3 Design

3.1 Design Context

3.1.1 Broader Context

Describe the broader context in which your design problem is situated. What communities are you designing for? What communities are affected by your design? What societal needs does your project address?

Our project is to virtually simulate the Internet of Things. The result of this project will be implemented in future Cyber Security classes and Cyber Defence Competitions. With this implementation future students can gain a greater understanding of the security risks that the Internet of Things poses.

List relevant considerations related to your project in each of the following areas:

Area	**Description**	**Examples**
Public health, safety, and welfare	We must produce a virtual machine that possesses vulnerabilities that can be exploited for education; However, we must also ensure that we do not maliciously introduce vulnerabilities which can be exploited from unwanted threat actors with the intention to cause harm. We have a responsibility to ensure the products we create do not threaten the integrity of legitimate networks and devices.	Exposing a vulnerable IoT device from a legitimate network to the public-facing internet. Configuring a vulnerable IoT device that compromises the security of a functional network
Global, cultural, and social	Our device will help the CDC create a cultural shift towards internet security. By bringing devices' vulnerabilities to peoples' attention, they will be more conscious of how cybersecurity affects their daily lives.	Enable people to gain hands-on experience on IoT vulnerabilities to educate and spread awareness.
Environmental	We must be conscious of the hardware we acquire and the software we produce. We have an obligation to make our deliverables as small and functional as possible.	We will try to select a physical device that has its raw resources responsibly resourced. We must not unnecessarily create virtual machines that consume excessive and unnecessary resources.
Economic	The physical device must be as affordable as we can make it. While we only have to have the one, our clients will have to purchase a	We shall not purchase an IoT device which costs more than $100.

	plethora. If the price is too high, this will quickly compound.	

3.1.2 User Needs

List each of your user groups. For each user group, list a needs statement in the form of:

The Cyber Security Department and the Cyber Defence Competition needs a way to simulate the Internet of Things because buying the devices for each group would be incredibly expensive.

The students in the Cyber Security Department and the participants in the Cyber Defense Competition must use the devices we implement in ISERink to complete schoolwork and the competition.

