black hat
EUROPE 2020
DECEMBER 9-10
BRIEFINGS

Light Commands: Hacking Voice Assistants with Lasers

Sara Rampazzi
Benjamin Cyr

Light Commands: Hacking Voice Assistants with Lasers

Light Commands

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

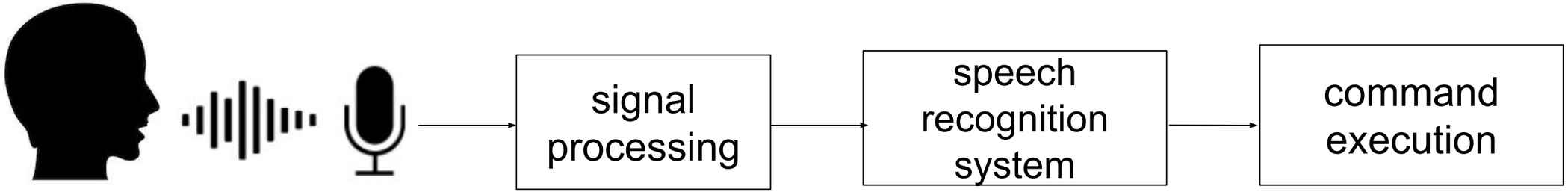
UEC TOKYO

CSE COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF MICHIGAN

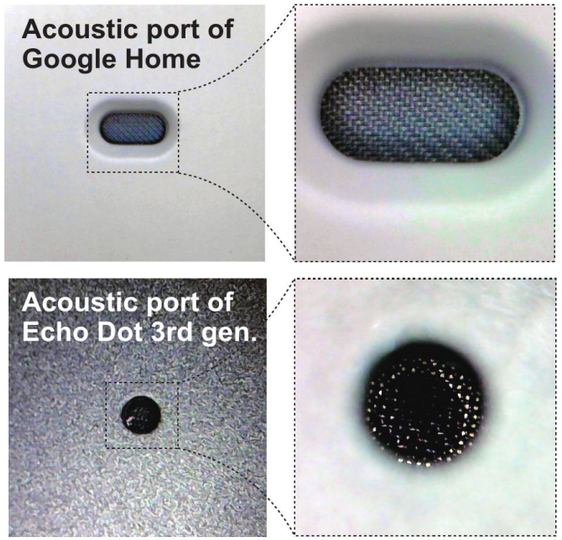
Voice Controllable IoT

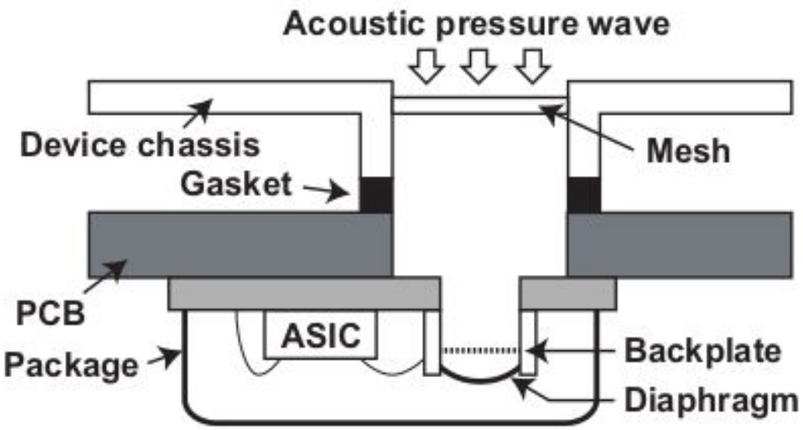
[Source: pandaily.com]

[Source: developers.google.com]

