Protecting Health Care and Cyberphysical Systems:
Wicked BiZaRrE Semiconductor Physics of Sensor Security: Sensors, Signals, Semiconductors, Software Systems

Kevin Fu

Professor

Electrical & Computer Engineering,
Khoury College of Computer Sciences,
Bioengineering

ACM Fellow, IEEE Fellow, AAAS Fellow,
Dr. Dwight E. Harken Memorial Lecturer
Director, Archimedes Center for
Health Care and Medical Device Cybersecurity

spqrlab1.github.io
secure-medicine.org
k.fu@northeastern.edu

Yan Long

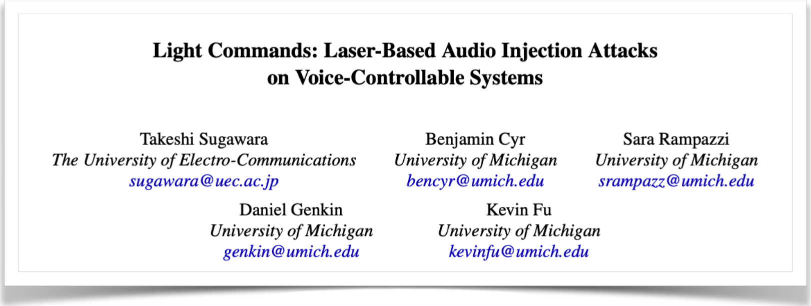
PhD Candidate
https://yanlong.site/

March 18, 2024

Supported in part by NSF CNS-2031077. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

Embedded Security Research

[USENIX Security]



Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems

Takeshi Sugawara
The University of Electro-Communications
sugawara@uec.ac.jp

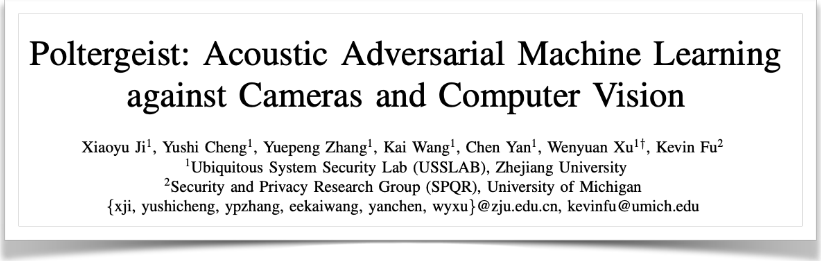
Benjamin Cyr
University of Michigan
bencyr@umich.edu

Sara Rampazzi
University of Michigan
srampazz@umich.edu

Daniel Genkin
University of Michigan
genkin@umich.edu

Kevin Fu
University of Michigan
kevinfu@umich.edu

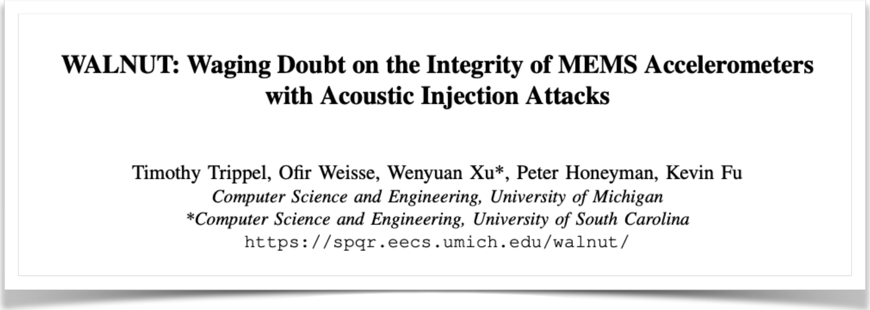
[IEEE S&P]



Poltergeist: Acoustic Adversarial Machine Learning against Cameras and Computer Vision

Xiaoyu Ji[1], Yushi Cheng[1], Yuepeng Zhang[1], Kai Wang[1], Chen Yan[1], Wenyuan Xu[1†], Kevin Fu[2]
[1]Ubiquitous System Security Lab (USSLAB), Zhejiang University
[2]Security and Privacy Research Group (SPQR), University of Michigan
{xji, yushicheng, ypzhang, eekaiwang, yanchen, wyxu}@zju.edu.cn, kevinfu@umich.edu

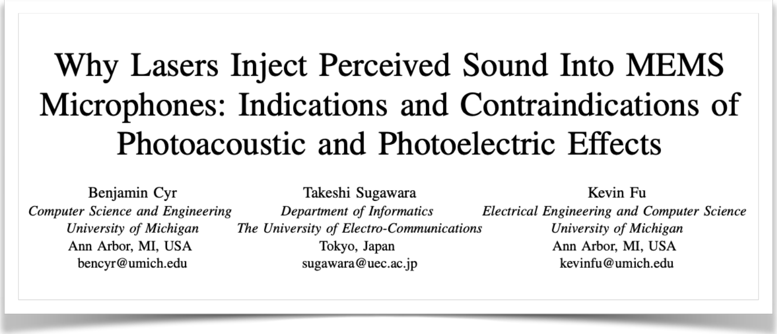
[IEEE Euro S&P]



WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks

Timothy Trippel, Ofir Weisse, Wenyuan Xu*, Peter Honeyman, Kevin Fu
Computer Science and Engineering, University of Michigan
**Computer Science and Engineering, University of South Carolina*
`https://spqr.eecs.umich.edu/walnut/`

[IEEE SENSORS]



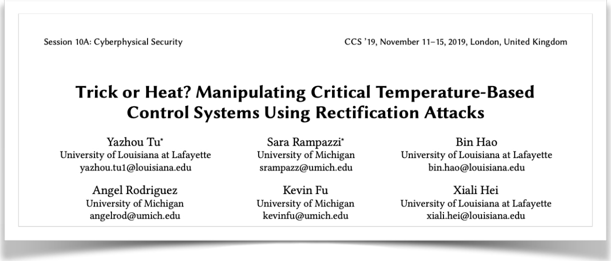
Why Lasers Inject Perceived Sound Into MEMS Microphones: Indications and Contraindications of Photoacoustic and Photoelectric Effects

Benjamin Cyr
Computer Science and Engineering
University of Michigan
Ann Arbor, MI, USA
bencyr@umich.edu

Takeshi Sugawara
Department of Informatics
The University of Electro-Communications
Tokyo, Japan
sugawara@uec.ac.jp

Kevin Fu
Electrical Engineering and Computer Science
University of Michigan
Ann Arbor, MI, USA
kevinfu@umich.edu

[ACM CCS]



Session 10A: Cyberphysical Security

CCS '19, November 11–15, 2019, London, United Kingdom

Trick or Heat? Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks

Yazhou Tu*
University of Louisiana at Lafayette
yazhou.tu1@louisiana.edu

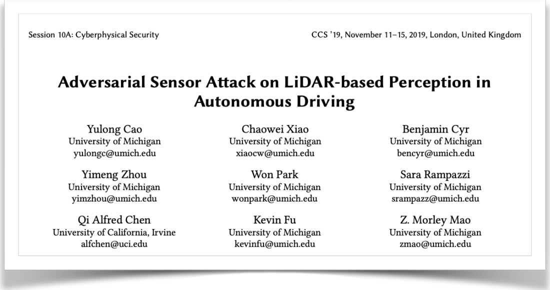
Sara Rampazzi*
University of Michigan
srampazz@umich.edu

Bin Hao
University of Louisiana at Lafayette
bin.hao@louisiana.edu

Angel Rodriguez
University of Michigan
angelrod@umich.edu

Kevin Fu
University of Michigan
kevinfu@umich.edu

Xiali Hei
University of Louisiana at Lafayette
xiali.hei@louisiana.edu



Session 10A: Cyberphysical Security

CCS '19, November 11–15, 2019, London, United Kingdom

Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving

Yulong Cao
University of Michigan
yulongc@umich.edu

Chaowei Xiao
University of Michigan
xiaocw@umich.edu

Benjamin Cyr
University of Michigan
bencyr@umich.edu

Yimeng Zhou
University of Michigan
yimzhou@umich.edu

Won Park
University of Michigan
wonpark@umich.edu

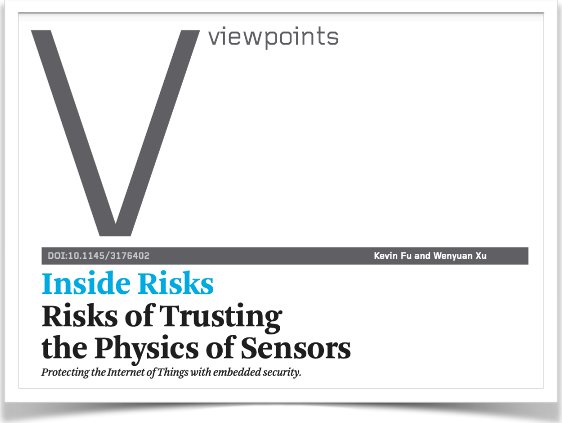
Sara Rampazzi
University of Michigan
srampazz@umich.edu

Qi Alfred Chen
University of California, Irvine
alfchen@uci.edu

Kevin Fu
University of Michigan
kevinfu@umich.edu

Z. Morley Mao
University of Michigan
zmao@umich.edu

[CACM]



V viewpoints

DOI:10.1145/3176402

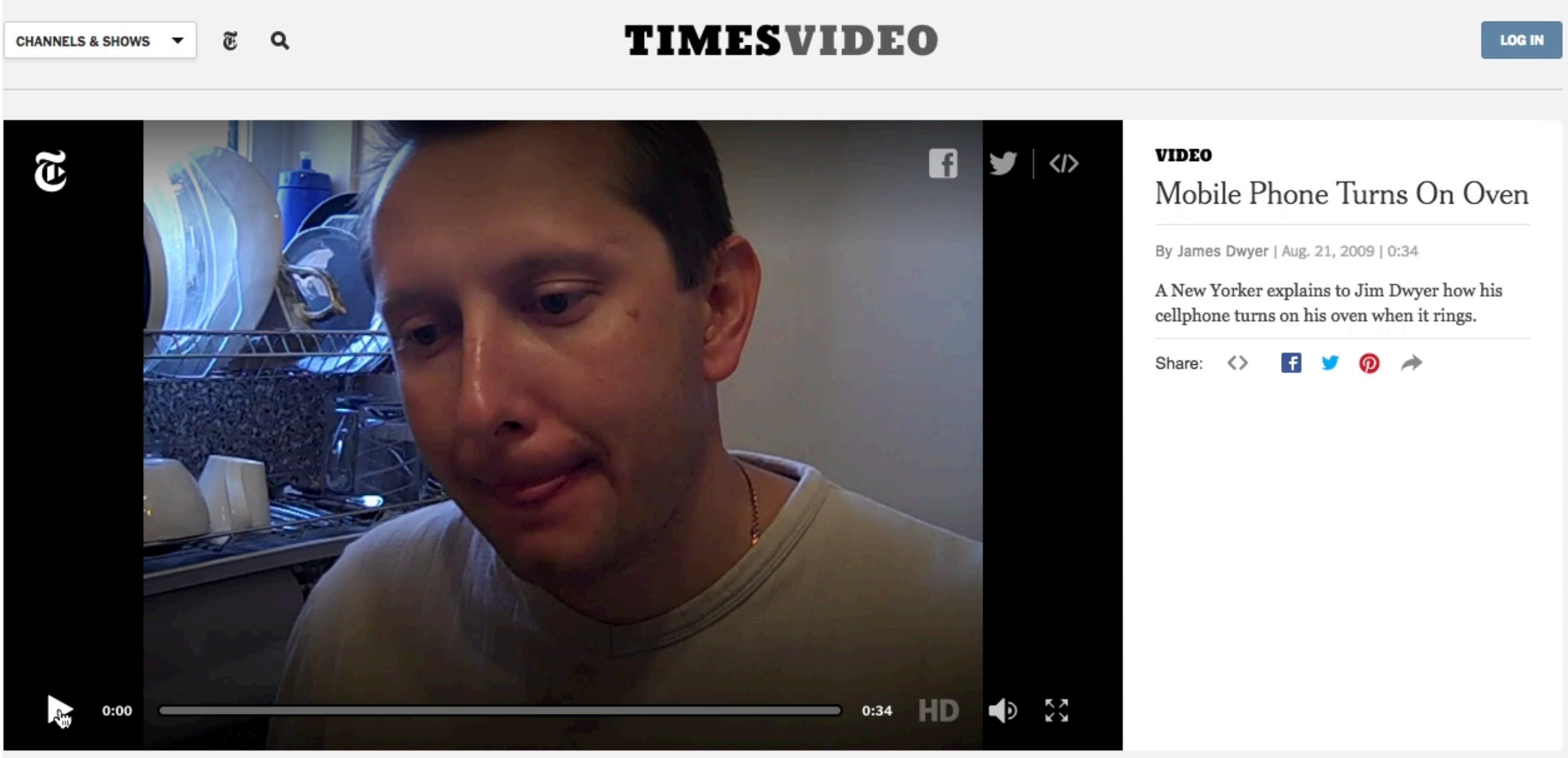
Kevin Fu and Wenyuan Xu

Inside Risks

Risks of Trusting the Physics of Sensors

Protecting the Internet of Things with embedded security.

Wicked Bizarre Physics of Sensor Security • k.fu@northeastern.edu • spqrlab1.github.io



VIDEO

Mobile Phone Turns On Oven

By James Dwyer | Aug. 21, 2009 | 0:34

A New Yorker explains to Jim Dwyer how his cellphone turns on his oven when it rings.

Share:

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

Security is hard.

Correctness is easy.

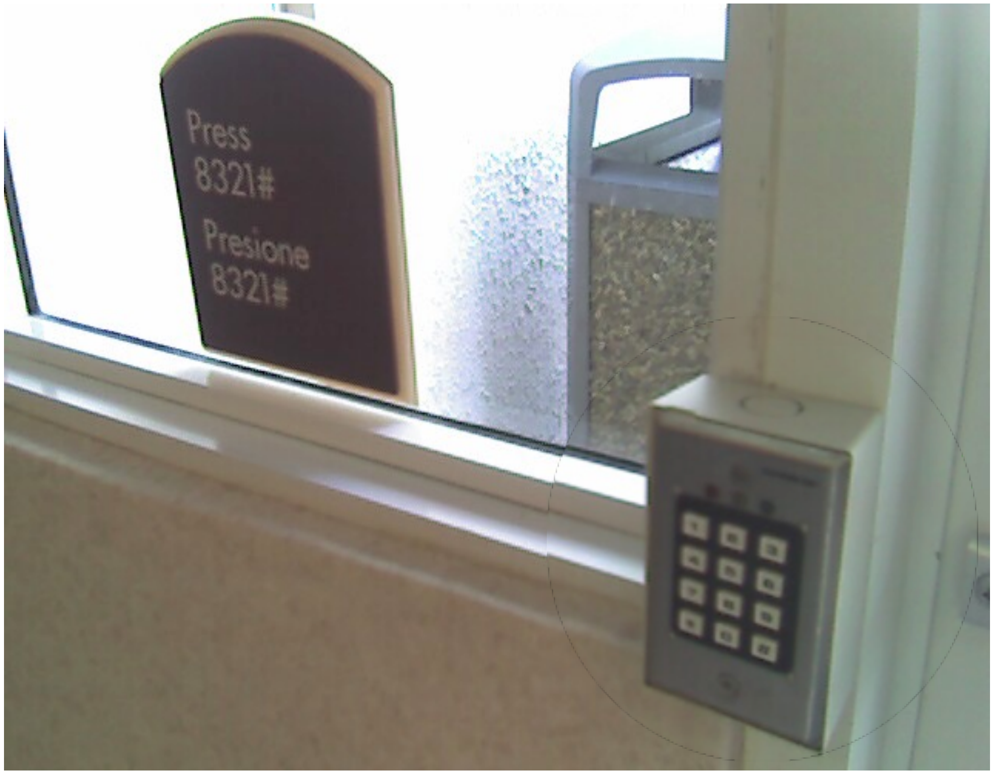
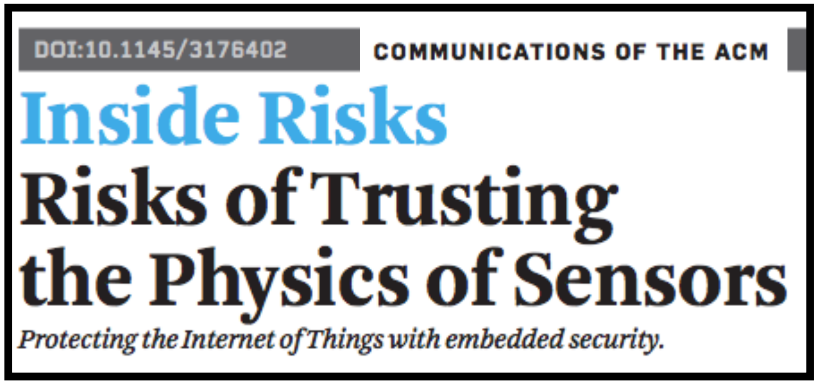


Photo by Kevin Fu

Sensors are Everywhere

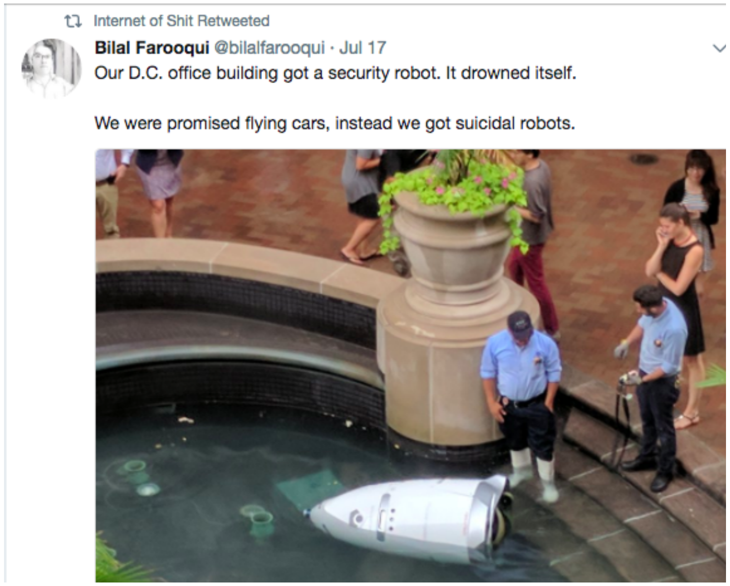


DOI:10.1145/3176402 COMMUNICATIONS OF THE ACM

Inside Risks

Risks of Trusting the Physics of Sensors

Protecting the Internet of Things with embedded security.



