Cryptographic Engineering Research Group Presents

ECE DEPARTMENTAL SEMINAR

Broken with Purpose - Fault Attacks on Embedded Systems

Friday, April 27th, 2018
3:00 pm — 4:00 pm
Engineering Building, Room 2901

Speaker: Colin O'Flynn
NewAE Technology Inc,

Abstract:

Embedded systems are present in almost every aspect of our life, and it's hard to start the day without them. From the latest IoT toaster you used to perfectly crisp your bread, to the automotive computers in the car you drove to school or work. This talk looks at how fault injection attacks can be used as an attack vector, and demonstrates attacks with voltage fault injection and Electromagnetic Fault Injection (EMFI) on embedded systems.

Discussions will include fault attacks for breaking fuse bits on devices, fault attacks for breaking cryptography, and using side channel power analysis for assistance with fault injection attacks. This talk will cover several low-cost and open-source tools available in addition to commercial tools, making it suitable for those interested in recreating the work on their own.

Biography:

Colin O'Flynn started the open-source ChipWhisperer project, which is a variety of hardware and software tools for power analysis and fault injection. He received his PhD from Dalhousie University in Halifax, NS, Canada in 2017. He is now running his start-up NewAE Technology Inc., which is commercializing the hardware platform. He has previously spoken at several security conferences such as Black Hat and DEFCON.