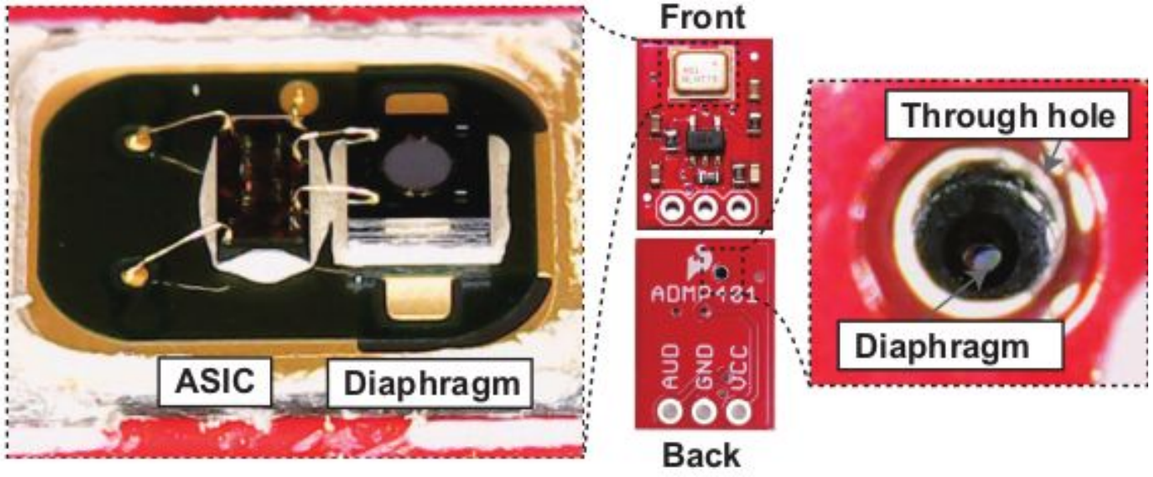


MEMS microphones





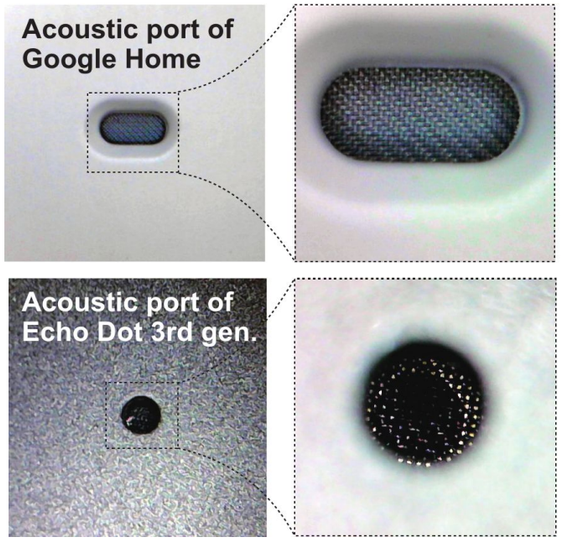
MEMS microphone

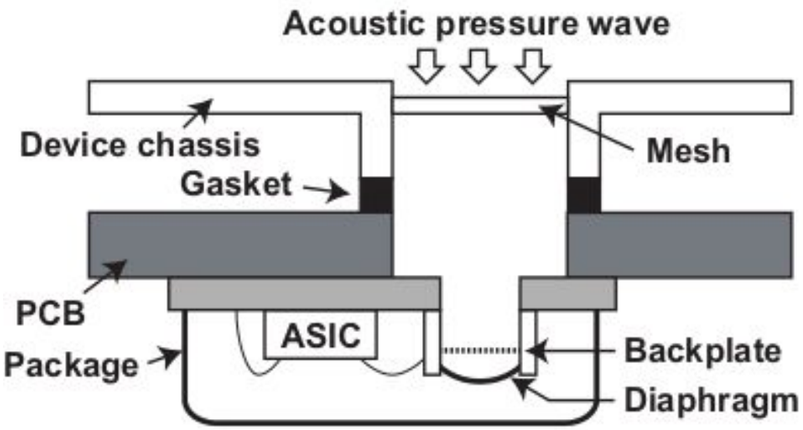


The diaphragm and backplate work as parallel-plate **capacitor**

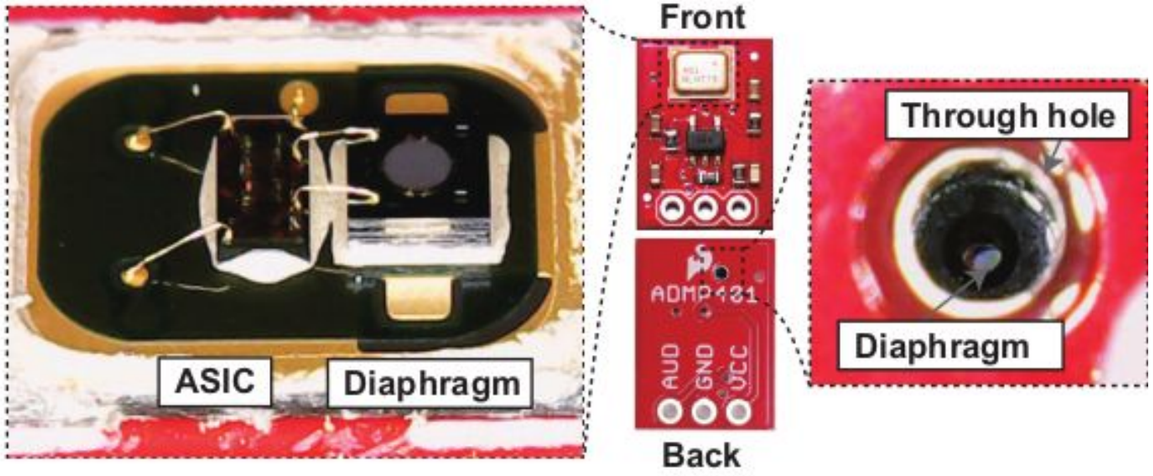
The ASIC converts the capacitive change to voltage

MEMS microphones





MEMS microphone

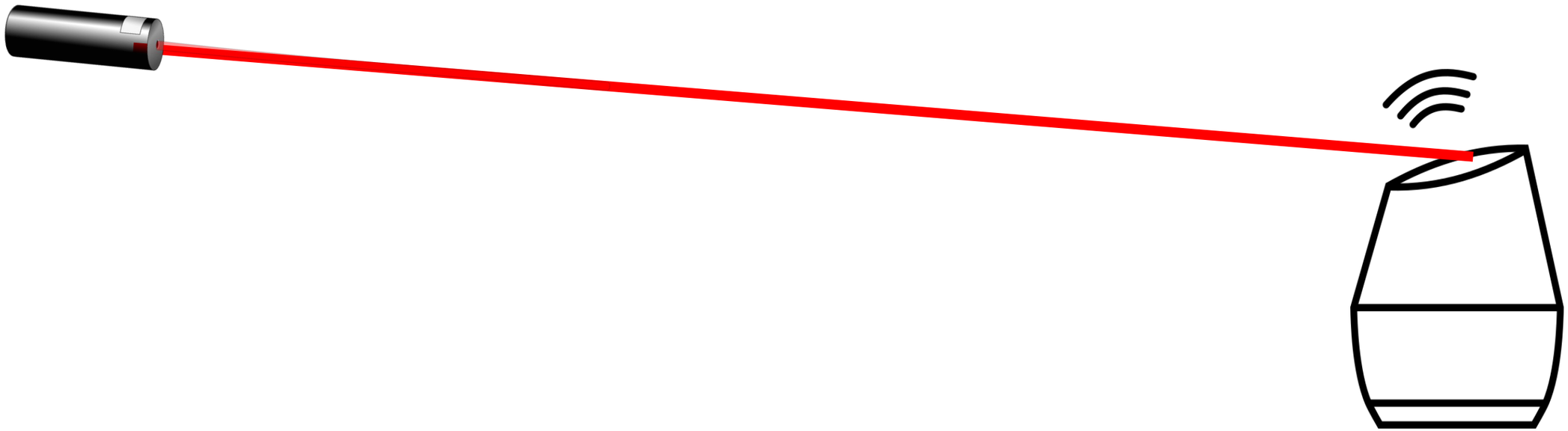


*"Microphones are designed to capture **only acoustic waves**"*

- The unaware systems designer -

The hard truth

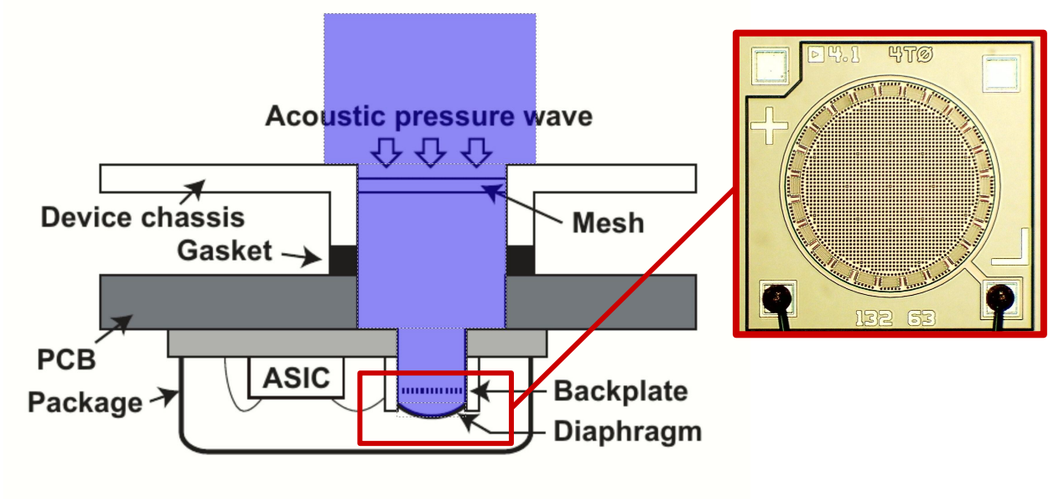
Microphones capture **acoustic** waves **& LIGHT signals**



The agenda

- **How inject light commands** into microphones
- Analyze the discovered **vulnerabilities of voice controllable systems & third-party systems**
- Show how the attack works to **new smart speakers and IoT devices!**
- Describe vendors' **defenses approaches** and changes from the attack release