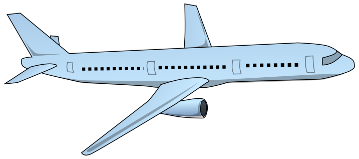
Internet of Shit Retweeted

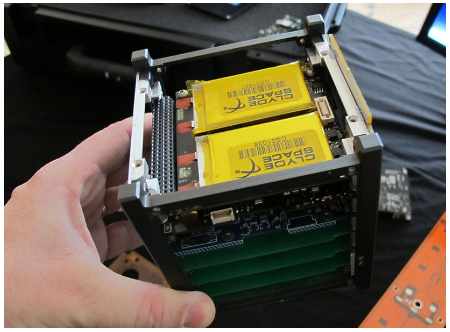
Bilal Farooqui @bilalfarooqui · Jul 17

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

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

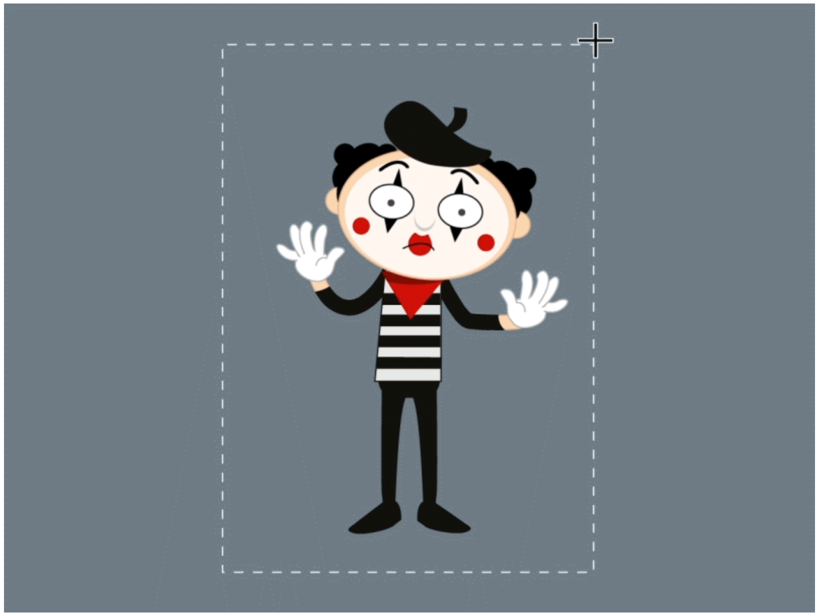
http://auto.howstuffworks.com/





Digital Abstraction != Force Field

intentional interference violates assumption of sensor output integrity



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

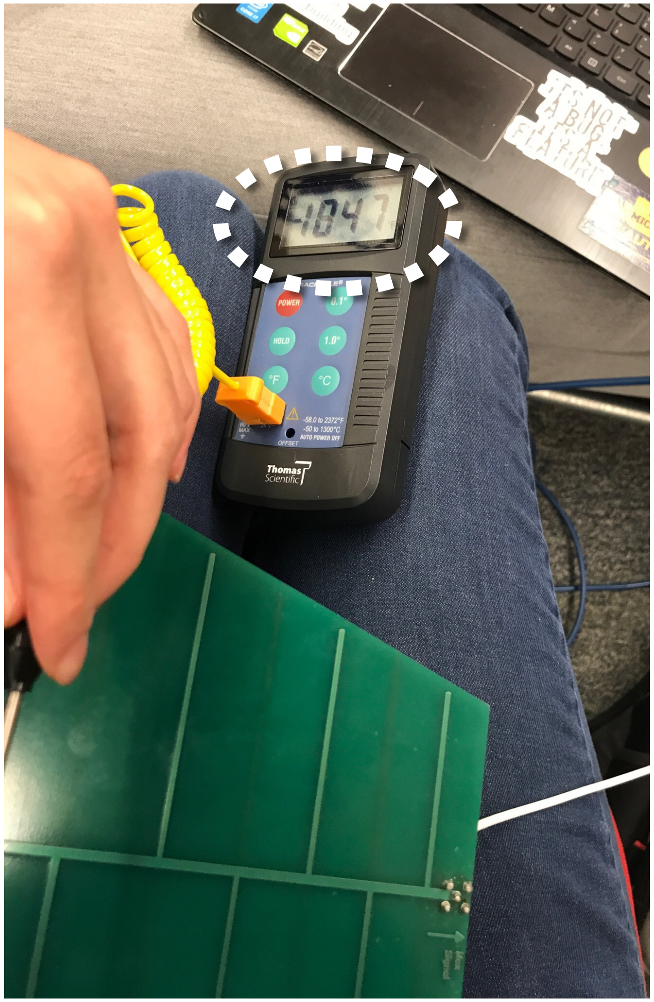
- **Vibration**
- **Acoustics**
- **RF**
- **Light**
- **Heat**

} ⇒ Analog Sensor Spoofing

Do Not Blindly Trust Sensors

Sensors are a proxy for reality

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



Absolute Zero Day Attack

Sensors are a proxy for reality

➡ Microphone measures electromagnetic potential of copper spool

✳ Not necessarily sound

➡ MEMS accelerometer measures vibration of a tiny element

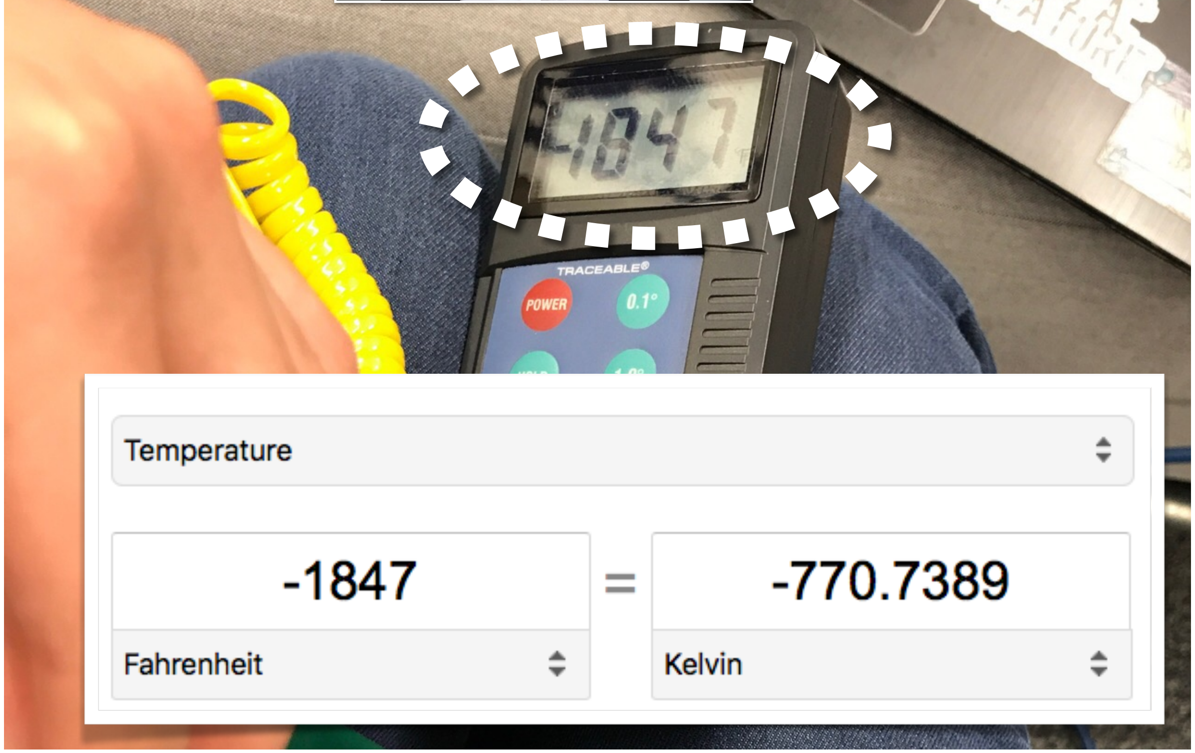
✳ Not necessarily sensor acceleration

➡ Thermocouple interpolates from a voltage potential

✳ Not necessarily temperature

Dr. Sara Rampazzi joins UFL faculty

Tu et al., “Trick or Heat? …” in **ACM CCS 2019**

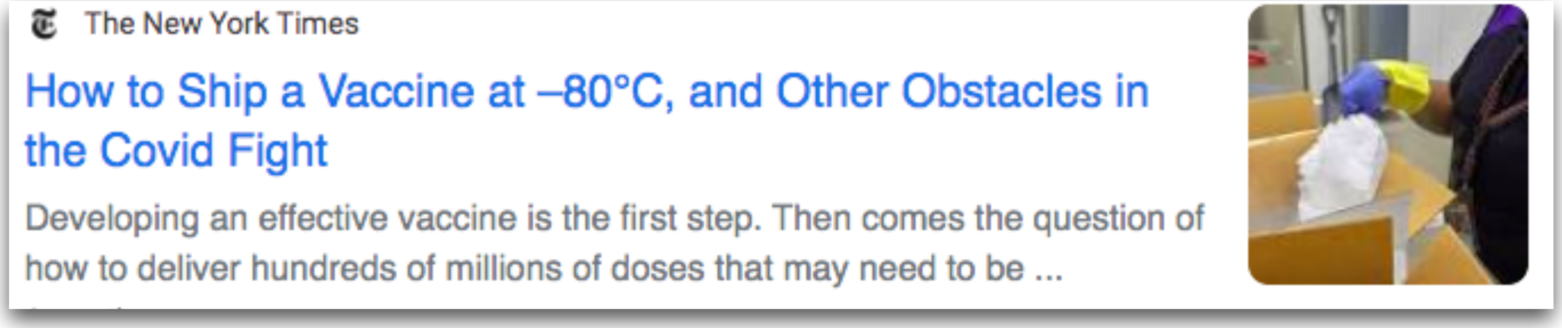


Temperature

-1847 = -770.7389

Fahrenheit | Kelvin

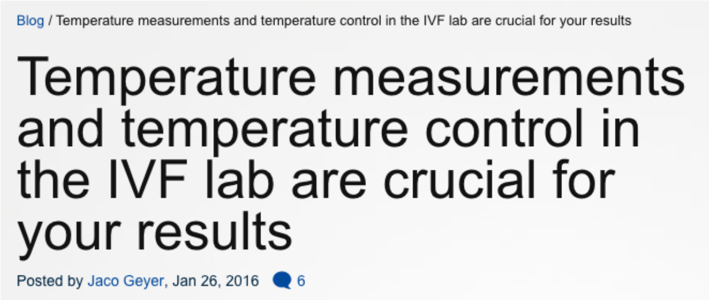
Where Do Thermocouples Matter?



The New York Times

How to Ship a Vaccine at –80°C, and Other Obstacles in the Covid Fight

Developing an effective vaccine is the first step. Then comes the question of how to deliver hundreds of millions of doses that may need to be ...



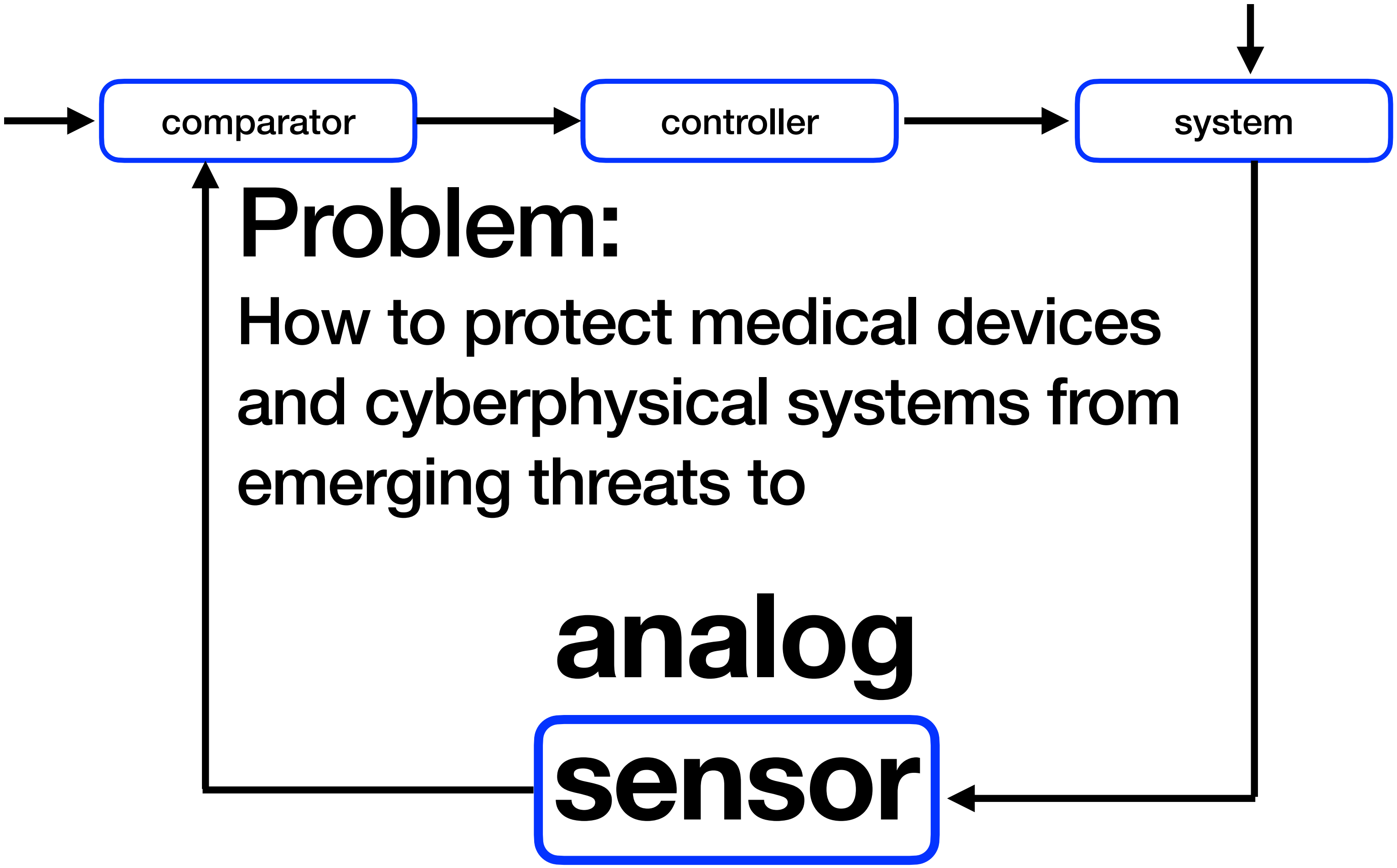
Blog / Temperature measurements and temperature control in the IVF lab are crucial for your results

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

Posted by Jaco Geyer, Jan 26, 2016 6

At Risk: Closed-Loop Feedback Systems

Photos: NYTimes, NBC Today, ABC News5 Cleveland



Problem:

How to protect medical devices and cyberphysical systems from emerging threats to

analog

sensor

integrity?

Outline: Protecting Sensor Integrity

Today: taste of sensor security research across three modalities:

- Defending against **radio-based attacks** on sensors
- Defending against **sound-based attacks** on sensors
- Defending against **light-based attacks** on sensors

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)

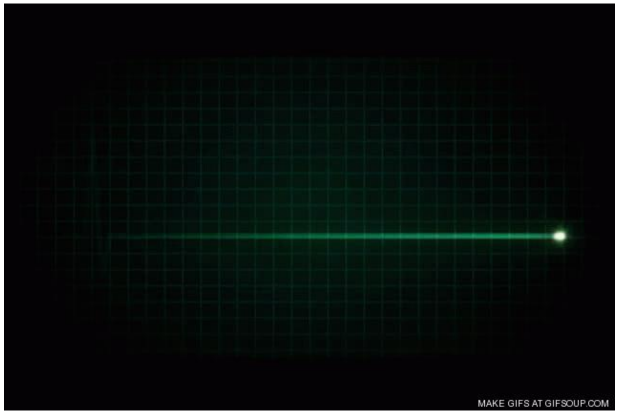
Supported in part by NSF CNS- 1035715, CNS-0845671, CNS-0923313, GEO-1124657, S121000000211, HHS 90TR0003/01, the Sloan Research Fellowship, the University of Minnesota Doctoral Dissertation fellowship, the Korean MEST NRF 2012-0000979, the Harvard Catalyst/Harvard Clinical and Translational Science 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.

Which one is the real cardiac signal?

