CS7351 传感系统原理与设计
Principles and Design of Sensing Systems

Side-channel Sensing Attack

陈东尧
上海交通大学
chendy@sjtu.edu.cn
2025年秋季

Guest Lecture Schedule

- Dec. 18

Rui Xiao

Assistant Professor at SUFE

“ My research interests lie at the intersection of ***security*** and ***AI/mobile/wireless/sensing systems***, with a particular focus on the innovative analysis of physical context to enable trustworthy interaction with the physical world in Artificial Internet-of-Things (AIoT) and Cyber-Physical Systems (CPS).”

https://ruixiao24.github.io/

Sensing System Security

Threat Modeling (Security Reviews)

威胁模型分析 (安全检查)

- Assets（保护对象）: What are we trying to protect? How valuable are those assets?
- Adversaries（攻击者分析）: Who might try to attack, and why?
- Vulnerabilities（漏洞探索）: How might the system be weak?
- Threats（攻击行为）: What actions might an adversary take to exploit vulnerabilities?
- Risk（风险分析）: How important are assets? How likely is exploit?
- Possible Defenses（保护措施）

What is Security

- Common general security goals: “CIA”
  - Confidentiality -- 保密性
  - Integrity – 完整性（真实性）
  - Availability -- 可用性（可控性）

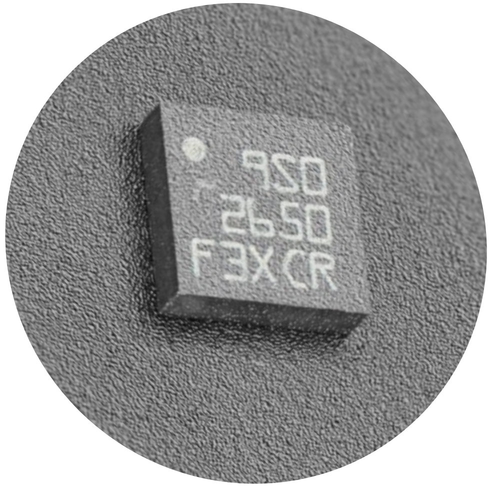
Attacker's Asymmetric Advantage

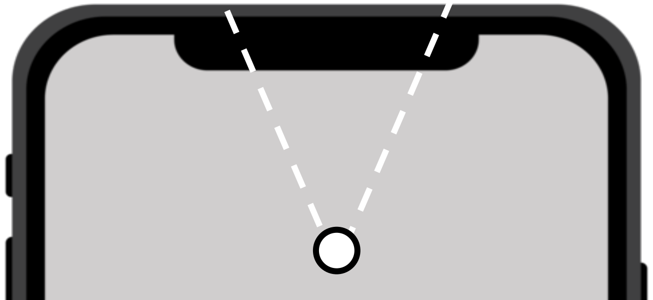
- Attacker only needs to win in one place
- Defender's response:
  - Defense in depth (层层嵌套的防御措施)
  - Think about the whole system

What is Side-channel Attack?

- In computer security, a **side-channel attack (旁路攻击)** is any attack based on extra information that can be gathered because of the **fundamental way a computer system is implemented**

Acoustic   Magnetic field   Acceleration   Angular speed





Four Exemplary Attacks and Defense

- [Attack-Acoustic] Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems
- [Attack-IMU] Guess Which Car Type I am Driving? Information Leak via Driving Apps
- [Attack-IMU] WALNUT: Waging Doubt on Integrity of MEMS Accelerometers with Acoustic Injection Attacks
- [Defense (Guest talk in Dec. 18)] MagTracer: Detecting GPU Cryptojacking Attacks via Magnetic Leakage Signals

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

Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin, Kevin Fu

USENIX 2020

Voice Controllable System (VCSs)

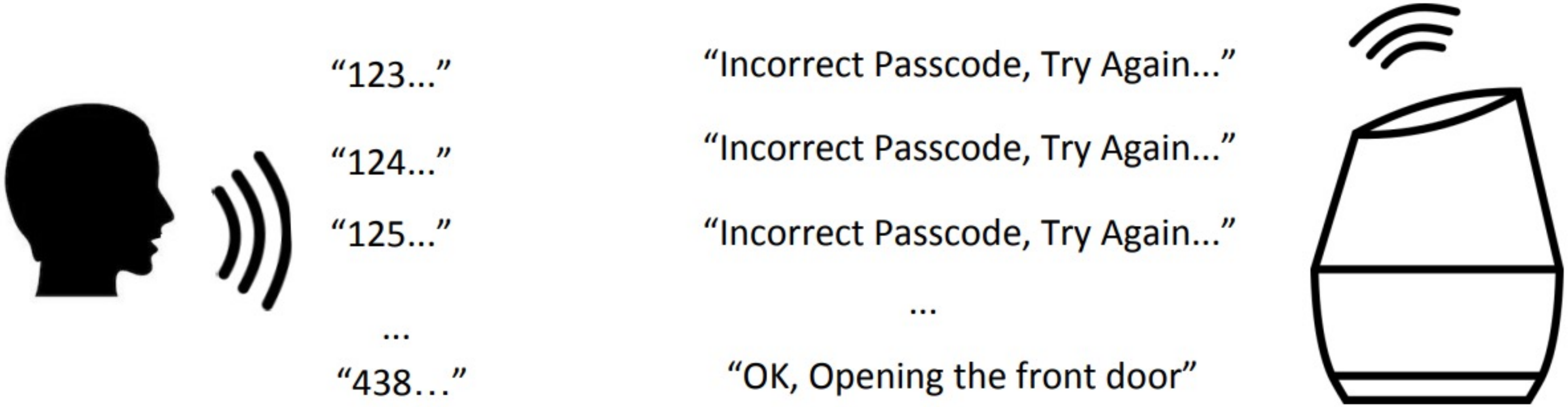
[Source: pandaily.com]

[Source: developers.google.com]

→ Signal processing → Speech recognition system → Command execution

Security Concerns

- Sacrifice of security to promote usability
- Interfacing with 3rd Party Software
- Blind trust in microphone readings



The Problem

- Assumption:

  Microphones capture acoustic signals

The Problem

- Reality:

  Microphones capture acoustic signals & LIGHT signals

The Problem

- Two questions:
  1. How does laser injection affect VCSs?
  2. How can we protect VCSs against laser injection

Highlights of this paper

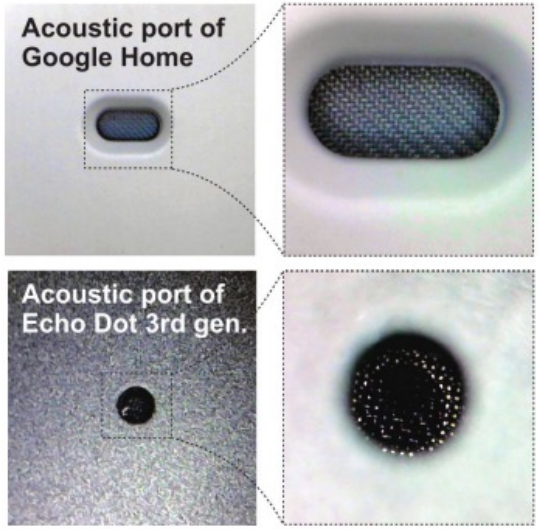
- Inject light commands via MEMS microphones
- Analyze limits of light-based VCS vulnerabilities
  - Success at 110 m with 5 mW laser pointer
  - Works through glass windows between buildings
- Demonstrate risks to smart speakers, phones, smart hones, and cars
- Suggest HW and SW countermeasures

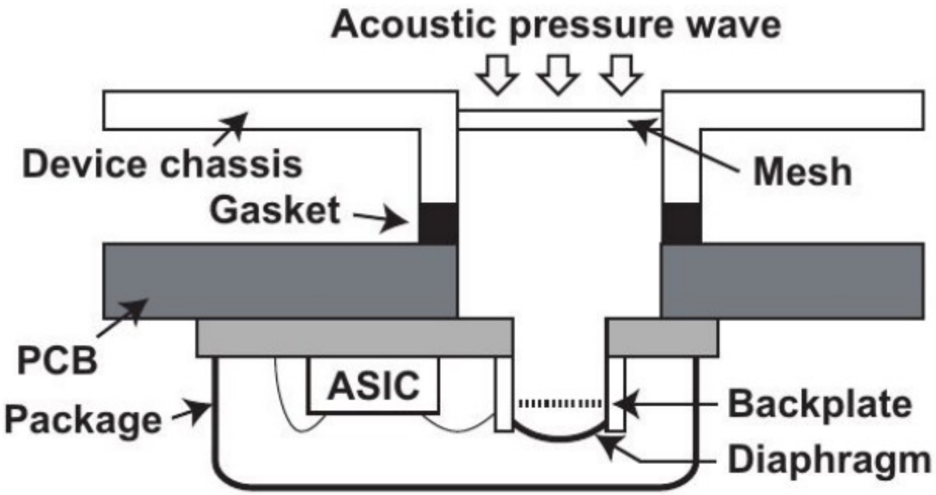
How it works?

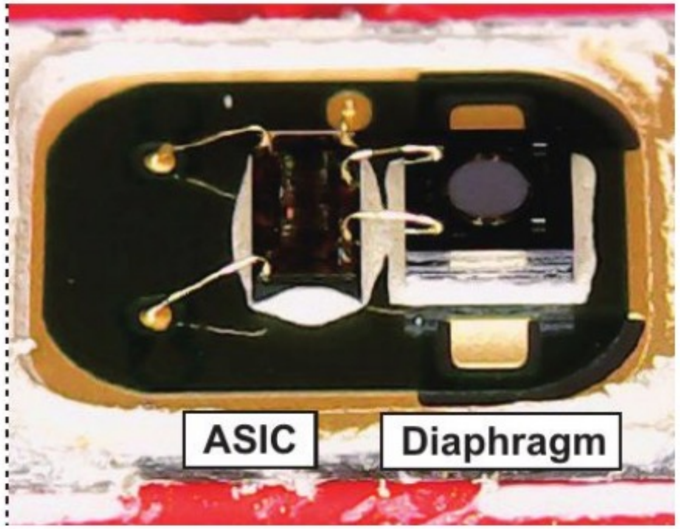
- Know the background of MEMS microphones

Background: MEMS Microphones

- Used in most Voice Controllable Systems
- The diaphragm and backplate (振动膜和背板) work as a capacitor
- When diaphragm moves, causes a change in capacitance
- The ASIC converts the capacitive change to voltage

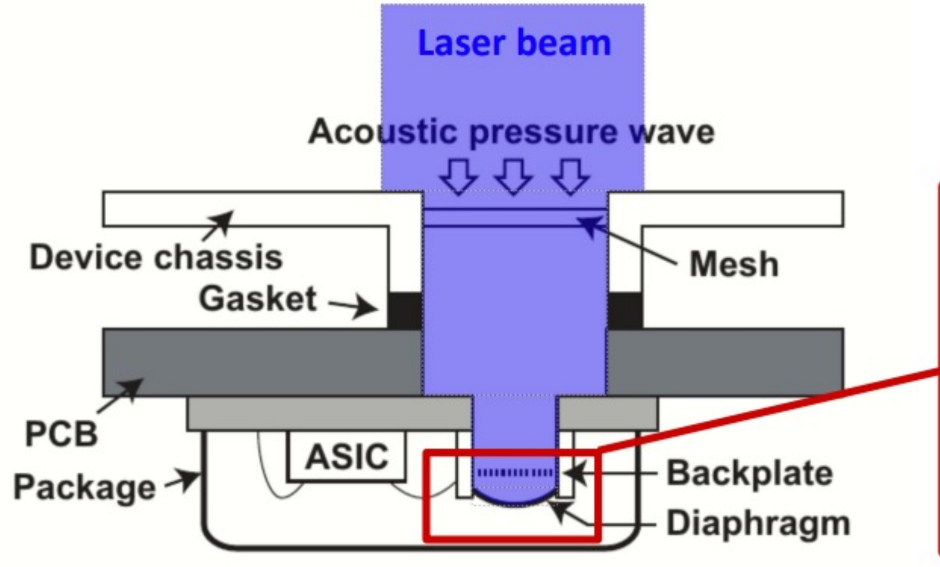


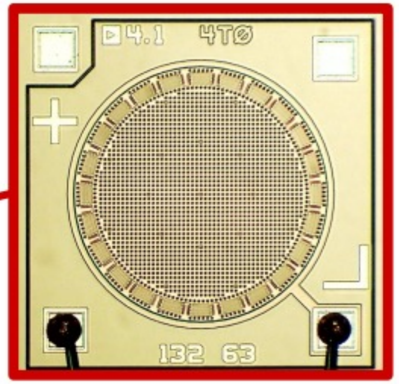




Background: MEMS Microphones

- MEMS microphones exhibit light sensitivity
- Output voltage affected by light irradiance (辐照度)
- Inject signal by modulating optical power



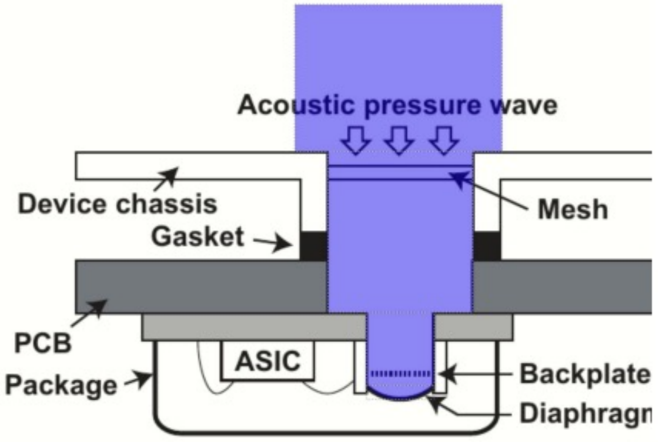


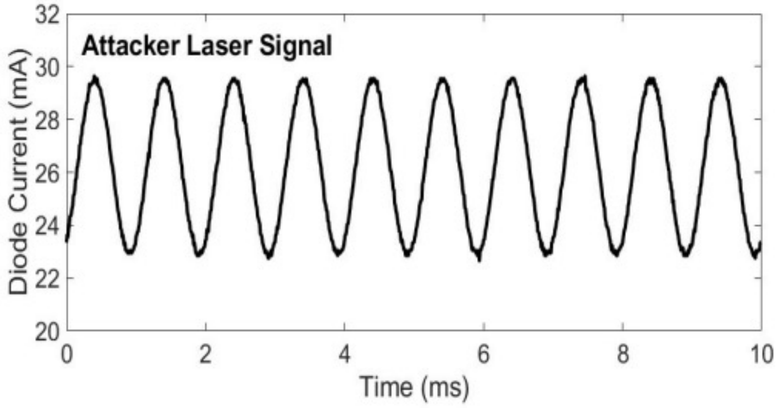
Irradiance:

