Acoustic Denial of Service Attacks on Hard Disk Drives

Mohammad Shahrad, Arsalan Mosenia, Liwei Song,
Mung Chiang*, David Wentzlaff, and Prateek Mittal

Princeton University *Purdue University

{mshahrad,arsalan,liweis,wentzlaf,pmittal}@princeton.edu,chiang@purdue.edu

ABSTRACT

Bridging concepts from information security and resonance theory, we propose a novel denial of service attack against hard disk drives (HDDs). In this attack, *acoustic signals are used to cause rotational vibrations* in HDD platters in an attempt to create failures in read/write operations, *ultimately halting the correct operation of HDDs.*

We perform a comprehensive examination of multiple HDDs to characterize the attack and show the feasibility of the attack in two real-world systems, namely, surveillance devices and personal computers. Our attack highlights an overlooked security vulnerability of HDDs, introducing a new threat that can potentially endanger the security of numerous systems.

CCS CONCEPTS

• **Security and privacy → Hardware attacks and countermeasures**; **Denial of service attacks**;

KEYWORDS

Hard disk drive (HDD); acoustic resonance; denial of service (DoS); hardware reliability; CCTV DVR

ACM Reference Format:
Mohammad Shahrad, Arsalan Mosenia, Liwei Song, Mung Chiang*, David Wentzlaff, and Prateek Mittal. 2018. Acoustic Denial of Service Attacks on Hard Disk Drives. In *The Second Workshop on Attacks and Solutions in Hardware Security (ASHES'18), October 19, 2018, Toronto, ON, Canada.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3266444.3266448

1 INTRODUCTION

Hard disk drives (HDDs) are the most commonly used type of non-volatile storage [1]. Since their introduction in the 1950s, their storage capacity, cost-effectiveness, energy efficacy, and reliability have significantly improved [15, 24, 36]. These advances in HDDs, along with the ever-growing data storage demand, has made them an integral part of numerous computing systems.

HDDs have a critical role in modern computing systems. Although there have been numerous studies on their failure and reliability models [16, 25, 26], their security has been overlooked. HDDs hold essential software components and sensitive data, and thus, can be appealing targets for a plethora of attackers. A few recent studies have shown the feasibility of information leakage from HDDs through electromagnetic [7, 19] and acoustic [14] emanations. *We pursue an entirely different angle to the security of HDDs: borrowing concepts from information security and resonance theory, we propose novel acoustic denial of service (DoS) attacks on HDDs that halt their normal operation.* Our key contributions can be summarized as follows:

- We present an extensive study on non-contact DoS attacks against HDDs. While a concurrent work (published after our arXiv preprint) also showed the vulnerability of HDDs to acoustic interference [8], we conduct such attacks persistently with lower sounds levels, as we discovered the significance of the attack angle.
- We explore how an attacker can exploit the acoustic resonance phenomenon to disrupt the operation of HDDs, and discuss how they can find appropriate frequencies needed for launching the attack.
- We examine several state-of-the-art HDD models. As shown in Section 4, our attack can completely halt the read/write operations for all tested models.
- We highlight negative consequences of our attack using two real-world case studies, namely a CCTV surveillance system and personal computer.
- To support our hypothesis that acoustic resonance causes the attack, we disassemble an HDD and demonstrate that the attack frequencies match the resonance frequencies of HDD platters.

The remainder of the paper is organized as follows. Section 2 provides the background. Section 3 describes the threat model. Characterization of the attack using multiple HDDs is explained in Section 4. Section 5 demonstrates the feasibility of our attack against real-world systems. Section 6 briefly discusses how our findings match the underlying theory and describe countermeasures. The related work is explained in Section 7. Section 8 concludes the paper.

2 BACKGROUND

Components of HDDs: HDDs have one or more *platters*, which are covered with a magnetizable coating. Information is stored in the form of magnetic orientation in small regions on this coating layer(s). A moving head, together with rotating platters, enables access to any point on this surface to perform read/write operations. Figure 1 shows the main moving components inside an HDD. Since a read/write operation requires precise placement of the head at specific radii of platters, any abnormal movement of these moving

