# Deep Note: Can Acoustic Interference Damage the Availability of Hard Disk Storage in Underwater Data Centers?

Jennifer Sheldon*, Weidong Zhu*, Adnan Abdullah†, Kevin Butler*, Md Jahidul Islam† and Sara Rampazzi*
Computer and Information Science and Engineering*, University of Florida
Electrical and Computer Engineering†, University of Florida
{jsheldon,weidong.zhu,adnanabdullah,butler,mdjahiduislam,srampazzi}@ufl.edu

## ABSTRACT

The growing worldwide attention toward large-scale subsea data centers has garnered substantial interest from commercial entities which have built and deployed underwater prototypes since 2015. These data centers utilize hard disk drives (HDDs) as a cost-effective method of data storage. However, researchers have demonstrated that acoustic waves can affect the availability and integrity of HDDs and applications that rely on them. These studies are all conducted in air on commercial laptops, hence their applicability and implications in submerged environments remain unexplored. In this position paper, we investigate potential vulnerabilities of storage devices deployed in underwater data centers and subsea storage platforms against targeted acoustic attacks. Based on our initial investigation of a simplified scenario, a victim HDD deployed in an enclosed submerged container is especially vulnerable to those acoustic attacks, which at frequencies ranging from 300 Hz 1300 Hz can result in up to 100% throughput loss and application crashes. Based on these findings, we argue that further study is necessary to assess underwater storage system security and develop effective defenses against overlooked acoustic attacks.

## CCS CONCEPTS

• **Security and privacy → Hardware attacks and countermeasures**; **Database and storage security**.


*HotStorage '23, July 9, 2023, Boston, MA, USA*

ACM ISBN 979-8-4007-0224-2/23/07…$15.00
https://doi.org/10.1145/3599691.3603403

## KEYWORDS

Hardware attacks; Storage security; Underwater data center.

**ACM Reference Format:**
Jennifer Sheldon*, Weidong Zhu*, Adnan Abdullah†, Kevin Butler*, Md Jahidul Islam† and Sara Rampazzi* . 2023. Deep Note: Can Acoustic Interference Damage the Availability of Hard Disk Storage in Underwater Data Centers?. In *15th ACM Workshop on Hot Topics in Storage and File Systems (HotStorage '23), July 9, 2023, Boston, MA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3599691.3603403

## 1 INTRODUCTION

Companies such as Microsoft and several offshore businesses have begun planning and testing prototypes of underwater data centers around the world [22, 34, 35] to keep up with the increasing demand, but also to reduce cooling costs and save emissions. This recent trend is likely to grow exponentially as the market size is projected to reach 74.02 billion by the year 2030 [42]. With surrounding water serving as a natural coolant [11], subsea data centers deploy groups of disks including hard disk drives (HDDs) [33] housed in a metal container filled with nitrogen gas to prevent corrosion [22, 29]. HDDs in particular remain extensively used in data centers due to their lower cost-to-storage-capacity ratio compared to other storage devices such as SSDs [3, 26]. However, over the last decade, researchers have demonstrated how these storage devices are vulnerable to multiple acoustic attacks, including side-channels [24], covert channels [18], and, in particular, acoustic injection attacks [6].

Despite these known vulnerabilities, storage system security against acoustic attacks has not been thoroughly explored in the underwater domain, and the ramifications of such attacks have not been considered in the context of data center security. Prior underwater security works focus on disrupting underwater acoustic networks (UWAs) by packet flooding and wormhole attacks on the network routing layer [13] and signal jamming [48, 50, 51], but these

