## 1.1 Problem Statement

The Internet of Things (IoT for short) is a Cyber Security concept concerning the interconnected devices and the vulnerabilities arising from these devices. Our project aims to educate the public about IoT vulnerabilities so that they can better defend themselves against such attacks. This is to be done through a deliverable package to the Cyber Defence Competition (CDC for short).

## 1.2 Requirements & Constraints

**Functional Requirements**

- IoT device integration into Iowa State's ISEAGE/CDC environment
    - Virtualization of at least two IoT devices for integration
    - At least one physical IoT device integrated

- Easily reproducible:
    - IoT infrastructure that can be used in future CDCs
    - Vulnerabilities, Attacks, Defense Strategies
    - Machines that can be remade and deployed as needed

- A packaged, distributable bundle which holds resources necessary to configure IoT devices into a CDC from group sdmay21-28 and sdmay22-14.
    - i.e., Documentation, ISOs, and packaged software to develop a CDC
    - Automated scripts to emulate the Green Team (Checking for service availability)
    - Automated scripts to emulate the Red Team (Exploiting the integrated vulnerabilities within each IoT VM. )

- Physical and Virtual IoT devices shall be different from each other
    - i.e, Smart Plug and Smart Watch, etc.

**Non-Functional Requirements**

- Ease-of-use network interfacing
- Different levels of vulnerability difficulty
- High performance virtual machines with minimal virtual hardware requirements
- Clear setup and use instructions

**Economic Requirements**

- Keep budget reasonable while looking at vulnerabilities vs. cost
    - Inexpensive equipment can be bought for more in depth recreation
    - Expensive equipment is to be completely virtual

**Ethical Requirements**

- Vulnerability Disclosure
    - International Organization for Standardization (ISO) 29147:2014 https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en
        - Follow this standard to create vulnerability reports and submit to vendors
    - MITRE CVE Database
        - Find relevant past vulnerability information in the MITRE CVE database

- These devices are constructed for the purposes of education, and not in any way to be malicious.

## 1.3 Engineering Standards

What Engineering standards are likely to apply to your project? Some standards might be built into your requirements (Use 802.11 ac wifi standard) and many others might fall out of design. For each standard listed, also provide a brief justification.

> https://standards.ieee.org/standard/802_1Qca-2015.html - Our simulated IoT will be connected to a simulated router/firewall that will act as a bridged network.
>
> https://www.iso.org/iso-9660-images-for-computer-files.html - Our project will employ the use of ISO-images which are used to configure the virtual machines in the our "Portable" CDC.

## 1.4 Intended Users and Uses

Who benefits from the results of your project? Who cares that it exists? How will they use it? Enumerating as many "use cases" as possible also helps you make sure that your requirements are complete (each use case may give rise to its own set of requirements).

- People learning about Cyber Security or the concept of IoT
- Participants of the ISU CDC
- Universities and highschools besides ISU