2020 Symposium on Security and Privacy Workshops (SPW)

On the Feasibility of Acoustic Attacks Using Commodity Smart Devices

Matt Wixey, Emiliano De Cristofaro, and Shane D Johnson
University College London
matthew.wixey.17@ucl.ac.uk, e.decristofaro@ucl.ac.uk, shane.johnson@ucl.ac.uk

***Abstract*—Sound at frequencies above (ultrasonic) or below (infrasonic) the range of human hearing can, in some settings, cause adverse physiological and psychological effects to individuals. We investigate the feasibility of cyber-attacks that could make smart consumer devices produce possibly imperceptible sound at both high (17–21kHz) and low (60–100Hz) frequencies, at the maximum available volume setting, potentially turning them into acoustic cyber-weapons. To do so, we deploy attacks targeting different smart devices and take sound measurements in an anechoic chamber. For comparison, we also test possible attacks on traditional devices. Overall, we find that some of the devices tested are capable of reproducing frequencies within both high and low ranges, at levels exceeding those recommended in published guidelines. Generally speaking, such attacks are often trivial to develop and in many cases could be added to existing malware payloads, as they may be attractive to adversaries with specific motivations or targets. Finally, we suggest a number of countermeasures for detection and prevention.**

***Keywords*-acoustic weapons, malware, cyber-attacks**

I. INTRODUCTION

Concerns about the potential for malware to harm citizens by compromising smart consumer devices have become increasingly prevalent [59], [12]. However, little attention has been paid to the ability to *directly* cause material harm to users of compromised systems.

In this paper, we focus on malware that may have direct *psychological* and/or *physical* impacts on the users of hosts under attack. In particular, we set out to study the feasibility of attacks developed to control consumer devices and make them reproduce *sound* that is likely to be *imperceptible* to a significant proportion of the population at both high (17kHz–21kHz) and low (60Hz–100Hz) frequencies, but also possibly damaging to them. If such noise is emitted at sufficient levels, and for sufficient periods of time, a number of short-term and long-term adverse physical and psychological effects may occur (see Section II for a primer on high- and low-frequency noise and their adverse affects).

We rely on an experimental methodology to design and deploy a range of attacks on a variety of devices and take sound measurements in an anechoic chamber in order to assess the capabilities of a sample of consumer equipment both in terms of the frequencies and sound levels achievable. We first report on a few *smart* devices, whereby smart here denotes devices with a remote or local network interface, including Internet-connected speakers and headphones. For comparison, we also run attacks against more "traditional" devices, which rely on intended control channels like Bluetooth, or on physical access to the device in question. All the devices we experiment with are publicly available, relatively modern and inexpensive, and commonly purchased in both home and business contexts.

Overall, we show that we can indeed re-purpose some devices for local or remote acoustic attacks by an attacker with the objective of causing direct harm to humans.

Of the eight device set-ups tested, four (two smart, two traditional) were capable of emitting high-frequency noise (HFN) and/or low-frequency noise (LFN), at levels which exceed published guidelines relating to the maximum recommended levels. More specifically, a smart speaker and a headphones set did that for both HFN and LFN; a parametric speaker for HFN only; and a loudspeaker for LFN only. To the best of our knowledge, ours is the first attempt to demonstrate the feasibility of extending malware and cyber-attacks into the field of acoustic weapons. For safety reasons, we do not provide full details of these devices but can do so upon request.

We also show that attacks such as these can have unintended but significant effects on the physical equipment itself; we were able to cause permanent damage to the smart speaker by playing a particular frequency for a few minutes at maximum volume. This was disclosed to the manufacturer, who subsequently notified us that a mitigation would be applied to address this issue. Finally, we discuss a number of possible countermeasures.

II. BACKGROUND

HFN and LFN. Frequencies believed to be above or below the range of human hearing are often defined as *ultrasonic* or *infrasonic*, respectively. More specifically, the former encompass higher frequencies, usually 20kHz and higher [30], while the latter are in the range 0–20Hz [37]. However, as highlighted by Duck and Leighton [17], founding a definition on a lack of a property (namely, non-audibility) is problematic, particularly with a concept that is highly subjective. In this paper, we focus on High-Frequency Noise (HFN) in the 17kHz–21kHz range, due to the reported capacity of some consumer devices, such as mobile phones, to produce noise at approximately these frequencies [19], [35], as well as Low-Frequency Noise (LFN), typically described as 20–200Hz [8]. However, for the latter, we restrict testing to the 60–100Hz range, following the results of a pilot study, presented in IV-A, which indicated that available devices would not be capable of reproducing lower frequencies.

Hearing Thresholds. A common misconception is that

DOI 10.1109/SPW50608.2020.00031

healthy humans are unable to perceive noise above a 20kHz threshold or below 20Hz [18]. However, perceptibility does not solely depend on theoretically defined cut-off points. In fact, the mechanisms of perception of both low and high frequencies are complex and not fully understood [33], and, there is a significant amount of variation in the ability of people to detect HFN and LFN [35], [37]. For instance, some individuals have reportedly been able to hear frequencies above 17.8kHz [17] or higher [16], [33], [47], or down to 1.5Hz in certain conditions [36]. To a large extent, this depends on a number of factors, including the sound pressure level (SPL), and levels of background noise, etc. Additionally, lower frequencies may be perceived, but not necessarily as "sound" [37], and the generation of high frequencies may cause subharmonics in the audible range [30], [17]. However, there is a general consensus that the likelihood that people can hear sounds declines non-linearly with increasingly higher [4] and lower frequencies [44] and that, for the former, hearing thresholds generally increase with age [38]. Put simply, it is likely that many people, particularly older adults, cannot hear sound at the ranges we test in this paper.

Adverse Effects of HFN/LFN. HFN and LFN have both been associated with adverse physiological and psychological effects. However, as with perceptibility, susceptibility is again likely to differ significantly between individuals [34], [51]. While there have been no reports of high frequencies causing permanent hearing loss [30], there have been numerous reported cases of ultrasound having adverse effects on hearing [17], including temporary threshold shifts [1]; reductions in hearing sensitivity in the audible range [38], [13], [68], [23]; neurasthenia, cardiac neurosis, hypotension, bradycardia, and functional changes in cardiovascular and central nervous systems [56]. Permanent threshold shifts have only been associated with high frequency exposure in the presence of high levels of lower frequencies [35]. High frequencies have also been linked to more subjective effects, including nausea, fatigue, and headaches [17], [65], [30]; tinnitus and ear pain [13], [20]; irritation [60]; somnolence, dizziness, palpitations, and decreased concentration [56].

