

Rapport d'une **attaque** Injection audio par laser



Commandes de lumière : Injection audio par laser sur les systèmes à commande vocale

SKIKER Hicham – skikerhicham@gmail.com

Février 2021

TABLE OF CONTENTS

I – Introduction & contexte	4
II – vcs voice command systems	9
III – Problématique & solutions	11
III.1. Context & Objectives	11
IV. Explication	15
IV.1.1. MEMS	
IV.1.2. Plan d’experience	15
IV.1.3. Results	18
V. Scénario d’attaque	24
VI. Solutions et propositions Mr. Benjamin ainsi (mes opinions)	30
VI.1. Solutions	30
VI.2. Propositions	30
VIII. Conclusion	36
Annexe	

I – Introduction

Dans cet article de Mr. Benjamine et son équipe ont proposés une nouvelle classe d'attaques par injection de signal sur les microphones en convertissant physiquement la lumière en son. Un attaquant peut injecter des signaux audio arbitraires dans un microphone cible en dirigeant une lumière modulée en amplitude vers l'ouverture du microphone. Ensuite comment cet effet conduit à une attaque par injection de commande vocale à distance sur des systèmes à commande vocale. En examinant divers produits qui utilisent Alexa d'Amazon, Siri d'Apple, le portail de Facebook et Google Assistant, après cette équipe à montrer comment utiliser la lumière pour obtenir le contrôle de ces dispositifs à des distances allant jusqu'à 110 mètres et à partir de deux bâtiments distincts.

Montrer l'authentification des utilisateurs sur ces dispositifs fait souvent défaut, ce qui permet à l'agresseur d'utiliser des commandes vocales par injection de lumière pour déverrouiller les portes d'entrée protégées par un smart lock de la cible, ouvrir des portes de garage, ou même déverrouiller et démarrer divers véhicules connectés au compte Google de la cible (par exemple, Tesla et Ford). Enfin, conclure avec les éventuelles défenses logicielles et matérielles contre ces attaques.

I - Contexte

Injection audio par laser sur les systèmes à commande vocale, constitue un risque d'attaque dans une vaste applications : voiture, bâtiment, téléphone, tablette.

II. vcs

Voix contrôlée par systèmes :



Un microphone est un capteur qui permet de transformer un signal sonore en un signal électrique que l'on peut visualiser à l'oscilloscope.

Le signal vocale est transmis via microphone soit un message correct ou non correct, le microphone le traite automatiquement en transformant ce signal acoustique en signal électrique, ce dernier porte notre information c'est le code, après cette étape c'est l'exécution d'ouvrir la porte. En effet nous possédons deux cas soit le code « 123 » qui va générer un message "mot de passe erroné, Essaie encore..." ou code « 456 » qui va générer un message "mot de passe correct" et donc automatiquement la porte va s'ouvrir.

III. Problématique

Les microphones captent les signaux acoustiques et les **signaux lumineux**.

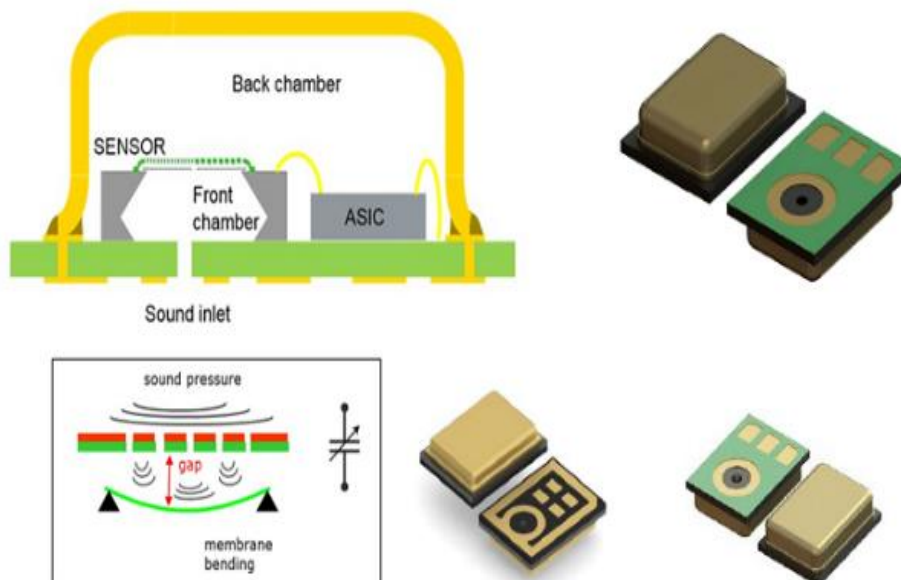
En effet les microphones captent les signaux acoustiques, mais aussi les signaux lumineux, Cela constitue une faiblesse dans ces gadgets.

