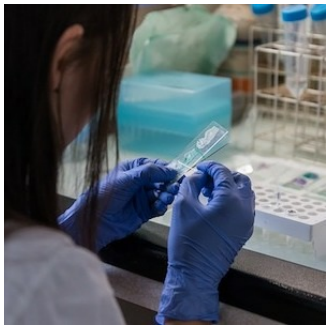
HealthManagement
Promoting Management and Leadership

Lab instruments in possible data leak



A new study warns **lab instruments** used in biomedical research, such as DNA synthesising machines, may be **leaking sensitive information t**hrough some kind of noise or sound that they make.

The study by University of California researchers serves to highlight new security risks created by the cyber-physical nature of biotechnology workflows. The researchers found that speakers similar to smartphone speakers had the capability to determine what a DNA synthesiser was producing from the sounds its components made as it went through its manufacturing routine.

You might also like: Integrating labs into clinical care pathways

Security measures must be implemented to ensure that such vulnerability is not exploited by hackers, according to study co-authors, Philip Brisk, a UC Riverside associate professor of computer science, and UC Irvine electrical and computer engineering professor Mohammad Abdullah Al Faruque. The authors recommend that access to lab machines or devices should be strictly controlled and innocuous-seeming recording devices, including mobile devices like smartphones, must not be left nearby or placed in a safe area. “Any active machine emits a trace of some form: physical residue, electromagnetic radiation, acoustic noise, et cetera,” Brisk explained.

“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.” DNA synthesisers typically include components that open and close to release chemicals as they manufacture each of these bases, mechanisms that make distinctive sounds as they work. Using a careful feature engineering and bespoke machine-learning algorithm written in the lab, the UC researchers were able to distinguish those differences in sound, which allow them to identify the correct type of DNA.

The researchers say that by listening in 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. If this type of information was exposed, according to the study, an attacker could create a contagious virus that is fatal to individuals or a small group, but otherwise benign to the general population. Al Faruque noted that while a study has already been published on a similar method for stealing plans of objects being fabricated in 3D printers, this DNA synthesiser attack is potentially much more serious.

Another recent example was the ability to encode information into a DNA sequence that can trigger a buffer overflow error in DNA sequencing software — this exploit can be used to inject malware into the computer running the sequencing algorithm. And with almost all machines used in biomedical research making or emitting some kind of sound, the **risk from hackers** could conceivably be applied to any machine. These security issues therefore must be carefully considered by bioengineers when designing instruments, according to William Grover, a bioengineering professor at UC Riverside.

Source: UC Riverside
Image credit: Pixabay

Published on : Tue, 5 Mar 2019