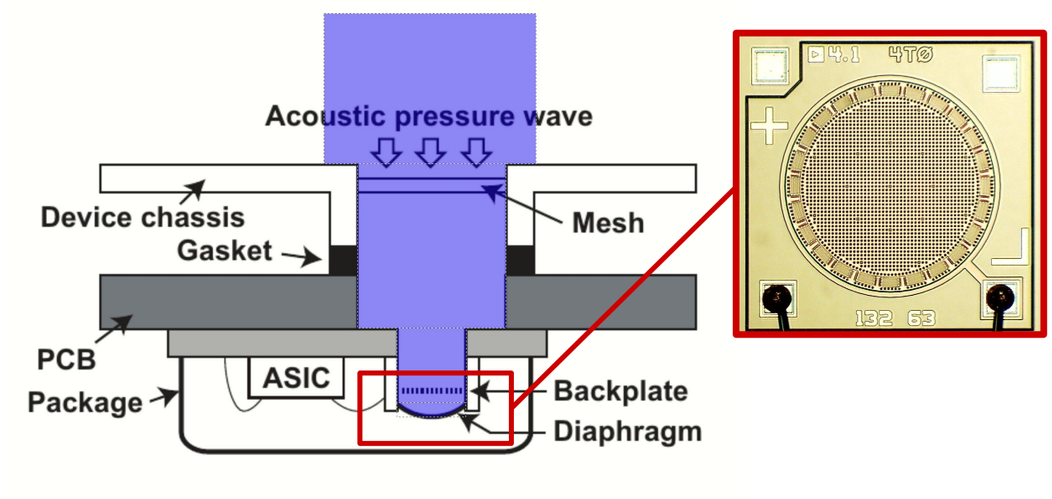
How the attack works



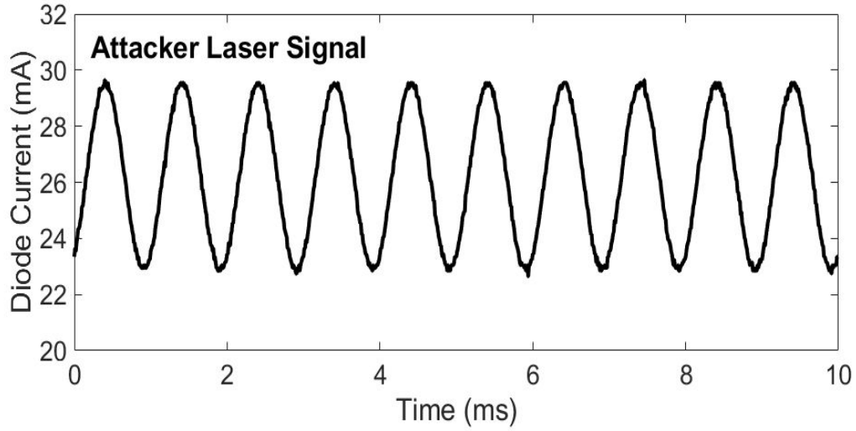
MEMS microphones are affected by light irradiance

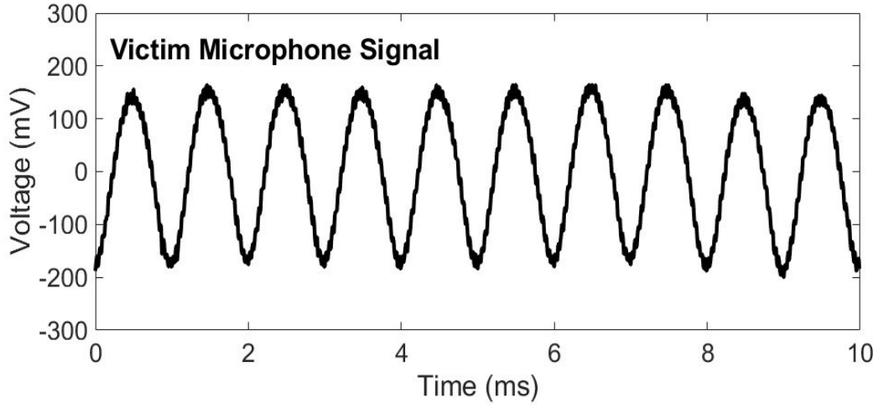
Inject light by modulating optical power (changing the light brightness) change the microphone output voltage

How the attack works



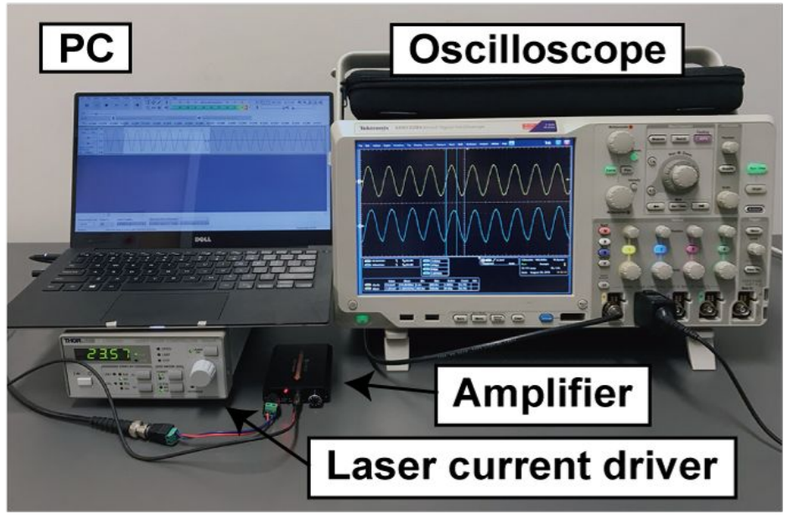
Amplitude modulated light generates a modulated voltage signal in the audio frequency range

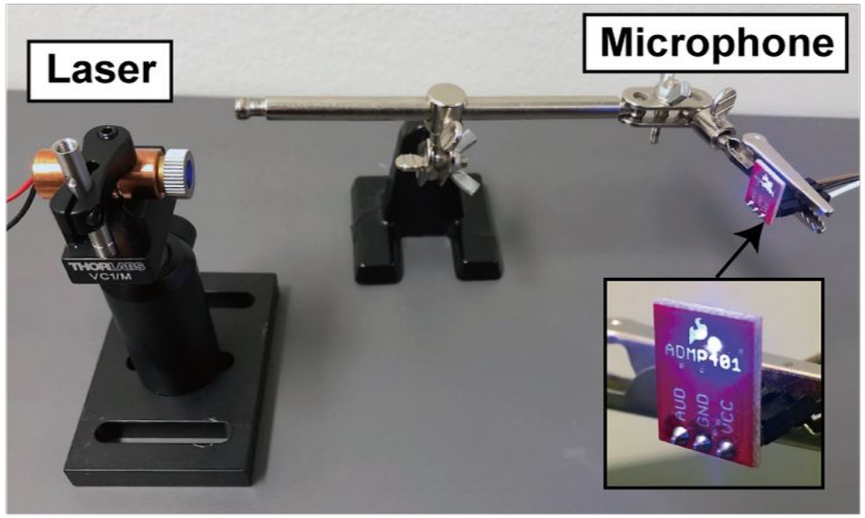


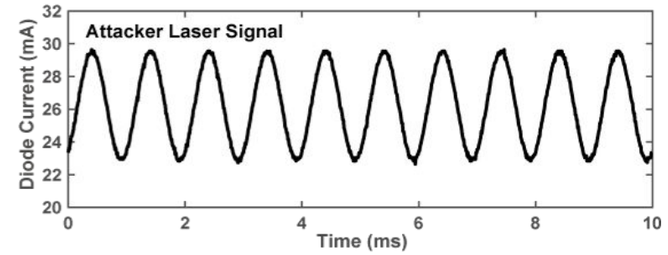


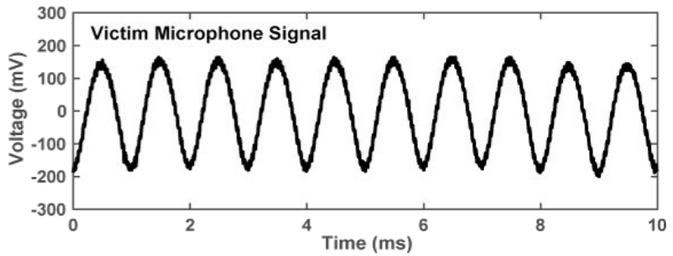
How to inject the audio signal

- The audio signal is recorded or generated using a laptop
- The laser current driver converts the **voltage** audio signal from the laptop audio port into **current** signal + a DC bias
- The generated **current is used to pilot the laser power**



