The Physics of Cybersecurity: Tickling Sensors with Malicious Sound Waves and RF

Kevin Fu

Associate Professor
Computer Science & Engineering
University of Michigan

web.eecs.umich.edu/~kevinfu/
kevinfu@umich.edu

AAAS
February 2019

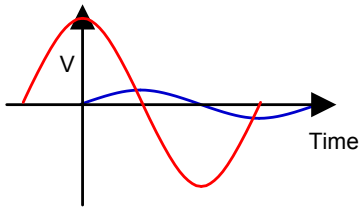
Supported in part by NSF CNS-1330142. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

Correctness is easy.

Security is hard.

Photo by Kevin Fu

Analog Side Channels



Analog **Digital**

"Read"
Property: Confidentiality
Spectre, Meltdown, …

"Read"
Property: Confidentiality
Example: Power Analysis

"Write"
Property: Integrity
Example: Sensors

Sensor Pain is Everywhere

COMMUNICATIONS OF THE ACM | FEBRUARY 2018

DOI:10.1145/3176402

Inside Risks

Risks of Trusting the Physics of Sensors

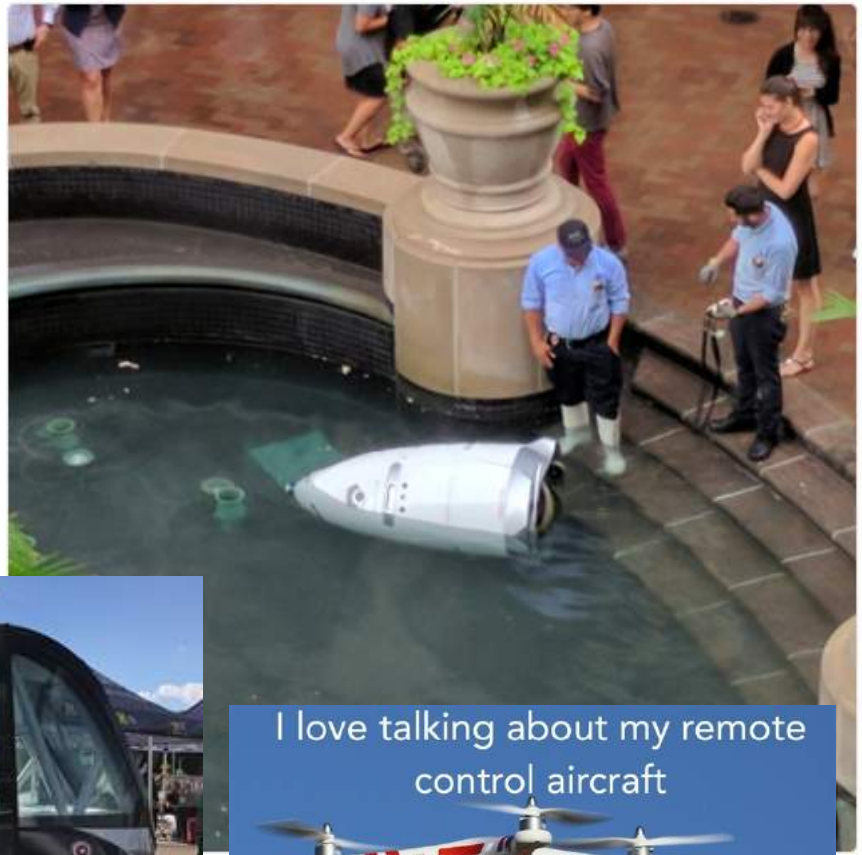
Protecting the Internet of Things with embedded security.

Internet of Shit Retweeted

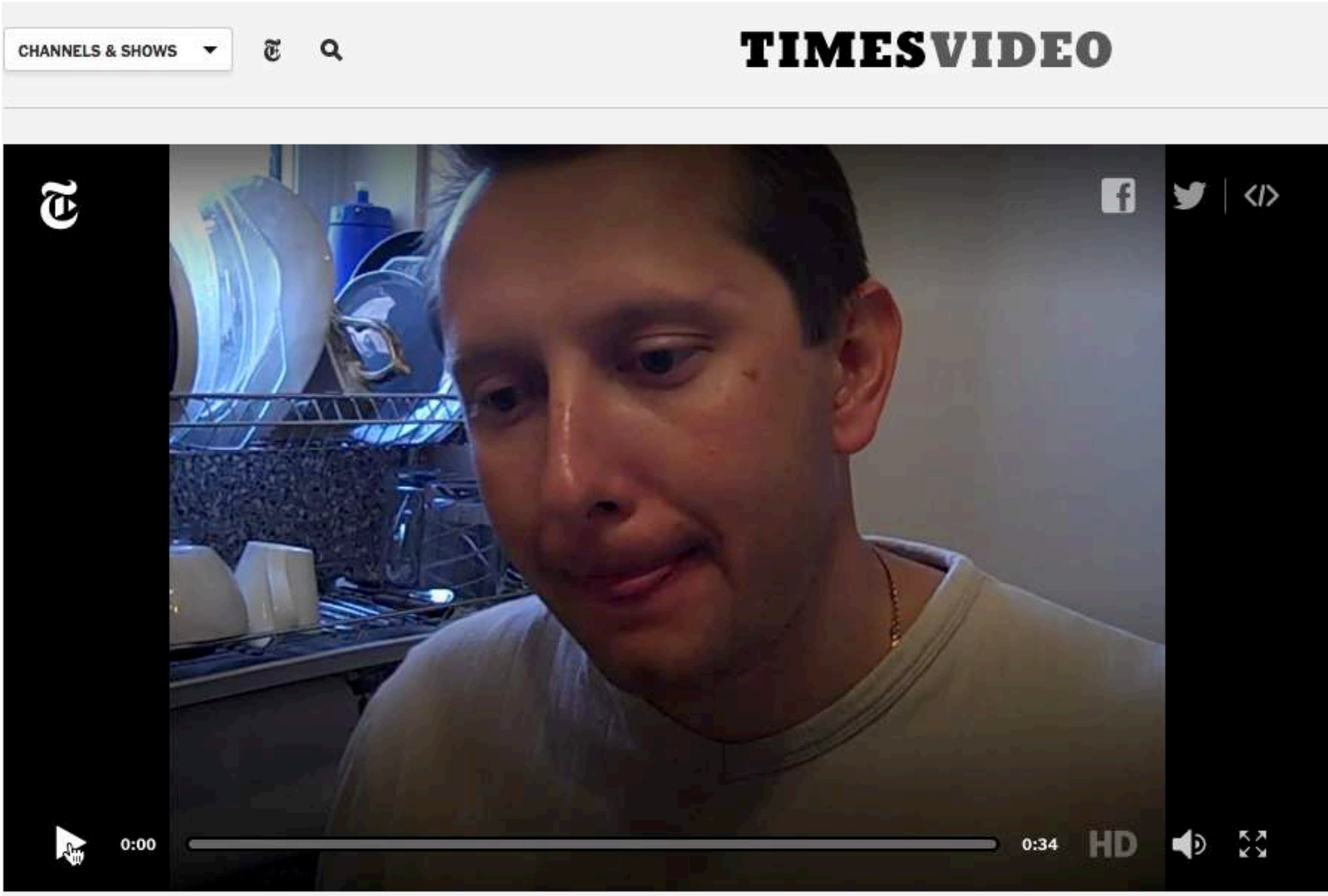
Bilal Farooqui @bilalfarooqui · Jul 17

Our D.C. office building got a security robot. It drowned itself.

We were promised flying cars, instead we got suicidal robots.

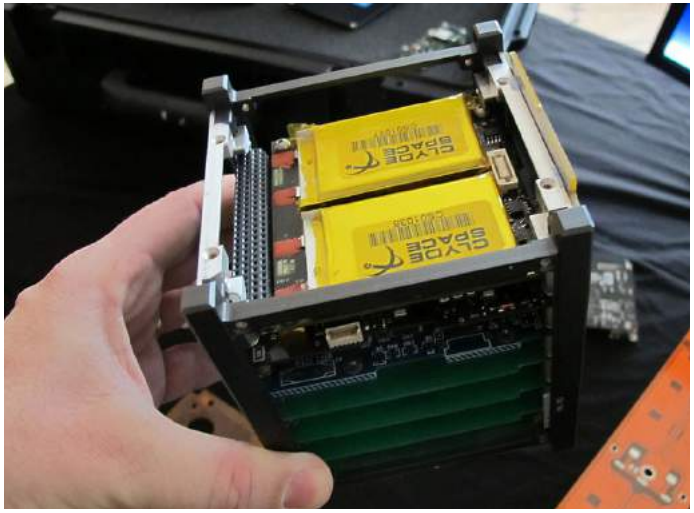


http://auto.howstuffworks.com/



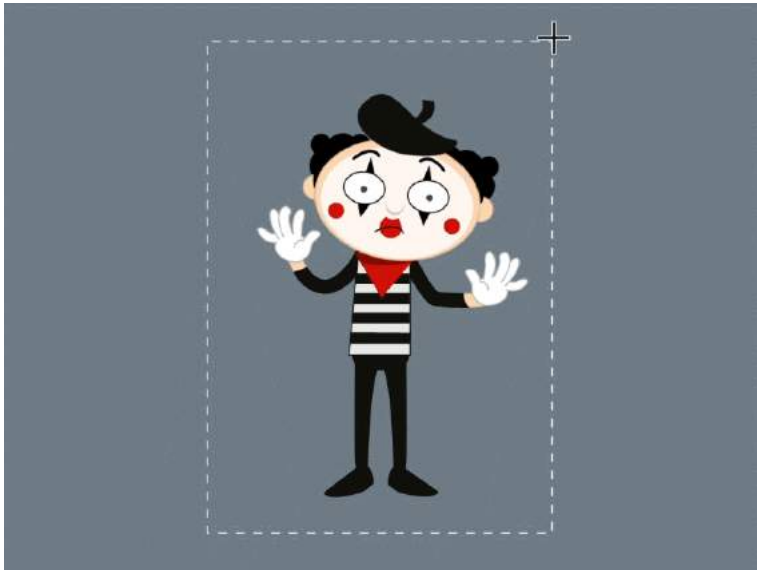
https://www.nytimes.com/video/multimedia/1247464146747/mobile-phone-turns-on-oven.html

