Interactive Attack on Smartphone Voice Systems

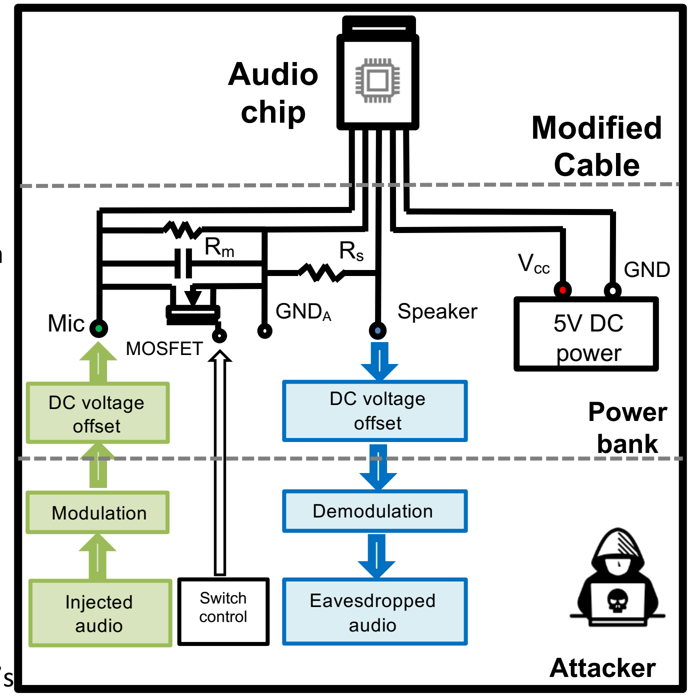
Challenge:

- How to make the audio attack resilient to noise?
- How to make the audio response inaudible?
- How to bypass the voice recognition without authenticated voice?
- How to efficiently authenticate smart home IoT devices and communications given the sheer amount of the devices to be managed in the near future?

Solution:

- By injecting electric signal, external will not disturb the voice commands.
- We emulate a “fake headphone” to force the smartphone output audio signal through charging ports.
- We design a MOSFET to short the mic and ground to spoof the smartphone without user’s voice.
- Design a device authentication mechanism without the reliance on credentials by leveraging signal features of the ambient radio-frequency and ultrasonic signals

NSF Award #: 1950171
PI: Qiben Yan
Dept. of Computer Science and Engineering
Michigan State University
East Lansing, MI
Email: qyan@msu.edu
Phone: (517)353-3541



An overview of attack system design. The attacker replaces the cable with a malicious one and remotely launches the attack.

Scientific Impact:

- This research is the first one illustrating the potential threat of voice commands from charging ports.
- Compared with attacks over the air, the attack addresses many existing challenges.
- The proposed solutions will be rigorously tested using large-scale simulations and experimentally tested via IoT testbeds. Results from this project will lead to a new knowledge frontier for the design and implementation of secure and reliable IoT systems.

Broader Impact and Broader Participation:

- The research conducted through this project will significantly improve the security of smart home networks to allow people to enjoy robust and trustworthy smart home services, and can be potentially extended to secure other IoT systems, including military, agriculture, healthcare, etc.
- The project has an emphasis on the practicality of the developed solutions, the PI works closely with IoT companies for possible technology transfer.
- Incorporate the knowledge developed in this project into both undergraduate and graduate course modules.
- Disseminate research finding to K-12 students in STEM disciplines through summer research program and seminars.