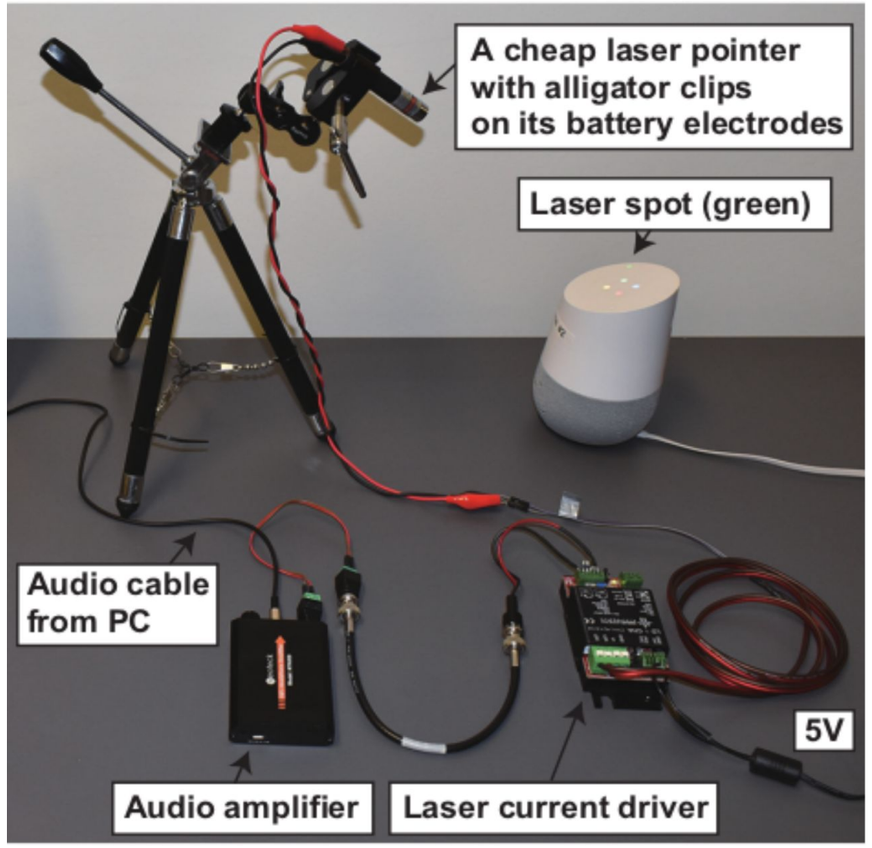




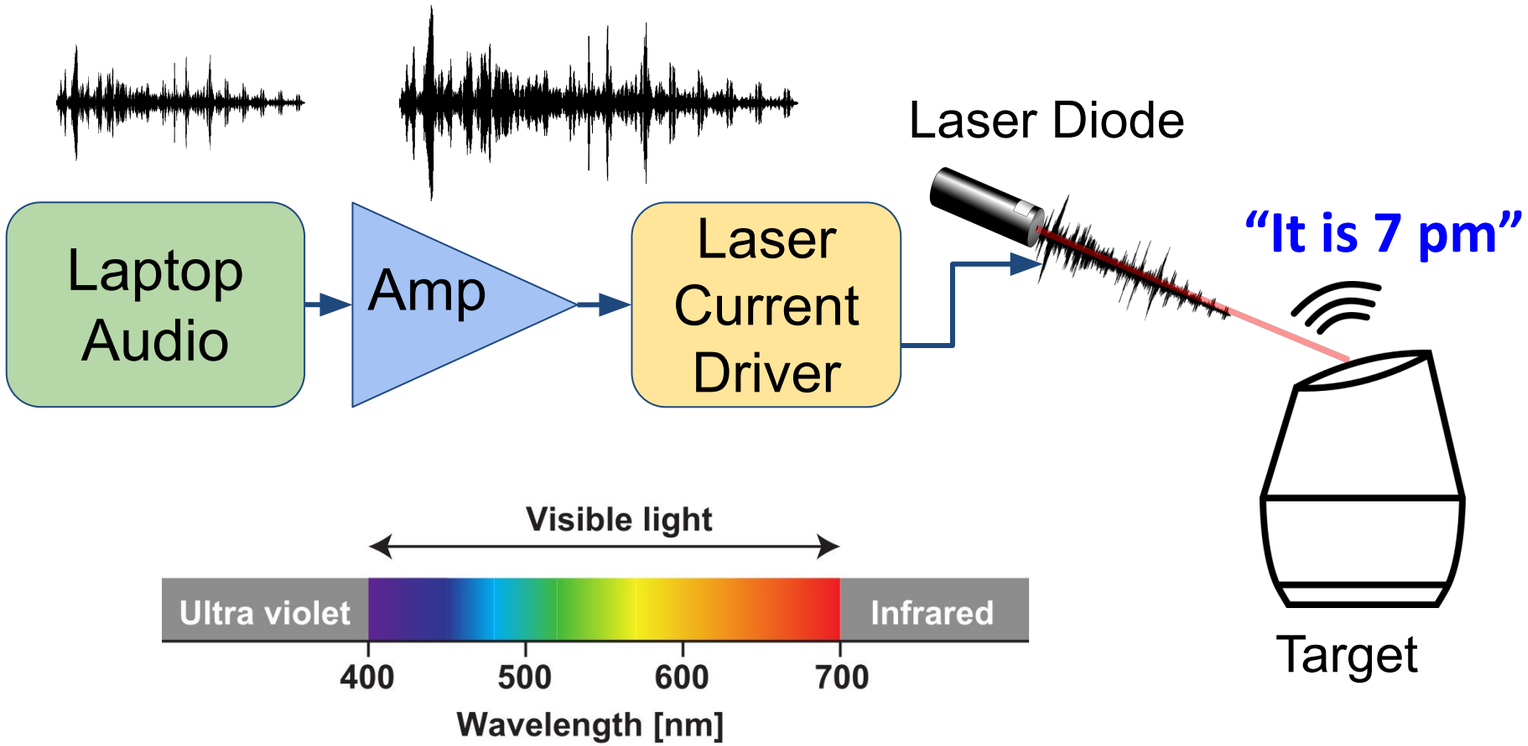


Attacking smart speakers

LIGHT COMMANDS

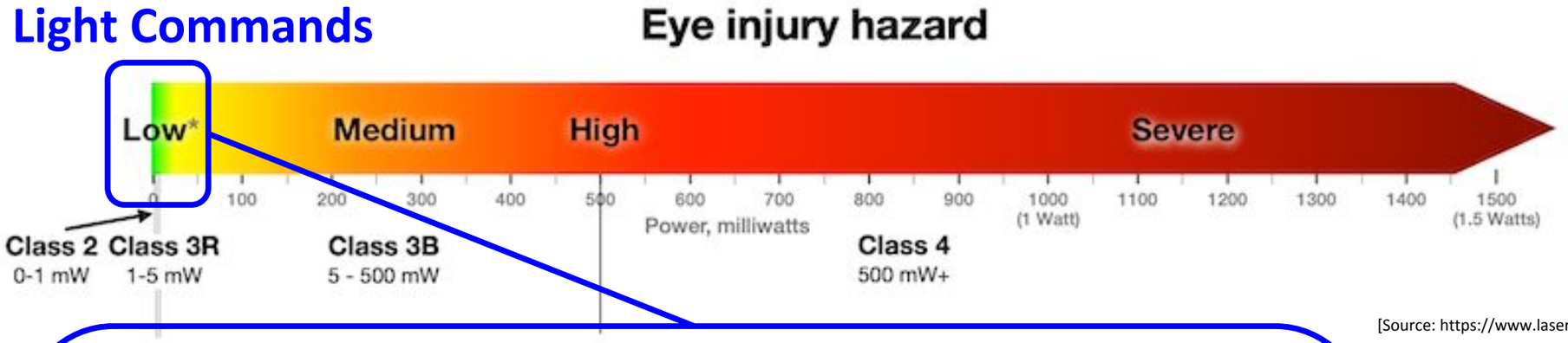


"OK Google, What time is it?"