Although LFN has been associated with temporary threshold shifts [37], and some correlation observed with various conditions such as heart ailments, chronic insomnia [40], and elevated levels of cortisol [8], annoyance is often the most common response [57], [48]. Other subjective effects include headaches and palpitations [42]; deterioration in task performance [9], [8]; decreased productivity [31]; and lower levels of cooperation and agreeableness [66]. These subjective effects are often reported even at relatively moderate levels of between 40 and 45 dB(A) [8], [66], [48], [49], with noise sensitivity reported to be a consistent predictor of depressive symptoms and psychological distress [57].

Remarks. It is crucial to highlight that there are often issues with definitively establishing a causal relationship between HFN and LFN and adverse effects. Data is often sparse and anecdotal [35], and detailed knowledge of the "noise dose" – including both the level and the duration of the exposure – is required in order to evaluate effects [16]. In fact, many effects have not been successfully reproduced in laboratory settings [21], although this may be in part due to ethical restrictions on exposing human subjects to potentially dangerous SPLs [35], [20], or to the possibility of nocebo effects [21]. However, as pointed out by Leighton [35], while it is not possible to make definitive statements about causality, there exists a significant evidence base for the threat of adverse effects at lower intensities in a subset of the population. Moreover, these threats are sufficiently evidenced that a number of organizations and researchers have developed guidelines detailing recommended maximum permissible exposure levels for both HFN and LFN.

Table I: Mean and median of maximum permissible sound pressure levels (MPSPLs), for different frequencies, as per [34].

(kHz)	8	10	12.5	16	20	25	31.5	40	50
Mean	80.00	83.08	82.67	83.89	96.91	111.08	113.91	114.09	115.28
Median	80.00	80.00	80.00	80.00	105.00	110.00	110.00	110.00	110.00

Exposure Guidelines. There are often significant differences in the way these levels are calculated and implemented, and in the proposed recommendations for comparison and evaluation against them. In this paper, we will not assess the merits, or lack thereof, of individual guidelines, but will instead use them to compare our generated levels.

Leighton [34] presents a compendium of maximum permissible sound pressure levels (MPSPLs), the means and medians of which are reported in Table I. As noted in Leighton's follow-up work [35], many of these guidelines are based on small samples, often only including adult males and predominantly focusing on occupational environments rather than public exposure. Although the research base may be too small to support such guidelines [34], there is, at least, something of a consensus [30], particularly for the fact that A-weighting – commonly used for exposure guidelines in the audible range – is limited, as it significantly underestimates higher frequencies [35]. Our measurements are thus taken using Z-weighting – a flat frequency response 10Hz–20kHz, which, unlike A-weighting, does not apply any attenuation for sounds above or below the commonly understood "audible range." In Section V, we will compare to the various guidelines using this weighting, with notation $\mathrm{LZ}_{\mathrm{eq}}$.

We are unaware of any similar compendium relating to safety guidelines regarding exposure to LFN. However, several bodies have published reference curves for the assessment of *disturbance* caused by LFN. For our analysis, we use a reference curve proposed in 2011 [43], reported in Table II, which was devised after an assessment of previously published reference curves. This reference curve proposes the use of L_{eq}. Since no weighting is applied, we measure and compare our results using $\mathrm{LA}_{\mathrm{eq}}$ in third-octave bands (TOBs). There is a general consensus that A-weighting may underestimate the effects of LFN [37], [62] due to its attenuation at lower frequencies, so this

Table II: Reference curve by Moorhouse et al. [43] for assessing LFN. Levels shown as L_{eq} in centered third-octave bands (TOBs).

(Hz)	10	12.5	16	20	25	31.5	40	50	63	80	100	125	160
	92	87	83	74	64	56	49	43	42	40	38	36	34

should be taken into account when reviewing our results in Section V.

III. RELATED WORK

High-Frequency Noise (HFN). Previous work has studied HFN in the context of enabling or supplementing attacks. More specifically, researchers have used ultrasound to create covert communication channels [27], [69], [15], finding that many consumer devices are capable of emitting HFN [35], [19]. Other research involving HFN includes the disruption of obstacle-detection systems by introducing attacker-controlled ultrasound to perform echolocation jamming [71], [69]. Also, Bolton et al. [10] explore the capability of both audible and inaudible noise to corrupt data being written to hard disk drives, while Mavroudis et al. [39] first and Cunche et al. [14] later investigate the use of ultrasonic beacons as tracking devices in the context of targeted marketing, exploring related privacy implications. Finally, we are not aware of any security-related research into the use of low frequencies.

Physical Harm. Researchers have examined the ways in which malware could be used to cause physical harm in a number of contexts, e.g., embedded medical devices [26], [67], [55]. Depending on the specific device and context, an attacker can cause significant, life-threatening harm by exploiting vulnerabilities in such systems. Other research in a similar vein has explored the physical risks posed by vulnerabilities in transport systems, such as connected cars [7] or air traffic control systems [11], as well as the manipulation of IoT devices to force them to strike humans [52].

Overall, there has been little research on the ability of attackers to *directly* harm users through malware and other attacks, i.e., by manipulating the ordinary outputs of devices to cause adverse effects. One exception appears to be work on the inducement of epileptic seizures. Poulsen [50] reports on a series of attacks against a forum for epilepsy sufferers: attackers uploaded flashing images, successfully causing a number of seizures in forum users. Oluwafemi et al. [46] and Ronen and Shamir [54] also discuss vulnerabilities in connected lighting devices, finding that an attacker can cause vulnerable systems to flash in patterns consistent with those known to induce seizures. To the best of our knowledge, our work is the first to examine the feasibility of acoustic attacks using malware or cyber-attacks.