A

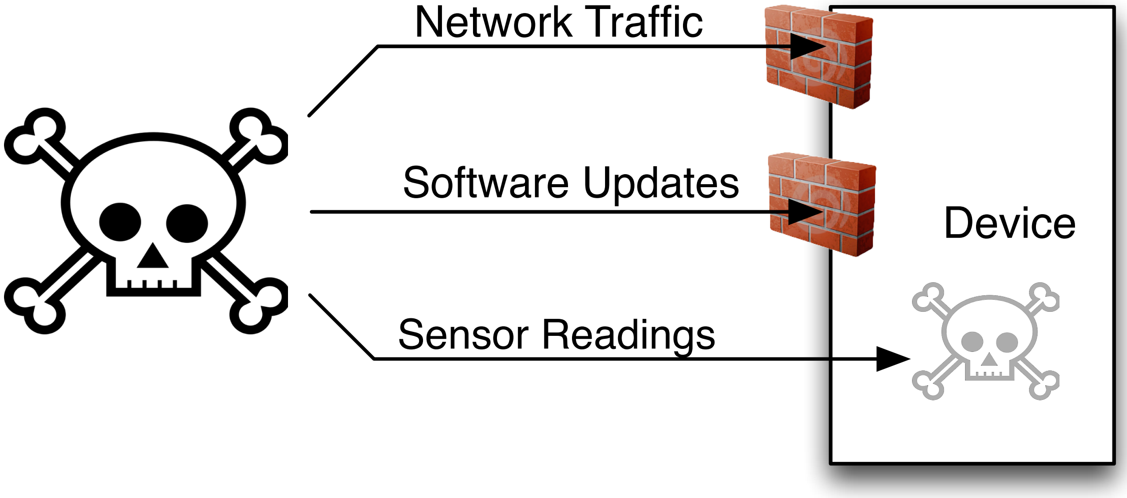
MAKE GIFS AT GIFSOUP.COM

B



[“Ghost Talk” by Foo Kune et al., IEEE S&P 2013]

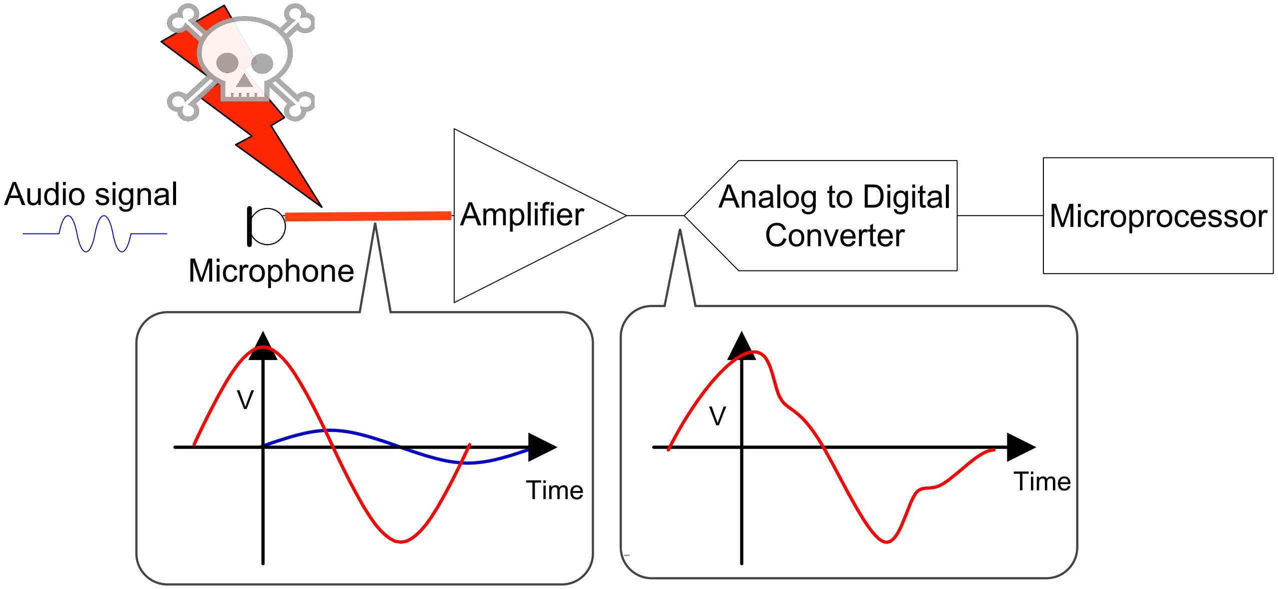
Inputs may not be trustworthy



[“Ghost Talk” by Foo Kune et al., IEEE S&P 2013]

Ghost Talk: Intentional interference

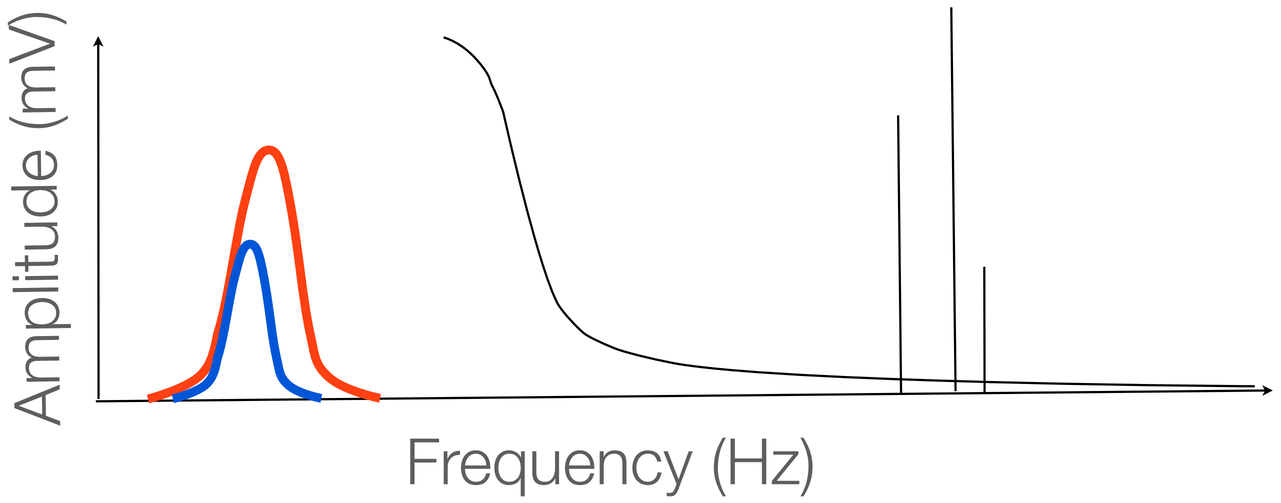
- Conducting traces can couple to EMI (back-door).
- Sensitive analog sensors can be affected.



["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

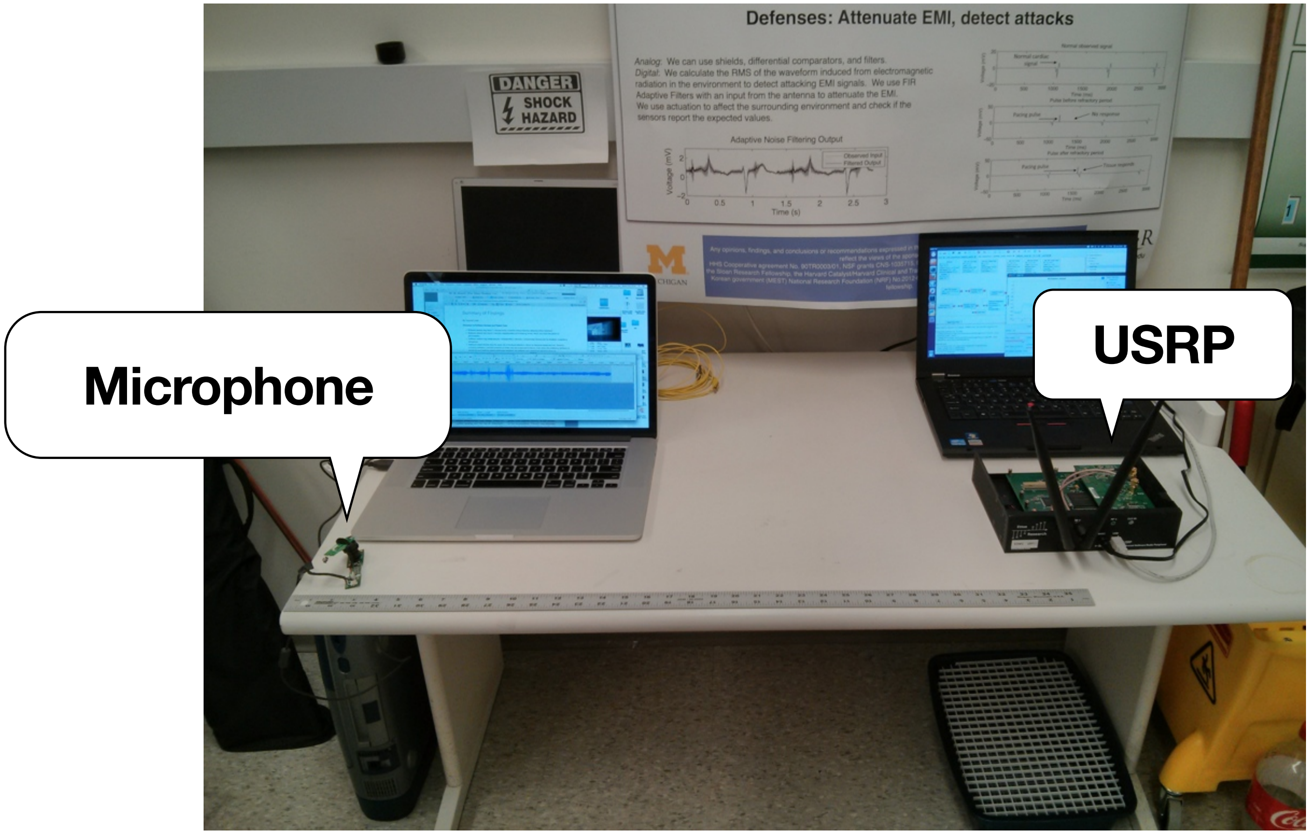
Fundamental Problem: Baseband

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



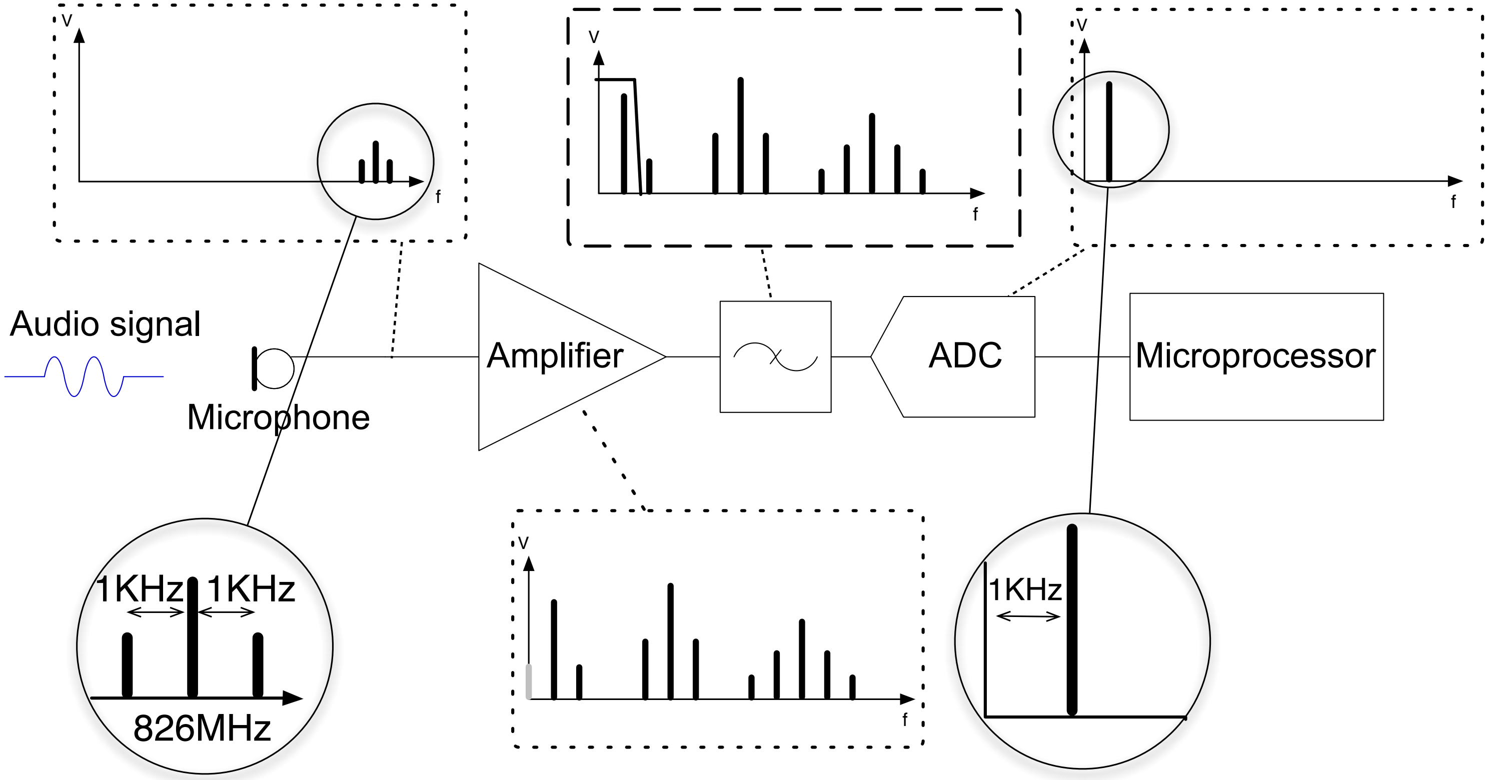
[“Ghost Talk” by Foo Kune et al., IEEE S&P 2013]

Microphone Interference with RF



["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Non-Linearity: Self Demodulation

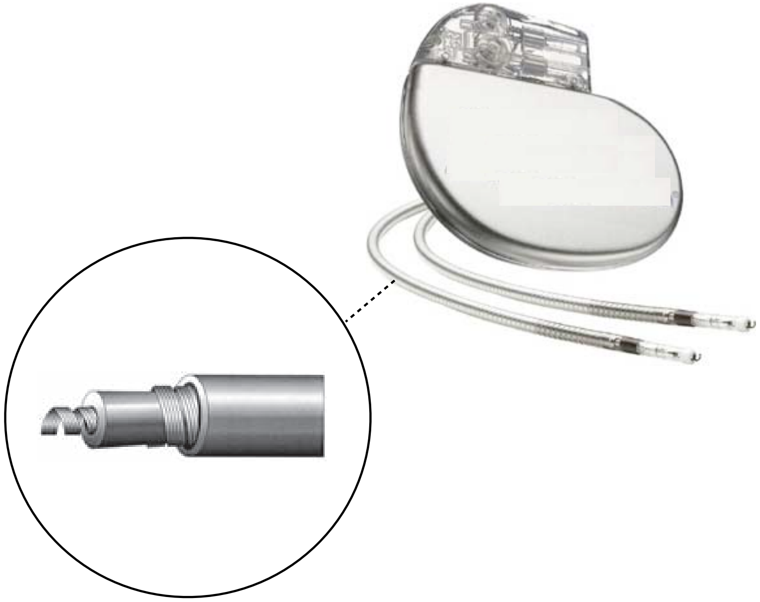


intermodulation distortion…

[“Ghost Talk” by Foo Kune et al., IEEE S&P 2013]

Intentional EMI on cardiac devices

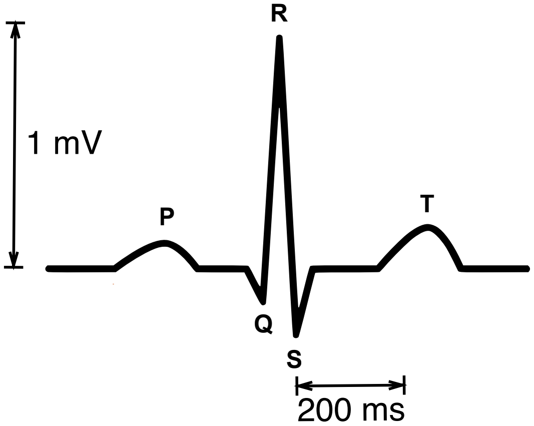
- Pacemakers, defibrillators
- Electrocardiogram machines

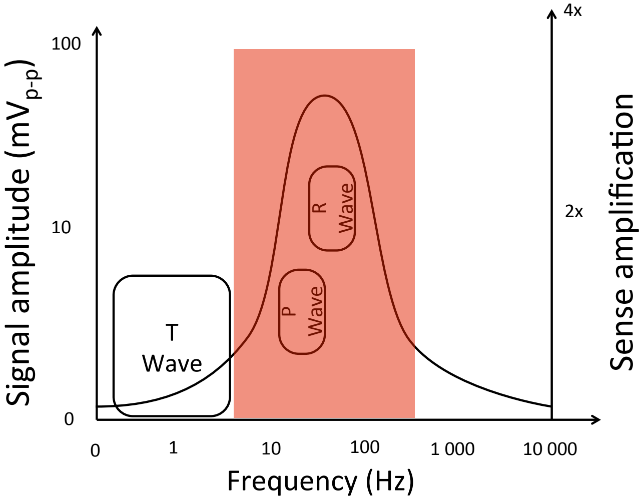


[“Ghost Talk” by Foo Kune et al., IEEE S&P 2013]

Cardiac devices vulnerable to baseband EMI

- Filter high frequency
  - 800MHz and GHz range: attenuation of up to 40dB
- Can’t filter baseband

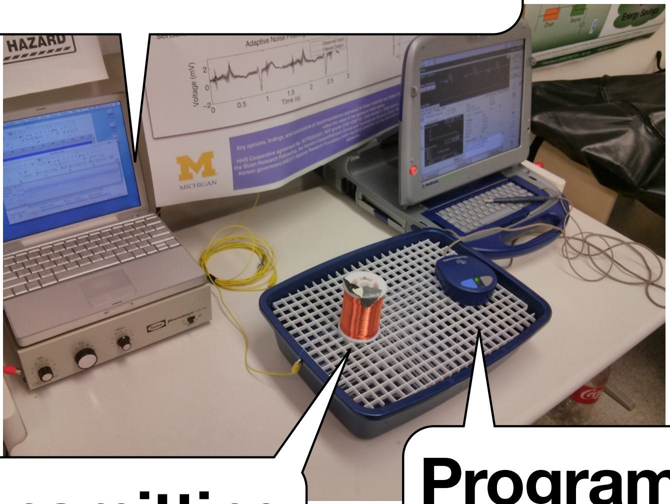




Cohan et al, 2008

[“Ghost Talk” by Foo Kune et al., IEEE S&P 2013]

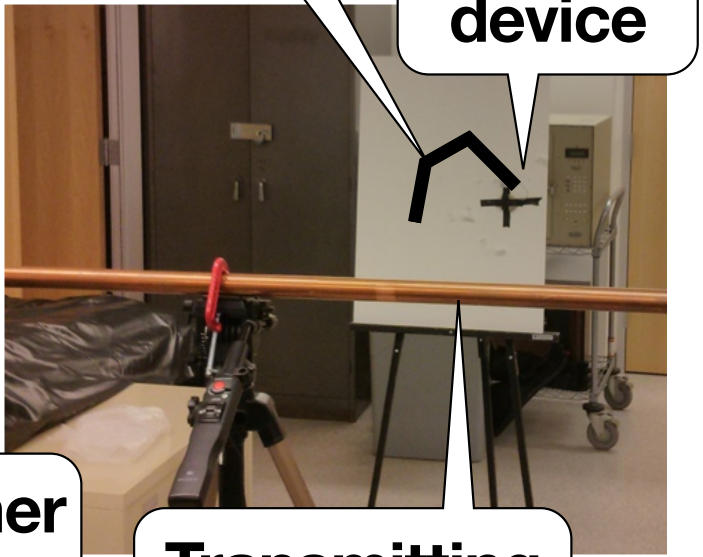
Experiment: Implants & Emitters



Waveform source and amplifier

Transmitting antenna

Programmer head over device



Curved leads

Cardiac device

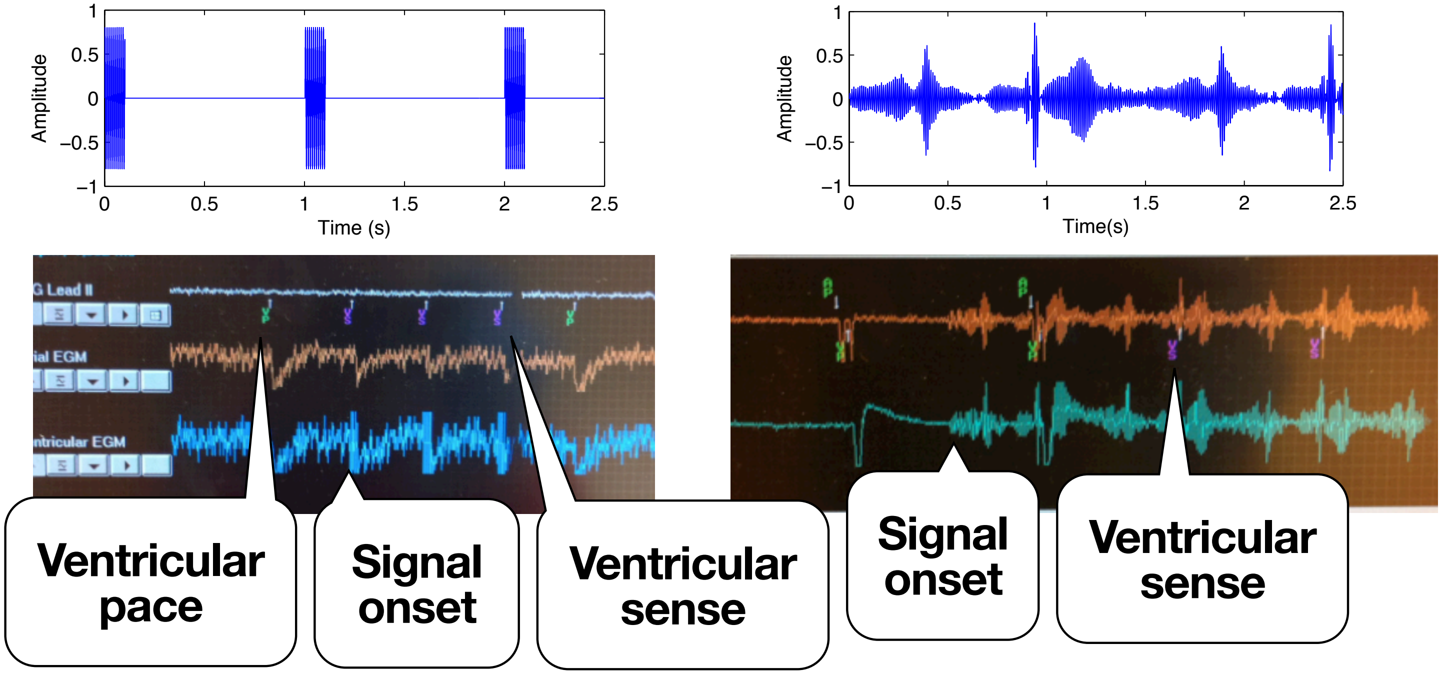
Transmitting antenna

[“Ghost Talk” by Foo Kune et al., IEEE S&P 2013]

