Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems

Connor Bolton[1], Sara Rampazzi[1], Chaohao Li[2], Andrew Kwong[1], Wenyuan Xu[2], and Kevin Fu[1]

[1]University of Michigan
[2]Zhejiang University

***Abstract*—Intentional acoustic interference causes unusual errors in the mechanics of magnetic hard disk drives in desktop and laptop computers, leading to damage to integrity and availability in both hardware and software such as file system corruption and operating system reboots. An adversary without any special purpose equipment can co-opt built-in speakers or nearby emitters to cause persistent errors. Our work traces the deeper causality of these risks from the physics of materials to the I/O request stack in operating systems for audible and ultrasonic sound. Our experiments show that audible sound causes the head stack assembly to vibrate outside of operational bounds; ultrasonic sound causes false positives in the shock sensor, which is designed to prevent a head crash.**

The problem poses a challenge for legacy magnetic disks that remain stubbornly common in safety critical applications such as medical devices and other highly utilized systems difficult to sunset. Thus, we created and modeled a new feedback controller that could be deployed as a firmware update to attenuate the intentional acoustic interference. Our sensor fusion method prevents unnecessary head parking by detecting ultrasonic triggering of the shock sensor.

Keywords*—*hard disk drives, embedded security, hardware security, denial of service.

I. Introduction

Availability is the most important security property of a consumer hard disk drive (HDD). Without availability, it is difficult to meaningfully consider preservation of security properties such as confidentiality and integrity. Our work explores to what extent an adversary can intentionally damage HDDs with malicious audible and inaudible acoustic waves (Figure 1) and what are the limits of defenses.

Magnetic HDDs remain common [1] because of the long tail of legacy systems and the relatively inexpensive cost for high capacity storage. However, sudden movement can damage the hard drive or corrupt data because of the tight operating constraints on the read/write head(s) and disk(s). Thus, modern drives use shock sensors to detect such movement and safely park the read/write head. Previous research has indicated that loud audible sounds, such as shouting or fire alarms, can cause drive components to vibrate, disturbing throughput [2], [3], [4], [5]. Audible sounds can even cause HDDs to become unresponsive [6].

What remains a mystery is *how* and *why* intentional vibration causes bizarre malfunctions in HDDs and undefined behavior in operating systems. In our work, we explore how sustained, intentional vibration at resonant frequencies can cause permanent data loss, program crashes, and unrecoverable physical loss in HDDs from three different vendors (Figure 2). We also propose, simulate, and implement several defenses against such attacks on HDDs. Moreover, our research addresses the gap in knowledge in how ultrasound affects HDDs by triggering the sensor, a different causality from audible interference. Our contributions explore the physics of cybersecurity [7] for availability and integrity of systems that depend on hard disk drives:

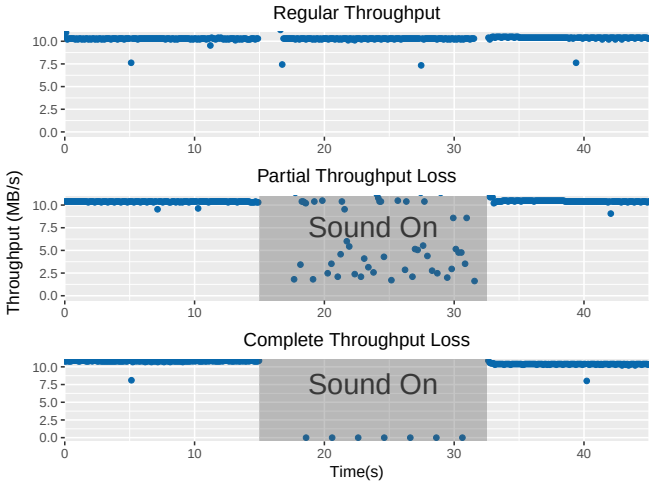


Fig. 1. Vibration can interrupt disk I/O. Three plots show a Western Digital Blue WD5000LPVX drive under normal operation (top), partial throughput with vibration induced by a 5 kHz tone at 115.3 dB SPL (middle), and halting of writes with 5 kHz tone at 117.2 dB SPL (bottom).

- **Physical Causality:** How intentional audible and ultrasonic sounds cause physical errors in hard disk drives.
- **System Consequences:** How intentional physical errors in the hard disk drive lead to system level errors.
- **Defenses:** We simulate, implement, and propose defenses that can prevent damage to availability.

Physical Causality: Our component-level experiments and simulations provide evidence attributing the root causes of the hard disk drive errors. Ultrasonic waves can alter the

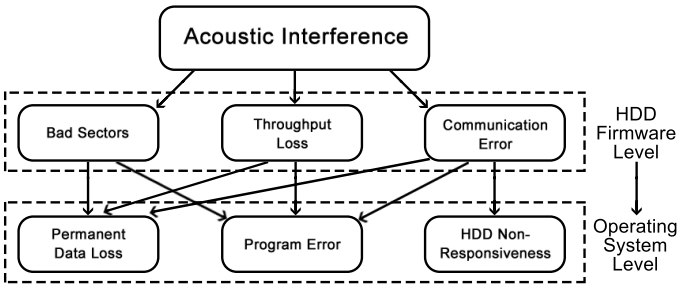


Fig. 2. Intentional acoustic interference causes HDD firmware errors, which in turn cause system-level errors and other undefined application-level behavior. An arrow indicates a confirmed cause and effect relationship.

HDD shock sensor's output, causing a drive to unnecessarily park its head. Audible tones can vibrate the read/write head(s) and disk outside of operational bounds. Both of these different methods result in improper function of the drive.

System Consequences: Our case studies show that an attacker can use the effects from hard disk drive vulnerabilities to launch system level consequences such as crashing Windows on a laptop using the built-in speaker and preventing surveillance systems from recording video. We delve into the details of the Windows and Linux operating systems to uncover the root causes of the crash in the I/O request stack.

Defenses: We simulate, discuss, and implement defenses against both hard disk drive vulnerabilities. In our simulation, we show how a new feedback controller can attenuate the physical effect on the head stack assembly. We implement and evaluate noise attenuating materials as a defense. Finally, we propose sensor fusion as a means to detect malicious acoustic signals, allowing the drive to operate when attacked by ultrasonic signals.

II. Background

A. Threat Model

Our work assumes an adversary that uses vibration to interfere with a HDD on a target machine, typically induced through use of a speaker. The adversary may catalog frequencies that are most effective for a given model of hard drive to speed up the attack. We foresee two distinct types of delivery: a *self stimulation attack* [8] and a *physical proximity attack*.

Self-Stimulated Attacks. An adversary can attack a HDD by inducing vibration via acoustic emitters built into the victim system (or a nearby system). In this case an adversary would temporarily control an emitter in the system though some means. The attack is more likely to succeed when the emitter is powerful and/or very close to the victim.

A self-stimulated attack may use a standard phishing attack, malicious email, or malicious javascript to deliver audio to a laptop's speakers. Most laptops have speakers and the ability to browse the Internet. Modern browsers support JavaScript and HTML5, both of which are capable of playing audio without user permission. Therefore, should a victim visit a page owned by the attacker, the attacker would be able to play audio over the victim's speakers.

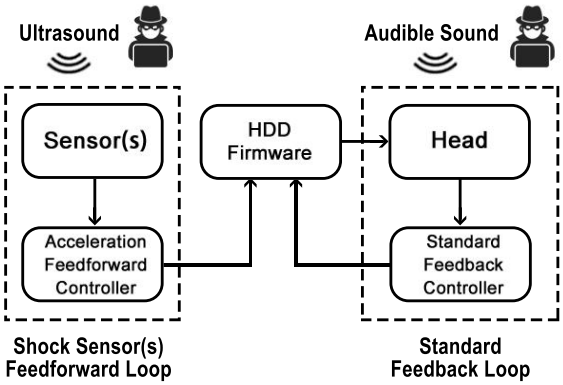


Fig. 3. Acoustics disturb the HDD head stack assembly and shock sensor. Modern HDDs use sensor-driven feedforward controllers to adjust the head's position. Our work finds that ultrasonic vibration triggers false positives for head parking; audible tones vibrate the head—causing poor positioning.

The frequency response of a built-in speaker may limit the ability for an adversary to deliver ultrasonic attacks, but some speakers may be able to deliver ultrasonic or near ultrasonic tones.

Physical Proximity Attacks. An attacker can induce vibration using a speaker near the victim system. The attacker must either control a speaker close to the victim HDD, or place a speaker in the proximity of the system. The case of controlling a speaker close to the victim HDD is similar to that of the self-stimulated attack. An example of this would be the attacker controlling an AM or FM station of a radio playing sound near the victim HDD with the desired signal.

When the attacker is able to physically place the speaker, the attacker can choose a speaker with the desired frequency range (audible, near ultrasound, or ultrasound). In addition, the attacker can choose non-traditional acoustic emitters that may beamform signals to attack a drive from long distance. A Long Range Acoustic Device (LRAD) can send audible acoustic waves above 95 dB SPL miles away in open air [9].

B. Hard Disks and Acoustics

Acoustics vibrate the HDD head stack assembly and shock sensor, leading to throughput loss and physical damage.

Hard Disk Mechanics. A HDD read/write head floats ($\sim$10 nm) above the surface of each spinning disk. Data is organized in tracks that circle the disk. To read or write data, the head stack assembly (HSA) must position the head above the desired track. There is a narrow margin of error (on the scale of nm) within which the read/write head can operate. For writes, there is a narrower margin of 10% of the width of the track, while there is a 15% margin for reads [10].

Vibration poses problems for HDD designers. First, vibration may push the head away from the center of the track and render the drive temporarily unable to write. Second, the head may crash into the surface of the platter, physically damaging the disk and leading to possible data loss.

Compensating for Vibration. Two approaches can correct for positional error due to vibration (Figure 3): (1) a standard feedback controller that adjusts the head position using the current positional offset of the head from the center

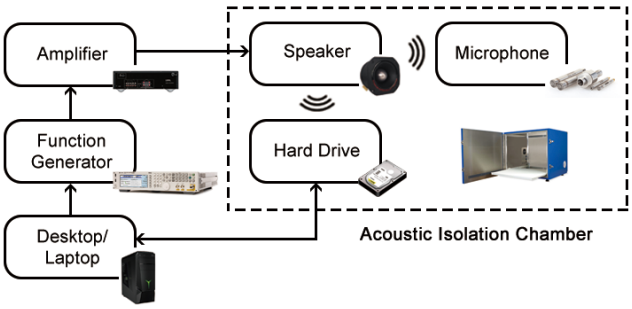


Fig. 4. The physical setup for testing mechanically uncoupled acoustic interference. For mechanically coupled tests, the device containing both the HDD and speaker (such as a laptop) lay directly inside the chamber.

of a track and (2) a feedforward controller where a shock sensor adjusts the head in anticipation of vibration. The HDD will park its head away from the track when the shock sensor senses extreme vibration, such as when a laptop falls.