ASHES'18, October 19, 2018, Toronto, ON, Canada

ACM ISBN 978-1-4503-5996-2/18/10…$15.00
https://doi.org/10.1145/3266444.3266448

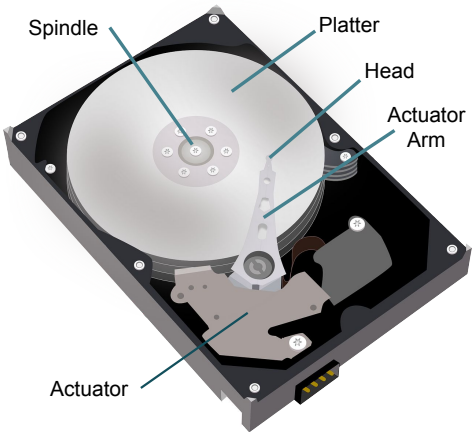

Figure 1: Main moving components inside an HDD.

components can potentially lead to a failure. However, data access happens at the granularity of a *sector* – a concentric circular track on the platter with a typical size of 512 bytes that is protected by error correcting codes (ECC). These codes have enabled HDDs to work reliably despite random failures. However, they fail if the number of failures is more than a certain threshold in a sector.

Acoustic Resonance: Based on resonance theory, any material object has well-defined natural oscillation frequencies (known as *resonance frequencies*) due to its constructive interference of internal and/or external surface waves [30]. Resonance is caused when external waves at frequencies close to those *resonance frequencies* are scattered by the object [13], something we base our acoustic attacks upon. Inversely, the sound scattered from an object after a physical impulse has dominant components revealing its resonance frequencies. We use this technique in Section 6 to determine resonance frequencies of HDD platters and confirm that these frequencies of platters match frequencies used in the proposed attack.

3 THREAT MODEL

In this section, we first describe consequences of acoustic resonance on HDDs and then discuss the threat model.

3.1 Problem Definition

Driven by rapid advances in storage technologies, modern HDDs offer a high areal density (over 1.2 Gb/in^2 [23]). Supporting such a high areal density requires a careful design of a head positioning scheme that can accurately place read/write heads of the HDD in the appropriate position. Even a small displacement of the head leads to malfunctioning of the HDD and may even accidentally scratch the platters, causing permanent damage to the HDD. In this paper, we demonstrate an active attack against HDDs that causes misplacement of internal read/write heads. As shown later, an intentionally-generated acoustic signal can cause unwanted acoustic resonance in internal components of an HDD, leading to *seek failures* [1] and severe failures in the whole system that relies on the HDD. For example, it can completely freeze the operating system (OS) running on a personal computer, requiring a reboot. *We provide a proof-of-concept of the proposed attack, shedding light on an overlooked vulnerability of HDDs.*

[1]Seek failure is a well-known failure mechanism in HDDs in which heads are not precisely positioned at the platter location where the data will be read or written.

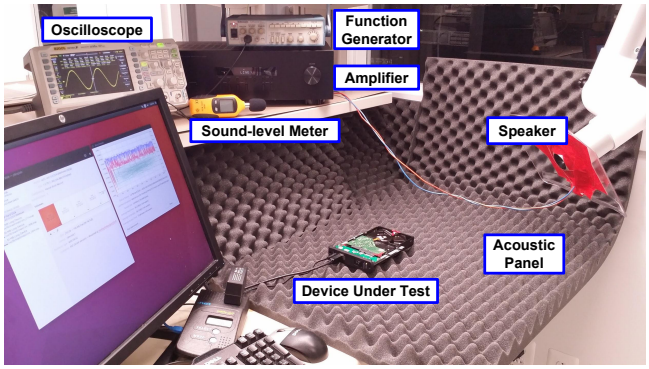

Figure 2: Experimental setup for acoustic DoS attacks.

3.2 Attackers and Their Capabilities

We envision HDDs to be an interesting target for attackers due to the vital role of HDDs in numerous computing systems, including, but not limited to, surveillance systems, cloud servers, industrial automation/monitoring system, and medical bedside monitors.

The attacker's capabilities: We make three main assumptions about a potential attacker: the attacker (i) can neither directly control nor touch the HDD, (ii) can generate acoustic signals in the vicinity of the victim device at resonance frequencies of the under-attack HDD, (iii) can control the amplitude/power of the acoustic signals. We do not put any limit on the ability of the attacker to study a specific targeted HDD in a controlled environment prior to the attack. The attacker can reverse engineer a sample (similar) computing system to extract the exact model, characteristics, and vulnerabilities of its HDD.

Potential attack approaches: The attacker can either apply the acoustic signal by using an external speaker or exploit a speaker near the target. Towards this end, they may potentially use remote software exploitation (e.g., remotely control the multimedia software in a personal device), deceive the user to play a malicious sound attached to an email or a web page [29], or embed the malicious sound in widespread multimedia, for instance in a TV advertisement or an embedded audio targeting gaming consoles.

