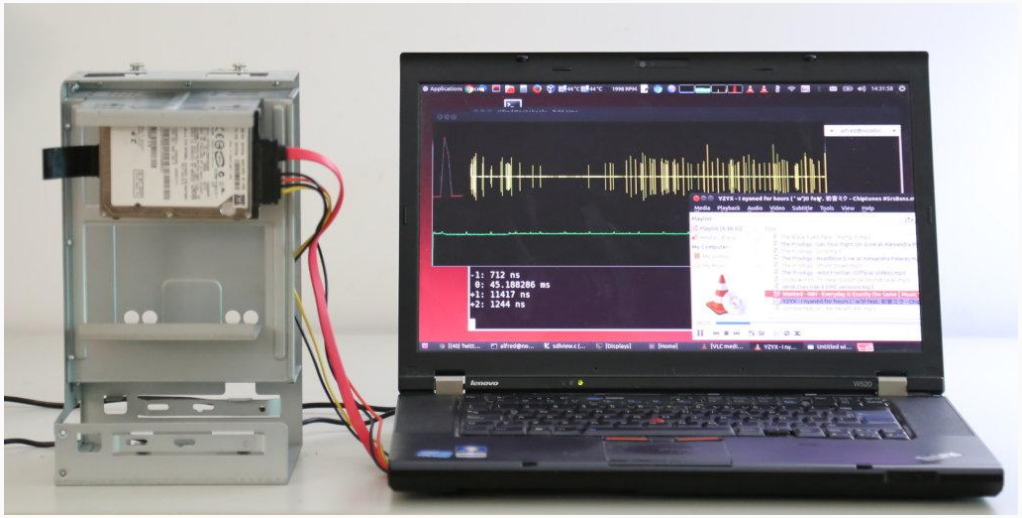
Sonic attacks to spinning hard drives

H2HC 2018

Alfredo Ortega

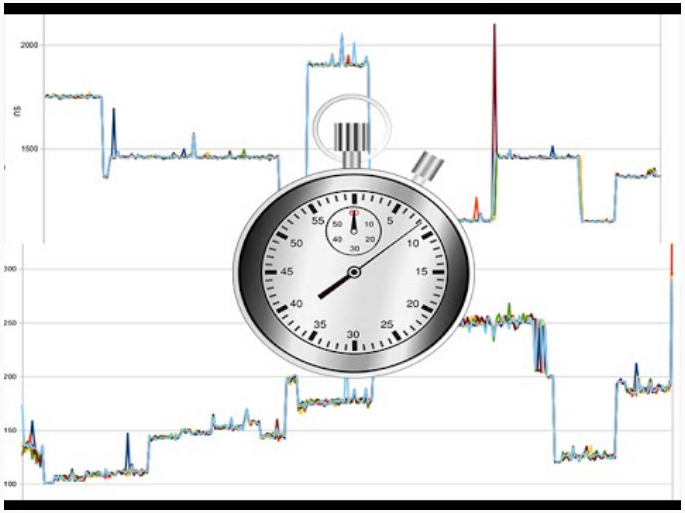
October 20, 2018

Table of contents



Introduction

Introduction



- Problem: Too much time measurement precision.
- Measuring time you can learn things you should not
- This is called a timing attact or timing side-channel attack.

Introduction: how this technique works

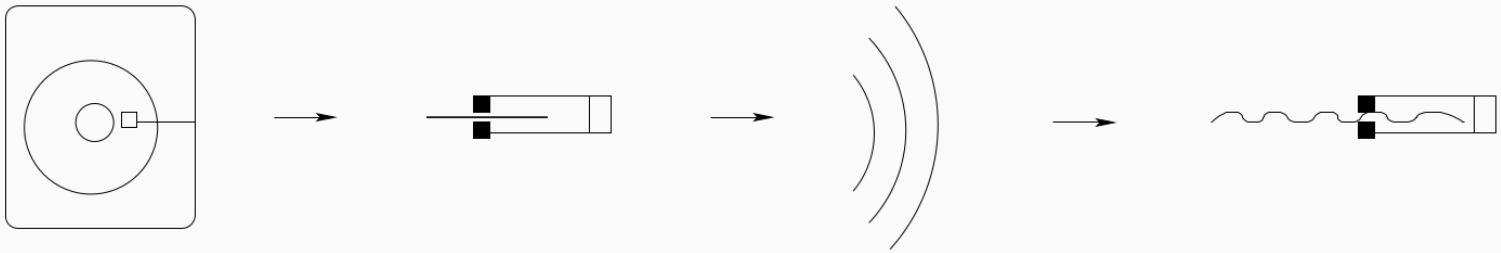


Figure 1: Effect of sound on HDDs

```
inline void measure(void) {
read(fd,buf,DISK_BUF_BYTES);
}
```

Introduction: Syscall timing

- We target the read() syscall.
- Read a sector and measure the time. That's it.

