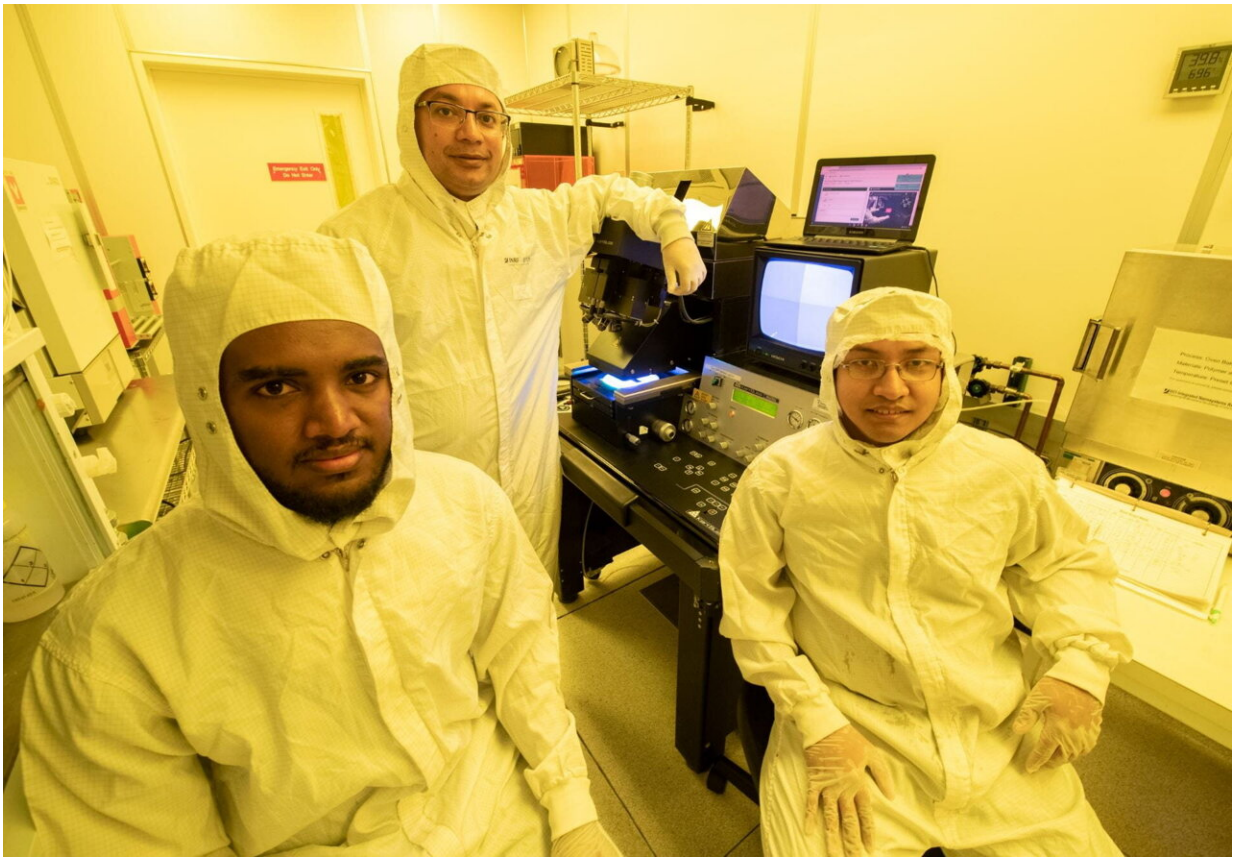
Researchers discover how music could be used to trigger a deadly pathogen release