4 CHARACTERIZATION OF THE PROPOSED ATTACK

In this section, we perform acoustic DoS attacks on hard drives in isolation. Without any barrier shielding the HDD, its exposure to sound waves is maximized, leading to better exploration of potential vulnerabilities. In Section 5 we will show that the acoustic attack is possible even when HDDs are embedded in metal cases.

4.1 Experimental Setup

Our experimental setup is depicted in Figure 2. A function generator was used to produce sine waves at certain frequencies to feed an amplifier. The output of the amplifier was then connected to a

Table 1: Attack frequencies for different HDD models.

HDD Model	Capacity	Attack Frequency Window(s) (Hz)
WD3200AAKS-75L9A0	320 GB	[2,300 - 2,510]
WD5000AAKS-75A7B0	500 GB	[2,240 - 2,520] [3,800 - 4,020] [4,725 - 5,006]
WD10EZEX-08WN4A0	1 TB	[2,265 - 2,281] [2,455 - 2,503] [6,700 - 6,845] [8,212 - 8,873] [12,839 - 12,840]
WD40EZRZ-00GXCB0	4 TB	[4,590 - 6,550] [7,502 - 7,900] [8,398 - 8,618] [9,420 - 10,200]

speaker and monitored by an oscilloscope. We mounted the speaker on a movable arm to study the implications of strength (controlled by distance) and direction of sound waves on the feasibility of the attack. A sound-level meter was used to measure the sound level in dbA. We covered the surrounding of the device under attack with sound absorbing panels to alleviate unwanted reflections. The operator performing experiments was protected with professional earmuffs.

Each target HDD was connected to a PC via a USB 3 SATA adapter. The standard read/write benchmark from the Linux Disk Utility was used to monitor the impact of sound on the performance of the disk drive. In addition, we used the Self-Monitoring, Analysis and Reporting Technology (SMART) interface through the `smartmontools` Linux package to gather detailed information on hard drive health. SMART is implemented in many modern hard drives and is widely used in HDD reliability studies [16–18, 25].

4.2 Halting Read/Write Operations

In our first experiment, we connected different hard drives to the computer externally and exposed them to a different sound frequency while performing the disk performance benchmark mentioned in Section 4.1. We then recorded frequency ranges leading to a full halt in read and write operations. During this experiment, the speaker was kept at a close distance (10 cm) with a fixed angle towards the disk under attack. We analyze the importance of the attack angle later. Table 1 reflects the attack frequency ranges for four different HDD models with varying storage capacities. While some of these attack windows are remarkably wide, some are as narrow as a few Hertz.

Following successful acoustic attacks, SMART logs of tested HDDs showed increased **`Seek_Error_Rate`**, an ordinarily pre-failure attribute [18]. We also ran the SMART extended self-test with and without performing the acoustic attack. The under-attack HDD failed due to **`servo/seek failure`** (Figure 3) confirming the previous observation. In general, rotational vibrations cause seek failures in HDD platters during the attack. This explains the higher susceptibility of denser HDDs to this attack (see Table 1), since seeking smaller magnetic regions on platters requires higher precision.

```
SMART Extended Self-test Log Version: 1 (1 sectors)
Num  Test_Description    Status                  Remaining
# 1  Short offline       Completed: servo/seek failure 90%
# 2  Short offline       Completed without error       00%
```

Figure 3: The HDD SMART self-test fails with servo/seek failure under acoustic attack (test number 1).

4.3 Determining the Best Attack Angle

Early in our experiments, we realized that the angle of the speaker towards the hard drive has a substantial influence on the attack success. Therefore, we used the setting described in Section 4.1 to sample the space around the HDD under attack and measured the maximum distance for a successful attack at various angles. During all measurements, we fixed the amplitude of the sound signal fed to the speaker. Figure 4 shows the spatial map of successful attack distances. The distance is color-coded, and a farther distance means more vulnerability in that spherical angle. Note that only sampled angles are colored. Rectangles in this figure indicate the position of the HDD and the small *A* marks are the side away from the SATA circuitry. While the two tested HDD models have distinct spacial attack maps, the attack frequency seems to be of great importance to conduct a successful attack. The farthest successful attack required a sound level of 92.8 dBA for the 1 TB HDD at 9.1 kHz, and 102.6 dbA for the 4 TB HDD at 8.5 kHz. Note that producing such a sound level is easily feasible for a Long Range Acoustic Device (LRAD) such as LRAD 2000X with a maximum continuous output of 162dB at one meter [22].

