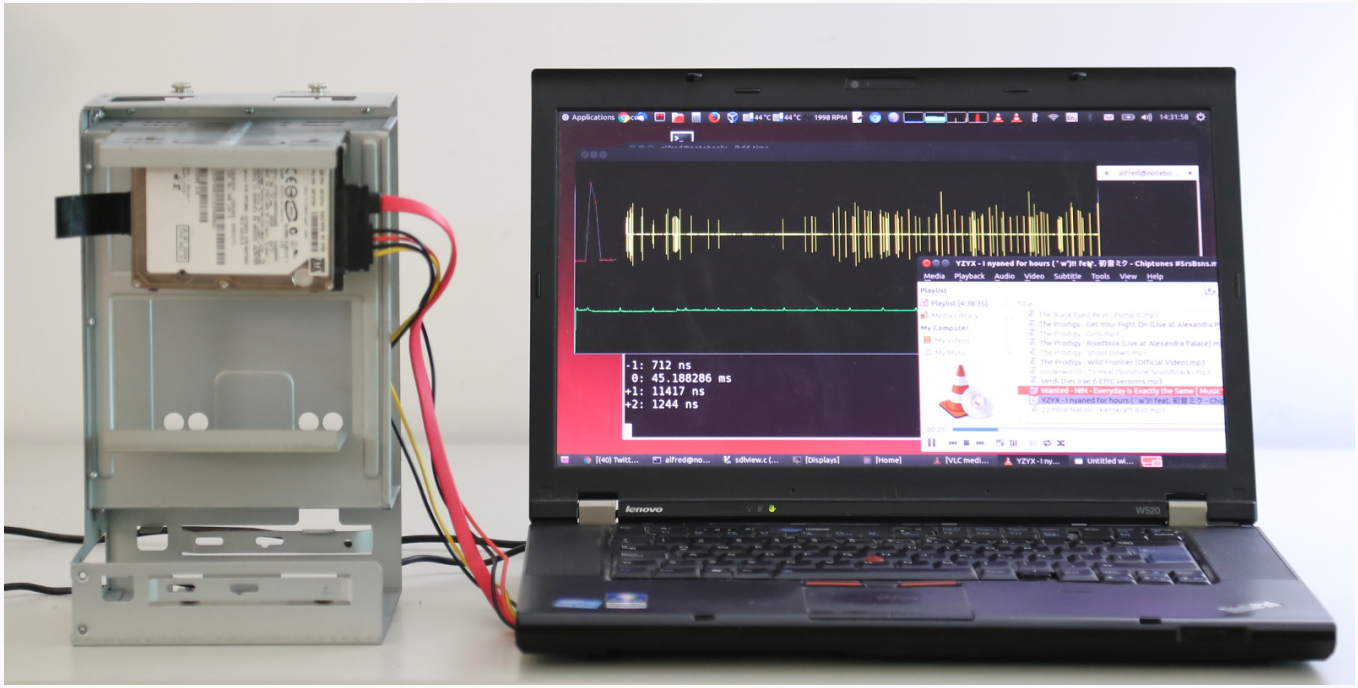
Turning hard disk drives into accidental microphones