Acoustic Waves. Acoustic waves vary in amplitude and frequency. Humans can hear acoustic waves between 20 Hz to 20 KHz. Ultrasonic waves have frequencies above 20 KHz, and are inaudible. When acoustic waves contact mechanical components, a vibrational force acts on those materials at the frequency of the wave, with a force proportional to the wave's amplitude. In addition, mechanical components have resonant frequencies, at which vibrational forces have an amplified effect. Acoustic resonance can induce large vibrations in HDDs, and in turn cause loss of throughput [2], [3], [4], [5].

III. Experimental Method

There are three operational challenges to quantify the effects of acoustic interference on hard disk drives: (1) isolating the experiment from uncontrolled signals, (2) inducing precise vibration at the HDD, and (3) accurately measuring HDD errors due to acoustic interference. Unless noted otherwise, the experiments in this paper shared the same physical setup described in this section. Note that a setup with this level of precision is only needed for scientific measurement to discover causality, but an attacker could use a simpler setup to cause the deleterious effects.

A. Isolating the Experiment

The setup must prevent environmental factors from significantly altering the results of the experiment. In our setup, the HDD lies in an acoustic isolation chamber, as shown in Figure 4, to prevent unintended noise from altering results. The setup also monitors the drive's temperature using SMART data to ensure the temperature stays within operational limits (below 50 °C [11]). The speaker hangs from the ceiling to mechanically uncouple it from the HDD in all tests.

B. Generating Vibration

Accurately generating vibration is crucial in observing the effectiveness of this attack. Audible and ultrasonic frequencies use the same basic setup (Figure 4).

Audible Frequencies. Our setup generates audible frequencies using a Tektronix AFG3251 function generator, a Yamaha R-S201 audio receiver, and a Pyramid Titanium Bullet Tweeter speaker. The setup measures the emitter's actual output using a G.R.A.S. Type 26CB microphone, a G.R.A.S. 12AL preamplifier, and a PicoScope 5444B.

Ultrasonic Frequencies. Our setup generates ultrasonic frequencies using a Keysight N5172B EXG X-Series RF Vector Signal Generator, a CRY584 Power Amplifier, and a NU C Series Ultrasonic Sensor. The setup measures the emitter's actual output using a CRY343 microphone and a RIGOL DS4022 oscilloscope.

Algorithm 1 Program that measures the effects of acoustic interference. It gathers information on raw throughput measurements and errors (various program crashes due to interference and program timeouts).

```
THROUGHPUT WORKER SUBPROCESS()
1  forever:
2      addr = rand()
3      data = rand()
4      write_to_disk(addr, data)
5      throughput = calc_throughput()
6      record(get_curr_time(), throughput)

TEST DRIVE(TESTTIME)
1  start_throughput_worker()
2  for testTime:
3      if errorType = worker_has_error()
4          record_dead_worker(get_curr_time(), errorType)
5          kill_worker()
6          start_throughput_worker()
7  kill_worker()
```

C. Measuring the Effects of Vibration

The effects of vibration on HDDs during operation are typically: (1) throughput loss, (2) program crashing when using the HDD, and (3) writes or reads taking an indefinite amount of time to return (even if the acoustic interference subsides in the middle of the write). The challenge is ensuring the measurement program is not affected by the effects it is monitoring. Our measurement program is shown in Algorithm 1.

The testing computer measures throughput using writes to the victim disk via the Linux `dd` utility with the `fdatasync` option. `dd` is a well known and tested tool for basic throughput measurement. The testing computer writes 1MB of pseudo-random data directly to a pseudorandom location on the disk to avoid caching that may speed up the write process. The `fdatasync` option forces `dd` to wait for each block of data to be physically written to disk before writing the next block.

Despite being well tested, `dd` often crashes or hangs indefinitely during use. By monitoring `dd` in a separate process, errors can be quickly intercepted and logged.

IV. Causation I: Head and Disk Displacement

Prior work reports that audible acoustic waves cause throughput loss [2], [3], [4], [6]. Yet, little is known on the root cause. To investigate, we use a Finite Element Model and

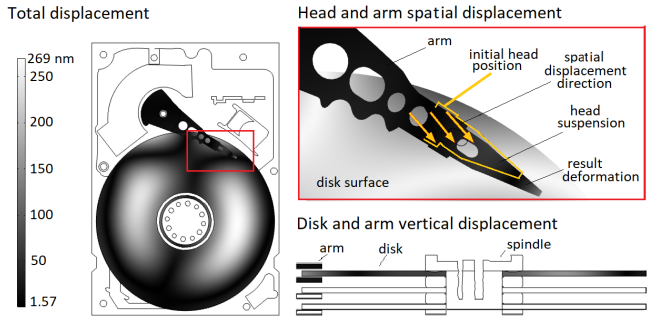


Fig. 5. COMSOL simulation showing displacement of a HDD head assembly and disk during 5 KHz acoustic signal attack (left: top view; bottom right: lateral cross-section; top right: R/W head displacement). Note the displacement on the disk surface (∼156 nm of maximum vertical displacement across the central tracks), and the maximum horizontal displacement of the head suspension (∼8 nm, rectangle box). This exceeds the 7.5 nm read and 5 nm write fault thresholds, assuming a 50 nm width.

numerous experiments to analyze how acoustic waves (and thus vibrations) displace the read/write head or disk platter outside of operational bounds, resulting in either partial throughput loss or complete loss of throughput (Figure 1).

A. Vulnerable Hard Disk Drive Mechanics

We use a Finite Element Model to explore the vibroacoustic response of the HDD's individual mechanical parts (a common use for Finite Element Models [12], [13]). We investigate how sufficiently powerful acoustic waves and vibration lead to throughput loss. Our specific model, made using COMSOL, uses common manufacturer materials and parameters [14].

Figure 5, generated using our model, shows how acoustic waves can displace a read/write head or disk platter outside of operational bounds, inducing throughput loss. This model is simulating a 5 kHz acoustic wave striking the HDD chassis from above at 120 dB SPL. The model estimates maximum disk displacement of about 33 nm horizontally and 156 nm vertically, while estimating maximum read/write head displacement of 9 nm horizontally and 112 nm vertically.

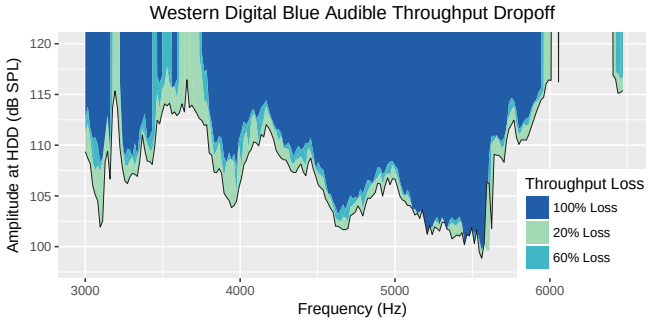
Given a track width of 50 nm [15], a 10% track width margin (i.e. a 5 nm margin) of error for writes and 15% margin for reads (i.e. a 7.5 nm margin) [10], and a vertical distance of 6 nm between the head and the disk [16], these displacements push the drive outside of its operational bounds for reading and writing. In addition, these numbers show the possibility of the read/write head crashing into the disk.

More details on this finite element model simulation appear in the appendix.

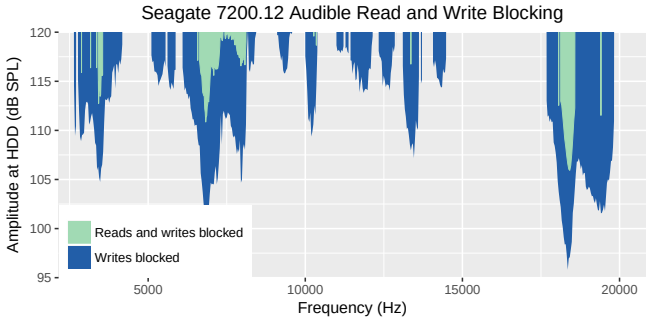
B. Mechanical Throughput Loss Observations

Using the setup described in Section III, we gathered data to show the two main qualities of throughput loss induced by head stack assembly and disk vibration: non-binary throughput loss and reads being significantly harder to block than writes.

Non-Binary Throughput Loss. One critical quality of throughput loss due to head stack assembly vibration is that it allows for partial throughput loss as shown in Figure 6a. A signal can be strong enough to vibrate the read/write head



(a) Thresholds of write throughput loss due to audible signals



(b) Read and write blocking thresholds due to audible signals

Fig. 6. Throughput loss under acoustic interference for a Western Digital Blue HDD and Seagate 7200.12 HDD. There is a measurable gradual degradation in throughput at each frequency for the audible range. Note that for audible frequencies it is far easier to block writes than reads because reads have a higher tolerance for error.

or disk sufficiently to hinder typical write throughput, but not strong enough to completely block the drive from reading or writing to disk. Figure 1 shows this behavior as the lower amplitude signal vibrates the read/write head enough to hinder operation, but not enough to completely block reads and writes. Then, when the amplitude of the signal increases, the vibration of the read/write head also increases, leading to the drive being unable to read or write.

Reads Require Higher Amplitudes to Block. Another quality of throughput loss via head stack assembly vibration is that read blocking generally requires greater amplitudes than write blocking, shown in Figure 6b. This is because the operational margin of error is greater for reads than for writes. Thus, the head may vibrate within the read error margin but outside the write error margin.

V. Causation II: Sensor Spoofing

Attackers can use sound waves or vibration to exploit the piezo shock sensors or MEMS capacitive accelerometers common in most modern HDDs, inducing a complete loss in capability to read or write to disk. These shock sensors and accelerometers detect sudden disturbances (e.g., dropping the HDD) such that the HDD can park its head to prevent damage. Accelerometers were shown to be vulnerable to malicious sound waves and vibration [8]. In this paper, we examined piezo shock sensors, and found acoustic waves (primarily inaudible ultrasonic waves) can alter sensor outputs. We analyze how ultrasound tricks the HDD into inadvertently parking its head, rendering the drive unable to read or write to disk.