Results: Waveforms & Responses

Pulsed sinusoid

Modulated heart beat



Ventricular pace

Signal onset

Ventricular sense

Signal onset

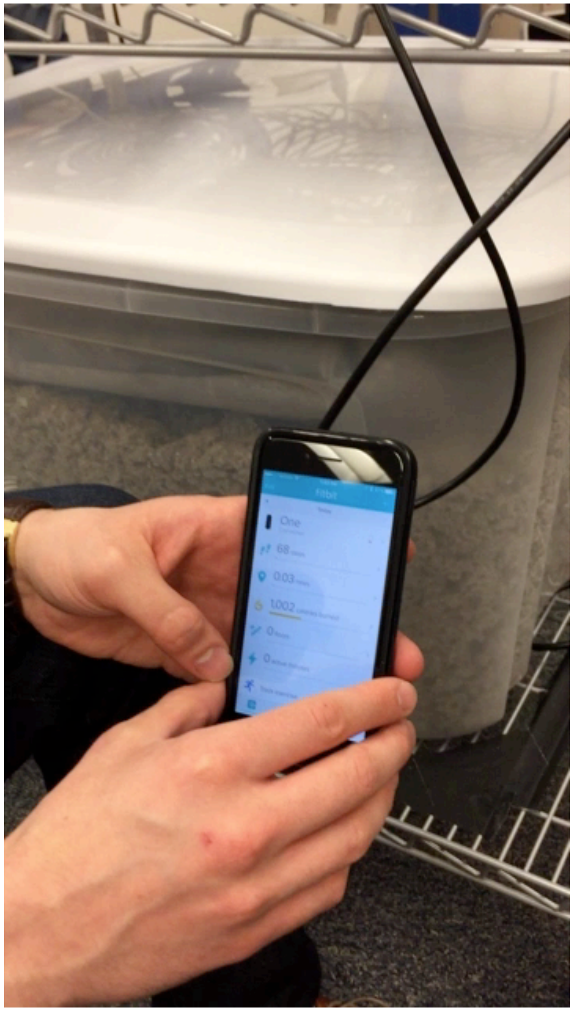
Ventricular sense

["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

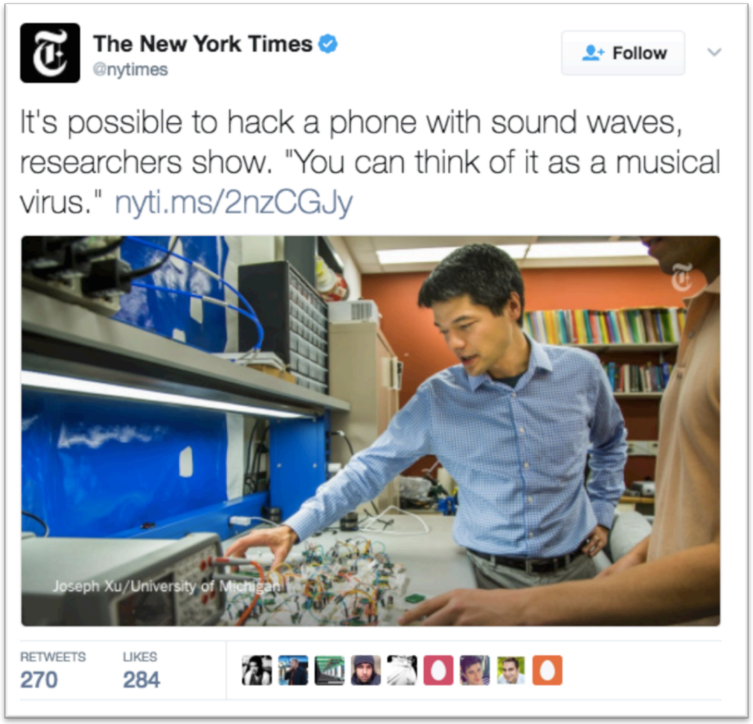
Good News: Distance

Device	Open air pacing	Open air Defib	Saline tips only	SynDaver
Medtronic Adapta	1.40m	NA	3cm	Untested
Medtronic InSync Sentry	1.57m	1.67m	5cm	8cm
Boston Scientific Cognis	1.34m	No defib	Untested	Untested
St. Jude Promote	0.68m	No defib	Untested	Untested

[“Ghost Talk” by Foo Kune et al., IEEE S&P 2013]



Sound and MEMS Sensor Security



The New York Times
@nytimes

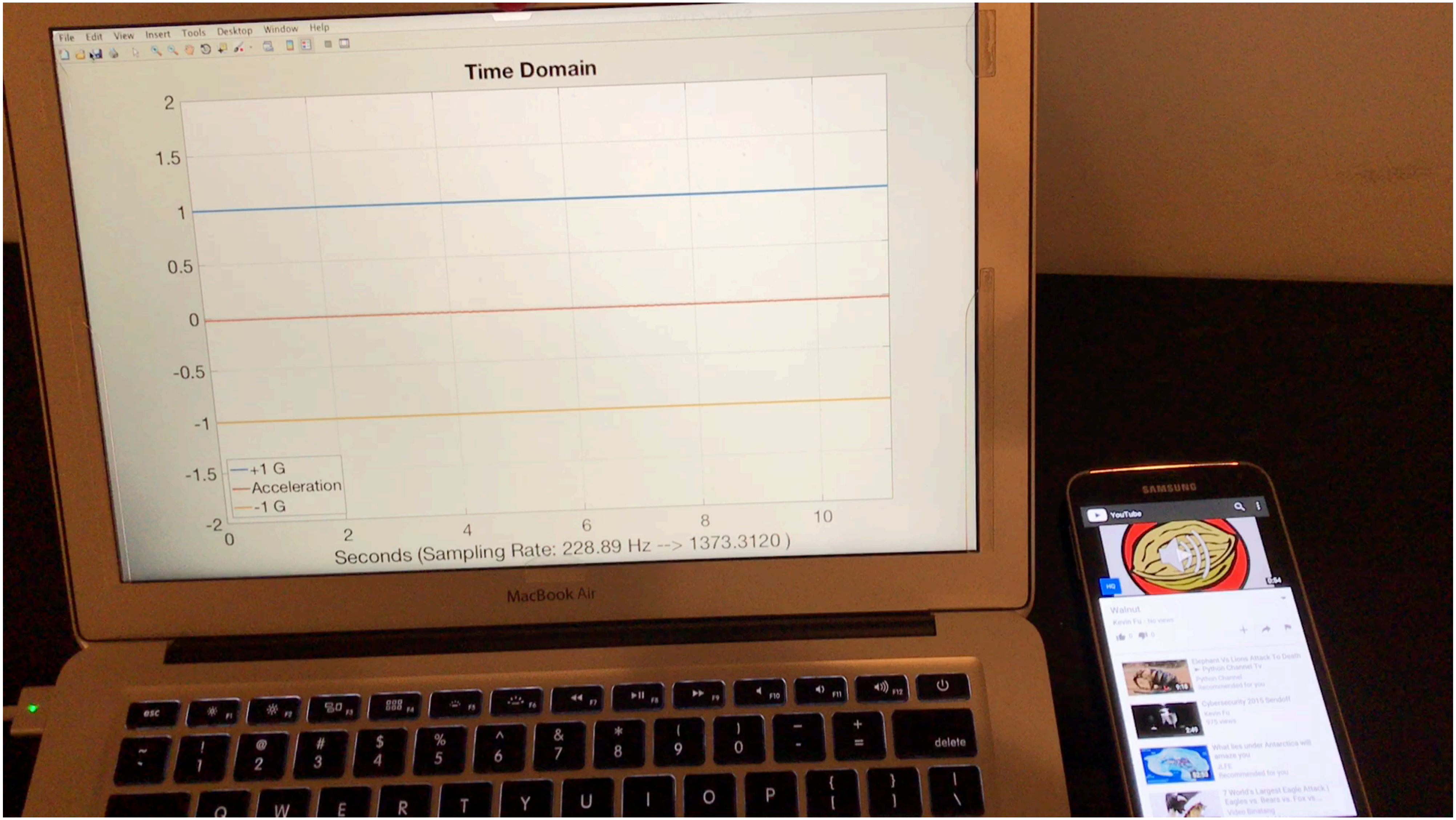
It's possible to hack a phone with sound waves, researchers show. "You can think of it as a musical virus." nyti.ms/2nzCGJy

Joseph Xu/University of Michigan

RETWEETS 270

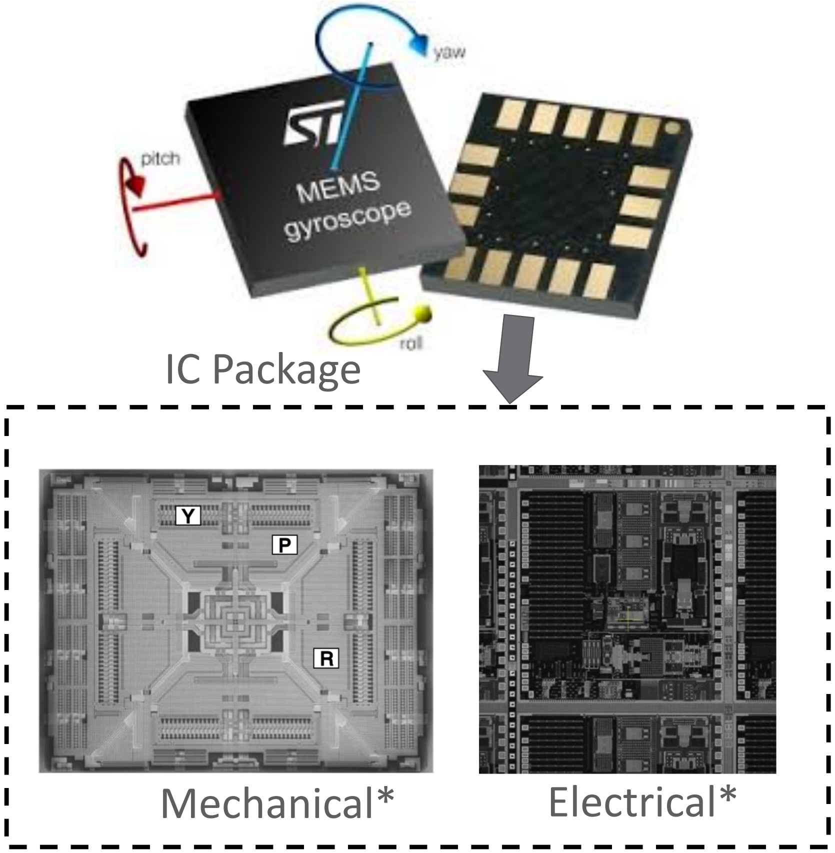
LIKES 284

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


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
HQ
0:54
Walnut
Kevin Fu · No views
Elephant Vs Lions Attack To Death ► Python Channel Tv
Python Channel
Recommended for you
9:10
Cybersecurity 2015 Sendoff
Kevin Fu
975 views
2:49
What lies under Antarctica will amaze you
JLFE
Recommended for you
02:53
7 World's Largest Eagle Attack | Eagles vs. Bears vs. Fox vs...
Video Binatang