Acoustic Weapons. Perhaps as a result of a substantial, albeit often anecdotal, evidence base, there has been significant historical interest in the development of devices that could be used to deliberately expose people to harmful levels of sound, and it it is generally agreed that, in principle, acoustic weapons could be used to covertly generate adverse effects in humans [35], [3]. However, this topic has been the subject of frequent misunderstandings, controversy, and rumors [63], [44]. For example, in late 2016, staff at the US embassy in Cuba reported health problems including tinnitus and cognitive difficulties, and some researchers, as well as many media outlets, speculated that these may have been caused by acoustic attacks [58]. However, others have disputed these claims, suggesting the cause may have been mass psychogenic illness [5] or microwave radiation [22], and that a recording of sound linked to the attack may be a calling song of an insect [58] or unintentional intermodulation distortion [70]. Whilst the exact cause is unknown, there is a consensus that acoustic weapons are an unlikely candidate, primarily due to their impracticality [5]. Practicality is often cited as one of the most prominent barriers to deploying acoustic weapons, which serves in part as a motivation for our work. Altmann [2], for example, notes that threshold shifts, not being immediately felt or causing an immediate impact, would be of little interest to those deploying acoustic weapons, and that it would be challenging to cause targeted, directional effects. Bartholomew and Perez [6] agree with the latter point, arguing that the need for close proximity, the required size of the acoustic weapon, and the rapid diffusion of ultrasound, would make such weapons impractical. However, as our results suggest, the deployment of acoustic attacks in the context of cyber-attacks could to some extent negate these disadvantages. Attackers may be able to affect victims over extended periods of time, particularly as users of consumer devices are typically within fairly close proximity to them, often for long periods. Therefore, concerns over practicality with regards to size and diffusion would seem less relevant with the advent of smart devices.

Remarks. Overall, while previous work has explored the ability of cyber-attacks to cause physical or psychological harm to users, there has not yet, to the best of our knowledge, been any empirical work on the capacity of malware to create localized acoustic weapons.

IV. METHODOLOGY

We now present our methodology to assess the feasibility of acoustic attacks on commodity hardware. We do so on several commonly purchased and publicly available "smart" devices that can produce sound, namely: laptops, mobile phones, and smart speakers. We also include a pair of smart headphones in this category. (Overall, *smart* here denotes devices with a remote or local network interface, including Internet-connected speakers and headphones.) As a comparison, we also use more traditional audio equipment: parametric speakers, loudspeakers, vibration speakers, and a vehicle-mounted PA system.

A. Pilot study

In order to obtain an initial indication as to whether consumer devices were indeed capable of producing HFN and LFN, we conducted a pilot study using four of the selected devices: a laptop, mobile phone, loudspeaker, and smart speaker. The experiments were also conducted in the anechoic chamber used for our full study, using the same proof-of-concept attacks (presented in Section IV-C). As the goal was not to precisely measure audio emissions, but to simply assess whether the devices could reproduce the required frequencies, we used two publicly available Android apps, Ultrasound Detector [25] and Infrasound Detector [24], and a factory-calibrated Dayton Audio iMM-6 external microphone connected to an Android phone. This is reasonable as modern smartphones are generally considered suitable for occupational noise measurements, within the limitations of the device in question [32].

Our findings showed that, while all the devices appeared to be capable of reproducing HFN, from around 60.5dBSPL to 91.5dBSPL, only the smart speaker and loudspeaker were capable of reproducing LFN at a reasonable level (50Hz at 63.4dBSPL).

We also observed a distinct increase in temperature in the smart speaker, following the production of HFN at maximum volume. More specifically, the speaker became noticeably hot to the touch and gave off a strong odor of burnt plastic after the HFN testing runs. However, we did not observe any smoke or flame coming from the device, and assumed that the production of HFN at maximum volume had caused some form of internal damage to an electronic component.

Moreover, some time after the pilot study, we noticed that the speaker's ability to reproduce higher frequencies had been impaired.

B. Experimental Setup

Testing Environment. Our experiments were conducted in an anechoic chamber at UCL. While this was necessary in order to accurately and safely measure emitted noise, it should be noted that in a real-world environment, ambient sounds and certain types of environment may amplify or reduce the effects of LFN or HFN. Owing to the nature of the study, and the reported association between high levels of LFN/HFN and adverse effects on people, we did not use human subjects for this research; instead, we measured the sound emitted from each device as a consequence of the attacks, and assessed whether or not the resulting levels exceeded published maximum permissible levels.

Ethics. A full risk assessment was conducted prior to the experiment, and ethics approval was obtained from our institution.

Device Set-Ups. Our experiments involved: 1) a Windows laptop, 2) an Android smartphone, 3) a pair of wireless over-ear headphones, 4) a smart speaker, 5) a loudspeaker, 6) a vibration speaker, 7) a parametric speaker, and 8) a vehicle-mounted PA system. To minimize risks to the general public, we do not include details of specific brands and models, or the code for our attacks, in this submission, however, they are available upon request.

Procedure. We placed each device inside an anechoic chamber, along with a Class I sound level meter, spot-calibrated by the supplier, and placed at a distance of one meter from the device. Each device was made to play or stream a WAV audio file of a single frequency tone, generated online[1]. We initiated each tone on each device for a period of ten minutes, using a specific attack developed to test that particular device, as discussed later in Section IV-C. Following each ten-minute period, the anechoic chamber was opened and readings were taken from the sound level meter.

Frequency Measurements. Note that all but one of the frequencies being tested was below 20kHz, thus, we took measurements using Z weighting (a flat frequency response in the band 10Hz–20kHz) in these cases. For test runs involving the ultrasonic frequency (21kHz), we used a proprietary high-pass filter weighting developed by the sound level meter manufacturer, known as HPE (high-pass extended). For test runs involving LFN, our original intention was to use G-weighting, which is the ISO 7196:1995 standard for measuring infrasound in the band 1Hz–20Hz. However, the results of our pilot study indicated that many consumer devices were not capable of producing noise in this range. Therefore, we increased the frequencies being tested to 60Hz, 80Hz, and 100Hz. These still fall within most definitions of LFN and are still associated with reported adverse effects, as discussed in Section III, but are not infrasonic, and were thus suitable for Z-weighted measurements rather than G-weighting, which is designed exclusively for infrasound [33].

C. Attacks on Smart Devices

Smart Speaker. Our attack against the smart speaker relied on a (previously disclosed) vulnerability affecting a number of smart audio products; specifically, that no authentication is required between the smart speaker and the controller. As previously discussed, we do not disclose details of specific models affected for safety reasons, however, we can say that our experiments are performed on a speaker released a couple of years ago for around $200.

To execute the attack, we wrote a script which scans the current local network for smart speakers of a particular brand. If any are found, and are inactive, the script retrieves the current volume level as an integer and stores it as a variable, raises the volume to maximum, and streams a requested WAV file hosted on a web server controlled by the attacker.

Headphones. We also used wireless headphones (released approximately two years ago, costing around $400). Note that we did not attack the headphones directly, but tested the capability of the headphones to reproduce HFN and LFN using the Windows malware described below, by connecting the headphones to the laptop over Bluetooth. Whilst some of the "traditional" devices we test also use Bluetooth, headphones are reported to be increasingly attached to smart devices [61], [41] and so we include them in the "smart" category, as attacks using headphones are not reliant on attacking an intended controlled channel

---

[1] https://www.audiocheck.net

such as Bluetooth, but could be achieved by attacking a smart device to which they may be attached. Here, we placed the sound level meter approximately one centimeter from the headphone's speakers, aiming to simulate as closely as possible the effect a user would experience while wearing the device.