5 CASE STUDIES

Using insights from the previous section, we present attacks on a CCTV Digital Video Recorder (DVR) as well as a PC to demonstrate the vulnerability of real-world systems to acoustic attacks.

5.1 CCTV DVR

DVRs are used to store videos recorded by CCTV systems, where each frame could be a crucial piece of forensic evidence [5, 32]. Due to the high storage capacity requirement and cost-effectiveness, magnetic hard drives are the prevailing storage type in DVRs. Therefore it is important to explore their vulnerabilities to acoustic DoS.

We evaluated this vulnerability by testing a commercial DVR (ZOSI ZR08AN/00 H.264 NDVR). The 4 TB HDD used in the previous section was installed in the DVR, and four digital security cameras were connected to it. We then exposed the DVR to a sound wave with a fixed 8.5 kHz frequency, which is a tested major attack frequency for that HDD (see Figure 4). We thereupon audited the monitor connected to the DVR for any anomalies. Figure 5 shows the diagram of our test setup.

After 230 seconds of an ongoing attack, a pop-up warning appeared on the monitor stating *"Disk lost!"*. After stopping the sound, we tried to replay the recorded videos from the cameras and found that they had been interrupted (Figure 6). We also tried formatting the HDD using DVR's Disk Management Tool, which failed. The DVR had to be restarted to fix this issue, but the video footage was permanently lost.

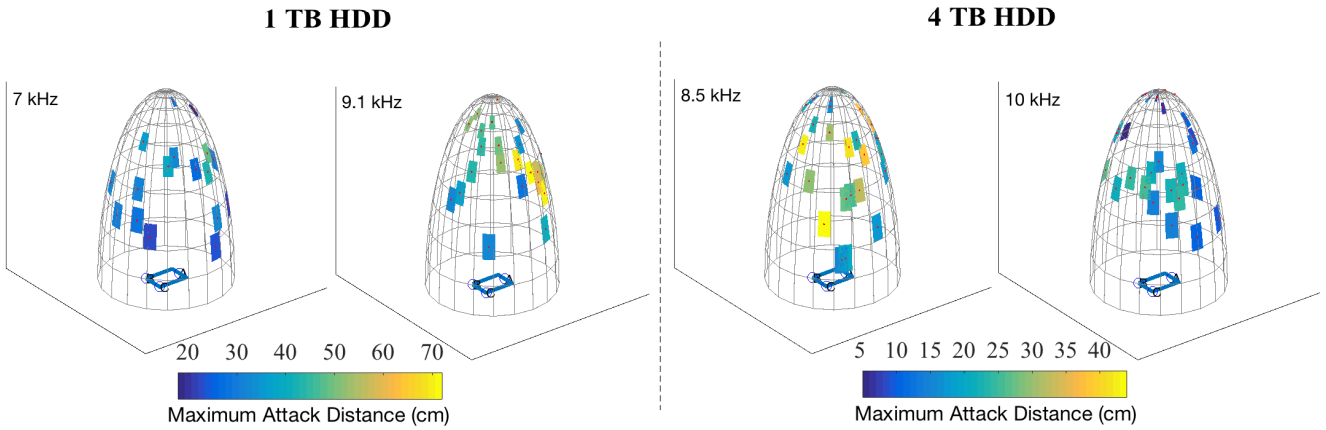

Figure 4: Maximum distance of successful acoustic attacks as a function of attack angle for a 1 TB as well as a 4 TB hard disk drive. Each HDD has been tested for two of its major resonance frequencies.

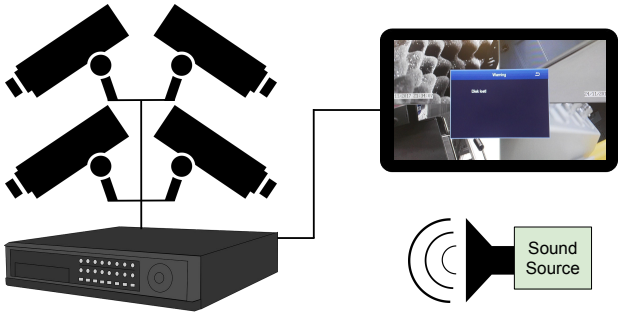

Figure 5: Experimental setup for performing acoustic attacks on the digital video recorder (DVR).