Ekoparty 2017

Alfredo Ortega

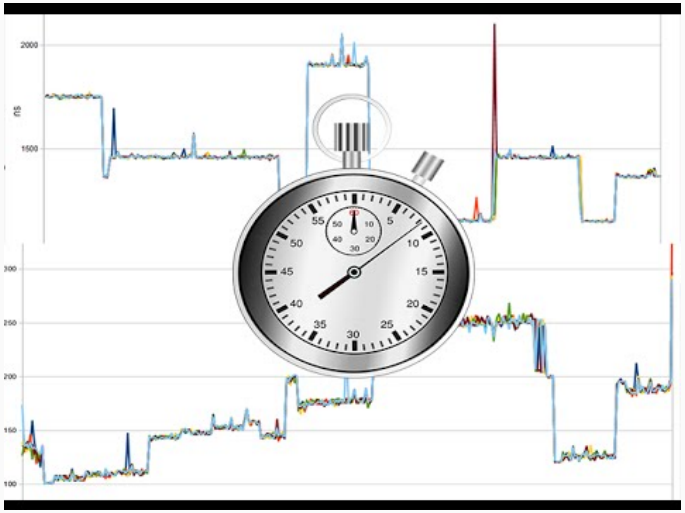
October 4, 2017

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 it works

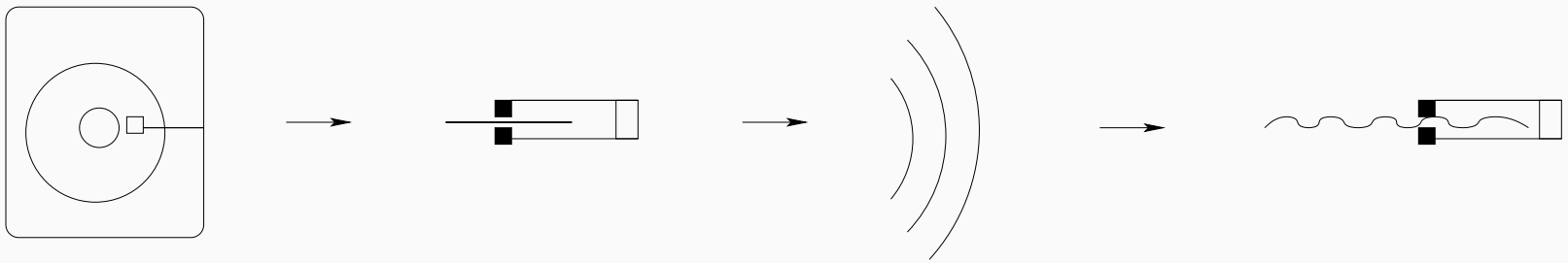


Figure 1: Effect of sound on HDDs

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

Introduction: Syscall measurements

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

What about all other 150 syscalls?

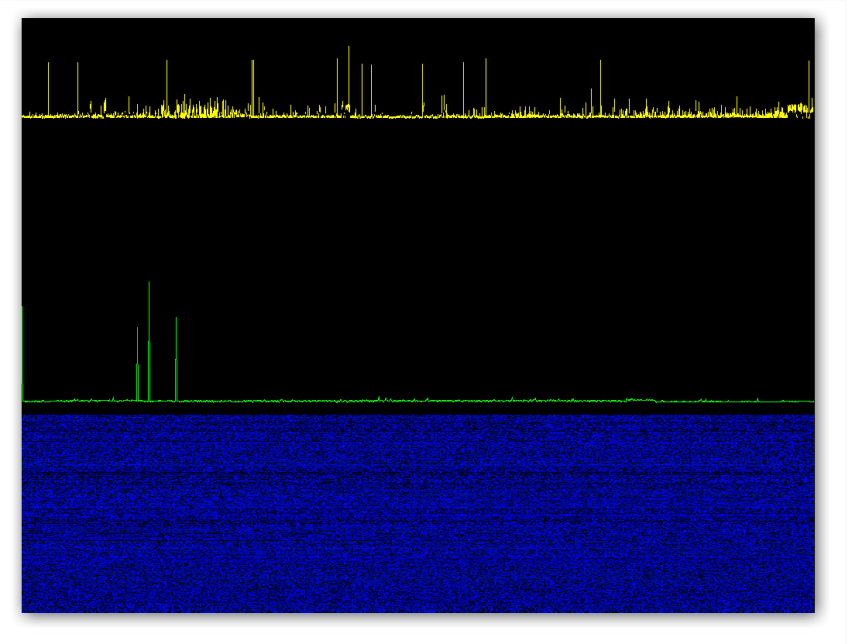


Figure 2: Kscope utility (stat() syscall)

Demo 1

Demo 1: kscope on different syscalls

Measurements

Frequency response (case)

