A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music

Anomadarshi Barua*
University of California, Irvine
Irvine, CA, USA
anomadab@uci.edu

Yonatan Gizachew Achamyeleh*
University of California, Irvine
Irvine, CA, USA
yachamye@uci.edu

Mohammad Abdullah Al Faruque
University of California, Irvine
Irvine, CA, USA
alfaruqu@uci.edu

ABSTRACT

A Negative Pressure Room (NPR) is an essential requirement by the Bio-Safety Levels (BSLs) in biolabs or infectious-control hospitals to prevent deadly pathogens from being leaked from the facility. An NPR maintains a negative pressure inside with respect to the outside reference space so that microbes are contained inside of an NPR. Nowadays, differential pressure sensors (DPSs) are utilized by the Building Management Systems (BMSs) to control and monitor the negative pressure in an NPR. This paper demonstrates a non-invasive and stealthy attack on NPRs by spoofing a DPS at its resonant frequency. Our contributions are: (1) We show that DPSs used in NPRs typically have resonant frequencies in the audible range. (2) We use this finding to design malicious music to create resonance in DPSs, resulting in an overshooting in the DPS's normal pressure readings. (3) We show how the resonance in DPSs can fool the BMSs so that the NPR turns its negative pressure to a positive one, causing a potential *leak* of deadly microbes from NPRs. We do experiments on 8 DPSs from 5 different manufacturers to evaluate their resonant frequencies considering the sampling tube length and find resonance in 6 DPSs. We can achieve a 2.5 Pa change in negative pressure from a ~7 cm distance when a sampling tube is not present and from a ~2.5 cm distance for a 1 m sampling tube length. We also introduce an interval-time variation approach for an adversarial control over the negative pressure and show that the *forged* pressure can be varied within 12 - 33 Pa. Our attack is also capable of attacking multiple NPRs simultaneously. Moreover, we demonstrate our attack at a real-world NPR located in an anonymous bioresearch facility, which is FDA approved and follows CDC guidelines. We also provide countermeasures to prevent the attack.

CCS CONCEPTS

• **Security and privacy → Embedded systems security**; *Hardware attacks and countermeasures.*

KEYWORDS

Pressure sensors; Resonance; Negative pressure room; Pathogens

*Both authors contributed equally to this research.

CCS '22, November 7–11, 2022, Los Angeles, CA, USA

ACM ISBN 978-1-4503-9450-5/22/11.
https://doi.org/10.1145/3548606.3560643

ACM Reference Format:
Anomadarshi Barua, Yonatan Gizachew Achamyeleh, and Mohammad Abdullah Al Faruque. 2022. A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music . In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22), November 7–11, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3548606.3560643

1 INTRODUCTION

A Bio-Safety Level (BSL) [68, 74] is a set of strict regulations assigned to a biolab or hospital facility to prevent deadly pathogens from being leaked from the facility. The BSL is ranked from BSL-1 (lowest safety level) to BSL-4 (highest safety level) depending on the microbes that are being contained in a laboratory or hospital setting. The Centers for Disease Control and Prevention (CDC) sets BSLs to exhibit specific controls for the containment of microbes to protect the surrounding environment and community.

BSLs require that the isolation rooms in a biolab or infectious-control hospital maintain negative pressure with respect to the outside hallway [74]. Therefore, the room is known as the Negative Pressure Room (NPR). An NPR ensures that potentially harmful microbes cannot leak from the facility through airflow by maintaining negative pressure inside. Therefore, an NPR is critical in preventing deadly bioaerosols from escaping from the facility.

With rising concerns of bioterrorism, an NPR must maintain a certain *negative pressure* following strict regulations established by the CDC, ASHRAE, or other authorities [53, 67]. The Differential Pressure Sensors (DPSs) are commonly used in NPRs to measure the negative pressure in the facility [65]. The DPSs provide the pressure data to the Heating, Ventilation, and Air Conditioning (HVAC) systems, which *maintains* the negative pressure by controlling the airflow into NPRs [79]. In addition, a Room Pressure Monitoring (RPM) system is also present in NPRs to *monitor* the room pressure [7]. The RPM system also depends on the reading from the DPSs installed in an NPR. Both RPM and HVAC systems are connected with the Building Management Systems (BMSs) for automated control and monitoring of the negative pressure in an NPR.

A DPS has an elastic diaphragm working as a pressure force collector. Therefore, a DPS can be modeled as a second-order dynamic system with a resonant frequency [83]. We demonstrate by thorough experiments that the resonant frequencies of DPSs used in NPRS are typically in the audible range. In addition, we show that the DPS with a sampling tube can be modeled as a Helmholtz resonator, and the resonant frequency of a DPS with a sampling tube still falls within the audible range. This finding is important because an attacker, who has an intention to change the negative

pressure in an NPR, may use an audible sound having a resonant frequency to create resonance in a DPS and generate a *forged* pressure to perturb the normal readings of a DPS located in an NPR.

However, a sound having a single-tone resonant frequency will create a "beep"-ish sound, which makes the attack easily identifiable by the authority. Moreover, the HVAC and RPM systems cannot be fooled by a simple resonance in DPS because these systems have a slower response time compared to a resonance. Therefore, a simple resonance in DPS is not enough to turn NPR's negative pressure into a positive pressure to leak airborne pathogens from an NPR.

To solve the above problems, this paper adopts a smart strategy by *disguising* the resonant frequency band inside popular music. The resonant frequencies are inserted as a *segment* into the music for a certain duration in every specific interval. Every inserted segment of the resonant frequency is ended at its peak. Therefore, the corresponding pressure wave inside a DPS also ends at its peak. As a DPS with a sampling tube is a second-order oscillating system [41], the pressure wave does not instantly fall to zero from the peak value. Instead, the pressure wave starts to attenuate from its peak exponentially. If the interval between two consecutive segments is small, the pressure wave never falls below a certain value. Therefore, a forged pressure is always present inside a DPS having an average value greater than zero. As a result, the malicious music injected into the DPS can fool the controller of HVAC and RPM systems connected with BMSs to change the negative pressure of an NPR into a positive one. Moreover, the segments of resonant frequency are camouflaged in the malicious music so that the attack is not identifiable by the authority. Therefore, we name this attack as "*the wolf in sheep's clothing*" since this strategy ensures stealthiness.

The consequences of changing a negative pressure into a positive one can be catastrophic. If the NPR has an infectious patient admitted or an ongoing bioresearch, the attacker can control the timing of the attack to *leak* a deadly pathogen *from* the NPR. Moreover, an abnormal change in NPR's pressure triggers an alarm that may create chaos in the facility. An attacker can use this chaos to initiate a stronger attack, such as stealing deadly microbes from the NPR or physically attacking the biosafety cabinets in an NPR. Therefore, our attack model is strong and impactful and has the potential to cause tremendous losses in human lives and monetary resources.

Contributions: We have the following technical contributions:

(1) We evaluate eight industry-used pressure sensors from five different manufacturers to show that the pressure sensors used in NPRs have resonant frequencies in the audible range.

(2) We design malicious music disguising the resonant frequencies of DPSs inside of the music to fool the HVAC and RPM systems of an NPR. We show through experiments that this strategy can change the negative pressure of an NPR to a positive one.

(3) We show that the attacker can adversarially control the forged pressure in DPSs by using the malicious music. Moreover, we show that the attacker can also *simultaneously* attack *multiple* NPRs in a facility using our attack model.

(4) We demonstrate our attack model at a real-world NPR located in an anonymous bioresearch facility. The NPR is approved by the Food and Drug Administration (FDA) and follows CDC guidelines. We also provide countermeasures to prevent the attack on NPRs.

Demonstration: The demonstration of the attack is shown in the following link: https://sites.google.com/view/awolfinsheepsclothing/home

2 BACKGROUND

2.1 NPR and its importance

An NPR [76] maintains lower pressure inside with respect to the outside reference space. As air typically travels from higher pressure areas to lower pressure areas, NPR ensures that clean air is drawn into the room so that contaminated particles inside the room are not able to escape. This is why NPRs are present in hospitals and biosafety labs as they prevent airborne particles like bacteria and viruses from spreading out from the facility. NPRs are also present in safety-critical facilities, such as pharmacies and clean rooms.

Importance: The safety of NPRs is paramount as spreading airborne microbes from NPRs may result in catastrophic consequences. For example, a deadly fungus belonging to the genus *Aspergillus* is an airborne pathogen that can cause Aspergillosis disease resulting in acute pneumonia and abscesses of the lungs and kidneys [1]. It has a mortality rate of ∼100% for people with neutropenia (i.e., low neutrophils). Respiratory tract infections, such as influenza, swine flu, and COVID-19, are great examples of airborne pathogens that result in a worldwide pandemic. Recently, a conspiracy theory has been rumored about the leakage of the COVID-19 as bioweapons from a biolab [13]. In this context, *imagine* an attacker with the intention of spreading infectious disease as bioweapons may target NPRs, where either infected patients are admitted for isolation or research is carried out on deadly pathogens. Therefore, the security of NPRs is critical and is regulated with strict guidelines.

2.2 Regulations for NPRs

With rising concerns about bioterrorism and emerging infectious diseases, there has been a greater emphasis on the proper regulations of NPRs. NPRs must follow requirements established by the CDC [53], ASHRAE [67], and healthcare design construction guidelines [43] to correctly manage airborne infections. Different authorities follow their own regulations [2, 3, 5, 63] to maintain a certain negative pressure in NPRs (see Table 1). For example, CDC requires that NPRs must maintain a negative pressure differential of at least ∼2.5 Pa (i.e., 0.01 inch water column) in a hospital or biolabs and change the air at least 12 times per hour [53]. Moreover, exhaust from NPRs must be allowed to exit directly outside without contaminating exhaust from other locations. In addition, all exhaust air must be discharged through a High-Efficiency Particulate Air (HEPA) filter to prevent any contamination in the environment.

Table 1: Regulations for a Negative Pressure Room (NPR).

Country	Taiwan	CDC(USA)	AIA(USA)	Australia
Negative pressure	-8 Pa	-2.5 Pa	-2.5 Pa	-15 Pa
Air change per hour (ACH)	8 -12	> 12	> 12	> 12

2.3 Types of pressure sensors used in NPRs

Traditionally, hot-wire anemometers [54] and ball pressure sensors [57] were used to measure pressure in NPRs. However, they have limitations, such as they are highly sensitive to dust, require periodic maintenance, and cannot be connected to a BMS or RPM for real-time control. Therefore, transducer-based pressure sensors

(TBPSs) are replacing hot-wire and ball pressure sensors in NPRs since TBPSs are more accurate, reliable, require low maintenance, and can be connected to BMS or RPM for real-time monitoring.

Physics of TBPSs: A force collector and a transducer are two fundamental components of TBPSs. A force collector, such as an elastic diaphragm, is combined with a transducer to generate an electrical signal [39] proportional to the input pressure.

Types of TBPSs: In general, TBPSs work in one of three modes: absolute, gauge, or differential measurement. Absolute pressure sensors use vacuum pressure, and gauge sensors use local atmospheric pressure as the static reference pressure. On the other hand, **Differential Pressure Sensors (DPSs)** measure the difference between any two pressure levels using two input ports (see Fig. 1). Therefore, DPSs are naturally suitable in such applications where the *pressure difference* is required to be measured, such as in NPRs [28]. As a DPS has *high sensitivity* to differential pressure and is deployed in NPRs, we focus on DPSs in next sections.

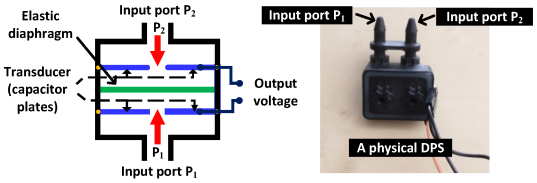

Figure 1: Basics of a DPS having two input ports.