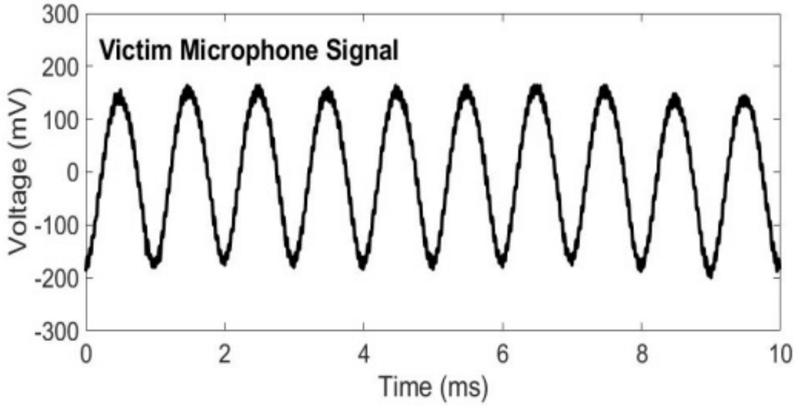
$$I = \frac{Optical\ Power\ (Watts)}{Beam\ Area\ (meters^2)}$$

Key Ideas

1. Amplitude modulated light generates a voltage signal on microphone output
2. Higher amplitude light == higher amplitude voltage
3. Very little distortion



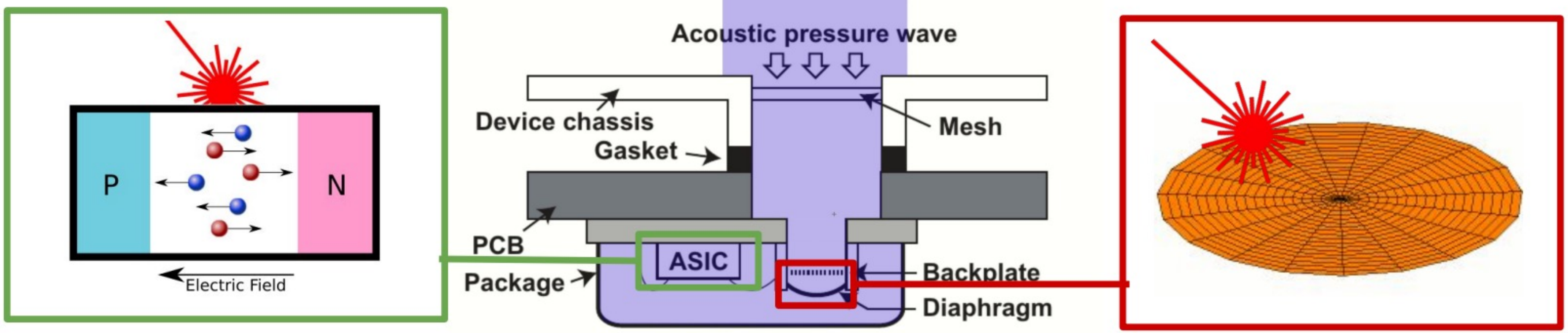




How is this Work?

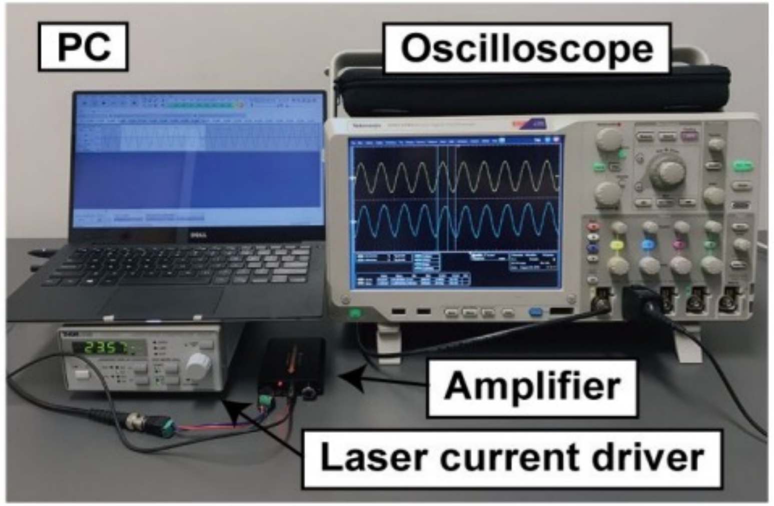
- Combination of two physical effects: photoelectric (光电效应) on ASIC (专用集成电路) and photoacoustic (光声效应) on diaphragm

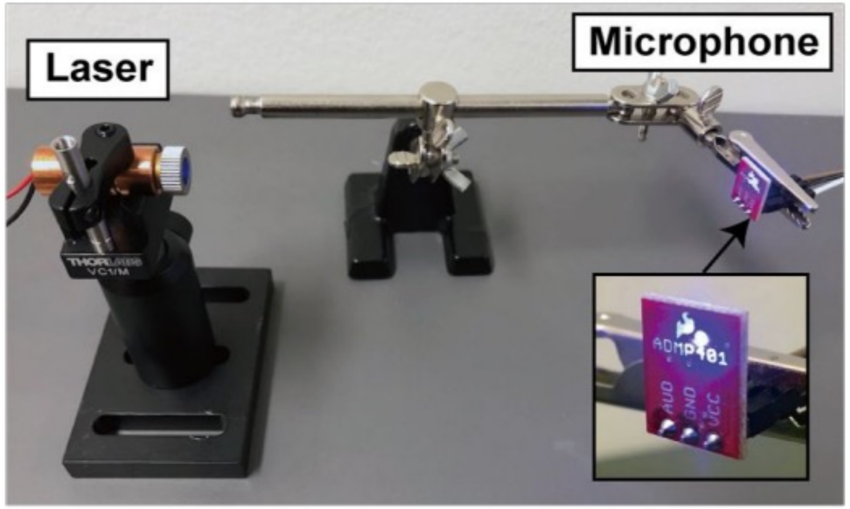
1. **Photoelectric** Effects on ASIC
2. **Photoacoustic** Effects on Diaphragm

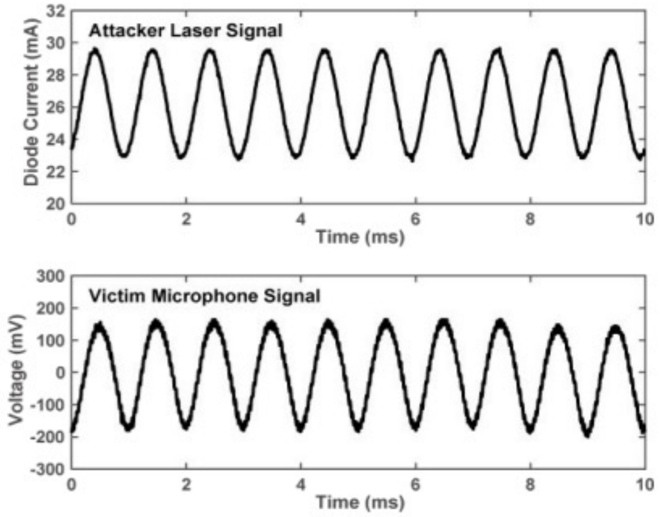


Signal Injection via Laser

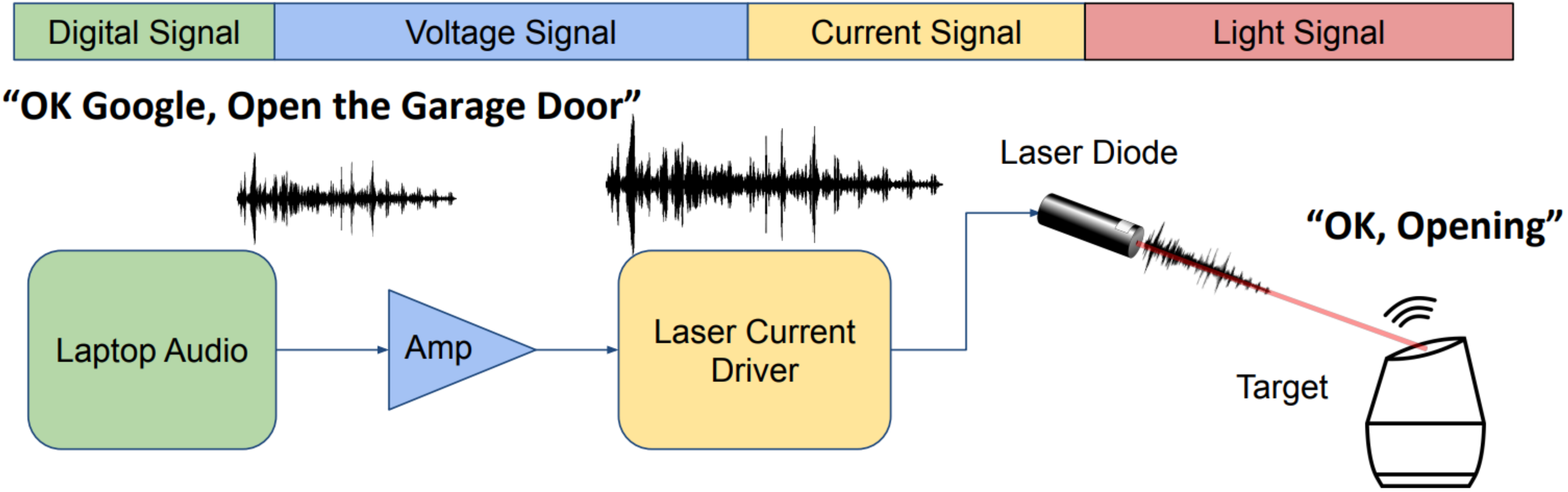
- Audio voltage signal from laptop
- Laser current driver converts to current signal – with DC Bias
- Laser output power is proportional to current





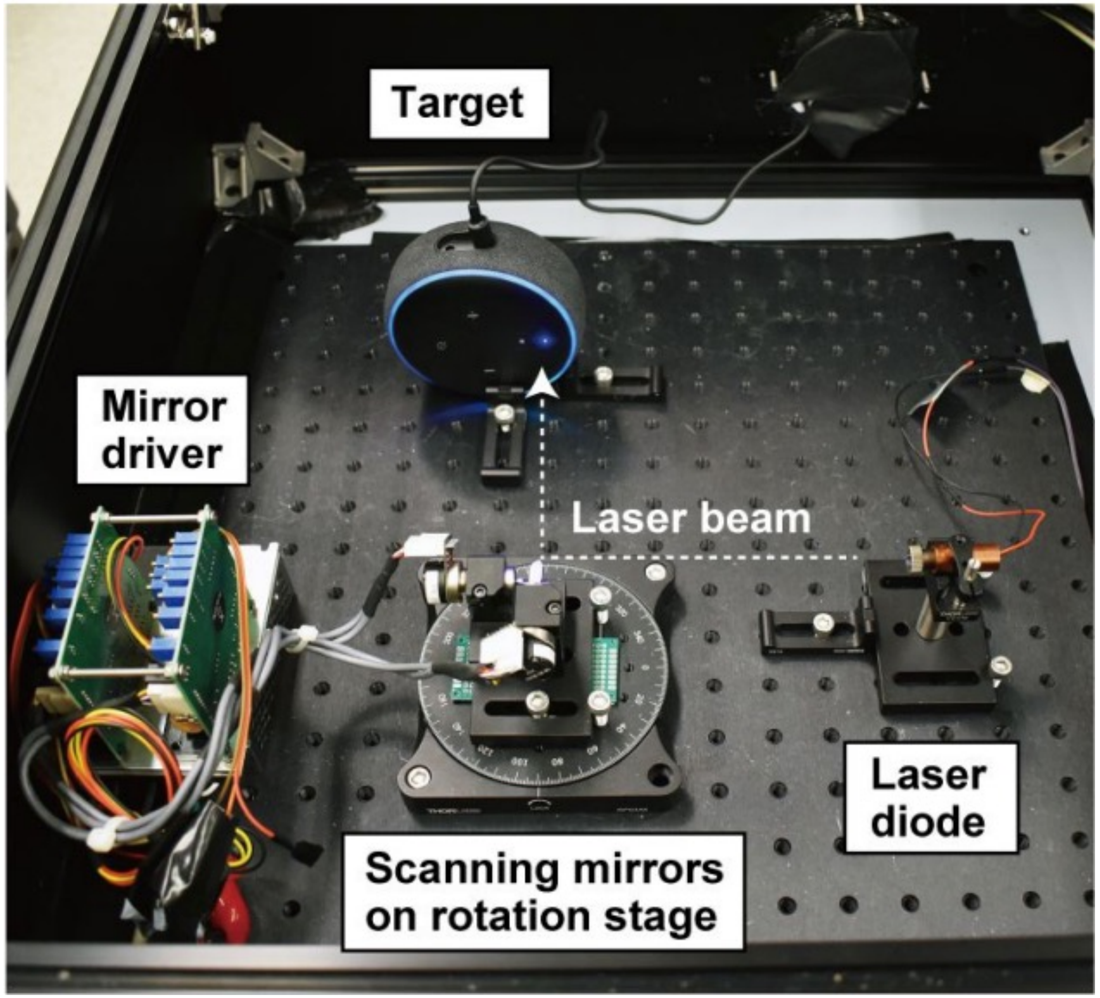


VCS Command Injection via Light



Measuring Vulnerability - Power

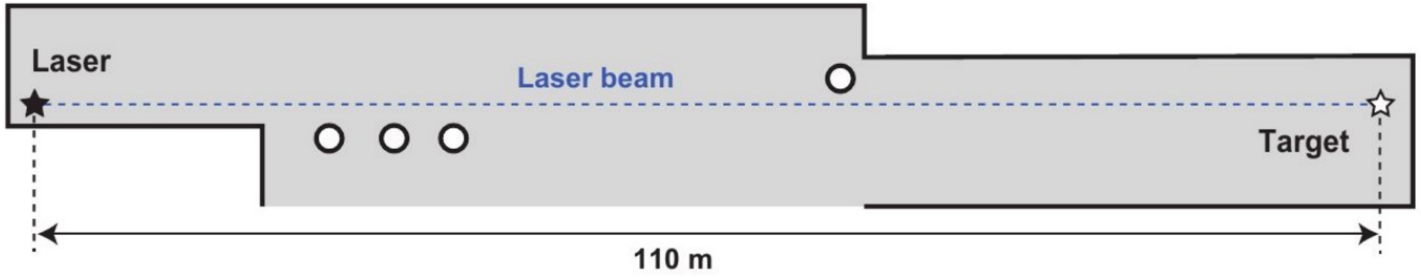
- Investigated 17 different devices
- Used scanning mirrors
- Measured minimum optical power to recognize commands



