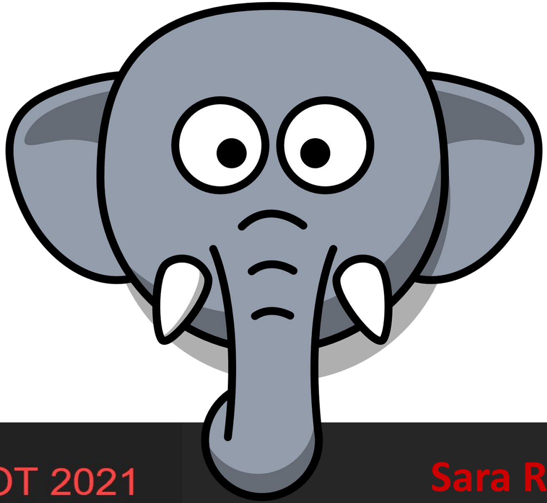
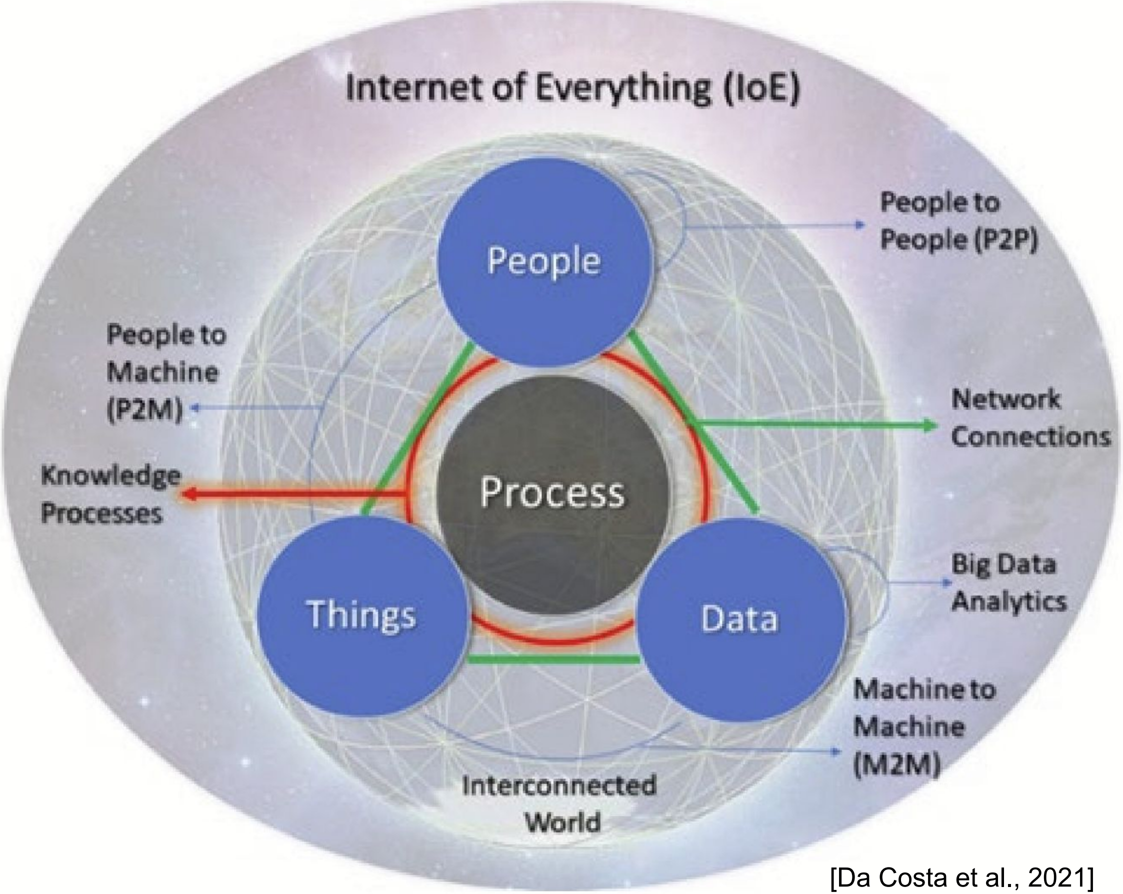
# Sensor Security

Sara Rampazzi
srampazzi@ufl.edu

# The Internet of Everything



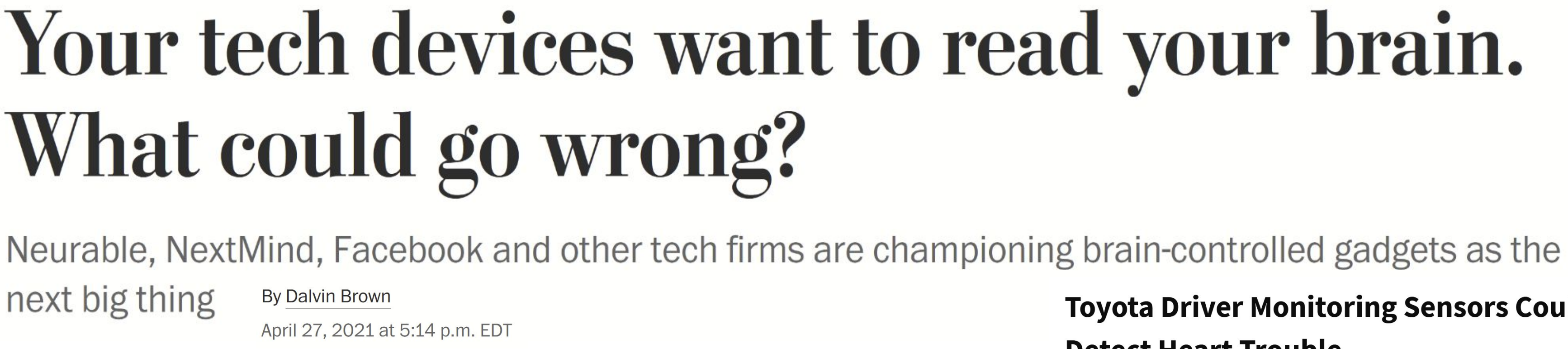


[Da Costa et al., 2021]

# Smarter decision

# Autonomous decision

SENSORS
EVERYWHERE



# Your tech devices want to read your brain. What could go wrong?

Neurable, NextMind, Facebook and other tech firms are championing brain-controlled gadgets as the next big thing

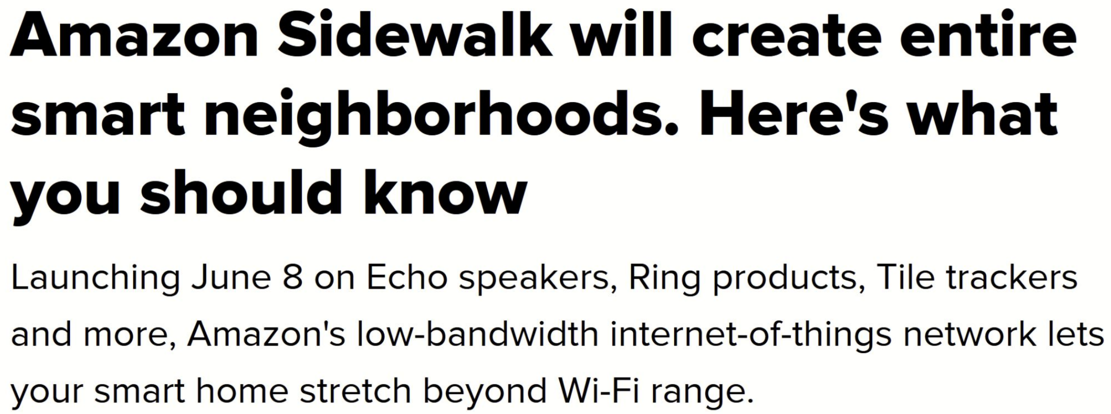
By Dalvin Brown

April 27, 2021 at 5:14 p.m. EDT

## Toyota Driver Monitoring Sensors Could Detect Heart Trouble

The raft of sensors in new Toyota cars could include some to detect heart anomalies in drivers before they strike.