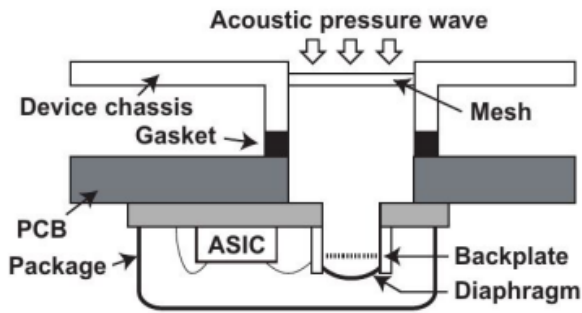
VI. Explication

VI.1.1. MEMS

Les microphones à base de MEMS Micro-Electro-Mechanical-Systems,

Le diaphragme des MEMS forme un condensateur et les ondes de pression sonore provoquent le mouvement du diaphragme. Les microphones MEMS contiennent généralement une deuxième puce à semi-conducteur qui fonctionne comme un préamplificateur audio, convertissant la capacité changeante du MEMS en un signal électrique. La sortie du préamplificateur audio est fournie à l'utilisateur si un signal de sortie analogique est souhaité. Si un signal de sortie numérique est souhaité, un convertisseur analogique-numérique (ADC) est alors inclus sur la même puce que le préamplificateur audio.





Etape n°1 :Le diaphragme et la backplate

Fonctionnent comme un condensateur, à cause de la vibration de la membrane.

Etape n°2 : Lorsque le diaphragme se déplace, il provoque une modification de la capacité

Etape n°3 : The ASIC convertir le changement de capacité en signal voltage .

A ce stade on aura un signal instantané avec une amplitude donnée.

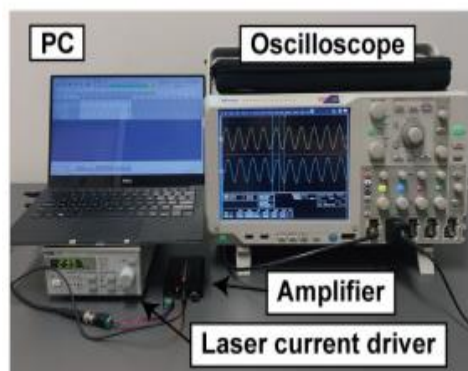
VI.1.2. Plan d'expérience

Injection signal laser

Préparation une expérience pour injecter signal laser avec un cible même caractéristique de notre victime .

Le Signal de tension audio provenant d'un ordinateur portable après amplifié.

- La puissance de sortie du laser est proportionnelle au courant

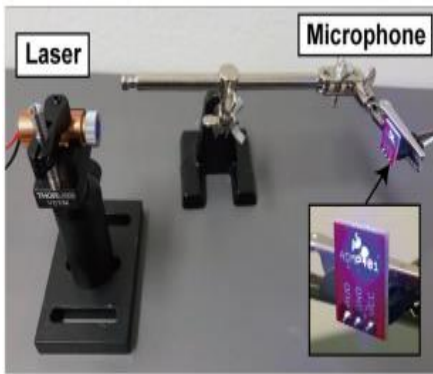


Pc + enregistreur audio +Laser+ Ampli+ driver de courant

Dans cette phase c'est tester la faisabilité de l'injection de signaux.