Sensors are Everywhere



Digital Abstraction != Force Field

intentional interference violates assumption of **sensor output integrity**



- Vibration
- Acoustics
- RF
- Light
- Heat

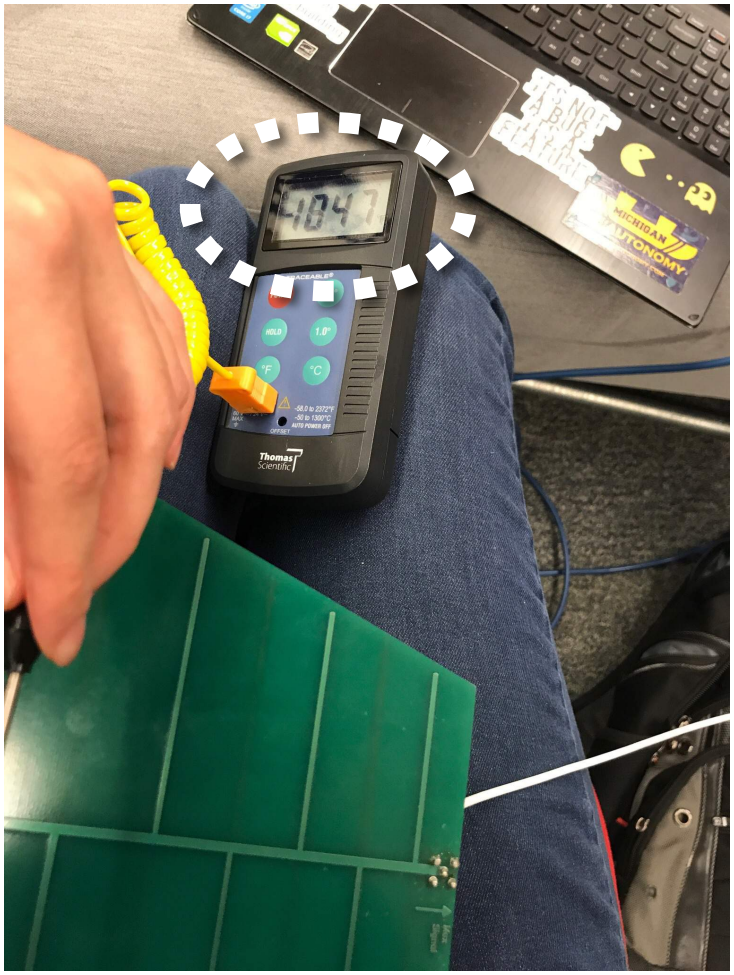
⟹ Sensor spoofing

https://dribbble.com/shots/2281625-Marquee-Tool-Mime

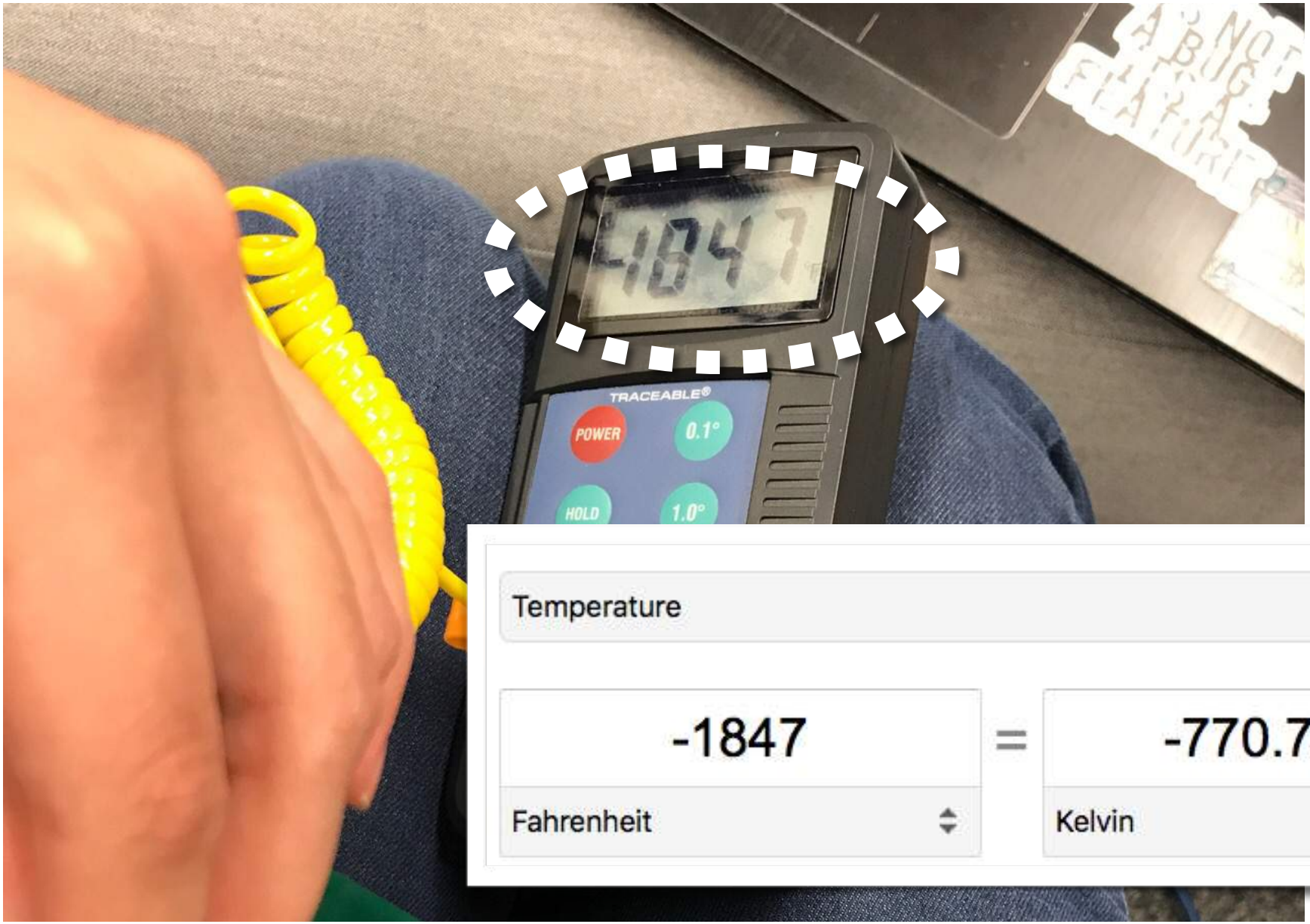
Do Not Blindly Trust Sensors

Sensors are a proxy for reality

- **Thermocouple interpolates from a voltage potential**
- **Not necessarily temperature**



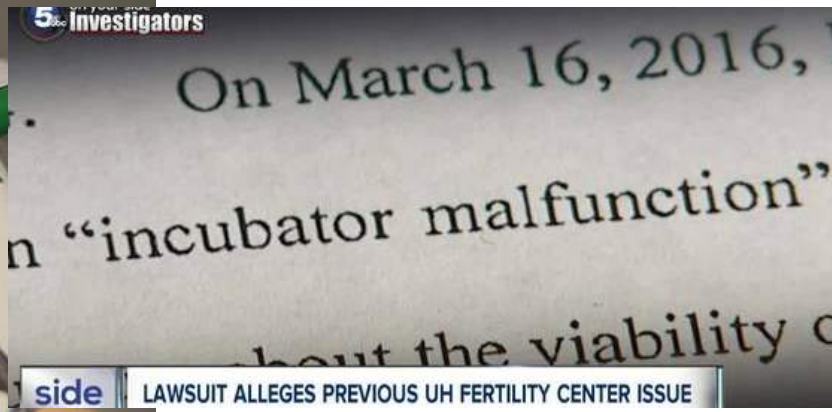
Absolute Zero Day Attack



Temperature

-1847	=	-770.7389
Fahrenheit		Kelvin

Where Do Thermocouples Matter?



At Risk: Closed-Loop Feedback Systems

Photos: NBC Today, ABC News5 Cleveland

Blog / Temperature measurements and temperature control in the IVF lab are crucial for your results

Temperature measurements and temperature control in the IVF lab are crucial for your results

Posted by Jaco Geyer, Jan 26, 2016 6

Intentional Electromagnetic Interference (Or Don't Trust Your Sensors)

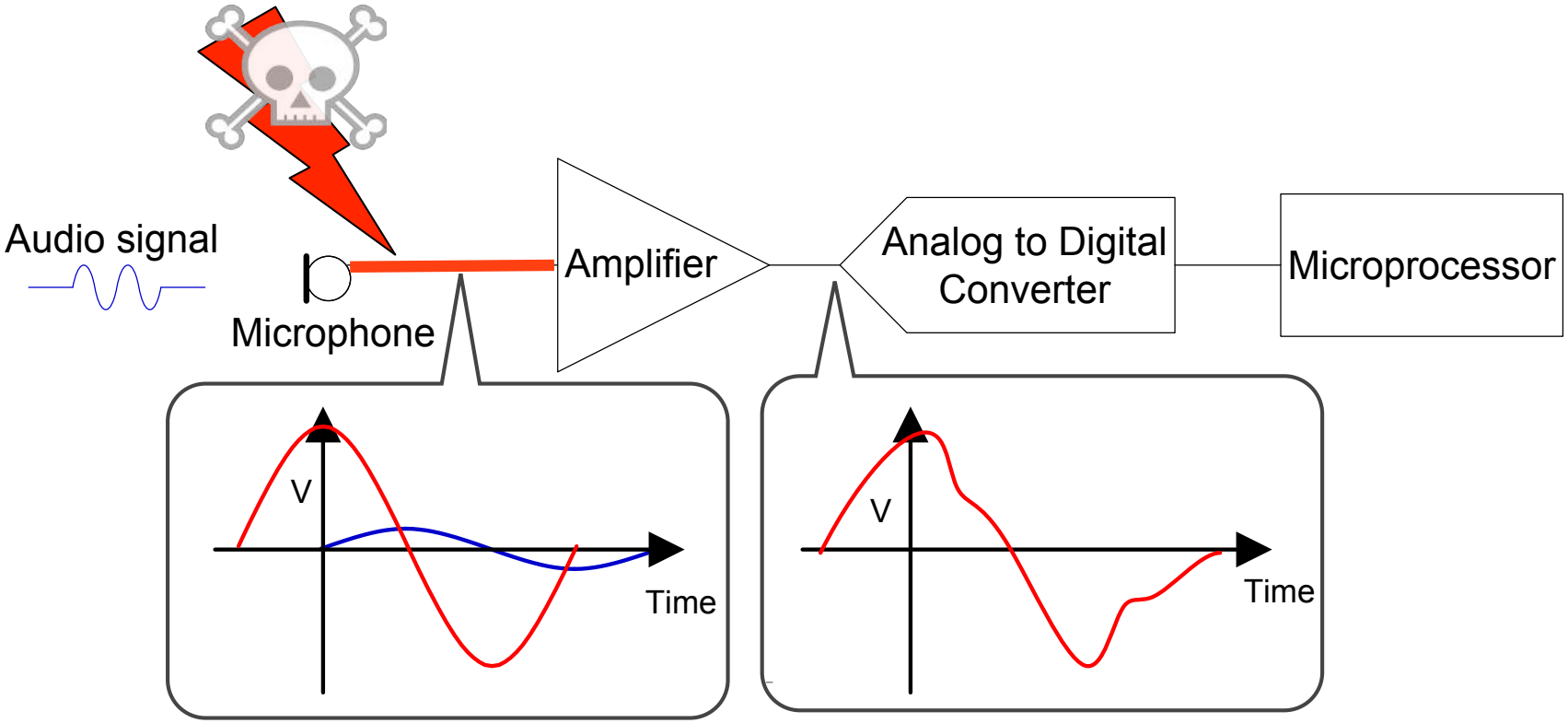
"Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors" by Foo Kune et al. In Proc. IEEE Symposium on Security and Privacy, 2013.

Joint work with Denis Foo Kune (U. Michigan),
John Backes (U. Minnesota), Shane Clark (U. Mass Amherst),
Dr. Dan Kramer (Beth Israel Deaconess Medical Center),
Dr. Matthew Reynolds (Harvard Clinical Research Institute),
Yongdae Kim (KAIST), Wenyuan Xu (U. South Carolina)

Supported in part by NSF CNS- 1035715, CNS-0845671, CNS-0923313, GEO-1124657, S121000000211, HHS 90TR0003/01, the Sloan Research Fellowship, the University of Minnesota Doctoral Dissertation fellowship, the Korean MEST NRF 2012-0000979, the Harvard Catalyst/Harvard Clinical and Translational Science Center MeRIT career development. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the HHS or NSF.

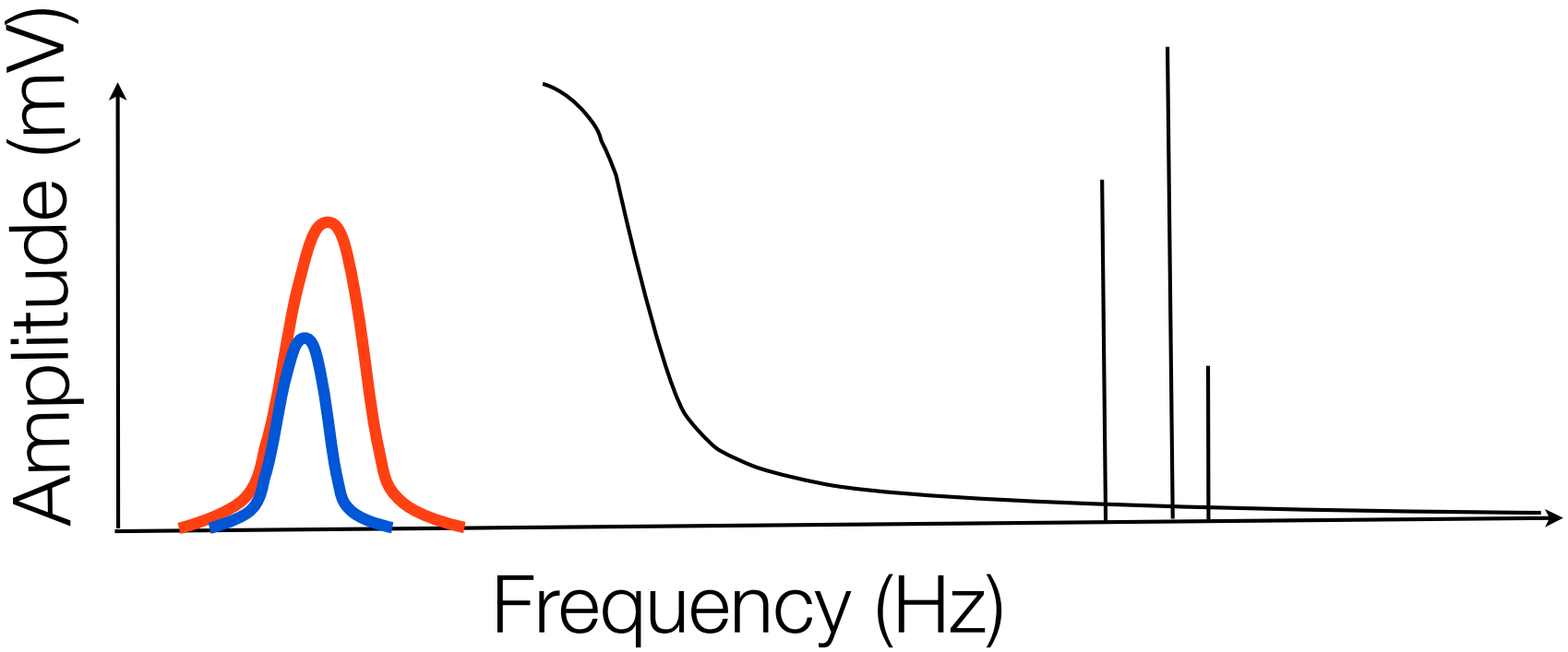
Ghost Talk: Intentional interference

- Conducting traces can couple to EMI (back-door).
- Sensitive analog sensors can be affected.