2.4 Types of differential pressure sensors

DPSs typically have a elastic diaphragm placed in between two pressure input ports P_1 and P_2 (see Fig. 1). The diaphragm senses the differential pressure P_1 - P_2 applied to the pressure input ports by changing its shape. The diaphragm's shape change is converted to a proportional output voltage by using a transducer. DPSs either use a *capacitor*, or a *piezoresistor*, or *thermal mass-flow* as a transducer. A DPS is named after the type of transducer it has.

Fig. 1 shows a capacitive DPS as an example. The diaphragm is placed in between rigid capacitor plates. A differential pressure applied to the diaphragm generates a proportional change in the capacitive transducer resulting in a proportional voltage at the sensor output. We refer to Appendix 13.1 for details on other types.

2.5 Differential pressure sensors used in NPRs

DPSs are highly sensitive to a small differential change in the low pressure range (i.e., Pa range) and are naturally suitable to measure a pressure difference. Therefore, DPSs are a *natural choice* to be used in most RPM/BMS systems to control the negative pressure. To prove the prevalence of DPSs in NPRs, we investigate six industry-used RPM systems designed by popular manufacturers. All of these RPM systems use different types of DPSs that are shown in Table 2.

Table 2: Differential pressure sensors used in NPRs

Sl.	RPM/DPS part#	Type	Technology	Manufacturer
1	Series RSME [12]	Capacitive	Differential	Dwyer
2	SRPM 0R1WB [7]	Capacitive	Differential	Setra
3	One Vue Sense [8]	Unknown	Differential	Primex
4	RSME-B-003 [10]	Piezoresistive	Differential	Dwyer
5	Siemens 547-101A [9]	Unknown	Differential	Siemens
6	Series A1 [11]	Piezoresistive	Differential	Sensocon
7	GUARDIAN [21]	Unknown	Differential	Paragon Con.

2.6 Resonant frequency of a DPS and resonance

Resonant frequency: As mentioned in Section 2.3 and 2.4, typically, DPSs have a diaphragm/membrane and a transducer. Therefore, the pressure transducer system in DPS is considered as a second-order dynamic system, analogous to a bouncing ball [83]. Hence, the transducer system in a DPS has its own resonant frequency, f_r, which depends on the mass and stiffness of the diaphragm and mass of the pressure medium as Eqn. 1 [35].

$$f_r = \frac{1}{2\pi}\sqrt{\frac{\text{stiffness of a diaphragm}}{\text{mass of the pressure medium and diaphragm}}} \quad (1)$$

Resonance: Resonance occurs when the frequency of the input pressure wave matches the resonant frequency of the driven transducer system in a DPS, resulting in oscillations [60] in the transducer at large amplitude. This results in significant error by overshooting the peaks and troughs in the actual pressure wave, with an overestimation/underestimation of the actual reading. Therefore, users ensure that a DPS typically operates below its resonant frequency to prevent the resonance. A thumb's rule is 20% of the resonant frequency is typically used as the usable frequency limit for a given DPS [24]. This concept is illustrated in Fig. 2.

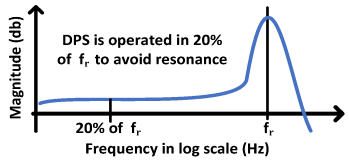

Figure 2: Resonant frequency in a DPS.

2.7 Electronics inside of a DPS

DPSs have a signal conditioning block in addition to a transducer (see Fig. 3). The signal conditioning block has differential amplifiers, low-pass filters (LPFs), and analog-to-digital converters (ADCs). A differential amplifier amplifies the output after removing the common-mode noises. An LPF with an ADC digitizes the measured value. Both analog and digital DPSs are available on the market. Analog DPSs output the analog signals from the differential amplifier directly, while digital DPSs contain the LPF and ADC.

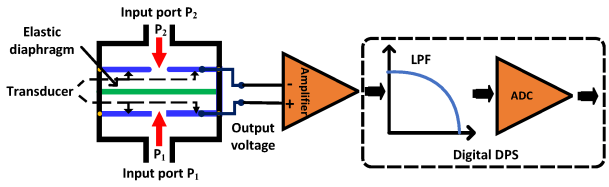

Figure 3: Different components inside of a DPS.

3 BASICS OF AN NPR

This section explains the construction of an NPR, where and how the DPSs are deployed in an NPR, and how the output from the DPS controls the NPR's control system.

3.1 Components of a real-world NPR

The components of an NPR vary depending upon the requirements of different facilities. However, the core components are more or less the same for most NPRs. Here, we detail the components of an anonymous NPR where we have visited and experimented with

to validate our attack model. **Please note that the target NPR evaluated in this paper is located in a clean room in an anonymous bioresearch facility. This NPR is also approved by the FDA and follows CDC guidelines.**

A typical construction of an NPR is shown in Fig. 4. An NPR has an HVAC system, which includes fresh air inlet ports. The fresh air from the outside is treated with multistage filters and then supplied to the isolation chamber of an NPR, including the anteroom, through an air conditioning (AC) unit. The AC has a Variable Air Volume (VAV) controller, which can increase or decrease the *supply* fan speed, controlling the fresh airflow to the NPR. An exhaust fan continuously moves the contaminated air out from the NPR through a HEPA filter using an exhaust pipe. The polluted air is further treated with a post-filtration unit having an Ultraviolet (UV) lamp. The room is maintained as airtight as possible. An RPM system is installed at the wall and integrated with the BMSs.

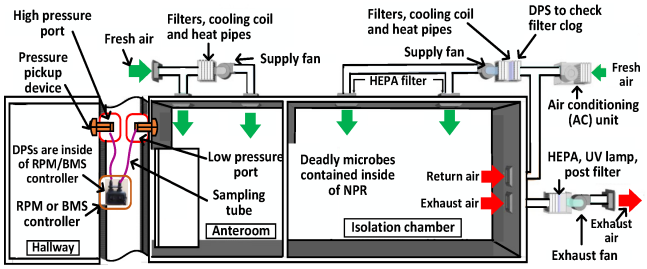

Figure 4: Different components of a real-world NPR.

3.2 How DPSs are deployed in an NPR

The HVAC system *ensures* a negative pressure in the NPR by controlling the fresh air and exhaust airflow using the supply and exhaust fan. An RPM system continuously *monitors* the negative room pressure. The RPM and HVAC systems use DPSs to monitor and control negative pressure in an NPR. The DPS is typically located inside of RPM or BMS controller. Commonly, the input ports of a DPS are connected with pressure ports using sampling tubes (see Fig. 4 and 5). The pressure port located inside an NPR is known as a *low pressure port*. The pressure port located outside an NPR in a hallway/reference space is known as a *high pressure port*. The sampling tube is connected with a pressure pickup device in the pressure ports. The pressure pick-up device increases the surface area of the sampling tube to pick up the target pressure accurately.

The low and high pressure ports are *exposed* and typically installed in *eyesight* near the door wall or on the ceiling of an NPR. There are other DPSs used in the HVAC system to indicate whether the filters of the HVAC are clogged or not. Typically they are not installed in the eyesight. Therefore, they are not accessible.

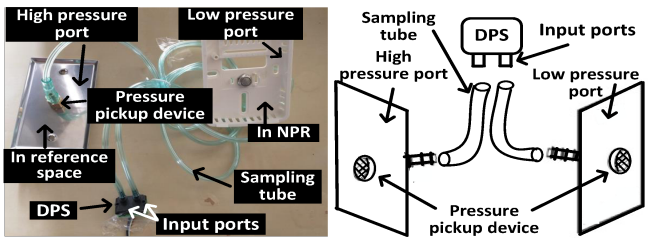

Figure 5: Pressure ports and sampling tube of a DPS.

3.3 Pressure control algorithm in an NPR

A pressure control algorithm running on the BMS controls the HVAC system of the NPR to maintain a constant negative pressure. A simplified control algorithm 1 is provided below. Algorithm 1 shows that the pressure readings from DPSs are used to control the speed of the supply fan and exhaust fan when the negative pressure increases or decreases from a reference value in the NPR, maintaining the negative pressure close to the reference value. The rest of the control algorithm 1 is self-explanatory.

Algorithm 1: Pressure control algorithm in an NPR.

Input: Pressure measurement data from DPSs
Output: Send control signals to the HVAC system
1 **for** $t \leftarrow 1$ ***to*** ∞ **do**
2 Track differential pressure reading from DPS's pressure ports
3 **if** *Negative differential pressure increases from a reference value* **then**
4 Reduce the supply fan speed of the AC to control the fresh airflow
5 Increase the exhaust fan speed to increase the exhaust airflow
6 **else if** *Negative differential pressure decreases from a reference value* **then**
7 Increase the supply fan speed of the AC to control the fresh airflow
8 Reduce the exhaust fan speed to reduce the exhaust airflow
9 **else**
10 Maintain the same state of the controller

4 ATTACK MODEL

Fig. 7 shows the different components of our attack model associated with NPRs. We discuss the components of the attack model below in a point-by-point fashion.

Attacker's intent: The attacker creates a forged resonance in the DPSs used in NPRs with malicious music having a frequency equal to the resonant frequency of the DPSs. As a result. the overshooting occurs in the actual pressure reading, resulting in a change in the negative pressure maintained in NPRs by the BMSs.

Target system: The attacker targets a facility where NPRs are used to contain deadly microbes and infectious airborne particles. Such facilities include isolation rooms, clean rooms and pharmacies in infectious-control hospitals, and biolabs in bioresearch facilities.

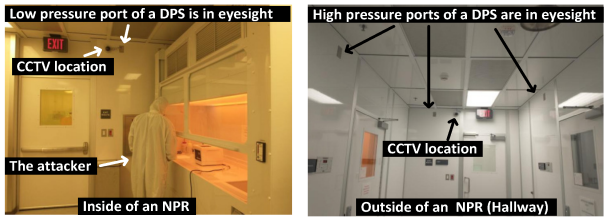

Figure 6: Pressure ports of DPSs are in eyesight in NPRs.

Attacker's capabilities: The attacker can surreptitiously place an attack tool near the target pressure ports of a DPS used in an NPR. The attack tool has an *audio source*. The audio source plays malicious music having a frequency equal to the resonant frequency of a DPS mounted in a target NPR. The audio source can be a simple cellphone or a speaker from an entertainment unit, such as televisions and radios, or CCTVs, placed in the vicinity of the pressure port of a target DPS. The low and high pressure ports are often mounted in eyesight, and placing the audio source near the target pressure port requires a *brief one-time access*. Moreover, audio sources, such as televisions or CCTVs with speakers, are often installed in NPR

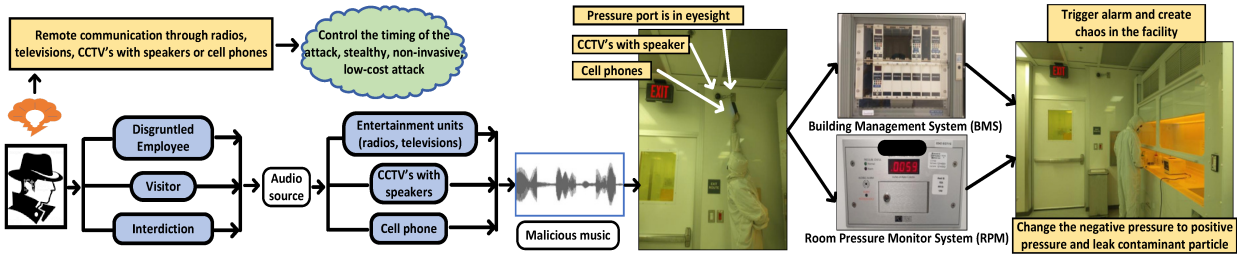

Figure 7: A brief overview of the attack model - A Wolf in Sheep's Clothing.

facilities near the pressure ports (see Fig. 6). The audio source may have wireless controls allowing for remote communication. Therefore, the attacker can remotely control the timing of the attack and can pick a vulnerable time (e.g., infectious patient admitted in an NPR, ongoing bioresearch, etc.) for a maximal consequence. The authority of the target NPR may not be aware of the attack model and would possibly neglect the security implications of any audio source placed near the pressure ports in an NPR.