Pour montrer la faisabilité de l'injection de signaux composée d'un pilote de courant laser, PC, Amplificateur audio, et oscilloscope.

Ainsi un plan d'expérience avec une miroir pour réflexion les rayons transmises, et une source de laser afin de générer notre signal pour attaquer la victime.

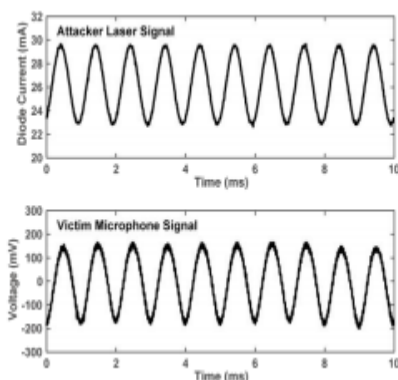


Source de laser +microphone +miroir pour réflexion

Benjamine à effectuer plusieurs expériences pour déterminer le Choix du laser. Enfin, les niveaux de signal audio injecté sont dans la même gamme et les formes des courbes de réponse en fréquence sont également similaires. Par conséquent,

La couleur n'est pas une priorité dans le choix d'un laser par rapport aux autres facteurs de création de Light Commands. Dans ce document, nous utilisons systématiquement le laser bleu de 450 nm principalement pour les raisons suivantes :

- (i) disponibilité de diodes de haute puissance
- (ii) l'avantage focalisation en raison d'une longueur d'onde plus courte.

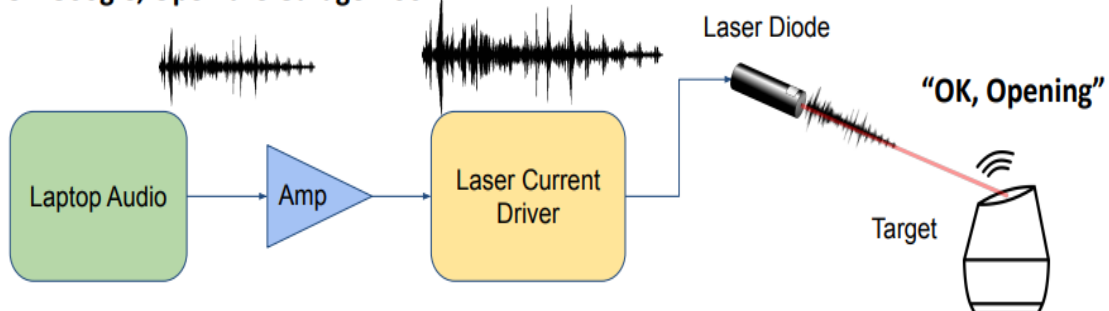


Le résultat entre le signal laser de notre victime et signal de l'attaquant est presque la même :

- ✚ La lumière modulée en amplitude génère une tension
- ✚ Signal sur la sortie du microphone.
- ✚ Lumière d'amplitude supérieure est presque la même tension d'amplitude supérieure
- ✚ Très peu de distorsion.

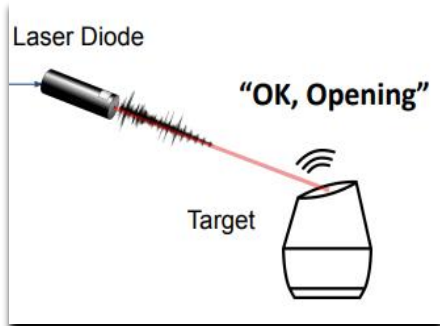
▪ Attaque par signal laser

"OK Google, Open the Garage Door"



▪ Victime signal microphone

Le message vocable est enregistré dans le laptop envoyé à travers un amplificateur, ensuite Envoyé dans le bloc laser current driver pour le transmettre vers une laser diode monofréquence ciblé sur notre capteur vocale.