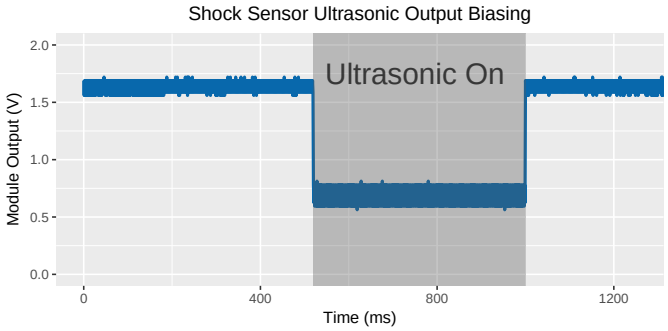


Fig. 7. An ultrasonic wave alters the output of a piezo shock sensor in a PKGX-14-4010 shock sensor evaluation module.

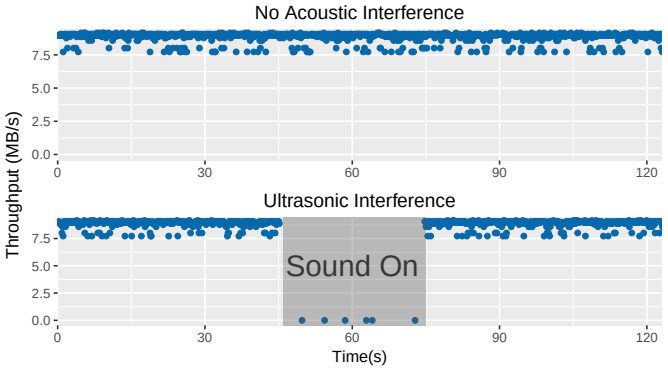


Fig. 8. A 31 kHz ultrasonic wave at 125 dB SPL induces complete throughput loss on a Western Digital Black 2.5" WD1600BJKT HDD.

A. *Vulnerable Sensor Mechanics*

Spoofing the Shock Sensor. One can vibrate the shock sensor mass at its resonant frequency to induce false sensor output similar to prior work on spoofing MEMS accelerometers [8] and MEMS gyroscopes [17]. Shock sensors work similarly to MEMS accelerometers in that vibration of a sensing mass creates a voltage representative of the motion perceived by the sensor. By placing a shock sensor on an object, the shock sensor can produce a voltage representative of the object's vibration. However, one can make the vibration of the mass of the piezo shock sensor different from the vibration of the object by exploiting resonant frequencies. This difference in vibration results in an altered output different from output that represents the actual vibration of the object.

We demonstrate altering output of a PKGX-14-4010 MEMS shock sensor evaluation module, which we believe is the same unit inside the Toshiba MQ01ABF050 HDD (Figure 7). The output of the shock sensor module under normal operation (with no intentional acoustic interference) is approximately 1.6 V. However, the output becomes 0.6 V when subjected to a 27 kHz tone at 130 dB SPL—translating roughly to a misperceived acceleration of over ten times the acceleration of Earth gravity at sea level.

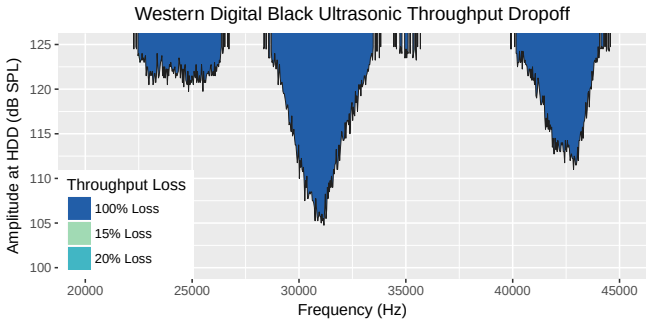
Throughput Loss from Sensor Spoofing. A spoofed sensor can lead to throughput loss by making the HDD inadvertently park its head. Under intentional acoustic interference, the shock sensor or accelerometer will report a false value to the HDD firmware. This false value implies that the HDD is moving violently, such as if it were dropped, and needs to park the read/write head. It follows that an attacker could continuously falsify the sensor's output to keep the head parked indefinitely, preventing the HDD from writing or reading.

Our experiments confirm throughput loss from sensor spoofing. First, we play inaudible sound at a resonant frequency of the shock sensor in the HDD (27 kHz at 125 dB SPL), which results in throughput loss (Figure 8). Second, to confirm that it is indeed the shock sensor that causes the throughput loss, instead of read/write head or disk vibration, we removed the shock sensor from the drive and measured throughput with and without acoustic interference. This confirms that the sensor's erroneous output caused by acoustic interference leads to throughput loss.

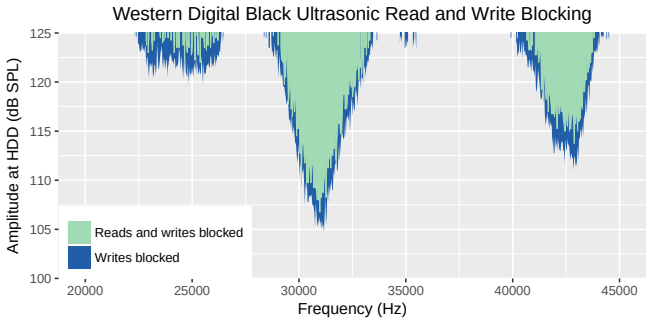
B. *Sensor Throughput Loss Observations*

Binary Throughput Loss. The throughput of the HDD is either unaffected or lost completely as shown in Figure 9a. This method cannot induce partial throughput loss as head parking is the root cause to throughput loss. The head can only be either parked or operate normally (assuming no other kind of interference).

Similar Amplitudes to Block Reads and Writes. Another observation is that write blocking and read blocking require similar amplitudes for sensor induced throughput loss shown in Figure 9b. This observation may be because the firmware's threshold for head parking is similar, but not exactly the same for reads and writes.



(a) Thresholds of write throughput loss due to ultrasonic waves



(b) Read and write blocking thresholds due to ultrasonic waves

Fig. 9. Ultrasonic throughput loss for a Western Digital Black WD1600BJKT HDD. In contrast to audible frequencies, ultrasonic frequencies cause full throughput loss (no partial) and block writes and reads using similar amplitudes.

VI. Pathologies During Testing

We observed several pathologies while testing HDDs with malicious acoustic interference including: HDDs of the same model exhibiting similar characteristics under attack and seeing unusual levels of bad sectors.

A. Consistent Resonance despite Manufacturing Variation

During testing, drives of the same model showed similar characteristics when subjected to acoustic interference. We attribute slight differences to process variation. Our observations are consistent with previous research [5] that shows unremarkable frequency-dependent variation across of drives of the same model. Thus, an adversary could profile one drive to predict the frequencies that most affect a victim drive of the same model.

To test this characteristic, we profiled one Western Digital Blue WD5000LPVX HDD to discover the frequency that most affects drives of this model. Then we subjected 13 other drives of the same make and model to this frequency. The vibration denied each drive from being able to read or write. We also observed that ultrasonic interference exhibited consistent resonant frequencies across drives of the same model. In practice, we find that the most vulnerable frequencies remain similar from drive to drive of the same model.

B. Bad Sectors

The vast majority of drives used in our tests developed several bad sectors or became nonoperational. While we do not specifically conduct an experiment to test for abnormal levels of bad sectors, we are able to easily spot this trend in the data collected for other experiments.

Gathering the Data. Throughout our experiments, we collected the bad sector data presented in Table I through the Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) system, a de-facto HDD monitoring standard that can measure bad sectors in HDDs [18], [19]. Our observations are anecdotal rather than controlled experiments. The drives were subjected to different frequencies, amplitudes, and durations of acoustic interference. All drives had between 15 and 500 power on hours, except one drive that had 755 hours.

Interpreting the Data. As shown in Table I, many of the drives tested showed high bad sector counts. In fact, every drive suffered at least one bad sector. As storage expert Erik Riedel [20] remarks "it would be highly unusual to regularly find bad sectors on hard disk drives under 500 power-on-hours."

Drive	# of Tested Drives	Avg # Bad Sectors
WD Blue WD5000LPVX	7	705
WD Enterprise WD1003FBYZ	1	82
WD Purple WD10PURX	1	500
Seagate 7200.12	3	961
WD Black WD1600BJKT	2	321
Toshiba MQ01ABF050	1	14,448
Total	15	1,639

TABLE I. The cumulative bad sector data for several drives used in various experiments. All drives had between 15 and 500 power on hours (except one that had 755 power on hours).

Analysis of bad sectors in consumer-grade drives from data center environments is consistent with the assertion that bad sectors are rare. Google found that only 9% of their consumer-grade hard disk drives developed any bad sectors [19] over eight continuous months of use.

We surmise that the alarming number of bad sectors is due to head crashes caused by the force that the sound exerts on the head stack assembly during experimentation (as outlined Section IV-A). For instance, we have found scratches visible to the human eye on platters after disassembling some of the tested drives. However, there could be several other factors at play. For example, it is possible that the HDD firmware is incorrectly marking sectors as physically damaged after failing to write to them several times because of the interference.

Ultrasonic attacks are less likely to cause a head crash, but could be damaging the drive in other ways such as causing the head to become unstable over time because of excessive parking. This instability could make the drive less reliable in its reads and writes, leading to sectors being marked as bad. For example, in a test that subjects the Toshiba HDD to an ultrasonic signal right at the head parking amplitude threshold, one can hear head parking in rapid succession, possibly causing damage to the head controller.

VII. Hard Disk Drive Non-Responsiveness

During throughput testing under malicious acoustic interference (Sections IV and V), HDDs become non-responsive to the operating system (both Windows and Linux). Prior research by the IT security community [6] observed similar phenomena, yet the exact causality in the operating system remained a mystery.

A. Causes of Non-Responsiveness Errors

Evidence suggests that prolonged throughput loss may cause a HDD to enter a non-responsive state by causing timeouts in I/O requests, along with other errors in the I/O request stack. This non-responsive state lasts until the HDD is physically unplugged and reconnected or the operating system restarts. Examining the Windows 10 I/O request path, particularly the port and miniport drivers, reveals what practices cause these errors.