Windows Laptop. We developed proof-of-concept Windows malware, with WAV files corresponding to each target frequency embedded in the malware. The malware contacts a simple command-and-control server to play specified WAV files on command. Note that we experiment on a mid-range laptop released a couple of years ago, priced in the order of $1,000.

Android Phone. We also developed a proof-of-concept Android app to simulate a malware-infected phone, with WAV files corresponding to each target frequency embedded in the malware. This app has the same functionality as that described for the Windows laptop malware. Again, we used a mid-range phone released about two years ago, priced at around $200.

D. Attacks on Traditional Devices

Vibration Speaker and Loudspeaker. Due to the lack of a diaphragm, vibration speakers typically have a smaller profile and can be attached to a variety of surfaces unobtrusively, possibly making them an attractive choice as repurposed acoustic weapons – either through an attacker executing an attack against another user's device, or purchasing and using their own. The vibration speaker we used was controlled through Bluetooth, as was the loudspeaker. For both of these devices, we paired the speaker to the Android phone and used our Android malware to play the targeted tones through these speakers. The loudspeaker model is about two years old and costs around $50, while the vibration speaker model is five years old and cost around $70.

Parametric Speaker. Parametric speakers use ultrasonic carrier waves, typically at 40kHz, to transmit high-intensity directional audio in a relatively small area of focus, essentially creating a "beam" of sound.

Note that the speaker we used has no smart capabilities and no remote or local command channels; instead, a standard 3.5mm audio cable is used to connect the speaker to an audio source. For our tests, we connected this speaker to our Windows laptop and used the Windows malware to play the targeted tones through the speaker. As this speaker is known to use 40kHz carrier waves, we also measured its emissions at this frequency using the HPE filter. This device is roughly the size of a mobile phone, and available for purchase online at a moderate cost, around $250, therefore, it could be used as a low-cost portable acoustic weapon by an attacker – particularly as the directional nature of the transmitted audio may allow them to target a specific location.

PA System. Finally, we used a vehicle-mounted PA system, which, like the parametric speaker, has no network interfaces. It automatically plays audio upon inserting a storage device, e.g., a USB drive or a SD card. For each test, we placed an audio file on a USB drive that was plugged into the device. As with the parametric speaker, the attacker could purchase a similar device with the intention of using it as a 'mobile' acoustic weapon when mounted on a vehicle.

Additional attacks. We devised two more possible attacks in addition to those described in Sections IV-C and IV-D, which, rather than targeting specific devices, would be suitable for deployment generally. However, as these would have utilized the same audio components being tested, and since they rely on targeted users having their volume set high enough to cause harm, we did not include them in our testing plan. Nevertheless, they might remain plausible attack scenarios, thus, we briefly discuss them here. The first additional attack relies on the HTML5 audio tag; specifically, the autoplay attribute. In this instance, an attacker would need to persuade a victim to visit a particular attacker-controlled server, and a selected tone hosted on the attacker's server would autoplay at whatever volume is currently set, without the user's knowledge—even though, depending on the browser being used, a small speaker icon might appear on the relevant tab. As it is not possible for code on a webpage to manipulate a user's system volume, the efficacy of this attack, in terms of causing harmful levels of audio, depends on the volume set on the user's device.

Another attack involves the deliberate manipulation and insertion of particular audio into a pre-existing audio track. Here the attacker may have access to a legitimate audio file that they know an intended victim will play at some point. This could be, for instance, a YouTube video, a film soundtrack, or some other audio. Using an audio editor, the attacker could decrease the level of the legitimate audio, and insert an ultrasonic or low-frequency tone of their choosing at a much higher level. Upon playing the manipulated file, the user is likely to assume that they do not have their system volume turned up high enough, or that the legitimate audio was not recorded at sufficient levels, and as a result may significantly increase their system volume – leading to exposure to potentially harmful levels of the attacker-selected tone. As with the previous attack, this approach would require the system volume of the device in question to be high enough to emit harmful levels of audio.

Remarks. Overall, our attacks are realistically viable in the wild. In addition to many of the smart devices we tested being ubiquitous in a number of diverse environments, including homes, businesses, and public or social events, many of the attack vectors are "generic." For instance, there are multiple ways to deploy malware infections on a laptop or mobile phone, and other devices, such as the headphones, could be used for attacks arising from a number of vectors.

We also experiment with a number of traditional devices. These attacks are perhaps less realistic, lacking vulnerable control channels and connectivity and typically requiring either physical access or close proximity. We

Table III: Levels observed during our HFN trials. Levels (LZ_{eq} in centered TOBs) which exceed the mean and/or median average of MPSPLs in Leighton [34]'s guidelines are in bold.

	17kHz	19kHz	21kHz(HPE)	40kHz
Smart speaker	**86**	35.2	43.8	-
Headphones	**87.5**	81.2	79.8	-
Laptop	63	64.5	45.5	-
Mobile phone	59.4	58.3	16.9	-
Loudspeaker	59.4	48.5	54.5	-
Vehicle PA	75.3	20.5	18.5	-
Vibration speaker	47.7	36.1	27.3	-
Parametric speaker	**85.1**	84.2	**97.1**	**117.7**

Table IV: Levels observed during our LFN trials. Levels (LA_{eq} in centered TOBs) over the reference curve values are in bold.

	60Hz	80Hz	100Hz
Smart speaker	**47.5**	**59**	**71.6**
Headphones	37.5	39.9	**40.2**
Laptop	2	0.1	3
Mobile phone	1	1.2	6.5
Loudspeaker	38.2	**51**	**64.2**
Vehicle PA	13.7	22.6	33.7
Vibration speaker	24	21.1	18.4
Parametric speaker	-0.6	0.5	28.6

include them in our testing both as a comparison to the tested smart devices, and to investigate whether the abuse of more traditional consumer equipment may also be an attractive avenue for attackers.

V. EXPERIMENTAL EVALUATION

Overview. Overall, we find that several devices (two smart, one traditional) were capable of producing HFN at levels exceeding the recommended exposure limits. Additionally, a number of devices (two smart, one traditional) were capable of producing levels at or above LFN limits.

