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

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

Usenix Security 2020

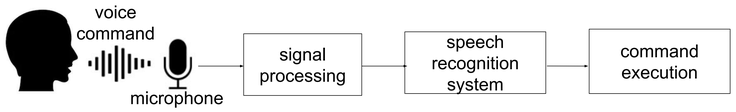
lightcommands.com

Motivation

Voice Controllable Systems (VCS) are increasingly prevalent in many households. These systems (such as Google Home, Amazon Echo, and Siri products) allow users to control an increasing number of smart home systems using only voice commands. This can be extremely helpful to a user, but what new threat vectors do these devices enable?

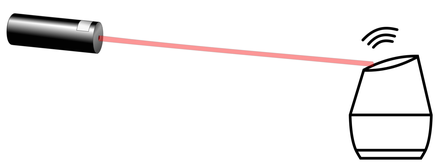
[Source: pandaily.com]

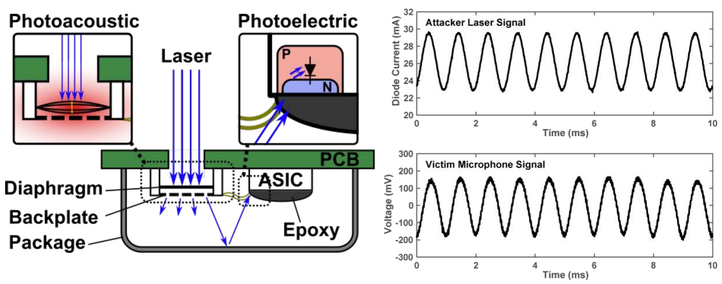
[Source: developers.google.com]



The Problem

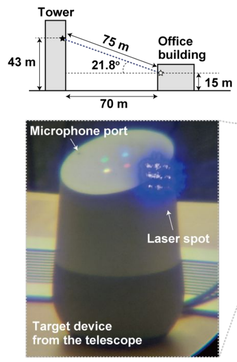
VCS devices are expected to measure acoustic signals via MEMS microphones, so security threats were expected in the acoustic domain. But MEMS microphones are also affected by **LIGHT**! Using a laser, an attacker can inject light signals that are interpreted as voice commands. We call these injected commands **Light Commands**.

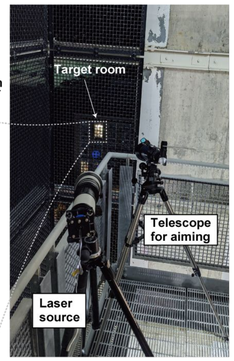




The Attack

Light Commands allow voice commands to be injected into VCSs from long range and through acoustic barriers such as windows. For example, we injected multiple commands into a Google Home from a different building over 75 meters away.





Results

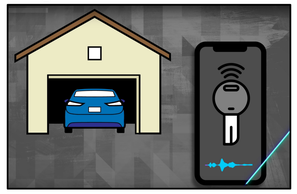
We were able to successfully perform Light Commands on more than 17 different VCSs, each requiring different optical power requirements and distances.

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	-

Consequences

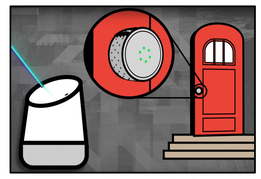
What can be done with Light Commands?

Smart Device Control



Unlock Car / Open Garage

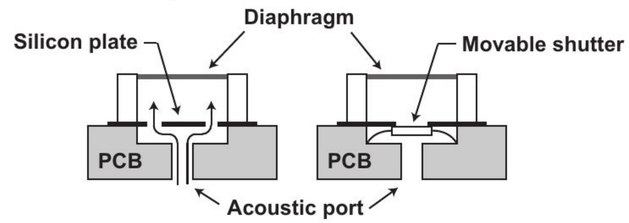
Unauthorized Purchases



Unlock Smart Doors

Potential Defenses

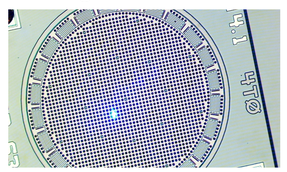
There are many software defenses that exist to ensure only privileged users can use voice commands, but the vulnerability of the microphones is at a fundamental level. New MEMS designs will need to be considered.



Future Work

We are actively investigating the physical causality of Light Commands with precise experimentation. Our preliminary results indicate that multiple photoelectric and photoacoustic phenomena are combining to affect the microphone output.

Our latest results can be found in our follow-up paper published in IEEE SENSORS 2021 [2].



[1] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, “Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems,” Usenix Security 2020, pp. 2631–2648. https://www.usenix.org/conference/usenixsecurity20/presentation/sugawara.
[2] B. Cyr, T. Sugawara and K. Fu, "Why Lasers Inject Perceived Sound Into MEMS Microphones: Indications and Contraindications of Photoacoustic and Photoelectric Effects," *2021 IEEE Sensors*, 2021, pp. 1-4, doi: 10.1109/SENSORS47087.2021.9639744.