November 17 2022



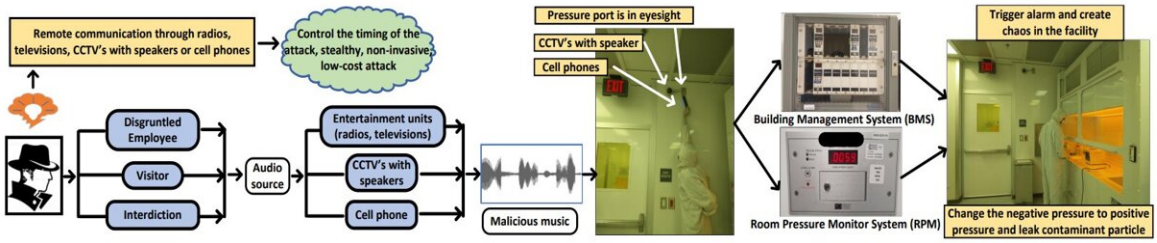
Achamyeleh, Al Faruque and Barua (from left) conducted part of their research into a potential threat to negative pressure facilities in an actual clean room designed to prevent external exposure to dangerous microbes. Credit: Steve Zylius / UCI

Researchers at the University of California, Irvine have discovered that the safe operation of a negative pressure room—a space in a hospital or biological research laboratory designed to protect outside areas from exposure to deadly pathogens—can be disrupted by an attacker armed with little more than a smartphone.

According to UCI cyber-physical systems security experts, who shared their findings with attendees at the Association for Computing Machinery's recent Conference on Computer and Communications Security in Los Angeles, mechanisms that control airflow in and out of biocontainment facilities can be tricked into functioning irregularly by a sound of a particular frequency, possibly tucked surreptitiously into a popular song.

"Someone could play a piece of music loaded on their smartphone or get it to transmit from a television or other audio device in or near a negative pressure room," said senior co-author Mohammad Al Faruque, UCI professor of electrical engineering and computer science. "If that music is embedded with a tone that matches the resonant frequency of the pressure controls of one of these spaces, it could cause a malfunction and a leak of deadly microbes."

Heating, ventilation and air conditioning infrastructure maintains the flow of fresh air into and contaminated air out of a given space. HVAC systems in scientific facilities typically include room pressure monitors, which in turn utilize differential pressure sensors that compare the atmospheres inside and outside rooms.



A brief overview of the attack model - A Wolf in Sheep's Clothing. Credit: Anomadarshi Barua et al

The researchers said that commonly used differential pressure sensors (DPSs) are vulnerable to remote manipulation, posing a previously unrealized threat to biosafety facilities. They tested their hypothesis on eight industry-standard DPSs from five manufacturers, demonstrating that all the devices operate with resonant frequencies in the audible range and are, therefore, subject to tampering.

"When sound waves collide with the diaphragms inside a DPS, it starts vibrating with the same frequency," said lead author Anomadarshi Barua, UCI Ph.D. candidate in electrical engineering and computer science. "An informed attacker can use this technique to artificially displace the diaphragm, changing the pressure reading and causing the whole system to malfunction."

He said that attackers could thwart negative pressure room systems in a variety of ways. They could manipulate them wirelessly or pose as maintenance personnel to place an audio device inside or near such a room. "A more sophisticated attack might involve perpetrators embedding sound-emitting technologies into a DPS before it's installed in a biocontainment facility," Barua said.

In their conference presentation, the researchers suggested several countermeasures to prevent a musical assault on biosafety facilities. Sound dampening can be achieved by lengthening the sampling tube of a DPS's port by as much as 7 meters. The team also proposed enclosing the pressure port in a boxlike structure. Both these measures would reduce the sensitivity of the DPS, Barua said.

Al Faruque said that this research project demonstrates the vulnerabilities of embedded systems to random attacks but stressed that with a little planning and forethought, facilities can be hardened against sabotage.

Joining Al Faruque and Barua on the study was Yonatan Gizachew Achamyeleh, UCI Ph.D. student in electrical engineering and computer science. The study was published as part of the *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*.

More information: Anomadarshi Barua et al, A Wolf in Sheep's Clothing, *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (2022). DOI: 10.1145/3548606.3560643

Full paper (arXiv preprint): A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music

Provided by University of California, Irvine