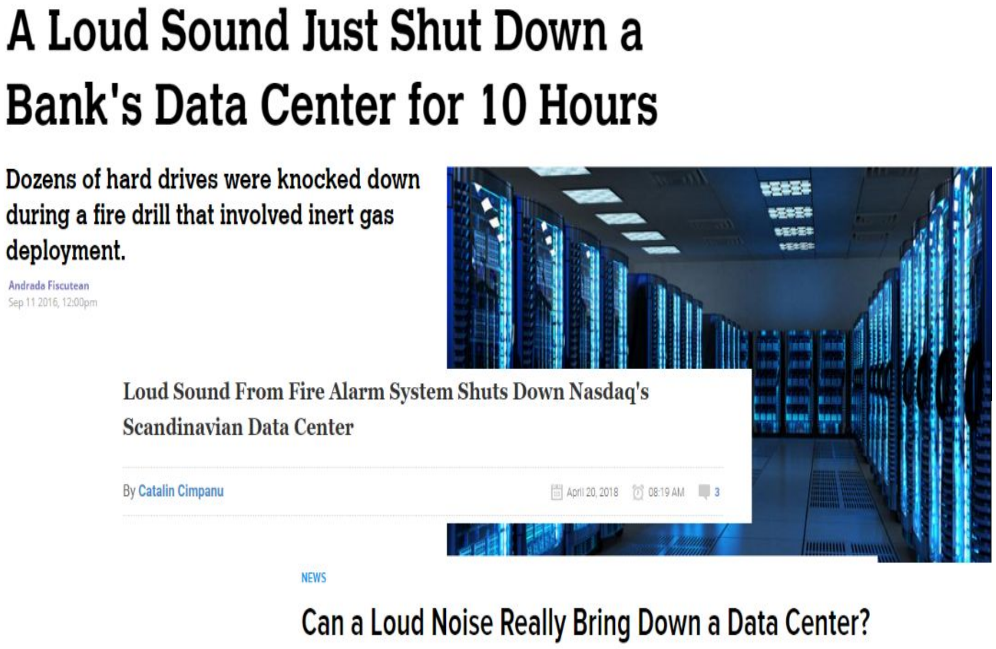
Dan Carney | Oct 28, 2020



# Amazon Sidewalk will create entire smart neighborhoods. Here's what you should know

Launching June 8 on Echo speakers, Ring products, Tile trackers and more, Amazon's low-bandwidth internet-of-things network lets your smart home stretch beyond Wi-Fi range.

# Unexpected effects



## A Loud Sound Just Shut Down a Bank's Data Center for 10 Hours

Dozens of hard drives were knocked down during a fire drill that involved inert gas deployment.

Andrada Fiscutean
Sep 11 2016, 12:00pm

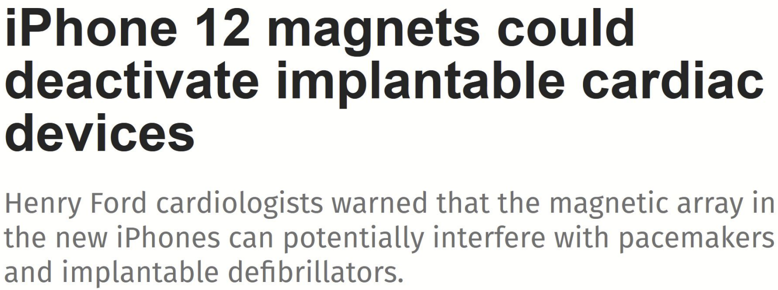
Loud Sound From Fire Alarm System Shuts Down Nasdaq's Scandinavian Data Center

By Catalin Cimpanu April 20, 2018 08:19 AM 3

NEWS

Can a Loud Noise Really Bring Down a Data Center?

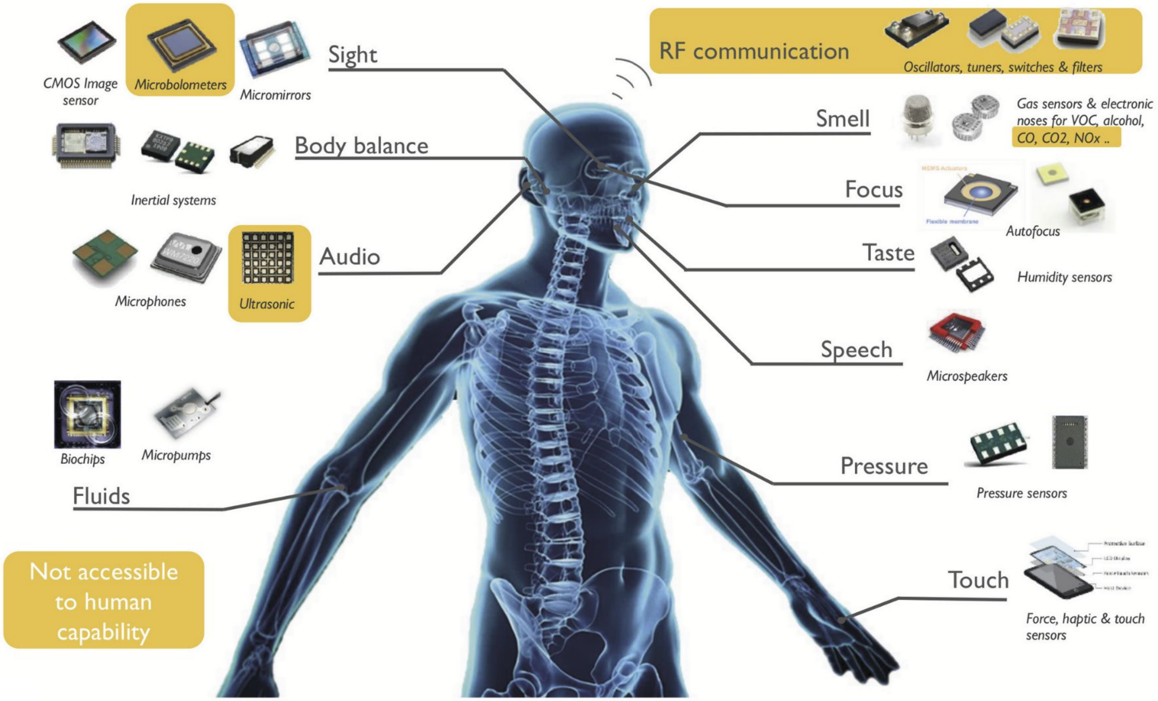
Engine vibration can apparently fool the software into thinking the seat is empty.



## iPhone 12 magnets could deactivate implantable cardiac devices

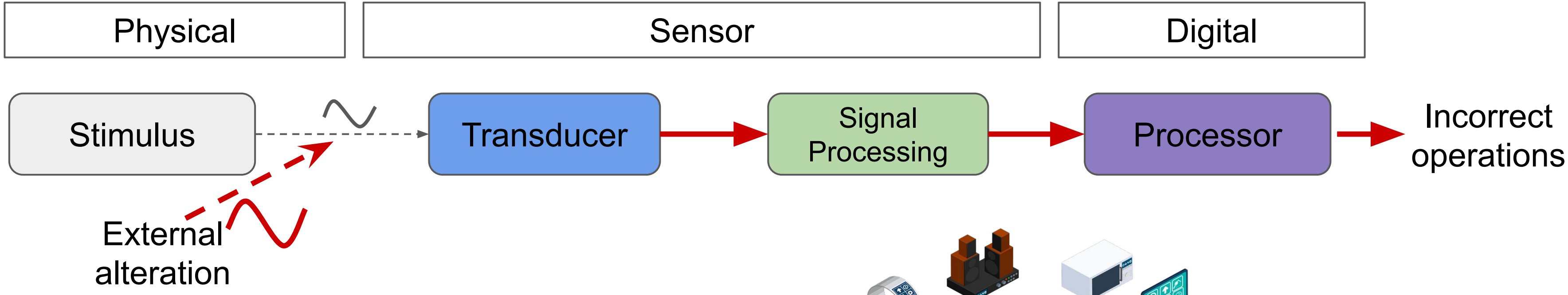
Henry Ford cardiologists warned that the magnetic array in the new iPhones can potentially interfere with pacemakers and implantable defibrillators.

# Do sensors act as our senses?



© 2019 | www.yole.fr – www.i-micronews.com

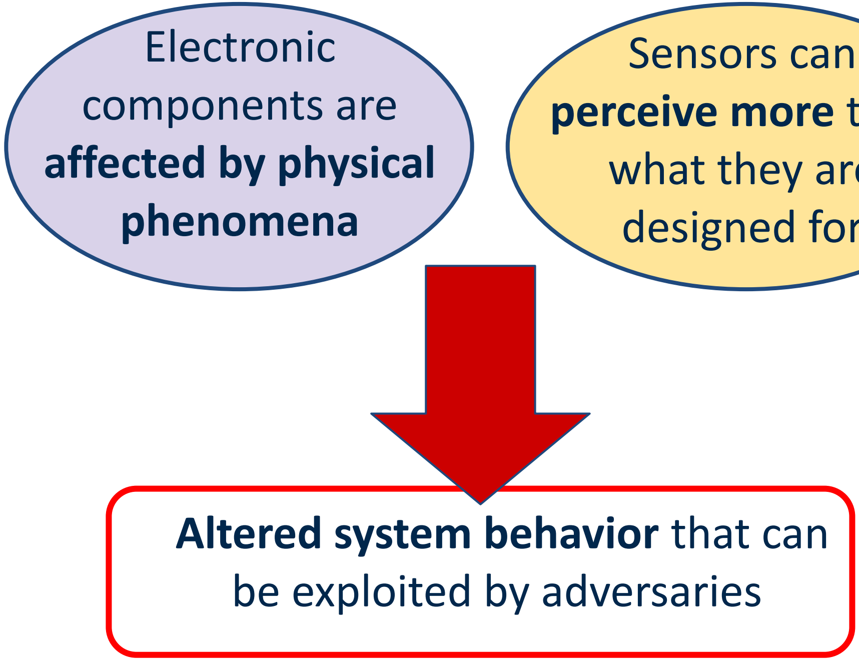
# What it means sensor attacks?