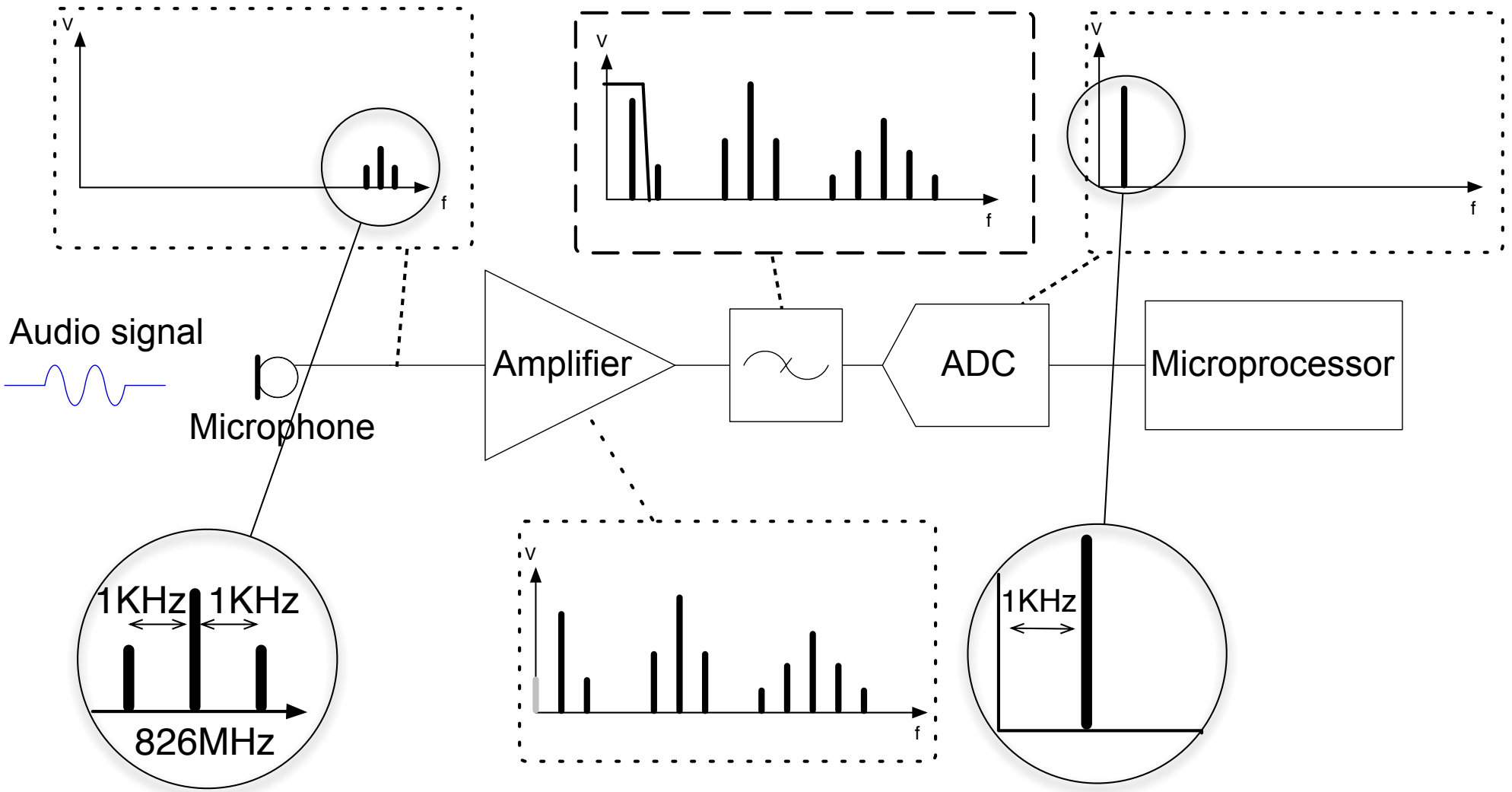
Fundamental Problem: Baseband

- Baseband: frequency range of desired signals.
- Interference outside the baseband is easy to filter.
- Interference in the baseband is hard to remove.