MEMS Sensors

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



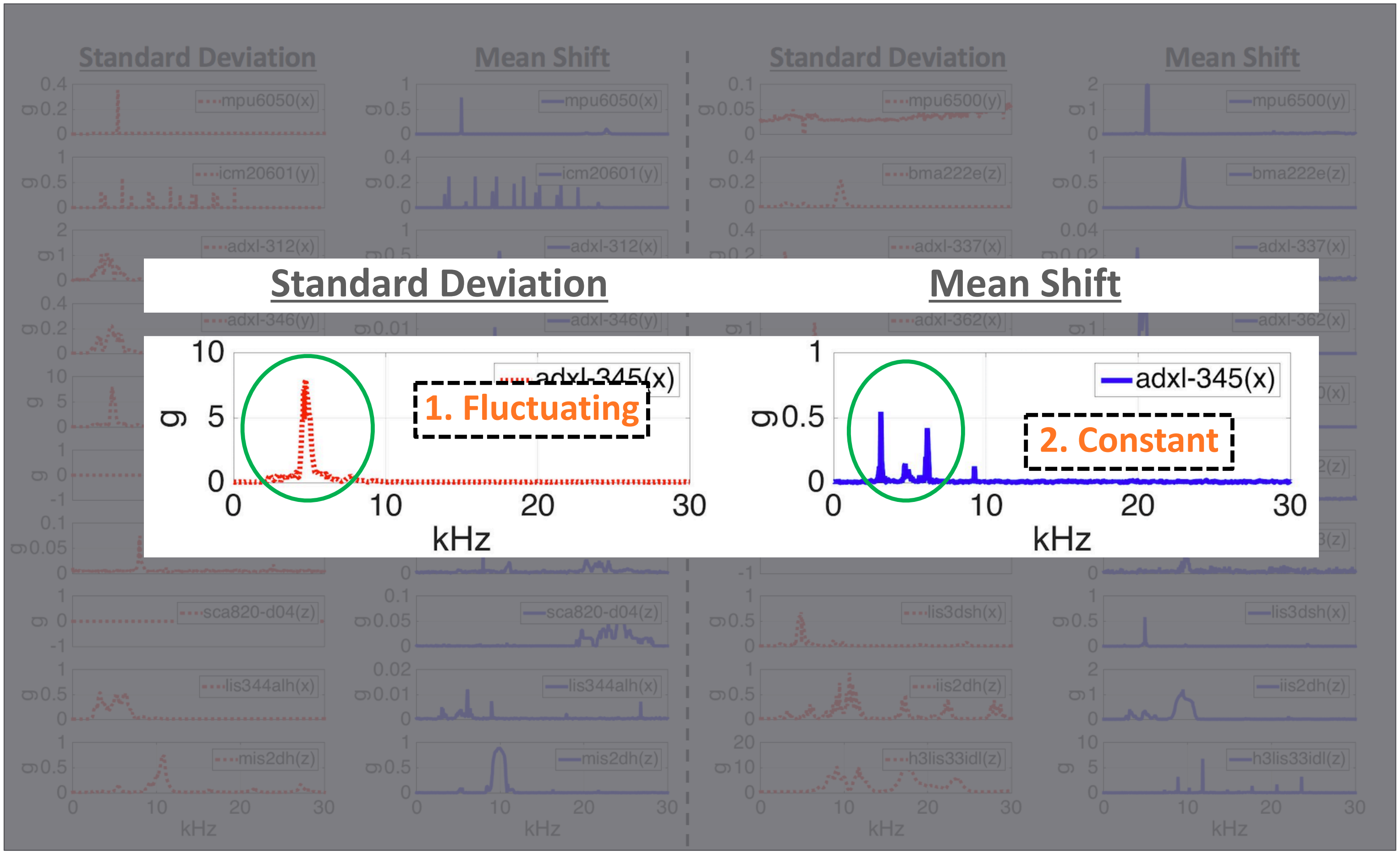
IC Package

Mechanical*

Electrical*

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

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



Standard Deviation

Mean Shift

1. Fluctuating

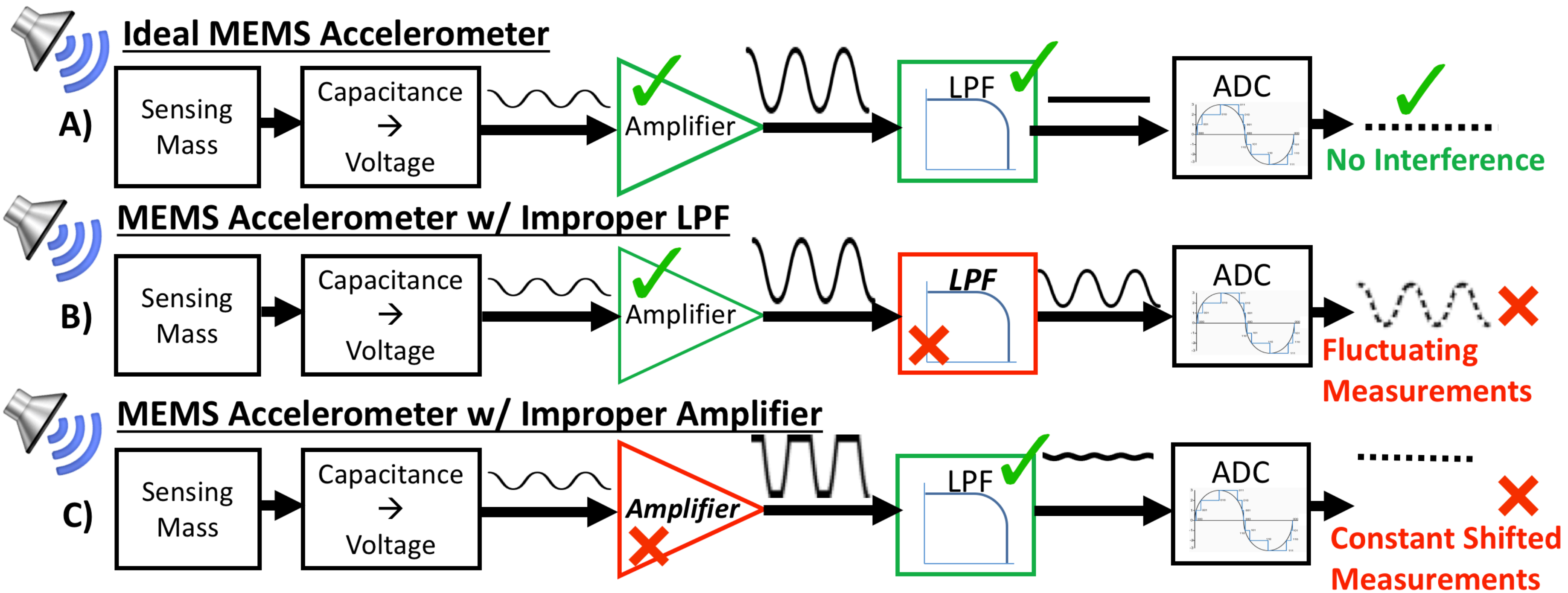
2. Constant

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

Signal Distortion

Two types of spoofed acceleration

- Fluctuating accelerometer output
- Constant accelerometer output

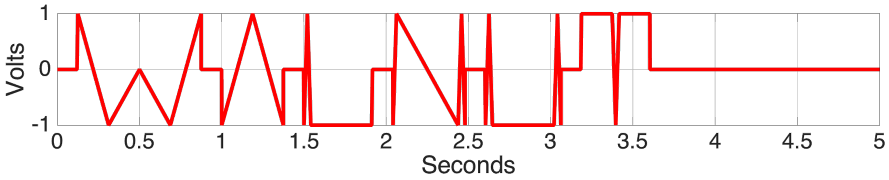


asymmetric clipping

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

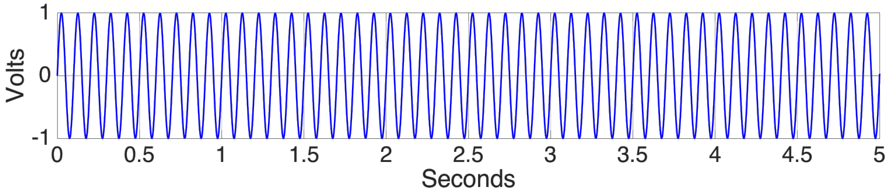
Output Control Modulation

Desired Accelerometer
Output Signal



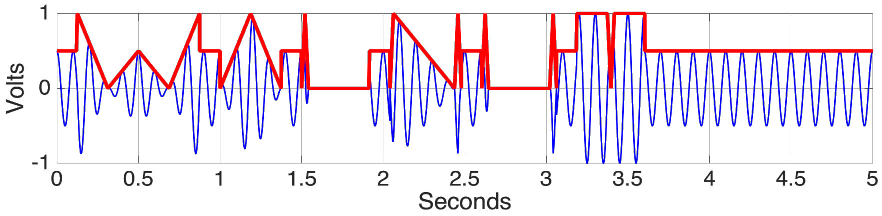
+

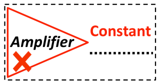
MEMS Resonant Frequency
(Carrier Signal)



=

Modulated Acoustic
Attack Signal





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

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

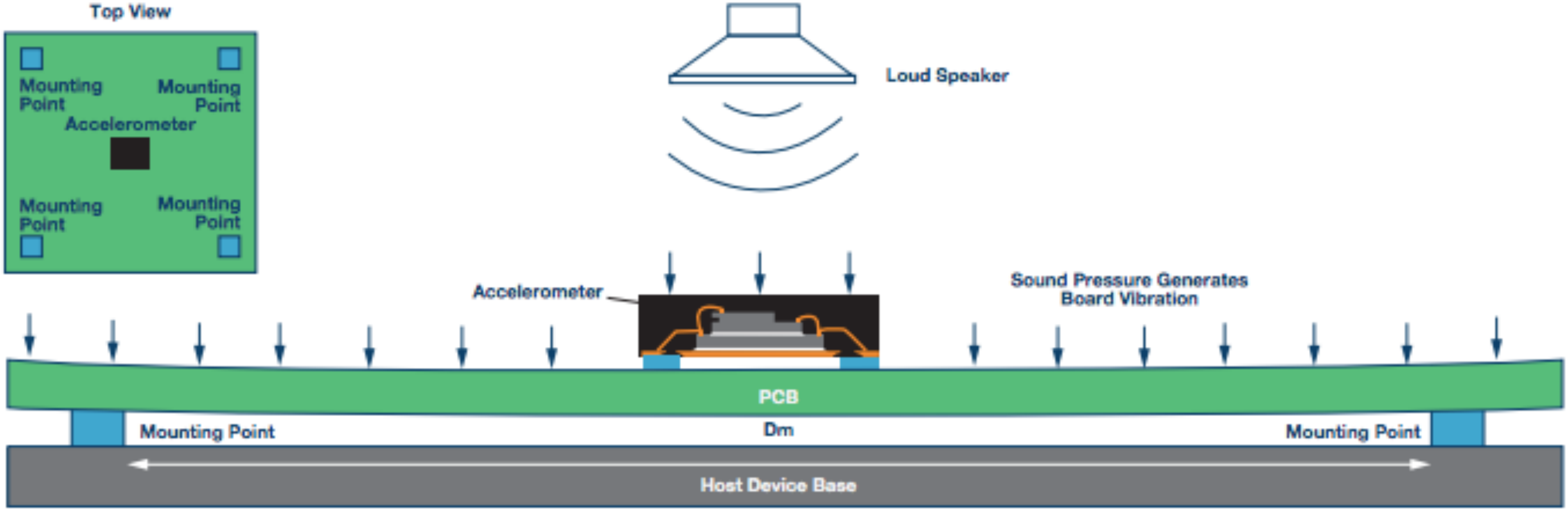


Figure 1. MEMS accelerometer board and mounting with acoustic vibration from off-board speaker.

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

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

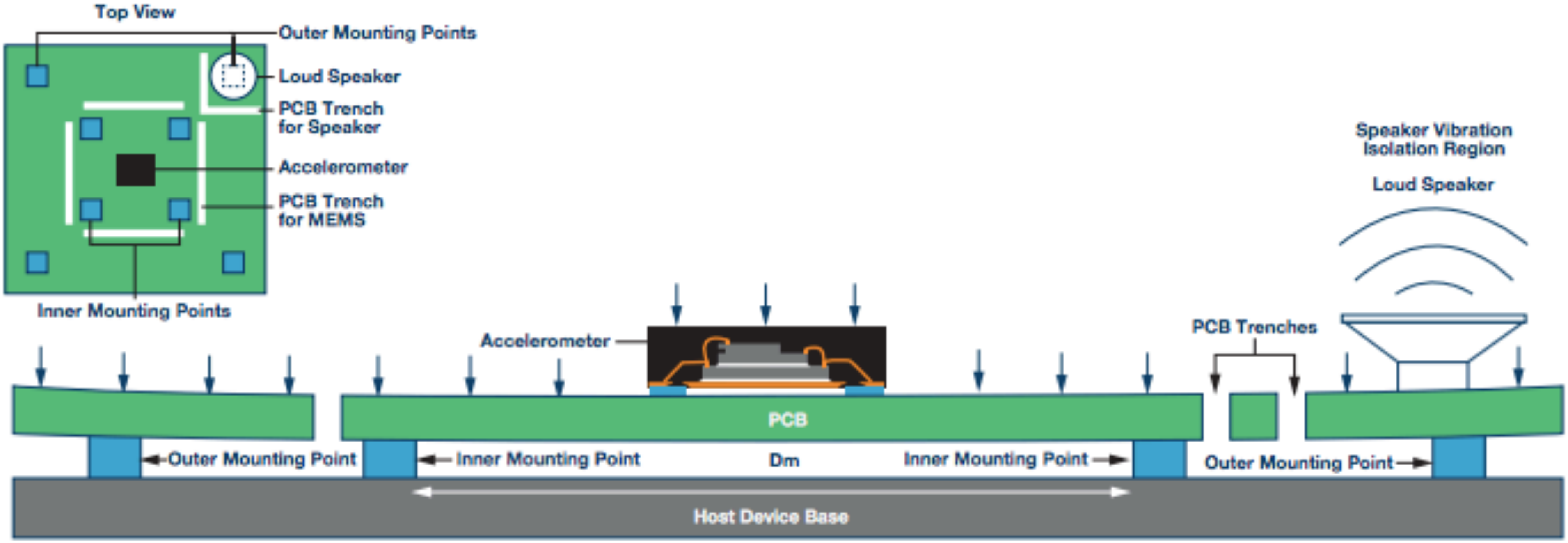
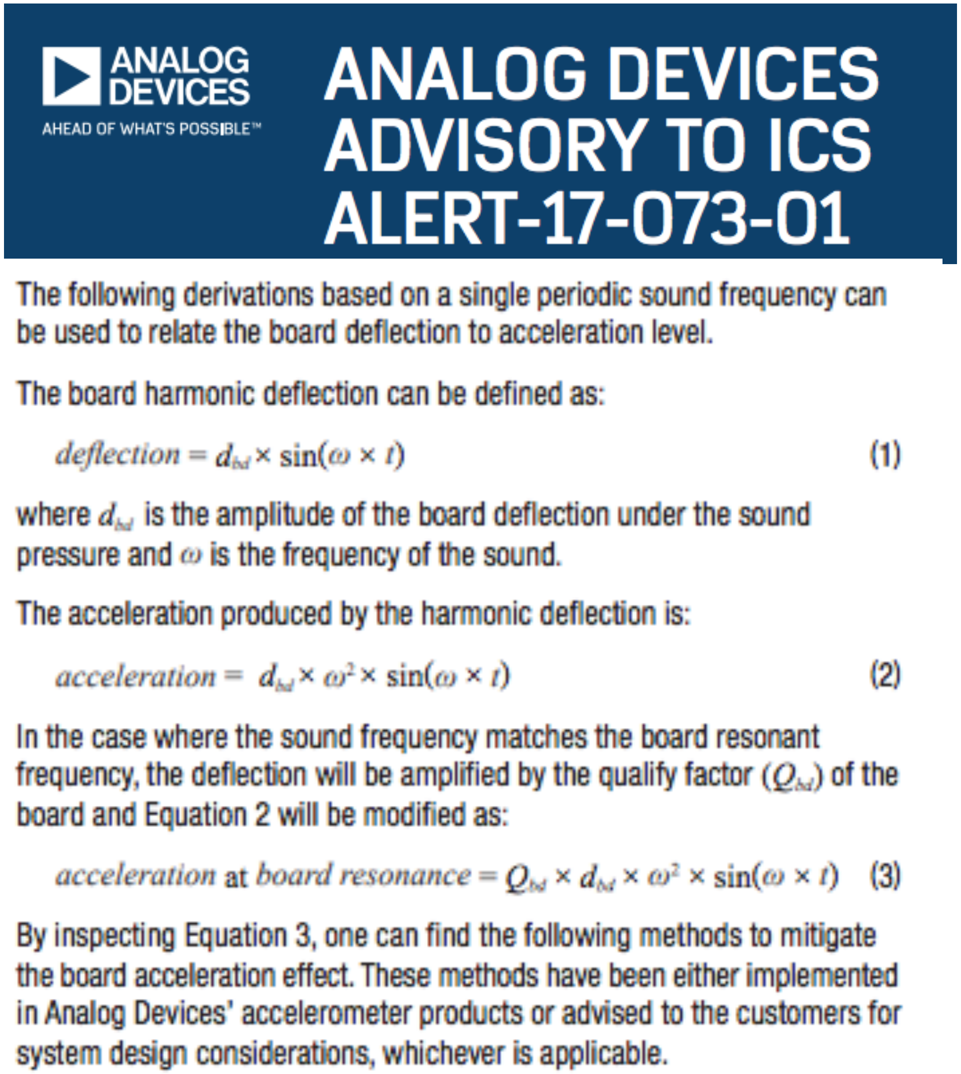


Figure 2. MEMS accelerometer board and mounting with acoustic and mechanical vibration from on-board speaker.

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:

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

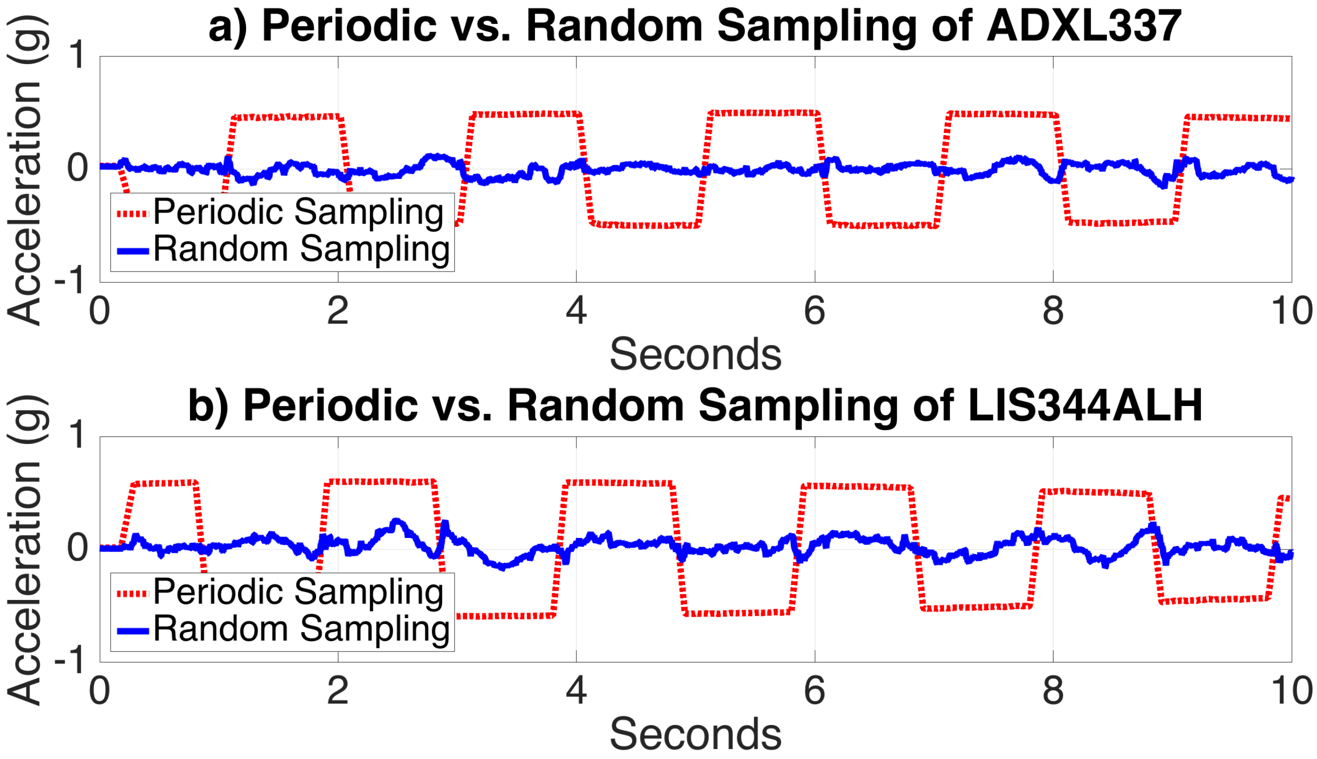
In the case where the sound frequency matches the board resonant frequency, the deflection will be amplified by the qualify factor (Q_{bd}) of the board and Equation 2 will be modified as:

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

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.

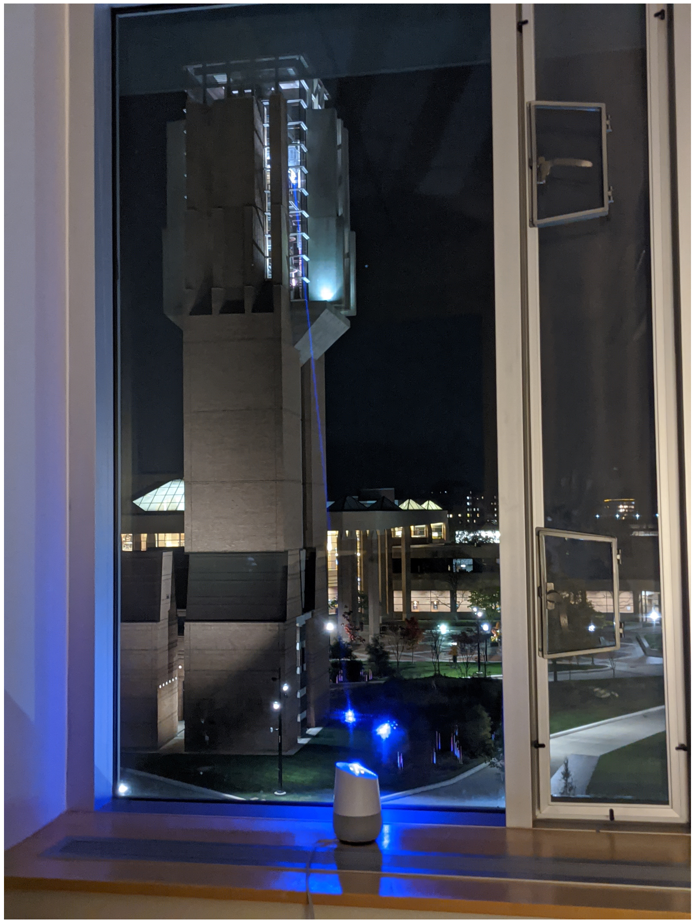
Randomized Sampling

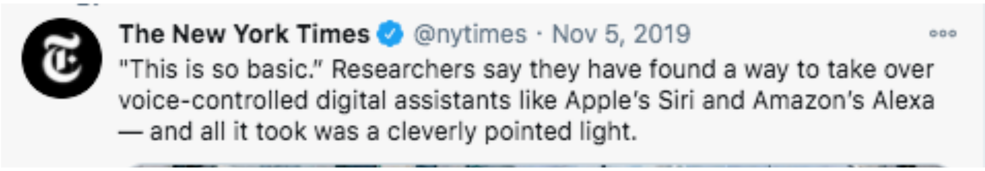
- Destroy predictability of sampling regime
- Randomize delay at each sampling interval



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

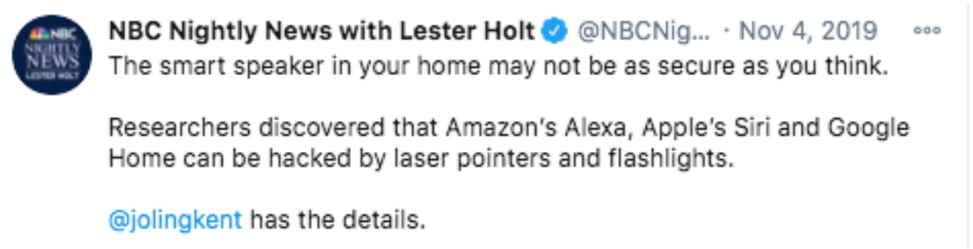
Lasers & Sensor Security





The New York Times @nytimes · Nov 5, 2019

"This is so basic." Researchers say they have found a way to take over voice-controlled digital assistants like Apple's Siri and Amazon's Alexa — and all it took was a cleverly pointed light.