- Electromagnetic interference
- Sound
- Light
- Mechanical vibration
- Heat
- Magnetic field

[Designed by  Emilio Pimentel]

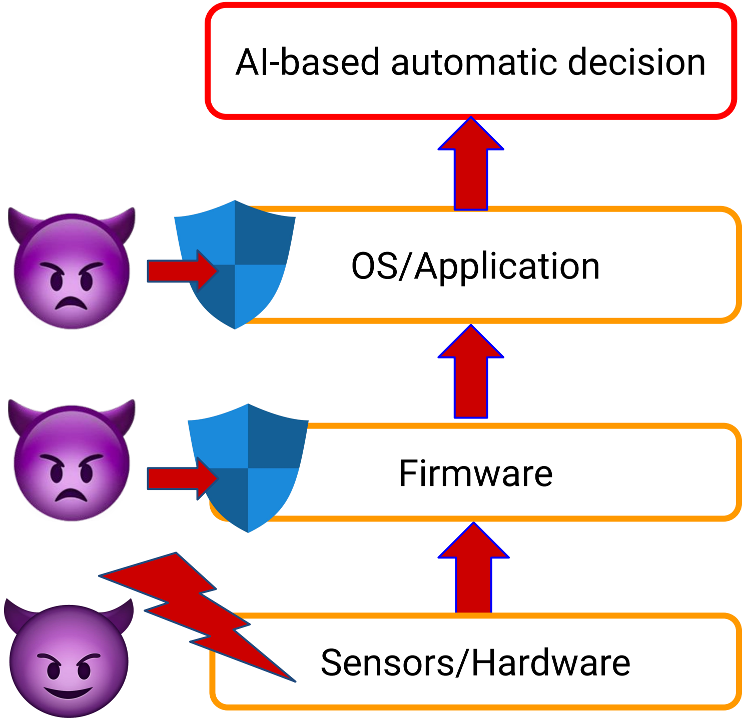
# What it means sensor attacks?



Electronic components are **affected by physical phenomena**

Sensors can **perceive more** than what they are designed for

**Altered system behavior** that can be exploited by adversaries



AI-based automatic decision

OS/Application

Firmware

Sensors/Hardware

# What it means sensor attacks?

Electronic components are **affected**

**phe**

Sensors can **perceive more** than

y are

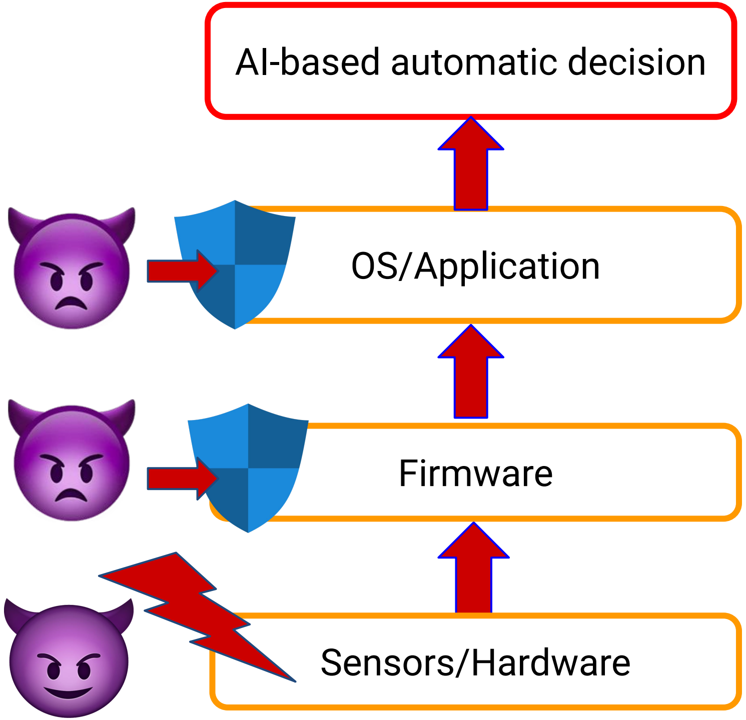
d for

**WARNING!**

**Integrity issue**

**How we can recognize a legitimate signal?**

**Altered system behavior** that can be exploited by adversaries



AI-based automatic decision

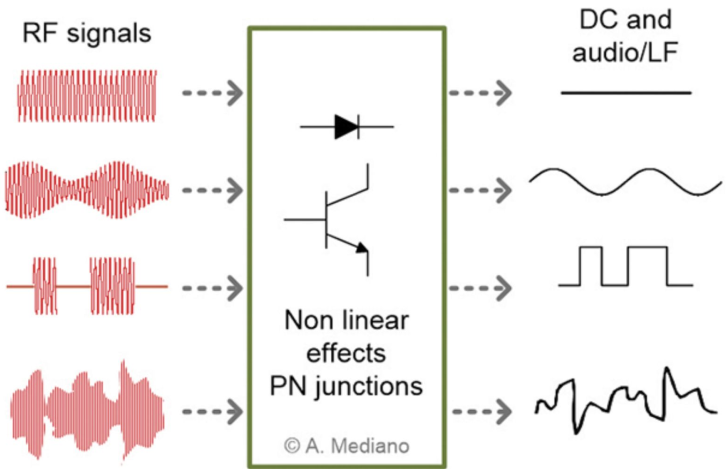
OS/Application

Firmware

Sensors/Hardware

# Sensor exploitation

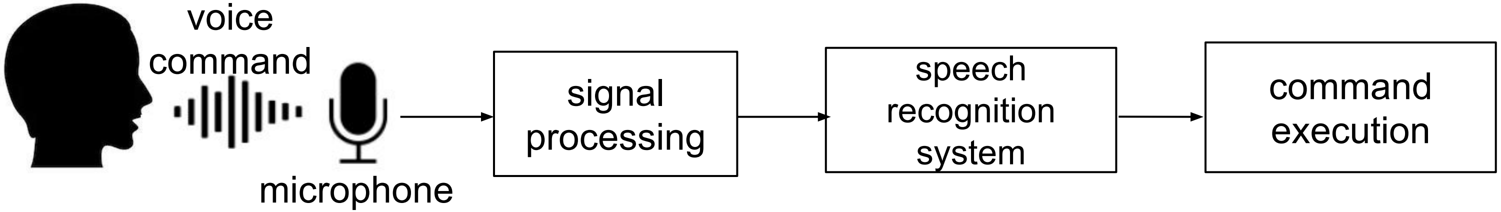
- **Coupling** (e.g. resonance frequencies)
- **Non-linearities** (e.g. rectification)
- **Intermodulation** (e.g. change in frequency range)
- **Periodicity** (e.g. sample frequency)
- **Oversensing** (e.g. signal conversion/demodulation)



# Voice Controllable Systems

[Source: pandaily.com]

[Source: developers.google.com]