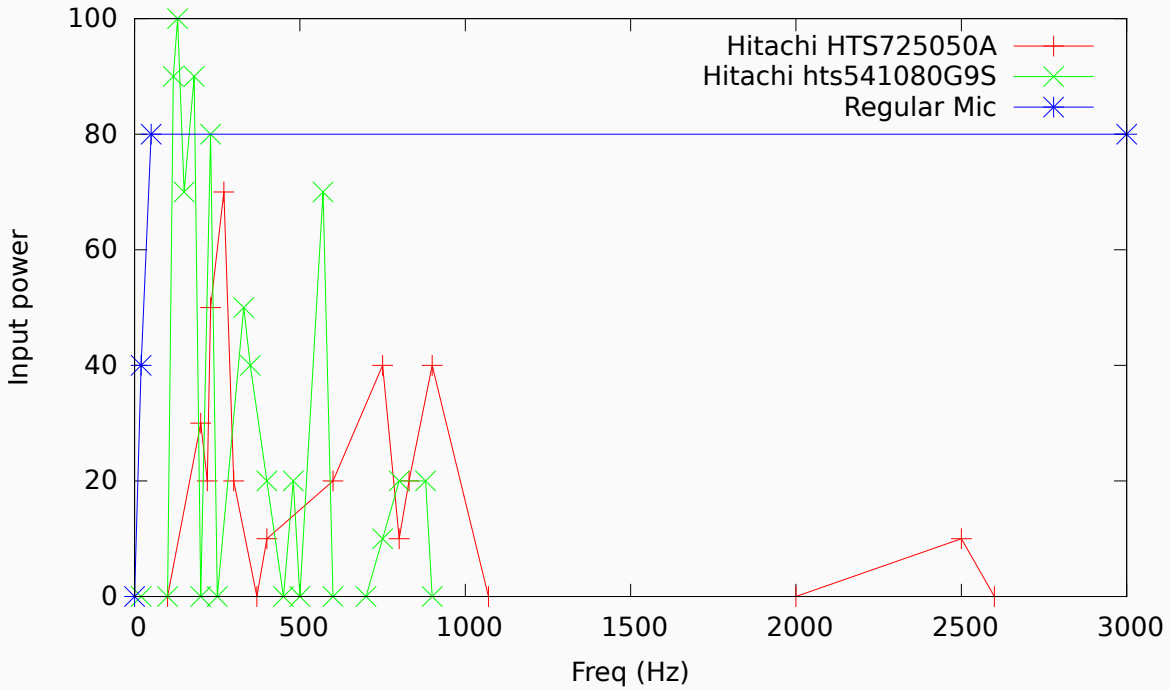


Figure 3: Disk in metal case

Frequency response (alone)

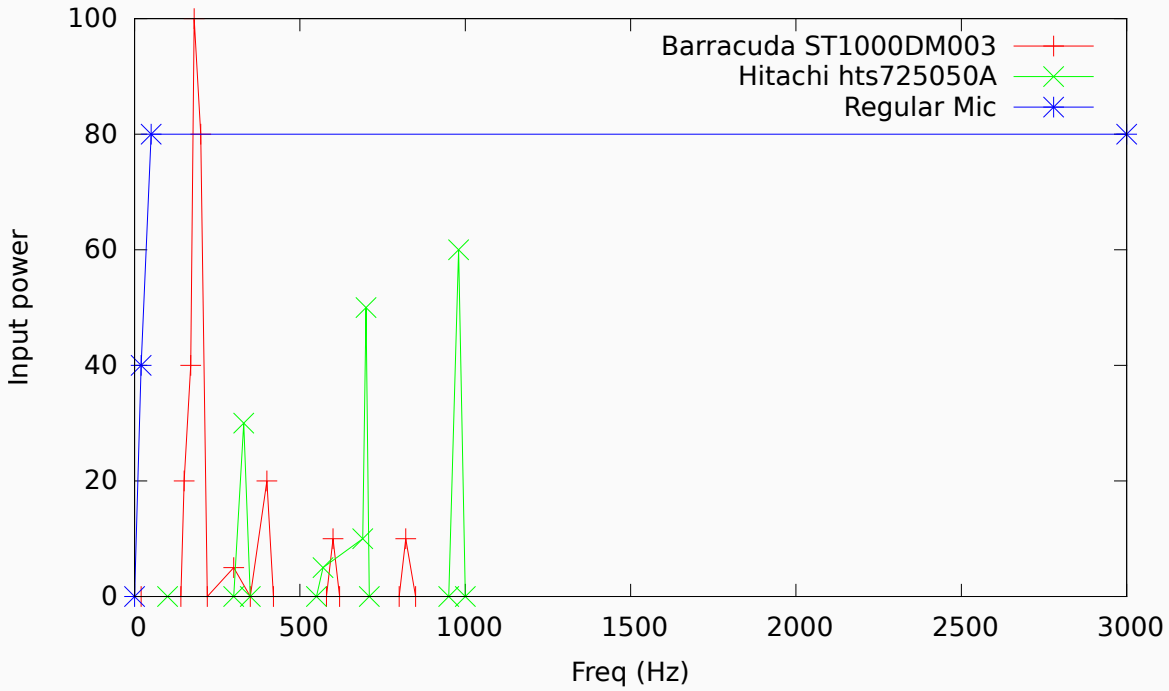


Figure 4: Disk alone (on table)