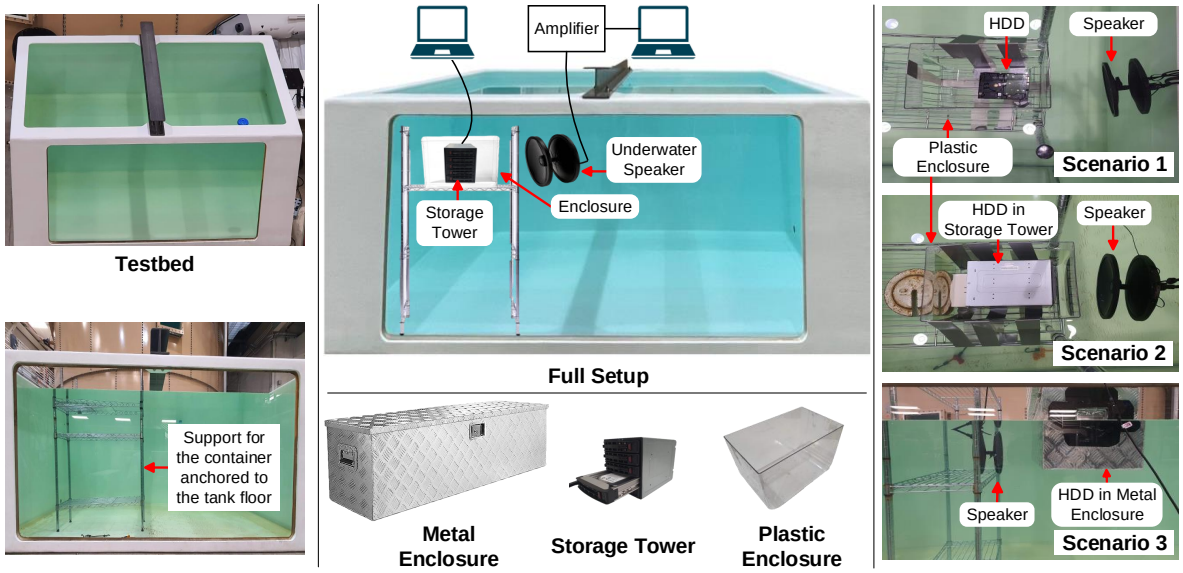



**Figure 1: Experimental setup used in three test scenarios. The victim HDD is placed in a submerged plastic container (Scenarios 1 and 2) or a metal container (Scenario 3) anchored to the tank floor. An additional storage tower is used in Scenario 2 and 3 to place the victim HDD (simulating a datacenter rack).**

studies only investigate vulnerabilities of acoustic communication. Prior works on data center security focus instead on traditional network attacks and defenses [7, 8, 31], and malware analysis and detection [2, 9, 14, 16, 25]. However, these works do not consider physical signal injection attacks that can alter data centers' internal functioning without the need for tampering with the network communication, gaining physical access to the storage systems, or executing malicious software. We attempt to address this knowledge gap by exploring the hardware security aspects, i.e., whether acoustic injection attacks deployed in data centers are feasible and whether these attacks can damage the availability of data center applications that rely on storage systems.

To demonstrate the feasibility of this class of attacks, our preliminary analysis simplifies the victim system using a container submerged in water which contains the victim HDD in various scenarios (see Figure 1). Our findings show that transmitting acoustic waves at specific frequencies (between 300 Hz and 1000 Hz) from an underwater speaker causes the victim HDD's throughput to drop to zero (comparable to acoustic attacks witnessed in air [6]). Furthermore, we show how prolonged attacks can crash crucial processes (e.g., filesystems), server Operating Systems, and applications such as those accessing databases. This phenomenon occurs because acoustic waves induce mechanical vibrations in the HDD and container structure; these vibrations jostle the HDD's internal components, preventing reading and writing operations.

Despite our simplified setup, our proof-of-concept analysis demonstrates how it is possible to remotely interfere with the correct functionalities of high-traffic storage systems deployed in closed, isolated, underwater environments without tampering with the victim system or leveraging malware and network attack vectors. In summary, we make the following contributions:

- We investigate the feasibility of underwater acoustic attacks against HDDs in several simplified scenarios.
- We show how such attacks on standard data center software such as Ext4 file systems, Ubuntu servers, and RocksDB database applications can reach up to 100% throughput loss and crashes within ~81 seconds.
- We argue the need for future research including models, testbeds, and methodologies for exploring security challenges of subsea storage platforms.

## 2 BACKGROUND & RELATED WORK

### 2.1 Acoustic Threats Against HDDs

A typical HDD consists of disk platters, a head stack assembly, read/write (r/w) heads, and a spindle motor [4]. Data is organized into tracks on the platter, which the spindle motor rotates. The head stack assembly positions the r/w head above the desired track to r/w data. The r/w head position must remain within a threshold distance (determined by whether the operation is a read or write) from the center of the track for successful data access.

Bolton et al. [6] et al. demonstrate how acoustic waves can undermine the availability and integrity of hard disk

drives used in laptops and embedded systems. The team found that audible sound waves transmitted in the proximity of a hard disk can cause the r/w head to vibrate outside of the r/w tolerance thresholds and ultrasonic waves can cause shock sensors located in the hard drives to erroneously detect the jostling of the device and cause the r/w head to park. This, in turn, causes failures of software applications (e.g., security cameras) and laptops' Operating Systems due to the impossibility of reading and writing to the storage system, including provoking physical damage and data corruption.