Attacker's access level: The access near the pressure port of a DPS needed for the attack can be possible in at least two scenarios. **First** (most likely), a malicious employee or a guest or a maintenance person, who has access to an NPR, may place the audio source near the pressure port. Though an NPR is restricted for unauthorized personnel, getting brief one-time access near the pressure port may not be difficult for an attacker in disguise of a guest or a maintenance person. **Second** is interdiction, which has been rumored to be used in the past [40, 51, 71, 80] and has been recently proven to be feasible [73]. During interdiction, a competitor can intercept the DPS during delivery or installation and may modify the DPS by placing an audio source inside and then proceed with delivery or installation to the NPR facility.

Playing malicious music: The attacker can play the malicious music in speakers to inject sound into DPS in the following three ways. **First**, the attacker can use a standard phishing attack to trick the authority into playing malicious music via email or a web page with autoplay audio enabled in CCTVs or televisions. **Second**, the attacker can play the malicious music using public radios. If some individuals place their radio near a pressure port, there is a good chance that the attack will be effective. **Third**, a physical proximity attack can happen if an attacker plays the music via a cell phone.

Outcomes of the attack: The attacker changes the actual pressure reading of DPSs and fools the BMS to turn the negative room pressure into a positive pressure or reduce the negative pressure from a reference value. This will trigger an alarm and create chaos in the facility. Moreover, the NPR cannot work properly for what it is intended to design for and may not contain the deadly microbes. The intentional leak of deadly microbes from NPRs may result in bioterrorism. The potential for mass destruction by bioterrorism is evident from a report from the U.S. Office of Technology, which predicted that the release of 100 kg of anthrax spores in Washington, DC, would cause 130,000 to 3 million deaths, matching the lethal potential of a hydrogen bomb [58]. The CDC reviewed potential microbes, such as smallpox and viral hemorrhagic fever, as airborne bioweapons [42]. An intentional leak of these bioweapons from an NPR by an attacker can trigger a worldwide pandemic with a tremendous loss of human lives and monetary resources.

Non-invasiveness: The spoofing attack is non-invasive and is performed without making physical contact with the target DPS. The attacker don't need to directly access or physically touch the sensor readings. However, we expect that attackers can examine the behavior of a similar sensor subjected to acoustic impacts before launching an actual attack.

Attacker's resources and cost: We assume that the attacker knows how the HVAC system works in NPRs and has a high school knowledge of resonance in DPSs. Moreover, a simple cell phone with a price of $60 - $100 can play the malicious music with a proper resonant frequency to attack the NPR.

5 THREATS IN AN NPR

Here, we find the resonant frequency of DPSs used in NPRs by thorough experiments and explain how the resonance can be affected by different factors in an NPR.

5.1 Sound wave as a threat to DPSs

Sound wave: Sound is frequently referred to as a pressure wave since it is made up of a repeating pattern of high and low-pressure regions traveling across a medium [4].

Threat to DPSs: As a result, when sound waves collide with the diaphragms of DPSs, the diaphragm starts vibrating with the same frequency of sound. Therefore, having the above knowledge, a smart attacker can use a sound with a frequency equal to the resonant frequency of the DPS to create a *resonance* and artificially displace the diaphragm in its maximal amplitude. The forged displacement of the diaphragm can change the pressure reading of a DPS by introducing overshooting in the actual pressure waveform.

5.2 Modeling sound effects on DPSs

We develop a model for how a sound wave perturbs the reading of a DPS. We measure the pressure as a linear combination of the original/equilibrium pressure $P_o(t)$ without a sound, and the external sound pressure $P_s(t)$. After a sound played at a frequency f, with an amplitude A_0, velocity v, and phase ϕ from a distance d, the total measured pressure $P(t)$ by a DPS can be modeled as:

$$\begin{aligned} P(t) &= P_o(t) + P_s(t) \\ &= P_o(t) + h(d,f) \cdot A_0 cos(2\pi f t + d/v + \phi) \end{aligned} \tag{2}$$

where $h(d,f)$ represents the attenuation of a sound wave, which depends on distance d and frequency f of the audio source. If the frequency f of the sound wave is equal to the DPS's resonant frequency f_r, the impact $P_s(t)$ will be maximum for a target DPS.

It should be clear from the above explanation that the attacker, at first, needs to identify the resonant frequency f_r of the DPS to orchestrate an attack. However, datasheets of the pressure sensors

used in NPRs do not provide information related to their resonant frequencies. Therefore, we use thorough experiments to find the resonant frequency discussed in detail in the next sections.

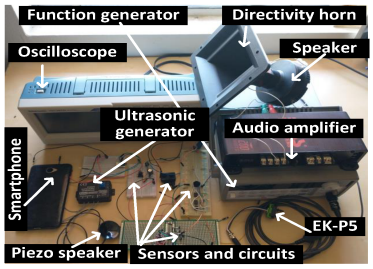

Figure 8: Experiment setup for different DPSs.

5.3 Experimental setup

Figure 8 depicts the experimental setup to evaluate the resonant frequency of TBPSs. We produce a single-tone sound wave at different frequencies from an audible value of 50 Hz to an inaudible value of 40 kHz with the following three different audio sources.

1. Source 1: We use a Samsung Galaxy S10 smartphone [29] to generate frequencies within 50 Hz to 13 kHz. We use an app named Function Generator to sweep frequencies within the specific frequency range using the smartphone, which has a *sound pressure level (SPL)* of ~ 80 dB [38] at its maximum volume at 1-inch distance.

2. Source 2: We use a function generator [25], a 200 W audio amplifier (part# BOSS Audio Systems R1002 [15]), a speaker (part# Goldwood Sound Module [19]), and a directivity tweeter horn (part# GT-1188 [20]) to generate frequencies within 100 Hz to 18 kHz. The directivity horn is connected with the speaker to direct the sound to the target sensor. This setup can generate an SPL up to ~ 95 dB at 1-inch distance. The reason for using audio *source 2* when we have the audio *source 1* is to test the sensors with a higher SPL. We use an app named Sound Meter [33] to measure the SPL.

3. Source 3: We use an ultrasound generator (part# Kemo Electronic M048N [37]), a piezo speaker (part# ToToT Ultrasonic Speaker [27]) to generate frequencies within a range of 15 kHz to 40 kHz.

We test 8 industry-used TBPSs from 5 different manufacturers including analog and digital types (see Table 3). Out of the 8 sensors, 6 of them are DPSs, and 2 of them are gauge pressure sensors (see Section 2.3). We use gauge sensors to identify that not only the DPSs but also the gauge pressure sensors have resonant frequencies that can be utilized by an attacker. This supports the idea that if an NPR uses a gauge pressure sensor instead of DPSs, an attacker can also target those NPRs. Therefore, our attack model will work for any TBPSs irrespective of gauge pressure sensors and DPSs.

The experimental setup is placed inside an acoustic isolation chamber to avoid external noise. To read and log the pressure measurements, we utilize an oscilloscope for analog TBPSs and a Ek-P5 [18] test kit connected with our laptop for digital DPSs.

Please note that a few pressure sensors require a separate unique circuit for testing, data collection, and signal conditioning. Therefore, we build a separate signal conditioning circuit for each of the sensors that requires it. As an example, a signal conditioning circuit using an instrumentation amplifier to collect data from a DPS with part# NSCSSNN015PDUNV is shown in Appendix 13.2.

5.4 Evaluating the resonant frequency

A single tone sound having a frequency between 50 Hz to 40 kHz with a 10 Hz increment is applied to *one of the two ports* of a DPS or to a single port of a gauge pressure sensor in our testbed *without* a sampling tube. We vary the frequency every 3 ms and record the data for every frequency using an oscilloscope for analog gauge/DPSs or using the Ek-P5 test kit for digital DPSs. We maintain the SPL within ~ 35 - 95 dB from 2 cm in our experiments.

We examine the difference in the sensor readings with and without sound signal. When there is no sound wave present, the two input ports of a DPS or a single input port of a gauge pressure sensor measure the unperturbed pressure from the environment. As a result, the intended output of the sensor should be zero in the absence of the single tone sound wave. When the single tone sound is applied to an input port of a DPS or a gauge sensor, the output of the target sensor starts oscillating. The oscillations reach a peak value at a resonant frequency of the target pressure sensor.

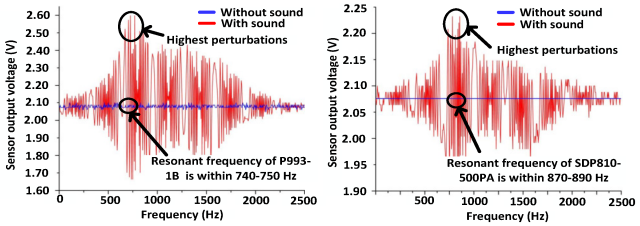

Figure 9: Sound injection effect on (left) P993-1B and (right) SDP810-500PA pressure sensors for different frequencies.

Two examples are shown in Fig. 9 as a proof-of-concept to support our observations on resonant frequencies. The outputs from an analog DPS with part# P993-1 and a digital DPS with part# SDP810-500Pa are shown in Fig. 9 (left) and (right), respectively. The blue color is the sensor output before applying the sound, and the red color is the sensor output after applying the sound. It is clear from Fig. 9 that the sensor output has the largest perturbations within 740-750 Hz for an analog DPS with the part# P993-1B and within 870-890 Hz for a digital DPS with the part# SDP810-500Pa.

Table 3 summarizes the experiment's findings on resonant frequencies. According to our findings, 6 of the 8 pressure sensors resonated in response to the applied sound wave. We find that the detected resonant frequencies range from ~600 Hz to ~1800 Hz, which are in the audible range.

We are unable to detect the resonant effect in 2 of the 8 sensors: part# TBPDPNS100PGUCV and NSCSS015PDUNV. We observe from Table 3 that with the increase of the pressure range, the value of the resonant frequency increases. The reason behind this is that the sensors, which work in high pressure range, have more stiff diaphragms compared to those sensors, which work in low pressure range. For example, MPVZ5004GW7U has a higher resonant frequency than P1K-2-2X16PA because of its higher pressure range. Therefore, it is possible that the resonant frequencies of TBPDPNS100PGUCV and NSCSS015PDUNV may fall outside of 40 kHz, which is the highest test frequency we use in our experiments.

5.5 Why resonant frequencies in audible range?

An interesting observation from Table 3 is that all resonant frequencies of the DPSs used in NPRs fall in the audible range. We only

Table 3: Summary of the resonant frequencies of Transducer Based Pressure Sensors (TBPSs) *without* a sampling tube.

