UCLA Samueli School of Engineering

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

Parangat Mittal, Bharthi Srinivasan, Ercem Yesil
Dept. of Electrical and Computer Engineering

Voice Controllable Systems

[Source: pandaily.com]

[Source: developers.google.com]

Problem

What we think

Microphones work with Acoustic Signals

But,

Microphones work with Acoustic Signals **AND** light signals

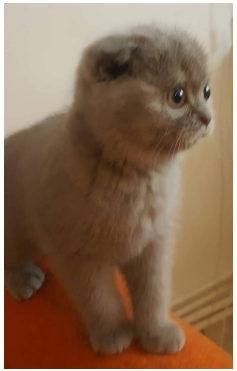
Threat Model

Attacker

- What do they know?
- What is their level of access?
- What is their goal?
- What are their resources?

Victim

- What needs protection?
- How well protected is it?



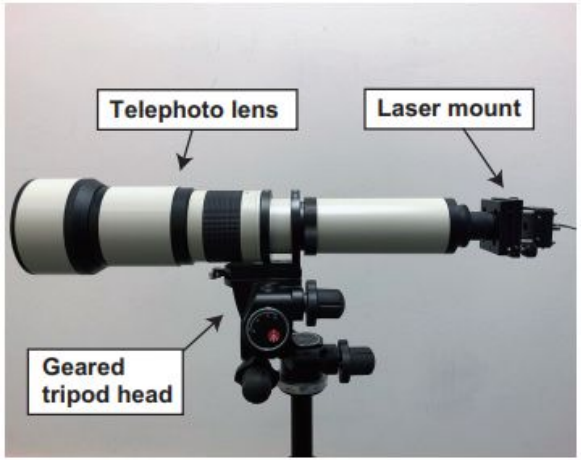
Proposed Contribution

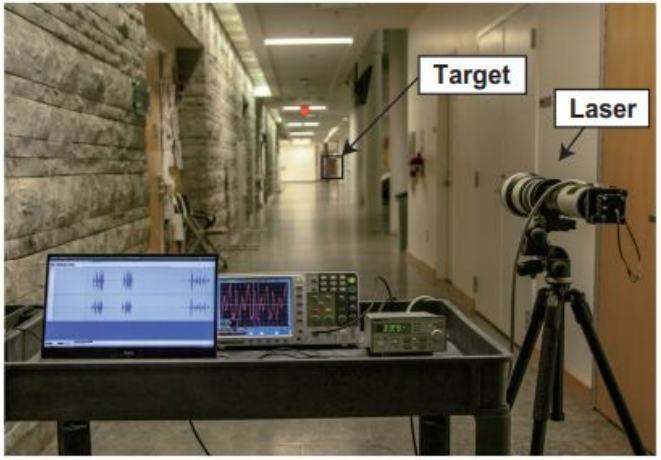
Method of using laser

Transfer low-frequency signal modulated on laser signal envelope.

Device Vulnerability

Microphone openings allow Quantum interactions of light to translate laser to electrical signals.





Proposed Contribution

Target selection

- Most popular Voice Control systems such as Alexa, Siri, Portal, and Google Assistant.

Command selection

- Demonstrate four different voice commands.
- “**What time is it?**”, “**Set the volume to zero**”, “**Purchase a laser pointer**”, and “**Open the garage door**”.

Table 2: Attack success accuracy as a function of distance.

Command	20m	25m	27m
What Time Is It?	100%	90%	0%
Set the Volume to Zero	100%	80%	0%
Purchase a Laser Pointer	90%	0%	0%
Open the Garage Door	100%	100%	0%

Evaluation Methodology

Attack performance demonstration on commercial products:

Device	Backend	Category	Authen-tication	Minimum Power [mW]*	Max Distance at 60 mW [m]**	Max Distance at 5 mW [m]***
Google Home	Google Assistant	Speaker	No	0.5	50+	110+
Google Home Mini	Google Assistant	Speaker	No	16	20	—
Google Nest Cam IQ	Google Assistant	Camera	No	9	50+	—
Echo Plus 1st Generation	Alexa	Speaker	No	2.4	50+	110+
Echo Plus 2nd Generation	Alexa	Speaker	No	2.9	50+	50
Echo	Alexa	Speaker	No	25	50+	—
Echo Dot 2nd Generation	Alexa	Speaker	No	7	50+	—
Echo Dot 3rd Generation	Alexa	Speaker	No	9	50+	—
Echo Show 5	Alexa	Speaker	No	17	50+	—
Echo Spot	Alexa	Speaker	No	29	50+	—
Facebook Portal Mini (Front Mic)	Alexa	Speaker	No	1	50+	40
Facebook Portal Mini (Front Mic)§	Portal	Speaker	No	6	40	—
Fire Cube TV	Alexa	Streamer	No	13	20	—
EcoBee 4	Alexa	Thermostat	No	1.7	50+	70
iPhone XR (Front Mic)	Siri	Phone	Yes	21	10	—
iPad 6th Gen	Siri	Tablet	Yes	27	20	—
Samsung Galaxy S9 (Bottom Mic)	Google Assistant	Phone	Yes	60	5	—
Google Pixel 2 (Bottom Mic)	Google Assistant	Phone	Yes	46	5	—

*at 30 cm distance, **Data limited to a 50 m long corridor, ***Data limited to a 110 m long corridor, §Data generated using only the first 3 commands.

Attack Scenarios

Low-power cross-building attack

- Long distance, precisely aimed, low-power laser attacks.

Authentication attack

- PIN brute forcing, bypassing, eavesdropping.

Car security

- Compromised voice controls such as engine start, open door, park…

Stealthy attacks

- Immediate volume controls, wide range of attack frequencies.

Demo

DEMO #3
THROUGH A WINDOW

Injecting "OK Google, open the garage door" to a Google Home by shining a laser from another building

Countermeasures

Software Approach

Added authentication

- Require the user to do additional steps to complete the requested action such as PIN
- Speaker/User's recognised voice-based authentication

Sensor Fusion

- Verify the validity of the voice command by comparing inputs from multiple microphones (present on most devices these days)

G1.2 - Who Are You (I Really Wanna Know)?

Hardware Approach

Physically blocking light

- Cover the microphone sensor (port) by non-transparent sheets.

Break the Line-of-Sight with Microphone

- Embed the microphone deep inside the device, making it difficult to focus the laser

Related Works

Increased AI, increased risks - fooling autonomous vehicles

- Attacks such as Light Commands physically attack the Microphone sensor on LiDAR based autonomous systems, and the resulting spoofed signals **cause the AV to incorrectly interpret some obstacles and not halt/brake accordingly**.

(Published in 32nd USENIX Security Symposium (2023))

Crimes with AI - physical cyber attacks against the common man

- Another application exploited vulnerabilities in voice-recognition systems. Replicating audio waveforms (some accurate to within 99.9% of the original), researchers sent hidden voice commands to these **smart speakers, making them dial phone numbers or open websites**.

(Published in Crime, Media, Culture: An International Journal)

Q&A