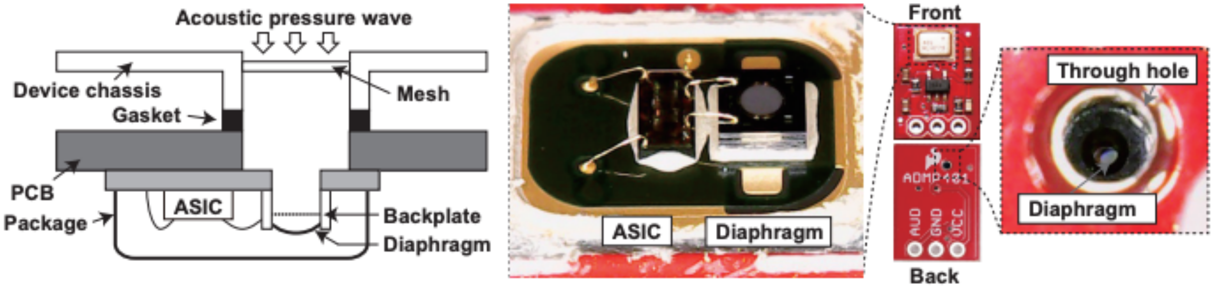


NBC Nightly News with Lester Holt @NBCNig... · Nov 4, 2019

The smart speaker in your home may not be as secure as you think.

Researchers discovered that Amazon's Alexa, Apple's Siri and Google Home can be hacked by laser pointers and flashlights.

@jolingkent has the details.



Sugawara et al., Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems, USENIX Security 2020

[“Light Commands” by Sugawara et al., USENIX Security 2020]

[“Light Commands” by Sugawara et al., USENIX Security 2020]

[“Light Commands” by Sugawara et al., USENIX Security 2020]

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

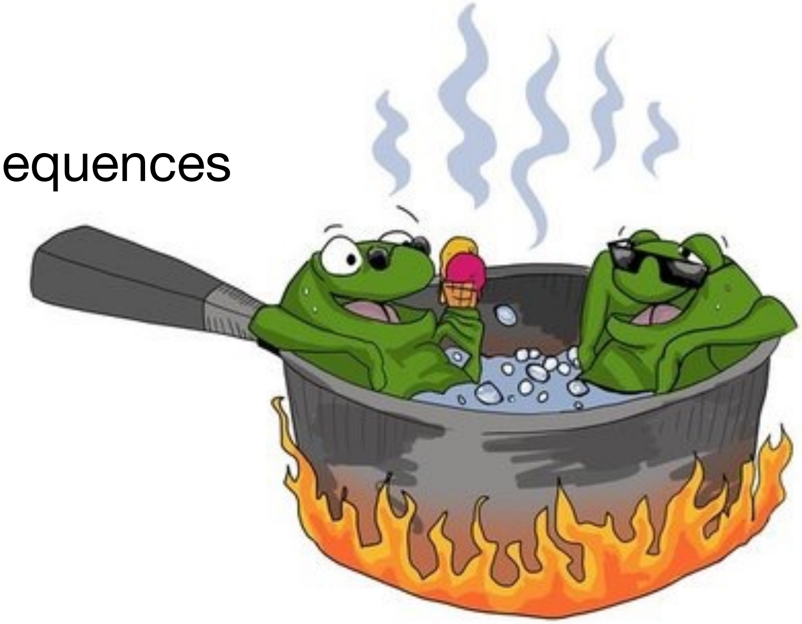
- 👉Physically de-risk **intentional interference** with more deliberate HW specs & design (e.g., resonance)

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



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

Embedded Security References

- CRA's Grand Challenges for Embedded Security Research in a Connected World
- 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
  - 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]
- Lasers and MEMS injection
  - Light Commands [Sugawara et al., USENIX Security 2020]

Research Vision:

A world where science-based security is built-in by design to all embedded systems:

  - medical devices
  - healthcare delivery
  - autonomous transportation
  - manufacturing
  - the Internet of Things (IoT)

- Why important now?
  - Consumers need confidence in security and privacy before they can trust innovative medical devices and other emerging technology

Conclusions

✶ Microprocessors should not blindly trust sensors

✓ Protect emerging devices with SW that leverages physics

✓ Focus on trustworthy systems, rather than just secure components

Seeking PhD appliants in CS, ECE, or bioengineering.
To join the team, ask us about
our values on our website!

Side Eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses

Yan Long[1], (yanlong@umich.edu),
Pirouz Naghavi[2], Blas Kojusner[2],
Sara Rampazzi[2], Kevin Butler[2], Kevin Fu[3]

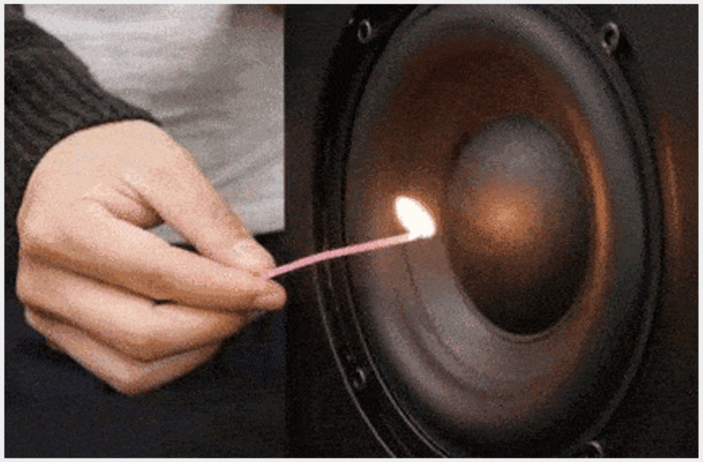
[1] University of Michigan, EECS

[2] University of Florida, CISE

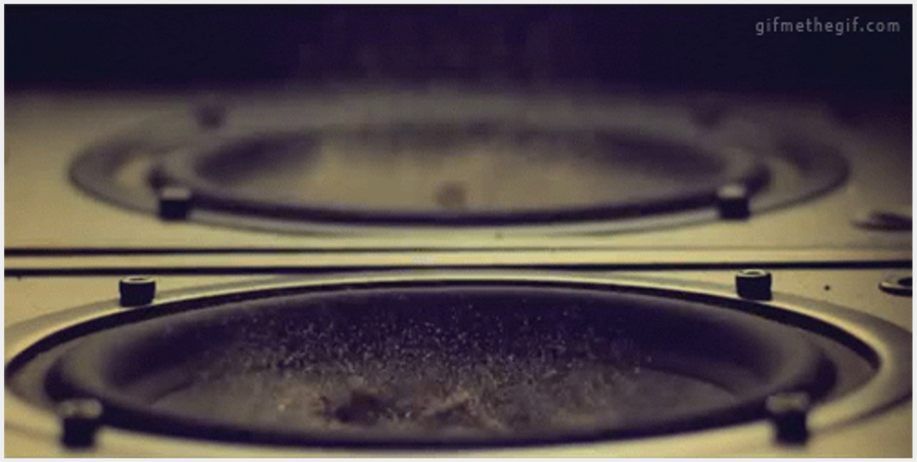
[3] Northeastern University, ECE & CS

Sound Vibrations

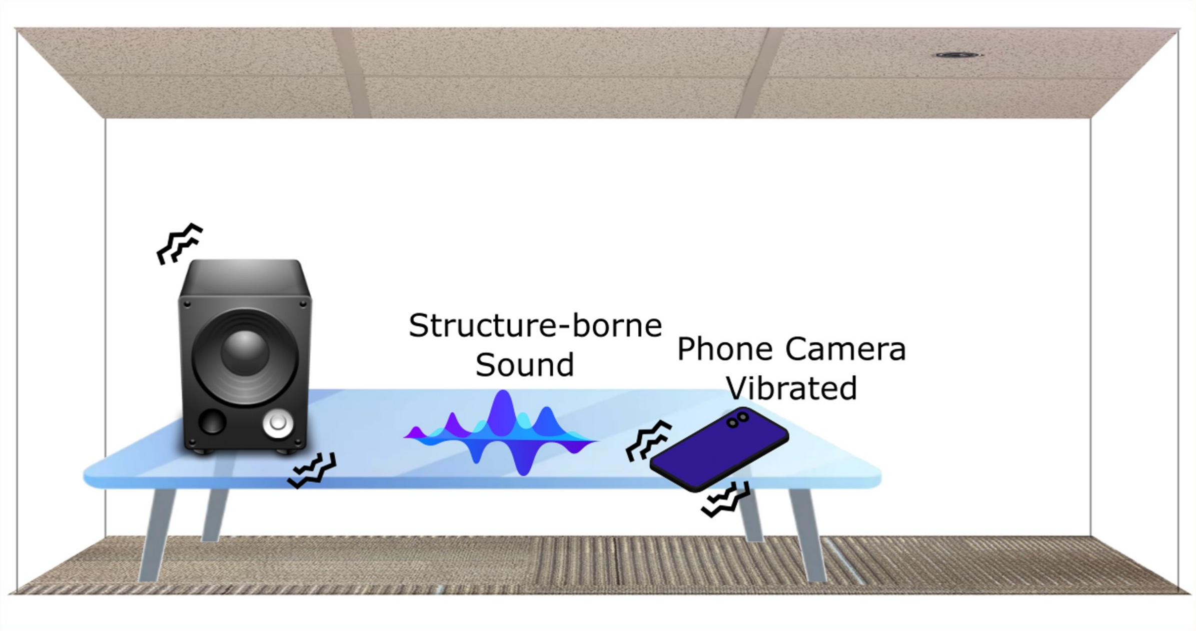
Air-borne



Structure-borne



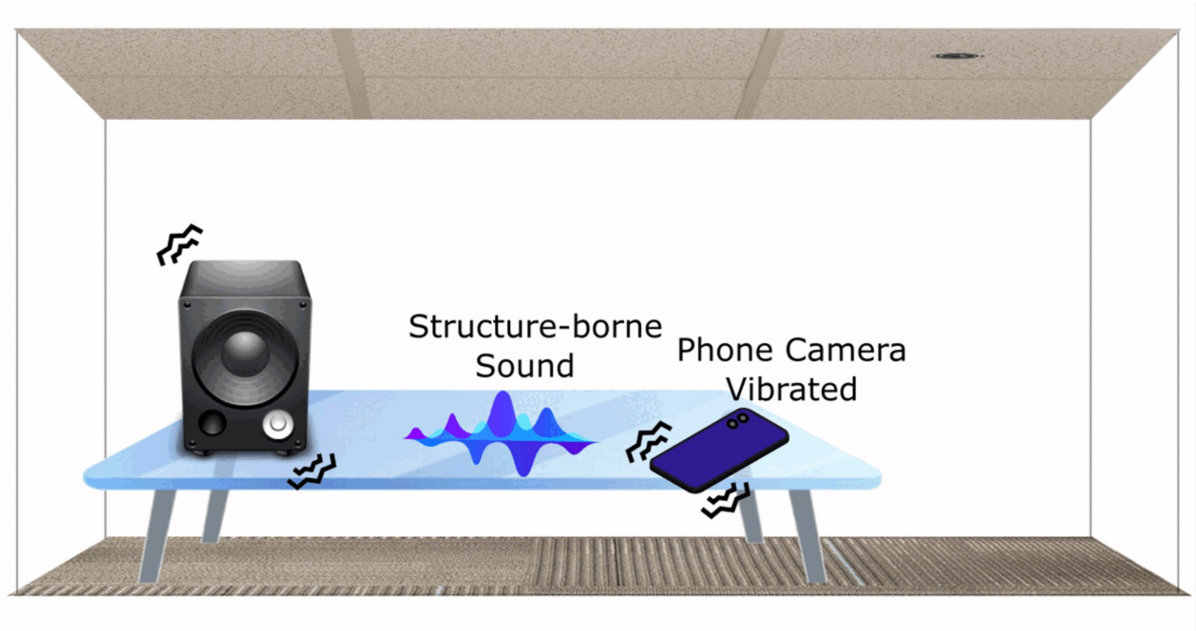
Overview



Adversary:

- Eavesdrop on sound
- Camera access
- No microphone access

Overview



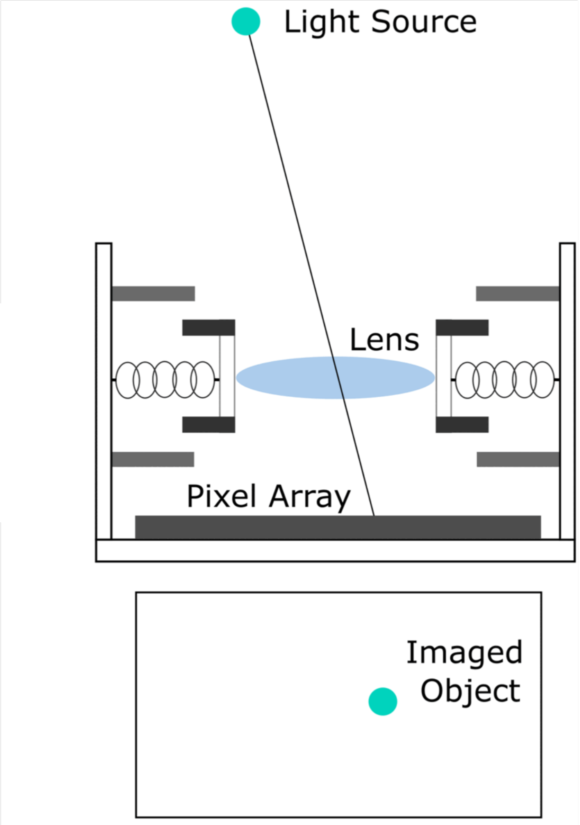
- Acoustic signals leak into **muted videos**

- 2 Gender (99.67%)
- 20 Speaker (91.28%)
- 10 Spoken digits (80.66%)

Fundamental Principles

Camera POV Variations

Camera Sensor

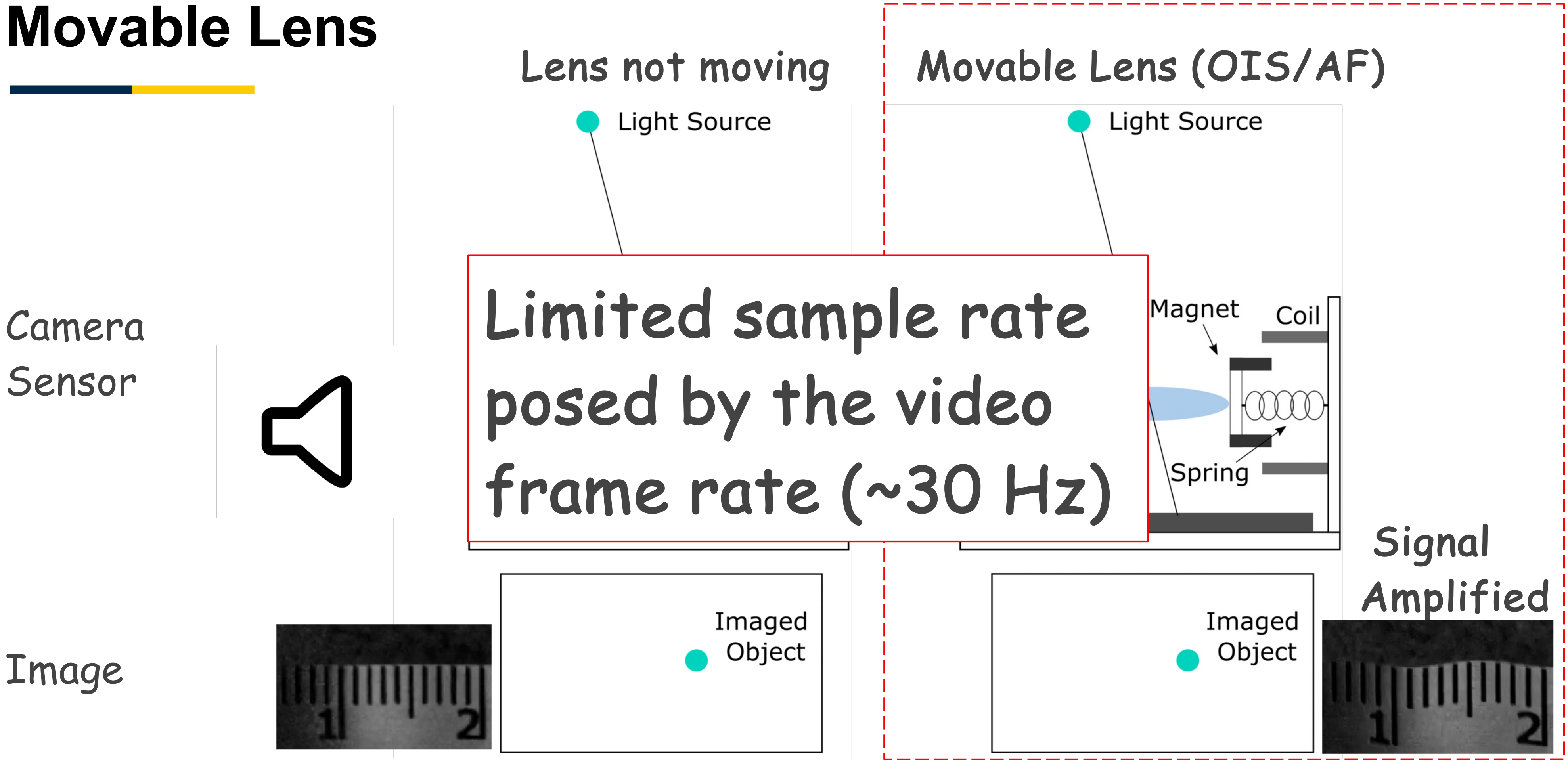


Image

$$f(Sound) = Image$$

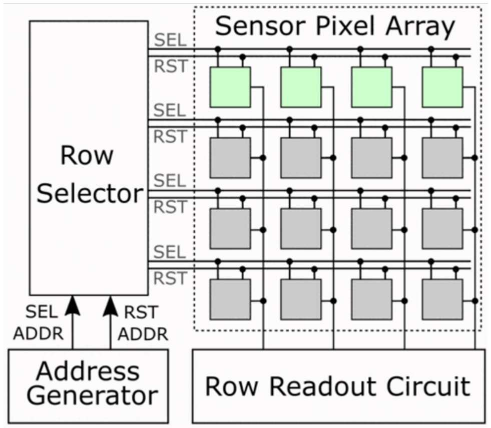
$$g(Image) = Sound$$

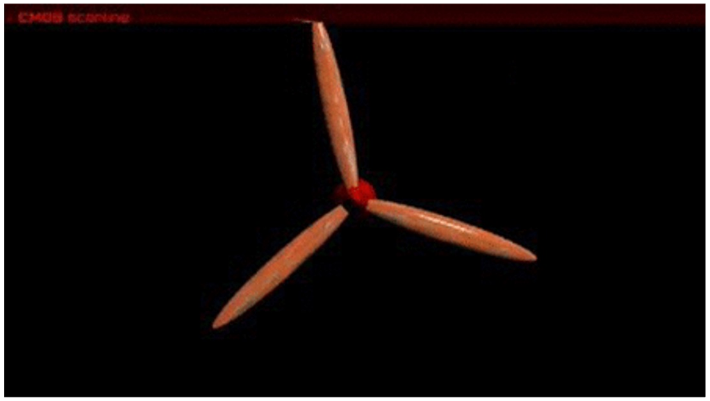
Movable Lens



Limited sample rate posed by the video frame rate (~30 Hz)

