ECE 498 - BackDoor: Paper Review

Amod Agrawal, amodka2

April 30, 2019

1 Summary

This work involves exploiting the non-linearity in the commercial off-the-shelf microphones to make them record the inaudible ultrasound signals. Sounds below 20kHz are audible to humans as well as microphones. Sounds above 23kHz are inaudible to the microphones which logically correlates with the human hearing range of 20kHz. However, backdoor exposes a non-linearity in the hardware that can move a part of the ultrasound wave to the audible range of the microphone. The core idea is that the amplifier of the microphone leaks a "backdoor" where two frequencies around 50kHz which are sent as inputs result in an output consisting of a component involving F1-F2, which falls in the audible range of the microphone.

This is particularly useful because now we have a new channel for device communication - which can be used for IoT devices for communication in proximity. It can also be used by an attacker to give silent inaudible commands to smart home assistants like Alexa. The paper shows there are various applications for such a communication channel that has remained unexplored because acoustic signals can disturb humans and animals.

The authors also talk about creating an ultrasound speaker array because while creating a signal a part of it leaks into the baseband. This can cause the system to be audible. They tackle this issue by keeping the baseband signals below the human hearing curve and splitting the bandwidth of the signal into smaller chunks and sending it over an array of speakers. This is very important as we pump more power into the system, audible leaks can increase.

2 Critique & Opinion

This is a very interesting piece of work because it exposes an unidentified non-linearity in COTS microphones that can potentially impact all microphones out there. While it's very interesting to see the use of BackDoor on systems like Alexa, it's often not trivial to actually perform a malicious job with software security systems. In my opinion, it's more exciting to see BackDoor as a new channel for communication among devices which can support up to 4kbps of data rate. However, since an array of ultrasonic speakers is used, the system uses much more directional signals which makes communication harder for mobile devices. For applications like fetching information for a specific aisle at a shopping center or a painting while standing next to a painting at a museum, this solution works great because of its directional nature.

I wonder if there is any way to exploit the non-linearity in air as well as the microphone to send inaudible data along with audible signals. The dual of it is also interesting, sending inaudible signals with selectively audible signals. This can be introduce new applications where we can have speakers everywhere but they can serve multiple purposes at the same time.