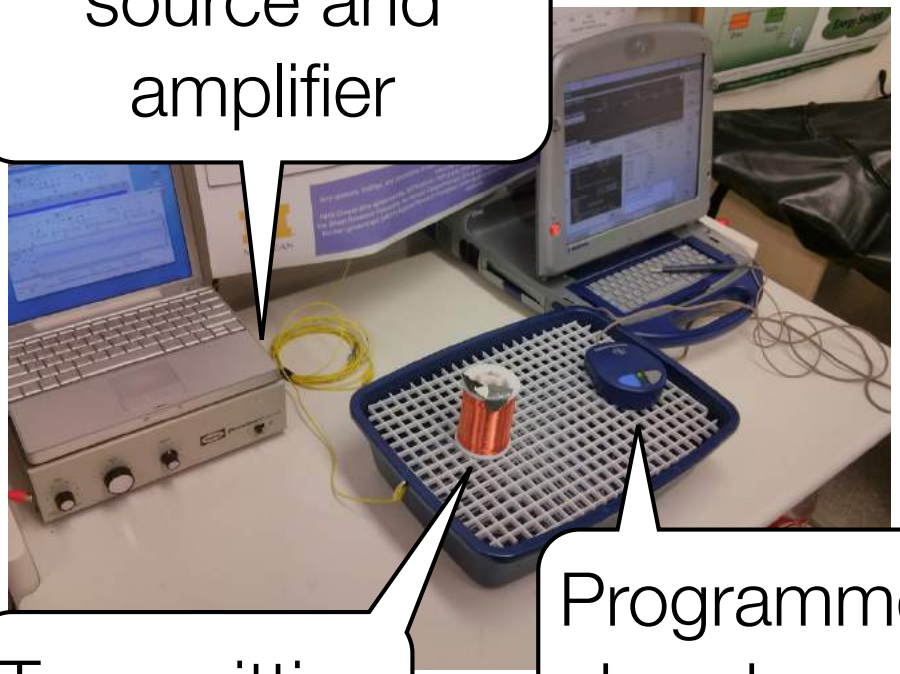
Microphone Interference with RF

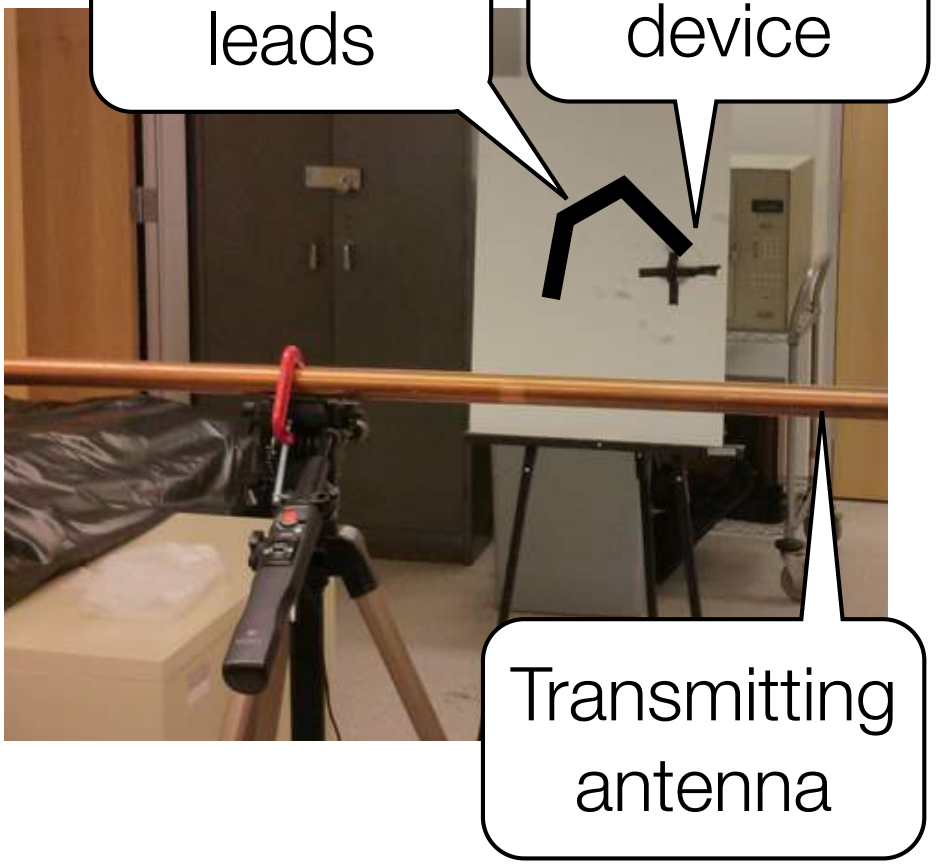
Non-Linearity: Self Demodulation



intermodulation distortion…

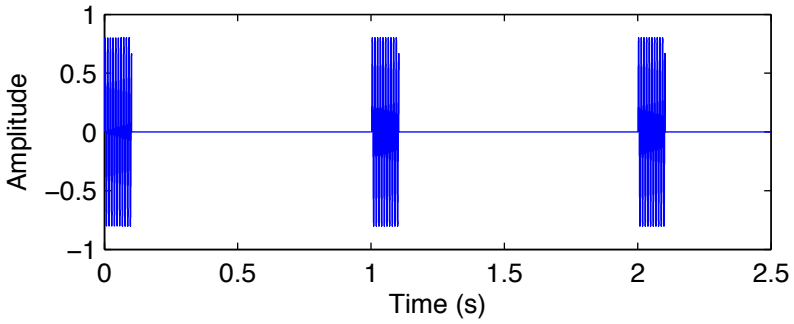
Experiment: Implants & Emitters

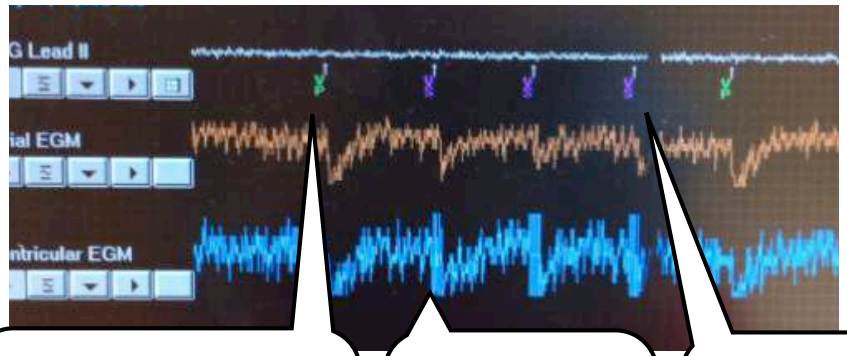




Results: Waveforms & Responses

Pulsed sinusoid



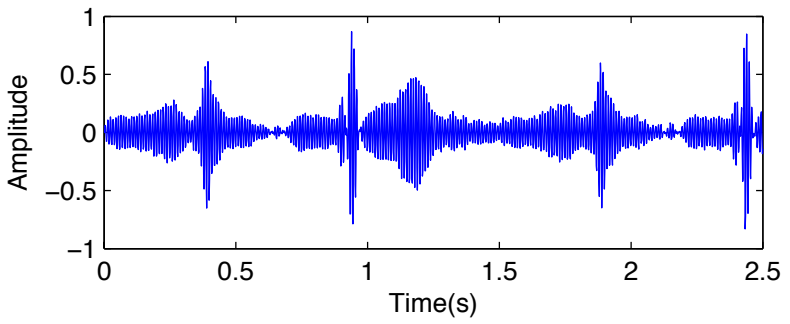


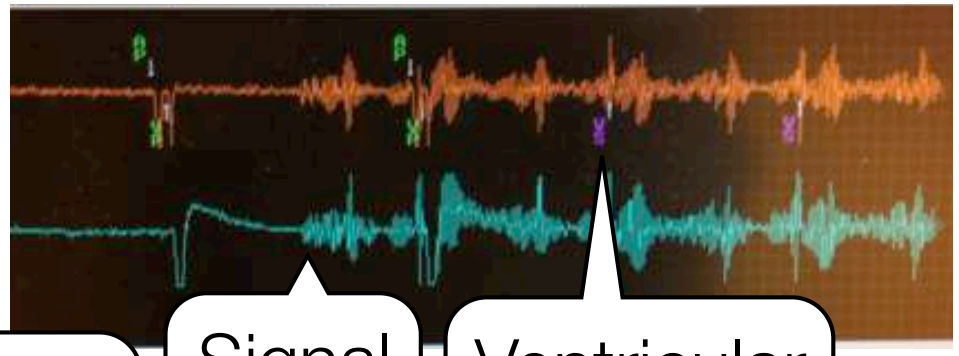
Ventricular pace

Signal onset

Ventricular sense

Modulated heart beat

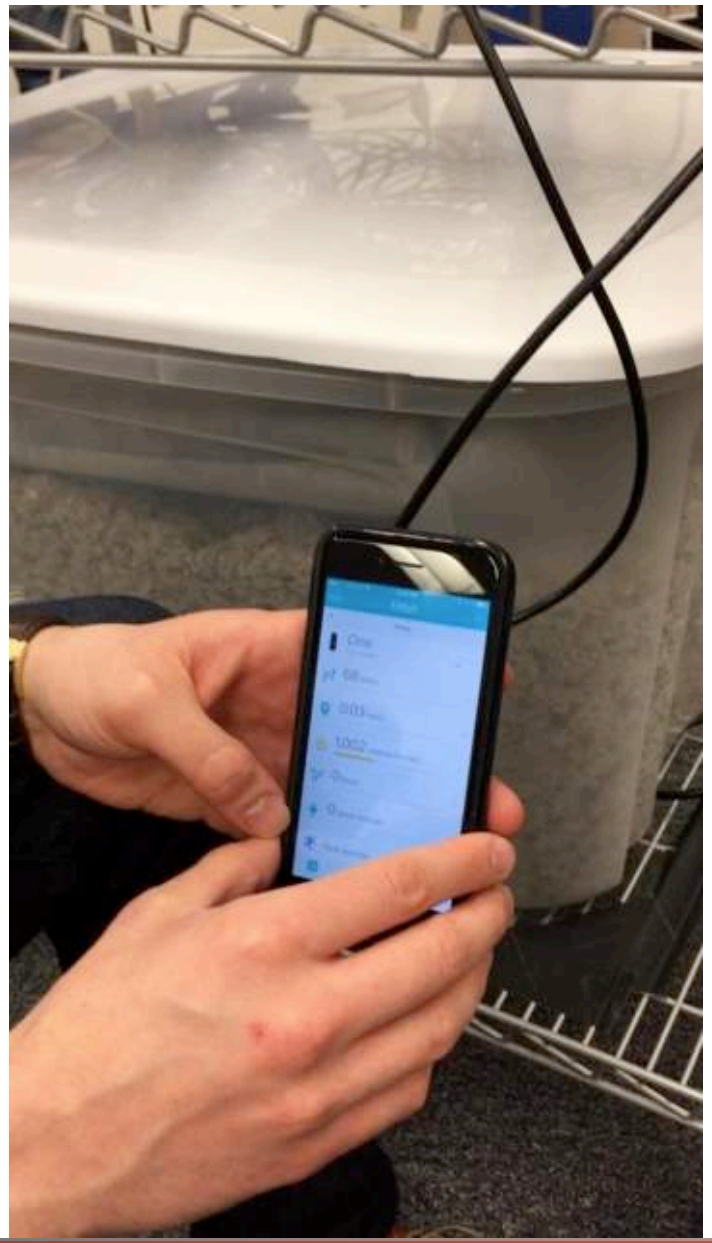




Signal onset

Ventricular sense

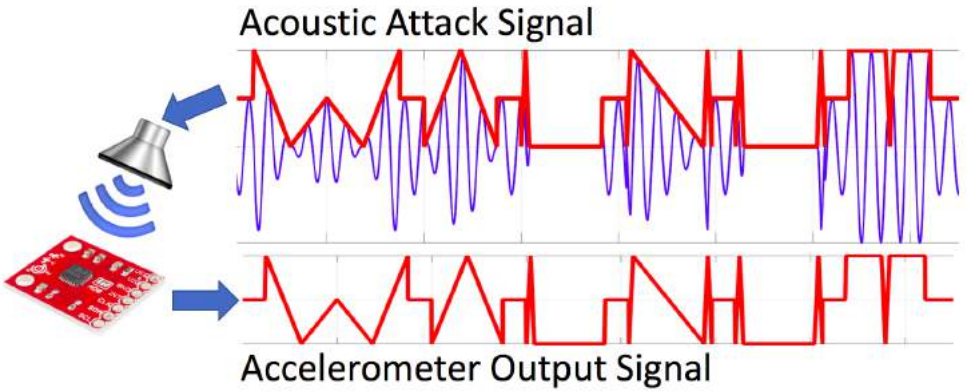
Acoustic Attacks on MEMS Accelerometers



spqr.eecs.umich.edu/walnut

["WALNUT" by Trippel et al., IEEE Euro S&P 2017]

Unintentional Demodulation

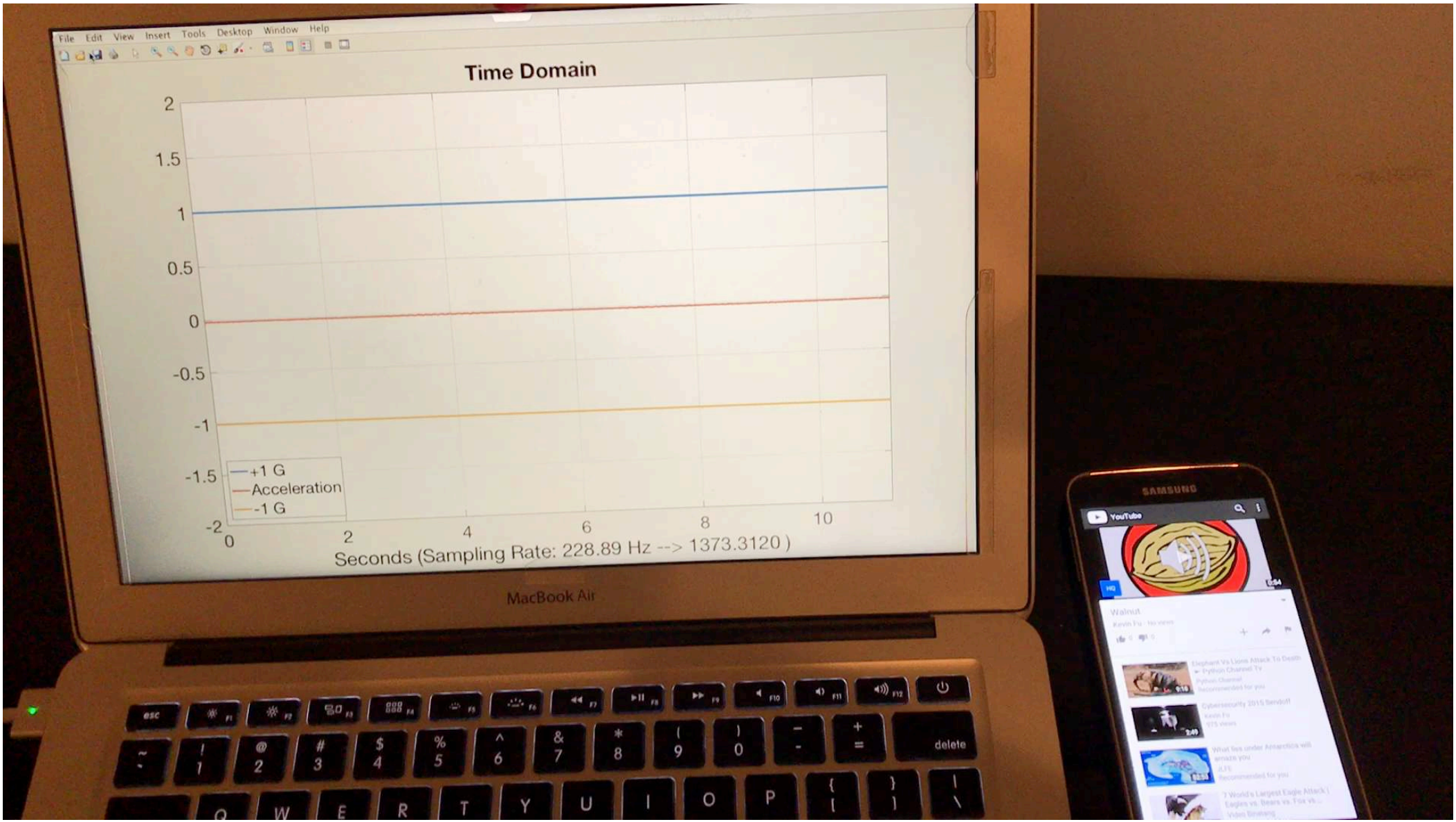


vs.

Both: Intentional signal modulation

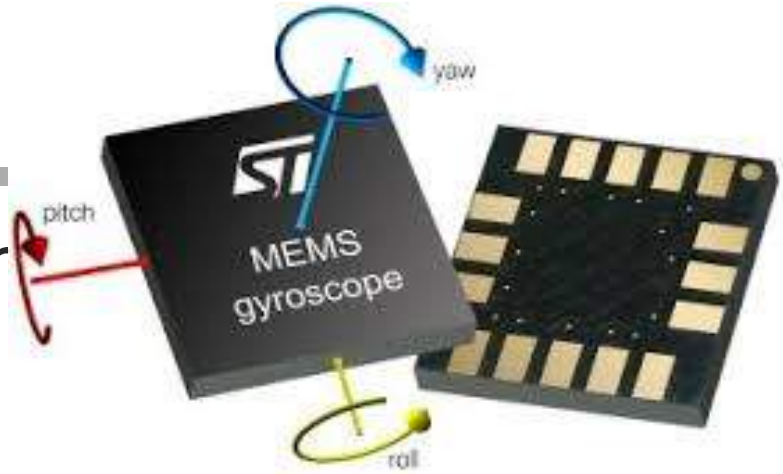
Intentional
signal demodulation

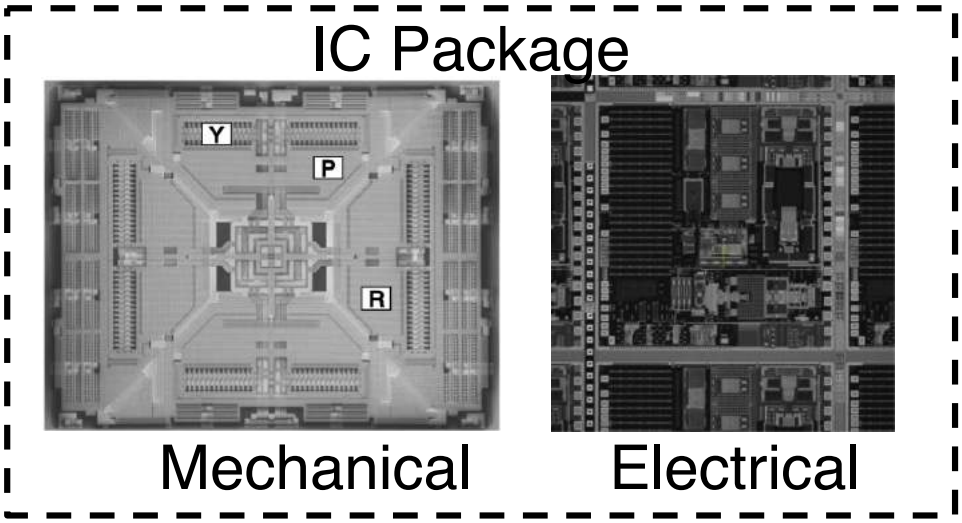
<u>Unintentional</u>
signal demodulation