**Causality.** Rigid objects generally have a natural frequency or set of frequencies at which they vibrate when force is applied [19]. These frequencies are usually called *resonant frequencies*. The acoustic waves used in Bolton et al. [6] attacks match the resonant frequency of the target victim device (e.g., the HDD) to amplify the mechanical vibrations [19]. Several previous works have explored attacks which use resonant frequencies to cause high-amplitude vibrations to interfere with the functioning of sensors and hardware components such as accelerometers [45], drone gyroscopes [40], and inertial sensors in cameras [21]. In this work, we investigate the feasibility of acoustic attacks in the underwater domain and characterize potential consequences on storage devices in submerged enclosed environments.

## 2.2 Acoustic Signal Propagation in Water

Acoustic signals are longitudinal waves that propagate through a medium with changes in pressure [36]. When an object vibrates, pressure is applied upon the surrounding medium, hence the particles vibrate as well. The energy of vibration is passed from one particle to another, creating the acoustic wave. Acoustic sources can be categorized in terms of their frequency and amplitude. High amplitude means a vibrating particle is displaced more from its rest condition which creates a loud sound. The instantaneous pressure that a sound source puts on the unit area is given by, $p(t) = d \cdot c \cdot v$, where $d$ is the density of the medium and $c$ and $v$ is the velocities of the sound wave and medium particle, respectively [28].

Typically, it is convenient to express the pressure in a logarithmic unit as Sound Pressure Level (SPL) which is the ratio of a measured level to a reference level. Sound wave travels approximately 4 times faster in water than air because the water medium is much denser than air [28]. Also, water molecules are more compressible which helps the wave to travel longer distances than in air. In air and water mediums, reference SPL levels are different [37], thus, generally, from a given SPL measurement in air, we can approximate the equivalent sound pressure level in water as $SPL_{Water} = SPL_{Air} + 20 \cdot \log \frac{20\,\mu Pa}{1\mu Pa} = SPL_{Air} + 26\,dB$. The sound attenuation at a certain distance from a sound source, which can be represented by an absorption coefficient in dB/km, is a function of the transmitted sound frequency as well as water temperature, pressure, and salinity [15].

# 3 THREAT MODEL & ATTACK OVERVIEW

The goal of the adversary is to disrupt the functioning of a target victim (e.g., an underwater data center) by interfering with its storage system using sound waves. In other words, we consider two potential attackers' objectives distinguished by severity. In the first, the attacker intends to provoke a controlled throughput loss of a single or multiple HDDs located in a submerged enclosure for a specific amount of time to induce applications or process delays. In the second, the attacker intends to prolong the attack to cause operating systems' crucial processes (e.g., filesystems) and applications to crash due to the unavailability of the storage systems. In both scenarios, we consider an attacker capable of generating underwater acoustic waves of a controllable frequency and amplitude (e.g., using a commercially available underwater speaker and amplifier). The attacker must also know the location to point the sound source to the target enclosure.

Note that, to achieve a successful attack, the attacker should perform a frequency sweep as described in previous work [6, 45, 46] to understand which vulnerable frequencies the target is susceptible to. This analysis is achievable, for example, by remotely varying the attack sound waves and observing resultant delays in online applications that use the target data center or by studying similar storage devices and their resonance frequencies.

We also assume that the adversary cannot tamper with any hardware or software of the target system, nor connect or attach equipment to the system's enclosure. Also, we don't consider the use of malware or network attacks that could directly affect the functioning of the target system.

**Research Problem.** Previous works on acoustic attacks against HDDs focus on sound transmission in the air to affect and eavesdrop on information from commercial target devices (e.g., laptops) [6, 24, 39]. In this work, we focus on investigating how acoustic injection attacks can be used to undermine complex data center storage systems and their applications deployed in harsh environments. Our analysis aims to open new research directions to protect these systems from such unexplored threats, by answering the following research questions: *Can an attacker use sound to damage the availability of HDDs housed in underwater data centers? If so, what effects might such attacks have on the crucial processes and applications in data centers that rely on storage systems? How does the underwater environment improve or hinder the attack's feasibility and effectiveness?*