What about all other 150 syscalls?

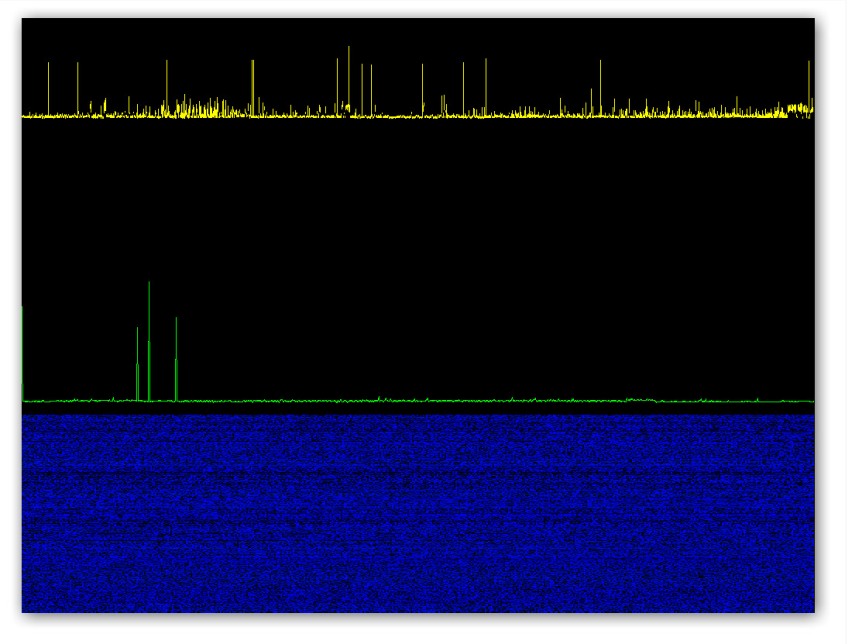


Figure 2: Kscope utility (stat() syscall)

Demo 1

Demo 1: kscope on different syscalls

Measurements

Frequency response (case)