High Frequency Noise. As discussed in Section II, we used the compendium of MPSPLs for airborne ultrasound in Leighton [34] to assess the capability of the devices to reproduce HFN. Results are reported in Table III, which show several results exceeding the mean average of these MPSPLs at relevant frequencies.

Note that the smart speaker produced a high of 86dB (all results LZ_{eq}) at 17kHz, but subsequent HFN trials produced much lower levels. This is due to the result of internal damage caused to the speaker during the experiment, which we discuss later in this section.

Low Frequency Noise. LFN tests generally produced lower levels than the HFN tests. However, as many researchers report [8], [66], [48], adverse psychological effects associated with low frequency sound are often observed at relatively moderate levels. To compare our results to the LFN reference curve [43], we apply A-weighting to the levels observed at TOB center frequencies, as shown in Table IV. It should be noted that A-weighting results in significant attenuation at lower frequencies, down to -26.2dB in the 63Hz centered TOB (the lowest band used in our analysis), and as much as -85.4dB at 6.3Hz. As a result, the A-weighted levels are significantly lower than our Z-weighted measurements.

Table V: Highest components outside our tested ranges, observed during LFN and HFN trials, between 125Hz and 12500Hz TOB centers. Levels shown in LZ_{eq}.

	TOB Center (Hz)	Level
Smart speaker (60Hz)	200	64.2
Smart speaker (80Hz)	160	72.5
Smart speaker (100Hz)	200	73.5
Smart speaker (17kHz)	6,300	75.1
Headphones 100Hz	125	39.5
Headphones (17kHz)	12,500	44.2
Headphones (19kHz)	1,000	23.6
Headphones (21kHz)	1,250	23.9
Loudspeaker (80Hz)	250	65.6
Loudspeaker (100Hz)	500	69.0
Vehicle PA (17kHz)	1,600	60.8
Parametric speaker (17kHz)	12,500	74.3
Parametric speaker (19kHz)	12,500	71.2
Parametric speaker (21kHz)	12,500	69.4
Parametric speaker (40kHz)	12,500	75.2

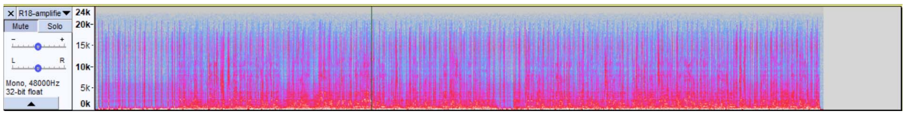
Audible components. In some cases, we observed that additional components outside our tested ranges, and therefore more likely to be audible, were also generated at significant levels. The highest levels, i.e., between 125Hz and 12500Hz (TOB centers), are reported in Table V for each device tested.

Note that sounds at other frequencies may not always present a significant obstacle to an attacker. The headphones, for instance, produced relatively low noise at other frequencies, which would likely go unnoticed. However, other devices produced substantial noise at other frequencies. The parametric speaker in particular produced sound of relatively high levels at 12.5kHz. Therefore, these issues may present significant obstacles to an attacker wishing to remain covert, depending on variables such as ambient noise, the environment, and the ability of users to perceive sounds at certain frequencies.

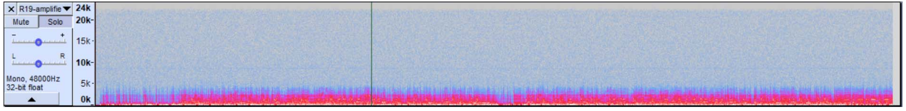
A. Damage

We could not replicate the significant temperature increases observed in the smart speaker during the pilot study. However, we did note a similar burning odor following the HFN test runs for the smart speaker, and observed a similar degradation in performance. Examining the time history from the sound level meter logs allowed us to investigate this further, and we noted that the speaker appeared to have experienced a marked and critical decrease in performance after approximately five minutes of emitting a 17kHz tone at maximum volume, from which the speaker did not recover.

To assess the damage to the smart speaker, we made two recordings of an audio track – a piece of popular music – played through a *newly* purchased smart speaker, in the anechoic chamber. One recording was made before testing, and the other after the HFN test runs had been completed. Comparing the recordings, we observed a significant decrease in the quality of the sound. Further examination using spectrograms, shown in Fig. 1, show



(a) Pre-Experiment



(b) Post-Experiment

Figure 1: Spectrograms in the audio editor software Audacity, for the pre-experiment recording (a) and post-experiment recording (b) of the smart speaker.

that the speaker appeared to have lost the ability to reproduce frequencies above approximately 5kHz. This effect, which may be the result of some sort of internal overheating or similar damage, appears to be permanent. This issue was disclosed privately to the manufacturer, and We received notification approximately two months after initial disclosure that an update would be rolled out to resolve the problem, however, at the time of writing, this has not yet been confirmed. We have not disclosed issues relating to the emission of HFN or LFN for any of the other devices as these are not addressable vulnerabilities as such. Rather, our attacks demonstrate repurposing of intended functionality.

VI. DISCUSSION

We now provide a broader discussion of our work and its implications.

A. *Results Summary*

Out of the eight device set-ups we tested in our experiments, we found that four (two smart, two traditional) were capable of emitting HFN and/or LFN at levels exceeding the averages of those deemed permissible by various bodies such as those referenced in Table I. More precisely:

1) The smart speaker and the headphones exceeded levels for both HFN and LFN;
2) The parametric speaker for HFN;
3) The loudspeaker for LFN.

Attacks against headphones in particular may be attractive to attackers seeking to attack smart devices in order to produce acoustic effects. Indeed, headphones are being increasingly used in developed countries [28], often at high volumes and associated with decreased hearing acuity and hearing loss [61], [41], particularly among young people [64], [29]. Moreover, as mentioned previously, they are often connected to devices such as laptops, mobile phones, and tablets.

It is also possible that the smart speaker is capable of producing HFN at high levels, and our results indicate this was the case for a short period of time. However, this led to the speaker suffering permanent damage.

There are also a number of other attacks, such as the browser or audio manipulation techniques described in Section IV-D, which could be used to target such users. A variation of the laptop or phone attacks (presented in Section IV-C) could also be used to trigger the delivery of sound only when the malware detects that headphones are attached.

B. *Limitations*

Naturally, our work is not without limitations. Our experiments were conducted on a relatively small scale and with a limited number of devices, as we aimed to provide a feasibility study of an understudied problem. Moreover, due to constraints on the availability of the anechoic chamber, we limited our testing to short exposure times of ten minutes per frequency per device, and to take consistent readings, we placed the sound level meter at a distance of one metre from the device in question, and did not examine other scenarios or distances, except for the headphone tests. We hope that future research in this area will both examine the effects of these attacks on equipment over longer periods – as the consistent emission of HFN or LFN at high volumes may significantly degrade electronic components, rendering these attacks much less effective – and in more realistic scenarios and distances.