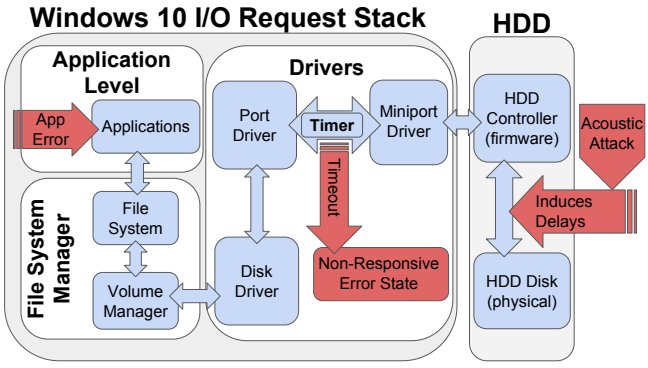


Fig. 10. On Windows 10, prolonged acoustic interference induces delays in the HDD that cause a timer in I/O requests between the port driver and miniport driver to timeout, leading to the HDD entering a non-responsive state. Light blue indicates the normal path of operation while dark red shows what happens during an acoustic attack.

I/O Request Path to a HDD. The non-responsiveness error originates in the I/O request path (Figure 10). In Windows 10, several actors process each I/O storage request (i.e. read, write, or control operations to the HDD) before delivering the request to the HDD [21]. When a typical file read/write request reaches the file system, the file system passes the file's location information to the volume manager as a partition offset. The volume manager converts this partition offset into a HDD block number and sends it to the disk driver. The disk driver converts the I/O storage request containing the HDD block number to a SCSI request block and sends the request block to the port driver, which interfaces with the HDD miniport driver. The miniport driver takes the request and sends it to the HDD.

I/O Timeouts and Other Errors. I/O timeouts and other errors in the I/O request path can lead to the drive entering a non-responsive state. In Windows 10, the timeout is specifically in the port and miniport drivers. The port driver manages general data flow for a class of devices, in this case HDDs, whereas the hardware manufacturer designs the miniport driver to handle data flow specific to the device [22]. The pair work in conjunction to pass information from the disk driver to the HDD. When an I/O request packet is sent from the port driver to the miniport driver, the I/O request packet is put in a pending queue until the request is completed [23]. A timer monitors each unfulfilled request. The timer should never expire normally as expiration implies the device has stopped responding [24].

We find two types of errors in Windows 10. (1) The port driver may timeout, indicated by an error with Event ID code 129. When this happens, all outstanding I/O requests report an error to the programs that issued the request, and the port driver sends a reset request to the hard drive [25]. (2) Some miniport drivers may also report a second error code with Event ID 153. Some miniport drivers may detect when port driver timeouts are about to occur and abort the request itself [26]. The miniport driver then returns an error code (ID 153) instead of the port driver returning an error code. The miniport driver may also return an error (also ID 153) if it detects HDD bus communication errors, unrecoverable read errors, or other undocumented errors.

B. Observations

Windows 10. During an attack, we mainly observe errors originating from the port driver (ID code 129), but also some from the miniport driver (ID code 153), that affected numerous applications and could even crash the operating system. The numerous port driver errors indicate I/O requests frequently timing out, and also that numerous HDD reset commands are sent to the miniport driver. However, some of these reset commands remain incomplete, resulting in all outstanding requests to remain stuck, and causing some operating system applications to freeze. The miniport driver also returned errors, indicating possible bus or unrecoverable read errors. Sporadically, the Windows 10 OS would crash with a `CRITICAL_PROCESS_DIED` or `UNEXPECTED_STORE_EXCEPTION` error, likely because a critical process did not handle the port or miniport errors correctly.

Ubuntu 16.04. Expired timers in the I/O request chain lead to Ubuntu remounting all loaded files as a read only file system, with any previously unaccessed files becoming inaccessible. Ubuntu 16.04 logging files (`dmesg`, `kern.log`, and `syslog`) confirm that the hard disk controller driver (in this case a generic ATA/SATA II controller driver) return errors to the operating system when under attack from acoustic interference. These errors are due to the expired timer of the outstanding I/O requests in the pending queue (e.g. `READ/WRITE FPDMA QUEUED` command failure) [27]. When the hard drive detects these conditions, it sends an error message to the controller driver, and waits to receive a reset command. Note that the controller driver tries a finite number of times (usually four) to send the reset request to the hard drive.

The file system disconnects and remounts as read only if the attack persists after the last reset request failures. `dmesg` shows `COMRESET failure (errono=-16)` four times until finally showing `reset failed, giving up`. Then, the attack can also generate `delayed block allocation of inode` error followed by a `This should not happen!! Data will be lost` message. In addition, the message `previous I/O error to superblock detected` might appear multiple times. These error messages indicate file system corruption and data loss.

C. Measuring Non-Responsiveness Errors

To characterize the non-responsive state, we measured how long it took to induce non-responsive errors on several HDDs.

Setup. We placed the drives in the experimental setup described in Section III and determined an effective frequency for acoustic interference. The test began throughput measurements as described in Section III-C for one minute without an acoustic signal present. Next, the experiment subjected the drive to intentional acoustic induced vibration, and afterwards queried the drive to provide its basic information such as serial number and device capacity.

Results. Drives exhibited similar behavior when the error occurred (Table II). After the acoustic signal subsided, the drive would still appear to the operating system as a block device. However, when queried for its basic info, the drive would typically not respond. In rare cases, it would send back nonsensical data, such as the WD Blue drive reporting non-displayable characters for its model number and that its capacity was 2,692 PB when its actual capacity was 500 GB. These problems persisted until either the computer was restarted, the

Model	Freq (kHz)	Amp (dB SPL)	Time (s)
WD Blue WD5000LPVX	4.6	118.1	100
WD Purple WD10PURX	6.9	118.9	130
Seagate 7200.12	7.0	119.1	120
WD Black WD1600BJKT	21	120.0	5
Toshiba MQ01ABF050	27	127.2	8
WD Blue WD5000LPVX	31	138.1	6
Seagate 7200.12	31	139.5	6

TABLE II. THE FREQUENCY, AMPLITUDE, AND THE MINIMUM REQUIRED DURATION OF ACOUSTIC SIGNALS USED TO INDUCE VIBRATION RESULTING IN COMMUNICATION ERRORS THAT PERSISTED UNTIL SYSTEM RESTART, HDD RESTART, OR PHYSICAL DISCONNECTION AND RECONNECTION OF THE HDD TO THE COMPUTER ON LINUX. ULTRASONIC FREQUENCIES WERE ABLE TO INDUCE ERRORS IN AS FEW AS 5 SECONDS WHILE AUDIBLE FREQUENCIES TOOK AS FEW AS 100 SECONDS.

HDD was power cycled, or the SATA cord was physically disconnected from the drive and reattached.

VIII. Operating Systems and Applications

We demonstrate a few of the attacker's capabilities using two case studies that utilize vibration interference. In addition, we describe how an attacker might select a frequency to attack a drive.

A. Attack Frequency Selection

To maximize effectiveness, an adversary would select a frequency that requires the smallest acoustic amplitude to disturb a target HDD. To do so, an adversary may consider the frequency responses of the speaker and HDD, and whether or not an inaudible signal is possible or desirable. Note that because of manufacturing variation having a low effect on drive characteristics (Section VI-A), an attacker can select a frequency using a different HDD of the same model as the victim drive.

Speaker Profiling. To profile a speaker's frequency response, one can simply record the loudness of the speaker at each desirable attack frequency. Alternatively, the frequency response of the speaker may be available online. Our tests indicate speakers of the same model share similar frequency responses, allowing an attacker to profile a speaker of the same make and model of a target speaker if the target speaker itself is unavailable.

HDD Profiling. An outline of how an attacker could develop a profile of a HDD model is shown in Algorithm 2. At each frequency, the algorithm finds the minimum amplitude that causes write blocking. In addition, the program should periodically check the drive to ensure it is still working properly within operating margins. This includes checking the drive temperature (to see if it has overheated), the number of bad sectors, and that the throughput of the HDD is similar to normal operating parameters.

Choosing a Frequency for Attack. Choosing an attack frequency can be as simple as overlaying the speaker profile and HDD profile, then observing the cross section (Figure 11). After doing so, one could choose a frequency in one of the largest areas of overlap for the best possibility of a successful attack. Alternatively, if ultrasound or near ultrasound (as some people cannot hear near ultrasonic frequencies because of high frequency hearing loss) is an available frequency, then it may be desirable to select that frequency over others to make the attack harder to detect.

B. Case Study 1: Blue Note

We demonstrate several proof of concept attacks that affect both Windows 10 and Ubuntu 16.04 systems in various scenarios. A webpage can launch a self-stimulated attack on a laptop using the laptop's own speakers, while requiring no extra user permissions. An attacker can place a speaker near a victim desktop computer to conduct an inaudible physical proximity attack on the desktop computer, even with the speaker and victim physically decoupled.

Test Methodology. This setup assumes that the attacker knows the model of the victim drive and determined the vulnerable frequencies via the method in Section VIII-A. For each test, we installed a fresh operating system on the victim HDD, then placed the victim system in an acoustic isolation chamber.

Algorithm 2 Creating an HDD profile. Note that test_drive is listed in Algorithm 1

```
PROFILE DRIVE(FREQMIN, FREQMAX, FREQSTEP)
baseline= test_drive()
for freq in range(freqMin, freqMax, freqStep):
    // Find min amp at this freq to block writes
    while min_amp_not_found(results):
        amp = decide_next_amp(results)
        start_sound(freq, amp)
        results.save_test(test_drive())
        end_sound()

        // Ensure drive functioning properly
        results.save_temp()
        results.save_bad_sectors()
        if is_not_similar(test_drive(), baseline):
            stop_testing()
```

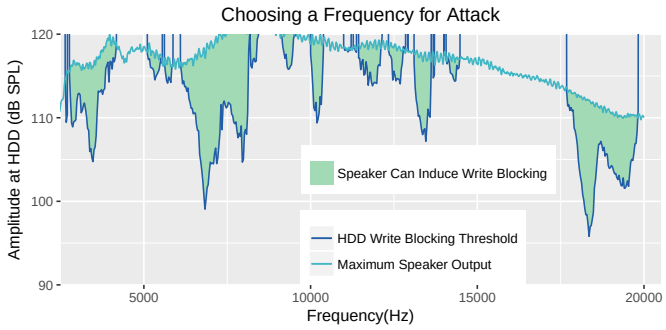


Fig. 11. Profiles for a Seagate 7200.12 HDD and a Pyramid TW28 speaker are shown above. The areas where the profiles overlap (the shaded areas) are those where the speaker can block HDD writes.