Sl.	Sensor	Manufac.	Type	Transducer	Pressure range	Interface	Resonant freq.
1	P1K-2-2X16PA [17]	Sensata	Differential	Piezoresistive	0 to 500 Pa	Analog	790 - 800 Hz
2	MPVZ5004GW7U [23]	Freescale	Gauge	Piezoresistive	0 to 3.92 kPa	Analog	1750 - 1800 Hz
3	SDP810-250PA [30]	Sensirion	Differential	Thermal mass-flow	±250 Pa	Digital	760 - 780 Hz
4	SDP810-500PA [30]	Sensirion	Differential	Thermal mass-flow	±500 Pa	Digital	870 - 890 Hz
5	TBPDPNS100PGUCV [14]	Honeywell	Gauge	Piezoresistive	0 to 689 kPa	Analog	not found
6	P993-1B [26]	Sensata	Differential	Capacitive	±248 Pa	Analog	740 - 750 Hz
7	NSCSS015PDUNV [36]	Honeywell	Differential	Piezoresistive	±103 kPa	Analog	not found
8	A1011-00 [32]	Sensocon	Differential	Piezoresistive	0 to 60 Pa	Digital	680 - 690 Hz

experimented with 8 sensors used in NPRs. Can we conclude from our experiments that most of the sensors used in NPRs typically have resonant frequencies in the audible range? The answer is *Yes*.

Reason: Table 1 shows that NPRs need to maintain a low negative pressure within 2.5 Pa to 15 Pa. Therefore, DPSs used in NPRs are selected to have high sensitivity in the low Pa range for an accurate measurement. The sensors working in the low pressure range have less stiff diaphragms compared to those sensors working in the high pressure range [22]. Eqn. 1 indicates that resonant frequency decreases in a square-root fashion with the decrease of stiffness of the diaphragms. Therefore, the DPSs working in a pressure range of few Pa, typically have less stiff diaphragms with low resonant frequencies typically in audible range (i.e., <20 kHz).

5.6 Factors influencing the resonant frequency

We measure resonant frequencies in Table 3 by directly applying the sound wave to the input ports of a pressure sensor. However, sampling tubes and a pressure pick-up device are often connected with the pressure ports of a DPS (see Fig. 4 and 5) to pick up the pressure from a target location. The *geometric properties* of the sampling tube affect the characteristics of the DPS's transducer systems. As a result, the resonant frequency of DPSs *with* sampling tubes differs from the value *without* sampling tubes.

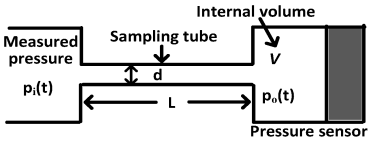

Figure 10: Modeling sound pressure inside of a DPS having a sampling tube as a Helmholtz resonator.

Helmholtz resonators: A pressure sensor with a sampling tube can be modeled as Fig. 10. Let's denote the internal volume of the sensor by V, and the internal diameter and length of the tube by d and L, respectively. As the sensor's internal volume and the connecting tube are similar to a structure having a cavity with a narrow neck, a pressure sensor with a tube is a basic form of discrete Helmholtz fluid resonator [41, 55]. The fluid in the tube acts as the oscillator mass, while the compressible fluid in the cavity acts as the oscillator spring. The Helmholtz resonator can be simplified by a second-order dynamic system (see Section 2.6), which yields the following relation between the sampling tube inlet pressure $p_i(t)$ and the sensor output pressure $p_o(t)$:

$$\frac{d^2p_o}{dt^2} + 2\xi\omega_h\frac{dp_o}{dt} + \omega_h^2 p_o = \omega_h^2 p_i \tag{3}$$

where $\omega_h = 2\pi f_h$, f_h is the overall resonant frequency of the sensor with a tube, and ξ is the damping ratio. The resonant frequency f_h of the sensor with a tube can be expressed as:

$$f_h = \frac{1}{2\pi}v\sqrt{\frac{AS}{LVM}} \tag{4}$$

where v is the sound velocity in air, A is the internal cross-sectional area of the tube, S is the stiffness of the diaphragm, M is the mass of the pressure medium and diaphragm. Eqn. 4 indicates that the resonant frequency of a DPS with a tube increases with the increase of the tube's internal cross-sectional area A and decreases with the increase of the tube length L. As the DPS used in NPRs has a standard diameter of its input ports, the diameter of the sampling tube is somewhat fixed. Therefore, we focus on the effect of sampling tube length on our attack model in the next section.

5.7 Resonance with sampling tube in NPRs

Fig. 4 and Fig. 5 show how the sampling tube is connected with the DPS's ports. For good sensitivity and error-free measurement, the DPS is placed close to the high and low pressure ports. Therefore, the length of the sampling tube is typically < 2 m. Therefore, we vary the length of the sampling tube up to 2 m with a 0.4 m increment for a diameter of 5/16 inch and calculate resonant frequencies for each of the 6 DPSs (i.e., having valid resonant frequency) from Table 3. Fig. 11 shows the results. We notice that with the increase of the sampling tube length, the sensor's overall resonant frequency f_h reduces, supporting Eqn. 4.

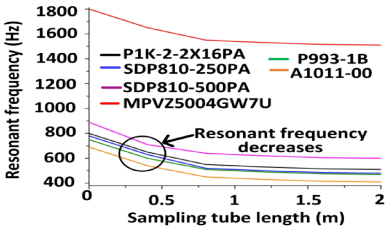

Figure 11: Resonant frequency decreases with tube length.

5.8 A wolf in sheep's clothing

It is evident from Section 5.7 that the resonant frequencies of DPSs even with the sampling tube fall within audible range. Attacking DPSs with a sound just having resonant frequencies would make the attacker immediately identifiable because resonant frequencies will generate a "beep"-ish sound, raising a concern to the authority.

We came up with a solution explained in **Section 6.1** to *disguise* the resonant frequencies inside a popular music so that the attack will not be identifiable. Once the attacker injects the malicious

music into DPSs, he/she can successfully create resonance in DPSs. This is referred to as putting *"the wolf in sheep's clothing"* since it is the resonant frequency that has been disguised inside music.

6 ATTACKING A NEGATIVE PRESSURE ROOM

As mentioned in Section 3.2, the low pressure port of the DPS is exposed to the negative pressure room and the high pressure port is linked to a hallway, which is a reference space. If the pressure at the low pressure and high pressure port is denoted by P_L and P_H, respectively, the DPS measures the differential pressure, P_D as:

$$P_D = P_L - P_H \tag{5}$$

As mentioned in Section 3.1, an NPR has an HVAC and an RPM system. There can be the following two scenarios depending on how the HVAC and RPM systems use the DPSs in NPRs.

First, the HVAC and RPM systems in NPRs use the *same* DPS to control and monitor the negative pressure in an NPR. This scenario exists in modern facilities where both HVAC and RPM systems are automated and integrated with the BMS.

Second, the HVAC uses a DPS to maintain the negative pressure, and the RPM uses a *separate* DPS to monitor the differential pressure in an NPR. Here, the RPM system only gives an alarm if the negative pressure falls below a threshold but is not responsible for maintaining a negative pressure in an NPR.

We discuss the above two scenarios below.

6.1 When HVAC and RPM use the same DPS

This scenario is easier for the attacker as he/she can attack both the HVAC and RPM systems of an NPR just by attacking a single DPS. The attacker can either inject sound to the low pressure port of the DPS if he/she is inside of the NPR and find that it is comparatively easier to access the low pressure port. Otherwise, the attacker can inject sound to the high pressure port of the DPS.

A simple resonance is not enough: If the attacker creates resonance either by attacking the low pressure or high pressure port of the target DPS in the NPR, the resonance changes the original pressure reading by overshooting the original pressure level in both upward and downward directions (see Fig. 9). Therefore, the differential pressure reading P_D in the DPS (Eqn. 5) starts fluctuating. As a result, the *supply fan* and the *exhaust fan* immediately track the DPS's pressure fluctuations and vary their fan speed to maintain a static negative pressure inside of the NPR, following the algorithm 1. However, the rate of change in the pressure reading because of the resonance is high for a mechanical fan to track. Therefore, the supply fan and the exhaust fan cannot vary their speed with the high fluctuating rate. As a result, the negative pressure in the NPR only fluctuates a little bit and truly does not change on a large scale from the reference value. Moreover, the attacker does not have any adversarial control over it. Therefore, the attack can not induce any noticeable effect in the target NPR.

A wolf in sheep's clothing: To create a maximal change in the NPR's negative pressure, a smart strategy is adopted in addition to simply *disguising* the resonant frequency band inside of music. The strategy is illustrated in Fig. 12. The resonant frequency is inserted into the music as a segment in a specific interval for a certain duration. Let us denote the interval by T_I and duration by T_D. Every inserted segment of resonant frequency is *ended at its peak* after duration T_D, and the same segment is inserted again in every interval T_I. When the inserted segment is ended at its peak, the corresponding pressure wave inside the DPS's transducer system also ends at its peak (see Fig. 12). As a DPS with a sampling tube is a second-order oscillating system (i.e., Helmholtz resonator), the pressure wave does not instantly fall to zero from the peak value. Instead, the pressure wave starts to attenuate from its peak exponentially following Eqn. 6 of a damped 2^{nd} order system [35].

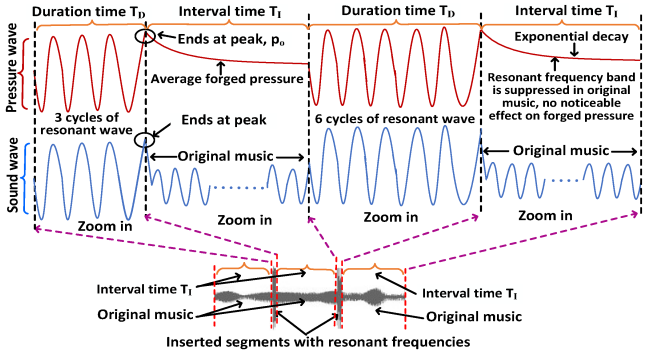

Figure 12: Turning a popular music into an attack tool.

$$p(t) = p_o e^{-\omega_h t} + (\omega_h p_o + v_o) t e^{-\omega_h t} \tag{6}$$

where p_o and v_o are the initial pressure and velocity at peak, respectively, and ω_h is the angular resonant frequency. The term v_o depends on the viscosity and density of the pressure medium.

The interval time T_I is selected in such a way that the pressure wave never falls to zero. Therefore, there is always an *average forged* pressure present inside the DPS's transducer system, originating from the injected music by the attacker. As the generated forged pressure has an *average* value greater than zero and changes *slowly*, the *supply fan* and the *exhaust fan* can track the pressure change in DPS, and they can vary their fan speed according to the pressure reading of the DPS. Therefore, this time the attack can induce a noticeable effect in the target NPR.

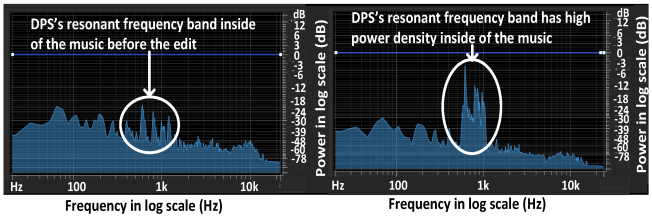

Figure 13: High power density of resonant frequencies inside of a music because of the inserted segments.

Between two consecutive inserted segments of resonant frequency (i.e., in the interval time T_I), the original music is inserted by suppressing its resonant frequency components. Therefore, the original music does not have a noticeable effect on the forged pressure present in the interval T_I. Moreover, the inserted segment with the resonant frequency has ~3.8x increased power density compared to the original music. Fig. 13 shows this phenomena for SDP810-500PA, which has resonant frequency within 700 - 900 Hz (see Fig. 11). Therefore, the inserted segment can create a maximal effect in the NPR by turning a negative pressure into a positive one.

Adversarial control: The attacker can control the average forged pressure in the DPS's transducer system by controlling the interval time T_I and duration time T_D.

The duration T_D cannot be too small as a small T_D cannot provide the inserted segment enough time to impact the DPS. The T_D cannot be too large because the inserted segment with large T_D can badly distort the music so that the attack might be identified. The duration of T_D should be equal to or larger than the period of the resonant frequency so that at least one cycle of the resonant wave is accommodated inside of the duration T_D (i.e., inserted segment).