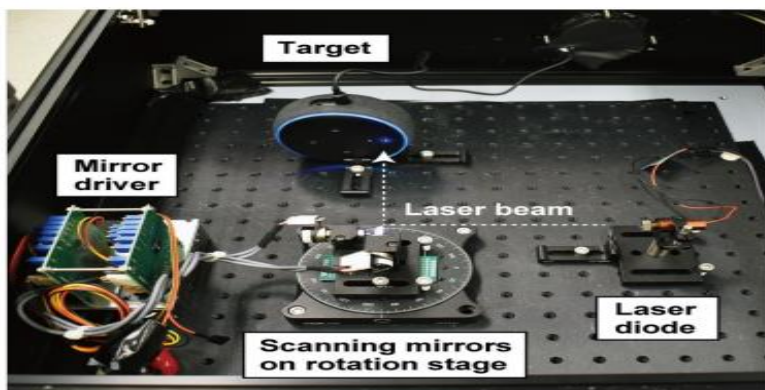


Le rayon laser cible attaque la victime par le message vocale « OK, Opening »

Mais la question qui se pose ! qu'elle est la distance optimale, ainsi qu'elle est la puissance optimale choisi pour attaquer notre victime correctement ? Surtout les gadgets microphone se diffèrent !!!!

Pour répondre à ces question Mr Benjamin a mis deux expériences :

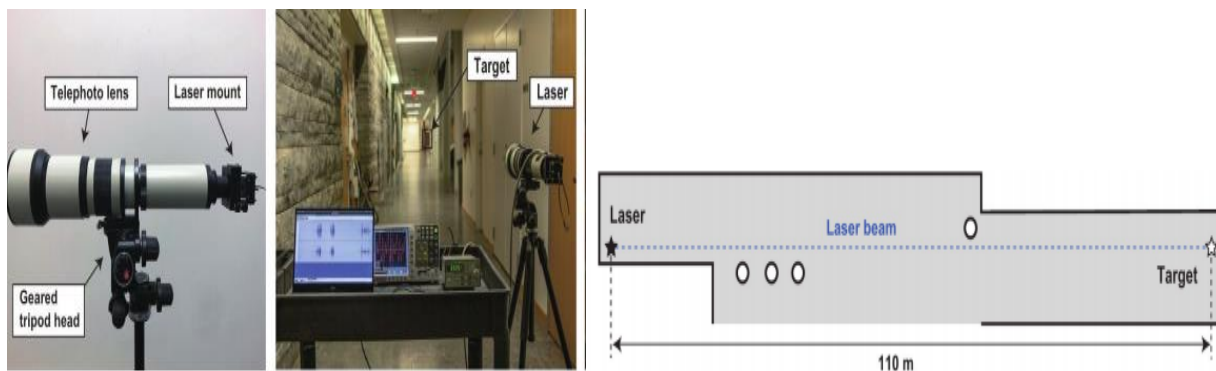
N°3: Mesure vulnérabilité :puissance & range .



Puissance

Le laser et la cible sont disposés à l'intérieur d'une enceinte. Le laser

Le spot est dirigé vers le port acoustique cible en utilisant des miroirs de balayage contrôlables à l'intérieur de l'enceinte. L'enceinte a été retiré pour des raisons de clarté visuelle.



Range (distance entre attaquant et victim)

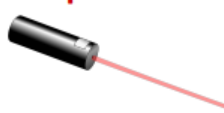
Objectif c'est detecter le cible dans une distance optimal.

$$\text{Irradiance} = \text{puissance} / (\text{distance (cible, source)})^2$$

Ces expériences donnent une vue sur les deux paramètres range et puissance sur différents gadgets

VI.1.3. Résultat

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	-

5mW: 110+ meters

60mW: 50+ meters

60mW: 5-20 meters

Phones/Tablets

Mr. Benjamin a effectuer plusieurs expériences sur différents types de microphone comme google home, Echo, Echo spot ainsi une expérience est étalée sur aussi les portables tablette comme iPhone XR et iPad 6th Gen, Samsung Galaxy S9.

Le résultat à montrer trois types des rayons laser à préparer pour ces gadgets :

5 mW avec une range 110 m le cible par exemple Google Home.