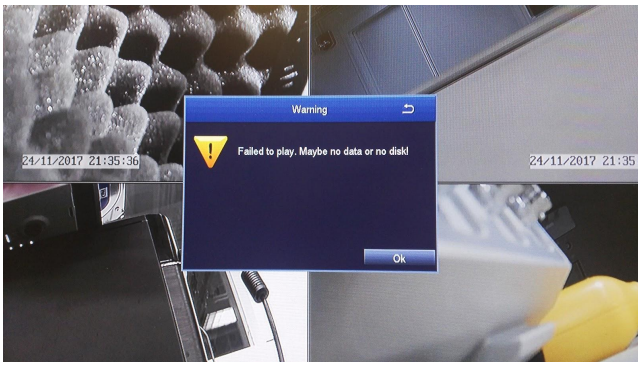

Figure 6: The acoustic attack disrupting the video recording on a DVR.

We believe the reason for data loss in this scenario is memory buffer overflow. Typically, the DVR memory acts as a buffer to temporarily store video data and guarantee that no frame is lost, given an HDD's variable write speed. However, this buffer can overflow if the HDD write throughput is predominantly less than the video data generation throughput. In fact, although causing a full write termination can accelerate this attack, even a partial write slowdown can lead to a successful interruption of video recording. Due to the sound blockage by the DVR case, the maximum attack distance was limited to 15 cm using the same speaker as in the previous section. More powerful sound sources would increase the attack range accordingly.

5.2 Desktop PC

To evaluate the impact of our proposed acoustic attack on an HDD enclosed in a PC case, we used a desktop PC (Lenovo H520s) and installed the 1 TB HDD used in Section 4 on it. We chose the previously tested 9.1 kHz frequency (see Figure 4) for this experiment. We then played the fixed-frequency sound from a 25-centimeter distance towards the case's airflow opening. This caused various kinds of malfunctions on the running PC.

We examined three modern OSs to verify the attack. Table 2 summarizes different observed anomaly symptoms from the acoustic attack. As seen, some of the symptoms persist after stopping the sound and require the PC to be restarted. Figure 7 shows errors when running Windows 10 as the OS. Such behaviors are entirely expected as the hard drive is the primary storage unit containing the OS, application data, and user data. While an HDD DoS attack can directly impact disk write operations, it could also cause a critical kernel process to freeze, requiring the system to be restarted.

Table 2: DoS symptoms of different OSs under attack.

OS	Attack Time	DoS Symptom	Restart Required
Windows 10	< 5 sec	Full file copy stoppage	N
	5 min	Blue screen	Y
		or	
		Error 1962: No operating system found	Y
Ubuntu 16.04 LTS	< 5 sec	Full file copy stoppage	N
	1.5 min	Unresponsive OS	Y
Fedora 27	< 5 sec	Full file copy stoppage	N
	2 min	Unresponsive OS	Y

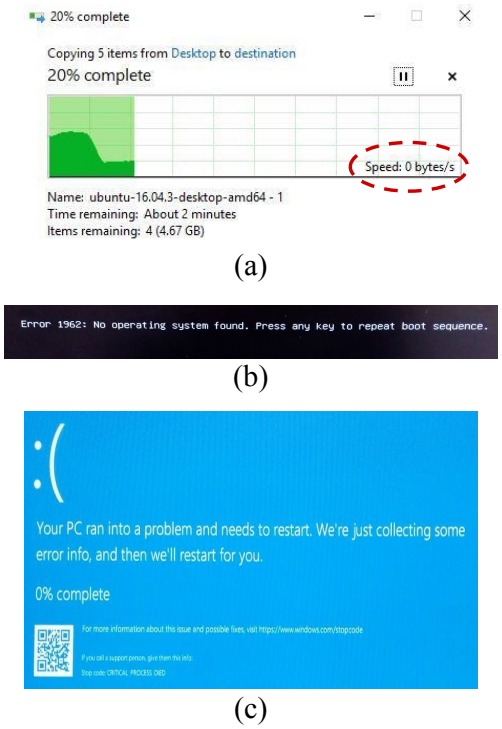

Figure 7: The attack leads to (a) stoppage of copy, (b) black screen error, and (c) blue screen error in Win 10.

