International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Frequencies and Lights Affecting IoT Devices

Shaveta Bhatia, Rishi Singh, Raas Khanna, Madhur Gupta, Vaishnavi Kaushik;

Abstract: ***IoT devices are everywhere, they are readily available to everyone around the world. These devices are predominately controlled via voice command. During my research I asked how we can prevent these devices from listening to us and are there any security risks associated with them. This led me to find articles on light commands where an intruder can point a laser at your hub and gain access to your IoT devices such as door locks and lights. We dive into the workings of a MEMs devices, which is included in all voice-controlled devices including your phone. We explore ways to attack these voice-controlled devices in order to gain access to them. Now ways of preventing these devices to listen to us we can project a frequency that our ears cannot hear but these devices can pick up thus interfering with their microphones and improving our privacy without being a hassle to us. The frequency, (40 kHz) we use to jam these microphones theoretically should not be able to interfere with these microphones, but they do because of this frequency shadow that occurs. This shadow frequency is very interesting because you can do various things other than just jamming microphones for example data communication up to 4kbps and even use this in order to prevent unauthorized recordings of live performances and movies at the theaters.This findings can be applied to various fields where privacy is a key factor.***

Keywords: Alexa, communication, google home, inaudible frequencies, IoT devices, machine learning, MEMS devices, privacy, Siri, security in IoT, ultrasonic frequencies, voice to light modulation.

I. INTRODUCTION

Doesn't the idea of IoT and devices constantly listening to you scare you? The thought that from a distance anyone with the right credentials gets access to your house and controls anything from the lights to the tv and much more. Or the fact these devices are constantly listening for a "wake phrase/word" and might in fact be spying on us without us even knowing.There are numerous ways to tackle these things from playing a high pitch noise that we cannot hear but the microphones can pick up to disconnecting their power when you're away from your home. Millions of devices that are IoT controllable have been sold throughout the world. This includes things like Alexa, Siri, google home and many others. The use of voice only authentication leaves many people and their devices vulnerable.

Revised Manuscript Received on June 15, 2020.
* Correspondence Author
Dr. Sheveta Bhatia*, Head, Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Haryana, India. E-mail: sheveta.fca@mriu.edu.in
Rishi Singh, Student, Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Haryana, India. E-mail: rishisinghjfk@gmail.com
Raas Khanna, Student, Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Haryana, India. E-mail: raask2701@gmail.com
Madhur Gupta, Student, Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Haryana, India. E-mail: madhurgupta3356@gmail.com
Vaishnavi Kaushik, Student, Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Haryana, India. E-mail:vkharidwar2000@gmail.com

What I found while researching these crucial questions that enticed me was that light can influence MEMS(Micro Electrical-Mechanical System) microphone. This can allow strangers to simply enter a voice command then transfer it over a laser, in turn unlocking your door, if pointed in the right direction. Microphones are everywhere from our smartphones to our smart speakers and everything in between. Being paranoid that these things are constantly listening to us is perfectly normal. Fun fact humans cannot hear frequency leaves more than 20 kHz, whiles microphones can capture sound at 24 kHz. Although microphones max out 24 kHz research at the University of Illinois created a frequency of 40 kHz which is both outside of the human and microphone range yet still is audible by microphones.

II. FINDINGS

Now we must find out how these things work; what tools are being used to achieve such things and how we may be able to use these things to our advantage. Voice controlled systems (VC) play a gigantic role in IoT devices at a residential level. These VCs usually accept commands in the person's native language,Hindi, English, Spanish and many more. This command is then used to connect with another IoT device like a door lock on your home and unlock it. Looking at the fundamentals of VC systems there are three components that it's made of: speech recognition, voice capture and command execution. The voice capture system takes the input in this case from your voice into electrical signals. After this the speech recognition system built inside the device is analyzing the audio for a wake word ("hey Siri" for apple products, "Alexa" for amazon products and so on.) after acquiring the wake word, it interprets the audio and executes the command.

A. Methods to attacking VCs

There has been various research done on how to attack these voice- controllable systems before, this includes malicious command injection, where a smartphone device would play a command using text to speech software into a nearby voice controllable system. This synthetic audio was audible to humans nearby. Another way to attack is called kill squatting attack, this is where the intruder tries to confuse the voice controlled system, causing it to infer what was said and issue the correct command while the humans in the room may not think anything of it.

B. MEMS Microphones

MEMS can be known as the integration of mechanical components onto a chip, in order to better utilize the space. MEMs microphone is our primary focus as these are found embedded in popular devices found around the world due to their small footprints and low prices.

The first column of Figure 1 shows the construction of a typical backport MEMs microphone, which is composed of a diaphragm and an ASIC circuit. ASIC microphones have three main functions, it works as an amplifier, an ADC for the digital microphone and a charger for the capacitors inside. This is a thin diaphragm that flexes when hit with an acoustic wave. The fixed back plate and the diaphragm work as a parallel-plate capacitor, whose capacitance changes because of the Diaphragm's mechanical deformation due to its response to the alternating sound pressure. Lastly, the ASIC die converts the capacitive change to a voltage signal on the output of the microphone. The microphone is on the
printed circuit board that is then fitted inside your phone. There is a small gap left to expose the diaphragm. Figure 1 is used to
demonstrate what a MEMS microphone looks like and how it works.