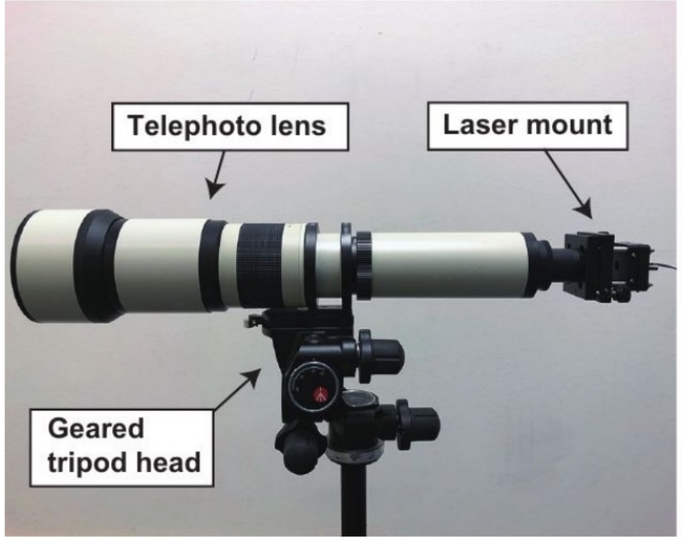
Measuring Vulnerability - Range

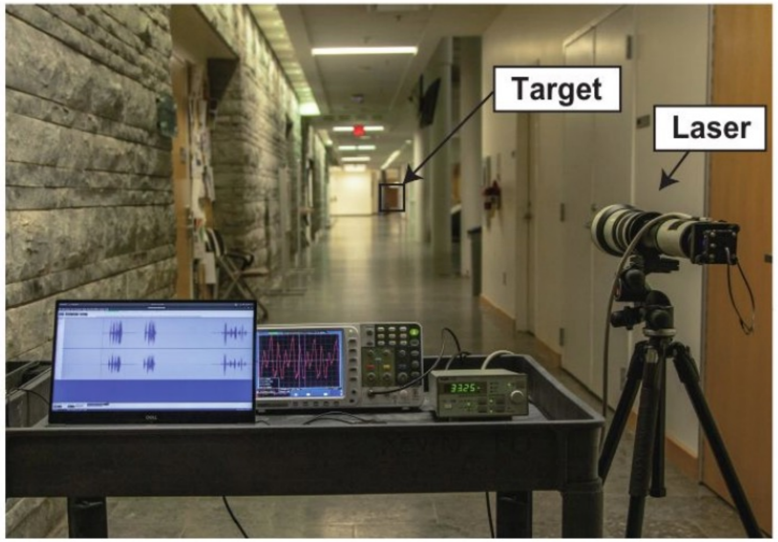
- Measuring the maximum range of the attack

$$\frac{\text{Optical Power (Watts)}}{\text{Beam Area (meters}^2\text{)}}$$



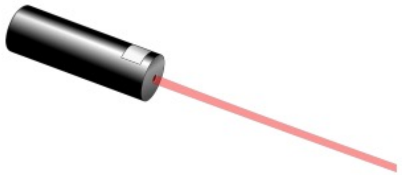
Optics!





Attack Results

Laser pointer power!



Device	Voice Recognition System	Minimun Laser Power at 30 cm [mW]	Max Distance at 60 mW [m]*	Max Distance at 5 mW [m]**
Google Home	Google Assistant	0.5	50+	110+
Google Home mini	Google Assistant	16	20	-
Google NEST Cam IQ	Google Assistant	9	50+	-
Echo Plus 1st Generation	Amazon Alexa	2.4	50+	110+
Echo Plus 2nd Generation	Amazon Alexa	2.9	50+	50
Echo	Amazon Alexa	25	50+	-
Echo Dot 2nd Generation	Amazon Alexa	7	50+	-
Echo Dot 3rd Generation	Amazon Alexa	9	50+	-
Echo Show 5	Amazon Alexa	17	50+	-
Echo Spot	Amazon Alexa	29	50+	-
Facebook Portal Mini	Alexa + Portal	18	5	-
Fire Cube TV	Amazon Alexa	13	20	-
EchoBee 4	Amazon Alexa	1.7	50+	70
iPhone XR	Siri	21	10	-
iPad 6th Gen	Siri	27	20	-
Samsung Galaxy S9	Google Assistant	60	5	-
Google Pixel 2	Google Assistant	46	5	-

5mW: 110+ meters

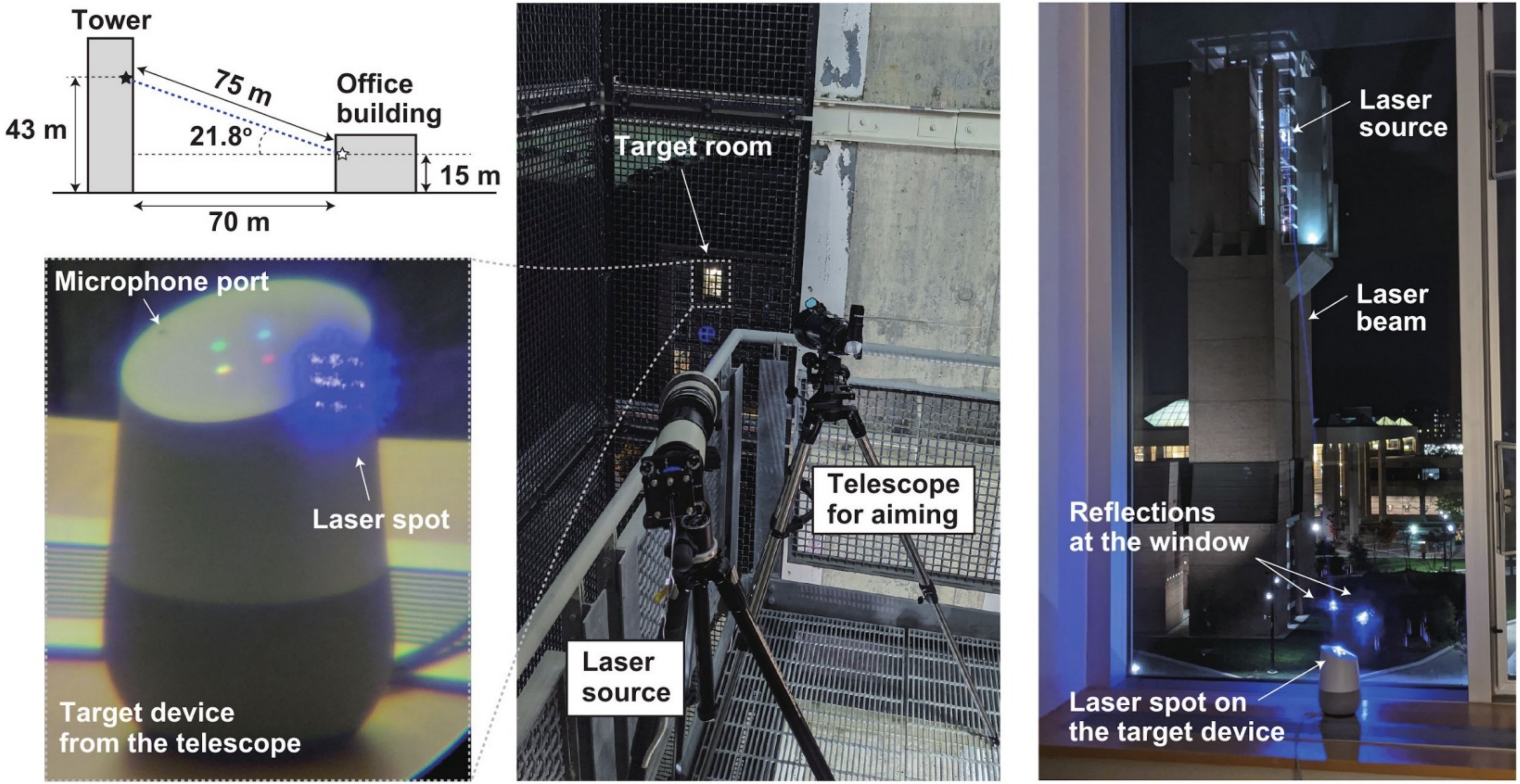
60mW: 50+ meters

Phones/Tablets

60mW: 5-20 meters

* Limited to a 50 m long corridor.
** Limited to a 110 m long corridor.

Cross-building Attack Scenario

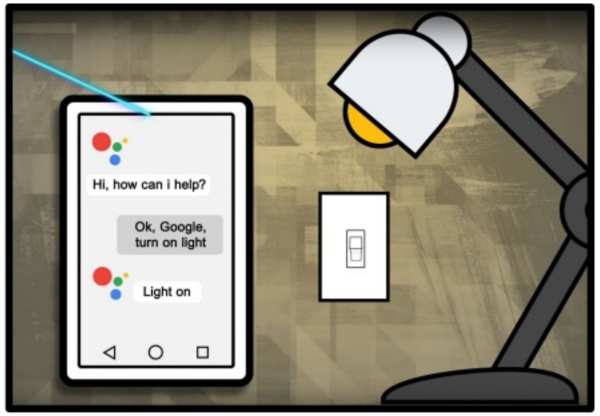


Attack Demo 1

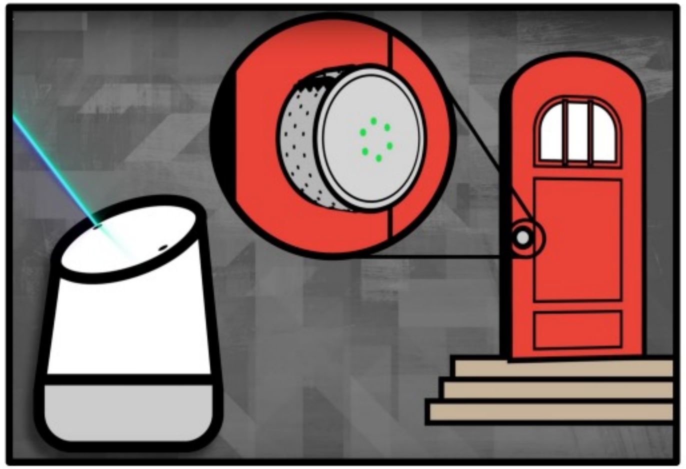
Attack Demo 2

Consequences

Turn on/off
Enable/Disable



Brute force unlock door

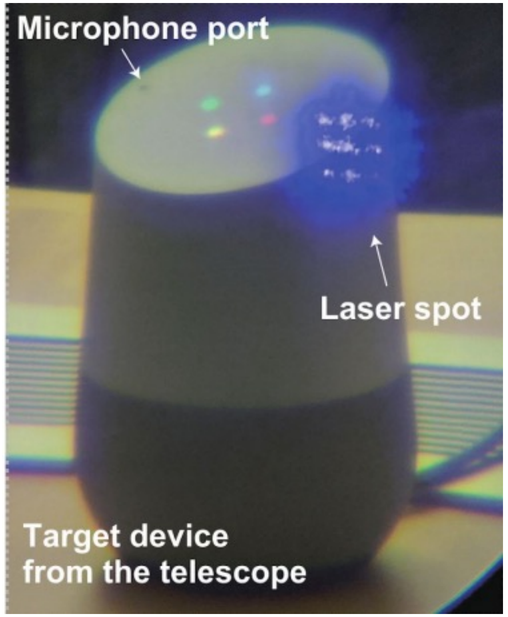


Unauthorized purchases

Open garage doors
Unlock car
Start engine

Limitations

- Dependence on Focusing, Aiming, Acoustic Noise, and Audio Quality
- Requires Line of Sight – Very little diffraction – Difficult to target top microphones
- Limited Feedback



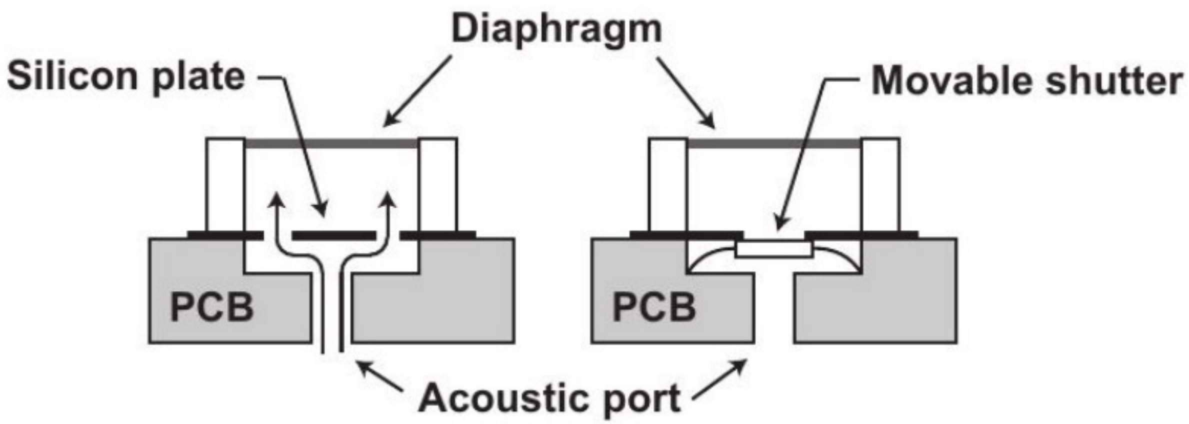
Countermeasures

- Software Approaches
  - Stronger Authentication
  - Liveness Tests
  - Sensor Fusion: Compare Multiple Microphones
- Hardware Approaches
  - Light-Blocking **Covers**
    - On the VCS (fabric)
    - Inside the MEMS Mic

"Please give the passcode to unlock the garage door"

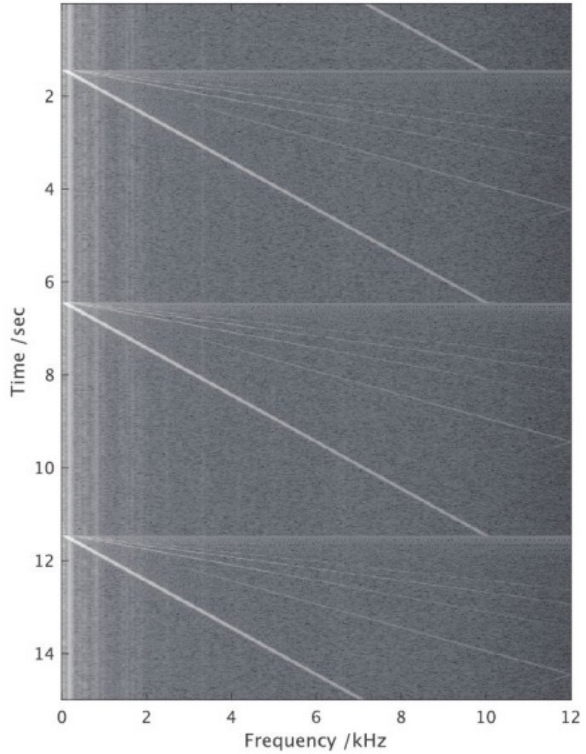
...