Notes on safety

Light Commands

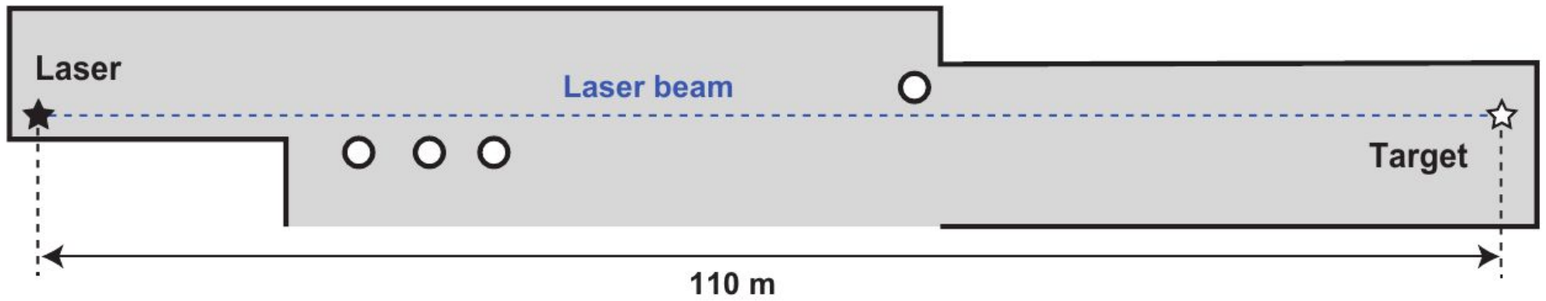


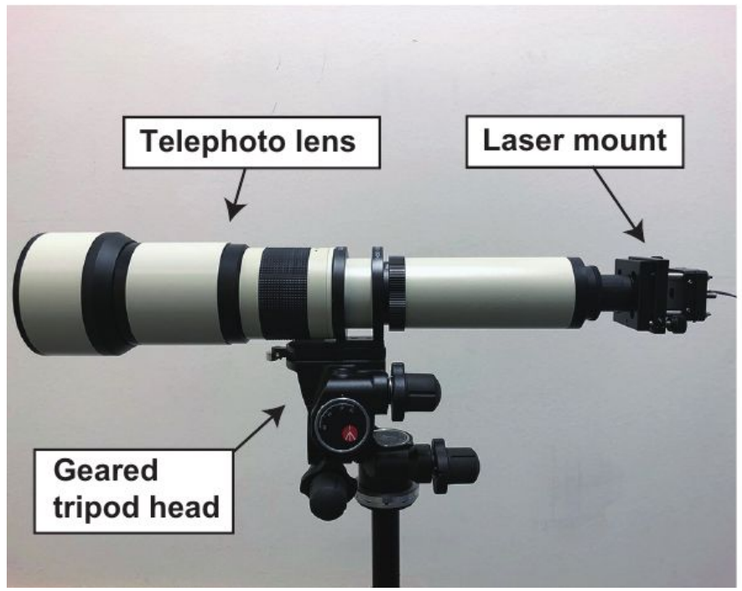
[Source: https://www.lasersafetyfacts.com/}

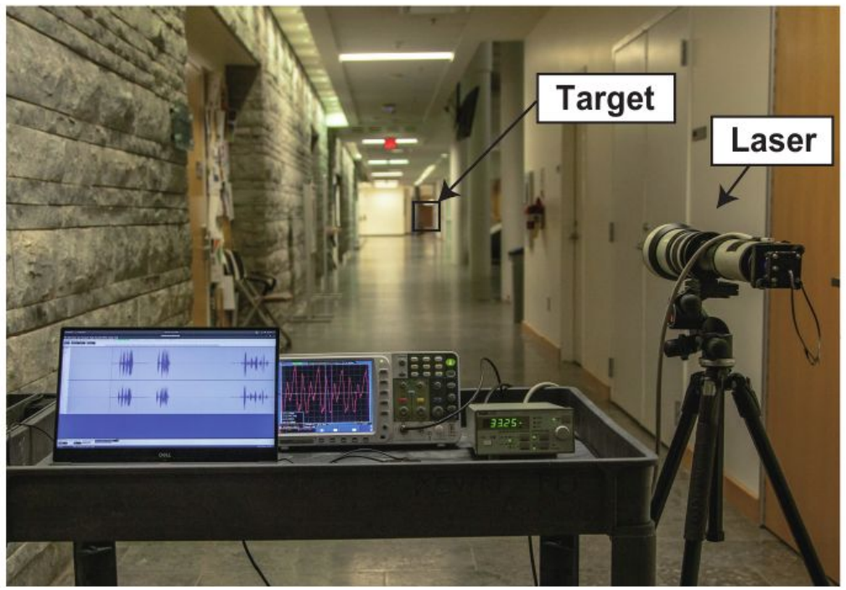
ANSI and IEC laser classification	Class 1		Class 2		Class 3		Class 4
Sub-class	Class 1	Class 1M	Class 2	Class 2M	Class 3R	Class 3B	Class 4
U.S. FDA laser classification	Class I	No special FDA class	Class II	No special FDA class	Class IIIa (definition is different but results are similar)	Class IIIb	Class IV
Human-accessible laser power (for visible light)	For visible light, emits beam less than 0.39 milliwatts, or beam of any power is inside device and is not accessible during operation.		Emits visible beam of less than 1 milliwatt.		For visible light, emits beam between 1 and 4.99 milliwatts.	For visible light, emits beam between Class 3R limit (e.g. 5 milliwatts) and 499.9 milliwatts	For visible light, emits beam of 500 milliwatts (1/2 Watt) or more
Caution/warning indication	No special caution/ warning indication		No special caution/ warning indication		CAUTION	WARNING	DANGER
Label descriptive text		DO NOT VIEW DIRECTLY WITH OPTICAL INSTRUMENTS	DO NOT STARE INTO BEAM	DO NOT STARE INTO BEAM OR EXPOSE USERS OF TELESCOPIC OPTICS	AVOID DIRECT EYE EXPOSURE	AVOID EXPOSURE TO BEAM	AVOID EYE OR SKIN EXPOSURE TO DIRECT OR SCATTERED RADIATION

WARNING: Wear goggles & avoid direct exposure to the beam!