File Edit View Insert Tools Desktop Window Help
Time Domain
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
0
2
4
6
8
10
+1 G
Acceleration
-1 G
Seconds (Sampling Rate: 228.89 Hz --> 1373.3120)
MacBook Air
SAMSUNG
YouTube
Walnut
delete

MEMS Sensors

- **M**icro-**E**lectro-**M**echanical **S**ystem
  - **Accelerometers**
  - **Gyroscopes**
  - **Clocks**
- Advantages
  - Low cost
  - Low power
    some < 1 mA
  - Small integrated circuit

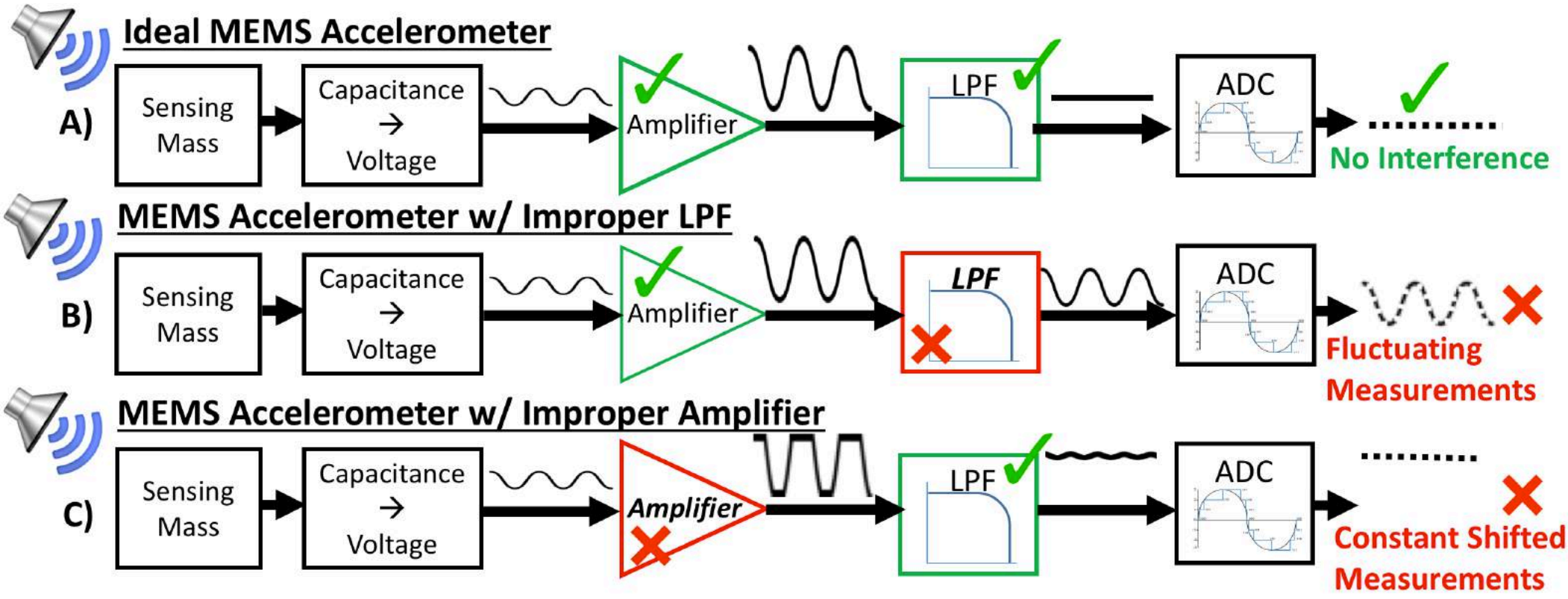




*Photos courtesy of "*Everything about STMicroelectronics' 3-axis digital MEMS gyroscopes – Technical Report*", by STMicroelectronics.

Signal Distortion

- Two types of spoofed acceleration
  - Fluctuating accelerometer output
  - Constant accelerometer output



asymmetric clipping

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ANALOG DEVICES ADVISORY TO ICS ALERT-17-073-01

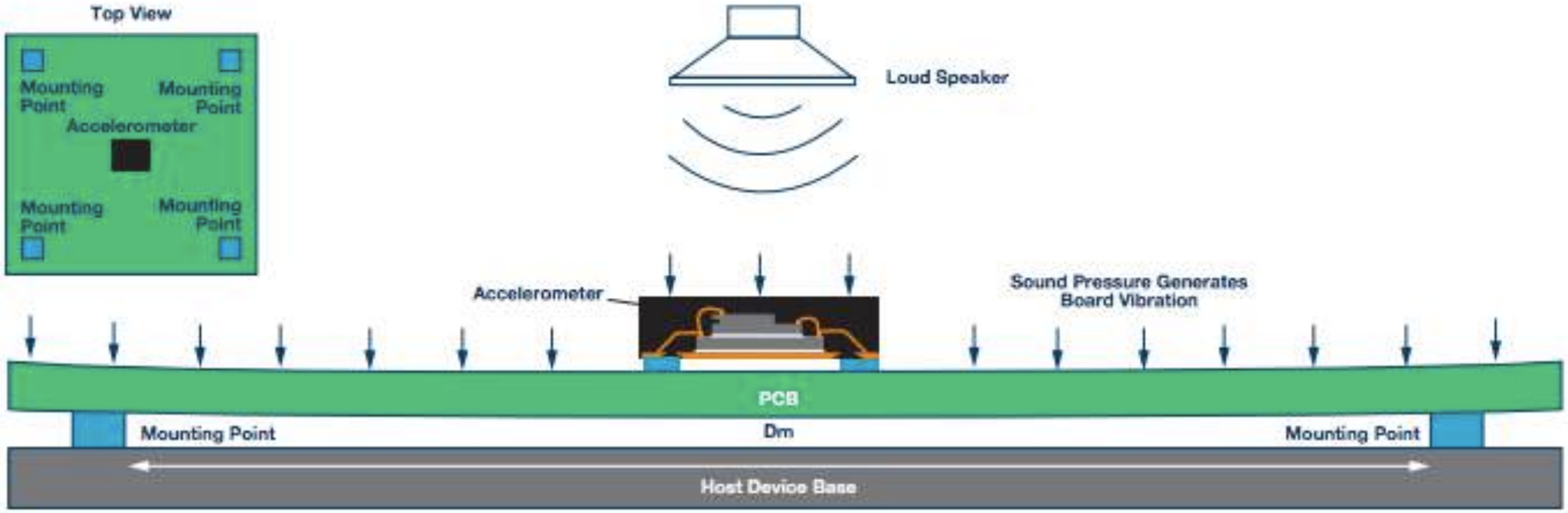


Figure 1. MEMS accelerometer board and mounting with acoustic vibration from off-board speaker.

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ANALOG DEVICES ADVISORY TO ICS ALERT-17-073-01

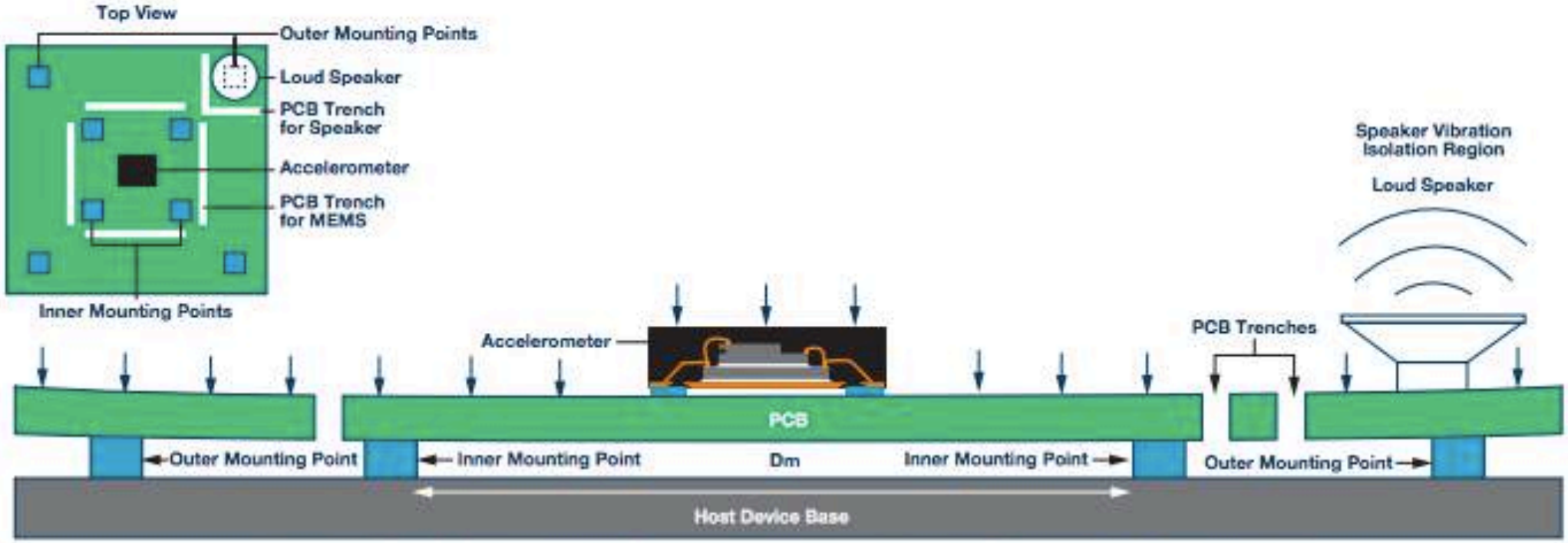


Figure 2. MEMS accelerometer board and mounting with acoustic and mechanical vibration from on-board speaker.

ICS-CERT is also working with several of the cooperative vendors to identify a list of affected devices that contain vulnerable capacitive MEMS accelerometer sensors.

The following MEMS Accelerometer sensors may be affected:

- Bosch BMA222E,
- STMicroelectronics MIS2DH,
- STMicroelectronics IIS2DH,
- STMicroelectronics LIS3DSH,
- STMicroelectronics LIS344ALH,
- STMicroelectronics H3LIS331DL,
- InvenSense MPU6050,
- InvenSense MPU6500,
- InvenSense ICM20601,
- Analog Devices ADXL312,
- Analog Devices ADXL337,
- Analog Devices ADXL345,
- Analog Devices ADXL346,
- Analog Devices ADXL350,
- Analog Devices ADXL362,
- Murata SCA610,
- Murata SCA820,
- Murata SCA1000,
- Murata SCA2100, and
- Murata SCA3100.

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ANALOG DEVICES ADVISORY TO ICS ALERT-17-073-01

The following derivations based on a single periodic sound frequency can be used to relate the board deflection to acceleration level.

The board harmonic deflection can be defined as:

$$deflection = d_{bd} \times \sin(\omega \times t) \quad (1)$$

where d_{bd} is the amplitude of the board deflection under the sound pressure and ω is the frequency of the sound.

