INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

SKIKER Hicham

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

Article d'une attaque

Agenda

- Introduction & contexte.
- Voix contrôlée par systèmes.
- Problématique.
- Explications :
  - MEMS microphone .
  - Injection signal laser.
  - Mesure vulnérabilité :puissance & range .
  - Résultat.
- Scénario d’attaque .
- Solutions & mes propositions.
- Conclusion .

Introduction & Context

Attaques dans IOT smart bâtiment(garage, porte, bureau,....)

Injection audio par laser sur les systèmes à commande vocale

Voix contrôlée par systèmes

Voix

“123, 456...”

Microphone

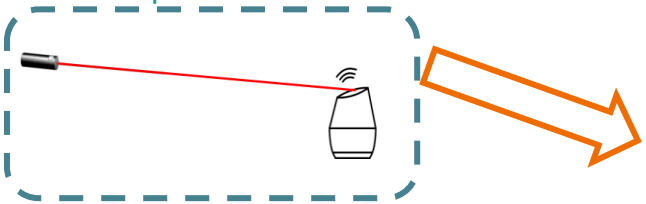
Signal electrique

456

Execution une commande

Problématiques

Origine du problème

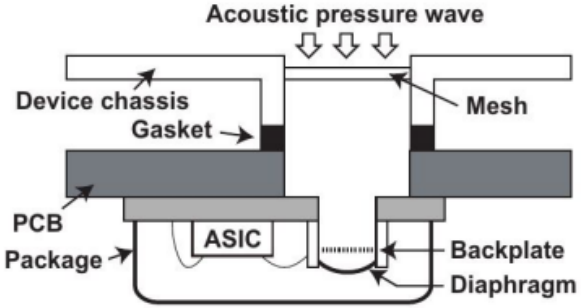


Les microphones captent

les signaux acoustiques et

les signaux lumineux

MEMS Microphones



Le diaphragme et la backplate fonctionnent comme un condensateur

Lorsque le diaphragme se déplace, il provoque une modification de la capacité

L'ASIC convertit le changement capacitif en tension

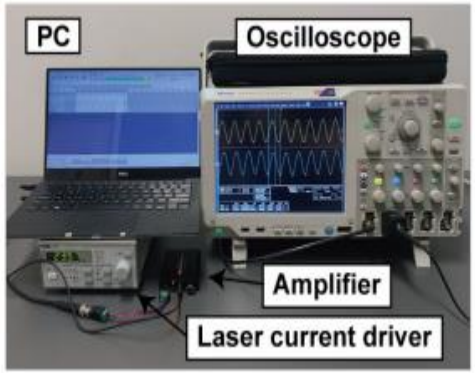
Injection de signaux par laser

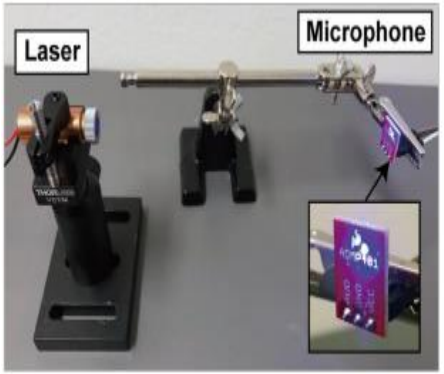
Pc + enregistreur audio +Laser+ Ampli+ driver de courant

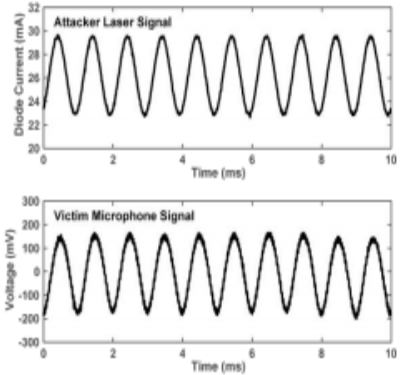
Source de laser +microphone +miroir pour réflexion

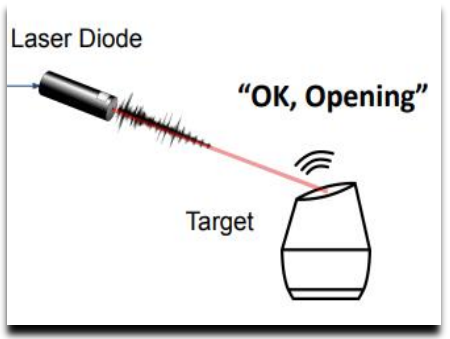
- Attaque par signal laser
- Victime signal microphone

