Why Do You Trust Sensors? Analog Cybersecurity Attack Demos

Andrew Kwong, Connor Bolton, Timothy Trippel, Wenyuan Xu, Kevin Fu
University of Michigan, SPQR Lab

Abstract

In this demonstration, we will show how subtle physical vulnerabilities in sensors combined with maliciously generated acoustic and electromagnetic interference allow us to control or bias the digital values perceived by microprocessors. The demonstration will show two attacks published in the IEEE Symposium on Security and Privacy and the IEEE Euro Symposium on Security and Privacy. One attack shows how to inject fake audio into microphones by emitting modulated electromagnetic interference at the resonant frequency of the wire connecting the microphone to the amplifier. The second attack shows how to control the digital output of accelerometers by emitting modulated acoustic interference at the resonant frequency of materials in MEMS sensors. The demo also includes an example for attendees to inject fake steps into Fitbits and hijack a smartphone-controlled RC car with custom music.

1 Demonstration Details

In our demonstration, the audience will have the opportunity to inject acoustic and electromagnetic interference (EMI) to exploit security vulnerabilities in analog sensors that blindly forward unvalidated sensor readings to microprocessors. The audience will use EMI to spoof audio signals to a webcam [1], and acoustic interference to spoof the sensor readings of micro-electrical-mechanical-systems (MEMS) accelerometers [2].

For our demonstration of EMI attacks, a Universal Software Radio Peripheral (USRP) transmits an audio file's waveform modulated over the RF resonant frequency of the microphone's wiring. The wires combined with the audio receiver circuits behave as an unintentional RF demodulator. The result is injecting arbitrary audio into microphones via radio.

In our acoustic injection attack, we will spell out phrases like "WALNUT" on oscilloscopes connected to MEMS accelerometers to show how we can cause unintentional demodulation of chosen signals. Our acoustic demo (Figure 1) shows how to hijack control of an accelerometer-based smartphone app that controls the movement of an RC car. The audience will then be able to observe the RC car moving under our control, even while the paired phone is lying motionless.

Figure 1: By playing specially crafted music on a phone, the audience will control the on-phone accelerometer that causes manipulation of a remote-controlled car.

References

[1] KUNE, D. F., BACKES, J., CLARK, S. S., KRAMER, D., REYNOLDS, M., FU, K., KIM, Y., AND XU, W. Ghost talk:mitigating EMI signal injection attacks against analog sensors. In *IEEE Symposium on Security and Privacy 2013* (San Francisco, California, May 2013).

[2] TRIPPEL, T., WEISSE, O., XU, W., HONEYMAN, P., AND FU, K. WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In *2nd IEEE European Symposium on Security and Privacy* (Paris, France, 2017).