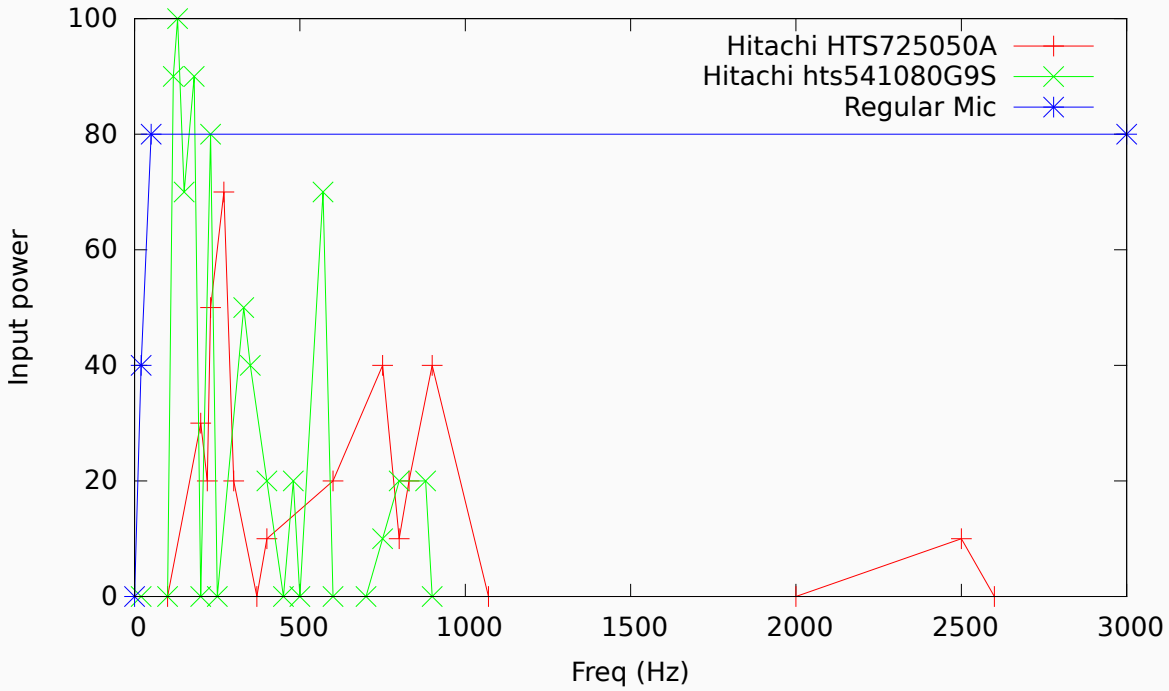


Figure 3: Disk in metal case

Frequency response (alone)

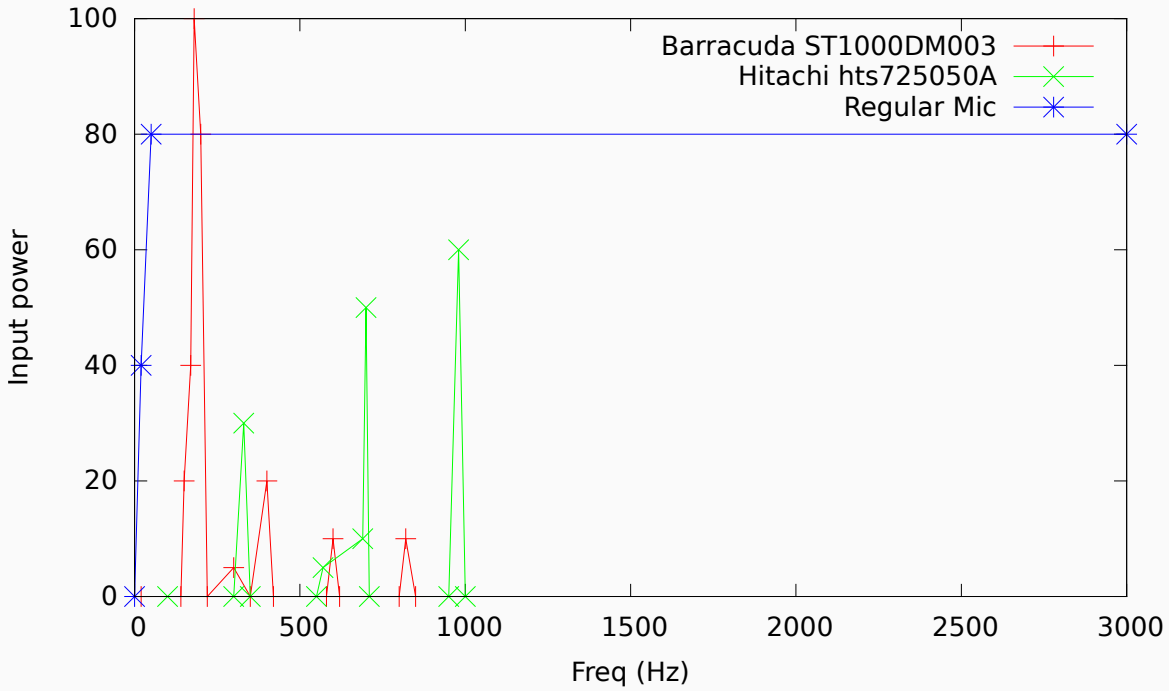


Figure 4: Disk alone (on table)

