1300 - Controlling IoT devices with crafted radio signals

Friday at 13:00 in 101 Track
45 minutes | Demo, Tool
Caleb Madrigal*Hacker, FireEye/Mandiant*

In this talk, we'll be exploring how wireless communication works. We'll capture digital data live (with Software-Defined Radio), and see how the actual bits are transmitted. From here, we'll see how to view, listen to, manipulate, and replay wireless signals. We'll also look at interrupting wireless communication, and finally, we'll even generate new radio waves from scratch (which can be useful for fuzzing and brute force attacks). I'll also be demoing some brand new tools I've written to help in the interception, manipulation, and generation of digital wireless signals with SDR.
Caleb Madrigal
Caleb Madrigal is a programmer who enjoys hacking and mathing. He is currently working as a senior software engineer on Incident Response software at Mandiant/FireEye. Most of his recent work has been in Python, Jupyter, Javascript, and C. Caleb has been into security for a while... in high school, he wrote his own (bad) cryptography and steganography software. In college, he did a good bit of "informal pen testing". Recently, Caleb has been playing around with SDR, IoT hacking, packet crafting, and a good bit of math/probability/AI/ML.

@caleb_madrigal, calebmadrigal.com

#defcon25/by_track/101/Friday #defcon25/By_Day/_Friday