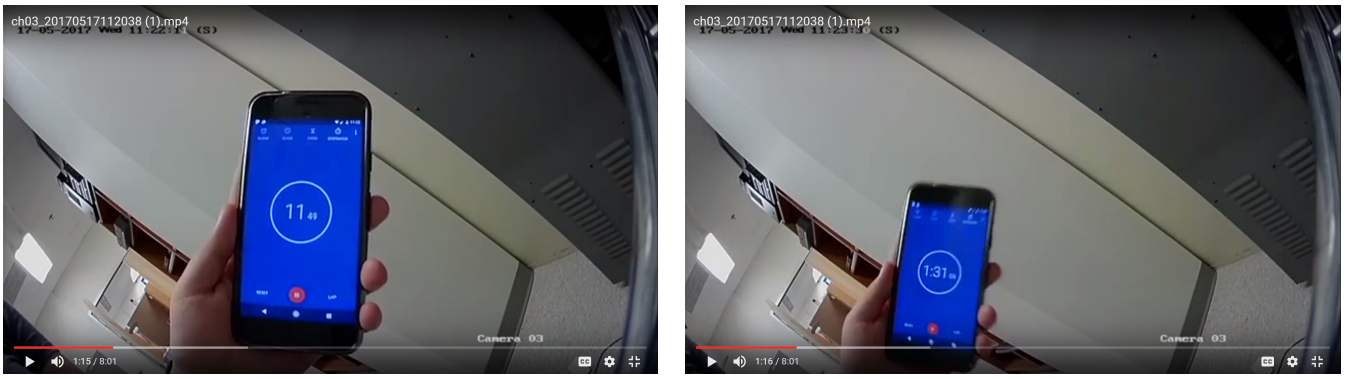
For self stimulation attacks, the victim accesses the adversary's web site—perhaps through a phishing attack or a link within a malicious email. The site then plays malicious audio without permission over the system's built-in speaker to attack the HDD. The victim accesses the malicious site using the latest version of Google Chrome (58.0.3029.110).

For physical proximity attacks, the attacker places a chosen speaker near the HDD. Thus, the malicious acoustic waves may be audible or inaudible depending on the chosen speaker.

Results. Table III summarizes a selection of repeatable attacks on different laptops, operating systems, frequencies, and the minimum required interference duration before the reported symptom appears. For Windows and Linux, the average case across all tests (the majority of which are not shown) was that the HDD became non-responsive (described in Section VII) after playing audio for a prolonged period of time. This was the case for both ultrasonic and audible attacks. However, one notable outlier symptom was the Windows operating system crashing after freezing, displaying a `CRITICAL_PROCESS_DIED`

Attack Type	Machine Description	Hard Disk Drive	Operating System	Freq (kHz)	Symptom	
					Time Until (s)	Description
Self Stimulation Attack	Dell XPS 15 9550 Laptop	WD Blue WD5000LPVX	Windows 10	7.83	45	Frozen
					125	System Crash
			Ubuntu 16.04.1	7.95	120	HDD Non-Responsive (until OS restart)
	HP Elite Minitower Desktop w/ HP DC7600U Speaker	WD Blue WD5000LPVX	Windows 10	4.60	80	Intermittent Freezing
Physical Proximity Attack	HP Elite Minitower Desktop	WD Blue WD5000LPVX	Windows 10	10.00	113	System Crash
			Ubuntu 16.04.1	10.00	225	HDD Non-Responsive (until OS restart)
	Intel NUC NUC5i5RYH	Seagate 7200.12	Windows 10	5.60	180	HDD Non-Responsive (until OS Restart)
			Ubuntu 16.04.3	5.60	120	HDD Non-Responsive (until OS Restart)
	Sony PCG Laptop	Samsung HM321HI	Windows 10	40.00	120	System Crash

TABLE III. A SELECTION OF ATTACKS AGAINST OPERATING SYSTEMS USING ACOUSTICALLY INDUCED VIBRATION. WINDOWS 10 COMMONLY FROZE, AND WOULD SOMETIMES CRASH. ON UBUNTU, THE DRIVE WOULD OFTEN REMOUNT AS READ ONLY.



(a) Frame Before Video Loss

(b) Frame After Video Loss

Fig. 12. Two frames from an unedited recording taken from a surveillance video system's HDD. During recording, the system was subjected to acoustic interference. The displayed images are roughly 5 frames apart (less than a second apart in video playback), including one frame that was only partially written because of acoustic interference. However, the timestamps indicate that roughly 80 seconds of video are missing due to the interference.

or `UNEXPECTED_STORE_EXCEPTION` message.

Possible Causes of System Crashing. It is likely that the Windows 10 crash is closely related to the non-responsive error discussed in Section VII. The information extracted from the crash dumps generated by the operating system reveals information about the crashes. The crash dumps show the miniport driver returning a device error (`STATUS_IO_DEVICE_ERROR`), indicating there was an error in the HDD. The operating system does not seem to handle this error correctly, leading to `UNEXPECTED_STORE_EXCEPTION`. This indicates that the memory manager required data from the disk, but was unable to write into memory because of an in-page I/O error.

C. Case Study 2: Video Surveillance

An attacker can prevent a video surveillance system from writing to its HDD, resulting in recorded video loss. Video surveillance systems constantly store large quantities of video. These systems typically use HDDs rather than SSDs because of the need for a large storage capacity. For such systems, the integrity of the recorded data is vital to the usefulness of the system, which makes them susceptible to acoustic interference or vibration attacks.

Video Surveillance System Setup. The attacked system is a Ezviz 720p 4-channel video surveillance system using its stock Western Digital 3.5" Purple 1 TB, part of Western Digital's surveillance series of HDDs. The system stores its operating system on an on-board flash chip, and so the operating system is not directly affected by vibration. The system lies in an acoustic isolation chamber as described in Section III-A. The speaker hangs from the ceiling, resting 10 cm directly above the video surveillance system's HDD. We did not tamper with the surveillance system, leaving its casing intact. Lastly, three (of the possible four) cameras were attached to the system, with one camera placed inside of the acoustic chamber and two cameras placed outside of the chamber.

Attacking the System. This test subjects the system to the malicious signal for increasing durations (Table IV) and records the results. We choose a 6,900 Hz sinusoidal signal at 120 dB SPL using the methods discussed in Section VIII-A. During the course of the experiment, we monitored the system manually by looking at the live video feed from the system. After the concluding the experiment, we examined the recordings from the HDD.

Interference Duration(s)	Delay Until Video Loss (s)	Video Loss Lasted Until
60	12	Interference Stoppage
90	12	Interference Stoppage
100	12	Interference Stoppage
105	0	System Restart
120	0	System Restart
180	0	System Restart

TABLE IV. ACOUSTICALLY INDUCED VIDEO LOSS IN RECORDINGS FROM A EZVIZ SURVEILLANCE CAMERA SYSTEM.

Results. For all tests, the observer did not notice any abnormalities in the live video stream, but attack durations longer than 12 seconds caused video loss in the video recorded on the HDD (Figure 12 and Table IV). There were two observed pathologies. (1) Recordings from periods of interference less than 105 seconds exhibited video loss from about 12 seconds after being subjected to acoustic induced vibration until the vibration subsided. In contrast, (2) interference for periods of 105 seconds or longer resulted in video loss from the beginning of the vibration until the device was restarted.

These two pathologies coincide with behavior exhibited by prior tests. The first pathology, with momentary video loss until interference subsides, is thought to be the write throughput blocking effect discussed in Sections IV and V. The system buffers video data until a certain limit, which in our configuration is about 12 seconds, after which subsequently recorded video is discarded until the drive becomes available once again. When the interference subsides, the system writes buffered data to disk and begins operation as usual.

The second pathology resembles non-responsiveness errors (Section VII). Unlike in the previous case, the HDD becomes non-responsive to the system until system restart. The system is never able to write the buffered video before being restarted, explaining the immediate effect on the recorded video.

In the case that a victim user is not physically near the system being attacked, an adversary can use any frequency to attack the system. The system's live camera stream never displays indication of an attack. Also the system does not provide any method to learn of audio in the environment. Thus, if a victim user were not physically near the system, an adversary can use audible signals while remaining undetected.

IX. Defenses Against Acoustic Interference

We discuss, simulate, or implement several methods to detect or prevent system level effects of acoustic interference from both the HDD level and from the system level.

A. Augmented Feed-Back Controller

Hard disk manufactures did not design modern hard drive controllers to withstand malicious forces of the magnitude presented in this paper; however, manufacturers can modify the firmware of the feed-back controller to defend vulnerable frequency bands against the disturbance generated by the acoustic attack. We suggest and simulate a controller augmented with a disturbance attenuator to defend against intentional acoustic interference attacks. Manufactures can implement this controller as a software update, with no extra cost to physically replace hardware.

Position Error Signal. The deviation of the R/W head from the center of the track can accurately approximate external vibration on the HDD. Vibration is a major contributor to this R/W head deviation [28]. The HDD measures the deviation as the Position Error Signal (PES). The PES varies mainly because of repeatable runout and/or non-repeatable runout. Repeatable runout refers to vibration caused by repetitive operating factors, typically internal to the HDD, such as the oscillation of an imbalanced disk rotating. Non-repeatable runout refers to vibration caused by non-repetitive operating factors, typically external to the HDD, such as the acoustic attacks presented in this paper [14].

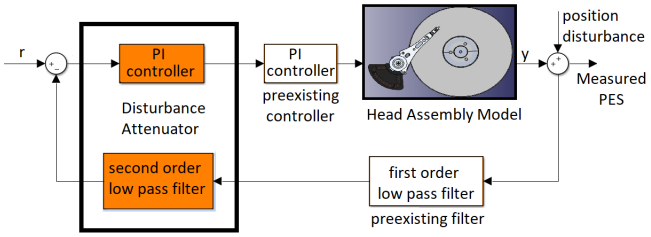


Fig. 13. The block diagram of the servo control system with the disturbance attenuator composed of a Proportional-Integral (PI) controller and a second order low-pass filter.