"Please confirm by repeating the second digit of your passcode"



Future Directions

- Deep exploration of physical causality
  - Lead to future defenses
- Other Vulnerabilities:
  - Non-MEMs Microphones
  - Other Motion Sensors



What we've learnt

- Lasers can inject commands into VCSs
- Physical vulnerability in MEMS microphones
- Highlights security flaws in VCSs
- Blind trust of any input often points to vulnerabilities

Guess Which Car Type I am Driving? Information Leak via Driving Apps

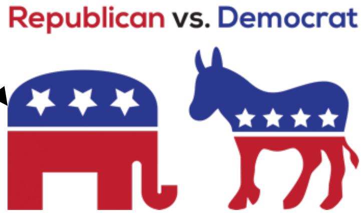
Dongyao Chen, Mert D. Pesé, and Kang G. Shin, the Inaugural Symposium on Vehicle Security & Privacy (VehicleSec), 2023

Vehicle Type can link to Sensitive Info

Vehicle type information
(i.e., truck vs compact)

Targeted advertising

Demographic information



Politic tendency

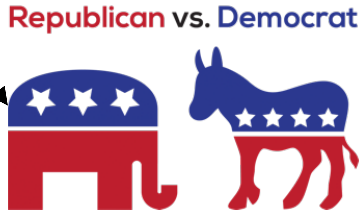
Sensitive information

Vehicle Type can link to Sensitive Info

Vehicle type information
(i.e., truck vs compact)

Targeted advertising

Demographic information



Politic tendency

Sensitive information

FORBES > LIFESTYLE > CARS & BIKES

Here's What Really 'Drives' Democrats And Republicans

Jim Gorzelany Senior Contributor
I write about how to maximize your automotive investment and more.
Follow

Nov 2, 2016, 01:48pm EDT

Unusually Popular Cars in Republican and Democratic Districts

Based On % of Cars Serviced by YourMechanic

Red Cars

Rank	Car Make and Model
1	Dodge Ram 1500
2	GMC Sierra 1500
3	Ford F-150
4	Chevrolet Silverado 1500
5	Chevrolet C1500
6	Toyota Tundra
7	Chevrolet Suburban 1500
8	Kia Sorento
9	Dodge Dakota
10	Chevrolet Tahoe

Blue Cars

Rank	Car Make and Model
1	Toyota Prius
2	Audi A4
3	BMW 328i
4	BMW 325i
5	Acura TSX
6	Mini Cooper
7	Saab 3-Sep
8	Toyota Matrix
9	Honda Fit
10	Toyota Yaris

JUNE 7, 2006

Gallup Poll Analysis: Political Correlates of Car Choice

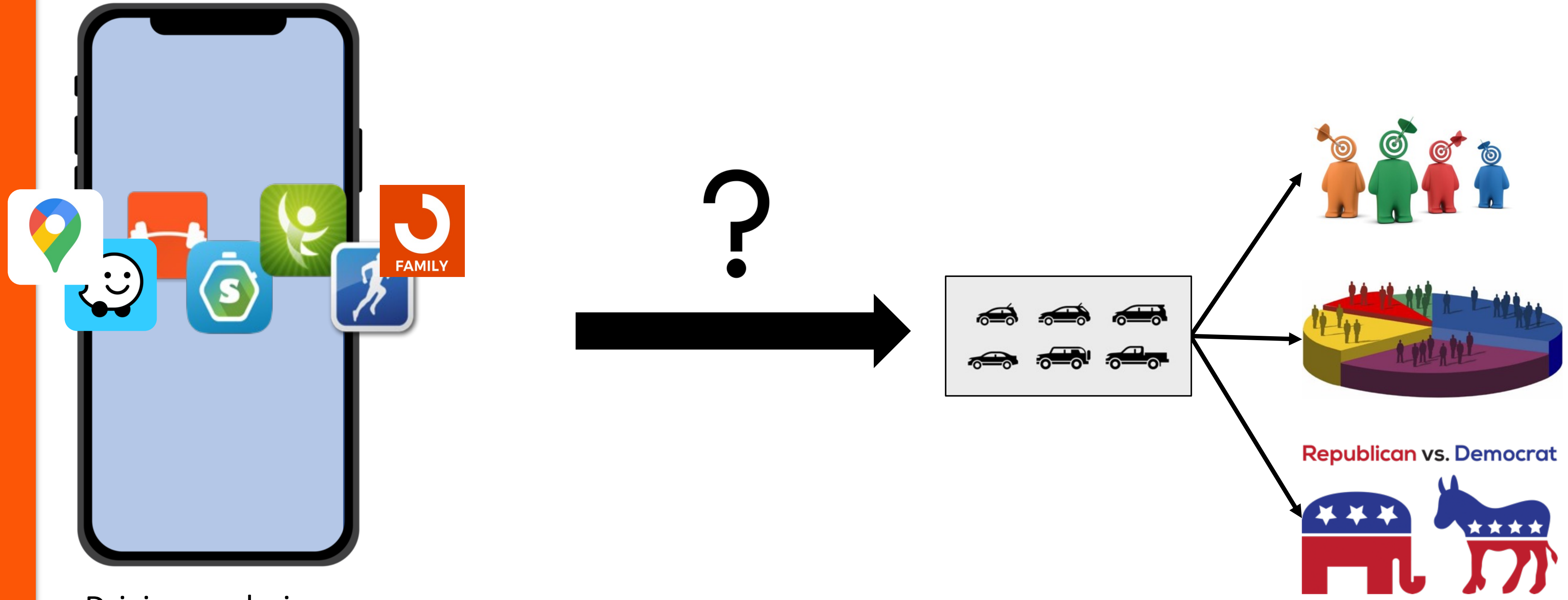
Americans' choice of car related to partisanship and ideology

BY FRANK NEWPORT

GALLUP NEWS SERVICE

PRINCETON, NJ -- Social scientists -- and automobile marketers -- have long noted that the choice of a car to drive is based on more than just price and functionality. Car brands and styles are associated with specific identities, positioning, and mental images, and one's choice of a car can be a significant statement about his or her desired presentation of self. A recent Gallup Panel Poll found that 93% of Americans say they personally drive a car or other vehicle. These drivers were asked to name the brand of car they personally drive most often.

Can our Smartphone Stealthily Leak this Info?



Driving analysis app,
motion tracking app

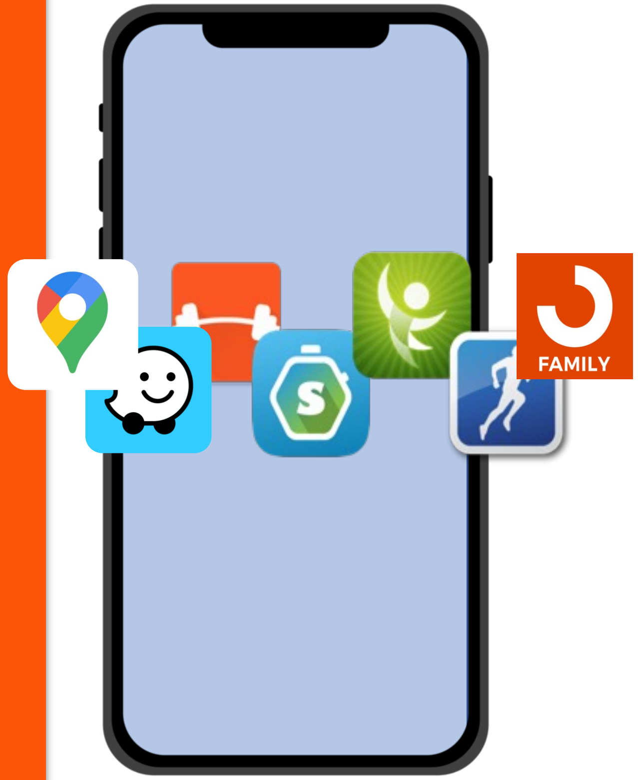
Targeted advertising

Demographic information

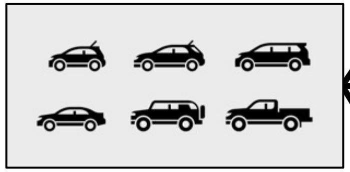
Politic tendency

Sensitive information

Can our Smartphone Stealthily Leak this Info?

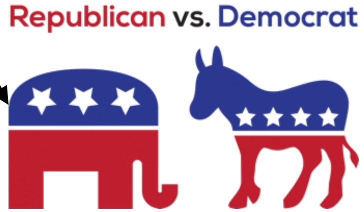


Characterizing
Vibration Patterns for
differentiating cars



Targeted
advertising

Demographic
information



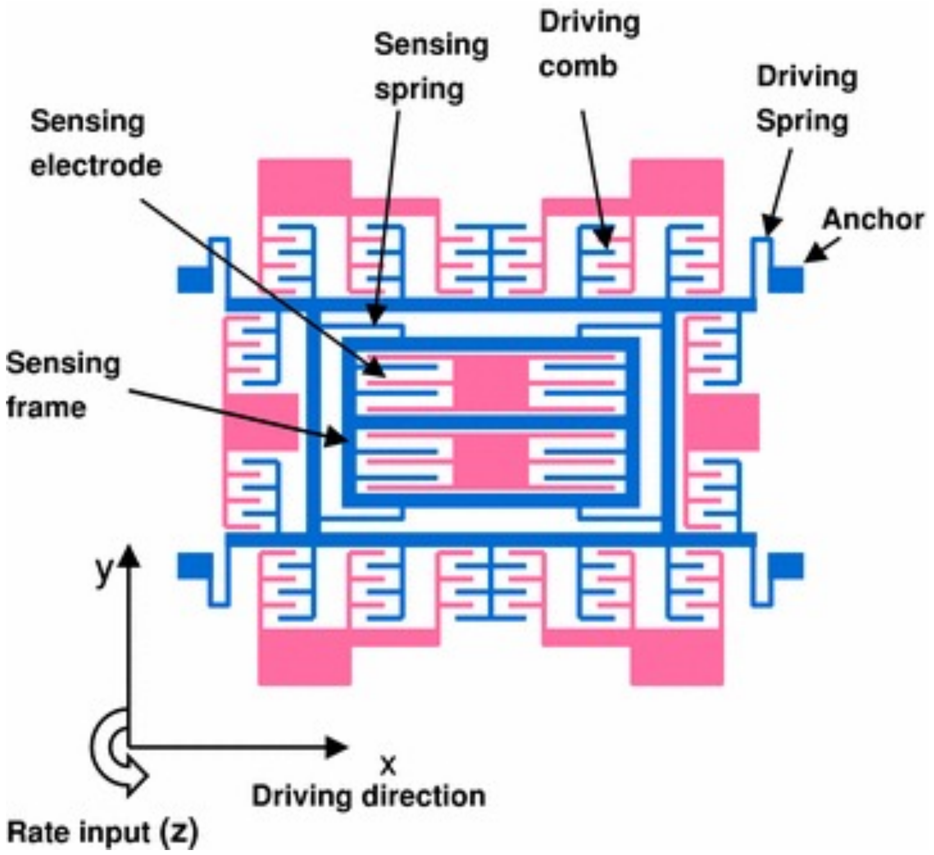
Politic
tendency

Motion Sensor
They are pivotal but requires zero-permission!

