### Problem Statement

- Electronics are vulnerable to channel attacks at many stages that can perturb operation or extract sensory data.
- Security vulnerabilities of IoT nodes include:
  1. **Power Side Channel Attack**
     - During AES encryption
  2. **EM Side Channel Attack**
     - Near-field and far-field distortion.
  3. **RF Channel Attack**
     - Interfere/alter communication.

### Proposed Solution

- **Generative Adversarial Network** will be trained for both reactive and proactive side channel attacks.
- During training, “Discriminator Network” will be fed by both real signals and fake signals generated by “Generator Network”.
- After training, “Discriminator” will be used by IoT node to distinguish channel attacks in milliseconds.

### Project Objectives

1. Adversarial networks (proactive and reactive) that act as embedded observers in IoT nodes.
2. Capability of detecting attacks (RF, power or EM side channel) within milliseconds.
3. Low overhead (<10%) circuit topologies and architectures to detect side channel attacks.

### Annual Milestones

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 1, 2018</td>
<td>Project Start</td>
</tr>
<tr>
<td>June 1, 2018</td>
<td>Develop ML methods based on both diagnostic and active learning techniques using ANN and Bayesian inference methods.</td>
</tr>
<tr>
<td>Nov 1, 2018</td>
<td>Apply Deep Learning techniques for detecting minute changes in the system response in milliseconds.</td>
</tr>
<tr>
<td>Dec 31, 2018</td>
<td>Develop a proof of concept strategy that can be used to extend the solution and its verification in Year 2.</td>
</tr>
</tbody>
</table>

### Deliverables and Outcomes

**Year 1**

1. Models of the system that include RF communication, WPT and security blocks that includes near field coupling through RF coils at ~1GHz using HFSS, ADS and Matlab
2. Model of adversarial network as an observer
3. Algorithms developed in Matlab for deep learning based on ANN and Bayesian inference methods
4. Model based demonstration of identification of cyber-attacks through RF, Power and EM Channels in milliseconds.

**Year 2**

1. Model based demonstration of counter measures
2. Prototype development with observer
3. Demonstration of trusted platform using prototype or evaluation board
4. Software for Deep Learning in matlab

---

**Methodologies and designs developed as a part of this project will open up opportunities for trusted electronics.**