Security for ‘Internet of Things’: Physical Attacks and Countermeasures

As our culture begins buying more and more Internet enabled devices for our person, in our cars, homes and office systems; we are wading deeper and deeper into the vulnerable, untested waters of “Internet of Things” (IoT) security. We are now seeing in the news that the safety of our embedded devices are at higher and higher risk of being “hacked”, and little is being with regards to IoT device security until after such systems are hacked and in the news.In this talk, we will cover several types of Physical Attacks that IoT hardware designers and users should all know about. Physical attacks are a type of cryptanalysis, or the analysis of information systems in order to discover the hidden aspects of devices and systems using their implementation properties. Fault Injection is the force used to change the physical behavior of the running device to discover additional security information or ways into the system. Physical attack and fault injection research is critical because it is a preferred low cost attack method used by both black hats to discover new IoT/hardware/software attack vectors, as well as by white hats to help discover and address these vulnerabilities early in the design cycle before they get to market. The more physical attack research that is done on IoT devices, the safer we all will be.