Sensitive information

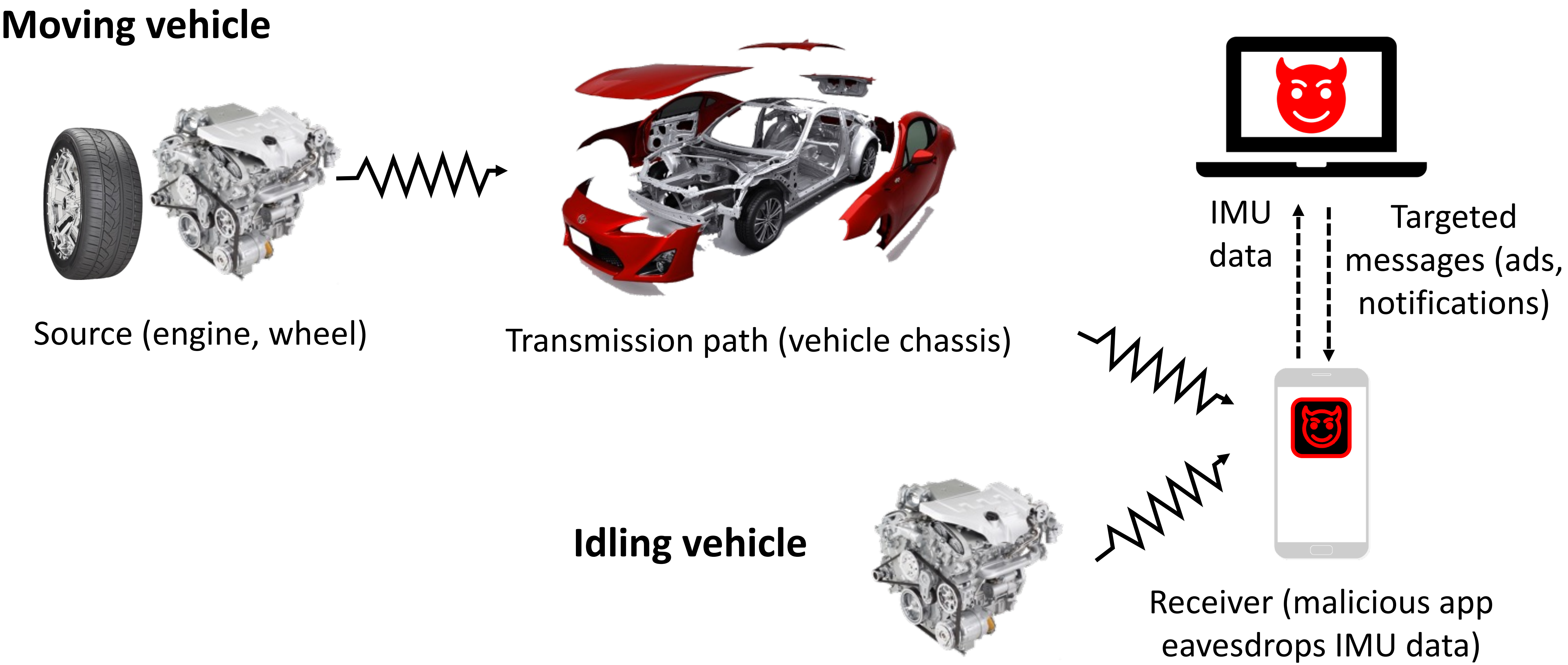
Sensing Vibrations from Motion Sensors (IMU)

- The embedded oscillator of accelerometer and gyroscopes can be used for sampling high-speed vibrations



[Michalevsky, et al, 2014]

Threat Model



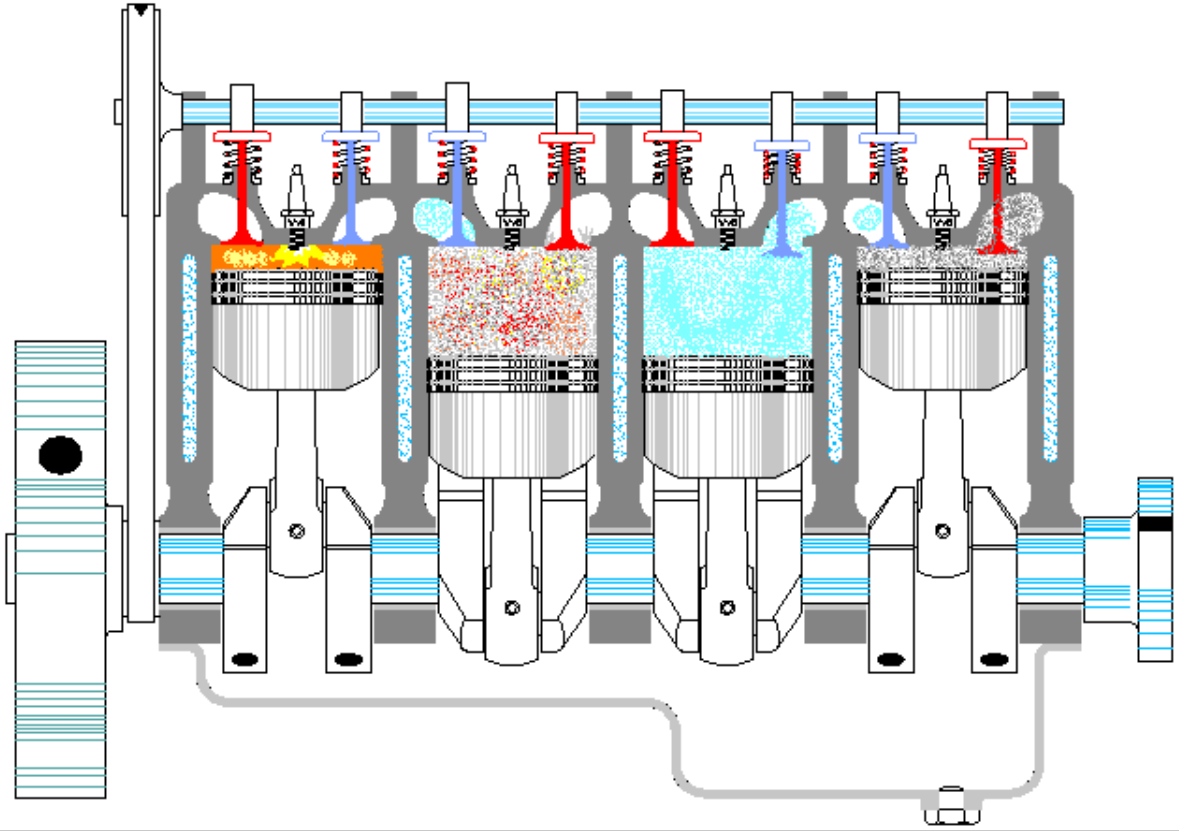
Inferring Idling and Moving Vehicle’s Type

- Vibration pattern varies depends on whether the vehicle is moving

Idling vehicle

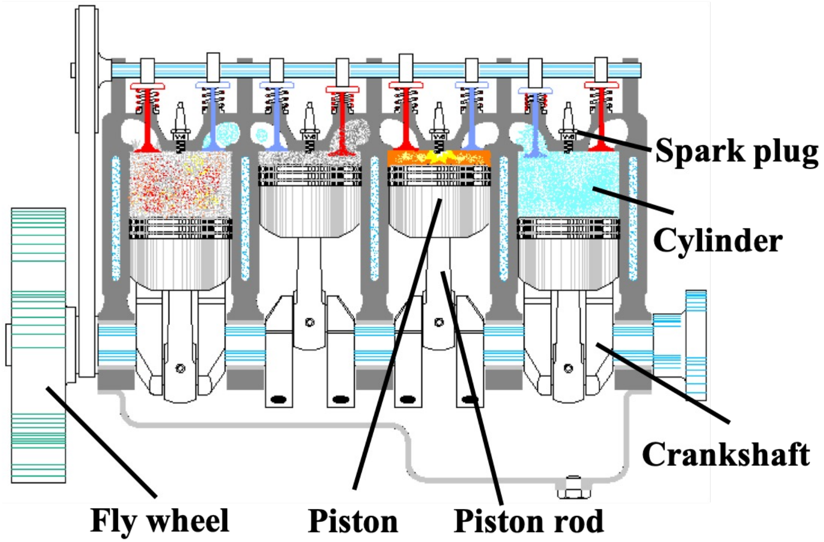
Moving vehicle

Inferring Idling Vehicle Type



- Engine is the dominant source of vibration when car is idling
- Engine is a representative factor for car types
  - Hybrid: 3~4-cylinder
  - Pickup truck: 6~8-cylinder

Inferring Idling Vehicle Type



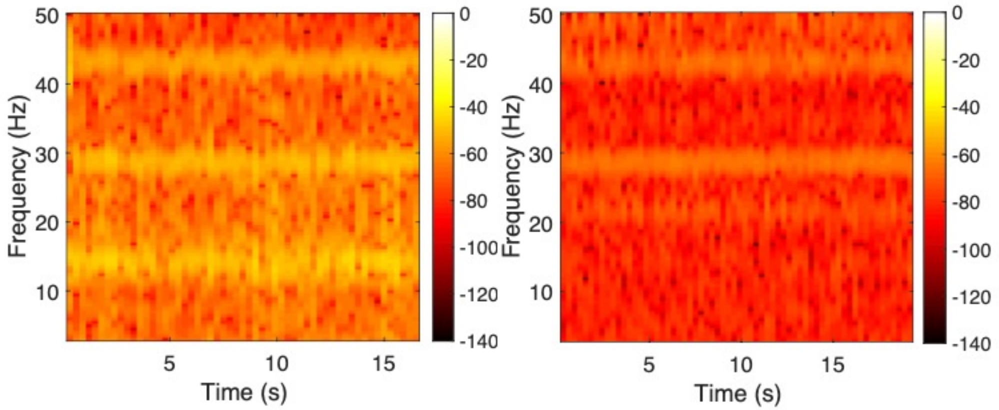
1. Combustion frequency: $f_C = \frac{RPM}{60}\frac{C}{2}$

A typical engine rev-range is from an idle of between 500 and 1000rpm, and a maximum speed of about 6000 to 7000rpm.

Do we have sufficient sampling range?

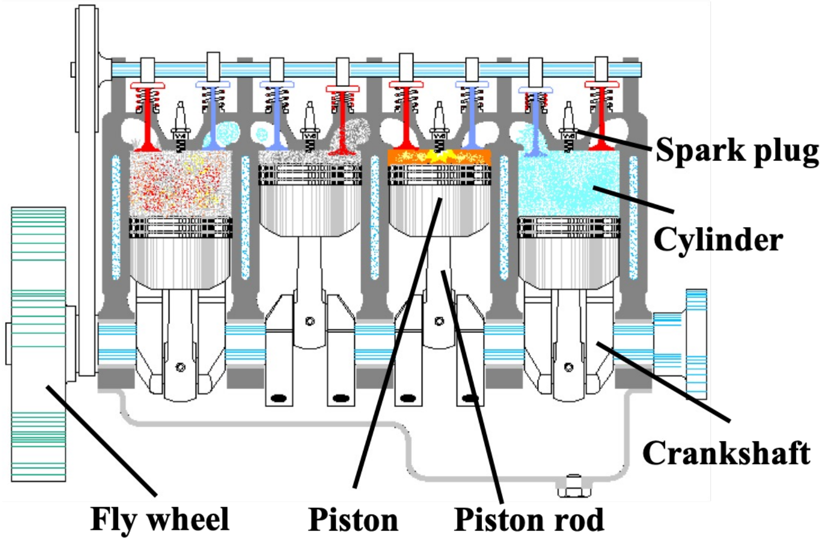
Real-world Data Traces

The idling engine's spectrogram obtained by gyroscope sensor sampling at 100 Hz with the device residing at different locations.



(a) On the engine (b) Inside the car (cup holder)

Inferring Idling Vehicle Type



1. Combustion frequency: $f_C = \frac{RPM}{60}\frac{C}{2}$

2. N-th order overtones: $f_{C,N} = N f_C$

3. **Aliased frequency** that can be detected by motion sensors

$$f^a_{C,N} = \left| f_{C,N} - K f_s \right|$$

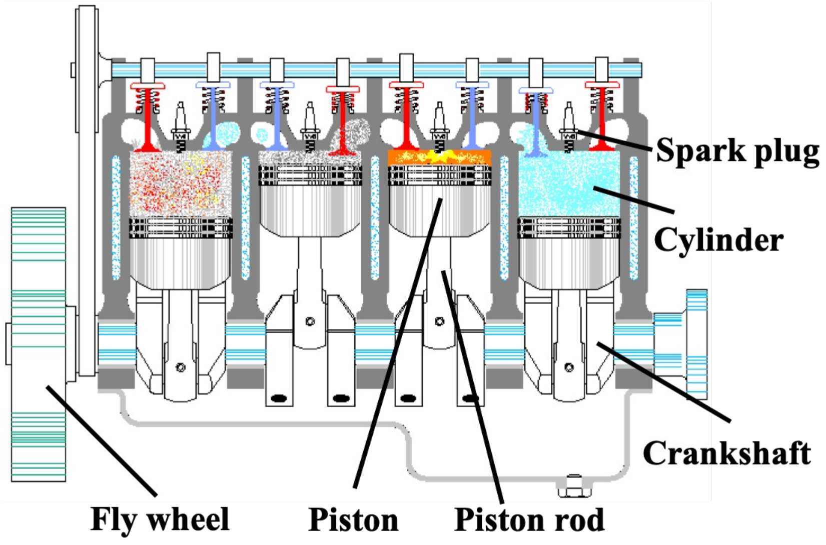
4. The detectable engine overtone at specific engine RPM is:

$$f^a_{C,N}(RPM) = \left| N \frac{RPM}{60}\frac{C}{2} - K f_s \right|$$

$$0 \le f^a_{C,N} \le {f_s}/{2} \quad K \in \mathbb{Z}$$

The first 2 order overtones are the strongest

Inferring Idling Vehicle Type

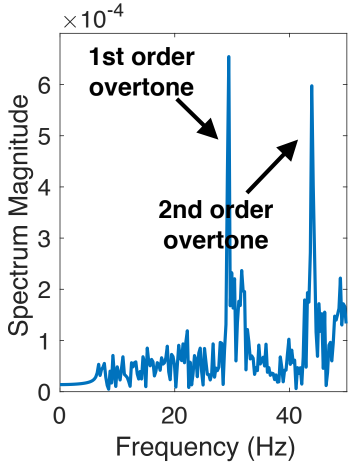


Overtone order / # cylinder	N=1	N=2	N=3
4	[20 33.3]	[33.3, 50]	[0, 40]
6	[30, 50]	[0, 40]	[0, 50]
8	[33.3, 50]	[0, 33.3]	[0, 50]

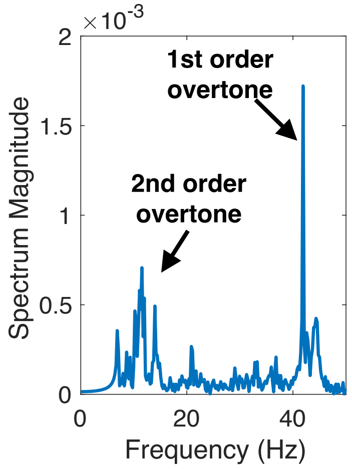
The detectable engine overtone at specific engine RPM:

$$f_{C,N}^{a}(RPM) = \left| N \frac{RPM}{60} \frac{C}{2} - K f_s \right|$$

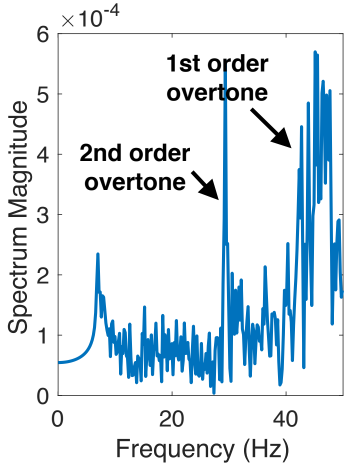
$$0 \leq f_{C,N}^{a} \leq {f_s}/{2} \quad K \in \mathbb{Z}$$