Moreover, to a large extent, successful acoustic attacks need to rely on (a) the attacker being able to manipulate a given device to emit sufficient levels of noise; (b) the victim not perceiving the emitted audio; (c) the victim being susceptible to the effects; and (d) the device being capable of producing high levels over time. While we have empirically demonstrated (a), and (d) to a certain extent, we acknowledge that further experiments would be required with respect to (b) and (c) especially. However, we are obviously constrained in carrying out these experiments by ethics regarding human experimentation and the safety of study participants.

Previous research has examined the effects of HFN and LFN on humans, albeit at attenuated levels [20], which has allowed us to extrapolate findings to real-world effects; this remains a limitation both in terms of assessing actual effects and in determining if the tones deployed, or artifacts thereof, would be perceived. As discussed above, some (but not all) of the tested devices emitted noise at frequencies and levels more likely to be perceived, which could therefore compromise the covert nature of the attacks.

VII. COUNTERMEASURES

We now discuss possible avenues to mitigate the acoustic attacks presented in this paper. Specifically, we consider specific countermeasures besides generic ones like restricting the installation or the execution of unauthorized code.

One avenue would be to follow suggestions by Deshotels [15] about prevention/detection of imperceptible sound as a covert channel. These include limiting the frequency range of speakers to frequencies in the typically audible range; visibly alerting users when device speakers are in use; filtering files during processing, such that frequencies outside the audible range are removed; and, in the case of mobile devices, implementing a permissions restriction on the use of speakers by apps, so that a user has to manually approve this.

As a proof-of-concept, we adapted an existing open-source software project[2], originally intended to be a sound-activated recorder and audio visualisation tool for Windows, to show alerts when noise above certain frequency ranges and user-specified thresholds is detected. Source code for this application is available publicly[3]. Naturally, this approach does rely on the capabilities of the microphone and soundcard on the host, arguably making it somewhat unrealistic for everyday consumer use, particularly in the case of true ultrasonic sound, or lower frequency sound sub-50Hz.

A similar approach could be used for mobile-based detection. In our pilot study, we used two free Android apps from the Google Play Store, along with a relatively inexpensive external microphone, and found that they were able to generate alerts when sounds exceeded certain levels, particularly with HFN. A wide range of other apps, for both iOS and Android, may be suitable for noise measurements, as a low-cost alternative to traditional SLMs [32], [45], [53], albeit within device limitations and with the caveat that there may be a decrease in accuracy. While many of these apps do not target HFN or LFN specifically, they may be able to generate alerts when certain level thresholds are exceeded.

It also remains crucial that employers comply with applicable legislation pertaining to acceptable noise limits. As noted in Section III, while a number of guidelines and measurement and assessment criteria exist for both LFN and HFN, researchers have argued that these may be inadequate due to methodological issues [34], underestimation of effects [37], [62], and a lack of clarity on the applicability of occupational guidelines in other contexts, such as public exposure [35].

An additional countermeasure could be to include heuristic features in consumer and enterprise antivirus detection engines, aiming to detect these attacks. For instance, there are few legitimate reasons for applications to need to alter the system or media volume.

We advise users owning smart speakers that allow control of certain functions (playing/streaming audio, changing volume) over a network to not employ port forwarding or UPnP, which would expose their speaker to potential remote attack. Where the control of such speakers over an API remains unauthenticated, this may still present a risk on a local network.

Finally, we argue that effective countermeasures mitigating the attacks presented in this paper could also be deployed to detect covert transmissions using ultrasonic audio, an active area of research as applied to both ultrasonic tracking, with subsequent privacy applications [39], and to air-gap bypasses [27], [15], [69].

VIII. CONCLUSION

This paper presented a novel class of attack, combining existing and new proof-of-concept malware and attacks to cause ordinary consumer devices to produce high-frequency noise (HFN) and low-frequency noise (LFN) at high levels. We empirically verified these attacks on a number of commodity hardware devices. Specifically, we found that a few devices appear to be capable of producing potentially imperceptible sounds at levels at or exceeding several recommended thresholds, as a direct result.

Like other researchers who previously attempted to examine the psychological and physical effects of high and low frequencies on humans, we found that the lack of consensus for adequate safety guidelines for HFN and LFN frequencies presents a challenge toward assessing the real-world consequences of these attacks.

However, the triviality of executing these attacks, and the size of the potential attack surface, could mean that the repurposing of consumer equipment for acoustic attacks may be viable for attackers aiming to directly cause harm to humans.

In future work, we plan to examine the capabilities of a wider range of equipment, in a variety of environments and at different distances. In particular, testing other smart speakers and headphones will provide a better understanding of the threats these devices may present. Moreover, for practical reasons, we limited our research to an assessment of consumer products which were relatively inexpensive and portable, and took measurements in an anechoic chamber at a distance of one meter. However, our attacks could be applied to larger and more powerful equipment with the potential to affect many more people in a wider area and to a much greater extent. For instance, an attack against a connected PA system at a music or sporting event, or against the speaker system in a vehicle, could produce audio at much more harmful levels. Other, more "noisy" channels, such as smart television broadcasts, or injecting HFN or LFN into phone conversations, may also be effective, particularly as the presence of other, more audible frequencies in such channels may decrease the likelihood of HFN/LFN being perceived by the victim.

We will also examine the applicability of these attacks to offensive cyber-campaigns at scale. For instance, an attack against an organization whereby many co-located user laptops in an office environment are infected with a self-replicating worm, using a payload similar to our

---

[2] https://www.codeproject.com/Articles/22951/Sound-Activated-Recorder-with-Spectrogram-in-C

[3] https://github.com/catz3/SoundAlert-example

proof-of-concept Windows malware, could result in users being exposed to more harmful levels of audio, for longer durations.

Availability. As mentioned earlier, we have not released the code of our proof-of-concept attacks, nor the specifications of the devices in our experiments, in order to minimize the risk to the general public. However, we can do so upon request.

REFERENCES

[1] W. Acton and M. Carson. Auditory and subjective effects of airborne noise from industrial ultrasonic sources. *Occupational and Environmental Medicine*, 24(4), 1967.

[2] J. Altmann. Acoustic weapons-a prospective assessment. *Science & Global Security*, 9(3), 2001.