voice command

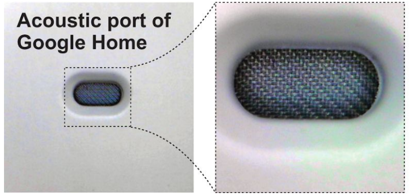
microphone

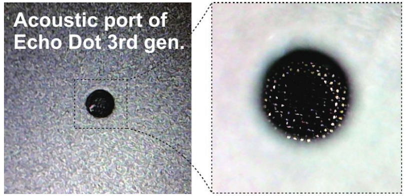
signal processing

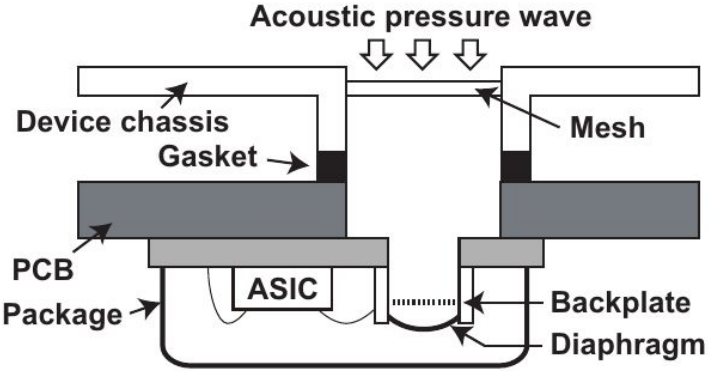
speech recognition system

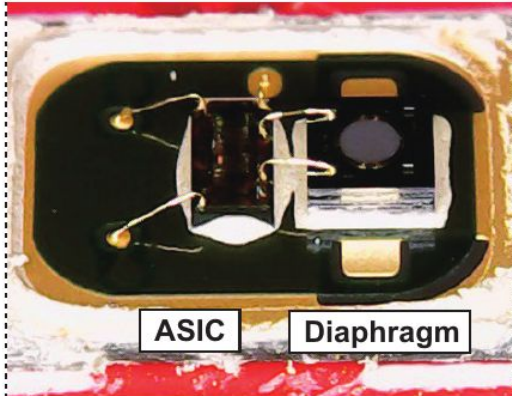
command execution

# MEMS microphone





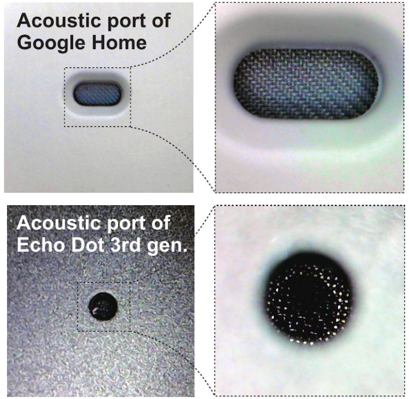


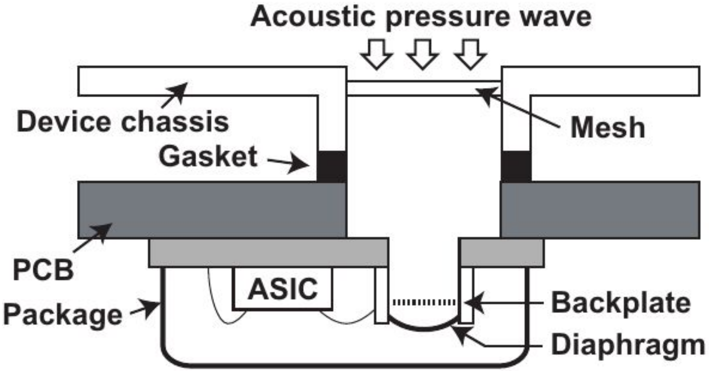


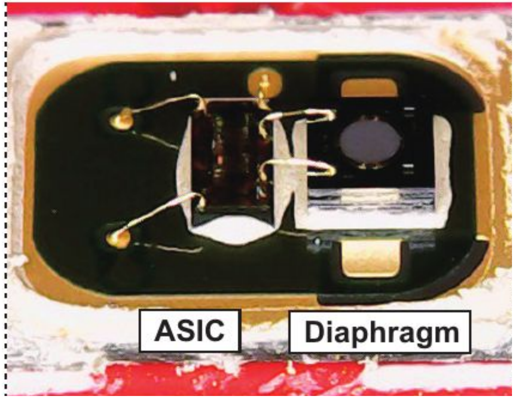
The diaphragm and backplate work as parallel-plate **capacitor**

The ASIC converts the capacitive change to voltage

# MEMS microphone


Acoustic port of Google Home
Acoustic port of Echo Dot 3rd gen.

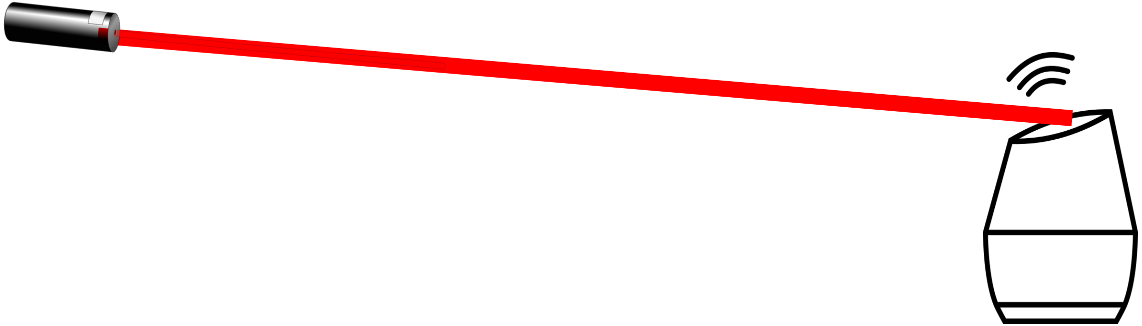




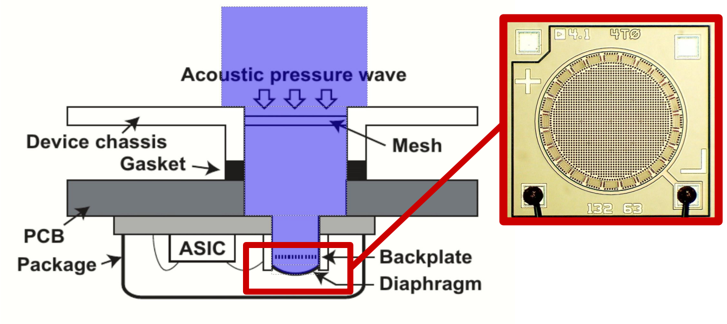
*“Microphones are designed to capture* ***only acoustic waves****”*

*- The unaware systems designer -*

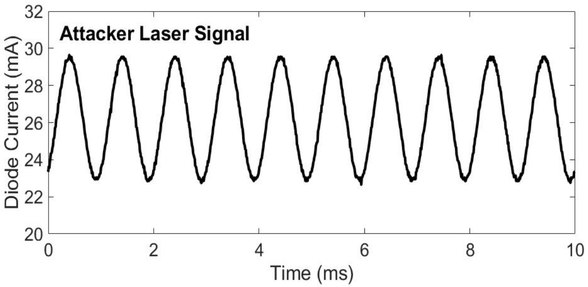
# MEMS microphones can capture light

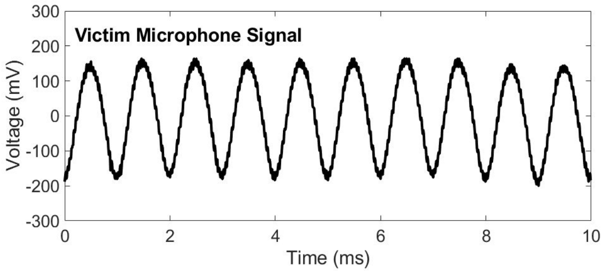


# MEMS microphones can capture light

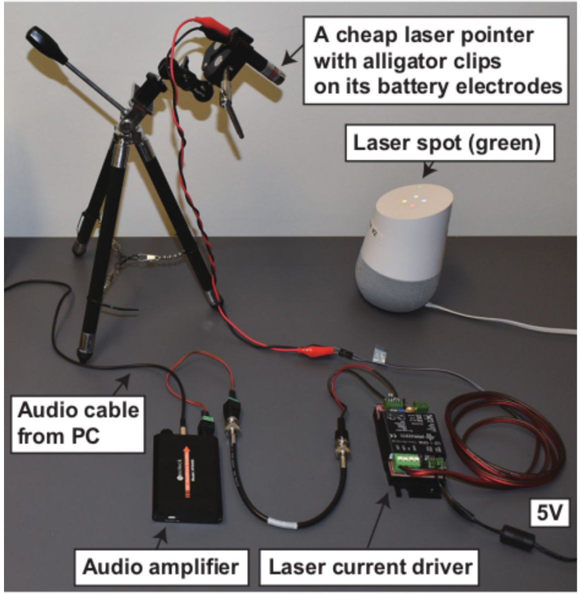


Amplitude modulated light generates a modulated voltage signal in the audio frequency range