4-cylinder



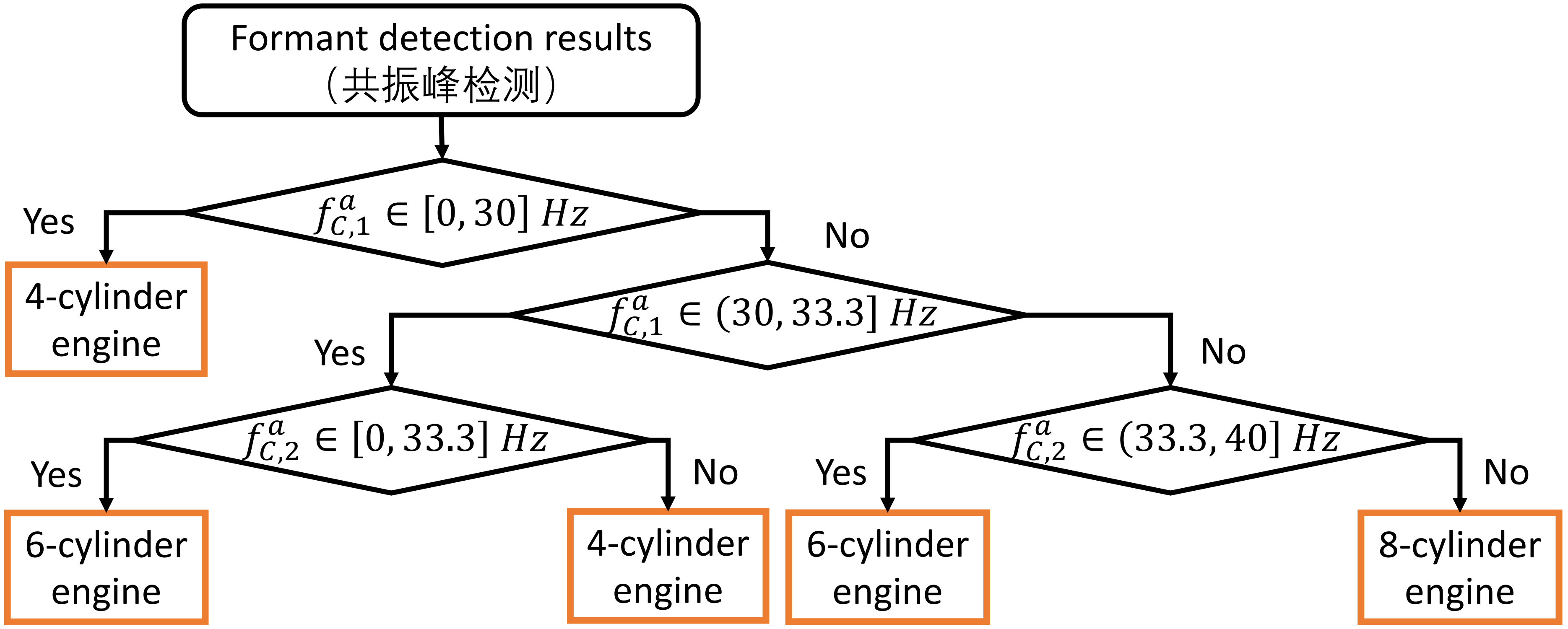
6-cylinder



8-cylinder

Inferring Idling Vehicle Type

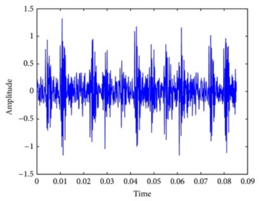
A decision tree can be constructed based on the distribution of $f_{C,N}^{a}$



Inferring Moving Vehicle Type

Vibration source
(Engine)

Filters (vehicle frame, chassis,
suspension etc.)

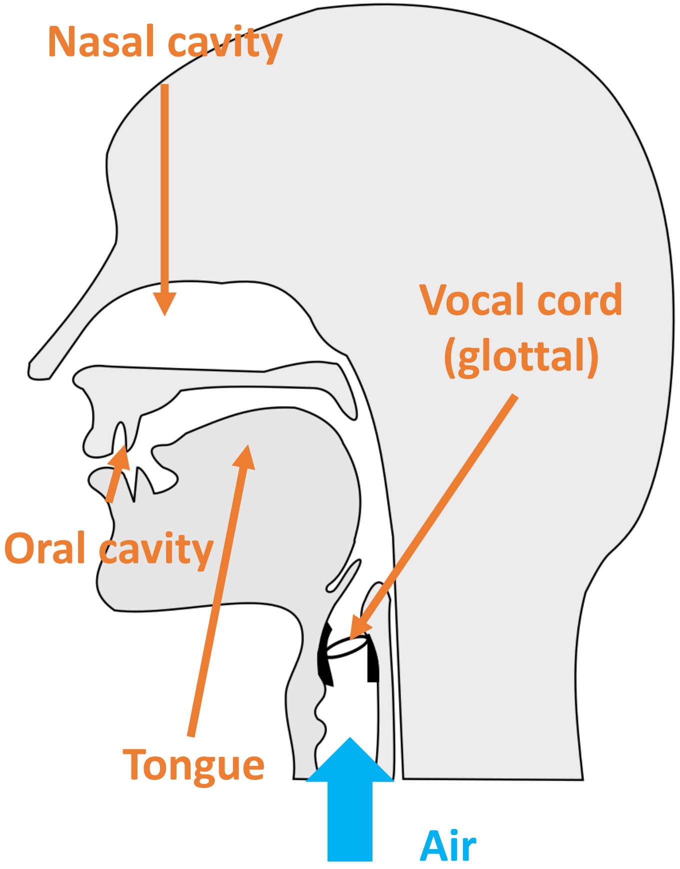


Vibration
signal

Inferring Moving Vehicle Type

- Insights from the pipeline of speaker recognition

Human vocal system → Source filter model → Characterizing speaker based the feature of the transition function



Final sound

Filter

Transfer function: vocal tract, nasal cavity, lips, etc.

Source

Glottal excitement

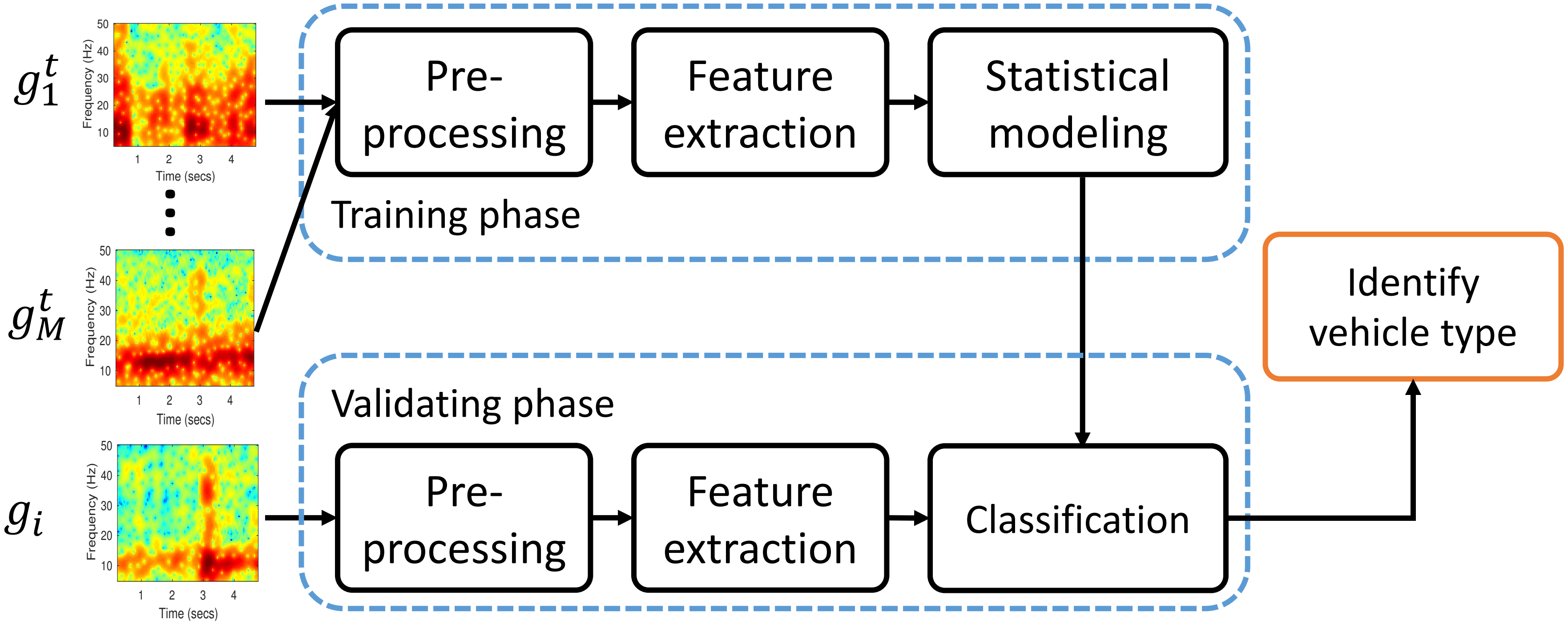
$$x(t) * \boxed{h(t)} = y(t)$$

Implication

Inferring Moving Vehicle Type

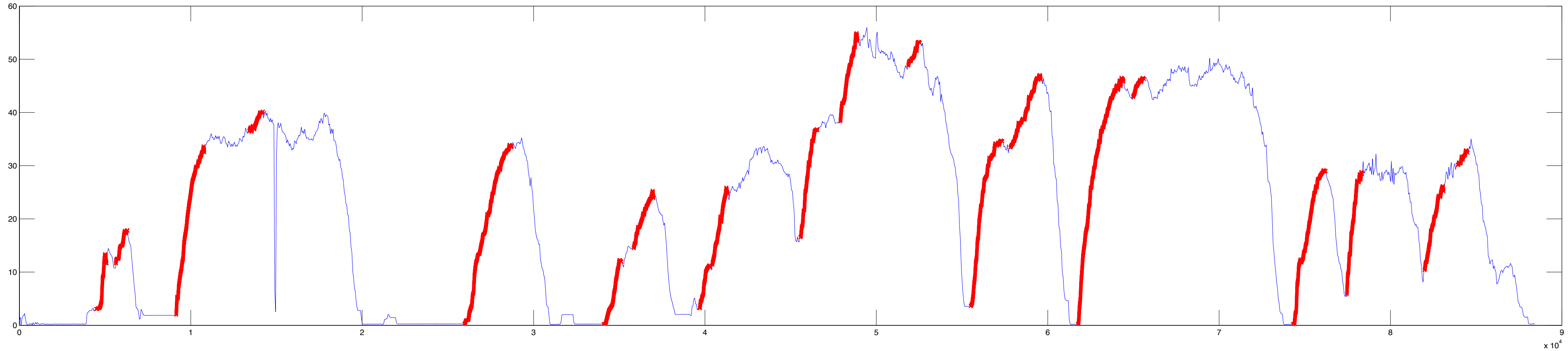
- Insights from the pipeline of speaker recognition

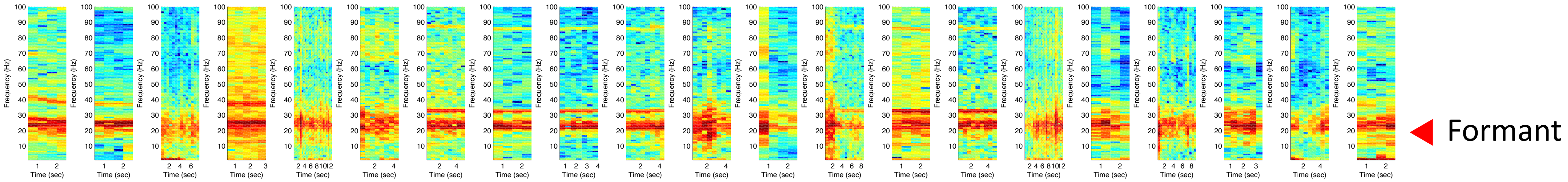
Raw vibration data → Source filter model → Characterizing the car type



Vibration Pattern Captured by IMU

- Data collected from Ford Mustang



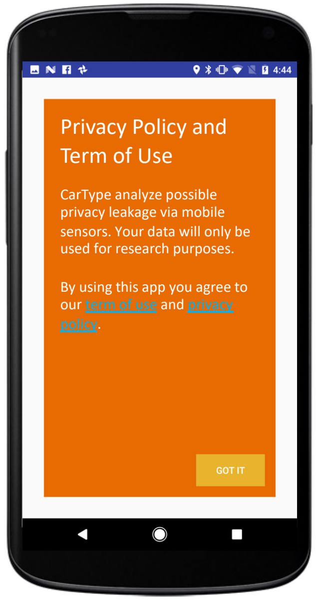


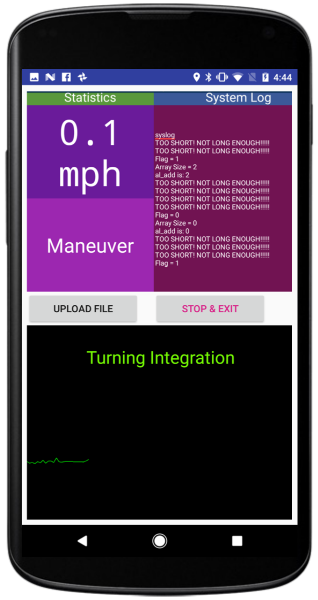
Evaluation Setting

Cases	Vehicle type	Experimental vehicle(s)
C-1	Compact	Toyota Corolla 2009; Hyundai Elantra 2008; Nissan Sentra 2018
C-2	Mid-size	Honda Accord 2006, 2013; Toyota Camry 2010, Toyota Camry 2010, 2011; Ford Fusion 2018; Mecedes Benz C180 2016
C-3	SUV	Honda CRV 2013, 2014; Jeep Campus 2014; Ford Explorer 2011, 2016
C-4	Pickup truck	GMC Sierra 2015, 2016; Ford F-150 2017