Long range attacks

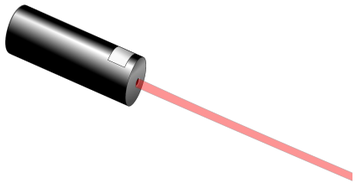






Light Commands: Hacking Voice Assistants with Lasers

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

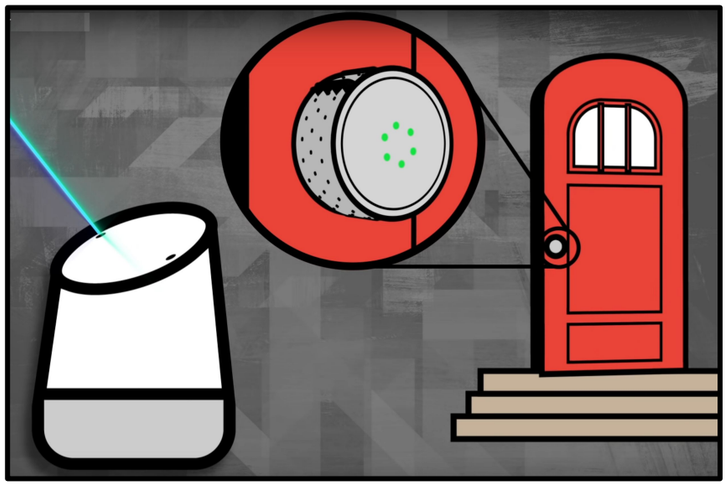
Phones/Tablets

60mW: 5-20 meters

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

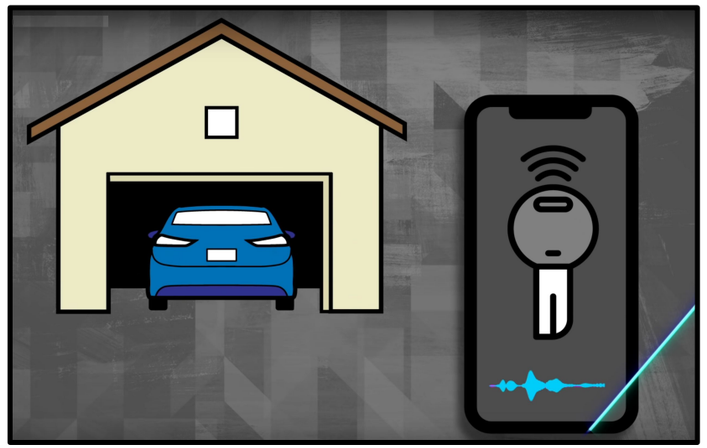
Consequences of the attack

Unlock doors



Turn on/off
Enable/Disable
Change settings

Open trunks
Unlock car
Start engine



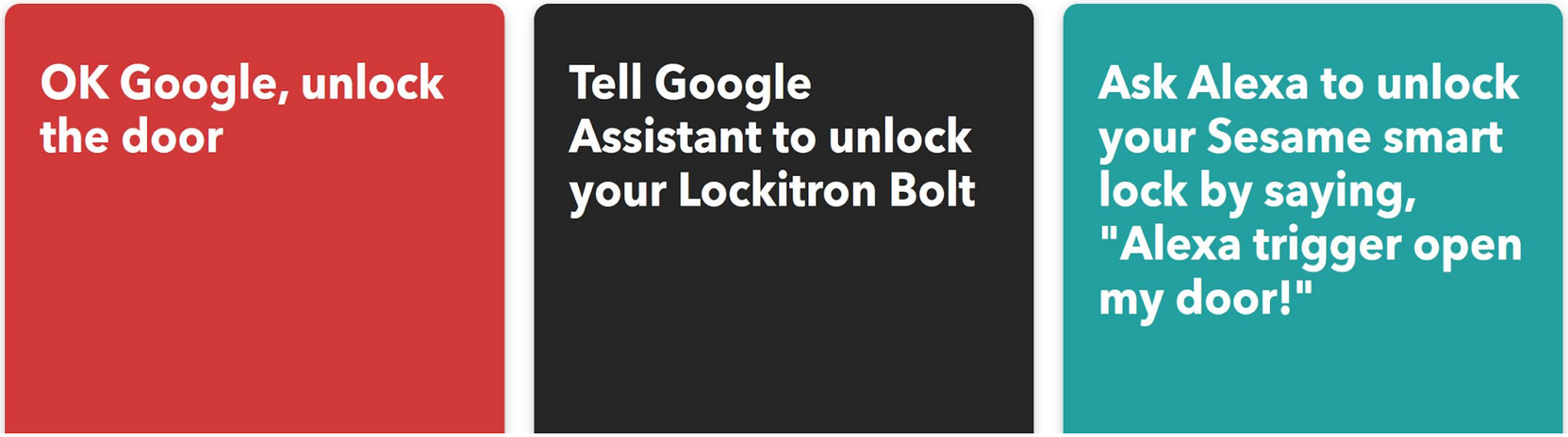
Unauthorized purchases

Personalization is not authentication

- No speaker authentication for smart speakers by default (only personalization)
- Inaccurate speech recognition (e.g. Text-to-Speech)
- Wake up word-only security (e.g. Siri)

Usability VS Security

Apps & routines that can be customized by the user (e.g. IFTTT)



Common security 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..."

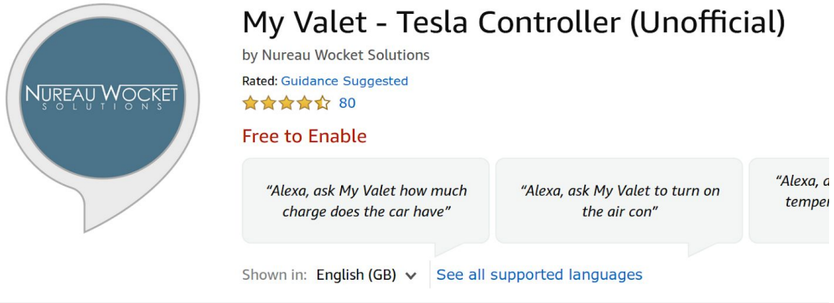
... ...

"438…" "OK, Opening the front door"

Attacking cars

TESLA Model S

1) EV Car integration with Google Home
   - No PIN for unlocking doors/trunk
   - No key proximity required
2) Unofficial apps & Alexa skills
   - no PIN required for certain operations



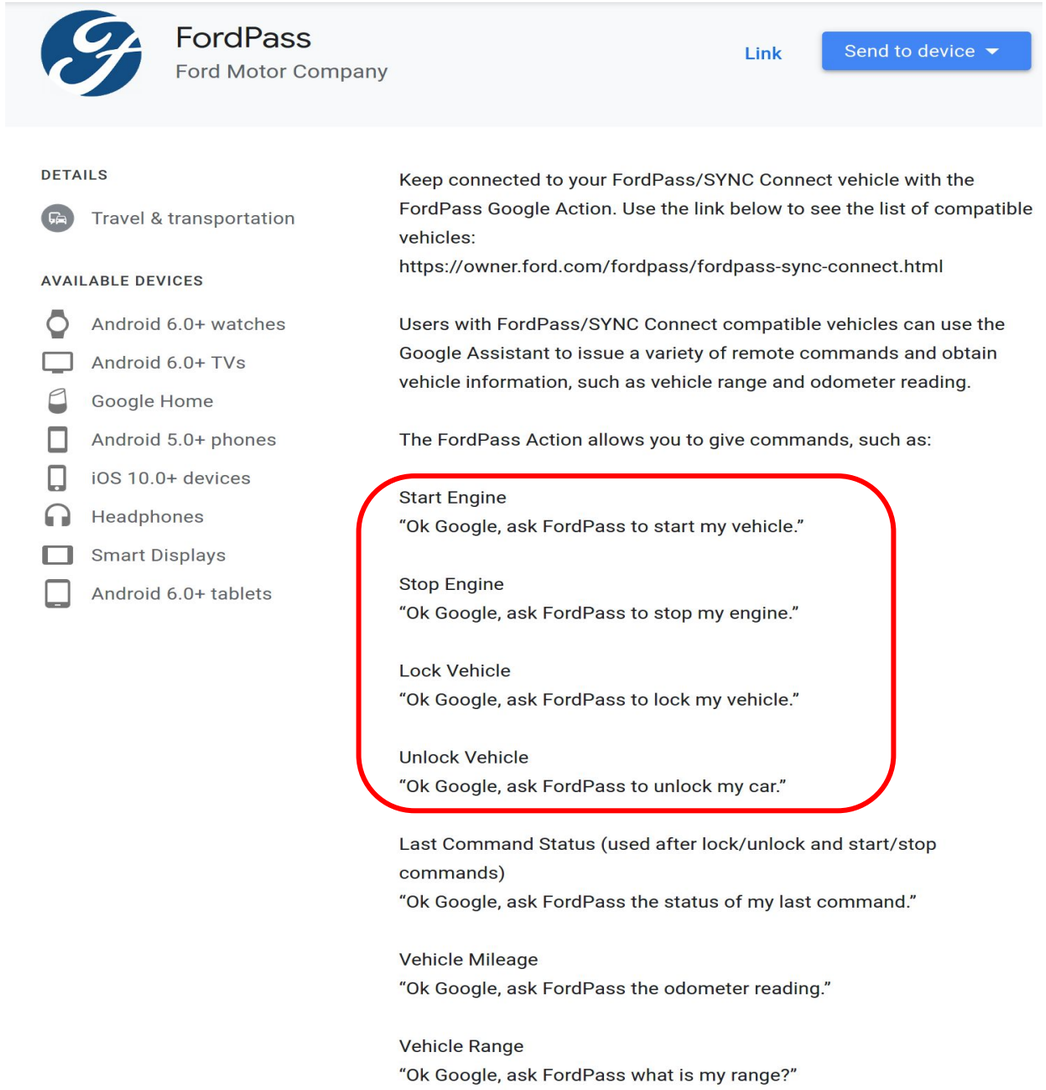
Some examples of what you can ask are:
- can I get to Oxford
- can I get to Colchester with my current charge level
- can I get to Plymouth on my current charge
- how long will it take me to get to Canterbury
- have I got enough battery to get to York
- have I got enough charge to get to Leeds
- close the roof / sunroof
- vent the roof / sunroof
- lock the car
- is the car locked
- what rate is the car charging at
- is the car charging
- when is the car scheduled to start charging
- when will charging begin
- when will charging finish
- how much charge does the car have
- what is the battery level on the car
- what is the range of the car
- how many miles has the car done
- where is the car
- what is the location of the car
- is the car plugged in
- open the charge port
- what is the temperature in the car
- turn on the air con / heating / cooling
- turn off the air con / heating / cooling
- honk the horn
- flash the lights
- start charging
- stop charging
- set the charge limit to XX percent
- set the temperature to XX degrees
- set the air con to XX degrees
- what is the battery limit set to
- what it the name of the car
- what version is the car
- open the frunk
- open the hood
- open the froot
- open the boot
- open the trunk
- open the tailgate
- close the boot
- close the trunk
- close the tailgate