With a small interval T_I, the average forged pressure is increased. However, a small T_I results in a large number of inserted segments that may distort the music significantly. We measured the forged pressure for a T_I between 15 ms to 60 ms for a ~65 dB sound for a DPS (part# A1011-00) with a 1 m sampling tube. The sound is applied at 0.2 cm from the pressure port. The result is shown in Fig. 14 for a duration time T_D = 1.47 ms, which is equal to the period of the resonant wave of part# A1011-00 (i.e., part# A1011-00 has resonant frequency 680 Hz from Table 3; 1/680 Hz = 1.47 ms).

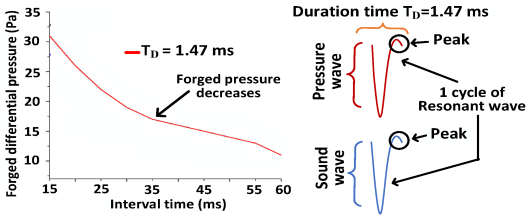

Figure 14: Adversarial control using malicious music.

As mentioned earlier, the resonant frequency can vary within a range depending upon the sampling tube length. As the attacker may not know the exact length of the sampling tube, the attacker may need to vary the duration time T_D within a range to accommodate at least one cycle of the variable resonant wave for a maximal impact (Fig. 14). The attacker can also vary the number of cycles in the duration T_D from one inserted segment to another inserted segment. For example, the first inserted segment in Fig. 12 has 3 cycles, whereas the second segment has 6 cycles within the duration T_D.

Tools for a malicious music: The attacker selects music and inserts segments of resonant frequencies within the music in a way already explained in Section 6.1 using a software named *Adobe Audition*. Though someone who has listened to the music many times before may identify the change in the music, the vast majority of people will either be oblivious of the change or will incorrectly ascribe the change in the music to a speaker issue. For example, we pick a popular song *Hello* by *Adele* and convert it into a malicious music in a way explained in Section 6.1 for T_D = 2 ms and T_I = 15 ms. The malicious music is uploaded in the following link: https://sites.google.com/view/awolfinsheepsclothing/home

Injecting music into the low pressure port: Let us give an example to elaborate on the result of injecting music into the low pressure port. Suppose, before an attack, the pressure at a low pressure port P_L = 10 Pa and at a high pressure port P_H = 12.5 Pa. Therefore, the differential pressure from Eqn. 5 is P_D = 10 - 12.5 = - 2.5 Pa, which is the reference differential pressure in the NPR. Suppose the forged pressure resulting from the injected malicious music into the low pressure port is 8 Pa. Now, after the attack, P_D = (10 + 8 = 18) - 12.5 = 5.5 Pa. Therefore, the HVAC system will reduce the NPR's pressure from 18 Pa to 10 Pa to keep the differential pressure at -2.5 Pa. The reduction of 8 Pa in the NPR will result in a *true* differential pressure of P_D = (10 - 8 = 2) - 12.5 = -10 Pa. The injection of music into the low pressure port results in more negative differential pressure (i.e., - 2.5 Pa to - 10 Pa), which is actually good for keeping deadly microbes in the NPR. However, the abnormal change in negative pressure may trigger an alarm by the RPM system and create chaos in the facility. An attacker can use this chaos to initiate a stronger attack, such as stealing deadly microbes from biosafety cabinets as he is already inside of the NPR.

Injecting music into the high pressure port: Let us use the previous example to elaborate on the effect of injecting music into the high pressure port. If the forged pressure resulting from the injected music into the high pressure port is 8 Pa, the P_D after the attack is 10 - (12.5 + 8) = -10.5 Pa. Therefore, the HVAC system will increase the NPR's pressure from 10 Pa to 18 Pa to keep the differential pressure at -2.5 Pa. The increase of 8 Pa in the NPR will result in a *true* differential pressure of P_D = (10 + 8 = 18) - 12.5 = 5.5 Pa, which is positive. The consequences of turning a negative pressure into a positive one in an NPR can be catastrophic as the NPR cannot contain the deadly microbes anymore, causing a potential leak of microbes from the compromised NPR. Moreover, an abnormal change in the negative pressure may trigger an alarm by the RPM system and create chaos in the facility. An attacker can use this chaos to initiate a stronger attack, such as entering the NPR and stealing deadly microbes from the biosafety cabinets.

6.2 When HVAC and RPM use separate DPSs

When the HVAC and RPM systems use separate DPSs, and if the attacker has a *single* audio source, he/she should attack the high or low pressure port of the DPS connected with the HVAC system to change the negative pressure in an NPR. Because the HVAC system maintains the negative pressure in an NPR. However, if the attacker attacks the high or low pressure port of the DPS connected with the RPM system, only an alarm may be triggered, and chaos will be created in the facility, but it will not change the NPR's pressure. The attacker can use the attack model already explained in Section 6.1 either to attack the HVAC or RPM system of an NPR.

A stronger attacker: Suppose we consider a stronger attacker, who can use *multiple* audio sources to attack the RPM and HVAC systems simultaneously. In that case, he/she can avoid the alarm triggered by the RPM system in the following way.

Let us explain this attack model using the same example from Section 6.1. Let us assume the attacker injects the same *forged* pressure of 8 Pa by music to the high pressure port of the DPS connected with the HVAC system. Therefore, the HVAC system similarly will increase the NPR's pressure from 10 Pa to 18 Pa, resulting in a positive differential pressure of 5.5 Pa. The RPM system will trigger an alarm for this abnormal change in the NPR's pressure. To prevent the alarm from being triggered, the attacker must need to inject the same 8 Pa *forged* pressure to the high pressure port of the DPS connected with the RPM system. As a result, the RPM will measure differential pressure of 18 - (12.5 + 8) = -2.5 Pa, which is equal to the NPR's reference pressure. Therefore, the RPM system will not trigger any alarm, and the attack will remain unidentified, resulting in a stronger attack model.

However, if both of the high pressure ports of the RPM and HVAC systems are in *close proximity*, the attacker can use a *single* audio source to attack the NPR without triggering the alarm.

6.3 Attacking multiple NPRs simultaneously

It is possible to simultaneously attack multiple NPRs just by injecting music into *a single* high pressure port of the DPS connected with the HVAC or RPM systems. As we mentioned earlier, the high pressure port is located in hallway to measure the reference pressure, and the NPR maintains a negative pressure inside with respect to the reference pressure. If there are multiple NPRs in a facility and if all the NPRs use a common place (e.g., hallway) as their reference pressure, it is a common practice to connect all the high pressure ports from all the NPRs into *one common* high pressure port to reduce cost. This is shown in Fig. 15. As multiple NPRs share a common high pressure port, the attacker can simultaneously attack multiple NPRs just by attacking the common high pressure port in the facility. It can trigger a combined leak of deadly microbes from multiple NPRs and can create chaos in different parts of the facility.

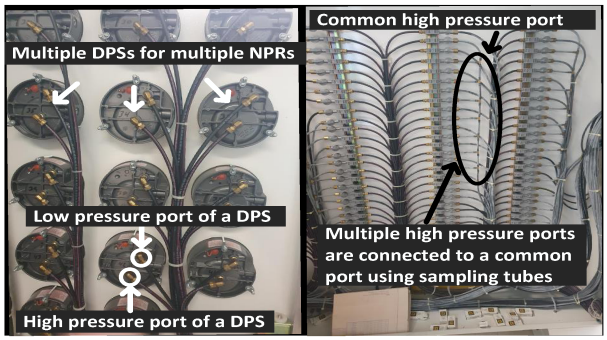

Figure 15: Multiple high pressure ports are connected together to a common high pressure port.

7 ATTACK MODEL DEMONSTRATION

We demonstrate our attack at an FDA-approved NPR located in an anonymous bioresearch facility. The demonstration is shown in Fig. 16. This facility uses separate DPSs for the HVAC and RPM systems. The location of the DPS connected with the RPM system is close to the exit door. The DPS connected with the HVAC is at the sidewall of the wet bench. The wet bench stores sensitive particles inside of it under negative pressure. The authority did not permit us to attack the DPS connected with the HVAC system due to safety protocols. Therefore, we only demonstrate the attack on the DPS connected with the RPM system.

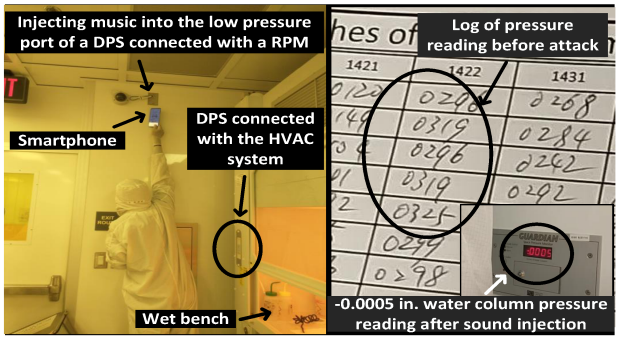

Figure 16: Attacking a practical NPR in a bioresearch facility.

We use a Samsung Galaxy S10 smartphone from a 0.1 cm distance with an SPL of ~ 65 dB to inject the malicious music into the low pressure port of the RPM system for a room #1422. We check the differential pressure for room #1422 before the attack from a logbook. We can see that the negative pressure stays within a range of 0.0278 - 0.0325 inch water column (i.e., 6.9 - 8 Pa). After injecting music from the smartphone, the negative pressure reading in the RPM system changes to a positive pressure of 0.0005 inch water column (i.e., 0.12 Pa). That is a 7 - 8 Pa pressure reading change in the RPM system due to an attack. A video demonstrating the attack model in the NPR is posted at the following link: https://sites.google.com/view/awolfinsheepsclothing/home

Though we are not permitted to attack the DPS connected with the HVAC system, according to the authority, our attack on the DPS connected with the HVAC system would create the same pressure change in the NPR.

8 ATTACK MODEL EVALUATION

We already evaluate resonant frequencies of DPSs in Section 5 in detail. Here, we evaluate our attack model further for other parameters related to the DPSs and NPRs.

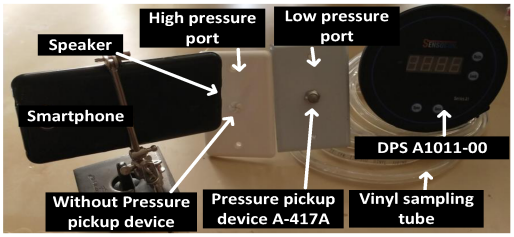

Figure 17: Experimental setup for evaluating attack model.

8.1 Experimental setup

We already show our attack at an FDA-approved NPR in a bioresearch facility in Section 7. As it is not *permitted* to vary different parameters of the DPS's transducer system located in the bioresearch facility, we prepare a testbed to evaluate our attack model. We use an industry used DPS from Sensocon with part# A1011-00 [11], two vinyl sampling tubes having inner diameters of 3/16" and 5/16" [16], a pressure pickup device with part# A-417A [34] and an oscilloscope in the testbed (see Fig. 17).

8.2 Varying the tube length and diameter

We vary the sampling tube length from 1 m to 5 m with a 1 m increment for two inner diameters of 3/16" and 5/16". We connect the sampling tube and pressure pickup device with the input ports of the A1011-00 sensor and inject sound into one of the pressure ports with the Samsung Galaxy S10 smartphone from a 0.1 cm distance. The result is shown in Fig. 18 (left). With the increase of the sampling tube length and the decrease of the sampling tube inner diameter, the sound damping inside the tube increases. Therefore, the forged differential pressure originated from the injected music reduces for larger length and smaller diameter.