- For each vehicle type we extract the gyroscope sensor data from idling and moving stages

Evaluation Setting





- For each vehicle type we extract the gyroscope sensor data from idling and moving stages

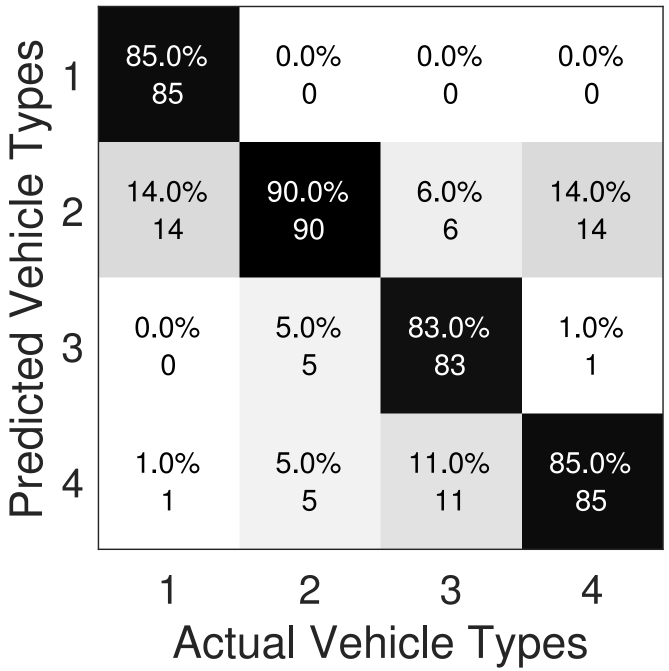
Evaluation

- Identifying idling vehicles' type

# cylinder	Precision	Recall	F-1
4	0.82	0.82	0.82
6	0.67	0.50	0.57
8	0.67	1.00	0.80

Evaluation

- Identifying moving vehicles’ type



The overall accuracy is **85.75%**

VeFi-Conclusion

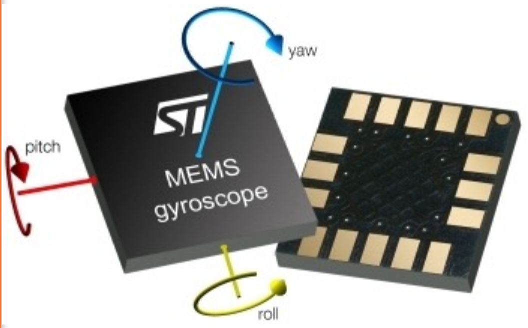
- VeFi explores the vibration pattern for differentiating vehicle types
- The high-frequency vibration pattern can characterize:
  - Engine type for idling cars
  - Car body type for moving cars

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

Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, Kevin Fu

IEEE European Symposium on Security & Privacy. 2017

MEMS IMUs are Essential

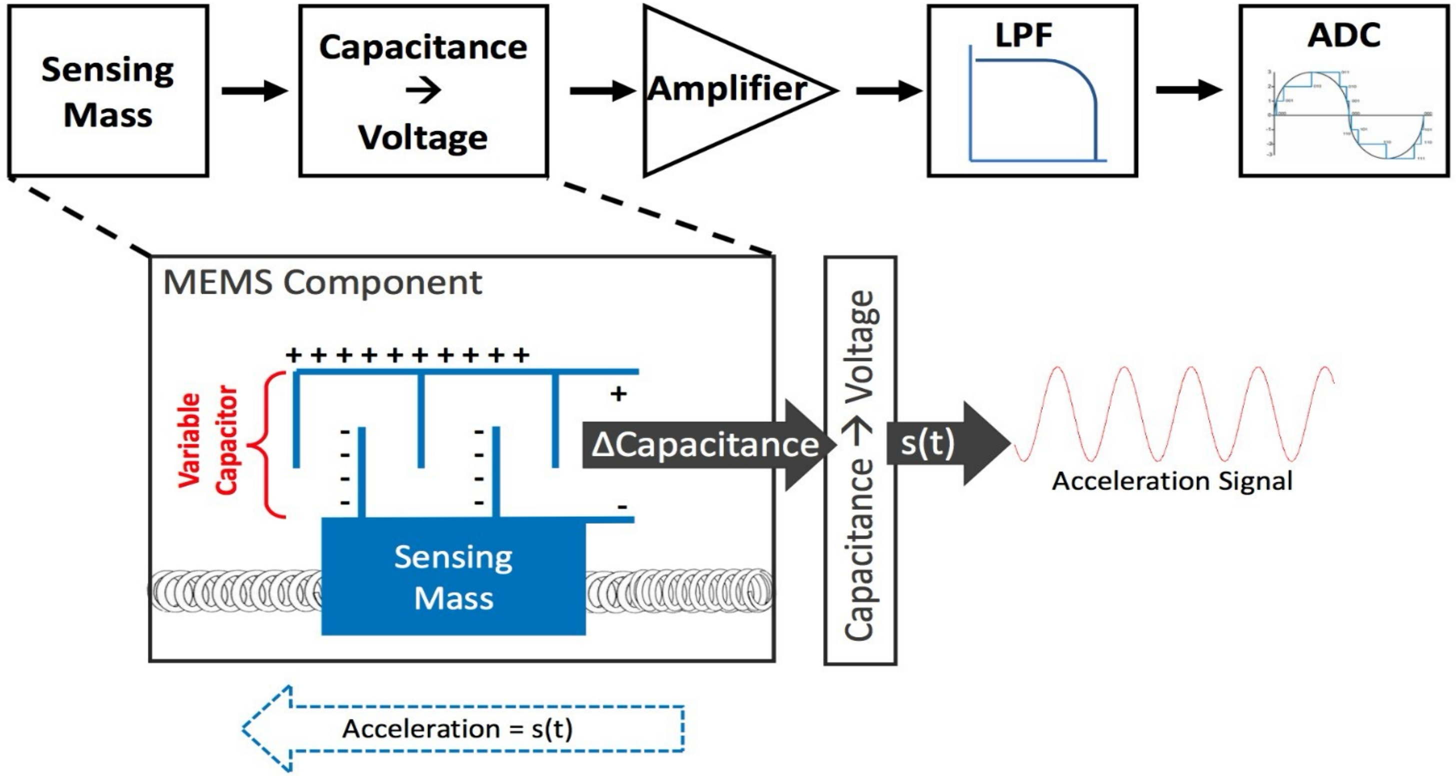


Acoustic (Sound) Signal can Impede MEMS Sensors

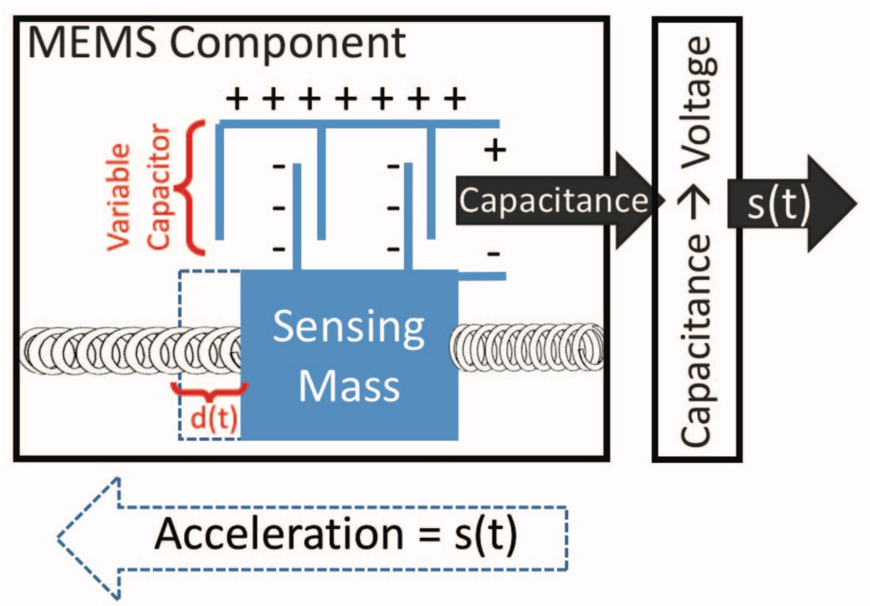
- Modulated acoustic wave can induce abnormal readings in the MEMS sensors