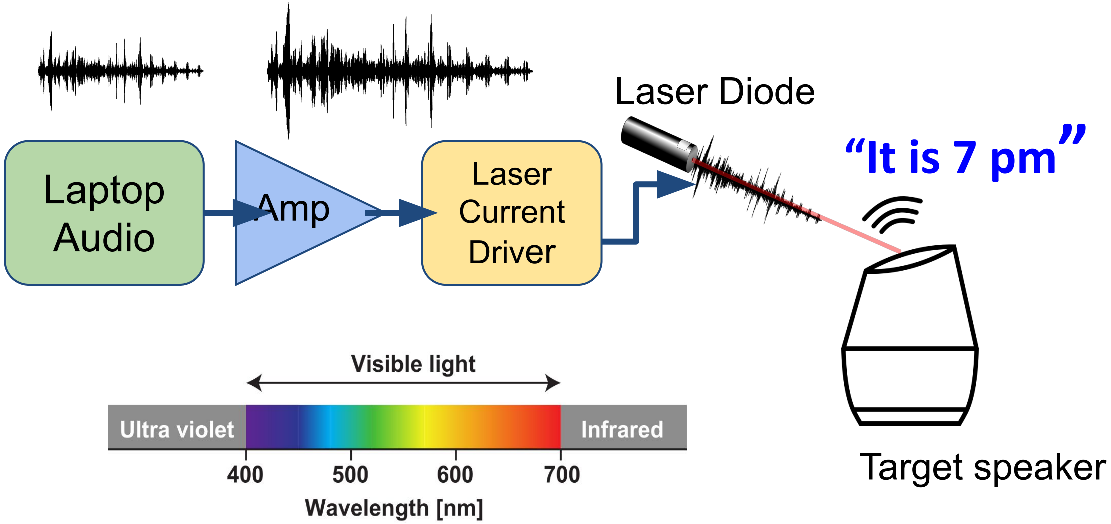




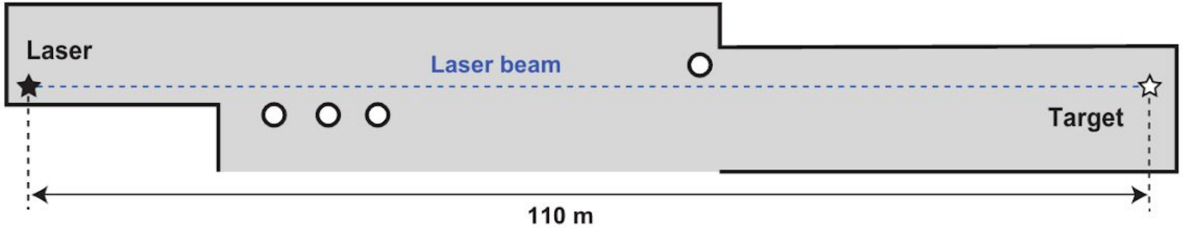
# LightCommands

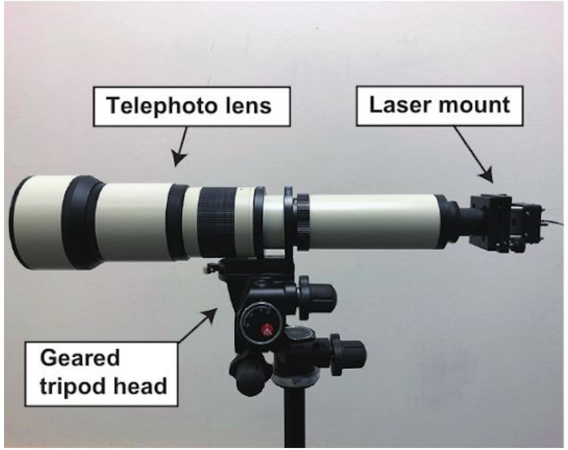


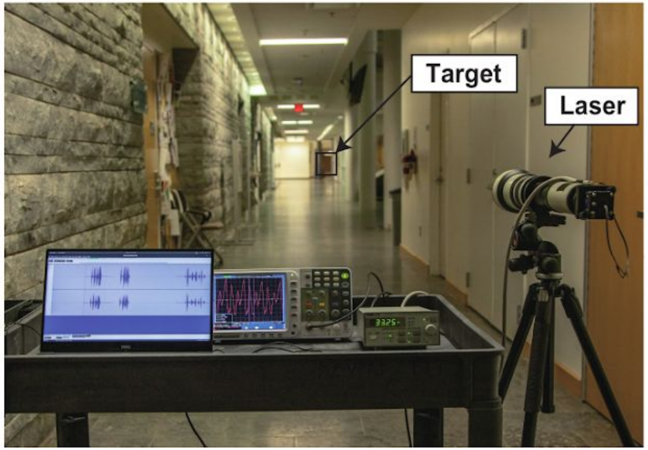
“OK Google, What time is it?”

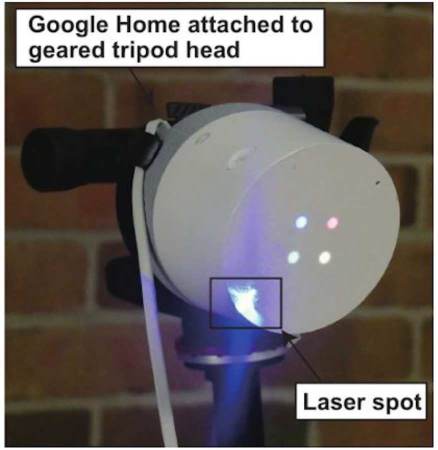


# MEMS microphones can capture light

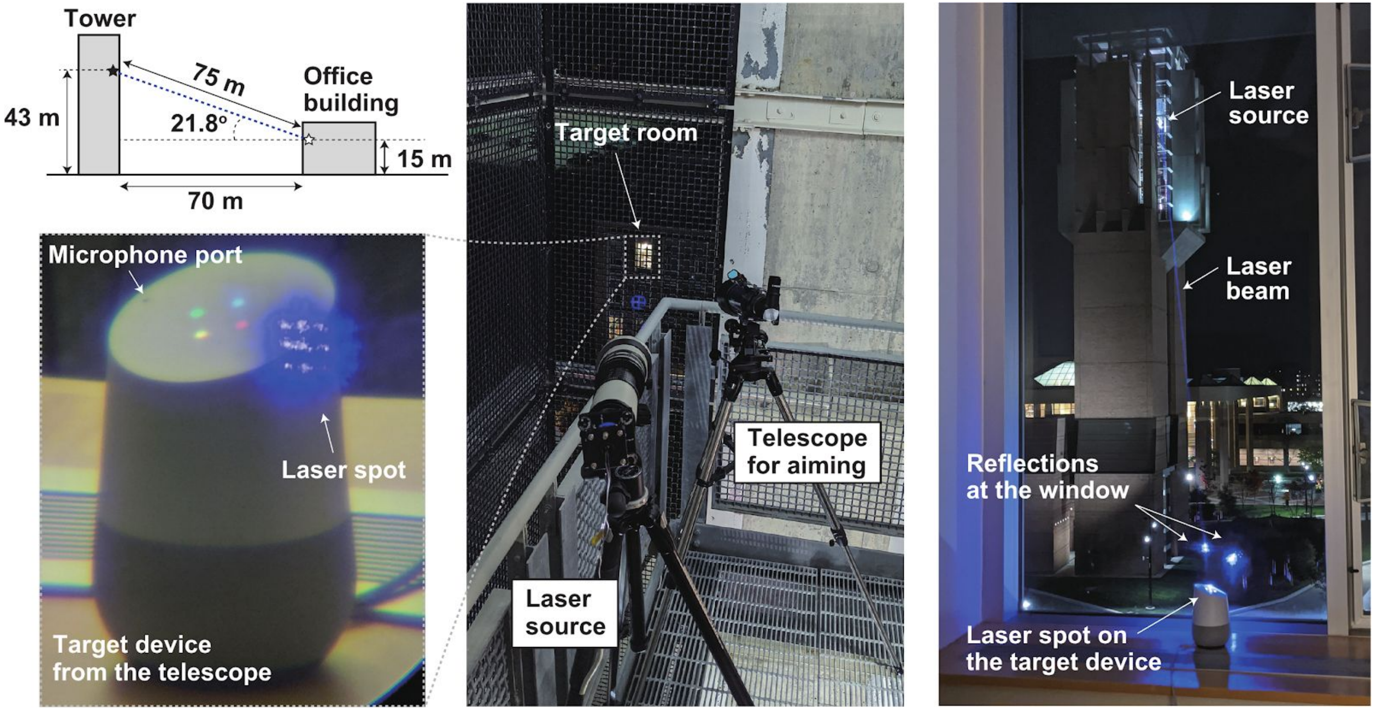




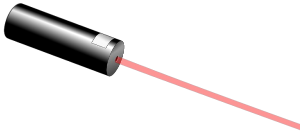


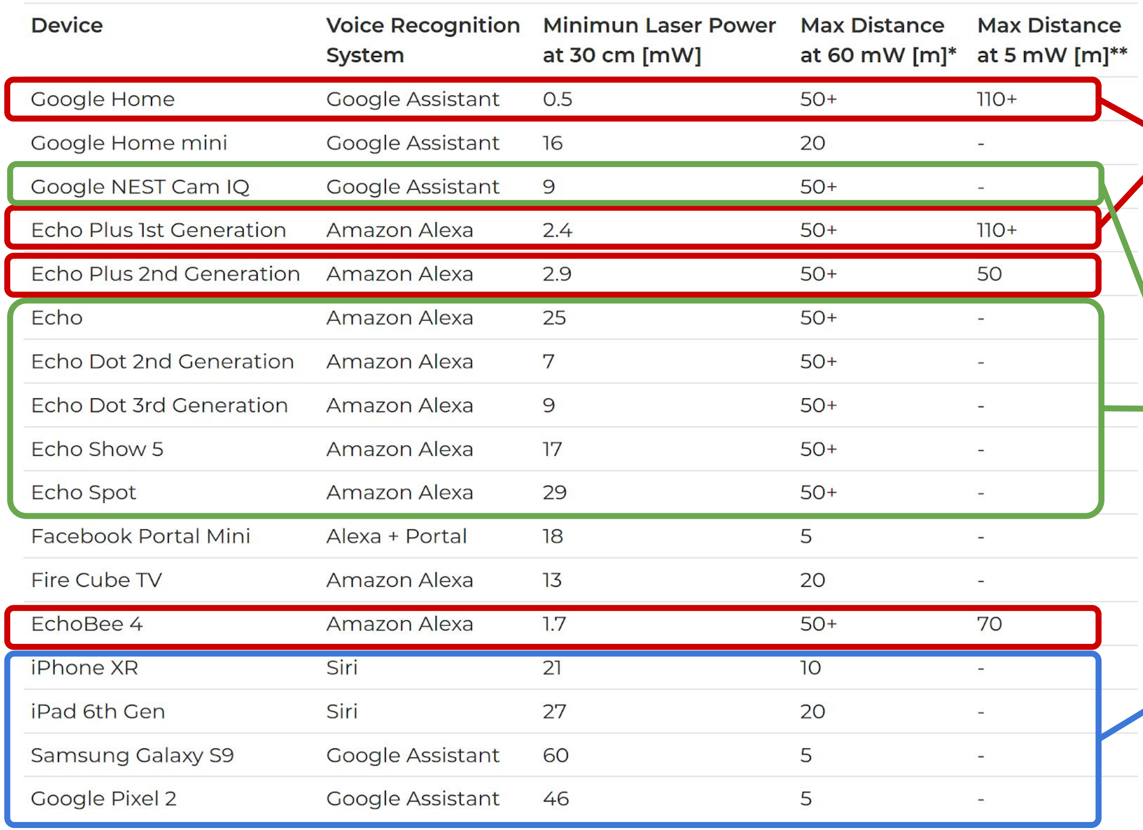


# MEMS microphones can capture light



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

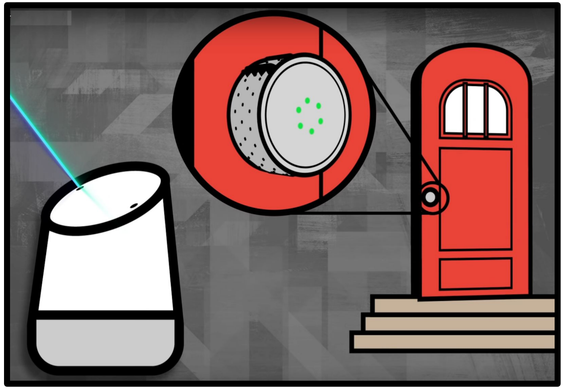
60mW:
50+ meters

Phones/Tablets

60mW:
5-20 meters

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

Unlock doors august



Hi, how can i help?