Setup

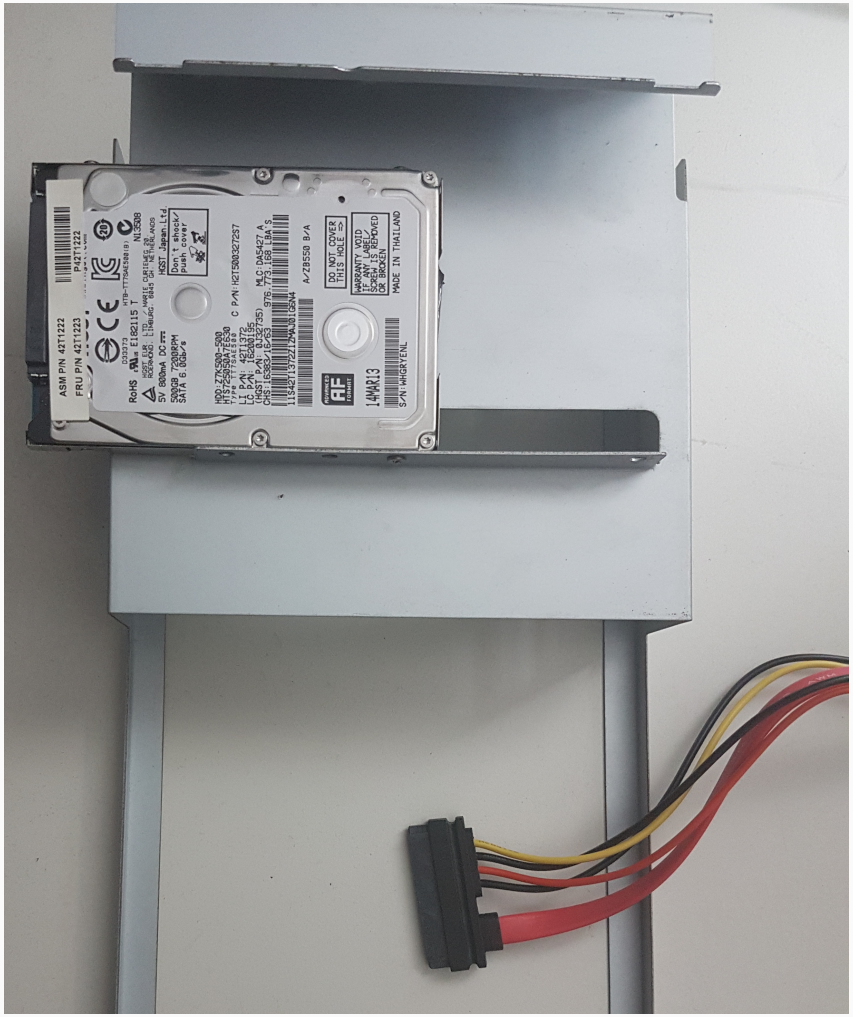


Figure 5: Disk case (setup)

Hdd: Pulse shape

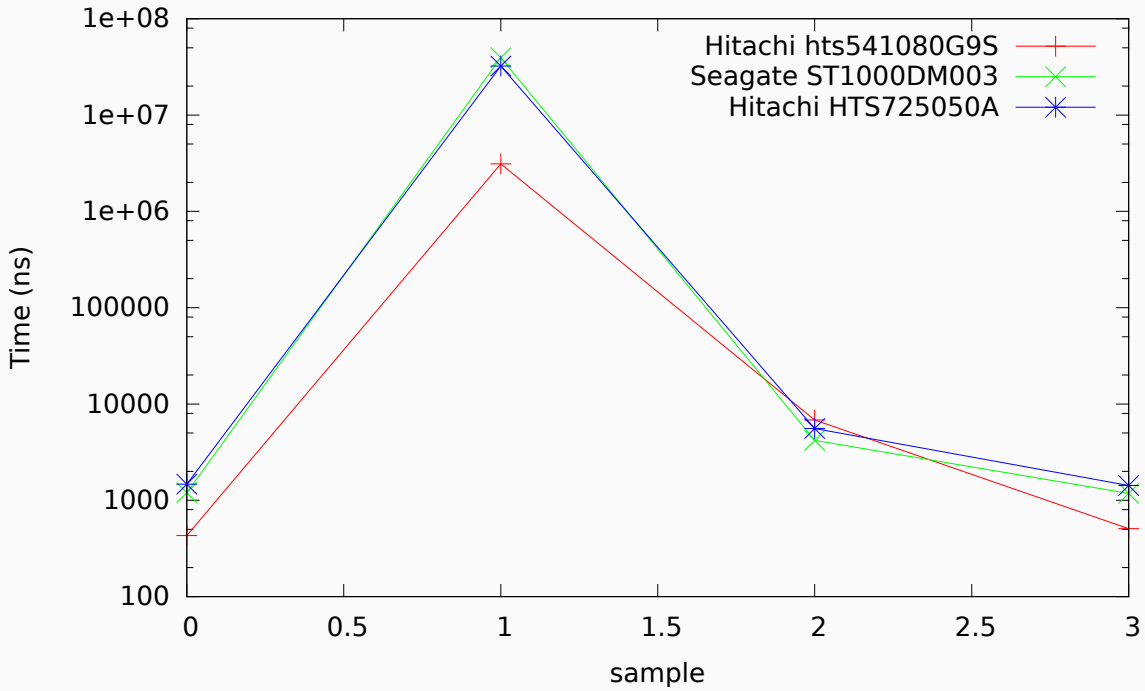


Figure 6: Smallest pulse shape several Hdds

Very slow sample rate

minimum 25 ms, 40hz, probably can be improved a lot.