Design of an Attenuator Controller. We design an attenuator controller to mitigate the effect of acoustic signals on the R/W head. Attenuator controllers typically compensate for precise, narrow-band peaks in mid-high frequency ranges [29], [30]. However, acoustic signals that affect the R/W head cover a wider frequency range than what is typical for an attenuator controller. Thus, we alter the controller to cover a wider frequency band than what is typical. This modification results in a controller that attenuates a wider frequency band, but with a lower attenuation strength.

Simulation Model. We design and simulate a feedback controller with an attenuator for a Seagate 7200.12 HDD that attenuates signals from 6 kHz to 8 kHz, the greatest range that affected the drive (Figure 6b).

The simulation includes a 9th-order Matlab model of the head-disk assembly and a controller designed using Simulink [31]. The original Matlab model comprises a pre-existing control structure consisting of a first order low-pass filter in the return path and a Proportional-Integral (PI) controller (Figure 13). PI controllers are a common type of feedback controller used in industrial control systems. The PI controller calculates the error value of the head position as the difference between a desired reference setpoint (in this case the center of the track) and the actual position, and adds a correction.

Assuming that the pre-existing control sufficiently controls the HDD under normal operation, fulfilling basic stability and trackseeking requirements, the augmented feed-back controller defense adds an attenuator (i.e. another PI controller [P= 0.0079, I=0.1442]) plus a second order low pass filter (transfer function: $[s + 2800]/[s^2 + 128s + 2800]$) to mitigate the attack effect. Its goal is to keep the PES within the read/write fault margins.

The simulation models the disturbance d induced by the attack as a sine wave with amplitude sampled from a uniform distribution, based on real PES data from a Seagate 7200.12 HDD measured during an attack at 7.5 kHz (Figure 14). On the non-attenuated controller, this signal induces a displacement up to 97.26% of a track width from the center of the track, well outside of the thresholds for reading and writing to disk (15% and 10% of track width respectively).

Simulation Results. The attenuator successfully keeps the PES within the read/write fault threshold within the range

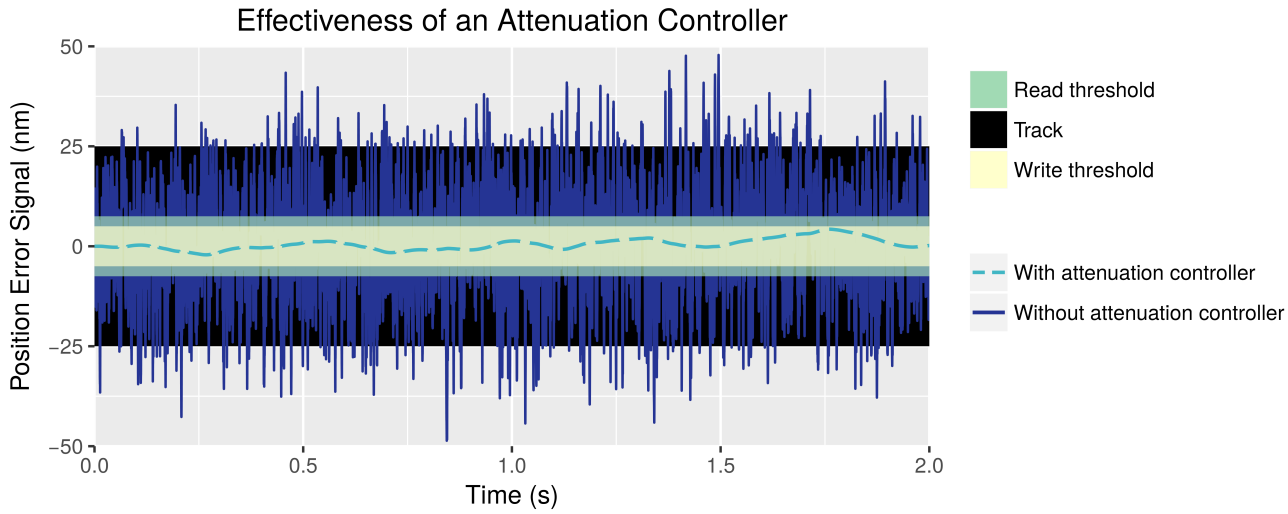


Fig. 14. Simulated position error variation for a 7.5 kHz attack. Our proposed attenuator reduces position error to within the read/write fault thresholds (15% and 10% of the track respectively).

of the attenuator. For example, the maximum displacement for a 7.5 kHz disturbance using the non-attenuated controller is 97.26% of the track width, while the maximum displacement when using the attenuated controller is only 8.54% of the track width (Figure 14). Similarly the maximum displacement for a 6.5 kHz disturbance with the non-attenuated controller is 58.36% of the track width, but only 5.12% of the track width with the attenuated controller.

B. Detecting Spoofing Attacks with Sensor Fusion

Defenses in the previous section would not prevent spoofing the vibration sensor, but HDDs could make use of redundant vibration sensors or a microphone to detect an ultrasonic attack. If the HDD were to detect such an attack, the drive could operate normally instead of parking the head as a malicious false positive.

The ultrasonic attacks work by vibrating the piezo shock sensor or the accelerometer's sensing mass at its resonant frequency, fooling the sensor into thinking the drive is violently moving. However, the drive may detect the malicious ultrasonic wave using sensor fusion, or combining various sensor data into a stronger source of information. These various sensors could consist of additional vibration sensors or microphones. After detecting the malicious ultrasonic wave, the sensors can signal to the drive to not park the head and to allow operation as usual.

Drawbacks are present in both of these defense methods. Wideband microphones that detect ultrasonic signals are expensive, but will detect the signal reliably. Redundant vibration sensors from sensor fusion are inexpensive (just a few cents per sensor), but for n sensors with relatively prime resonant frequencies the adversary will need to emit n tones to disrupt all the sensors. While not a perfect defense, this low cost method significantly increases the effort the adversary must use.

C. Acoustic Signal Reduction

Reducing the amplitude of acoustic signals is another way to defend against intentional acoustic interference. Signal reduction approaches are either passive, such as using noise dampening material, or active, such as active noise cancellation. We implement a passive noise dampening solution, finding it to be effective against higher frequencies but having the drawback of increasing drive temperature. We also discuss active noise cancellation, finding it to be infeasible.

Passive Acoustic Attenuation. Many applications use noise dampening materials to passively reduce incoming acoustic signals. To test the viability of noise dampening materials as a defense, we placed sound dampening foam molded into a 4 cm thick block on top of the HDD as described in Section III. We developed acoustic vulnerability profiles with and without the foam block, as shown in Figure 15.

Our experiments showed that the foam significantly reduced a HDD's susceptibility to write blocking. However, it did not attenuate lower frequency signals to the same degree as higher frequency signals. This result is likely because of the physics behind how acoustic waves diffract. One could simply encapsulate a HDD with noise reduction materials, but this has one major drawback. Noise dampening material typically acts as a thermal insulator, leading to increases in operating temperature (10 C in our tests). Increased temperature has been linked to increases in drive failure, and thus makes this solution impractical. In addition, this solution can be costly. Depending on the quality of the sound dampening material, this can cost between $10 to $100 per drive.

Active Acoustic Attenuation. Noise cancelation may seem like a natural defense against acoustic attacks. However, several difficulties arise when faced with implementing such a defense that would likely make it impractical. It is simple enough to cancel noise along a single plane of points orthogonal to an oncoming wave. However, because of the high frequency of our injected waves, it is more difficult to cancel over an area large enough such that the read/write head is completely enveloped as it moves across the disk [32]. This is not accounting for canceling over the portions of the PCB where the sensors are mounted. In addition, without a high end microphone, the machine under attack cannot easily determine

which direction the sound is coming from without use of multiple receivers. Lastly, a noise canceling defense requires a sound wave equal in amplitude to the attacking wave to completely cancel it, which could be difficult to generate without affecting the hard drive's operation. In combination, these difficulties make us believe that sound cancelation is not a practical defense for a hard disk drive.

D. Other Simple Defenses

There are a variety of other simple techniques that manufactures or users could apply to defend against acoustic interference on HDDs. The most obvious defense is to use solid state drives (SSDs) instead of HDDs. However, SSDs remain significantly more expensive per gigabyte than HDDs. Another defense would be to write data to multiple disks spatially spread out in a RAID configuration such that if an attacker simultaneously attacks drives, the system could later reconstruct the lost data from the other drives. If the drives are spatially distant in separately secure areas, denial of service would be significantly harder. Another defense is to simply disable all nearby unused emitters.

X. Discussion

Feasibility of Acoustic Attacks. There are two hurdles for an adversary to cross: the acoustic signal must be strong enough to cause errors and the attack must be difficult to detect or stop. For instance, the attack in Cuba that allegedly used inaudible ultrasonic waves to damage US diplomats' hearing would be an example of being difficult to detect. The attack would also be difficult to stop; no one has claimed to have found any ultrasonic emitters.

Ultrasound may remain unnoticed by those in the vicinity of the attack despite the strength of the signal, as ultrasonic waves are inaudible to humans. Near ultrasonic attacks may remain unnoticed because of high-frequency hearing loss occurring in human beings, caused by factors including age and poor choice in music.

An adversary may attempt an attack when a victim steps away from a computer. A malicious program or webpage might only play audio when people are likely to be present. If the program or webpage is targeting a specific person or group of people, it could utilize specific knowledge of that group to target times they are not around. Our tests have measured a Dell XPS 15 9550 laptop's output to be as high as 103 dB SPL from 1 cm away from the laptop. We have observed write blocking using signals as low as 95.6 dB SPL. This demonstrates the possibility of using the laptop's own speakers to attack its own hard disk drive.

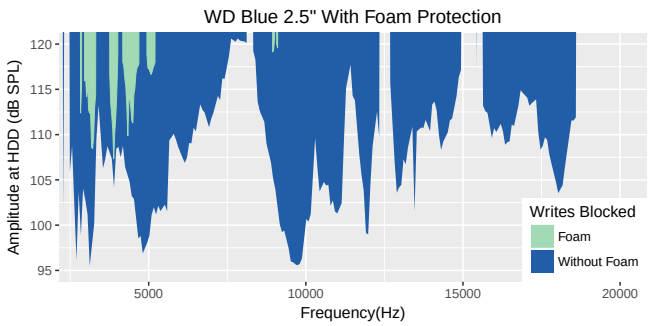


Fig. 15. The effectiveness of mitigating acoustic interference by simply placing a 4 cm thick piece of foam on top of a HDD.