[3] W. M. Arkin. Acoustic anti-personnel weapons: An inhumane future? *Medicine, Conflict and Survival*, 13(4), 1997.

[4] K. Ashihara, K. Kurakata, T. Mizunami, and K. Matsushita. Hearing threshold for pure tones above 20 kHz. *Acoustical science and technology*, 27(1), 2006.

[5] R. E. Bartholomew and D. F. Z. Pérez. Chasing ghosts in cuba: Is mass psychogenic illness masquerading as an acoustical attack?, 2018.

[6] R. E. Bartholomew and D. F. Z. Pérez. Chasing ghosts in Cuba: Is mass psychogenic illness masquerading as an acoustical attack? *International Journal of Social Psychiatry*, 64(5), 2018.

[7] L. Ben Othmane, A. Al-Fuqaha, E. ben Hamida, and M. Van Den Brand. Towards extended safety in connected vehicles. In *16th International IEEE Conference on Intelligent Transportation Systems*, 2013.

[8] J. Bengtsson. *Low Frequency Noise During Work: Effects on Performance and Annoyance*. PhD thesis, Götenburg University, 2003.

[9] V. A. Benignus, D. A. Otto, and J. H. Knelson. Effect of low-frequency random noises on performance of a numeric monitoring task. *Perceptual and motor skills*, 40(1), 1975.

[10] C. Bolton, S. Rampazzi, C. Li, A. Kwong, W. Xu, and K. Fu. Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems. In *IEEE Symposium on Security & Privacy*, 2018.

[11] R. G. Brody, H. U. Chang, and E. S. Schoenberg. Malware at its worst: death and destruction. *International Journal of Accounting & Information Management*, 26(4), 2018.

[12] T. M. Chen. Cyberterrorism after Stuxnet. Technical report, Strategic Studies Institute, Army War College (U.S.), 2014.

[13] A. Chopra, B. S. Thomas, K. Mohan, and K. Sivaraman. Auditory and Nonauditory Effects of Ultrasonic Scaler Use and Its Role in the Development of Permanent Hearing Loss. *Oral Health & Preventive Dentistry*, 14(6), 2016.

[14] M. Cunche and L. S. Cardoso. Analyzing Ultrasound-based Physical Tracking Systems. In *GreHack*, 2018.

[15] L. Deshotels. Inaudible Sound as a Covert Channel in Mobile Devices. In *WOOT*, 2014.

[16] C. N. Dolder, M. D. Fletcher, S. Lloyd Jones, B. Lineton, S. R. Dennison, M. Symmonds, P. R. White, and T. G. Leighton. Measurements of ultrasonic deterrents and an acoustically branded hairdryer: Ambiguities in guideline compliance. *Journal of the Acoustical Society of America*, 144(4), 2018.

[17] F. Duck and T. G. Leighton. Frequency bands for ultrasound, suitable for the consideration of its health effects. *Journal of the Acoustical Society of America*, 144(4), 2018.

[18] J. D. Durrant and J. H. Lovrinic. *Bases of hearing science*. Lippincott Williams and Wilkins, 1995.

[19] V. Filonenko, C. Cullen, and J. Carswell. Investigating Ultrasonic Positioning on Mobile Phones. In *International Conference on Indoor Positioning and Indoor Navigation*, 2010.

[20] M. D. Fletcher, S. Lloyd Jones, P. R. White, C. N. Dolder, T. G. Leighton, and B. Lineton. Effects of very high-frequency sound and ultrasound on humans. Part I: Adverse symptoms after exposure to audible very-high frequency sound. *Journal of the Acoustical Society of America*, 144(4), 2018.

[21] M. D. Fletcher, S. Lloyd Jones, P. R. White, C. N. Dolder, T. G. Leighton, and B. Lineton. Effects of very high-frequency sound and ultrasound on humans. Part II: A double-blind randomized provocation study of inaudible 20-kHz ultrasound. *Journal of the Acoustical Society of America*, 144(4), 2018.

[22] B. A. Golomb. Diplomats' mystery illness and pulsed radiofrequency/microwave radiation. *Neural computation*, 30(11):2882–2985, 2018.

[23] J. Grzesik and E. Pluta. Dynamics of high-frequency hearing loss of operators of industrial ultrasonic devices. *International archives of occupational and environmental health*, 57(2), 1986.

[24] S. Gudkov. Google Play Store – InfraSound Detector App. https://play.google.com/store/apps/details?id=com.microcadsystems.serge.infrasounddetector, 2019.

[25] S. Gudkov. Google Play Store – UltraSound Detector App. https://play.google.com/store/apps/details?id=com.microcadsystems.serge.ultrasounddetector, 2019.

[26] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE Symposium on Security & Privacy*, 2008.

[27] M. Hanspach and M. Goetz. On covert acoustical mesh networks in air. *arXiv preprint 1406.1213*, 2014.

[28] E. Henderson, M. A. Testa, and C. Hartnick. Prevalence of noise-induced hearing-threshold shifts and hearing loss among US youths. *Pediatrics*, 127(1), 2011.

[29] S. Herrera, A. B. M. de Lacerda, D. Lurdes, P. A. Alcaras, L. H. Ribeiro, et al. Amplified music with headphones and its implications on hearing health in teens. *International Tinnitus Journal*, 20(1), 2016.

[30] C. Q. Howard, C. H. Hansen, and A. C. Zander. A review of current ultrasound exposure limits. *Journal of Occupational Health and Safety of Australia and New Zealand*, 21(3), 2005.

[31] A. Kaczmarska and A. Łuczak. A study of annoyance caused by low-frequency noise during mental work. *International Journal of Occupational Safety and Ergonomics*, 13(2), 2007.

[32] C. A. Kardous and P. B. Shaw. Evaluation of smartphone sound measurement applications. *Journal of the Acoustical Society of America*, 135(4), 2014.

[33] C. Koch. Hearing beyond the limit: Measurement, perception and impact of infrasound and ultrasonic noise. In *12th ICBEN Congress on Noise as a Public Health Problem*, 2017.

[34] T. G. Leighton. Are some people suffering as a result of increasing mass exposure of the public to ultrasound in air? *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 472(2185), 2016.

[35] T. G. Leighton. Ultrasound in air—Guidelines, applications, public exposures, and claims of attacks in Cuba and China. *Journal of the Acoustical Society of America*, 144(4), 2018.

[36] G. Leventhall. Low Frequency Noise. What we know, what we do not know, and what we would like to know. *Journal of Low Frequency Noise, Vibration and Active Control*, 28(2), 2009.

[37] G. Leventhall, P. Pelmear, and S. Benton. A review of published research on low frequency noise and its effects, 2003.