Setup

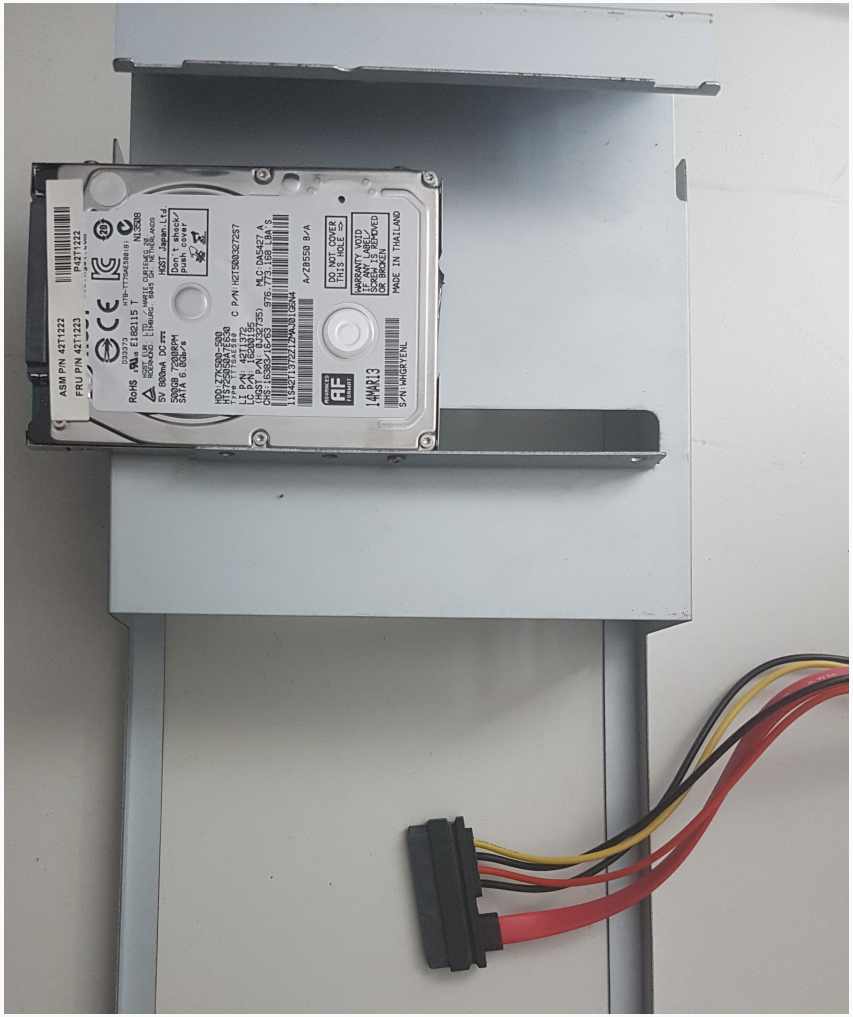


Figure 5: Disk case (setup)