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





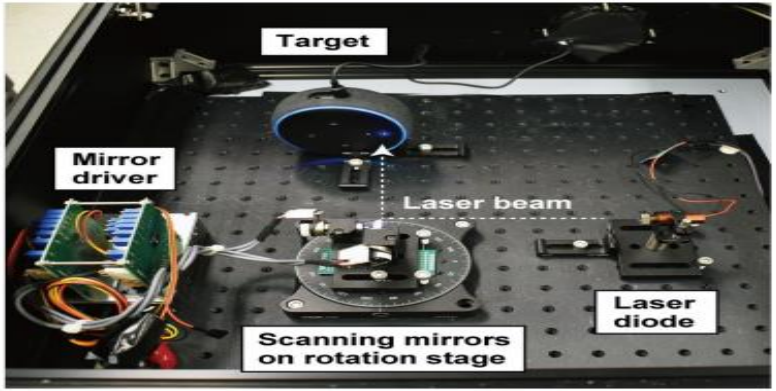




Mesurer la vulnérabilité : Puissance - Range

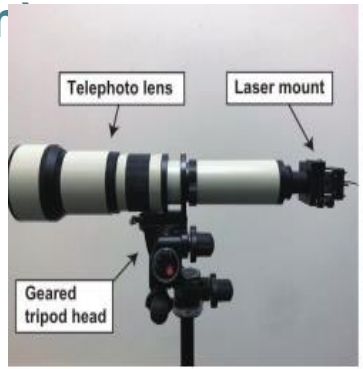
Puissance

Déterminer le minimum de puissance pour détecter le cible



Range (distance entre attaquant et victim

Irradiance = puissance /(distance (cible ,source))²



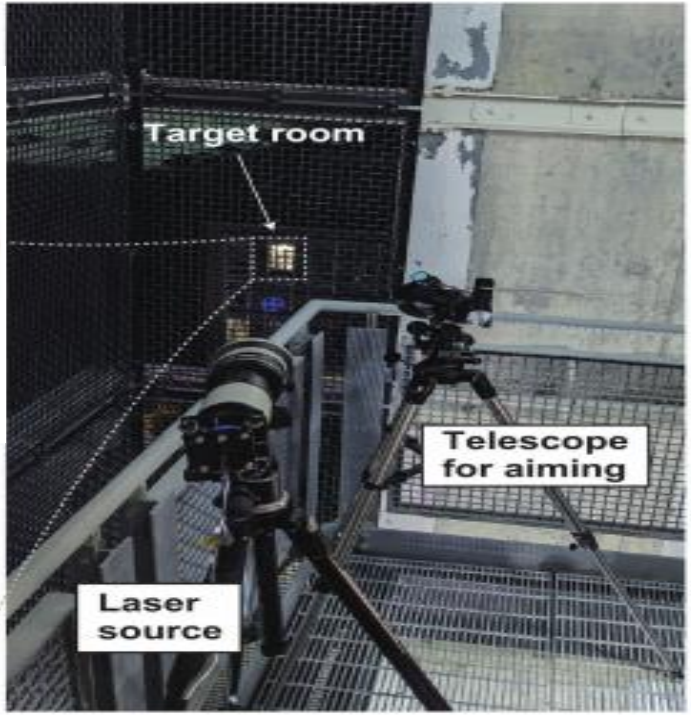
Résultat(sur 17 accessoires)

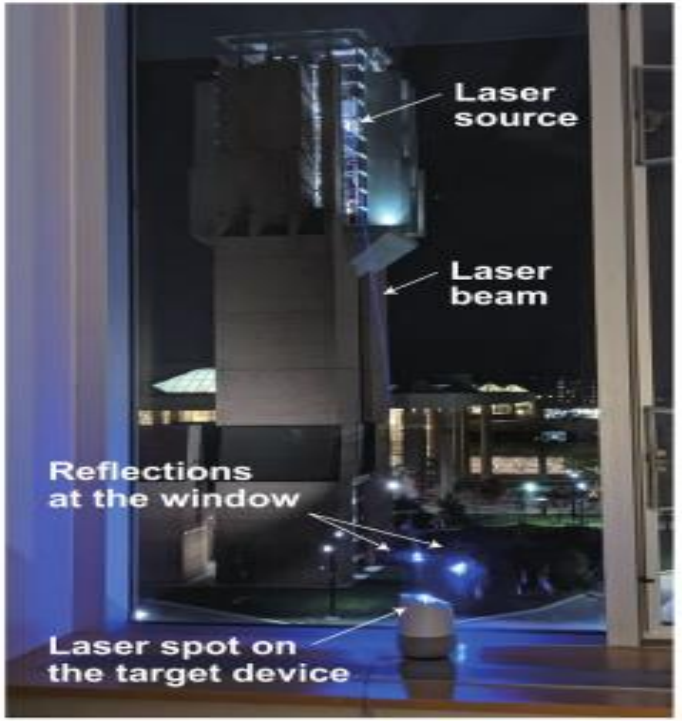
60MW – 5 – 20m: portable /tablette
Exemple Iphone XR.

5MW – 110m: devise Google home .

60MW – 50m: devise Echo .

scénario **d'attaque**





Solutions & Propositions pour mettre barrière contre ces attaques

Soft

- Authentification renforcée
- Exemple
- “Please confirm by repeating the second digit of your passcode”
- Changement le code periodiquement .

Matériel

- Couverture de blocage de la lumière
- capteurs de mouvement en plus
- Capteurs de caméra en plus
- Capteurs empreint
- Eliminer réflexion rayon par la fenêtre(couche anti réflexion par exemple)

Conclusion

Merci!

Questions ?

Authors: Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin, Kevin Fu