Attacking cars

2019 Ford Escape

FordPass/SYNC 3 integration with Google Home:

- No mechanisms to prevent PIN brute forcing
- Open doors & start engine only using voice



FordPass
Ford Motor Company

Link | Send to device

DETAILS

Travel & transportation

AVAILABLE DEVICES

Android 6.0+ watches
Android 6.0+ TVs
Google Home
Android 5.0+ phones
iOS 10.0+ devices
Headphones
Smart Displays
Android 6.0+ tablets

Keep connected to your FordPass/SYNC Connect vehicle with the FordPass Google Action. Use the link below to see the list of compatible vehicles:
https://owner.ford.com/fordpass/fordpass-sync-connect.html

Users with FordPass/SYNC Connect compatible vehicles can use the Google Assistant to issue a variety of remote commands and obtain vehicle information, such as vehicle range and odometer reading.

The FordPass Action allows you to give commands, such as:

Start Engine
"Ok Google, ask FordPass to start my vehicle."

Stop Engine
"Ok Google, ask FordPass to stop my engine."

Lock Vehicle
"Ok Google, ask FordPass to lock my vehicle."

Unlock Vehicle
"Ok Google, ask FordPass to unlock my car."

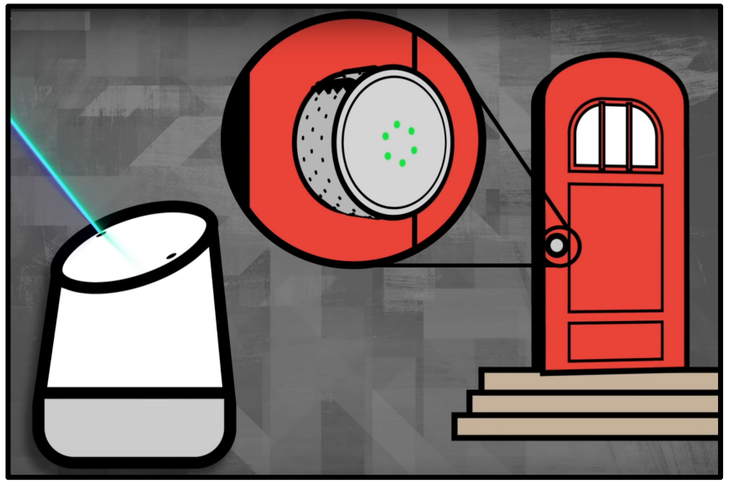
Last Command Status (used after lock/unlock and start/stop commands)
"Ok Google, ask FordPass the status of my last command."

Vehicle Mileage
"Ok Google, ask FordPass the odometer reading."

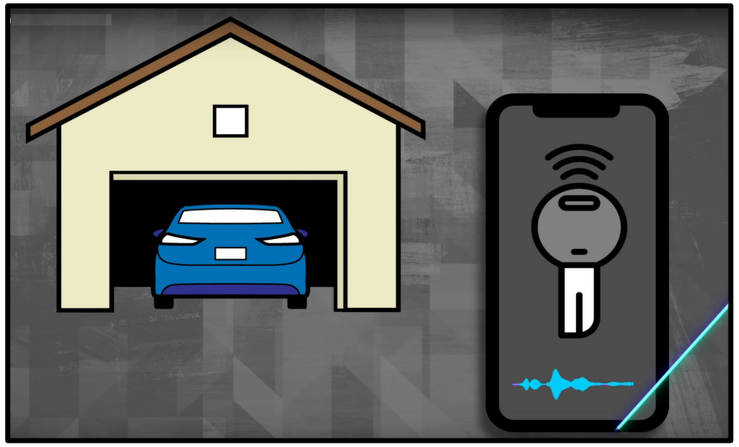
Vehicle Range
"Ok Google, ask FordPass what is my range?"

Patches & changes

Augmented device personalization

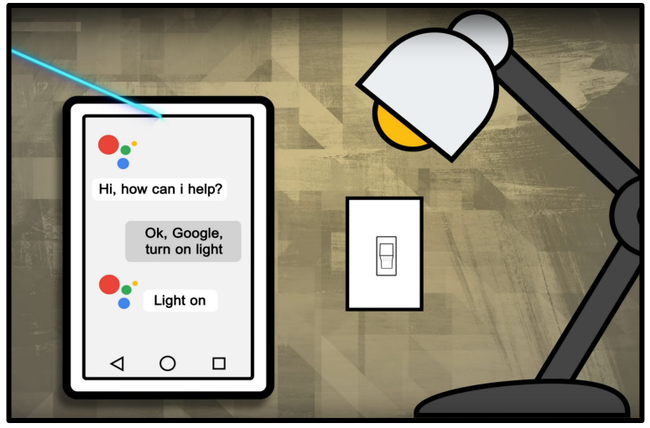


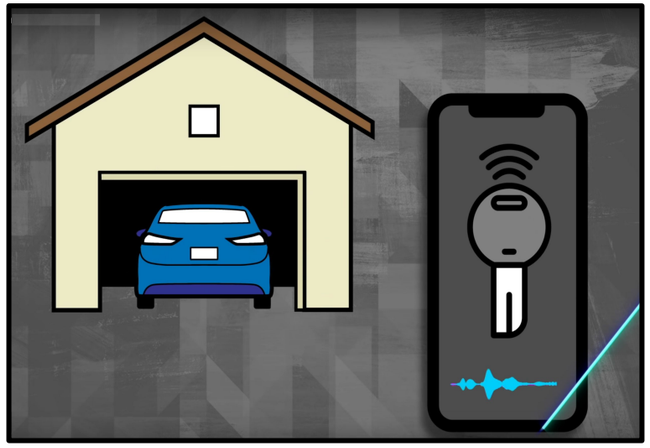
Brute force attacks mitigations



Authorization control & multifactor authentication

Still vulnerable!

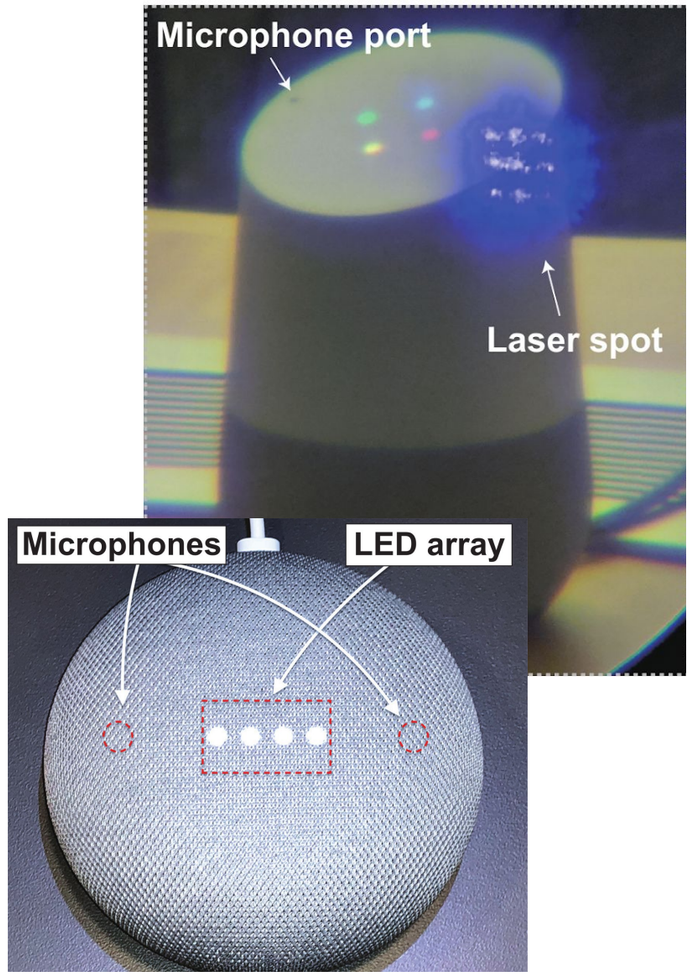




- Apps & services compatible with several IoT devices
- Still IoT devices operations without security checks
- 1 attacked microphone to compromise the VA and connected smart devices