Beamforming or concealing a speaker can make the speaker harder to locate and harder to stop. For example, a beamforming Long Range Acoustic Device could target a device from a distance greater than 1 mile and may cause malicious effects before the victim would be able to find the emitter.

Acoustic Attacks in Data Centers and Medical Devices. In a private data center, the environment is controlled by a single entity and the systems often have no co-located speakers to mount a self-stimulation attack. Companies or individuals can rent a rack, cabinet, cage, or room in a co-located data center. Thus, in a co-located data center, an adversary could pay to place a speaker next to other targeted machines. However, the speaker would need to produce inaudible ultrasonic waves because of constant datacenter monitoring.

Medical devices require high availability. However, in most hospitals and other medical buildings, there is typically an abundance of people, making it difficult to attack with audible frequencies. In the chaos of a hospital or other such building, it may be possible to conceal a device on one's person, but it may also be just as easy to cause denial of service in other ways without the need of such equipment, such as by unplugging cables. However, acoustic attacks could cause denial of service through more sophisticated means that leave little traceability back to the adversary.

XI. Related Work

Acoustic Interference on Hard Drives. Sandahl et al. [2], Siemens [4], and Rawson and Green [3] have investigated HDD throughput loss due to acoustic interference; however, they did not consider malicious actors and did not test ultrasonic signals. An engineer demonstrated how yelling at HDD arrays can lead to perceptible drops in I/O throughput[1]. Ortega [6] demonstrated how hard disk drives can be interfered with by finding their resonant frequency. This interference can lead to the operating system losing its ability to communicate with the drive. Ortega also suggested that physically damaging the drives is possible using sound.

Hard Drive Covert and Side Channels. Previous research has made use of HDD components' analog features to establish covert channels. Guri et al. [33] utilized the HDD's built-in thermal sensors to receive data transmitted over the machine's heat emissions. Guri et al. [1] used the movements of a hard drive's actuator arm to generate audible emissions that were used to exfiltrate data from airgapped machines. Since the head of a hard drive is made up of magnetic materials, the movement of the head can produce a sufficiently strong magnetic field that can be detected by a smartphone's magnetic field sensors. Matyunin et al. [34] utilized this phenomenon to build a covert channel by manipulating the movement of the head.

Much less attention has been devoted to side-channel information-leakage attacks on HDDs. Biedermann et al. [35] showed how an attacker could use a smartphone's magnetic field

[1] https://www.youtube.com/watch?v=tDacjrSCeq4

sensors to deduce information about a machine's operations. Previous research has demonstrated how to establish a covert channel, our work explores the effects induced by *injecting* acoustic waves into HDDs.

Acoustic Side Channels. Recent research has demonstrated how attackers can utilize acoustic side channels to interfere with computer systems. Genkin et al. [36] showed how to extract cryptographic keys by observing the coil whine of a machine during the decryption process. Son et al. [17] used sound to crash drones by affecting gyroscopic sensors. This work was extended by Trippel et al. [8] to spoof the output of capacitive MEMS accelerometers. We utilized both audible and ultrasonic acoustic waves to attack HDDs.

Sensors. Intentionally altering sensor output using physical signals sources is a topic of recent research. Depending on the structure of a MEMS gyroscope, performance degradation can be induced by acoustic resonance [37], [38], [39], [17]. Moreover, researchers have used the data from gyroscopic sensors as a side channel to extract information [40], [41]. By utilizing the induction of magnetic sensors, the researchers were able to apply side-channel attacks for anti-lock braking systems [42], hard drives [35], and 3D printers [43]. Park et al. [44] implemented a spoofing attack for an IR drop sensor in medical infusion pumps so that they could control the infusion rate of the pump. Foo Kune et al. [45] demonstrated how to use electromagnetic interference to inject signals into analog sensors. In addition, researchers have demonstrated that spoofing attacks can control optical flow sensors [46] and accelerometers [8]. Our study expands this work by examining the vibration sensor of the hard drive and exploiting it to DoS HDDs.

XII. Conclusion

Adversaries without special purpose equipment can cause errors in the hard disk drive using either audible or ultrasonic acoustic waves. Audible waves vibrate the read/write head and platters; ultrasonic waves alter the output of the HDD's shock sensor, intentionally causing the head to park. These errors can lead to operating system level or application level consequences including persistent corruption and reboots. Defenses include mitigating attacks in vulnerable frequency bands with attenuation controllers, using sensor fusion to detect attacks, and noise dampening materials to attenuate the signal.

Acknowledgments

This research is supported by NSF CNS-1330142, NSFC 61472358, and a gift from Analog Devices, Inc. The views and conclusions contained in this paper are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF or ADI. We thank our shepherd Kevin Butler, the anonymous reviewers, Shane Clark, Josiah Hester, and Ben Ransford for feedback on early drafts; Tianchen Zhang for assisting with operating systems experiments; Greg Wakefield for the acoustic chamber; CERT/CC for vendor facilitation; and Barbara Zhong for assisting with experiments.

References

[1] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise," *arXiv preprint arXiv:1608.03431*, 2016.

[2] D. Sandahl, A. Elder, and A. Barnard, "The Impact of Sound on Computer Hard Disk Drives and Risk Mitigation Measures," Tyco, Michigan Technical University, Tech. Rep., 2015, https://www.ansul.com/en/us/DocMedia/T-2016367.PDF.

[3] B. Rawson and K. Green, "Inert Gas Data Center Fire Protection and Hard Disk Drive Damage," The Datacenter Journal, Tech. Rep., August 2012, http://www.datacenterjournal.com/inert-gas-data-center-fire-protection-and-hard-disk-drive-damage/.

[4] "Silent Extinguishing," Siemens, Tech. Rep., Sep. 2015, https://www.downloads.siemens.com/download-center/d/White-Paper---Silent-Extinguishing-EN-PDF_A6V10699087_hq-en.pdf?mandator=ic_bt&segment=HQ&fct=downloadasset&pos=download&id1=A6V10699087.

[5] T. Dutta and A. R. Barnard, "Performance of hard disk drives in high noise environments," *Noise Control Engineering Journal*, vol. 65, no. 5, pp. 386–395, 2017.

[6] A. Ortega, "Turning hard disk drives into accidental microphones," October 2017, ekoparty. [Online]. Available: https://github.com/ortegaalfredo/kscope/blob/master/doc/HDD-microphones.pdf

[7] K. Fu and W. Xu, "Inside risks: Risks of trusting the physics of sensors," *Communications of the ACM*, vol. 61, no. 2, pp. 20–23, Feb. 2018.

[8] T. Trippel, W. Ofir, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging Doubt on Integrity of MEMS Accelerometers by Injecting Acoustics," in *IEEE EuroS&P*, 2017.

[9] L. Corporation, "LRAD 2000X," https://www.dropbox.com/s/4qth9beayjx5gxr/LRAD_Datasheet_2000X.pdf?dl=0, 2017, accessed: 2017-05-19.

[10] A. Dayes and J. Treder, "Drive Performance-TMR," http://www.logicsmith.com/performance.html, 2017, accessed: 2017-05-15.

[11] "What is the normal operating temperature for Seagate disk drives?" 2017, accessed: 2017-05-17. [Online]. Available: http://knowledge.seagate.com/articles/en_US/FAQ/193771en

[12] H. Djojodihardjo, "Vibro-acoustic analysis of the acoustic-structure interaction of flexible structure due to acoustic excitation," *Acta Astronautica*, vol. 108, pp. 129–145, 2015.

[13] G. D. Pasquale, L. Rufer, S. Basrour, and A. Soma, "Modeling and validation of acoustic performances of micro-acoustic sources for hearing applications," *Sensors and Actuators A: Physical*, vol. 247, pp. 614–628, 2016.

[14] A. A. Mamunm, G. Guo, and C. Bi, *Hard Disk Drive: Mechatronics and Control*. CRC Press, 2006.

[15] K. O. Aung, C. Shankaran, R. Sbiaa, E. L. Tan, S. K. Wong, and S. N. Piramanayagam, "Achieving High Aspect Ratio of Track Length to Width in Molds for Discrete Track Recording Media," *Research Letters in Nanotechnology*, vol. 2008, pp. 1–4, 2008.

[16] J. Xu and R. Tsuchiyama, "Ultra-low-flying-height design from the viewpoint of contact vibration," *In Tribology International*, vol. 36, pp. 459–466, 2003.

[17] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors," in *24th USENIX Security Symposium (USENIX Security)*, 2015, pp. 881–896.

[18] J. F. Murray, G. F. Hughes, and K. Kreutz-Delgado, "Hard drive failure prediction using non-parametric statistical methods," in *Proceedings of ICANN/ICONIP*, 2003.

[19] E. Pinheiro, W.-D. Weber, and L. A. Barroso, "Failure Trends in a Large Disk Drive Population." in *USENIX FAST*, vol. 7, 2007, pp. 17–23.

[20] E. Riedel, Personal Communication, Jan. 2018.

[21] "Driver stacks," 2017, accessed: 2017-10-30. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/driver-stacks

[22] "Minidrivers, Miniport drivers, and driver pairs," 2017, accessed: 2017-10-30. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/minidrivers-and-driver-pairs

[23] "Queuing and Dequeuing IRPs," 2017, accessed: 2017-10-30. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/queuing-and-dequeuing-irps

[24] "Understanding Storage Timeouts and Event 129 Errors," 2017, accessed: 2017-10-30. [Online]. Available: https://blogs.msdn.microsoft.com/ntdebugging/2011/05/06/understanding-storage-timeouts-and-event-129-errors/

[25] "Multi-Tier Reset in Storport," 2017, accessed: 2017-10-30. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/storage/multi-tier-reset-in-storport

[26] "Interpreting Event 153 Errors," 2017, accessed: 2017-10-30. [Online]. Available: https://blogs.msdn.microsoft.com/ntdebugging/2013/04/30/interpreting-event-153-errors/

[27] "Serial ATA II Native Command Queuing Overview Application Note," Intel, Tech. Rep., Apr. 2003, http://download.intel.com/support/chipsets/imsm/sb/sata2_ncq_overview.pdf.