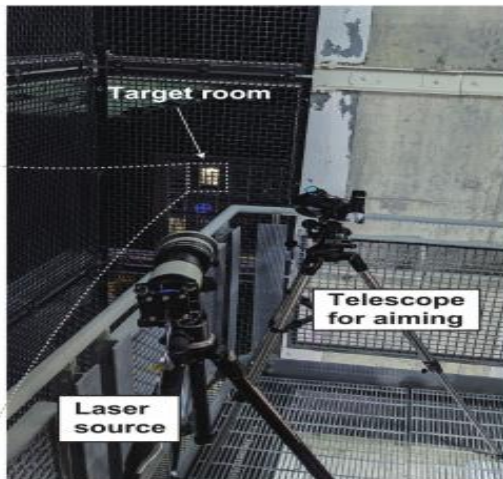
60 mW avec une range 50 m le cible par exemple Echo.

60 mW avec une range 5-20 m le cible par exemple Samsung Galaxy S9.

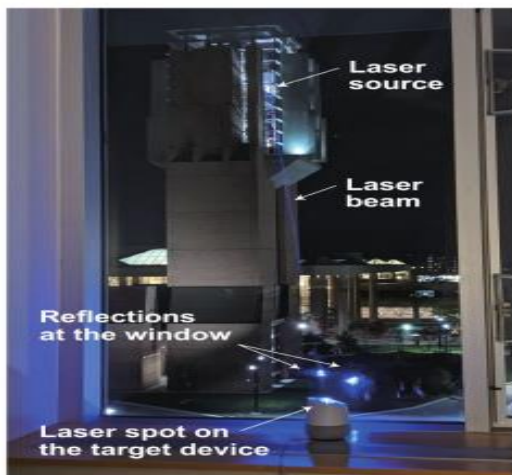
V. Scenario d'attaque

Préparation de l'attaque de faible puissance : Disposition du laser et de la cible. Image de la

Le dispositif cible est visible à travers le télescope, avec les ports du microphone et le spot laser clairement visibles. Derrière le télescope une source de laser générés, pour choisir une seule onde laser porte notre information code de notre gadget microphone



Le dispositif cible est visible à travers le télescope, exercé sur note microphone a travers la fenêtre, le laser est bien positionné dans notre gadget.



Résultat de cette attaque est réussi avec une distance 110 m. le code pin « message vocale » est envoyé via notre rayon laser dans notre cible.

VI. Solutions et propositions(Mr Benjamin et moi-même)

Soft

1-Authentification renforcée

2-Exemple

“Please confirm by repeating the second digit of your passcode”

3-Changement le code periodiquement, afin de créer des obstacles contre les attaquants.

4-Chaque activation du code pin, utilisateur doit valider activation du code par mail sur le telephone.

5-Informer le client toutes les manipulation d’un utilisateur avec un feedback photo et le code pin dans quelques second.

Matériel

1-Couverture de blocage de la lumière, afin d’éliminer la pénétration des rayons laser à notre gadget.

2-capteurs de mouvement en plus, pour marquer ma présence.

3-Capteurs de caméra en plus, pour marquer en personne.

4-Capteurs empreint, justement pour renforcer la sécurité de mon bâtiment.

5-Eliminer toute type réflexion rayon, exemple la fenêtre, qui aide attaquant à accéder à notre gadget facilement.

6- Mettre en place alarme connecté.

7- Vlaider avec code datamatrix.

VII. Conclusion

Les lasers peuvent injecter des commandes dans les VCS avec une longue portée (110m) et une faible puissance optique

- Vulnérabilité physique des microphones MEMS, aussi à aider attaquant à franchir le territoire de la victime

- Mettre le capteur accoté de la fenêtre, à aider beaucoup attaquant pour cibler le gadget.

- Ignorance de l’utilisateur de ces gadgets peut transformer attaque dans un stade de danger humaine et matériels.

Annexes :

<https://www.usenix.org/conference/usenixsecurity20/presentation/sugawara>