**Table 1: Read and Write operations throughput of HDD when an acoustic attack occurs at varied distances; the HDD and container are deployed in Scenario 2.**

| Distance | Throughput (MB/s) | | Latency (ms)* | |
|---|---|---|---|---|
| | Read | Write | Read | Write |
| No Attack | 18.0 | 22.7 | 0.2 | 0.2 |
| 1 cm | 0 | 0 | - | - |
| 5 cm | 0 | 0 | - | - |
| 10 cm | 12.6 | 0.3 | 0.3 | - |
| 15 cm | 17.6 | 2.9 | 0.2 | 4.0 |
| 20 cm | 17.6 | 21.1 | 0.2 | 0.2 |
| 25 cm | 18.0 | 22.0 | 0.2 | 0.2 |

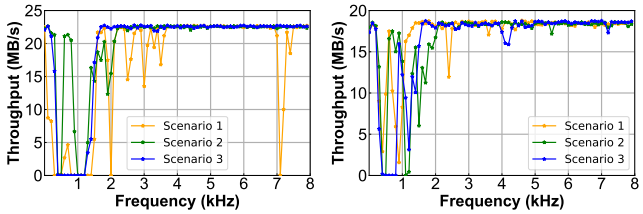
(*) The "-" symbol indicates no response.

## 4 CASE STUDY

This section presents a proof-of-concept preliminary analysis to demonstrate the potential feasibility of deploying the attack described in Section 3 in underwater scenarios and start addressing our research questions. To achieve this, we first built a simplified testbed to simulate the baseline conditions of a submerged data center.

**Experimental Setup.** Figure 1 shows the setup used in our underwater experimental analysis. We select a 500 GB Seagate Barracuda HDD [38] as the victim storage drive as a proof-of-concept. Then, we perform our experiments separately in metal (aluminum) and plastic containers submerged in water to simulate the water barrier between HDDs and underwater sound sources in the real world. The containers are anchored on a metal shelf in contact with the bottom of the water tank similarly to submerged data centers [49].

**Evaluation Scenarios.** We perform the acoustic attack in three scenarios: (*i*) in Scenario 1, the hard disk is placed directly on the bottom of a hard plastic container, (*ii*) in Scenario 2, it is held in the second level from the bottom of a Supermicro CSE-M35TQB 5-in-3 Hot Swap SAS/SATA storage tower [43] to simulate a rack, (*iii*) and in Scenario 3, it is held in the aforementioned tower in an aluminum container. We vary the scenarios to understand the attack's feasibility under different basic conditions. In each scenario, the container is submerged to cover the entire height of the tower and hard disk sits below the water surface level. To deliver the audio signal, we use a commercial Clark Synthesis AQ339 Diluvio underwater speaker [10] and a TOA amplifier [44] connected to a laptop generating output sine wave signals using GNU radio [17]. In all our scenarios, we transmit a 140 dB SPL acoustic signal (similar to the transmitting acoustic power used on air by previous work [6]), which is achievable by commercially-available swimming pool underwater speakers to play music, and significantly below 220 dB SPL pressure level typically used in underwater sonars [5]).




(a) Sequential Write (b) Sequential Read

**Figure 2: The HDD read/write throughput during an acoustic attack at different frequencies in all scenarios.**

**Metrics.** We leverage Flexible I/O Tester (i.e., FIO [20]) to evaluate the I/O throughput and latency of the hard disk with sequential read and sequential write workloads as performance metrics (4KB data access granularity). We then implement a popular database, RocksDB [32], used by server applications that need low latency database access key-value pairs. We monitor the performance changes with the *db_bench* benchmark with a *readwhilewriting* workload, which is a standard workload provided by RocksDB.

### 4.1 Frequency Analysis

To identify the effective frequencies for our underwater scenarios, we perform a frequency sweep starting at 100 Hz and ending at 16.9 KHz and narrowing to 50 Hz increments between vulnerable frequencies with the speaker at 1 cm from the container (the HDD is located in the enclosure at 3 cm from the side facing the speaker as in Figure 1). We then monitor the I/O throughput variation, meaning the storage device's capability for serving incoming I/O requests when FIO performs sequential read and write workloads.

**Results and Observations.** Figure 2 shows the throughput variation of the HDD when the acoustic attack happens at different frequencies. The results show that the throughput losses occur in all three scenarios at the frequency range between 300 Hz to 1.7 KHz. Moreover, the acoustic attack generates major throughput degradation during write operations compared to read. We believe this is because the read operations have a wider tolerance threshold than write operations, which has also been verified in previous work [6]. For instance, in Scenario 3, the write throughput degrades from 22.7 MB/s to 0 MB/s at frequencies between 300 Hz to 1.3 KHz, whereas the read throughput drop from 18.0 MB/s to 0 MB/s when the acoustic frequency ranges from 300 Hz to 800 Hz. Finally, the metal container Scenario 3 presents attack effectiveness from 300 Hz to 1.3 KHz. Our analysis also highlights how the container material is a critical factor due to the performance degradation variance in plastic and metal containers.

