who worked on the project.

In a paper presented at the Network and Distributed System Security Symposium, the group showed they could reconstruct what a researcher was doing by recording the sounds of the lab instrument used. That means academic, industrial, and government labs are potentially wide open to espionage that could destabilize research, jeopardize product development, and even put national security at risk.

The researchers wondered if it was possible to determine what a DNA synthesizer was producing from the sounds its components made as it went through its manufacturing routine.

DNA synthesizers are machines that allow users to build custom DNA molecules from a few basic ingredients. Researchers commonly construct segments of DNA to insert in the genome of other organisms, especially bacteria, to make new organisms. Sometimes these living systems are used to make valuable new pharmaceuticals or other products.

Brisk and UC Irvine electrical and computer engineering professor Mohammad Abdullah Al Faruque and his doctoral student Sina Faezi;

along with John C. Chaput, a professor of pharmaceutical sciences at UC Irvine; and William Grover, a bioengineering professor at UC Riverside, set microphones similar to those in a smartphone in several spots near a DNA synthesizer in Chaput's lab.

All DNA is built from just four bases, adenine (A), guanine (G), cytosine (C), and thymine (T), arranged in almost infinite combinations. The specific patterns, or sequences, can be read as a clue to what kind of DNA it is.

DNA synthesizers contain components that open and close to release chemicals as they manufacture each of these bases, along with the tubes and chambers through which they flow. These mechanisms make distinctive sounds as they work.

After filtering out background noise and running several adjustments to the recorded sound, the researchers found the differences were too subtle for humans to notice.

"But through a careful feature engineering and bespoke machine-learning algorithm written in our lab, we were able to pinpoint those differences," Faezi said. The researchers could easily distinguish each time the machine produced A, G, C, or T.

When the researchers used software to analyze the AGCT patterns they acquired through the recordings, they identified the correct type of DNA with 86 percent accuracy. By running it through additional well-known DNA sequencing software, they boosted the accuracy to almost 100 percent.

Using this method, a knowledgeable observer could tell if the machine was making anthrax, smallpox, or Ebola DNA, for example, or a commercially valuable DNA intended to be a trade secret. The method

could help law enforcement prevent bioterrorism, but it could also be used by criminals or terrorists to intercept biological secrets.

"A few years ago, we published a study on a similar method for stealing plans of objects being fabricated in 3-D printers, but this DNA synthesizer attack is potentially much more serious," Al Faruque said.

The researchers recommend that labs using DNA synthesizing machines institute security measures, such as strictly controlling access to the machines and removing innocuous-seeming recording devices left near the machine. They also recommend that machine manufacturers begin designing machine components to reduce the number of sounds they make, either by redesigning or repositioning the components or swaddling them in sound absorbent material.

Almost all machines used in biomedical research make some kind of sound, noted Brisk and Grover, and the hack could conceivably be applied to any machine.

"The take-home message for bioengineers is that we have to worry about these security issues when we're designing instruments," Grover said.

In addition to Al Faruque, Brisk, Grover, Chaput, and Faezi, authors include UC Irvine doctoral students Sujit Rokka Chhetri and Arnav Vaibhav Malawad. The paper, Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines, will be presented at the 2019 Network and Distributed Systems Security Symposium, which takes place in San Diego between Feb. 24-27.

More information: DOI: 10.14722/ndss.2019.23544