Ok, Google, turn on light

Light on

Turn on/off
Enable/Disable
Change settings

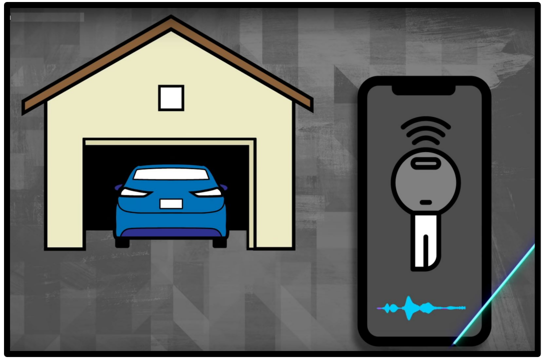
Nest
ecobee
Garadget

Unauthorized purchases

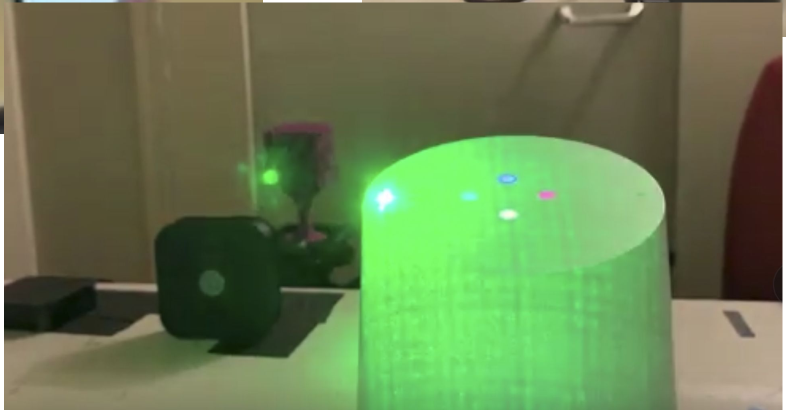
amazon.com

Ford
TESLA

Open trunks
Unlock car
Start engine



blink

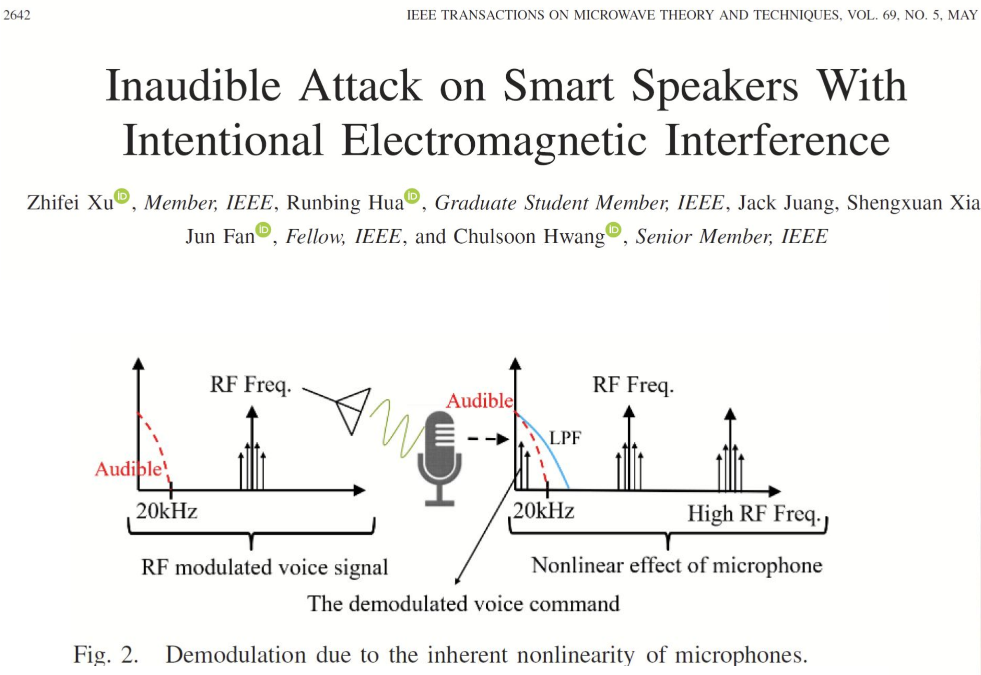


[Demo: https://www.youtube.com/watch?v=L3CAZWLoG1Y]

**Enable/Disable security cameras**

[Source: https://voicebot.ai]

[Source: store.google.com]



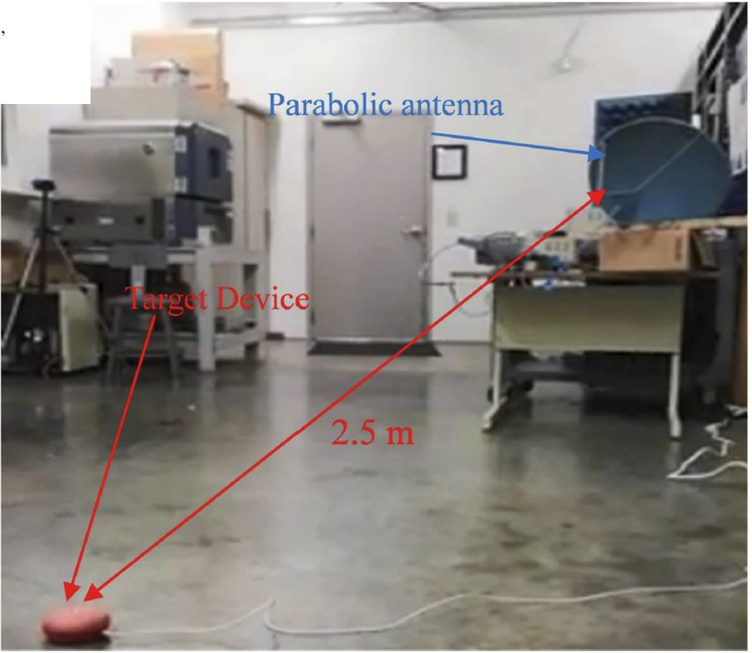
2642 IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, VOL. 69, NO. 5, MAY 2021

# Inaudible Attack on Smart Speakers With Intentional Electromagnetic Interference

Zhifei Xu, *Member, IEEE*, Runbing Hua, *Graduate Student Member, IEEE*, Jack Juang, Shengxuan Xia, Jun Fan, *Fellow, IEEE*, and Chulsoon Hwang, *Senior Member, IEEE*

RF Freq.
Audible
20kHz
RF modulated voice signal
Audible
LPF
RF Freq.
20kHz
High RF Freq.
Nonlinear effect of microphone
The demodulated voice command

Fig. 2. Demodulation due to the inherent nonlinearity of microphones.



# Vulnerabilities combination

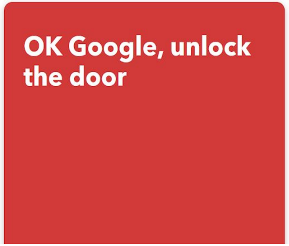
Personalization is not authentication

- No speaker authentication, only personalization
- Inaccurate speech recognition (e.g.  Text-to-Speech)
- Wake up word-only security (e.g. Siri)

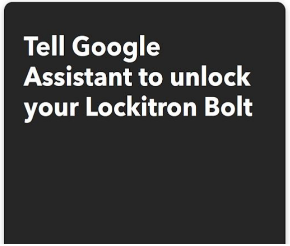
# Vulnerabilities combination

Usability Vs Security

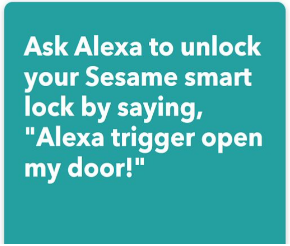
- Apps & routines customizable by third-party software (e.g. IFTTT)
- Voice-only operations



OK Google, unlock the door



Tell Google Assistant to unlock your Lockitron Bolt



Ask Alexa to unlock your Sesame smart lock by saying, "Alexa trigger open my door!"

# Vulnerabilities combination

Common IoT vulnerabilities

- Not protected operations (e.g. open the garage door)
- Easy PIN bruteforcing (e.g. 1-digit PIN)

“123...”

“Incorrect Passcode, Try Again...”

“124...”

“Incorrect Passcode, Try Again...”

“125...”