**Table 2: Throughput and I/O rate of RocksDB when an underwater acoustic attack occurs at varied distances; the HDD and container are deployed in Scenario 2.**

| Distance | Throughput (MB/s) | I/O Rate (x100,000 ops/s) |
|---|---|---|
| No Attack | 8.7 | 1.1 |
| 1 cm | 0 | 0 |
| 5 cm | 0 | 0 |
| 10 cm | 0 | 0 |
| 15 cm | 3.7 | 0.9 |
| 20 cm | 8.6 | 1.1 |
| 25 cm | 8.6 | 1.1 |

## 4.2 Range Testing

To evaluate the maximum achievable distance from the enclosure at which the attack can cause a measurable throughput loss in our simplified testbed, we select Scenario 2 as the more realistic scenario, and we transmit a sound wave at 650 Hz (which presents a significant performance degradation as shown in Table 2). We then adjust the distances between the container and the speaker to observe the performance changes during our underwater acoustic attack.

**Results and Observations.** Table 1 shows the FIO read and write throughput and latency of the drive at different distances from the container. We tested our underwater acoustic attack by positioning the speaker at the minimum distance of 1 cm from the enclosure to pursue a proof-of-concept remote attack. Note that mechanical vibrations can be induced as well by direct contact with the enclosure (0 cm).

The maximum effective distance achievable by our attack with a commercially available speaker is 25 cm. Within this range, the attack can successfully degrade the performance of the victim HDD. Our attack achieves 0 MB/s throughput without serving the I/O requests (i.e., no response) at 1 cm and 5 cm. This demonstrates how the sound wave attenuates for far distances and throughput is less impacted by the attack. Note that a more sophisticated attacker with a powerful speaker (e.g., military-grade marine loudspeakers) can achieve further distances by increasing the source volume to account for sound absorption. For example, water at a 50 m depth in the Baltic Sea was found to attenuate a 500 Hz signal by 0.038 dB/km [47]. Attackers can raise the source dB SPL based on the distance from the victim enclosure and approximating the absorption coefficient [15].

## 4.3 Performance Testing on RocksDB

To validate the performance degradation of our attack in real-world applications, we evaluate the performance of RocksDB with the metrics described in Section 4.2.

**Results and Observations.** Table 2 shows the bandwidth and I/O rate of RocksDB in attack Scenario 2 under various distances. The results show 100% throughput degradation without processing any I/O operations within 10 cm between the speaker and the enclosure. Similarly to the results of Table 1, this indicates that the functionality of RocksDB will be blocked due to inaccessible storage with zero r/w operation throughput. This preliminary experiment indicates the potential severity of the impact on server processes.

**Table 3: Crashes in real-world applications. The HDD and container are deployed in Scenario 2.**

| Application | Description | Time to Crash |
|---|---|---|
| Ext4 [12] | Journaling filesystem | 80.0 seconds |
| Ubuntu [1] | Ubuntu server 16.04 | 81.0 seconds |
| RockDB [32] | Key-value database | 81.3 seconds |

## 4.4 Software Crashes

Underwater acoustic attacks, prolonged over a certain amount of time, can potentially permanently paralyze the running of real-world applications. As a proof-of-concept, we deploy an underwater acoustic attack on four critical processes, including a filesystem (i.e., Ext4 [12]), an Server Operating System (i.e., Ubuntu 16.04 [1]), and RocksDB to evaluate potential crashes. We use the best-attacking parameters by transmitting at 650 Hz and 140 dB SPL acoustic waves at a distance of 1 cm based on our experiments in Section 4.1 and Section 4.2. We deem a crash happens when the application stops running with an error output.

**Results and Observations.** Table 3 shows real-world crashes of Ext4, Ubuntu, and RocksDB with an average crash time of 80.8 seconds. We believe this happens because the induced vibrations cause inaccessibility of the drive for enough time to cause a crash. We also observe the error output of each application when crashes happen. Ext4 terminates its service with a Journal Block Device (JBD) error in code $-5$, which occurs because the journal superblock cannot be updated due to the blocked I/O. Ubuntu crash happens with an indication of inability to access all files, including regular files and common Linux commands, such as *ls*. Moreover, the reported errors from *dmesg* indicate that the buffer I/O error on the storage device leads to OS crashing. Finally, RocksDB crashes with a failure of *sysc_without_flush_called*. Since the drive stops serving I/O requests, the newly arrived key-value pairs written into the write-ahead log (WAL) cannot be persisted into the drive, leading to a crash in RocksDB.