6 DISCUSSION

6.1 Physics Behind the Attack

We removed the external cover of an HDD to find resonance frequencies of its moving components. We then used a pen to exert mechanical impulses on each component and recorded the waves scattered from the component. Each component leaves a unique pattern in the frequency domain, in which the dominant frequencies correspond to natural frequencies of the component. Figure 8 depicts the natural frequencies of platters in the experimented 320GB HDD. Comparing primary resonance frequencies of this hard drive shown in Figure 8 with attack frequencies included in Table 1 readily reveals that the frequency range corresponding to the successful attack overlaps with the primary resonance frequency range of HDD platters. This is also consistent with our findings in Section 4, where we observed that the attack causes servo/seek failures that are a common consequence of the failure of the head positioning system in reaching the appropriate location on the platter.

6.2 Countermeasures

Isolating HDDs offers a proactive approach to prevent the proposed attack. However, full isolation of HDDs is impractical due to the heat dissipation and thermal constraints. We suggest that the primary means for fortifying against this attack can be improving the seek control mechanism. Commonplace resonance detection mechanisms that are typically used to monitor HDD failures [33, 34] could be used to sense external sources of resonance. Using solid-state drives which are resistant to vibrations is a more costly solution

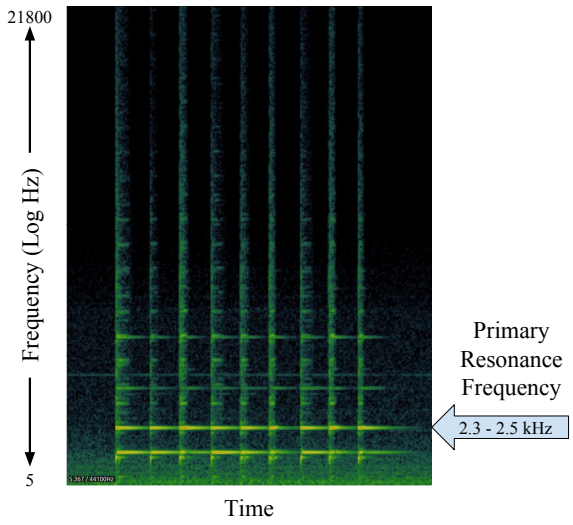

Figure 8: To extract resonance frequencies of an HDD platter, we opened the hard drive and exerted mechanical impulses on platter, while recording the scattered sound.

recommended for sensitive applications [10, 35]. It is worth mentioning that we tried to damp the HDD vibrations with rubber spacers, but the attack could not be alleviated.

7 RELATED WORK

Our proposed attack is among the first threats against HDDs. While acoustic/electromagnetic side-channel attacks have been extensively discussed in the literature [6, 20, 21], Biedermann et al. [7] have discussed the possibility of capturing and processing electromagnetic emanation of HDDs. They demonstrated that the magnetic field generated by the moving head of an HDD could be measured externally to extract information about ongoing operations. In particular, they were able to detect the OS booting up or applications being started. It has been suggested that environmental conditions, such as a high level of humidity or ambient noise, may negatively affect the reliability of HDDs [2, 4, 18]. In a blog post, Kruszelnicki [2] suggested that loud environmental noise can degrade the performance of a hard drive. The post has described a 2008 experiment by Brendan Gregg (YouTube demo [4]) where shouting at spinning HDDs located in data centers drops their performance. Further, a recent YouTube demo has shown that playing sound waves with the frequency of 130Hz can negatively affect the performance of a Linux machine [3].

Some recent studies have discussed noise-induced performance degradation in IO devices. Dean et al. [11, 12] have examined how the performance of Micro-Electro-Mechanical Systems (MEMS) gyroscopes may be negatively affected by environmental acoustic noise. Son et al. [27] proposed an attack against MEMS gyroscopes embedded in drones and demonstrated that an attacker could incapacitate drones using intentional sound noise. Trippel et al. [29] investigated how analog acoustic injection attacks can damage the digital integrity of widely-used MEMS accelerometer. Carlini et al. [9] and Vaidya [31] have shown that obfuscated (hidden in another sound in the audible range) voice commands can be interpreted by speech recognition systems. In two independent studies,

Zhang et al. [37] and Song et al. [28] have shown the vulnerability of microphones against inaudible acoustic commands. In this paper, we examined how intentionally-created acoustic signals can degrade the performance of a fundamental component of computing and embedded systems, namely HDDs.