Hdd: Pulse shape

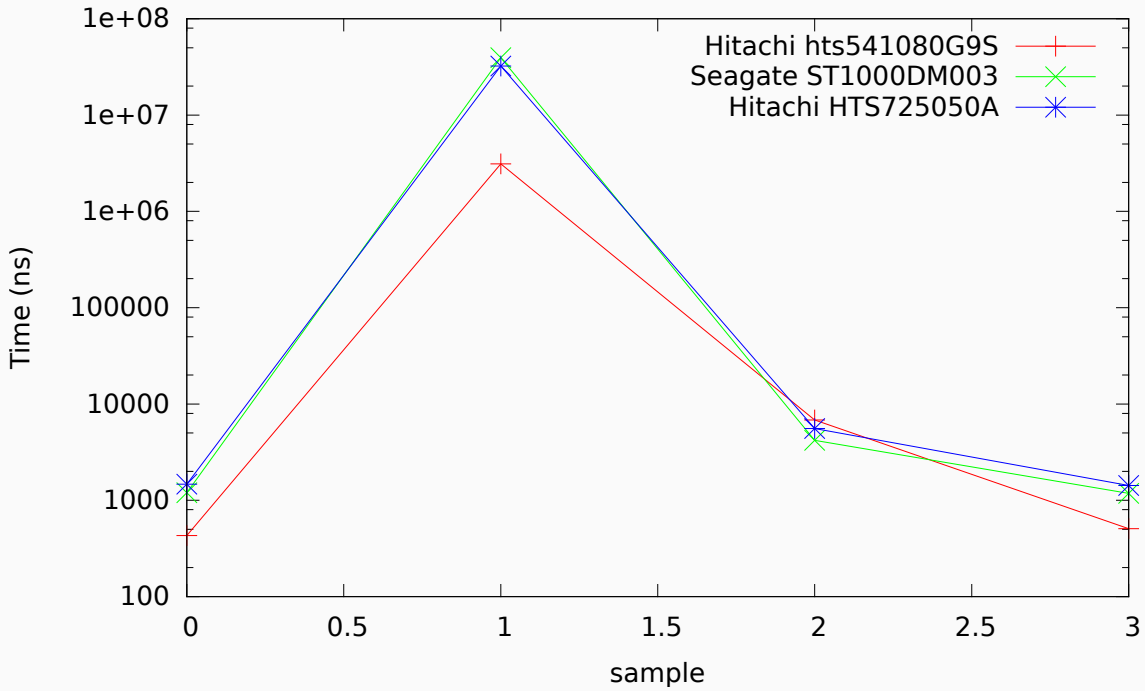


Figure 6: Smallest pulse shape several Hdds

Very slow sample rate

minimum 25 ms, 40hz, probably can be improved considerably.

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 1: Distance measurment

Demo 3

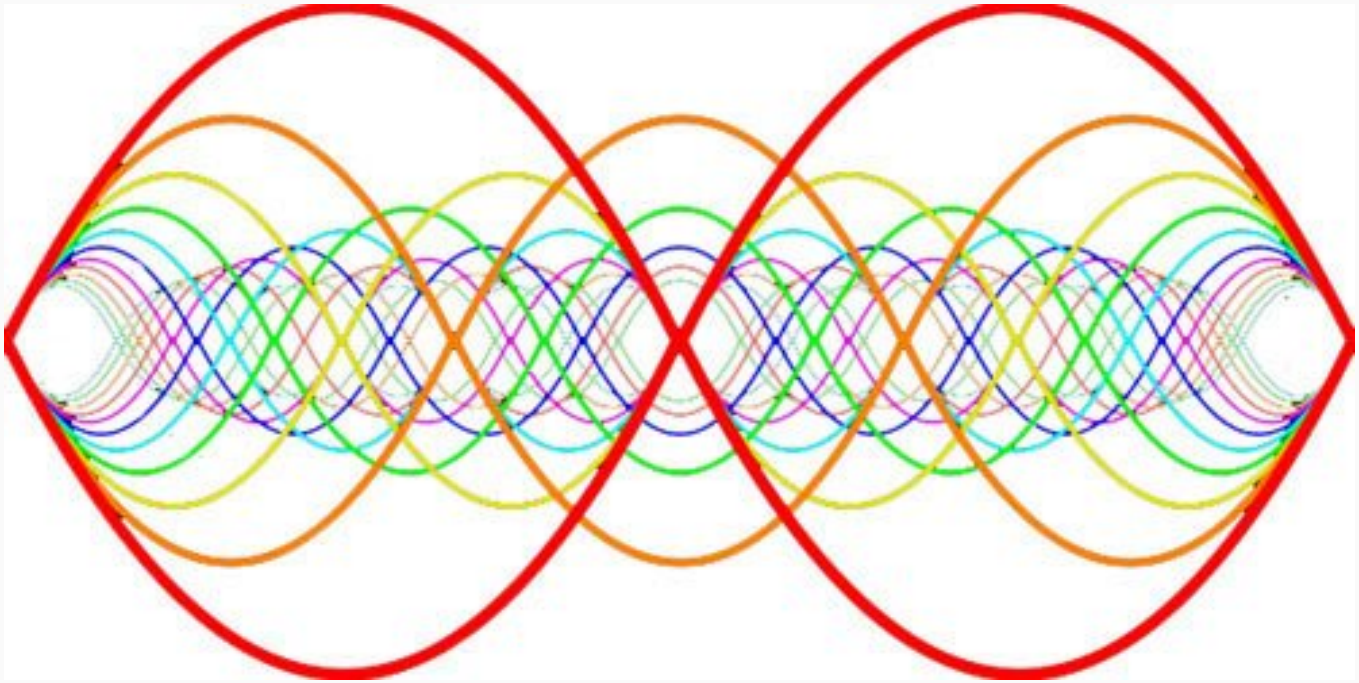
VM scape

Also work on VPSs?

Attacking HDDs with sound?

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

Demo 4: Yes, attacking HDDs with sound



Attacking HDDs with sound

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

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

Source: https://github.com/ortegaalfredo/kscope

Thank you!