# 5 CHALLENGES & OPEN PROBLEMS

In this section, we discuss some challenges and open problems introduced by our preliminary experiments.

**Water Conditions.** In water, sound speed is affected by temperature, salinity, and water depth [23, 30]. These factors can vary considerably for the same attack if it is mounted from a long distance (e.g., an attacker places their setup

near the surface of the ocean to target a data center in deep water). For instance, in our experiments, the water in the tank remained at a nearly constant room temperature. As temperature increases, sound speed increases [23], which can augment the attacker range. Our experiments were conducted in the freshwater of constant salinity. Salinity affects the speed of sound (higher salinity increases speed), so this must be considered when evaluating the security of subsea data centers. Finally, Microsoft placed its test underwater data center about 36 m underwater [22], and the Offshore Oil Engineering Company plans to place its data center at about 20 m depth [35]. Increasing depth increases sound speed [23] and, consequently, might increase the attack range. Further investigation is necessary to understand the interactions of attack parameters related to the speed of sound in water.

**Effective Range.** Sound travels faster underwater than in air. Previous studies in air have mounted acoustic attacks on HDDs at distances of 10 cm and hypothesized potential distances above 1 mile using specialized equipment [6]. Attackers capable to emit sound at higher sound pressure levels (e.g., military-grade equipment) might substantially increase the attack's success over wide distances.

**Data Center Structure and HDD types.** The success of acoustic attacks depends upon reaching sufficient vibration amplitude in the victim HDDs. Different hard disks, materials between the HDD and the sound source such as the steel walls of a data center [11], the nitrogen gas within the data center casing [22], structures such as underwater cables to maintain the data center position, and the rack containing the HDDs, may attenuate the signal or amplify the induced mechanical vibrations.

**In-air Defenses.** Bolton et al. [6] and other previous works [21, 45, 46] suggest various defenses against acoustic attacks, including augmented feedback controllers, and firmware modifications of the storage device. Other potential defenses include using acoustically adsorbing materials [27] or dampening mechanical vibrations [41] to attenuate the vibration. However, these defenses may cause overheating as observed in the in-air case [6]. Further research can evaluate whether such suggested defenses can sufficiently defend against underwater acoustic attacks.

## 5.1 Open Problems & Future Works

Our preliminary results show that acoustic attacks might be achievable underwater, and they will pose a greater security risk as more companies are planning to submerge their data centers. Our preliminary analysis, even if limited to proof-of-concept scenarios, unveils new attack vectors that might undermine the availability of storage devices housed in underwater data centers. We advocate that further research needs to be done in the underwater domain in order to understand and potentially defend against these attacks before they can cause serious harm. Open problems we are planning to address include (*i*) the development of testbeds to better represent the conditions outlined in Section 5; (*ii*) extensive evaluation of the attacker's capabilities in terms of the parameters listed in Section 5; and (*iii*) evaluation of potential underwater defense strategies.

## ACKNOWLEDGEMENTS

This research was supported in part by the National Science Foundation (NSF) under CNS-2054911, the Air Force Office for Scientific Research under FA8650-19-1-1741, and gifts from Facebook and Texas Instrument. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

## REFERENCES

[1] 2021. Install Ubuntu Server 16.04. https://ubuntu.com/tutorials/install-ubuntu-server-1604#1-overview.

[2] Mahmoud Abdelsalam, Ram Krishnan, Yufei Huang, and Ravi Sandhu. 2018. Malware detection in cloud infrastructures using convolutional neural networks. In *2018 IEEE 11th international conference on cloud computing (CLOUD)*. IEEE, 162–169.

[3] Adrien Ramirez. [n. d.]. What's The difference Between A Hard Drive And A Solid State Drive? https://reviewed.usatoday.com/laptops/features/ssd-vs-hdd.

[4] Alexander Gillis and Sarah Wilson. 2021. Hard Disk Drive (HDD). https://www.techtarget.com/searchstorage/definition/hard-disk-drive#:~:text=Hard%20disk%20drive%20components%20include,arm%20and%20read%2Fwrite%20head.