What can be detected?

- High-intensity, mostly low-freq sound
- Movement
- Vibrations

Possible fixes

- Randomize syscall return time
- Make high-precision timers a privileged operation

Demos

Demo 2

Demo 2: Distance measurment

Demo 3

VM scape

Also work on VPSs?

Attacking HDDs with sound?

- Resonance attacks
- Previous work: Stuxnet
- It is possible?

Demo 4: Yes, attacking HDDs with sound

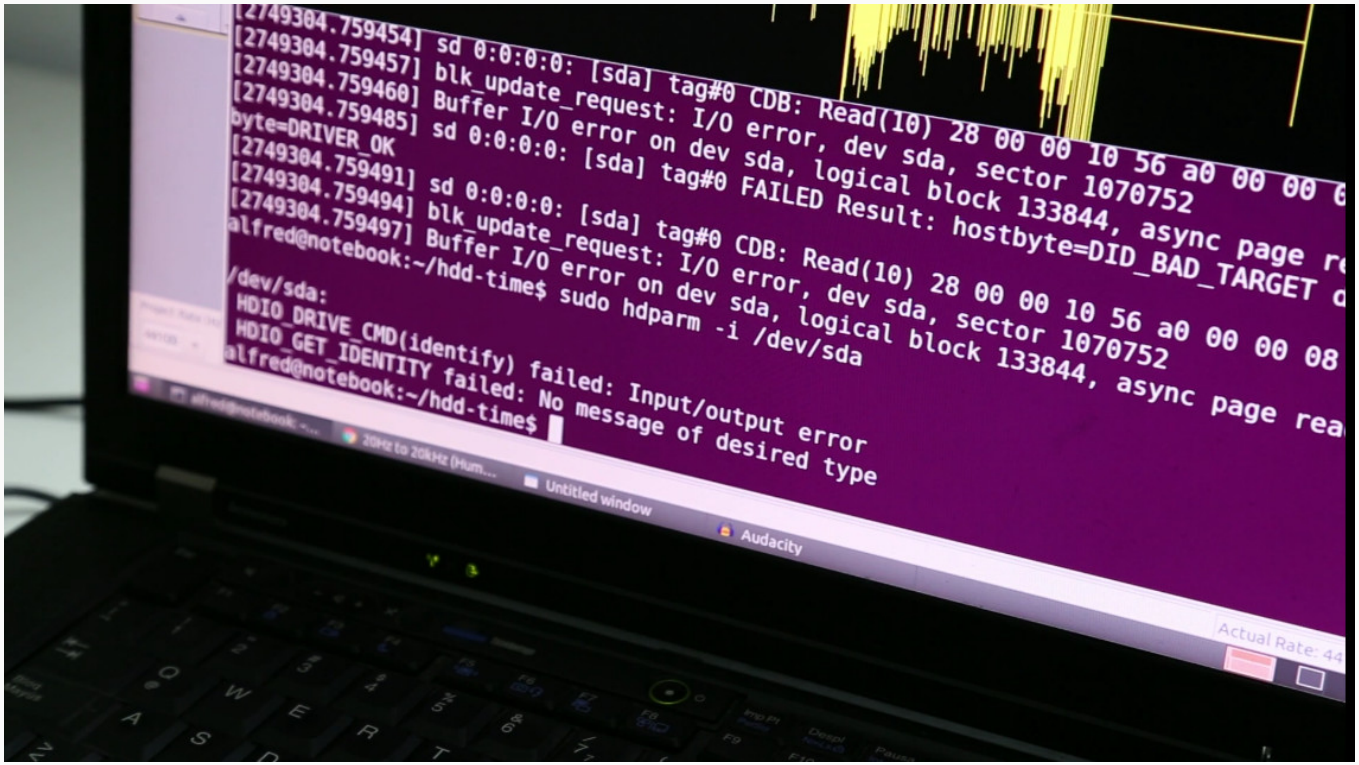


Figure 7: (Video) https://www.youtube.com/watch?v=8DdqTz3CW5Y

Attacking HDDs with sound

- HDD can be DOSed by finding the resonant frequency
- OS disconnects it after a while.
- Physical damage possible (Demo 5)

