**Intentional Electromagnetic Interference Attack on Embedded Systems**

# Abstract

Embedded systems are critically relying on the integrity its input and output signals to ensure proper operation. Signal from sensors, either analog or digital, are blindly trusted by the embedded systems, to estimate the environment, in which the system is set to monitor and respond to. Similarly, actuators, that are connected to and controlled by an embedded system, are expected to behave in a reliable manner, to perform a particular physical motion. However, recent publications, from hardware security researchers, have shown that sensor signals can be manipulated by injection of false data, using intentional electromagnetic interference (IEMI). In this work, the author proves that both the input as well as the output signals of an embedded system are vulnerable to data manipulation, via physical layer of this system, which would bypass any traditional defense mechanism.

By using specially crafted IEMI attack techniques, this work has shown that the physical layer input/ output signals can be manipulated by an attacker, thereby providing the attacker, with the ability to remotely control an embedded system. Three different attack scenarios had been analyzed and the effectiveness of the attack against each scenario has been experimentally verified. First, an embedded system, gathering data through an analog sensor, was manipulated to output arbitrary sensor data, while in the second scenario, a slightly modified attack technique, has been shown to successfully inject false data into digital communication lines. Finally, commonly used digital actuators, which were controlled by embedded system, has been shown as a potential target for false data injection attack, using IEMI techniques. These attacks have been shown to be effective, at appreciable distances from the victim circuit, while using attack signals with relatively less power.