[5] A.R. Collins. [n. d.]. Underwater sound pressure levels. https://www.arc.id.au/SoundLevels.html.

[6] 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.

[7] Ming-Hung Chen, Jyun-Yan Ciou, I-Hsin Chung, and Cheng-Fu Chou. 2018. FlexProtect: A SDN-based DDoS attack protection architecture for multi-tenant data centers. In *Proceedings of the International Conference on High Performance Computing in Asia-Pacific Region*. 202–209.

[8] Yu-Jia Chen, Li-Chun Wang, and Chen-Hung Liao. 2015. Eavesdropping prevention for network coding encrypted cloud storage systems. *IEEE Transactions on Parallel and Distributed Systems* 27, 8 (2015), 2261–2273.

[9] Keywhan Chung, Zbigniew T Kalbarczyk, and Ravishankar K Iyer. 2019. Availability attacks on computing systems through alteration of environmental control: smart malware approach. In *Proceedings of the 10th ACM/IEEE international conference on cyber-physical systems*. 1–12.

[10] Clark Synthesis. [n. d.]. AQ339 Diluvio Underwater Loudspeaker. https://clarksynthesis.com/aq339/.

[11] Ben Cutler, Spencer Fowers, Jeffrey Kramer, and Eric Peterson. 2017. Dunking the data center. *IEEE Spectrum* 54, 3 (2017), 26–31. https://doi.org/10.1109/MSPEC.2017.7864753

[12] David Both. 2021. An introduction to Linux's EXT4 filesystem. https://opensource.com/article/17/5/introduction-ext4-filesystem.

[13] Yangze Dong, Hefeng Dong, and Gangqiang Zhang. 2014. Study on denial of service against underwater acoustic networks. *J. Commun.* 9, 2 (2014), 135–143.

[14] Andreas Fischer, Thomas Kittel, Bojan Kolosnjaji, Tamas K Lengyel, Waseem Mandarawi, Hermann Meer, Tilo Müller, Mykola Protsenko, Hans P Reiser, Benjamin Taubmann, et al. 2015. CloudIDEA: A Malware Defense Architecture for Cloud Data Centers. In *Proceedings of the Confederated International Conferences on On the Move to Meaningful Internet Systems: OTM 2015 Conferences-Volume 9415*. 594–611.

[15] FH Fisher and VP Simmons. 1977. Sound absorption in sea water. *The Journal of the Acoustical Society of America* 62, 3 (1977), 558–564.

[16] Xing Gao, Guannan Liu, Zhang Xu, Haining Wang, Li Li, and Xiaorui Wang. 2020. Investigating security vulnerabilities in a hot data center with reduced cooling redundancy. *IEEE Transactions on Dependable and Secure Computing* 19, 1 (2020), 208–226.

[17] GNU Radio Project. [n. d.]. GNU Radio. https://www.gnuradio.org/

[18] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici. 2017. Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise ('DiskFiltration'). In *22nd European Symposium on Research in Computer Security, (ESORICS 2017)*. Springer, 98–115.

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

[20] Jens Axboe. [n. d.]. Flexible I/O Tester. https://github.com/axboe/fio.

[21] Xiaoyu Ji, Yushi Cheng, Yuepeng Zhang, Kai Wang, Chen Yan, Wenyuan Xu, and Kevin Fu. 2021. Poltergeist: Acoustic adversarial machine learning against cameras and computer vision. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 160–175.

[22] John Roach. 2020. Microsoft finds underwater datacenters are reliable, practical and use energy sustainably. https://news.microsoft.com/source/features/sustainability/project-natick-underwater-datacenter/.

[23] William Kuperman and Philippe Roux. 2007. Underwater acoustics. *Springer Handbook of Acoustics* (2007), 149–204.

[24] Andrew Kwong, Wenyuan Xu, and Kevin Fu. 2019. Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone. In *2019 IEEE Symposium on Security and Privacy (SP)*. 905–919. https://doi.org/10.1109/SP.2019.00008

[25] Antonio Libri, Andrea Bartolini, and Luca Benini. 2020. pAElla: Edge AI-based real-time malware detection in data centers. *IEEE Internet of Things Journal* 7, 10 (2020), 9589–9599.

[26] Litton Power. 2021. The Ongoing Value of Hard Disk Drives in Data Centers. https://www.enterprisestorageforum.com/news/hard-disk-drives-data-centers/.

[27] Tiara J Lu, Audrey Hess, and MF Ashby. 1999. Sound absorption in metallic foams. *Journal of applied physics* 85, 11 (1999), 7528–7539.