8.3 Varying the SPL of the audio source

A logarithmic scale known as Sound Pressure Level (SPL) is used to measure the loudness of a sound. SPL is measured in decibels (dB). We vary the SPL of the audio source (i.e., Samsung Galaxy S10) from 30 dB to 80 dB with a 10 dB increment for 1m, 2 m, and 3 m of

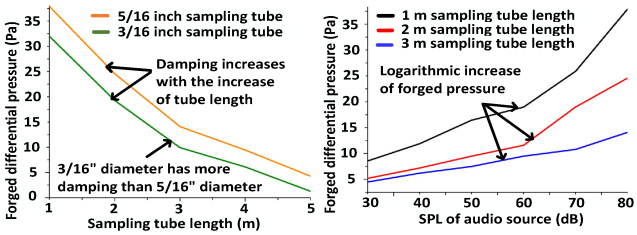

Figure 18: (left) Impact of sampling tube length and diameter. (right) Impact of the SPL of the audio source on the attack

sampling tube (5/16" diameter) lengths for a 0.1 cm distance from the pressure pickup device. The result is shown in Fig. 18 (right). As with the increase of the SPL, the sound pressure from the audio source logarithmically increases. Therefore, the forged differential pressure also increases logarithmically. As sound damping increases with the increase of sampling tube length, the shorter sampling tube causes higher forged differential pressure.

8.4 Varying the distance of the audio source

We vary the distance of the audio source (i.e., Samsung Galaxy S10) from the pressure pickup device for 0 m (no sampling tube), 1 m, 2 m, and 3 m of sampling tube (5/16" diameter) lengths. The result is shown in Fig. 19. In acoustics, the SPL of a sound wave radiating from a point source decreases as the distance increases following the inverse-proportional law [6]: $SPL \propto 1/distance$. Therefore, the forged differential pressure also decreases with the increase of audio source distance from the pressure pickup device. Fig. 19 (right) shows that an audio source has more impact on the DPS without a sampling tube (i.e., no dampening) with a saturated output.

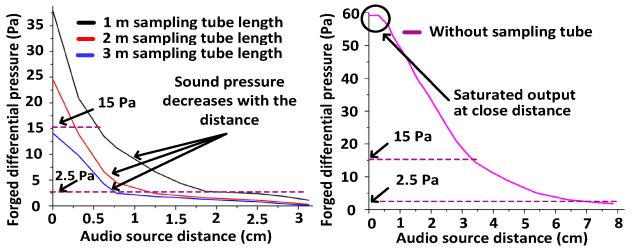

Figure 19: Impact of audio source distance on the attack.

8.5 With and without a pressure pickup device

A pressure pickup device is connected with the other end of the sampling tube and installed at the high and low pressure ports, mounted on the wall. The pressure pickup device increases the exposed area of the sampling tube end. Therefore, a small change in pressure can be sensed without an error. It is possible that some NPRs don't use pressure pickup devices; instead, a simple hole is mounted at the pressure ports. To evaluate the effect of the pressure pickup device, we inject music from a 0.1 cm distance into the pressure port with and without the pressure pickup device and vary the sampling tube length from 1 m to 5 m with a 1 m increment. We see from the results in Fig. 20 that the forged pressure is lower with a pressure pickup device. Because a pressure pickup device has foam gasket inside, which dampens the injected sound into it.

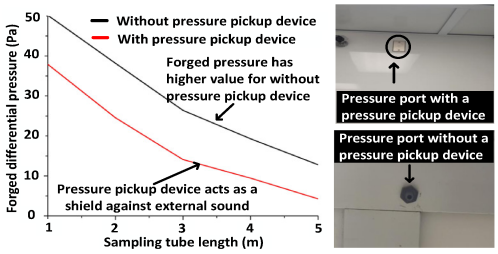

Figure 20: Impact of the pressure pickup device on the attack.

9 FEASIBILITY OF THE ATTACK

1. Audio source distance: Section 8 indicates that the sampling tube's length and audio source's distance can restrict the effectiveness of the attack. Moreover, Table 1 indicates that the negative pressure has to be maintained between -2.5 Pa to -15 Pa for country-specific requirements. Now, Fig. 19 (left) indicates that the audio source should be less than 0.6 cm away (1 m tube length) from pressure ports to generate a 15 Pa forged pressure, which can turn a -15 Pa negative pressure into a positive pressure. Fig. 19 (left) also indicates that the audio source should be less than 2.5 cm away from the pressure port to generate a 2.5 Pa forged pressure, which can turn a -2.5 Pa negative pressure into a positive pressure. *This indicates that the CDC guidelines (i.e., -2.5 Pa) in Table 1 can be impacted from a larger audio source distance compared to the guidelines adopted in Taiwan and Australia.*

However, the audio source needs to be in close proximity to the pressure ports to have a feasible attack. CCTV's with speakers and entertainment units are often located in such close proximity to the pressure ports. Moreover, Fig. 19 indicates that the attacker can use an audio source from a larger distance if the sampling tube length is shorter or no sampling tube is present. For example, the audio source can generate a 2.5 Pa forged pressure at 7 cm far from the pressure ports without a sampling tube (Fig. 19 (right)). Sampling tube length depends on the location of DPSs from the pressure ports. Depending upon different locations of DPSs, the sampling tube length can be very short, or even no sampling tube can be present. The attacker can target those DPSs for greater impact.

2. LPF and the resonant frequency: Section 2.7 mentions that a DPS has an LPF. Therefore, simply filtering the resonant frequency using an LPF can prevent the resonance in DPS. However, manufacturers don't use the LPF to filter out the resonant frequency because the resonant frequency of a DPS is not constant. A resonant frequency not only depends on the transducer and diaphragm of the DPS but also depends on the sampling tube's length and diameter, the fluid's viscosity and density inside of the sampling tube (see Sections 5.6 and 5.7). Therefore, it **varies** within a *band* for different transducer systems depending upon different applications. Moreover, manufacturers also don't filter out the whole *band* where the resonant frequency may belong. The reason is that a DPS is not only used in NPRs but also used in other *dynamic pressure sensing* applications where removing a frequency band might remove important information from the input data.

We can find a simple proof of this concept in Table 3. Both of the digital DPSs in Table 3 have ~ 2.1 kHz sampling frequency and 760-890 Hz resonant frequency. If the LPF in the DPS filtered out the resonant frequency, we would not find the resonance.

9.1 Limitations

In this paper, the introduced adversarial control does not offer fine-grained control compared to [75, 77]. The reason behind this is that the direct feedback from the compromised NPR to the attacker is absent. Because, typically, the audio sources, such as cellphones, radios, televisions, and CCTVs, which inject malicious music, do not have pressure sensors to measure the pressure after the attack and send it back to the attacker. However, the attack is strong enough to change the negative pressure in an NPR. Moreover, close access near the pressure ports in an NPR, short-attacking range, and prior knowledge of the NPR are also the limitations of our attack model.

10 COUNTERMEASURES

The following techniques should be adopted together to prevent our attack - a wolf in sheep's clothing.

Dampening of the music: The simplest method of preventing resonance originating from the malicious music is to dampen the music. The smart way to dampen the music is to use a long sampling tube with the DPS's port. Even if the pressure port is very close to the DPS and the DPS would not require the sampling tube, we still suggest using a long sampling tube with the DPS. We find that a tube length greater than 7 m can completely dampen music having an SPL of 90 dB. The long tube can be coiled if space is limited for the mounting (see Fig. 21). However, a long sampling tube reduces the sensitivity of the DPS, resulting in a measurement error.

Enclosure around the pressure port: A box-like enclosure should enclose the pressure pickup device mounted in the pressure port (see Fig. 21). The box-like enclosure should be filled with sound damping foam to dampen the malicious music. However, this method also reduces the sensitivity of the DPS.

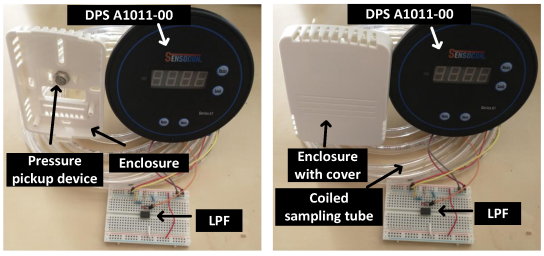

Figure 21: Different countermeasures to prevent the attack.

Filtering the resonant frequency: Though the DPSs don't use their LPFs to remove the resonant frequency, the authority of the NPR facility can ask the company, that install the RPM system or BMS, to cascade an LPF just after the DPS. The LPF must have a lower cut-off frequency, such as a frequency ~20% of the resonant frequency of a DPS (see Fig. 2). Therefore, the variability of the resonant frequency will not impact the safety of the DPS. For example, we use a first-order LPF built with an Op-Amp having a cut-off frequency of ~120 Hz with the A1011-00 DPS from Sensocon (see Fig. 21). A low cut-off frequency of an LPF will not hamper the normal operation of a DPS in an NPR as the pressure does not change in high frequency in an NPR. Another complex approach is to use a microphone to sense the music first and then filter out the music from the pressure reading using an LPF. Similar techniques are found here [47–49, 52]. Moreover, a guideline should be adopted by CDC or other authorities that NPRs should strictly use LPFs to protect from the resonance in DPSs.

Increasing the reference negative pressure: The CDC or other authorities should have a guideline to maintain a negative pressure higher than -2.5 Pa, such as at least 20 Pa. An attacker may find it difficult to turn a high negative pressure into a positive pressure through malicious music.

Removing audio sources: Any audio source should be removed from the close proximity to the DPS. Even CCTVs should be mounted at least 3 m away from the pressure ports in an NPR.

11 RELATED WORK

To the best of our knowledge, there is no work in the literature that shows an attack on an NPR facility using malicious music by exploiting the resonant frequency of a DPS. We compare our work with the state-of-the-art works in the following four categories.

Attacks on pressure Sensors: Rouf et al. [69] used unauthenticated wireless transmission to spoof a tire pressure sensor using a radio frequency (RF) channel and attacked a moving vehicle from a close distance. Tu et al. [78] showed a deliberate EMI attack on an inflation pump's pressure sensor while inflating a car tire and studied the attack impacts on the system's actuation. Yan et al. [85] did a formal analysis of semantic attacks on pressure sensors *without* mentioning how the pressure sensors can be attacked.

Attacks with acoustic signals: Wang et al. [82] used an ultrasonic gun to create resonance at membranes of different inertial sensors, such as MEMS accelerometers and gyroscopes and spoofed the inertial sensors to create havoc in the connected systems. Son et al. [72] used a high-power acoustic signal in audible range to compromise the gyroscope of a drone creating a resonance and made it uncontrollable. Trippel et al. [75], and Tu et al. [77] showed an adversarial control over MEMS accelerometers and gyroscopes using audible acoustic signals at their resonant frequencies. Yan et al. [84] showed an attack on ultrasonic sensors of a vehicle using acoustic waves to impair vehicle safety. Zhang et al. [86] injected acoustic commands into a microphone using ultrasonic carriers. Bolton et al. [50] showed an acoustic attack on hard disk drives.

Resonant frequencies in pressure sensors: The resonant frequency of a pressure sensor influences its dynamic characteristics [62] and is a critical parameter in designing a pressure sensor. Designers use this frequency to design resonant pressure sensors for dynamic applications, such as [61], [59], and [70]. We are not aware of any acoustic attack on pressure sensors exploiting resonant frequencies. However, designers design pressure sensors to acquire acoustic pressure in different applications, such as for cardiac pressure [81] and sound pressure [66].

Attacks on other sensors: Barua et al. [44–46] showed a non-invasive magnetic spoofing attack on Hall sensors of solar inverters, causing a shut down in a micro-grid. Kune et al. [64] attacked analog sensors using EMIs to cause defibrillation shocks on implantable cardiac devices. Davidson et al. [56] showed how spoofing optical sensors of an unmanned aerial vehicle (UAV) can compromise complete control of its lateral movement.