[28] H. S. Yang, J. Jeong, C. H. Park, and Y.-P. Park, "Identification of contributors to HDD servo errors by measuring PES only," *IEEE Transactions on Magnetics*, vol. 37, no. 2, pp. 883–887, 2001.

[29] Kim, Y., C. Kang, and Masayoshi Tomizuka, "Adaptive and optimal rejection of non-repeatable disturbance in hard disk drives," in *IEEE/ASME Int. Conf. Advanced Intelligent Mechatronics*, Monterey, California, August 2005.

[30] J. Teoh, C. Du, G. Guo, and L. Xie, "Rejecting high frequency disturbances with disturbance observer and phase stabilized control," *Mechatronics*, vol. 18, no. 1, pp. 53–60, 2008.

[31] "Design Hard-Disk Read/Write Head Controller," 2017, accessed: 2017-09-22. [Online]. Available: https://www.mathworks.com/help/control/ug/hard-disk-readwrite-head-controller.html

[32] E. Kaymak, M. Atherton, K. R. G. Rotter, and B. Millar, "Active Noise Control at High Frequencies," in *13th International Congress on Sound and Vibration*, 2006.

[33] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations," pp. 276–289, 2015.

[34] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors," in *Asia and South Pacific Design Automation Conference*, 2016, pp. 525–532.

[35] S. Biedermann, S. Katzenbeisser, and J. Szefer, *Hard Drive Side-Channel Attacks Using Smartphone Magnetic Field Sensors*. Springer Berlin Heidelberg, 2015.

[36] D. Genkin, A. Shamir, and E. Tromer, "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis," in *International Cryptology Conference 2014 (CRYPTO)*, Santa Barbara, California, August 2014.

[37] S. Castro, R. Dean, G. Roth, G. T. Flowers, and B. Grantham, "Influence of acoustic noise on the dynamic performance of MEMS gyroscopes," in *ASME 2007 International Mechanical Engineering Congress and Exposition*. American Society of Mechanical Engineers, 2007, pp. 1825–1831.

[38] R. N. Dean, S. T. Castro, G. T. Flowers, G. Roth, A. Ahmed, A. S. Hodel, B. E. Grantham, D. A. Bittle, and J. P. Brunsch, "A characterization of the performance of a MEMS gyroscope in acoustically harsh environments," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 7, pp. 2591–2596, 2011.

[39] R. N. Dean, G. T. Flowers, A. S. Hodel, G. Roth, S. Castro, R. Zhou, A. Moreira, A. Ahmed, R. Rifki, B. E. Grantham *et al.*, "On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise," in *IEEE International Symposium on Industrial Electronics*, 2007, pp. 1435–1440.

[40] B. Farshteindiker, N. Hasidim, A. Grosz, and Y. Oren, "How to Phone Home with Someone Elses Phone: Information Exfiltration Using Intentional Sound Noise on Gyroscopic Sensors," in *10th USENIX Workshop on Offensive Technologies*, 2016.

[41] Y. Michalevsky, D. Boneh, and G. Nakibly, "Gyrophone: Recognizing Speech from Gyroscope Signals." in *USENIX Security*, 2014, pp. 1053–1067.

[42] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2013, pp. 55–72.

[43] C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, and W. Xu, "My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks Against 3D Printers," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2016, pp. 895–907.

[44] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, "This aint your dose: Sensor Spoofing Attack on Medical Infusion Pump," in *10th USENIX Workshop on Offensive Technologies*, 2016.

[45] D. Foo Kune, J. Backes, S. S. Clark, D. B. Kramer, M. R. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors," in *Proceedings of the 34th Annual IEEE Symposium on Security and Privacy*, May 2013.

[46] D. Davidson, H. Wu, R. Jellinek, T. Ristenpart, C. Tech, and V. Singh, "Controlling UAVs with sensor input spoofing attacks," in *10th USENIX Workshop on Offensive Technologies*, 2016, pp. 221–231.

[47] "Lumped Loudspeaker Driver," 2017, accessed: 2017-10-09. [Online]. Available: https://www.comsol.it/model/download/386391/models.aco.lumped_loudspeaker_driver.pdf

[48] D. Don and E. Patronis, *Sound system engineering*. CRC Press, 2014.

[49] H. Çalloğlu, E. Demir, Y. Ylmaz, and Z. Girgin, "Vibration behavior of a radially functionally graded annular disc with variable geometry," *Science and Engineering of Composite Materials*, vol. 21(3), pp. 453–461, 2017.

[50] S. W. Kang, J. M. Lee, and Y. J. Kang, "Vibration analysis of arbitrarily shaped membranes using non-dimensional dynamic influence function," *Journal of Sound and Vibration*, vol. 221, pp. 117–132, 1999.

[51] N. Fantuzzi, F. Tornabene, and E. Viola, "Generalized Differential Quadrature Finite Element Method for vibration analysis of arbitrarily shaped membranes," *International Journal of Mechanical Sciences*, vol. 79, pp. 216–251, 2014.

APPENDIX A
FEM MODEL DETAILS

We built a 3D Finite Element Model (FEM) to study the effect of acoustic interference on hard disks using COMSOL (Figure 16).

The goal of our simulation is to give evidence that: (i) the throughput loss is mainly caused by an abnormal displacement between the head disk assembly and the disk; and (ii) this displacement is because of the mechanical vibrations induced by the acoustic interference.

Our analysis explores an example of physical proximity attack scenario, with the hard drive positioned at 10 cm from the speaker (Figure 17).

The model estimates, for the head stack assembly top head suspension, a horizontal/vertical maximum displacement of roughly 8 nm and 112 nm respectively; and for the top disk a maximum horizontal/vertical displacement of about 33 nm and 156 nm respectively (Figure 5).

This stationary model highlights how the magnitude of our attack can induce head stack assembly position errors considering the track read/write thresholds (15/10 percentage of the track width respectively) [15] and the distance between the head and the disk (roughly 6 nm) [16].

Model Mechanics. The model explores the fine-grained physics of how sound waves affect the mechanical parts composing the hard drive, exposing how: (i) the attack mainly affects the head stack assembly and the disks; (ii) the magnitude of the vibration effect depends from the sound pressure generated by the source, i.e. the more the sound pressure increases, the greater is the mechanical vibration induced to the hard drive.

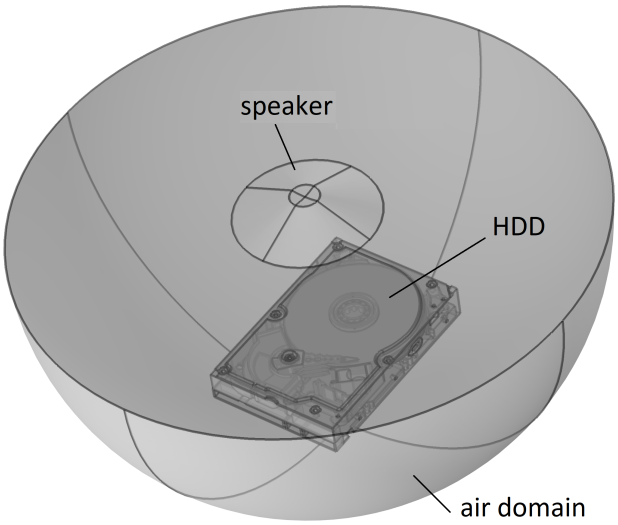


Fig. 16. The complete geometry of the 3D COMSOL model. The speaker diaphragm and the dust cap are positioned at the top of the air domain semi-sphere to replicate an example of physical proximity attack scenario.

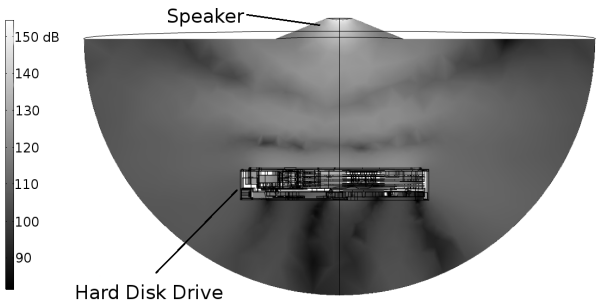


Fig. 17. Vertical cross-section plot of the sound pressure level distribution generated by the speaker at 5 kHz frequency. The model replicates a physical proximity attack scenario with the hard drive positioned at 10 cm from the sound source. Note how the sound pressure level decreases with distance following the Inverse Square Law.

A radius cone, set in an infinite baffle, represents the diaphragm and the dust cap of a common speaker. A known sound pressure applied on the dust cap boundary simulates the generated acoustic interference [47]. We designed the mechanical structure of the hard disk in SolidWorks-CAD 3.5. The model includes four read/write heads, an actuator bearing, a voice coil motor, magnets, a spindle, three disks, and the HDD chassis. A semi-sphere represents the acoustic radiation domain of the model, truncated with a Perfectly Matched Layer (PML) to mimic an infinite open air domain.

A 100 Pa sound wave at 5 kHz generated by the simulated speaker reaches the hard drive and causes mechanical deformations. Considering for example 10 cm of distance between the sound source and the HDD, the sound pressure level measured on the chassis surface is about 120 dB SPL (Figure 17). This follows the Inverse Square Law, i.e. the sound pressure level of a spherical wave decreases with doubling of the distance by -6 dB [48].

Halving the sound pressure of the source to 50 Pa, while maintaining the same frequency and distance from the hard drive, the total displacement of the head assembly top head suspension and disks halved too.

Increasing the sound pressure of the source to 360 Pa, the total displacement of the head assembly top head suspension increases to a horizontal/vertical displacement of about 26 nm and 300 nm, respectively. The top disk, on the other hand, reaches a horizontal/vertical total displacement of roughly 50 nm and greater than 1 m, respectively.

The latter analysis highlights how the sound pressure induced by the speaker increases the mechanical displacement of both disks and head assembly of one order of magnitude. This phenomenon significantly increases the probability of performance degradation and throughput loss, because of the possibilities of the read/write head exceeding the read/write fault thresholds or head crashes.

Model limitations. There are two main limitations of this model. (i) The model is stationary, i.e. it does not consider the spindle system rotation. (ii) The simulation does not consider all the dynamics of the hard drive components such as fluid or ball pivot bearing effects.

Despite these assumptions, the simulation is consistent with previous studies in terms of free vibrations and mode shapes of both disks and head assembly under acoustic interference attack [49], [50], [51].

Furthermore, the simulation correctly predicts the throughput loss investigated in our dynamic study (Section IV).