[38] I. Maccà, M. L. Scapellato, M. Carrieri, S. Maso, A. Trevisan, and G. B. Bartolucci. High-frequency hearing thresholds: effects of age, occupational ultrasound and noise exposure. *International Archives of Occupational and Environmental Health*, 88(2), 2015.

[39] V. Mavroudis, S. Hao, Y. Fratantonio, F. Maggi, C. Kruegel, and G. Vigna. On the privacy and security of the ultrasound ecosystem. *Proceedings on Privacy Enhancing Technologies*, 2017(2), 2017.

[40] M. Mirowska and E. Mroz. Effect of low frequency noise at low levels on human health in light of questionnaire investigation. In *InterNoise 2000*, 2000.

[41] A. Mohammadpoorasl, M. Hajizadeh, S. Marin, P. Heydari, and M. Ghalenoei. Prevalence and pattern of using headphones and its relationship with hearing loss among students. *Health Scope*, 7(4), 2018.

[42] H. Møller and M. Lydolf. A questionnaire survey of complaints of infrasound and low-frequency noise. *Journal of Low Frequency Noise, Vibration and Active Control*, 21(2), 2002.

[43] A. Moorhouse, D. Waddington, M. Adams, et al. Proposed criteria for the assessment of low frequency noise disturbance (Revision 1). http://usir.salford.ac.uk/491/1/NANR45-criteria__rev1_23_12_2011_(2).pdf, 2011.

[44] J. H. Mühlhans. Low frequency and infrasound: A critical review of the myths, misbeliefs and their relevance to music perception research. *Musicae Scientiae*, 21(3), 2017.

[45] E. Murphy and E. A. King. Testing the accuracy of smartphones and sound level meter applications for measuring environmental noise. *Applied Acoustics*, 106, 2016.

[46] T. Oluwafemi, T. Kohno, S. Gupta, and S. Patel. Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of Home Automation Security. In *LASER*, 2013.

[47] T. Oohashi, E. Nishina, M. Honda, Y. Yonekura, Y. Fuwamoto, N. Kawai, T. Maekawa, S. Nakamura, H. Fukuyama, and H. Shibasaki. Inaudible high-frequency sounds affect brain activity: hypersonic effect. *Journal of neurophysiology*, 83(6), 2000.

[48] M. Pawlaczyk-łuszczyńska, A. Dudarewicz, M. Waszkowska, W. Szymczak, M. Kameduła, and M. Śliwińska-Kowalska. Does low frequency noise at modarate levels influence human mental performance? *Journal of Low Frequency Noise, Vibration, and Active Control*, 24(1), 2005.

[49] K. Persson and M. Bjorkman. Annoyance due to low frequency noise and the use of the dB (A) scale. *Journal of Sound and Vibration*, 127(3), 1988.

[50] K. Poulsen. Hackers assault epilepsy patients via computer. https://www.wired.com/2008/03/hackers-assault-epilepsy-patients-via-computer/, 2008.

[51] C. Y. H. Qibai and H. Shi. An investigation on the physiological and psychological effects of infrasound on persons. *Journal of Low Frequency Noise, Vibration and Active Control*, 23(1), 2004.

[52] B. Rios and J. Butts. When IoT Attacks: understanding the safety risks associated with connected devices. *Black Hat USA*, 2017.

[53] B. Roberts, C. Kardous, and R. Neitzel. Improving the accuracy of smart devices to measure noise exposure. *Journal of Occupational and Environmental Hygiene*, 13(11), 2016.

[54] E. Ronen and A. Shamir. Extended functionality attacks on IoT devices: The case of smart lights. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*, 2016.

[55] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson. Sok: Security and privacy in implantable medical devices and body area networks. In *IEEE Symposium on Security & Privacy*, 2014.

[56] B. Smagowska and M. Pawlaczyk-Łuszczyńska. Effects of ultrasonic noise on the human body–A bibliographic review. *International Journal of Occupational Safety and Ergonomics*, 19(2), 2013.

[57] S. Stansfeld and M. Shipley. Noise sensitivity and future risk of illness and mortality. *Science of the Total Environment*, 520, 2015.

[58] A. L. Stubbs and F. Montealegre-Z. Recording of" sonic attacks" on us diplomats in cuba spectrally matches the echoing call of a caribbean cricket. *bioRxiv*, page 510834, 2019.

[59] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker. Cyber-physical vunerabilities in additive manufacturing systems. *Context*, 7(8), 2014.

[60] M. Ueda, A. Ota, and H. Takahashi. Investigation on high-frequency noise in public space—We tried noise abatement measures for displeasure people. In *Proceedings of the 7th Forum Acusticum*, 2014.

[61] L. Vaidya, N. Shah, and A. H. Mistry. Evaluation of hearing acuity in young adults using personal listening devices with earphones. *Int J Basic Appl Physiol*, 7(1):89, 2018.

[62] R. Vasudevan and H. Leventhall. A study of annoyance due to low frequency noise in the home. *Journal of Low Frequency Noise, Vibration and Active Control*, 1(4), 1982.

[63] R. Vinokur. Acoustic noise as a non-lethal weapon. *Sound and Vibration*, 38(10), 2004.

[64] I. Vogel, J. Brug, C. P. Van der Ploeg, and H. Raat. Young people's exposure to loud music: a summary of the literature. *American journal of Preventive Medicine*, 33(2), 2007.

[65] H. E. Von Gierke and C. W. a. Nixon. Damage risk criteria for hearing and human body vibration. *Noise and vibration control engineering: principles and applications*, 1992.

[66] K. P. Waye, R. Rylander, S. Benton, and H. Leventhall. Effects on performance and work quality due to low frequency ventilation noise. *Journal of Sound and Vibration*, 205(4), 1997.

[67] P. A. Williams and A. J. Woodward. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices*, 8, 2015.

[68] J. D. Wilson, M. L. Darby, S. L. Tolle, and J. C. Sever Jr. Effects of occupational ultrasonic noise exposure on hearing of dental hygienists: a pilot study. *Journal of Dental Hygiene*, 76(4), 2002.

[69] M. Wixey. See no evil, hear no evil: Hacking invisibly and silently with light and sound. In *DEFCON 25*, 2017.

[70] C. Yan, K. Fu, and W. Xu. On cuba, diplomats, ultrasound, and intermodulation distortion. *Computers in biology and medicine*, 104:250–266, 2019.

[71] C. Yan, W. Xu, and J. Liu. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. In *DEFCON 24*, 2016.