In a concurrent work that appeared after our arXiv preprint, Bolton et al. also showed the vulnerability of HDDs to acoustic interference [8]. Their COMSOL simulations show that disk platters experience the maximum displacement, confirming what we found through resonance frequency matching in Section 6.1. In this work, however, we discovered the significance of the angle of attack which allowed us to increase the attack distance considerably. Specifically, we conducted attacks with **persistent vibrations** using a minimum of 94.7 dB (92.8 dBA at 9.1kHz), while Bolton et al. required sound pressure levels beyond 118 dB [8].

8 CONCLUSION

HDDs are an integral part of critical systems, including, personal computers, CCTVs, bedside monitors, cloud servers, and ATMs. Borrowing concepts from acoustics and mechanics, we conducted an extensive study on non-contact DoS attacks against HDDs and demonstrated the vulnerability of real-world systems against such attacks. We experimentally determined that vibration in HDD platters are the primary cause of such attacks and discovered that HDDs are more vulnerable to attacks targeted from certain angles. Our proof-of-concept sheds light on a new threat against computing systems, paving the way for further exploring overlooked susceptibilities of HDDs.

ACKNOWLEDGMENTS

We thank Adi Fuchs and anonymous reviewers for their helpful feedback on this work. This work was supported in part by the U.S. National Science Foundation under Grant No. CNS-1553437. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of our sponsors.