[28] Xavier Lurton. 2002. *An introduction to underwater acoustics: principles and applications*. Vol. 2. Springer.

[29] Mark Shaw and Martin Goldstein. 2015. Open CloudServer JBOD specification. https://www.opencompute.org/documents/microsoft-ocs-v1-jbod-blade.

[30] Herman Medwin. 1975. Speed of sound in water: A simple equation for realistic parameters. *The Journal of the Acoustical Society of America* 58, 6 (1975), 1318–1319.

[31] Bi Meng, Wang Andi, Xu Jian, and Zhou Fucai. 2017. Ddos attack detection system based on analysis of users' behaviors for application layer. In *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Vol. 1. IEEE, 596–599.

[32] Meta. [n. d.]. A persistent key-value database for fast storage environments. https://rocksdb.org/.

[33] Mukund Agarwal. [n. d.]. Microsoft's Project NATICK(Underwater Data Center)). https://vdocuments.mx/microsofts-project-natickunderwater-datacentre.html?page=1.

[34] Peter Judge. 2022. Subsea Cloud announces three underwater data center projects. https://www.datacenterdynamics.com/en/news/subsea-cloud-announces-three-underwater-data-center-projects/.

[35] Peter Judge. 2022. Work begins on Chinese underwater data center. https://www.datacenterdynamics.com/en/news/work-begins-on-chinese-underwater-data-center/.

[36] Allan D Pierce. 2019. *Acoustics: an introduction to its physical principles and applications*. Springer.

[37] William John Richardson. 1991. *Effects of noise on marine mammals*. Number 93. The Region.

[38] Seagate. 2015. Desktop HDD Product Manual. https://www.seagate.com/www-content/product-content/desktop-hdd-fam/en-us/docs/100768625b.pdf.

[39] Mohammad Shahrad, Arsalan Mosenia, Liwei Song, Mung Chiang, David Wentzlaff, and Prateek Mittal. 2018. Acoustic denial of service attacks on hard disk drives. In *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security*. 34–39.

[40] 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.

[41] Leslie Howard Sperling. 1990. Sound and vibration damping with polymers: Basic viscoelastic definitions and concepts. ACS Publications.

[42] Straits Research. [n. d.]. Data Center Storage Market Size is projected to reach USD 74.02 Billion by 2030, growing at a CAGR of 4.4%: Straits Research. https://www.globenewswire.com/news-release/2023/03/14/2626744/0/en/Data-Center-Storage-Market-Size-is-projected-to-reach-USD-74-02-Billion-by-2030-growing-at-a-CAGR-of-4-4-Straits-Research.html.

[43] Supermicro. [n. d.]. Mobile Rack CSE-M35TQB. https://www.supermicro.com/en/products/accessories/mobilerack/CSE-M35TQB.php.

[44] TOA Electronics. [n. d.]. Mixer / Amplifier - 120W. https://toaelectronics.com/product/BG-2120.

[45] 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.

[46] Yazhou Tu, Sara Rampazzi, Bin Hao, Angel Rodriguez, Kevin Fu, and Xiali Hei. 2019. Trick or heat? Manipulating critical temperature-based control systems using rectification attacks. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2301–2315.

[47] Camiel AM van Moll, Michael A Ainslie, and Robbert van Vossen. 2009. A simple and accurate formula for the absorption of sound in seawater. *IEEE Journal of Oceanic Engineering* 34, 4 (2009), 610–616.

[48] Peng Xiao, Michael Kowalski, Daniel McCulley, and Michael Zuba. 2015. An experimental study of jamming attacks in underwater acoustic communication. In *Proceedings of the 10th International Conference on Underwater Networks & Systems*. 1–5.

[49] Yevgeniy Sverdlik. [n. d.]. Mcrosoft's Project NATICK (Underwater Datacenter). https://www.datacenterknowledge.com/archives/2017/01/09/microsoft-wants-to-patent-an-underwater-data-center-reef.

[50] Michael Zuba, Zhijie Shi, Zheng Peng, and Jun-Hong Cui. 2011. Launching denial-of-service jamming attacks in underwater sensor networks. In *Proceedings of the 6th International Workshop on Underwater Networks*. 1–5.

[51] Michael Zuba, Zhijie Shi, Zheng Peng, Jun-Hong Cui, and Shengli Zhou. 2015. Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks. *Security and Communication Networks* 8, 16 (2015), 2635–2645.