C. Penetrating the VC System

Using lasers to gain access to MEMs devices of our choice is a simple task. We have to choose a laser that we can modify and get a continuous 5 mW laser beam. Then we have to aim the laser beam at or target. We use a recording device to record our command and send it through an oscilloscope to observe its amplitude and frequency to be further processed and be shot through the laser onto our target. We used the current driver to modulate a sine wave on top of the diode's current Itvia amplitude modulation (AM), given by the following equation:

$$I_t = I_{DC} + I_{pp} \sin(2\pi ft) \quad [3]$$

where I_{DC} is a DC bias, Ipp is the peak-to-peak amplitude, and fis the frequency. In our case, we set IDC = 26.2 mA, I_{pp} = 7 mA and f= 1 kHz, where the sine wave was generated using an on-board DAC on a laptop computer, and was supplied to the modulation port on the current driver through an audio amplifier.
Once the laser is pointing at the device and the audio has been processed you are ready to send your command over. This command may be to unlock an IoT device such as a door lock to your front entrance, or even the temperature to unbearable levels inside your own home.

D. Machine learning

Machine learning is a branch of Artificial intelligence that usually helps automate tedious tacks as well as learn to improvise on tasks given enough time to learn. There are three main types of machine learning methods: Supervised learning, Unsupervised learning, and implementing machine learning using the supervised method to help you align the laser to send to hit your target can have huge impacts. This will decrease the amount of time an attacker needs to set up and infiltrate the secure location. Machine learning can also be used to detect if someone is shining a laser into your home and alert, thus greatly reducing the chances of you being a victim of a crime.

E. Ultrasonic frequencies

Now a way to prevent this and all devices from listening to you would be to produce a frequency that humans in the room cannot pick up but the devices can. This will interfere with any culprit that might try to manipulate your IoT devices for their own gain and improve your privacy. There has been research done on how you can produce a frequency without it affecting the humans. If you produce a frequency between 40k and 50k which is practically ultrasound.[2] Any regular microphone theoretically should not be able to pick it up. But research shows that this frequency creates a sort of shadow that the microphones are able to pick up. The pressure change in the diaphragm of the microphone picks up something thus making all other sound getting inside the diaphragm inaudible. Producing this frequency is not easy but if done right you can even transfer data through it. Although the speed is limited to around 4 kbps, this can still be very vital in critical situations. When playing at this frequency we are basically jamming the microphones in the devices nearby. This is because when we play the ultrasound frequency the automatic gain control circuit built into the microphones lowers and thus making it ineffective at picking up audio. This is because microphones face a huge difficulty when dealing with a variation of volume while humans do not. A jamming technique that is used today is a sort of white noise to rude the signal to noise ratio of the target device. The white noise that has been created does not affect humans at all, they do not even know that there is anything playing around them. This is due to the limitation of the human ear and how it is not able to pick up on sounds above 24k frequency. This allows you to implement and play this white noise and have complete privacy wherever you like. This includes things like military bunkers and government building where things are classified and need to stay that way. Though it should be that anyone that has a hearing aid will be affected due to their microphone being affected as well. The use of phones and their ability to call each other and exchange information will also be limited due to their frequency.

III. CONCLUSION.

There are many limitations and disabilities when it comes to the safety and security of our home and personal devices. It is our job to know their vulnerability and try to ensure that due to them we will not fall in the face of danger. In this research paper I have shown you a typical MEMs microphone and how it picks up audio. These devices are then put inside of your smart voice-controlled systems like Alexa and Siri. These voice-controlled systems are now integrated with our smart homes and many other IoT devices that can pose a risk to us if we don't understand their vulnerabilities. These voice-controlled systems can be manipulated through lasers and be used against us in our own homes. Therefore,it is recommended that you have your voice-controlled devices pointed away and not viewable from an outside window, this will ensure your security and the integrity of your own home. Further along we talked about how we can ensure our privacy engaging a speaker to play at a frequency that humans cannot hear at, but the microphones can pick up. This can be used in indispensable locations where privacy matters above all. I hope you use this information to your advantage and ensure your safety by keeping this IoT devices away from windows to make it harder for intruders to use these techniques to break into your home.

The things discussed in this article can be used both for good and bad. Companies can make it their responsibility to add additional features to their products so intruders cannot invade the privacy of their users. Companies can also implement the ultrasonic frequencies into their board meetings this way their trade secrets are not leaked, and no one can use their devices to gain information to commit insider trading. This information can benefit both individuals and companies alike.

REFERENCES:

1. T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, K. Fu, (2020/04), Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems. https://www.researchgate.net/publication/338126679_Light_Commands_Laser-Based_Audio_Injection_Attacks_on_Voice-Controllable_Systems
2. N. Roy, H. Hassanieh, R. Choudhury, (2020/04), BackDoor: Making microphones hear inaudible sounds. https://synrg.csl.illinois.edu/papers/backdoor_mobisys17.pdf

AUTHOR PROFILES

Dr. Sheveta Bhatia, sheveta.fca@mriu.edu.in, Head of Computer Applications department at Manav Rachna International institute of research and Studies.

Rishi Singh, rishisinghjfk@gmail.com, student at Manav Rachna International institute of research and Studies.

Raas Khanna. raask2701@gmail.com, student at Manav Rachna International institute of research and Studies.

Madhur Gupta, madhurgupta3356@gmail.com, student at Manav Rachna International institute of research and Studies.

Vaishnavi Kaushik, vkharidwar2000@gmail.com, student at Manav Rachna International institute of research and Studies.