Limitations

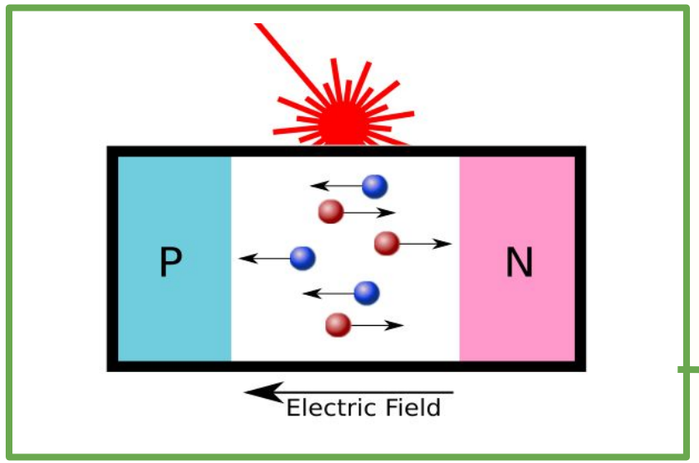
- Dependence on Focusing, Aiming, Acoustic Noise, and Audio Quality
- Requires **Line of Sight**
- Limited **Feedback from the device**

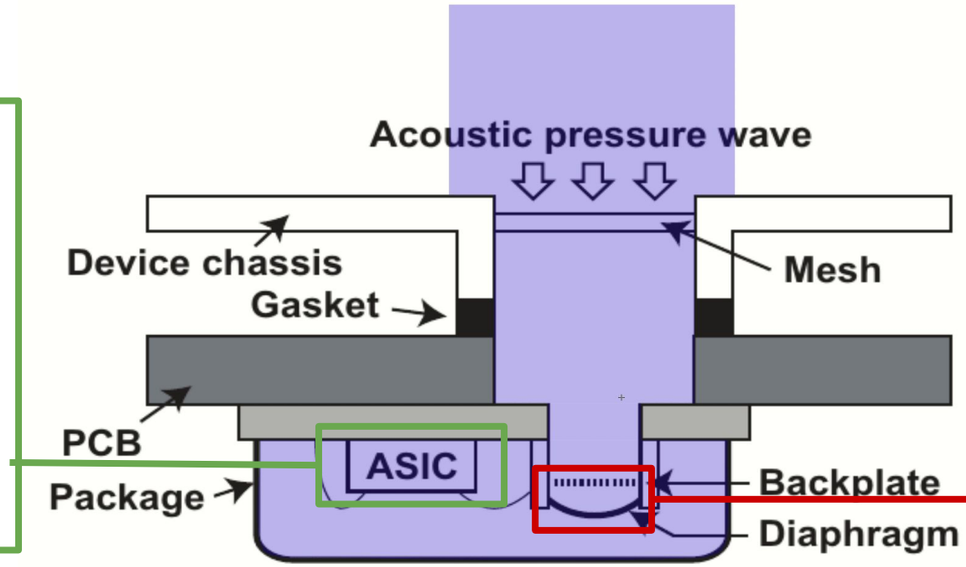


Future research

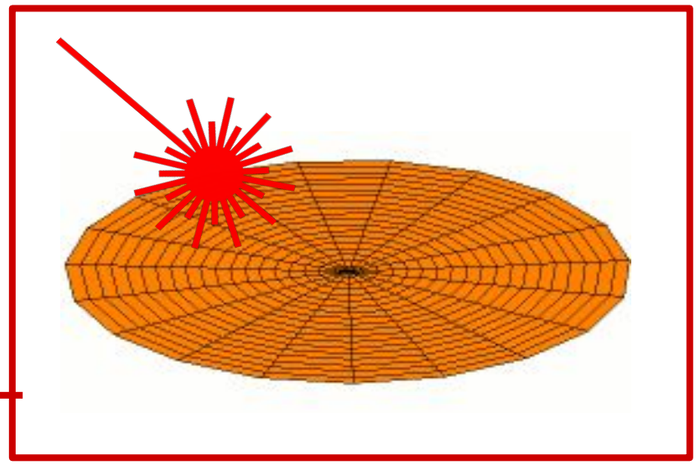
Deep exploration of physical causality:

1. **Photoelectric** Effects on ASIC





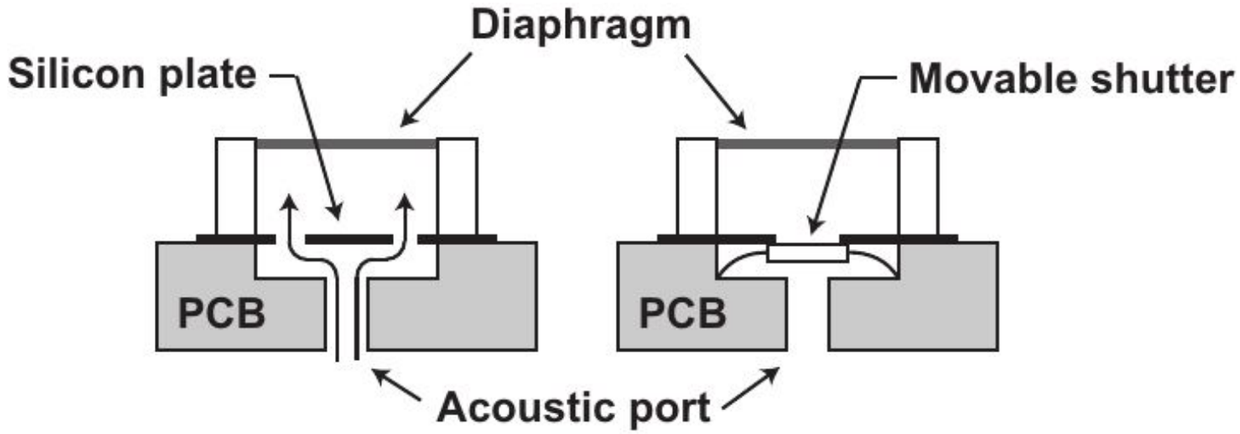
2. **Photoacoustic** Effects on Diaphragm



Future research

- HW design solutions (e.g. microphones and ports design)

- Multiple microphone recognition



Takeaways

- **Sensors can perceive more that what we expect** and what we design them for.
- Consumer electronics and sensors are less protected against malicious injection attacks because the systems blind rely on sensor data. **IoT devices can be attacked through these weak channels**.
- Safety-critical application and systems require a careful SW design to minimize every attack surface, **including from IoT connected to them**
- **Sacrifice of security to promote usability is not always a good idea**

Light Commands

https://lightcommands.com/

Contact us at
LightCommandsTeam@gmail.com

Light Commands: Hacking Voice Assistants with Lasers

Sara Rampazzi - srampazzi@ufl.edu
Benjamin Cyr - bencyr@umich.edu