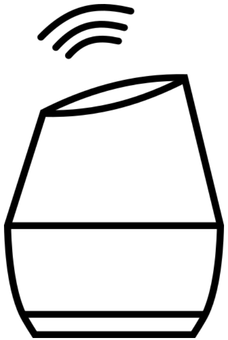
“Incorrect Passcode, Try Again...”

...

“438...”

...

“OK, Opening the front door”



# Vulnerabilities combination

While attacking cars:

- No key proximity required (e.g. voice-only activation)
- Unofficial apps & skills used to perform additional actions not permitted by the official apps
- no PIN required for certain operations
- No mechanisms to prevent PIN brute forcing

# While IoE evolve fast...

… Vulnerabilities can sum to each other ...

... Consumer electronics and sensors still remain exposed to new and evolved malicious attacks …

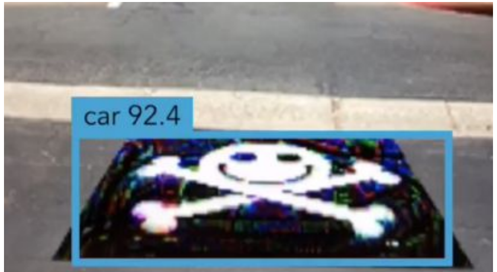
… The patch/fix strategy is not effective.

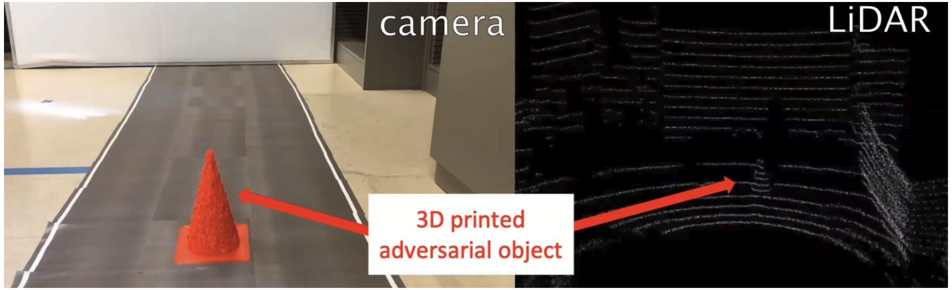
# What about AI?

# Advanced Driver Assistance Systems

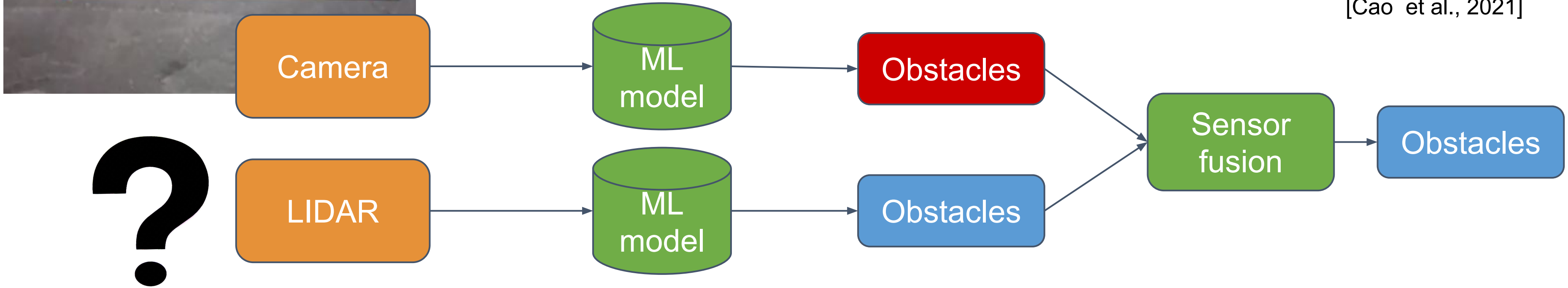
- Enhance the driver's capabilities  (navigation, night vision, etc.)
- Take partial or full automatic control of critical driving processes (breaking, steering, parking, speed, etc.)

# Advanced Driver Assistance Systems





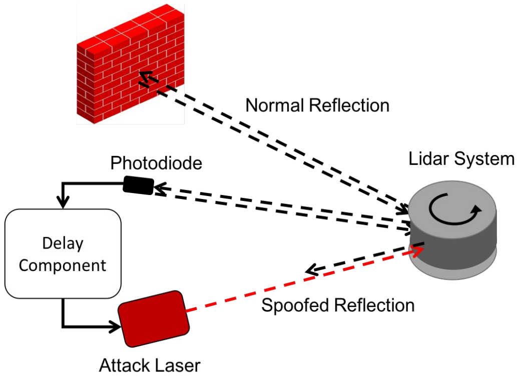
[Cao  et al., 2021]



# Laser-based attacks on LiDARs

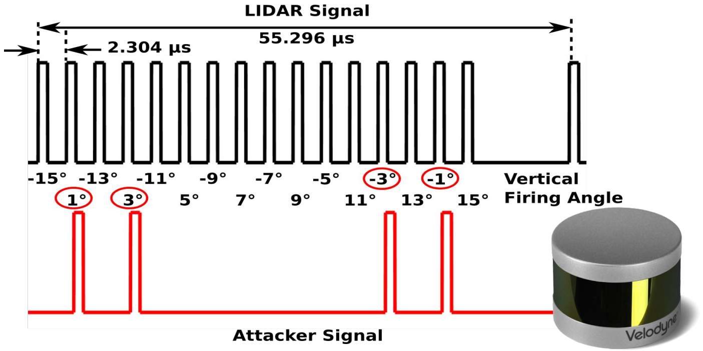
Relay attack using a pulsed laser:

- Fake cloud points generation
- Shaping spoofing objects

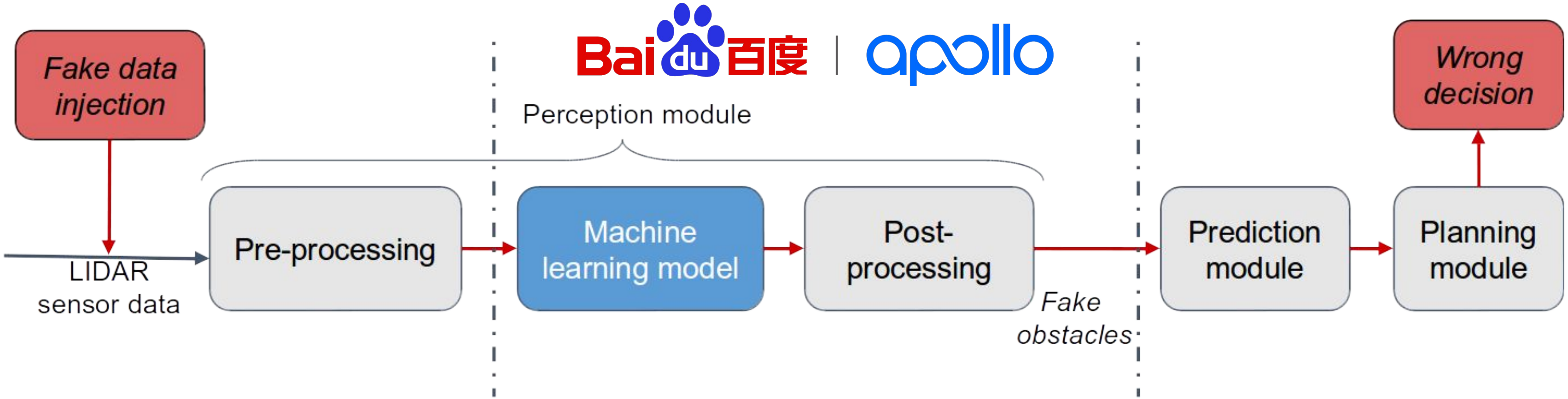


Impact on the control decisions:

Inputs selection to cause the system to make the **wrong decision**



# Laser-based attacks on LiDARs



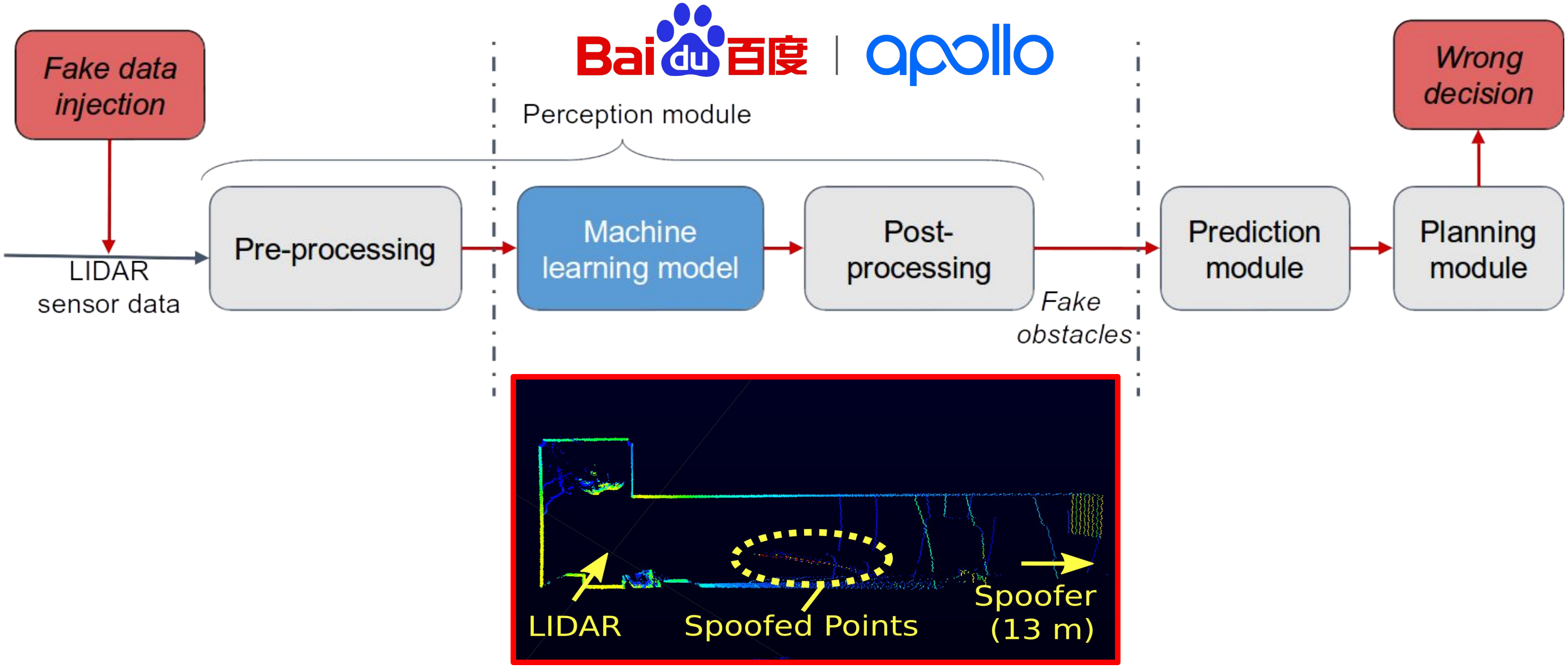
```
x’ = P(x)
Find x’ that Maximize
J(x’,M)
```

**Objectness:** probability of a group of points to be part of an obstacle

**Confidence:** confidence score of the detection

$J(x',M) =$ objectness * confidence * target position

# Laser-based attacks on LiDARs



Baidu 百度 | apollo

Fake data injection

LIDAR sensor data

Perception module

Pre-processing

Machine learning model

Post-processing

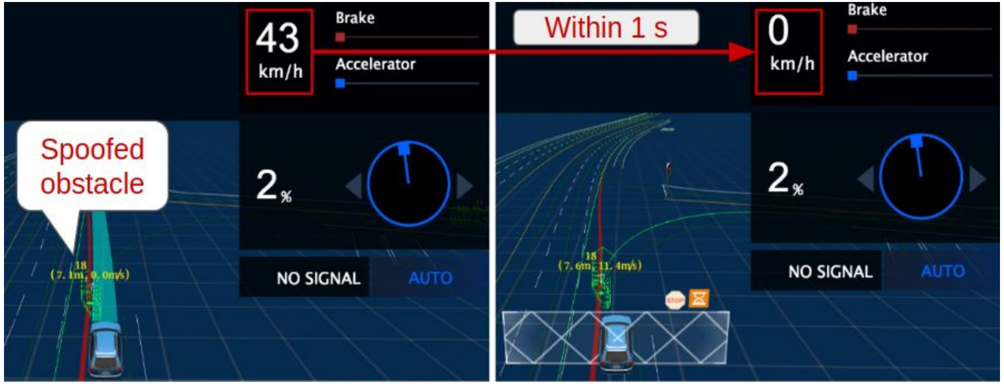
*Fake obstacles*

Prediction module

Planning module

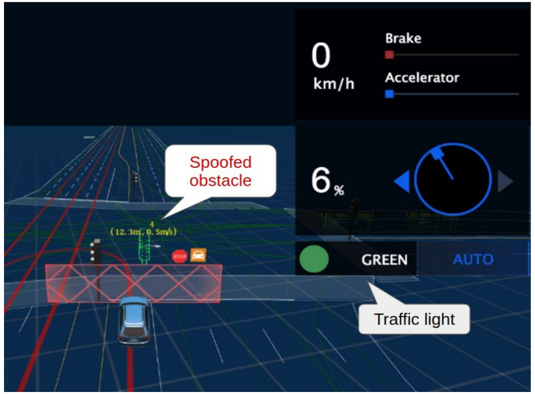
*Wrong decision*

# Laser-based attacks on LiDARs



## Emergency brake attack

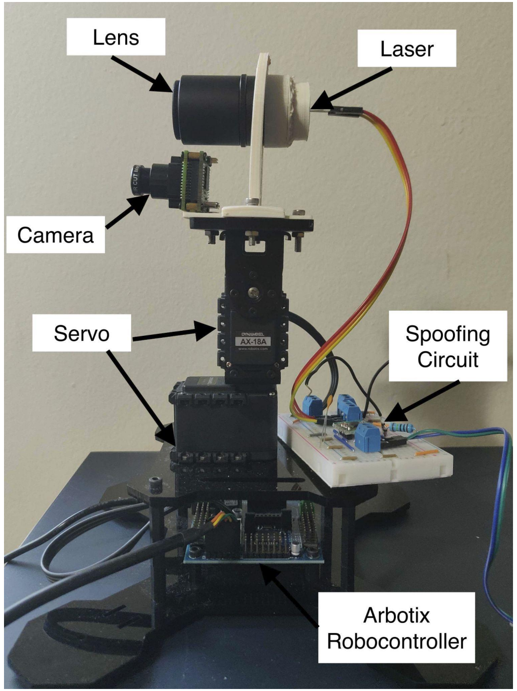
Security implication:
Rear-end collision
Passenger/driver injury

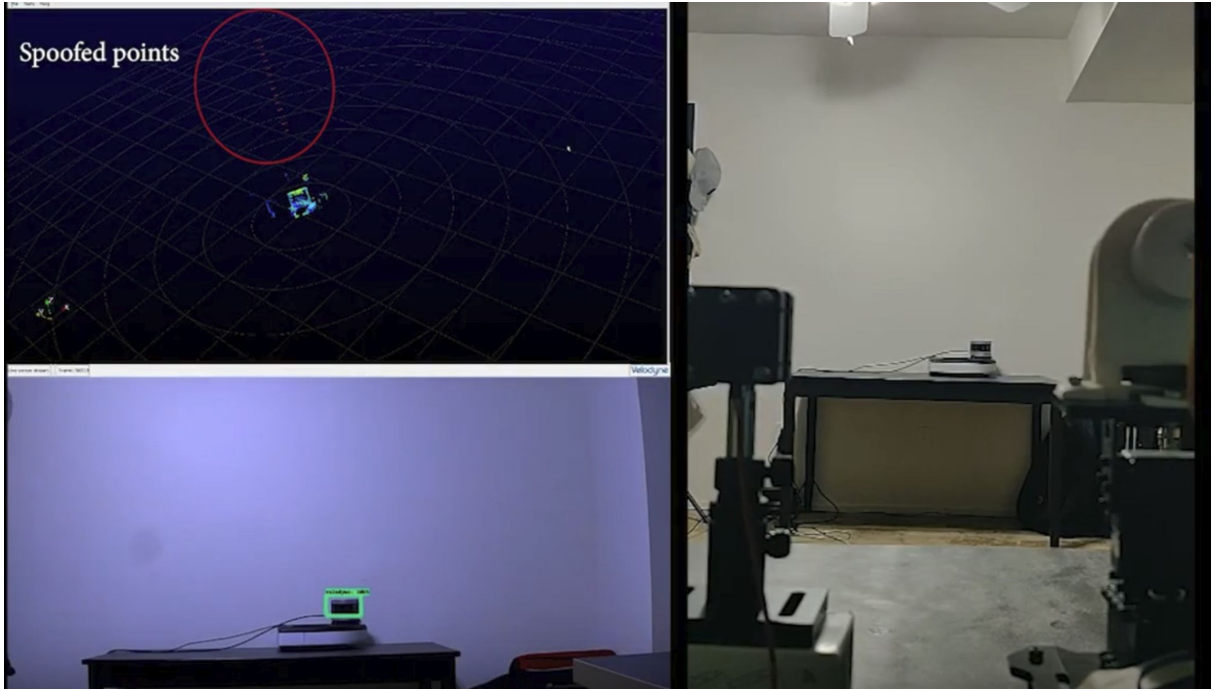


## Freezing attack

“Freeze” AV at intersection
Security implication: Blocking traffic

# Laser-based attacks on LiDARs





[Demo: https://sites.google.com/view/lidarspoofingattack]

# While IoE evolve fast...

… Attackers can easily access to AI-based technology to perform more sophisticated attacks ...

... Consumer electronics and sensors can be used as a vector to undermine AI-based technology …

# While IoE evolve fast...

… we need to STOP thinking about hardware and software as separate entities for addressing security.

# Be prepared for the future!

TOM GAULD
NewScientist
MY VIRTUAL ASSISTANT AND MY ROBOT-CLEANER STOLE ALL MY CRYPTO-CURRENCY AND ELOPED IN MY SELF-DRIVING CAR.