# Light Commands

DJ Olaiya
Jasdeep GIll
Patrick Klassen

# Background

- A light command attacks a vulnerability of MEMS microphones that allows an attacker to inject an inaudible and invisible command using light.
- Micro-Electrical-Mechanical System (MEMS) microphones are used in most digital devices, due to the low cost.
- This means that most voice assistants such as Google Home, Siri, and Alexa, are vulnerable

# Motivation

Voice assistants are extremely prevalent in today's society, and are often given power to make purchases upon command. An attack which allows arbitrary commands to be made without warning is an extremely relevant problem.

This attack was discovered last year, which means that there are a lot of avenues to explore to make sure these systems' are secure.

# Project Idea

- Replicate light command attack
- Extend it by piggybacking off the attack and using it to inject malicious code.
- Create a defense that  recognizes  light injected commands based on  a difference in audio quality.

# Problem

We need to first successfully replicate the attack

Then we need to explore ways to extend the attack as well as ways to defend against it

Find a way to differentiate sound coming from a laser and sound coming from someone’s mouth.

# Attack Replication

- In order to replicate the attack we needed the equipment. We were able to obtain most of it from the physics department.
- Equipment used:
- Laser Driver
- Sound Amplifier
- Amazon Echo 2nd gen
- Google Home
- Oscilloscope

# Setup

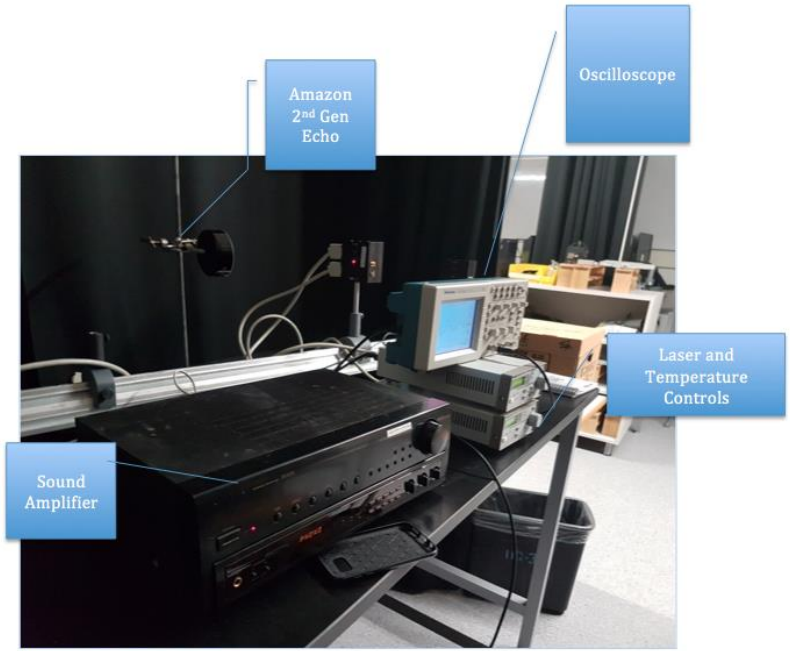


Figure 5 Macro view of the Setup

# Challenges

Originally tried to parallelize the objectives by working on replicating the attack and extending it independently.

Attack Extension: Worked on writing an Alexa skill. Amazon marketplace vetting, and malicious software updates not possible.

Attack Replication: We were unable to replicate the attack prior to shutdown of classes.

# Reasons for Failure

- Laser was not generating enough power to activate microphone

- Software patch might have been implemented already to prevent such an attack.

# Future Steps

Take project in new direction

# Questions