Similar works: Michigan Uni: Bluenote

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

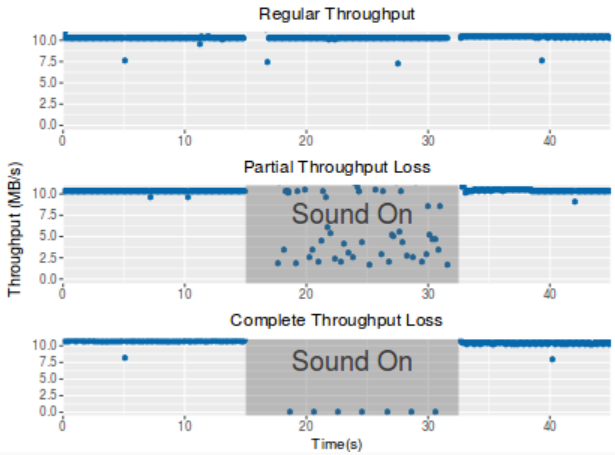


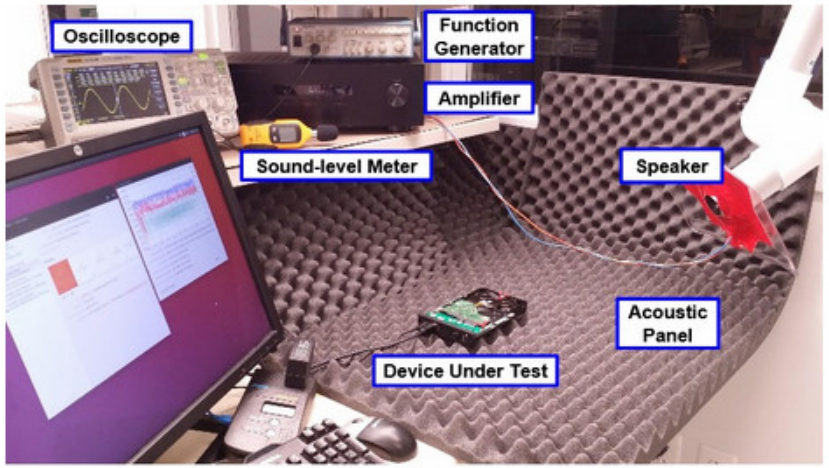
Figure 8: Bluenote: 2018 IEEE Symposium on Security and Privacy (SP) (2018)

Similar works: Purdue/Princeton Uni: HDD attack

New research shows practicality of HDD acoustic attacks

Last week, scientists from the Princeton and Purdue universities published new research into the topic, expanding on the previous findings with the results of additional practical tests.

The research team used a specially crafted test rig to blast audio waves at a hard drive from different angles, recording results to determine the sound frequency, attack time, distance from the hard drive, and sound wave angle at which the HDD stopped working.



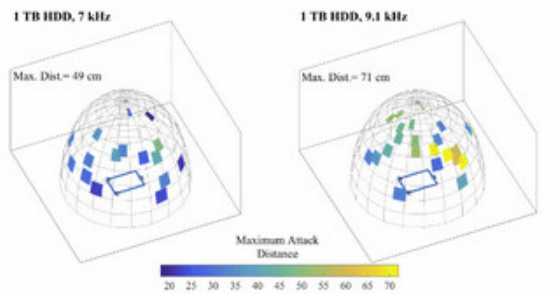


Fig. 1. Experimental setup for performing acoustic attacks.

Figure 9: Acoustic Denial of Service Attacks on HDDs: Princeton, Purdue Univ. (2018)

Conclusion

- Timing attacks on Hdds read delay can be used as poor microphones.
- Can be used with no/few privileges.
- Can jump across VM boundaries.
- Can be used remotely in cloud settings.
- Privacy problem in general.
- Temporal/Permanent damege using resonance attacks on HDD.

References I

Thank you!

Follow me on twitter for updates: @ortegaalfredo