REFERENCES

[1] HDDs and SSDs: global shipments 2015-2021. https://www.statista.com/statistics/285474/hdds-and-ssds-in-pcs-global-shipments-2012-2017/. Accessed: 2018-2-6.
[2] Loud sounds can kill computer hard drives. http://www.abc.net.au/radionational/programs/greatmomentsinscience/loud-sounds-can-kill-computer-hard-drives/7938388. Accessed: 2017-12-10.
[3] Resonance attack against HDD . https://www.youtube.com/watch?v=8DdqTz3CW5Y. Accessed: 2017-11-19.
[4] Shouting in the Datacenter. https://www.youtube.com/watch?v=tDacjrSCeq4. Accessed: 2017-12-10.
[5] AlShaikh, A., and Sedky, M. Post incident analysis framework for automated video forensic investigation. *International Journal of Computer Applications 135*, 12 (2016), 1–7.
[6] Backes, M., Dürmuth, M., Gerling, S., Pinkal, M., and Sporleder, C. Acoustic side-channel attacks on printers. In *USENIX Security Symp.* (2010), pp. 307–322.
[7] Biedermann, S., Katzenbeisser, S., and Szefer, J. Hard drive side-channel attacks using smartphone magnetic field sensors. In *International Conference on Financial Cryptography and Data Security* (2015), Springer, pp. 489–496.
[8] Bolton, C., Rampazzi, S., Li, C., Kwong, A., Xu, W., and Fu, K. 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)* (2018), pp. 824–838.
[9] Carlini, N., Mishra, P., Vaidya, T., Zhang, Y., Sherr, M., Shields, C., Wagner, D., and Zhou, W. Hidden voice commands. In *USENIX Security Symposium* (2016), pp. 513–530.
[10] Chan, C. S., Pan, B., Gross, K., Vaidyanathan, K., and Rosing, T. v. Correcting vibration-induced performance degradation in enterprise servers. *SIGMETRICS Perform. Eval. Rev. 41*, 3 (Jan. 2014), 83–88.
[11] Dean, R. N., Castro, S. T., Flowers, G. T., Roth, G., Ahmed, A., Hodel, A. S., Grantham, B. E., Bittle, D. A., and Brunsch, J. P. A characterization of the performance of a MEMS gyroscope in acoustically harsh environments. *IEEE Transactions on Industrial Electronics 58*, 7 (2011), 2591–2596.
[12] Dean, R. N., Flowers, G. T., Hodel, A. S., Roth, G., Castro, S., Zhou, R., Moreira, A., Ahmed, A., Rifki, R., Grantham, B. E., et al. On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise. In *Industrial Electronics, 2007. ISIE 2007. IEEE International Symposium on* (2007), IEEE, pp. 1435–1440.
[13] Flax, L., Gaunaurd, G. C., and Uberall, H. Theory of resonance scattering. *Physical acoustics 15* (1981), 191–294.
[14] Guri, M., Solewicz, Y., Daidakulov, A., and Elovici, Y. *Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise (DiskFiltration).* Springer International Publishing, Cham, 2017, pp. 98–115.
[15] Igami, M., and Uetake, K. Mergers, innovation, and entry-exit dynamics: Consolidation of the hard disk drive industry, 1996-2015, 2016.
[16] Li, J., Ji, X., Jia, Y., Zhu, B., Wang, G., Li, Z., and Liu, X. Hard drive failure prediction using classification and regression trees. In *Dependable Systems and Networks (DSN), 44th Annual IEEE/IFIP Int. Conference on* (2014), IEEE, pp. 383–394.
[17] Mahdisoltani, F., Stefanovici, I., and Schroeder, B. Proactive error prediction to improve storage system reliability. In *2017 USENIX Annual Technical Conference (USENIX ATC 17)* (Santa Clara, CA, 2017), USENIX Association, pp. 391–402.
[18] Manousakis, I., Sankar, S., McKnight, G., Nguyen, T. D., and Bianchini, R. Environmental conditions and disk reliability in free-cooled datacenters. In *14th USENIX Conference on File and Storage Technologies (FAST 16)* (Santa Clara, CA, 2016), USENIX Association, pp. 53–65.
[19] Matyunin, N., Szefer, J., Biedermann, S., and Katzenbeisser, S. Covert channels using mobile device's magnetic field sensors. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)* (Jan 2016), pp. 525–532.
[20] Mosenia, A., and Jha, N. K. A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing 5*, 4 (2017), 586–602.
[21] Nia, A. M., Sur-Kolay, S., Raghunathan, A., and Jha, N. K. Physiological information leakage: A new frontier in health information security. *IEEE Transactions on Emerging Topics in Computing 4*, 3 (2016), 321–334.
[22] Parker, J. E. Towards an acoustic jurisprudence: Law and the long range acoustic device. *Law, Culture and the Humanities 14*, 2 (2018), 202–218.
[23] Re, M. Hackers can now steal data by listening to the sound of a computer's hard drive. https://www.forbes.com/sites/tomcoughlin/2015/06/28/progress-in-hdd-areal-density/#4f4554a61671. Accessed: 2017-12-10.
[24] Re, M. Tech talk on HDD areal density. https://www.seagate.com/www-content/investors/_shared/docs/tech-talk-mark-re-20150825.pdf. Accessed: 2017-12-10.
[25] Schroeder, B., and Gibson, G. A. Disk failures in the real world: What does an MTTF of 1,000,000 hours mean to you? In *FAST* (2007), vol. 7, pp. 1–16.
[26] Shahrad, M., and Wentzlaff, D. Availability Knob: Flexible user-defined availability in the cloud. In *Proceedings of the Seventh ACM Symposium on Cloud Computing* (2016), SoCC '16, ACM, pp. 42–56.
[27] Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., Choi, J., and Kim, Y. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security Symposium* (2015), USENIX Association, pp. 881–896.
[28] Song, L., and Mittal, P. Inaudible voice commands. *arXiv preprint arXiv:1708.07238* (2017).
[29] Trippel, T., Weisse, O., Xu, W., Honeyman, P., and Fu, K. WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In *In Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017).*
[30] Uberall, H., Moser, P., Murphy, J., Nagl, A., Igiri, G., Subrahmanyam, J., Gaunard, G., Brill, D., Delsanto, P., Alemar, J., et al. Electromagnetic and acoustic resonance scattering theory. *Wave Motion 5*, 4 (1983), 307–329.
[31] Vaidya, T. Cocaine Noodles: exploiting the gap between human and machine speech recognition. *Presented at WOOT 15* (2015), 10–11.
[32] Valentine, T., and Davis, J. P. *Forensic facial identification: Theory and practice of identification from eyewitnesses, composites and CCTV.* John Wiley & Sons, 2015.
[33] Wang, W., Guo, G., and Chong, T.-C. HDD actuator resonance detection through acoustic signal analysis. *IEEE transactions on magnetics 36*, 5 (2000), 3585–3587.
[34] Wang, Y., Miao, Q., Ma, E. W., Tsui, K.-L., and Pecht, M. G. Online anomaly detection for hard disk drives based on mahalanobis distance. *IEEE Transactions on Reliability 62*, 1 (2013), 136–145.
[35] Xu, X., and Huang, H. H. Exploring data-level error tolerance in high-performance solid-state drives. *IEEE Trans. on Reliability 64*, 1 (2015), 15–30.
[36] Yamaguchi, T., Hirata, M., and Pang, J. C. K. *High-speed precision motion control.* CRC press, 2017.
[37] Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., and Xu, W. DolphinAttack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (2017), CCS '17, ACM, pp. 103–117.