Rolling Shutter



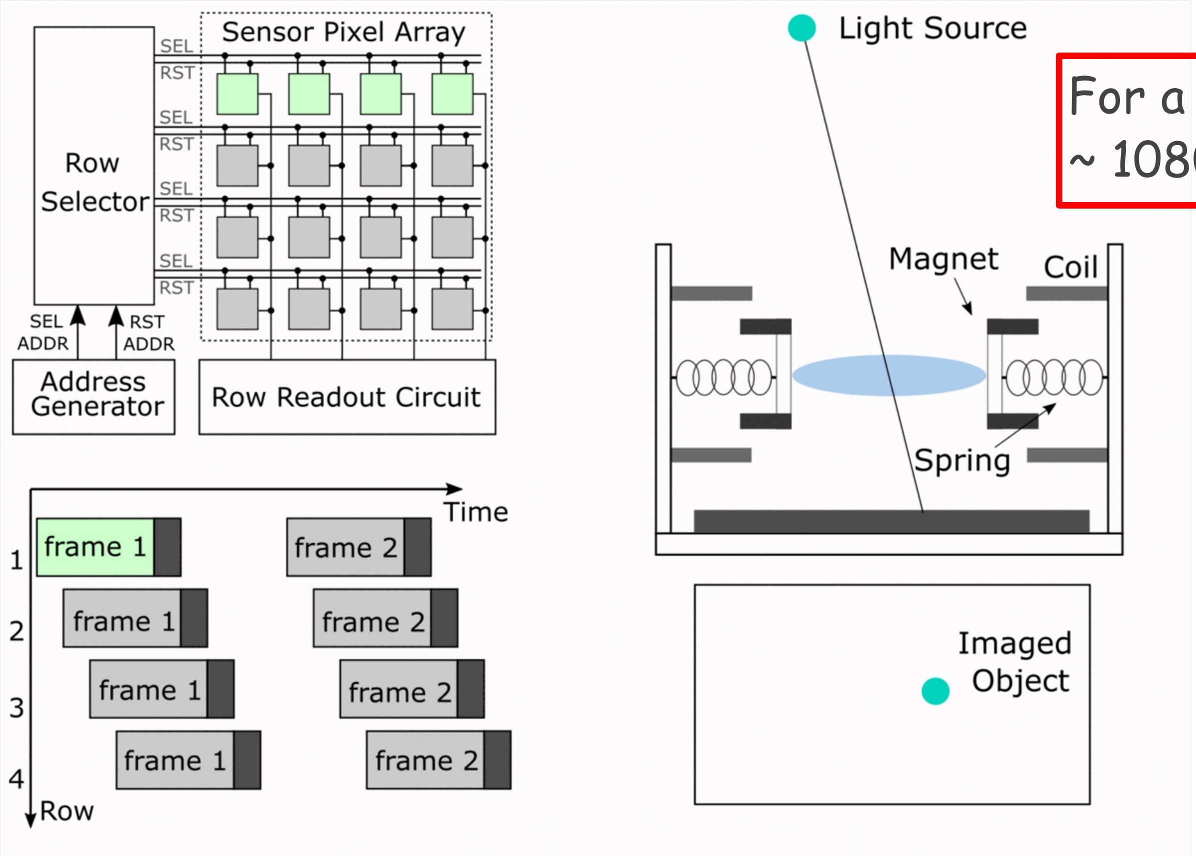


Rotational Motion

[Photo by David Adler]

Horizontal Motion

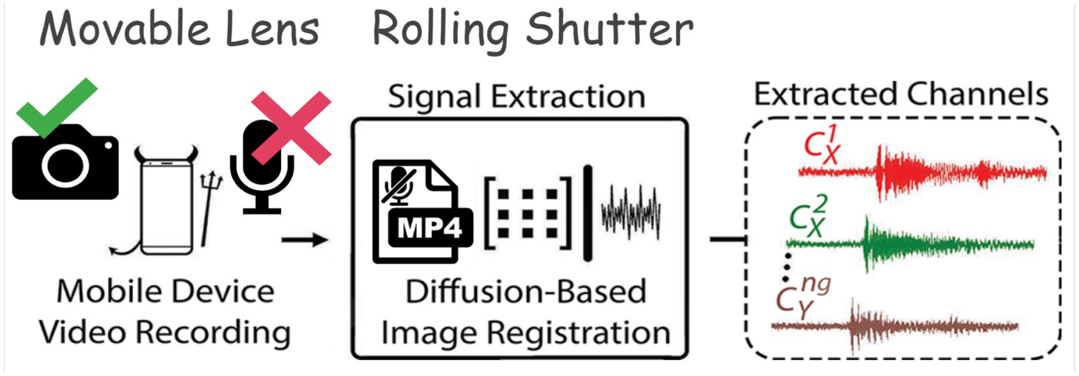
Rolling shutter

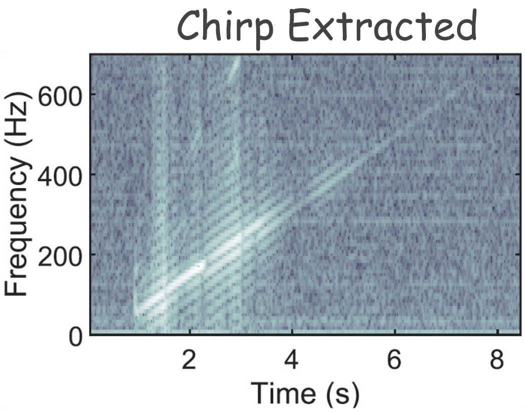


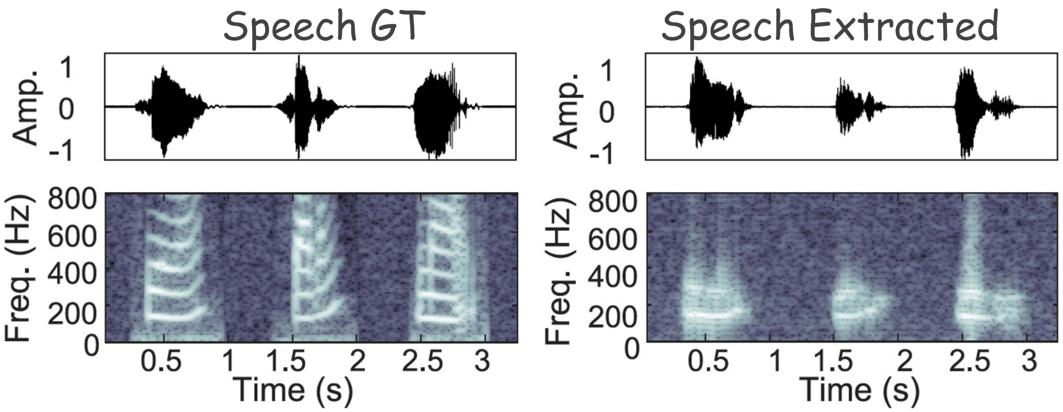
For a 1080p video:
~ 1080x sample points

System Design & Results

Attack Mechanism

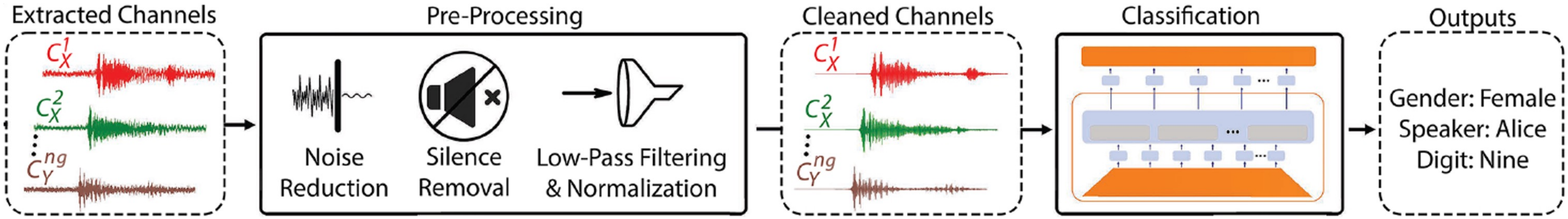






Audio Samples: https://sideeyeattack.github.io/Website/

Attack Mechanism

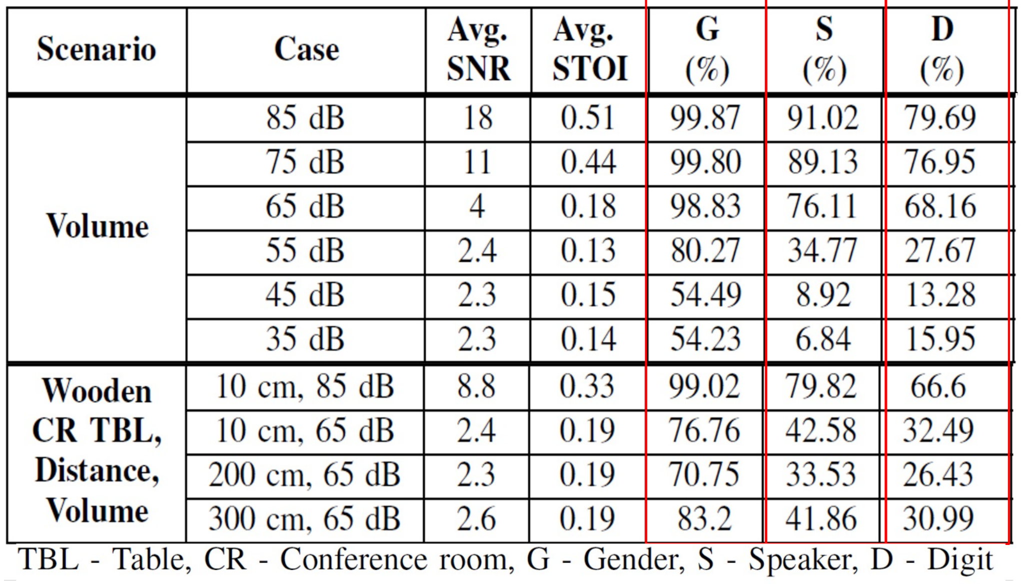


Customized HuBERT Model

Same-surface Scenarios

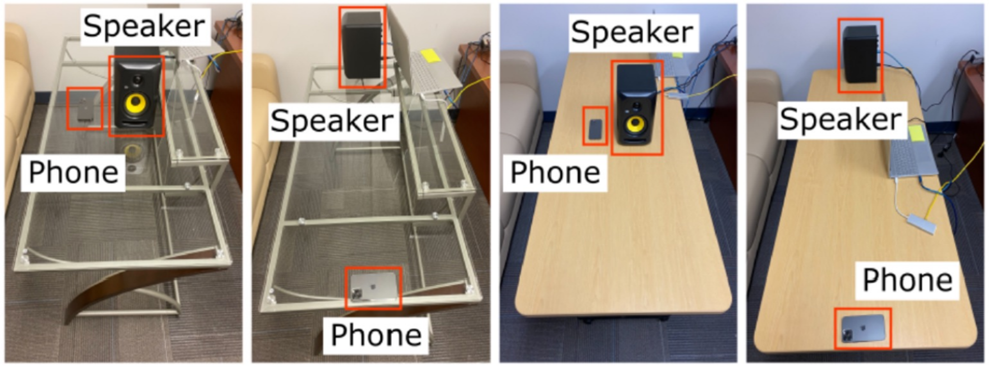
(random guess)

>50% >5% >10%



Scenario	Case	Avg. SNR	Avg. STOI	G (%)	S (%)	D (%)
Volume	85 dB	18	0.51	99.87	91.02	79.69
	75 dB	11	0.44	99.80	89.13	76.95
	65 dB	4	0.18	98.83	76.11	68.16
	55 dB	2.4	0.13	80.27	34.77	27.67
	45 dB	2.3	0.15	54.49	8.92	13.28
	35 dB	2.3	0.14	54.23	6.84	15.95
Wooden CR TBL, Distance, Volume	10 cm, 85 dB	8.8	0.33	99.02	79.82	66.6
	10 cm, 65 dB	2.4	0.19	76.76	42.58	32.49
	200 cm, 65 dB	2.3	0.19	70.75	33.53	26.43
	300 cm, 65 dB	2.6	0.19	83.2	41.86	30.99

TBL - Table, CR - Conference room, G - Gender, S - Speaker, D - Digit

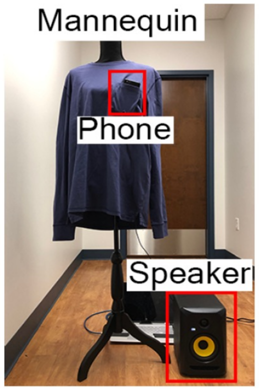


2 genders, 20 speakers, 10 spoken digits

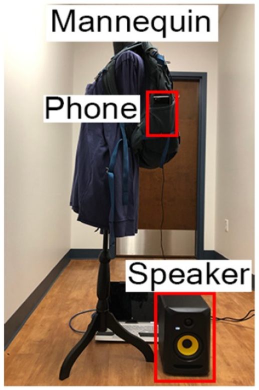
(https://github.com/soerenab/AudioMNIST)

Different-surface Scenarios

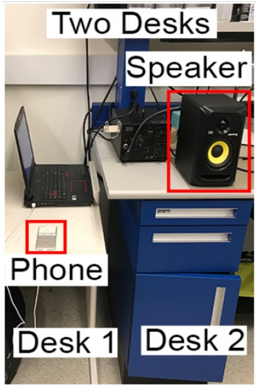
Shirt Pocket



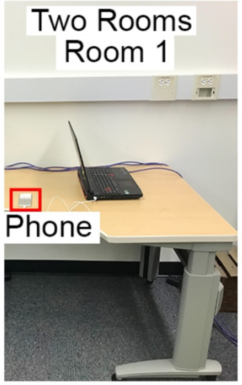
Bag Pocket

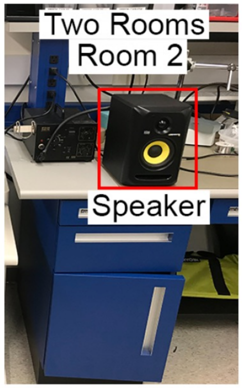


Two desks



Two Different Rooms

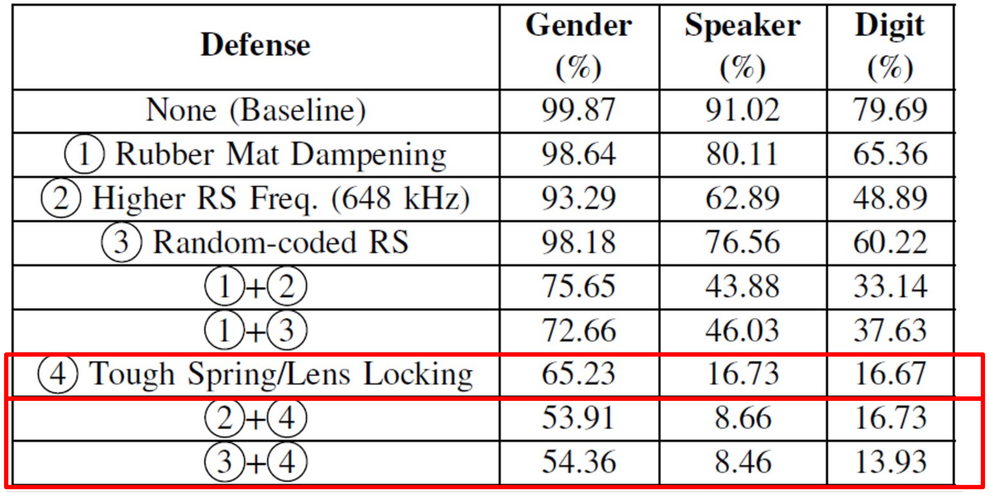




			>50%	>5%	>10%
Scenario	**Avg. SNR**	**Avg. STOI**	**G (%)**	**S (%)**	**D (%)**
Monitor Stand 85 dB	11	0.45	99.09	80.53	60.42
Monitor Stand 65 dB	2.6	0.09	84.05	42.32	32.1
Two Desks 85 dB	2.6	0.08	75.72	19.6	14.26
Two Rooms 85 dB	2.3	0.06	66.93	15.17	15.17
Shirt Pocket 85 dB	2.5	0.19	95.9	66.37	45.7
Bag Pocket 85 dB	4.1	0.23	93.1	40.1	55.34

Mitigation

- User-based: (1) lower-quality cameras, (2) larger distances, (3) dampening
- Address rolling shutters (RS): (1) higher RS frequency, (2) random-coded RS
- Address movable lens: (1) tougher springs, (2) lens locking



Defense	Gender (%)	Speaker (%)	Digit (%)
None (Baseline)	99.87	91.02	79.69
① Rubber Mat Dampening	98.64	80.11	65.36
② Higher RS Freq. (648 kHz)	93.29	62.89	48.89
③ Random-coded RS	98.18	76.56	60.22
①+②	75.65	43.88	33.14
①+③	72.66	46.03	37.63
④ Tough Spring/Lens Locking	65.23	16.73	16.67
②+④	53.91	8.66	16.73
③+④	54.36	8.46	13.93

2-class 20-class 10-class

Applications

- Digital forensics on photographs for prosecution or defense
    - Opto-acoustic equivalent to DNA profiling
    - Exonerate by showing absence of opto-acoustic fingerprint
    - Implicate by showing presence of opto-acoustic fingerprint
- Law enforcement and private investigation
    - De-anonymize disguised or muted voices from kidnapping videos and propaganda
    - Determine likely gender and identity associated with voices modulated into pixels
    - Line up of the usual suspects: Determine statistical likelihood of presence or absence of a speaking individual from a recorded off-camera scene
    - Determine probability of phrases spoken behind the camera in dubbed videos (TikTok, IG, etc.)
- Detecting deep fakes or synthetic media in political videos, propaganda, etc.
- Advertising based on posted photographs that contain hints of conversations and individual interests

Summary

- Acoustic signals can leak into muted videos/image streams as POV variations
- Movable lens amplifies signals, rolling shutter increases sampling rates.