While the above works address the physical-level signal injection attacks on different sensors, our work differs from them in the following ways. **First**, our attack is the first of its kind that exploits resonant frequencies of DPSs to attack the RPM and HVAC systems in an NPR facility. **Second**, we intelligently use malicious music to attack NPRs for stealthiness (i.e., a wolf in sheep's clothing).

Last, more importantly, our attack has the potential to trigger catastrophic consequences by leaking deadly microbes from an NPR, causing losses in terms of human lives and monetary resources.

12 CONCLUSION

We present a non-invasive attack using malicious music on DPSs located in an NPR. We show that the NPRs have RPM and HVAC systems, which use DPSs to maintain a negative pressure inside an NPR with respect to the outside reference space. We find the resonant frequency of DPSs used in NPRs by proper experiments and show that the resonant frequencies are in the audible range. We also show that the resonant frequencies of DPSs vary within a band depending on other parameters, such as the length and diameter of the sampling tube. Therefore, we insert segments of the resonant frequency band in specific interval inside of music and end the inserted segments with their peak to maintain an average forged pressure in the DPS's transducer system. As a result, the attacker can use the malicious music to fool the DPSs used in the RPM and HVAC systems of an NPR and can turn the NPR's negative pressure into a positive pressure. This may cause an alarm, resulting in chaos in the facility and has a potential to leak deadly microbes from the facility. Our attack is strong, non-invasive, and stealthy, similar to a wolf in a sheep's clothing. The consequences of leaking deadly microbes from an NPR will be catastrophic in terms of losses in human lives and monetary resources. Therefore, our attack is impactful, and the countermeasures should be adopted to prevent any future attack like ours in an NPR.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments that greatly helped to improve this paper. This work was partially supported by the National Science Foundation (NSF) under award ECCS-2028269 and the University of California, Office of the President award LFR-18-548175. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding agencies.

13 APPENDIX

13.1 Types of differential pressure sensors

Capacitive DPS: It uses a diaphragm placed in between the rigid plates of a capacitor that is shown in Fig. 22. The diaphragm works as a partition between two ports - port 1 and port 2, of the DPS. If port 1 is in pressure level P_1 and port 2 is in pressure level P_2, the diaphragm changes its shape in proportion to the amount of differential pressure P_1 - P_2 applied to it. The change of shape of the diaphragm changes the capacitance of the capacitor. The change of capacitance generates a proportional voltage at the sensor output.

Piezoresistive DPS: It uses a piezoresistive strain gauge as a transducer that is connected with a diaphragm (see Fig. 23). As the diaphragm is placed in between two ports of the DPS, the diaphragm's shape changes in proportion to the differential pressure P_1 - P_2 applied on the diaphragm, causing a change in shape of the piezoresistive element connected to the diaphragm. This changes the resistance of the piezoresistive element, which is typically used as an arm of a Wheatstone bridge. Therefore, the change in resistance results in a proportional voltage change at the sensor output.

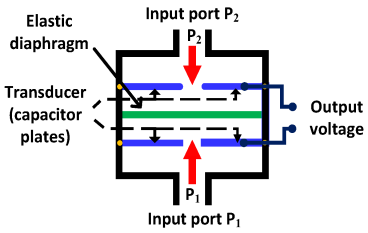

Figure 22: A capacitive transducer based DPS.

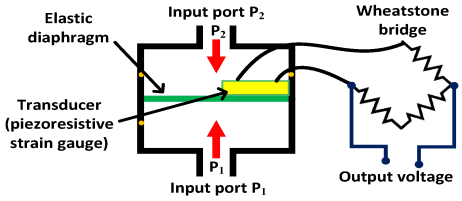

Figure 23: A piezoresistive transducer based DPS.

Thermal mass-flow DPS: It uses temperature sensors as transducers and can measure differential pressure utilizing the thermal gas-flow principle [31]. As shown in Fig. 24, it has two temperature sensors T_1 and T_2, and a small heating element is placed in the middle of the temperature sensors. The structure is etched into a passivation glass layer, which forms a thin membrane. A differential pressure across the sensor ports P_1 and P_2 induces a tiny gas flow, which results a temperature difference T_1 - T_2 between the two temperature sensors. The temperature difference results in a proportional voltage change at the sensor output.

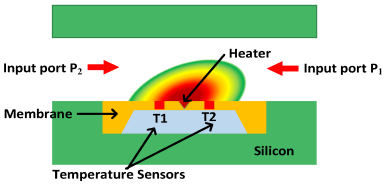

Figure 24: A thermal mass-flow based DPS.

13.2 Signal conditioning circuit

Fig. 25 shows an instrumentation amplifier to collect data from a DPS with the part# NSCSSNN015PDUNV.

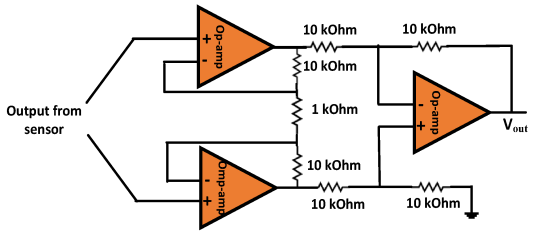

Figure 25: Instrumentation amplifier.

REFERENCES

[1] 2003. Guidelines for Environmental Infection Control in Health-Care Facilities. (2003). https://www.cdc.gov/infectioncontrol/guidelines/environmental/background/air.html. (Accessed: 05-01-2022).

[2] 2003. Institute of Occupational Safety and Health (Taiwan). Recommended Guidelines for Inspection of Isolation Wards for SARS Patients. (2003). https://www.ilosh.gov.tw/1261/1274/1276/8875/?cprint=pt. (Accessed: 05-01-2022).

[3] 2006. American Institute of Architects Guidelines for the Construction of Hospitals and Health Care Facilities. Washington: The Institute. (2006). https://fgiguidelines.org/wp-content/uploads/2015/08/2001guidelines.pdf. (Accessed: 05-01-2022).

[4] 2006. The Feynman Lectures on Physics Vol. I Ch. 47: Sound. The wave equation. (2006). https://www.feynmanlectures.caltech.edu/I_47.html. (Accessed: 05-01-2022).

[5] 2007. Guidelines for the classification and design of isolation rooms in health care facilities, Victorian Advisory Committee on Infection Control. (2007). https://galihendradita.files.wordpress.com/2019/11/australia_isolation_rooms_2007.pdf. (Accessed: 05-01-2022).

[6] 2016. Sound Waves | University Physics Volume 1. (2016). https://courses.lumenlearning.com/suny-osuniversityphysics/chapter/17-1-sound-waves/. (Accessed: 05-01-2022).

[7] 2020. Model SRPMRoom Pressure Monitor. (2020). https://www.setra.com/hubfs/Product_Data_Sheets/Setra_Model_SRPM_Data_Sheet.pdf?t=1516657591048&hsLang=en. (Accessed: 05-01-2022).

[8] 2020. One Vue Sense. (2020). https://www.primexinc.com/en/assets?download=Primex_OneVUE-DiffPressure.pdf. (Accessed: 05-01-2022).

[9] 2020. Room Pressure Monitor. (2020). https://sid.siemens.com/v/u/A6V10322677. (Accessed: 05-01-2022).

[10] 2020. ROOM STATUS MONITOR. (2020). https://www.dwyer-inst.com/PDF_files/RSME.pdf. (Accessed: 05-01-2022).

[11] 2020. Sensocon Series A1. (2020). https://www.sensocon.com/uploads/Files/Install16/A1-Digital-Differential-Pressure-Gauge-IOM.pdf. (Accessed: 05-01-2022).

[12] 2020. Series RSM Rom Status Monitor. (2020). https://www.dwyer-inst.com/PDF_files/P_3_RSM.pdf. (Accessed: 05-01-2022).

[13] 2021. Wuhan lab leak theory: How Fort Detrick became a centre for Chinese conspiracies. (2021). https://www.bbc.com/news/world-us-canada-58273322. (Accessed: 05-01-2022).

[14] 2022. Basic Board Mount Pressure Sensors. (2022). https://www.mouser.com/datasheet/2/187/honeywell_sensing_board_mount_pressure_tbp_nbp_ser-1837963.pdf. (Accessed: 05-01-2022).

[15] 2022. BOSS Audio Systems R1002 Car Amplifier - 2 Channel, 200 Watts Max Power, 2 4 Ohm Stable, Class AB, Full Range. (2022). https://www.amazon.com/BOSS-Audio-R1002-Car-Amplifier/dp/B004S50ZB2/ref=sr_1_2?dchild=1&keywords=200+watt+audio+amplifier&qid=1588804890&sr=8-2. (Accessed: 05-01-2022).

[16] 2022. Clear Vinyl Tubing. (2022). https://www.homedepot.com/p/UDP-3-16-in-I-D-x-5-16-in-O-D-x-20-ft-Clear-Vinyl-Tubing-T10007004/304185167. (Accessed: 05-01-2022).

[17] 2022. Data SheetP1KPressure Sensor. (2022). https://datasheet.octopart.com/P1K-2-2X16PA-Kavlico-datasheet-81473203.pdf. (Accessed: 05-01-2022).

[18] 2022. EK-P5: Differential pressure evaluation kit SDP8xx series. (2022). https://sensirion.com/products/catalog/EK-P5/. (Accessed: 05-01-2022).

[19] 2022. Goldwood Sound Inc. Sound Module. (2022). https://www.amazon.com/Goldwood-Sound-Inc-GT-300PB-1188-2/dp/B071R82KPS. (Accessed: 05-01-2022).

[20] 2022. GT-1188 Tweeter Drivers Replacements for KSN1188A. (2022). https://www.amazon.com/Goldwood-Sound-Inc-GT-300PB-1188-2/dp/B071R82KPS. (Accessed: 05-01-2022).

[21] 2022. Guardian Space Pressure Monitor. (2022). https://paragoncontrols.com/wp-content/uploads/2021/07/SPM-1000-IOM.pdf. (Accessed: 05-01-2022).

[22] 2022. Improving Differential Pressure Diaphragm Seal System Performance and Installed Cost. (2022). https://www.emerson.com/documents/automation/white-paper-improving-differential-pressure-diaphragm-seal-system-performance-installed-cost-rosemount-en-76672.pdf. (Accessed: 05-01-2022).

[23] 2022. Integrated Silicon Pressure sensor On-Chip Signal Conditioned, Temperature Compensated and Calibrated. (2022). https://media.digikey.com/pdf/Data%20Sheets/Freescale%20Semi/MPVZ5004G.pdf. (Accessed: 05-01-2022).

[24] 2022. Introduction to Dynamic Pressure Sensors. (2022). https://www.pcb.com/resources/technical-information/introduction-to-pressure-sensors. (Accessed: 05-01-2022).

[25] 2022. Keysight / Agilent 33120A Function / Arbitrary Waveform Generator, 15 MHz. (2022). https://www.keysight.com/us/en/product/33120A/function--arbitrary-waveform-generator-15-mhz.html. (Accessed: 05-01-2022).

[26] 2022. P993 Low Range Differential Pressure PCB Mount Sensor. (2022). https://www.sensata.com/sites/default/files/a/sensata-p993%20series-differential%20pressure%20mount%20sensor-datasheet.pdf. (Accessed: 05-01-2022).

[27] 2022. Piezoelectric Tweeter HornToToT. (2022). https://www.amazon.com/ToToT-Ultrasonic-Speaker-Loudspeaker-Piezoelectric/dp/B07RW7ZNB4/ref=sr_1_3?dchild=1&keywords=ultrasonic+speaker&qid=1588806704&sr=8-3. (Accessed: 05-01-2022).