The acceleration produced by the harmonic deflection is:

$$acceleration = d_{bd} \times \omega^2 \times \sin(\omega \times t) \quad (2)$$

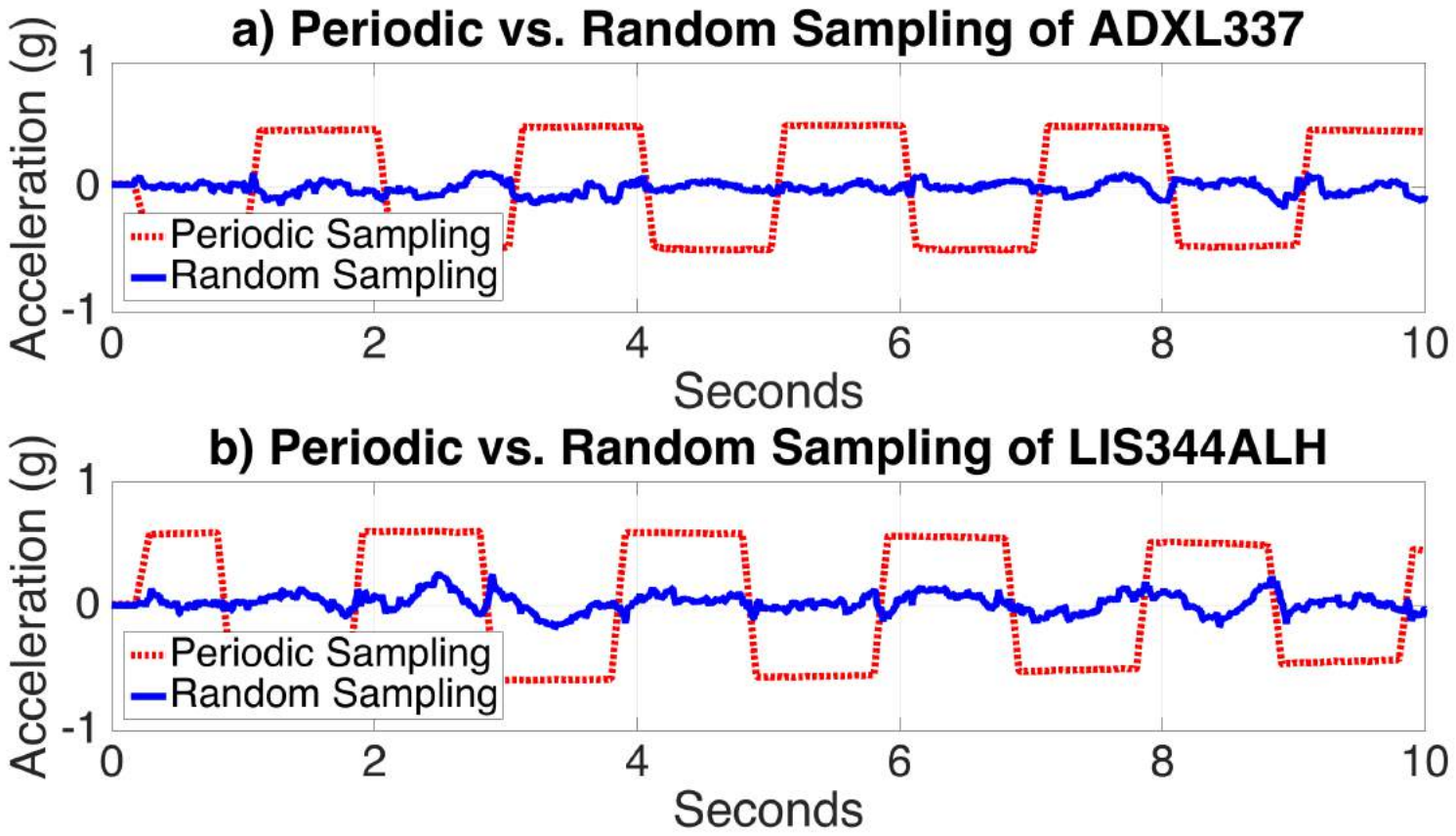
In the case where the sound frequency matches the board resonant frequency, the deflection will be amplified by the qualify factor (Q_{bd}) of the board and Equation 2 will be modified as:

$$acceleration \text{ at } board\ resonance = Q_{bd} \times d_{bd} \times \omega^2 \times \sin(\omega \times t) \quad (3)$$

By inspecting Equation 3, one can find the following methods to mitigate the board acceleration effect. These methods have been either implemented in Analog Devices' accelerometer products or advised to the customers for system design considerations, whichever is applicable.

Randomized Sampling

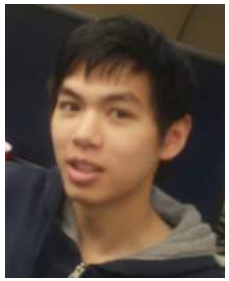
- Destroy predictability of sampling regime
- Randomize delay at each sampling interval



Blue N💩te:

How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives & Operating Systems [Oakland '18]



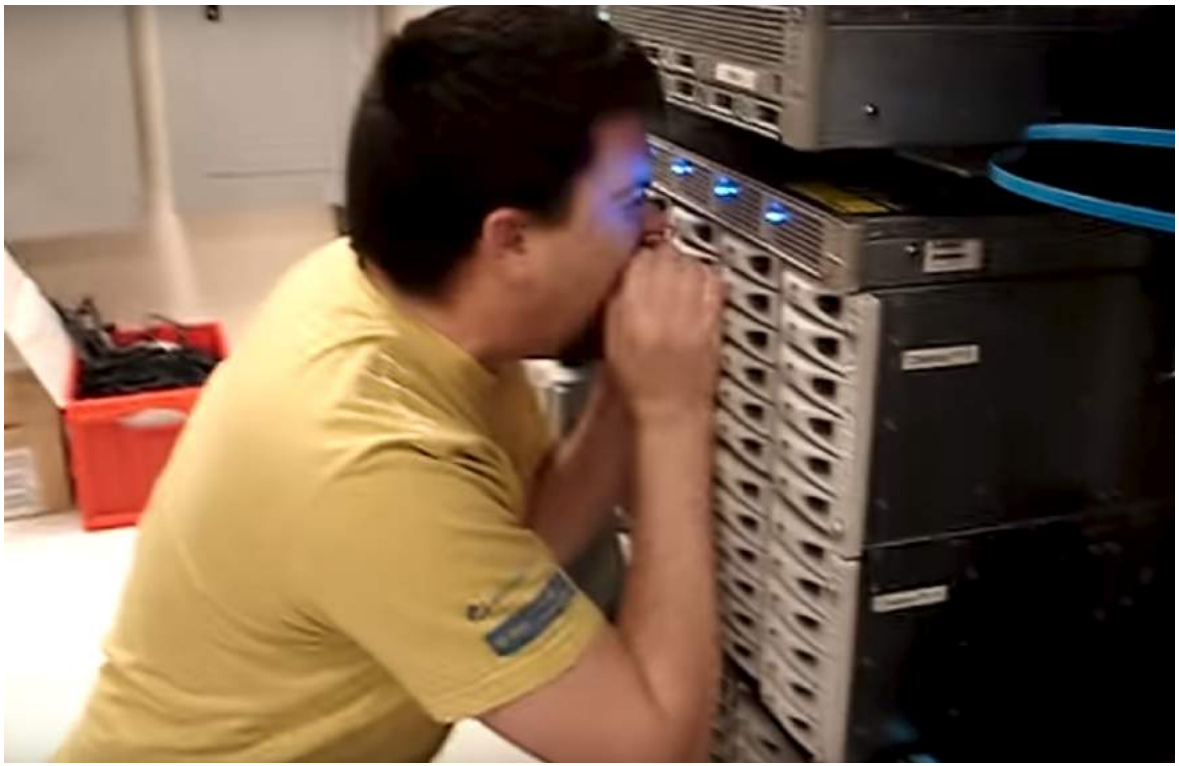



University of Michigan

Zhejiang University

Connor Bolton,
Sara Rampazzi,
Chaohao Li,
Andrew Kwong,
Wenyuan Xu, Kevin Fu

Sound Affecting HDDs?



https://www.youtube.com/watch?v=tDacjrSCeq4
Dec 31, 2008

Threat Model

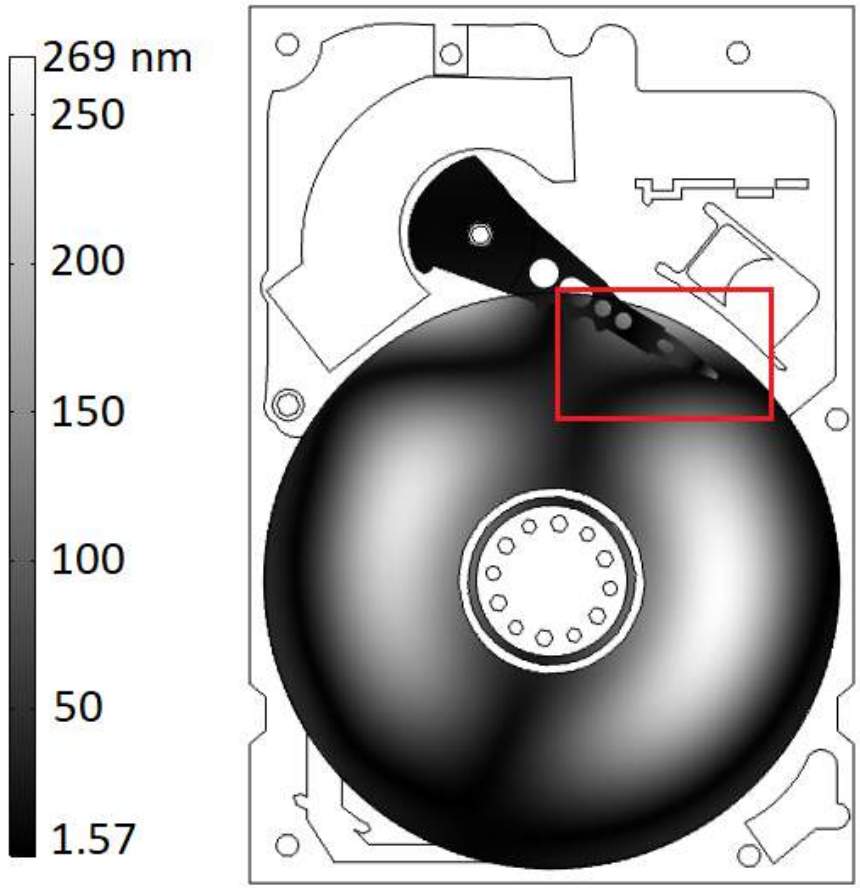
Placed Speaker

Ultrasonic transducer: https://www.vellemanstore.com/en/velleman-ma40a5r-40khz-ultrasonic-sensor-transducer-receiver

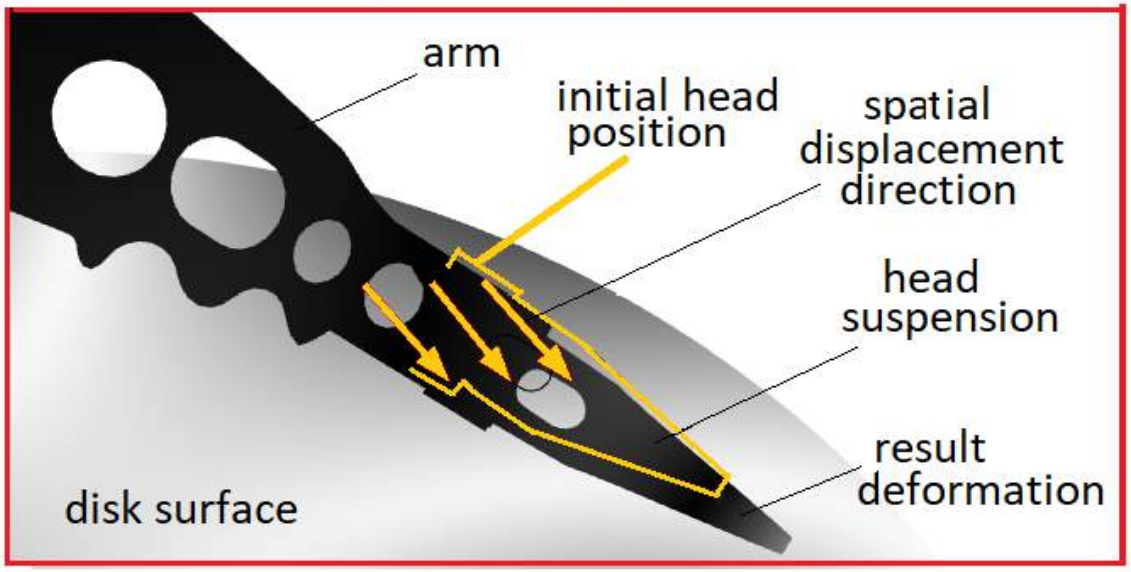
Audible Frequencies:

Vibrating the head and disk platters

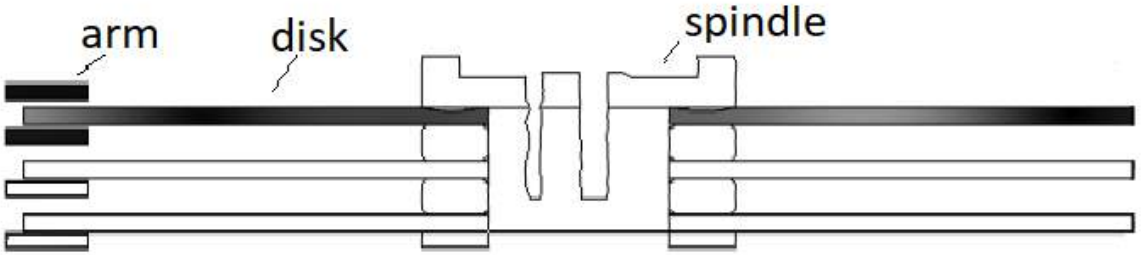
Total displacement



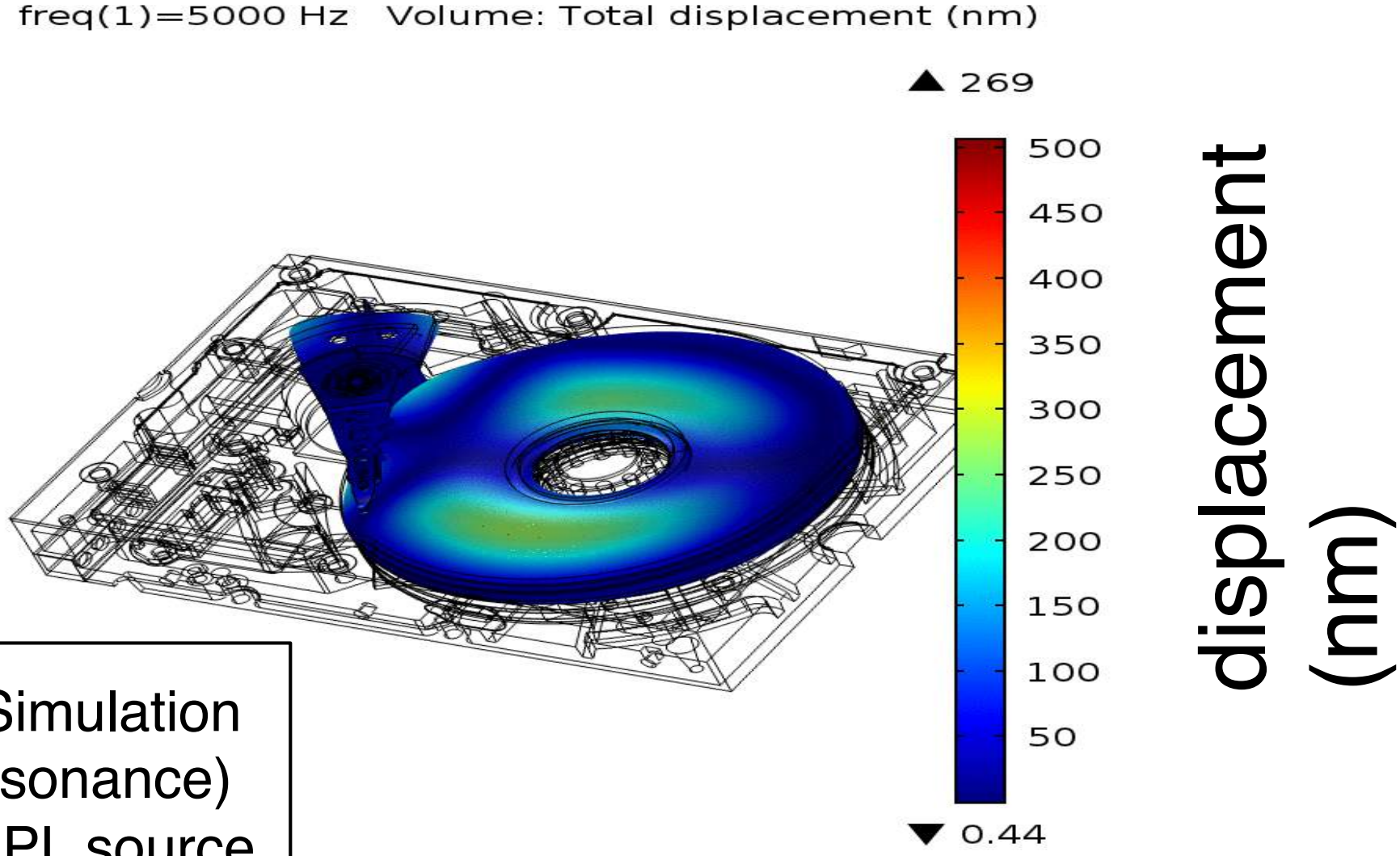
Head and arm spatial displacement



Disk and arm vertical displacement

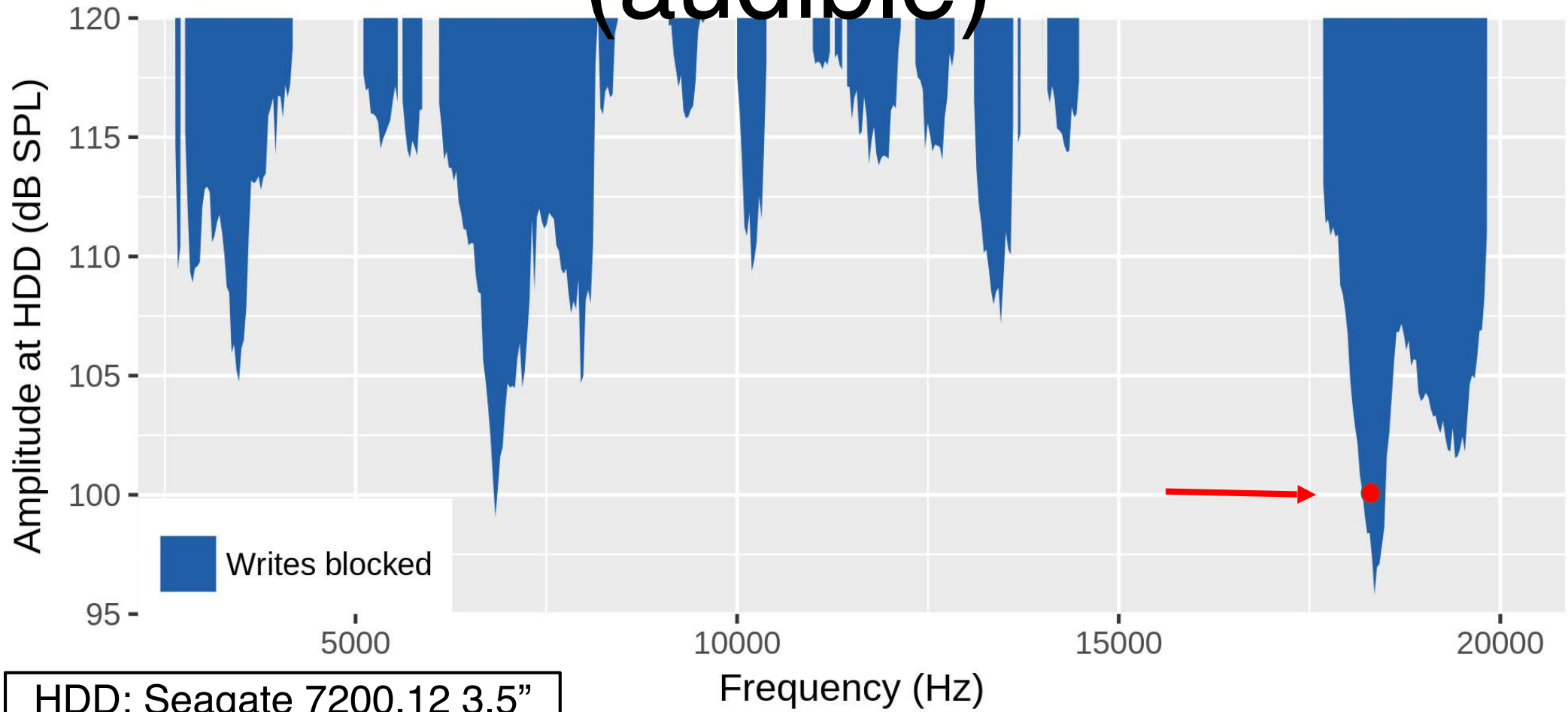


Sound distorts the HDD



Comsol Simulation
5 kHz (resonance)
120 dB SPL source
70 dB SPL at disk

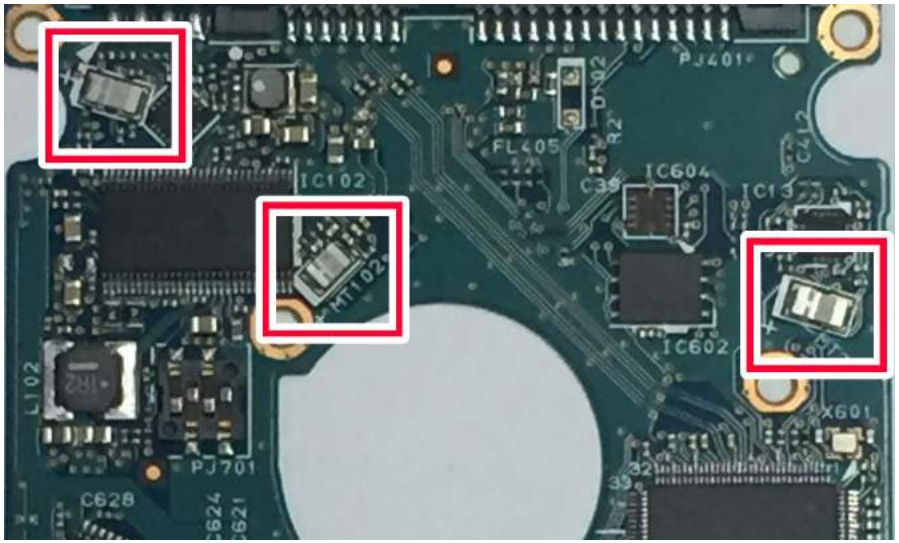
Resonant Frequencies (audible)



HDD: Seagate 7200.12 3.5”

Ultrasonic Frequencies:

Shock Sensor Spoofing

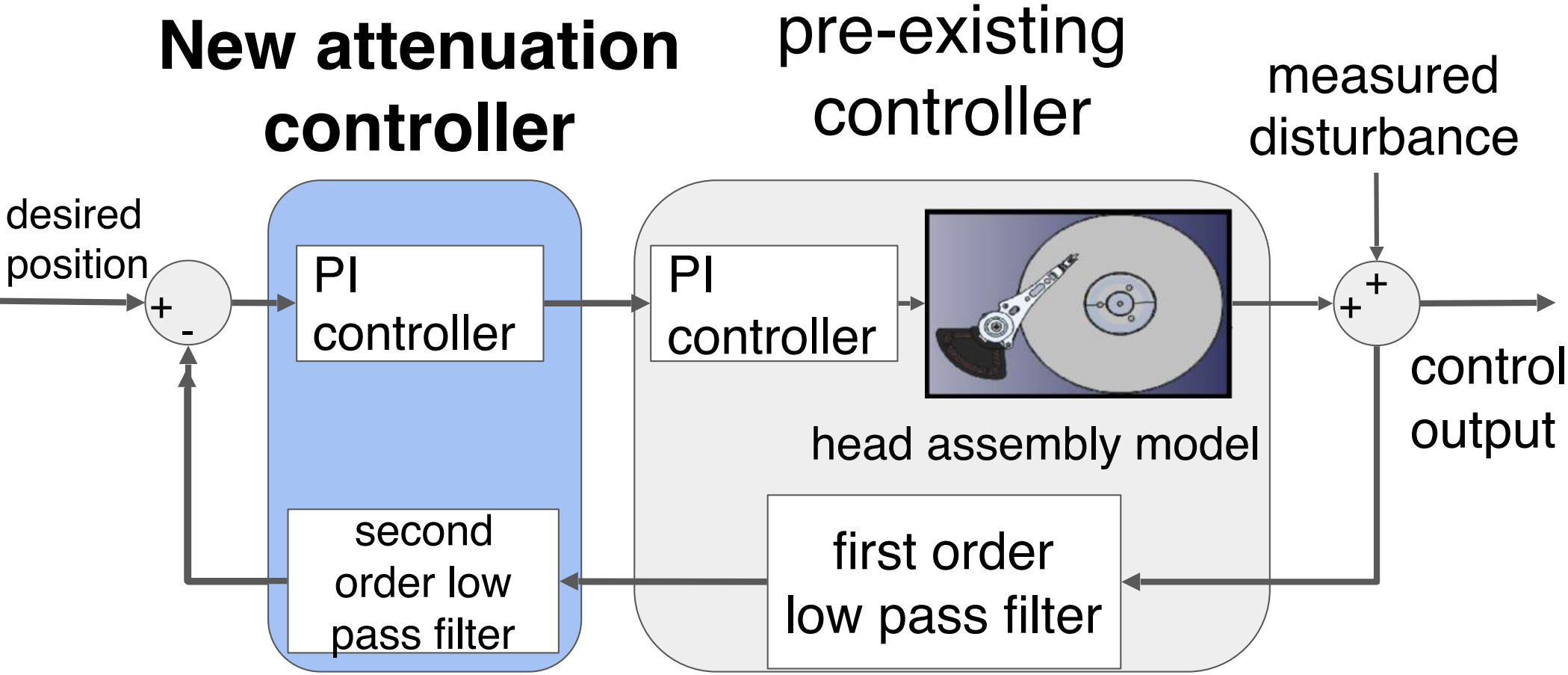


Disabling Video Surveillance DVR

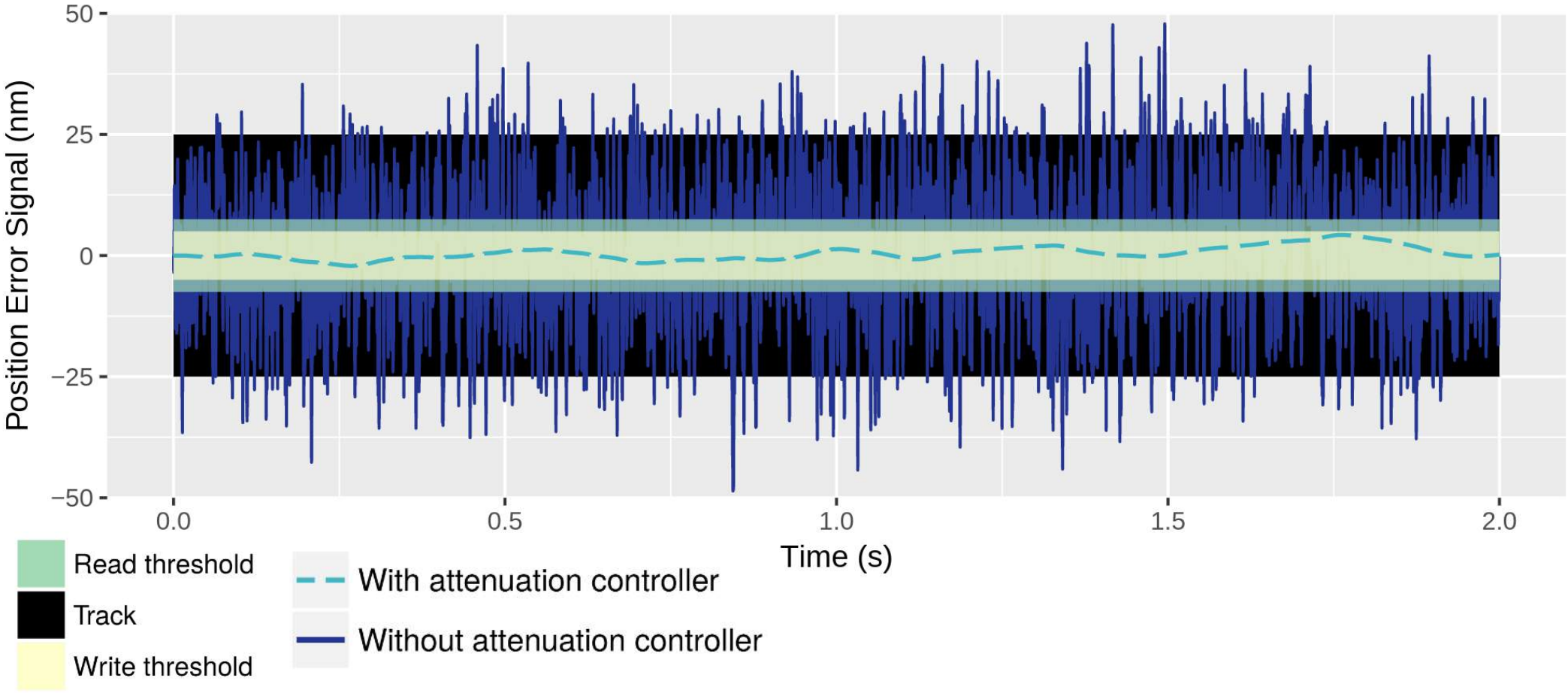
Defenses:

Passive Noise Canceling

Feedback Controller: Adding Resilience



Attenuation Controller Effectiveness



HDD model based off Seagate 7200.12 3.5”

Hard Drive of Hearing [IEEE S&P '19]

Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone

Andrew Kwong[1], Wenyuan Xu[2], and Kevin Fu[1]

[1]University of Michigan
[2]Zhejiang University

Abstract—**Security conscious individuals may take considerable measures to disable sensors in order to protect their privacy. However, they often overlook the cyberphysical attack surface exposed by devices that were never designed to be sensors in the first place. Our research demonstrates that the mechanical components in hard drives behave as microphones with sufficient precision to extract and parse human speech. These unintentional microphones sense speech with high enough fidelity for the Shazam service to recognize a song recorded through the hard drive. This proof of concept attack sheds light on the possibility of invasion of privacy even in absence of traditional sensors. We also present defense mechanisms, such as the use of ultrasonic aliasing, that can mitigate acoustic eavesdropping attacks by hard drives.**

1. Introduction

Magnetic hard disk drives continue to persist in everything from legacy laptops to server racks [1]. Because of their critical role in a wide variety of applications, hard drives make an appealing target for both cyber criminals

use this offset, known as the Position Error Signal (PES), in a feedback control loop; the microprocessor takes the PES as input for actuating the read/write head by use of a voice-coil motor (VCM) [4].

For both read and write operations, the read/write head can tolerate deviation from the center only on the order of nanometers. Accordingly, PES measurements are taken at a very fine granularity. These extremely precise measurements are sensitive to vibrations caused by even the slightest fluctuations in air pressure, such as those induced by human vocalizations.

Extracting speech from the PES, however, is complicated due to a weak signal-to-noise-ratio (SNR). Imperfections in the eccentricity of the platters, thermal drift, and turbulence from the rapid rotation of the disks all contribute to a large quantity of noise in the signal [5]. Through a mixture of digital filtering techniques in both the time domain and the frequency domain, however, we have managed to sufficiently clean the signal such that human speech can be completely reconstructed under certain conditions.

To prove the existence of this acoustic side-channel, we

Turn hard drives into microphones with firmware

Ph.D. student: Andrew Kwong

So, you depend on sensors?

https://www.pinterest.com/pin/499547783640216987/

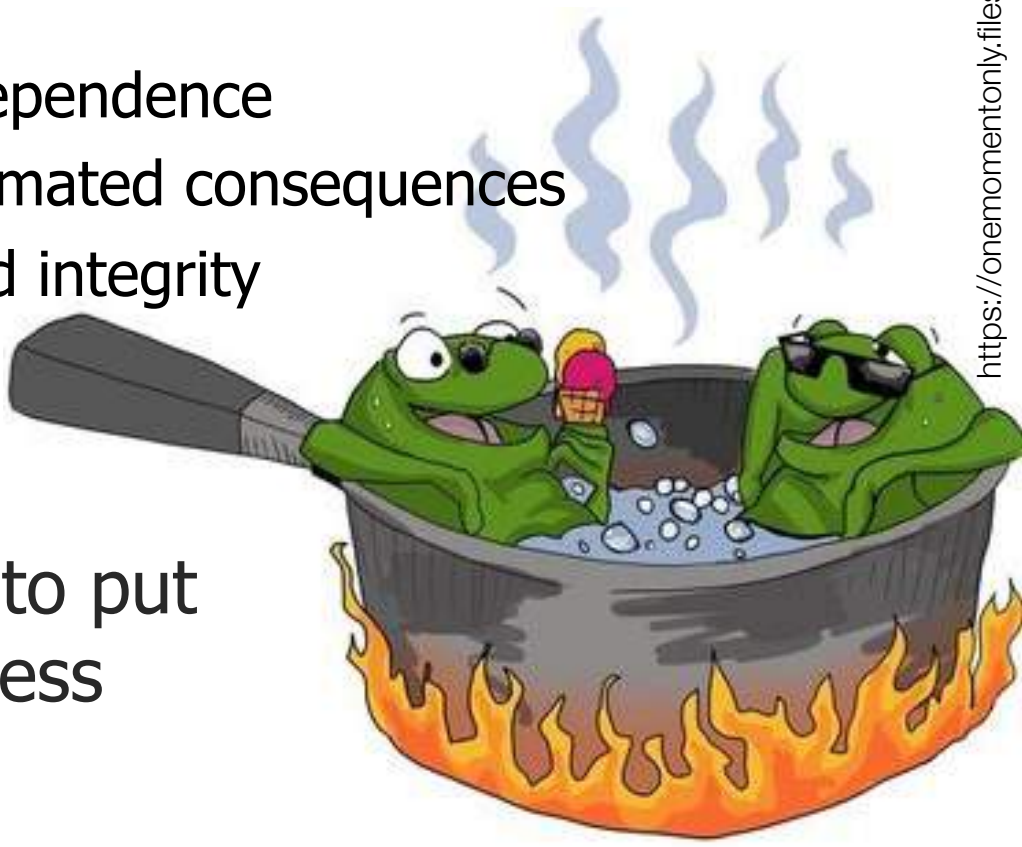
Creating Trustworthy Sensors

- Demystify analog sensor attack surface
  - Test to security **FAILURE**, not test to ¯_(ツ)_/¯
  - **Unwrap abstractions** of electrical engineering, mechanical engineering, materials science
- Ad-hoc security ⇨ measurable science
  - Physically de-risk **intentional interference** with more deliberate HW specs & design (e.g., resonance)
- Rethink ICs and hardware-software APIs
  - Convey to SW stack **WHY** trust sensor output
  - HW should expose **HINTS** of trustworthiness

Analog Cybersecurity Risks

- Computers have always been vulnerable to analog cybersecurity threats

- What's changing?
  - Degree of connectedness and dependence
  - From human-in-the-loop to automated consequences
  - Increased risks to availability and integrity



https://onemomentonly.files.wordpress.com/2013/06/boiling-frog1.jpg

- Maybe it's a not a good idea to put a computer in everything unless there's a good reason

Embedded Security References

- Classic fault and data injection
  - Chinese Remainder Theorem and ion beams [Boneh et al., EuroCrypt '97]
  - Cars [Koscher et al., IEEE S&P '10; Checkoway et al., USENIX Sec '11]
- Back door acoustic injection
  - Gyroscopes: Drone DoS [Son et al., USENIX Sec '15]
  - **Dolphin Attacks: Ultrasound voice recognition injection [Zhang et al., ACM CCS'17]**
  - **Walnut: Acoustic injection on MEMS accelerometers [Trippel et al., IEEE Euro S&P'17]**
- RF, IR, EMFI injection
  - Car tire pressure sensors: [Rouf et al., USENIX Sec '10]
  - Infusion pumps [Park et al., USENIX WOOT '16]
  - BADFET [Cui & Housley, USENIX WOOT '17]
  - **Ghost Talk: RF injection on microphones, pacemakers [Foo Kune et al., IEEE S&P '13],** GSMem [Guri et al., USENIX Sec '15]

Research Summary

- Microprocessors should not blindly trust **sensors**
- Protect IoT with SW that leverages **physics**
- Focus on **trustworthy systems**, rather than just secure components