Team

https://sideeyeattack.github.io/Website/

Yan Long

Pirouz Naghavi

Blas Kojusner

Kevin Butler

Sara Rampazzi

Kevin Fu

SPQR

FICS Research

Fall 2023

P21_23: EM-Eye: Limiting the Optical-Electromagnetic Side Channel Leakage of Smartphone Cameras

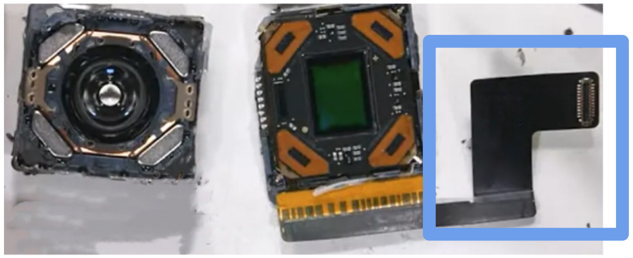
PI: Dr. Kevin Fu, Northeastern University

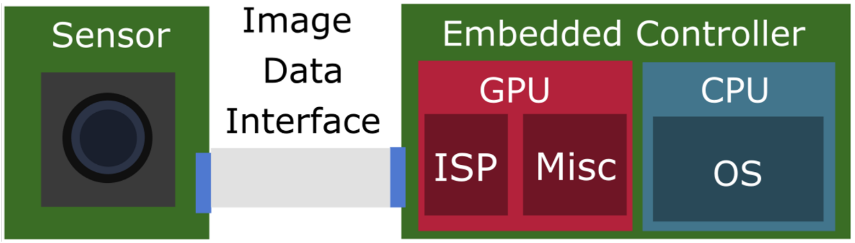
Student Researchers: Yan Long, Nina Shamsi

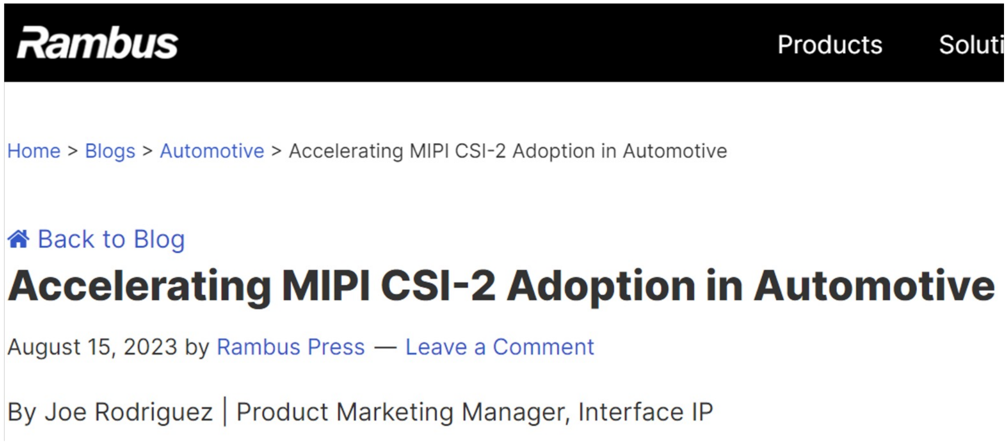
CHEST
CENTER FOR
HARDWARE AND
EMBEDDED SYSTEMS
SECURITY AND TRUST

EM-Eye: Limiting the Optical-Electromagnetic Side Channel Leakage of Smartphone Cameras

Fall 2023







Rambus

Products Soluti

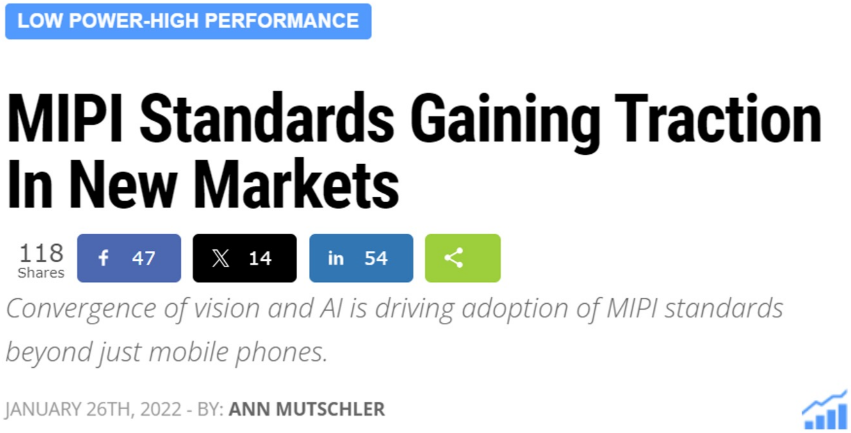
Home > Blogs > Automotive > Accelerating MIPI CSI-2 Adoption in Automotive

Back to Blog

Accelerating MIPI CSI-2 Adoption in Automotive

August 15, 2023 by Rambus Press — Leave a Comment

By Joe Rodriguez | Product Marketing Manager, Interface IP



LOW POWER-HIGH PERFORMANCE

MIPI Standards Gaining Traction In New Markets

118 Shares | f 47 | 𝕏 14 | in 54

Convergence of vision and AI is driving adoption of MIPI standards beyond just mobile phones.

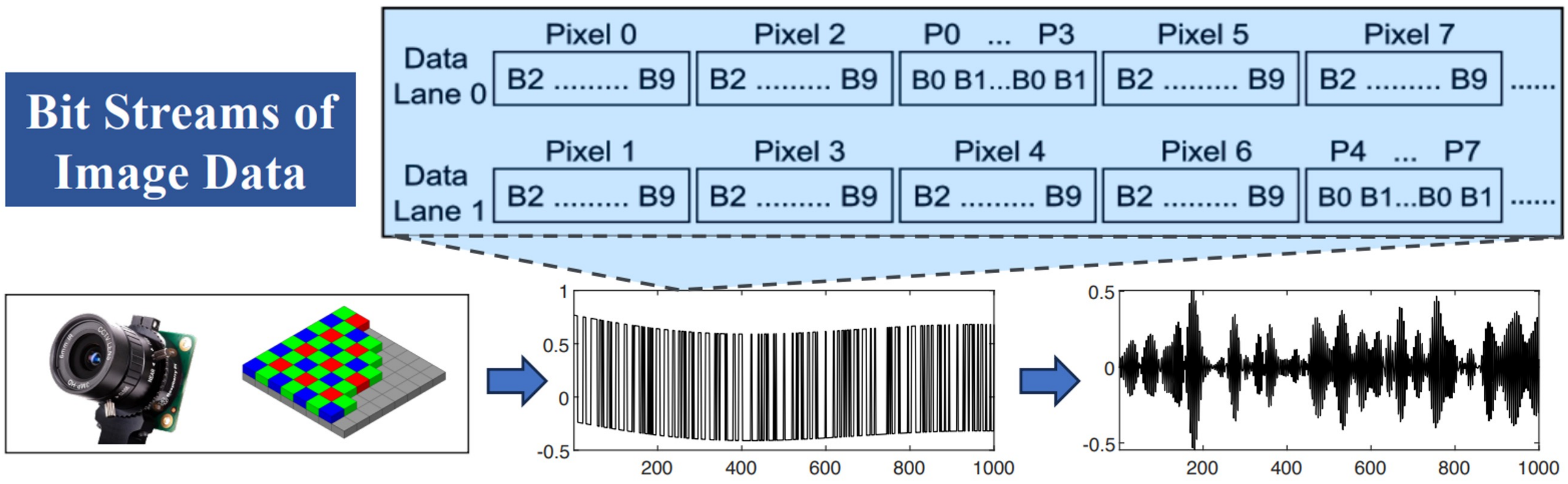
JANUARY 26TH, 2022 - BY: **ANN MUTSCHLER**

NSF UVa NU UCONN UCD UTD UC

CHEST
CENTER FOR HARDWARE AND EMBEDDED SYSTEMS SECURITY AND TRUST

EM-Eye: Limiting the Optical-Electromagnetic Side Channel Leakage of Smartphone Cameras

Fall 2023

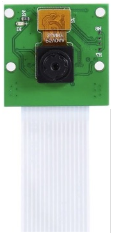


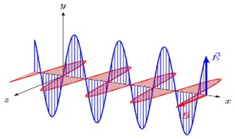
Bit Streams of Image Data

	Pixel 0	Pixel 2	P0 ... P3	Pixel 5	Pixel 7	
Data Lane 0	B2 .... B9	B2 .... B9	B0 B1...B0 B1	B2 .... B9	B2 .... B9	......

	Pixel 1	Pixel 3	Pixel 4	Pixel 6	P4 ... P7	
Data Lane 1	B2 .... B9	B2 .... B9	B2 .... B9	B2 .... B9	B0 B1...B0 B1	......

Optical **RAW Digital** **Electromagnetic**



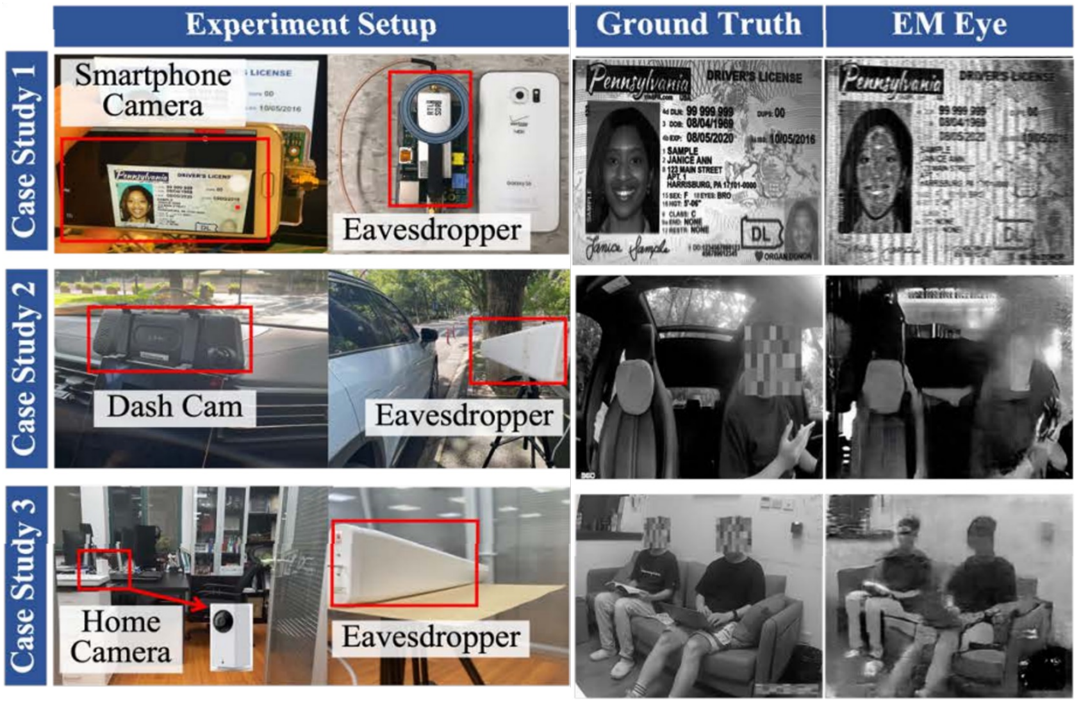


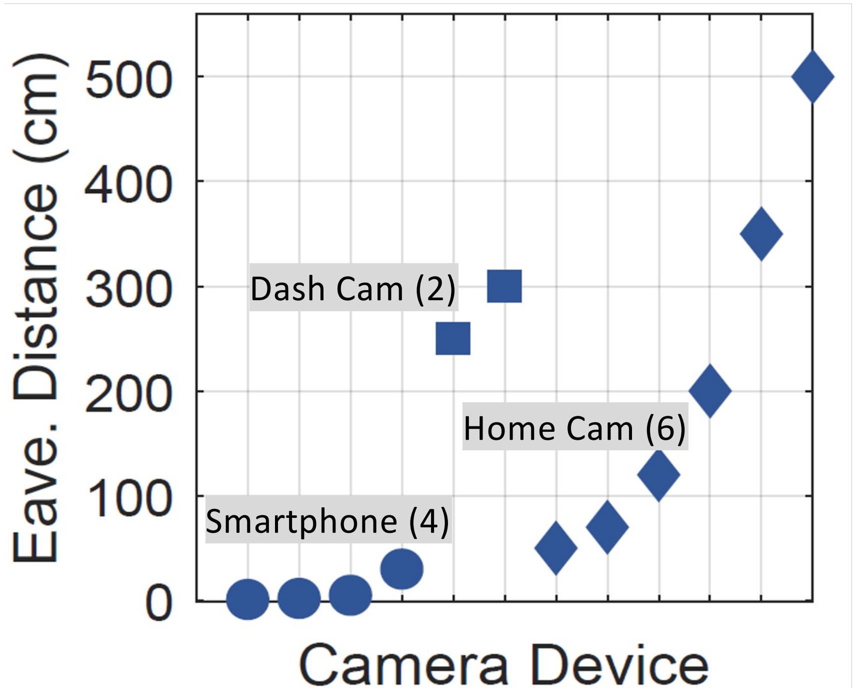
NSF UVa NU UCONN UCD UTD UC

CHEST
CENTER FOR HARDWARE AND EMBEDDED SYSTEMS SECURITY AND TRUST

EM-Eye: Limiting the Optical-Electromagnetic Side Channel Leakage of Smartphone Cameras

Fall 2023





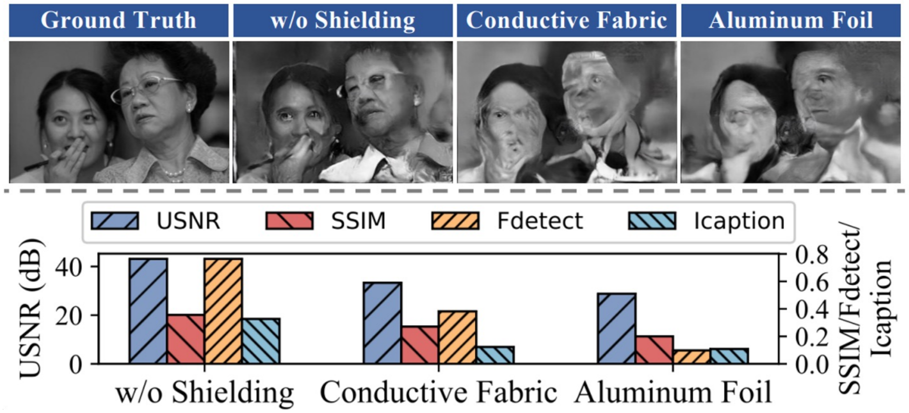
NSF
UVa
NU
UCONN
UCD
UTD
UC

CHEST
CENTER FOR
HARDWARE AND
EMBEDDED SYSTEMS
SECURITY AND TRUST

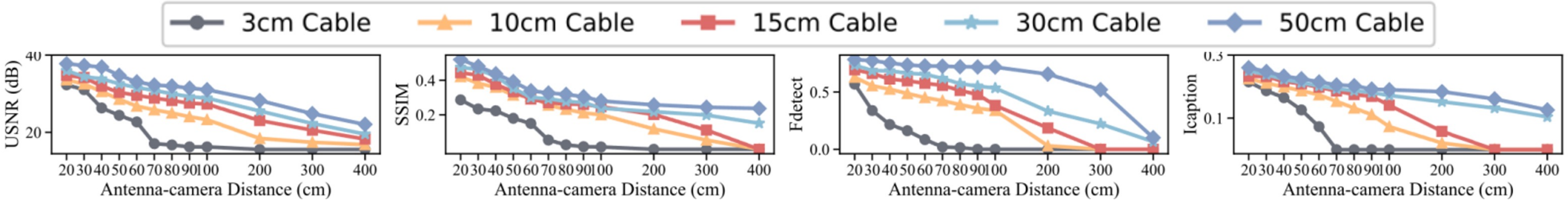
EM-Eye: Limiting the Optical-Electromagnetic Side Channel Leakage of Smartphone Cameras

Fall
2023

Impact of Shielding Transmission Cables



Impact of Transmission Cable Length and Distance



UVa
NU
UCONN
UCD
UTD
UC

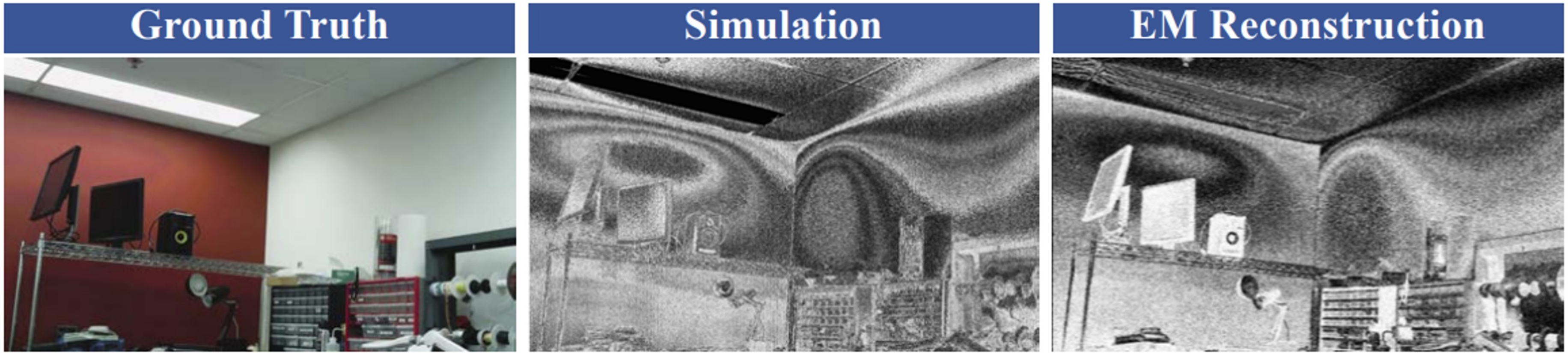
EM-Eye: Limiting the Optical-Electromagnetic Side Channel Leakage of Smartphone Cameras

Fall 2023

Prediction of EM Reconstruction

Camera RAW Ground-truth Capture

$$\boxed{I_{EM}^{[l,h]}} = \mathcal{R}_{base}\left\{ z + b_{clk} + \mathcal{F}_{filt}\left[l, h, \mathcal{F}_{data}\boxed{(I_{GT})}\right]\right\}$$



Ground Truth

Simulation

EM Reconstruction