[28] 2022. Pressure Sensing 101 – Absolute, Gauge, Differential & Sealed pressure. (2022). https://esenssys.com/differences-between-pressure-sensors/. (Accessed: 05-01-2022).

[29] 2022. Samusng Galaxy S10. (2022). https://www.samsung.com/global/galaxy/galaxy-s10//. (Accessed: 05-01-2022).

[30] 2022. The SDP800 Series. (2022). https://sensirion.com/media/documents/099567E0/6166D20B/Sensirion_Differential_Pressure_Sensors_Chart_SDP800Series.pdf. (Accessed: 05-01-2022).

[31] 2022. SDP831-500Pa - Digital DP sensor. (2022). https://sensirion.com/products/catalog/SDP831-500Pa/. (Accessed: 05-01-2022).

[32] 2022. SERIES A1 Digital Differential Pressure Gauge. (2022). https://www.sensocon.com/uploads/Files/English/Sensocon-Series-A1-Digital-Differential-Pressure-Gauge-Datasheet.pdf. (Accessed: 05-01-2022).

[33] 2022. Sound Meter. (2022). https://play.google.com/store/apps/details?id=kr.sira.sound&hl=en. (Accessed: 05-01-2022).

[34] 2022. Static pressure pickup. (2022). https://www.dwyer-inst.com/Product/Pressure/RoomStatusMonitors/SeriesRSME#accessories. (Accessed: 05-01-2022).

[35] 2022. Theory of Second-Order Systems. (2022). https://www.uml.edu/docs/Second-Theory_tcm18-190098.pdf. (Accessed: 05-01-2022).

[36] 2022. TruStability® Board Mount Pressure Sensors. (2022). https://www.mouser.com/datasheet/2/187/honeywell-sensing-trustability-board-mount-pressur-1228675.pdf. (Accessed: 05-01-2022).

[37] 2022. Ultrasonic Signal Generator Module. (2022). https://www.kemo-electronic.de/en/Car/Modules/M048N-Ultrasonic-Generator.php. (Accessed: 05-01-2022).

[38] 2022. Which Loudspeakers are Loudest? (2022). https://www.razmobility.com/assistive-technology-blog/which-loudspeakers-are-loudest/. (Accessed: 05-01-2022).

[39] Avnet Abacus. 2021. Pressure sensors: The design engineers guide. *Avnet Reach Further* (2021).

[40] J.R. Appelbaum, L. Poitras, M. Rosenbach, C. Stöcker, J. Schindler, and H. Stark. 2013. Inside TAO : documents reveal top NSA hacking unit. *Der Spiegel* (29 12 2013).

[41] Ivan Bajsić, Jože Kutin, and Tomaž Žagar. 2007. Response time of a pressure measurement system with a connecting tube. *Instrumentation Science and Technology* 35, 4 (2007), 399–409.

[42] John G. Bartlett. 2012. 20 - Bioterrorism. In *Goldman's Cecil Medicine (Twenty Fourth Edition)* (twenty fourth edition ed.), Lee Goldman and Andrew I. Schafer (Eds.). W.B. Saunders, Philadelphia, 84–88. https://doi.org/10.1016/B978-1-4377-1604-7.00020-8

[43] Judene M Bartley, Russell N Olmsted, and Janet Haas. 2010. Current views of health care design and construction: Practical implications for safer, cleaner environments. *American Journal of Infection Control* 38, 5 (2010), S1–S12.

[44] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2020. Hall Spoofing: A {Non-Invasive}{DoS} Attack on {Grid-Tied} Solar Inverter. In *29th USENIX Security Symposium (USENIX Security 20)*. 1273–1290.

[45] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2020. Special session: Noninvasive sensor-spoofing attacks on embedded and cyber-physical systems. In *2020 IEEE 38th International Conference on Computer Design (ICCD)*. IEEE, 45–48.

[46] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2021. The Hall Sensor Security. (2021).

[47] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2022. HALC: A Real-time In-sensor Defense against the Magnetic Spoofing Attack on Hall Sensors. In *25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022)*.

[48] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2022. PreMSat: Preventing Magnetic Saturation Attack on Hall Sensors. In *International Conference on Cryptographic Hardware and Embedded Systems (TCHES 2022)*.

[49] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2022. Sensor Security: Current Progress, Research Challenges, and Future Roadmap (Invited Paper). In *International Conference on Computer-Aided Design (ICCAD 2022)*.

[50] Connor Bolton, Sara Rampazzi, Chaohao Li, Andrew Kwong, Wenyuan Xu, and Kevin Fu. 2018. Blue note: How intentional acoustic interference damages availability and integrity in hard disk drives and operating systems. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1048–1062.

[51] Sujit Rokka Chhetri et al. 2019. Tool of Spies: Leaking your IP by Altering the 3D Printer Compiler. *IEEE Transactions on Dependable and Secure Computing* (2019).

[52] Sujit Rokka Chhetri, Jiang Wan, and Mohammad Abdullah Al Faruque. 2017. Cross-domain security of cyber-physical systems. In *2017 22nd Asia and South Pacific design automation conference (ASP-DAC)*. IEEE, 200–205.

[53] Raymond YW Chinn and Lynne Sehulster. 2003. Guidelines for environmental infection control in health-care facilities; recommendations of CDC and Healthcare Infection Control Practices Advisory Committee (HICPAC). (2003).

[54] Stanley Corrsin. 1947. Extended Applications of the Hot-Wire Anemometer. *Review of Scientific Instruments* 18, 7 (1947), 469–471.

[55] Robert E Curry and Glenn B Gilyard. 1990. Experimental Characterization of the Effects of Pneumatic Tubing on Unsteady Pressure Measurements. *NASA Technical Memorandum* 41 (1990), 71.

[56] Drew Davidson, Hao Wu, Rob Jellinek, Vikas Singh, and Thomas Ristenpart. 2016. Controlling {UAVs} with Sensor Input Spoofing Attacks. In *10th USENIX workshop on offensive technologies (WOOT 16)*.

[57] Finn and Inc. Conway. 2020. Room Pressure Monitors and Environmental Monitors. (2020). https://finnandconway.com/news/18694/setra-critical-room-pressure-monitors. (Accessed: 05-01-2022).

[58] Anna Goldenberg, Galit Shmueli, Richard A Caruana, and Stephen E Fienberg. 2002. Early statistical detection of anthrax outbreaks by tracking over-the-counter medication sales. *Proceedings of the National Academy of Sciences* 99, 8 (2002), 5237–5240.

[59] JC Greenwood and DW Satchell. 1988. Miniature silicon resonant pressure sensor. In *IEE Proceedings D (Control Theory and Applications)*, Vol. 135. IET, 369–372.

[60] David Halliday, Robert Resnick, and Jearl Walker. 2013. *Fundamentals of physics*. John Wiley & Sons.

[61] Xiangguang Han, Qi Mao, Libo Zhao, Xuejiao Li, Li Wang, Ping Yang, Dejiang Lu, Yonglu Wang, Xin Yan, Songli Wang, et al. 2020. Novel resonant pressure sensor based on piezoresistive detection and symmetrical in-plane mode vibration. *Microsystems & nanoengineering* 6, 1 (2020), 1–11.

[62] Jan Hjelmgren. 2002. Dynamic measurement of pressure.-A literature survey. (2002).

[63] Paul A Jensen, Lauren A Lambert, Michael F Iademarco, and Renee Ridzon. 2005. Guidelines for preventing the transmission of Mycobacterium tuberculosis in health-care settings, 2005. (2005).

[64] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. 2013. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy*. IEEE, 145–159.

[65] Shelly L Miller, Nicholas Clements, Steven A Elliott, Shobha S Subhash, Aaron Eagan, and Lewis J Radonovich. 2017. Implementing a negative-pressure isolation ward for a surge in airborne infectious patients. *American journal of infection control* 45, 6 (2017), 652–659.

[66] A Nagiub, Elias Soupos, and Hassan Nagib. 1999. Characterization of a MEMS acoustic/pressure sensor. In *37th Aerospace Sciences Meeting and Exhibit*. 520.

[67] PE Paul Ninomura and PE Richard Hermans. 2008. Ventilation standard for health care facilities. *ASHRAE Journal* 50, 10 (2008), 52–57.

[68] George F Risi, Marshall E Bloom, Nancy P Hoe, Thomas Arminio, Paul Carlson, Tamara Powers, Heinz Feldmann, and Deborah Wilson. 2010. Preparing a community hospital to manage work-related exposures to infectious agents in biosafety level 3 and 4 laboratories. *Emerging infectious diseases* 16, 3 (2010), 373.

[69] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. 2010. Security and Privacy Vulnerabilities of {In-Car} Wireless Networks: A Tire Pressure Monitoring System Case Study. In *19th USENIX Security Symposium (USENIX Security 10)*.

[70] Xun Shen, Yahui Zhang, and Tielong Shen. 2019. Cylinder pressure resonant frequency cyclic estimation-based knock intensity metric in combustion engines. *Applied Thermal Engineering* 158 (2019), 113756.

[71] Bill Snyder. 2014. Snowden: The NSA planted backdoors in cisco products. *InfoWorld* 15 (2014).

[72] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security Symposium (USENIX Security 15)*. 881–896.

[73] Pawel Swierczynski, Marc Fyrbiak, Philipp Koppe, Amir Moradi, and Christof Paar. 2017. Interdiction in practice—Hardware Trojan against a high-security USB flash drive. *Journal of Cryptographic Engineering* 7, 3 (2017), 199–211.

[74] Lisa Ta, Laura Gosa, and David A Nathanson. 2019. Biosafety and biohazards: understanding biosafety levels and meeting safety requirements of a biobank. *Biobanking* (2019), 213–225.

[75] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In *2017 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 3–18.

[76] Ying-Huang Tsai, Gwo-Hwa Wan, Yao-Kuang Wu, and Kuo-Chien Tsao. 2006. Airborne severe acute respiratory syndrome coronavirus concentrations in a negative-pressure isolation room. *Infection Control & Hospital Epidemiology* 27, 5 (2006), 523–525.

[77] Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. 2018. Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors. In *27th USENIX Security Symposium (USENIX Security 18)*. 1545–1562.

[78] Yazhou Tu, Vijay Srinivas Tida, Zhongqi Pan, and Xiali Hei. 2021. Transduction Shield: A Low-Complexity Method to Detect and Correct the Effects of EMI Injection Attacks on Sensors. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*. 901–915.

[79] Chris P Underwood. 2002. *HVAC control systems: Modelling, analysis and design*. Routledge.

[80] Lonneke Van der Velden. 2015. Leaky apps and data shots: Technologies of leakage and insertion in NSA-surveillance. *Surveillance & Society* 13, 2 (2015), 182–196.

[81] Tian Wang, Meihui Gong, Xiaoyu Yu, Guangdong Lan, and Yunbo Shi. 2021. Acoustic-pressure sensor array system for cardiac-sound acquisition. *Biomedical Signal Processing and Control* 69 (2021), 102836.

[82] Zhengbo Wang, Kang Wang, Bo Yang, Shangyuan Li, and Aimin Pan. 2017. Sonic gun to smart devices: Your devices lose control under ultrasound/sound. *BlackHat USA* (2017).

[83] MB Wilkinson and M Outram. 2009. Principles of pressure transducers, resonance, damping and frequency response. *Anaesthesia & Intensive Care Medicine* 10, 2 (2009), 102–105.

[84] Chen Yan, Wenyuan Xu, and Jianhao Liu. 2016. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def Con* 24, 8 (2016), 109.

[85] Renchi Yan, Teng Xu, and Miodrag Potkonjak. 2014. Semantic attacks on wireless medical devices. In *SENSORS, 2014 IEEE*. 482–485. https://doi.org/10.1109/ICSENS.2014.6985040

[86] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. 2017. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 103–117.