https://futurism.com/hackers-can-take-control-of-devices-using-sound-waves

MEMS Accelerometer



MEMS Accelerometer



Newton's 2nd law of motion

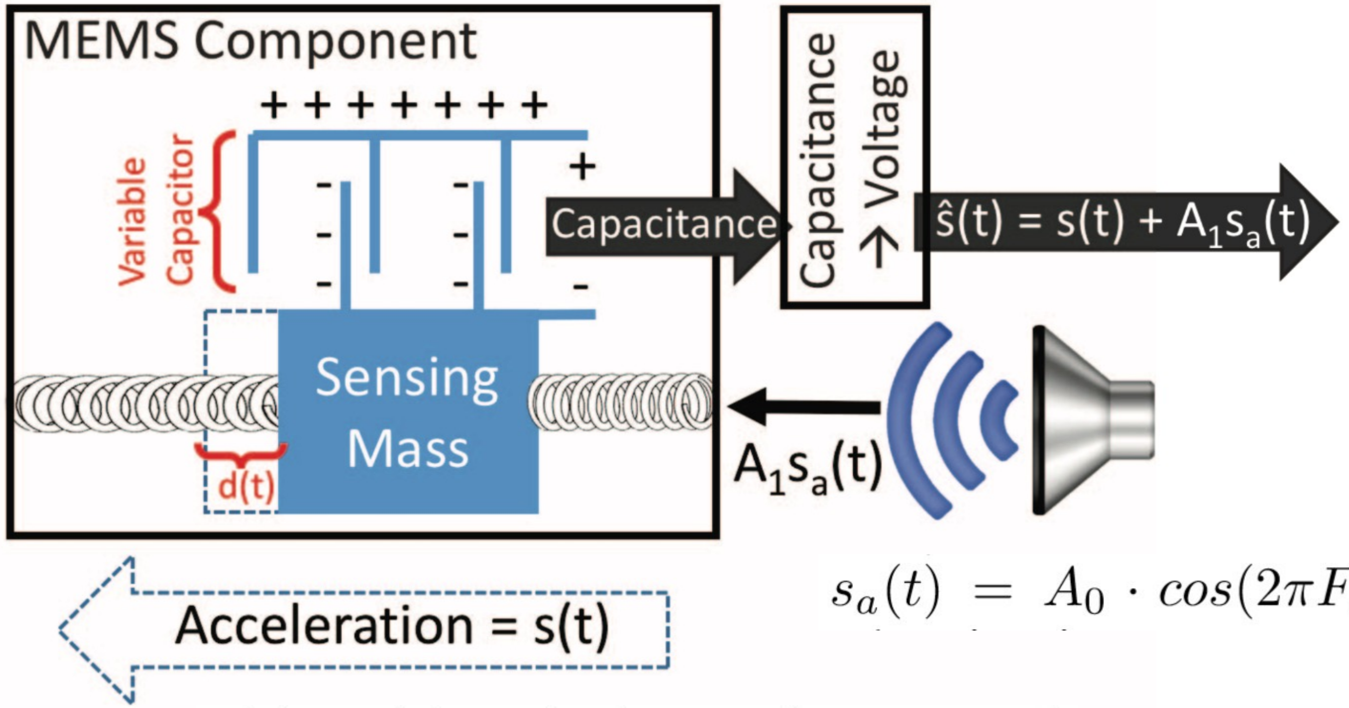
$$F = ma$$

Hooke's law

$$F = -k_s d$$

Acceleration voltage signal $a = -\frac{k_s d}{m}$

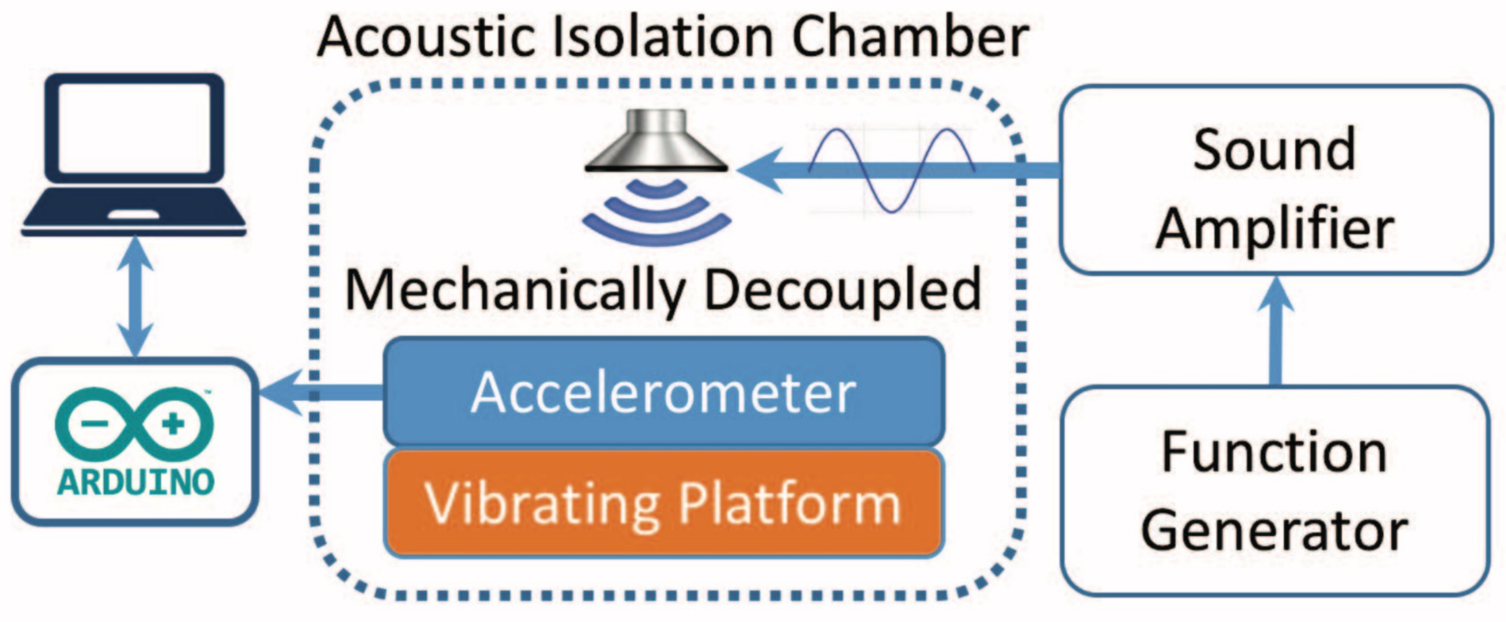
Attack Modeling



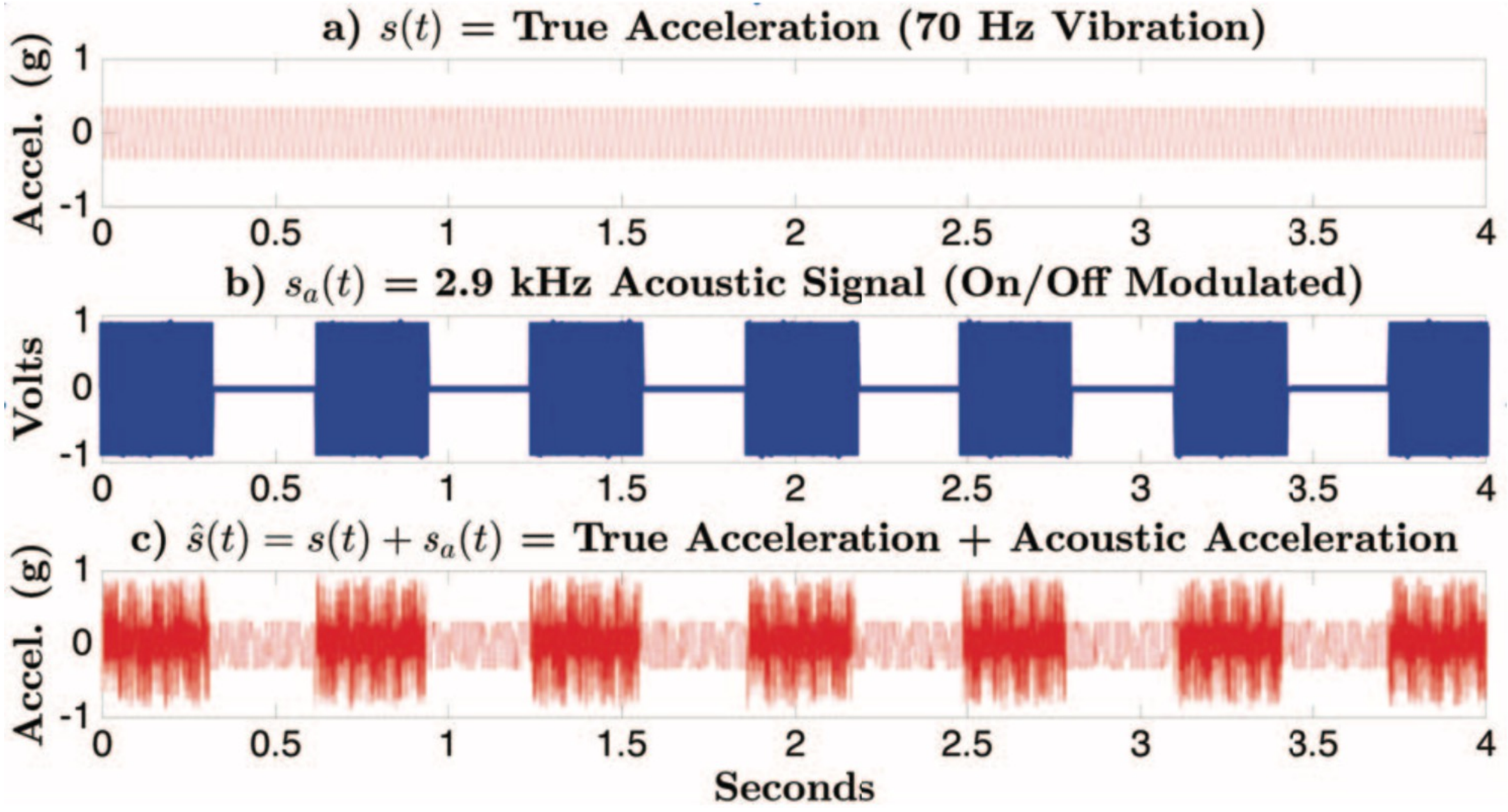
$$s_a(t) = A_0 \cdot cos(2\pi F_a t + \phi)$$

$$\hat{s}(t) = s(t) + A_1 A_0 \cdot cos(2\pi F_a t + \phi)$$

Experiment: Evaluating the Model



Experiment Results

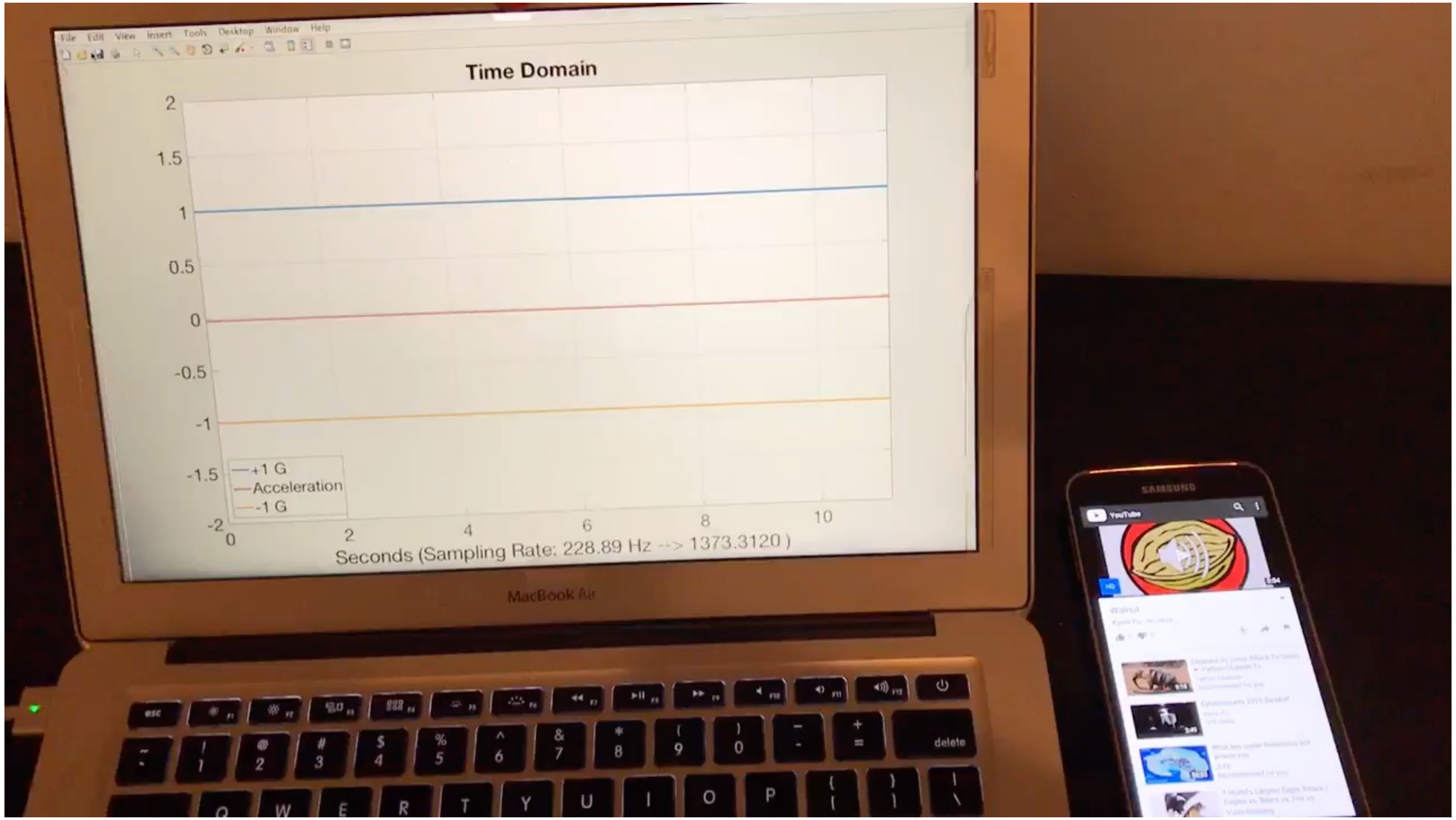


Maximizing the Acoustic Disturbance

$$\hat{s}(t) = s(t) + A_1 \cdot s_a(t)$$

Maximize A_1 $\longrightarrow$ Resonance

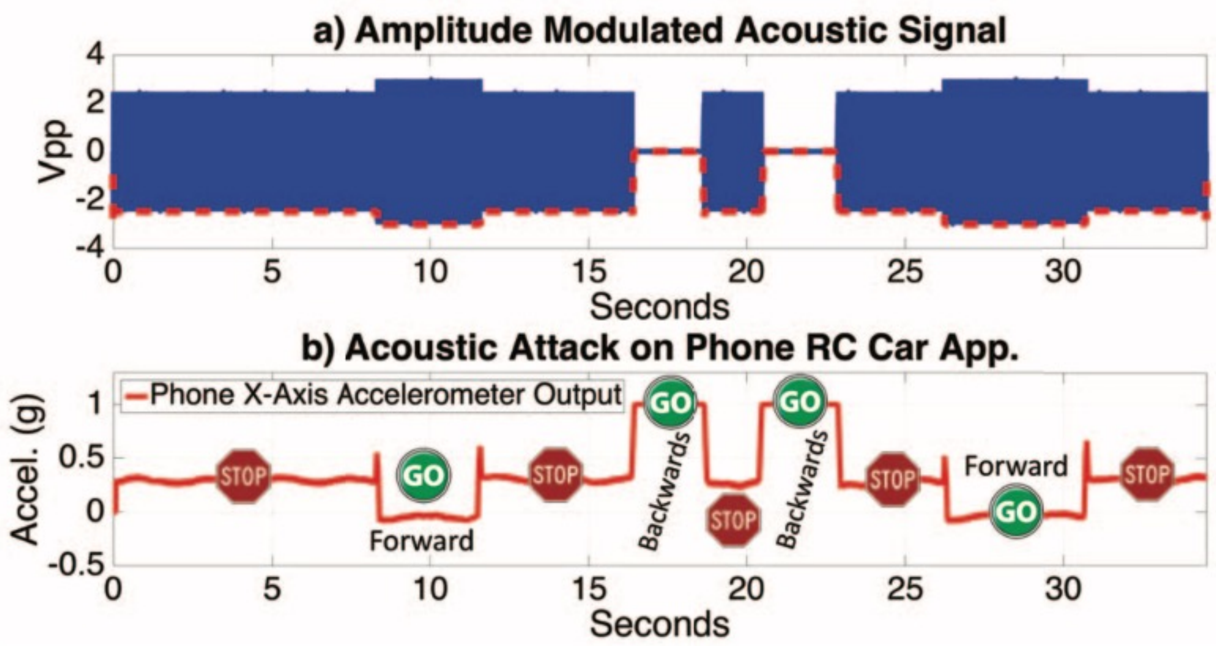
Attack Demo


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

Packaging effects on resonant frequencies

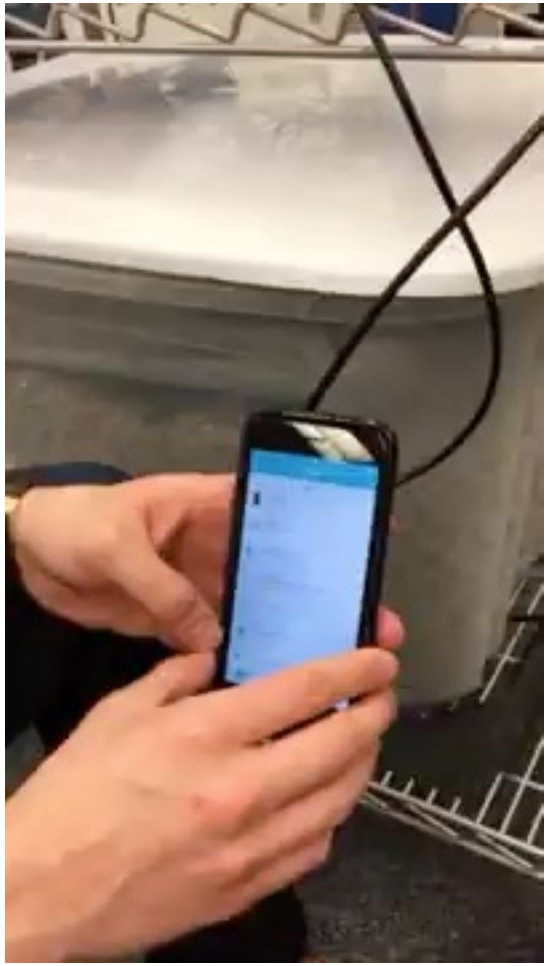
Device Model	Resonant Frequency (kHz)			Amplitude (g)
	X	Y	Z	
MPU6500 Sensor Only	5.1, 20.3	5.1–5.3	None	1.9
Galaxy S5	5.25–5.55	5.35	None	2
Galaxy Note 3	5.3–5.4	None	None	0.4

Attack 1: Smartphone controlled RC car



Attack 2: Fitbit

Attack 2: Fitbit



Defense: H/W defense

LPF (Low Pass Filter)

- Add LPF
- Lower the cut-off frequency or narrow the transition band
- Change physical design

Amplifier

- Make tolerant or filter out resonant frequency prior to amp

Acoustic Dampening Materials

- Requires an additional space

Defense: S/W defense

Randomized Sampling

- Prevents tuning to a resonant frequency to create a DC alias

180° Out-of-Phase Sampling

- Creates a simple band-stop filter around resonant frequency by summing signal with time-shifted version of signal

Final Remarks: As System Builder

- Know your system well
- Understand the possible loopholes of your system