POSTER: Inaudible Voice Commands

Submitted by grigby1 on Tue, 02/27/2018 - 2:30pm

Title	POSTER: Inaudible Voice Commands
Publication Type	Conference Paper
Year of Publication	2017
Authors	Song, Liwei, Mittal, Prateek
Conference Name	Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security
Publisher	ACM
Conference Location	New York, NY, USA
ISBN Number	978-1-4503-4946-8
Keywords	command injection attacks, composability, inaudible ultrasound injection, intermodulation distortion, Metrics, microphone, non-linearity, pubcrawl, resilience, Resiliency

Abstract

Voice assistants like Siri enable us to control IoT devices conveniently with voice commands, however, they also provide new attack opportunities for adversaries. Previous papers attack voice assistants with obfuscated voice commands by leveraging the gap between speech recognition system and human voice perception. The limitation is that these obfuscated commands are audible and thus conspicuous to device owners. In this poster, we propose a novel mechanism to directly attack the microphone used for sensing voice data with inaudible voice commands. We show that the adversary can exploit the microphone's non-linearity and play well-designed inaudible ultrasounds to cause the microphone to record normal voice commands, and thus control the victim device inconspicuously. We demonstrate via end-to-end real-world experiments that our inaudible voice commands can attack an Android phone and an Amazon Echo device with high success rates at a range of 2-3 meters.

URL	https://dl.acm.org/citation.cfm?doid=3133956.3138836
DOI	10.1145/3133956.3138836
Citation Key	song_poster:_2017

command injection attacks composability inaudible ultrasound injection intermodulation distortion Metrics microphone non-linearity pubcrawl resilience Resiliency