3.1.3 Prior Work/Solutions

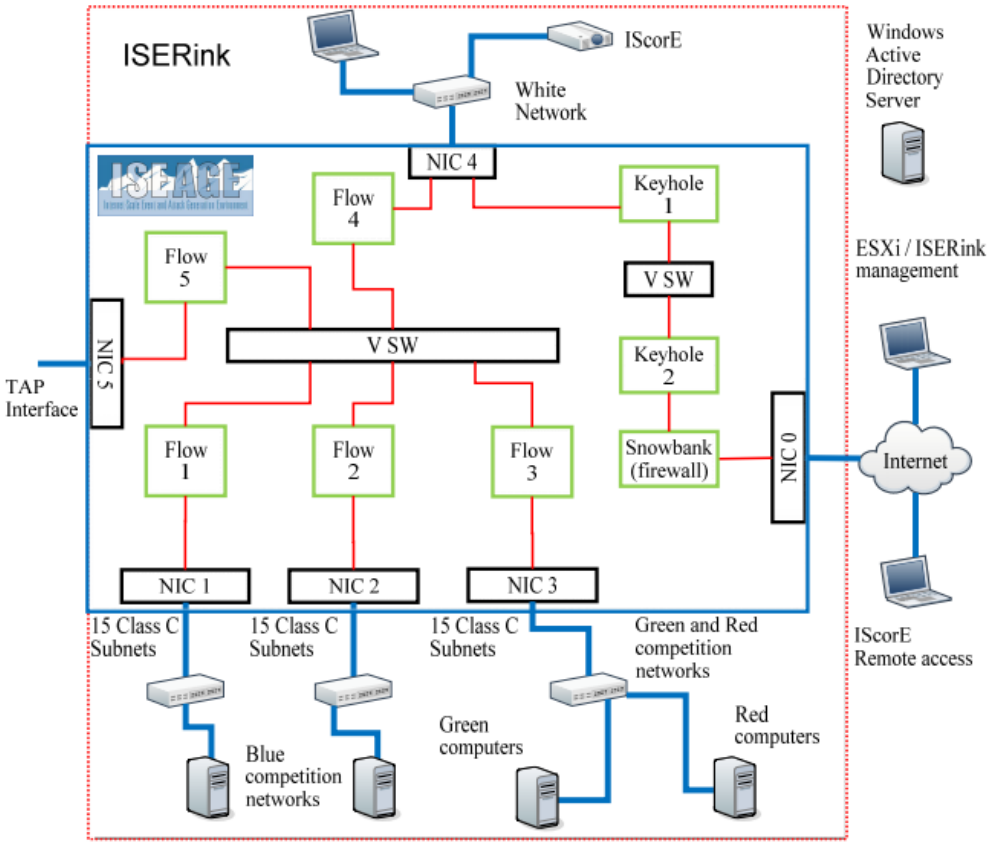


Figure 3 ISERink VM topology

- Our project design stems from the already existing ISERink environment. ISERink is a virtual environment that allows multiple teams to safely defend and attack virtual devices/machines. The

virtual machines are implemented with services that have vulnerabilities that need to be mitigated by the Blue Team, exploited by the Red Team, and usable by the White Team.

Include relevant background/literature review for the project

– OWASP Top 10 is a good resource. Many IoT devices have web interfaces with common vulnerabilities listed and described in the OWASP Top 10.

– We are following the work documented for ISERink as seen here. This link contains information about the network architecture of which we are to follow to successfully integrate our IoT components into the Spring CDC for Iowa State University.

– There was a team last year with a nearly identical goal to ours. We both are tasked with creating a physical and virtual IoT device that the CDC can use. The end parts should be similar, but we want a much heavier emphasis on usability. We will modify the previous team's work to match our own allowing the CDC to have an easier time with its use. Previous team's getlab here.

3.1.4 Technical Complexity

Provide evidence that your project is of sufficient technical complexity. Use the following metric or argue for one of your own. Justify your statements (e.g., list the components/subsystems and describe the applicable scientific, mathematical, or engineering principles)

1. The design consists of multiple components/subsystems that each utilize distinct scientific, mathematical, or engineering principles

   Our project includes integrating physical and virtualized IoT devices into ISERink. This includes manually configuring these devices to use DHCP, export their commands and traffic to use Iowa State's ISELAB proxy, and configure other various exports to manually configure network settings.

2. The problem scope contains multiple challenging requirements that match or exceed current solutions or industry standards.

   Alongside our requirements to integrate our deliverables into ISEAGE, we must also study and replicate common security vulnerabilities. We must not only be proficient enough to comprehend security vulnerabilities (i.e., Buffer Overflow, XSS, CSRF), but we must also know enough of the underlying causes to emulate and fully recreate them within an already secure product.

3.2 Design Exploration

3.2.1 Design Decisions

1. Choose an IoT device to implement.
2. Decide vulnerabilities that can be both attacked and mitigated.
3. Implement a virtual machine from within ISERink
4. Implement a physical device through a Raspberry Pi

3.2.2 Ideation and 3.2.3 Decision-Making and Trade-Off

For one design decision, describe how you ideated or identified potential options (e.g., lotus blossom technique). List at least five options that you considered.

"Choose an IoT device to implement."

1. We will choose an IoT device from a decision matrix composed of the following traits. These traits were given to us as considerations to keep in mind when picking our IoT devices.

    a. Flashiness: The final product should have some aesthetic/entertaining exploit that can be demonstrated

    b. Cost: The estimated cost to acquire the IoT device

    c. CVSS Score: The common vulnerability score system ranks the harm of a given exploit from Low, Medium, High, and Critical. We want a High CVSS score. This is weighted double as it is the most important aspect.

    d. Hacking Difficulty: The difficulty/expertise needed to successfully exploit the device. (i.e., default passwords (Easy) vs buffer overflow (Hard))

    e. CDC Integration: How well the device would integrate into the CDC (i.e., providing green team services, red team vulnerabilities, blue team defenses)

    f. Total Score: A higher score a score is, the better the device

Device	CVEs	Flashyness	Cost	CVSS Score	Hacking Difficulty	CDC Integration	Total Score
Jector Smart TV FM-K75	CVE-2019-9871	5	0 (Very Expensive)	9.8 (Critical)	4.0 (Easy)	3.0 (Somewhat Intregratable)	21.8
Yi Home Camera 27US	CVE-2018-3934	--	5 (Cheap)	9.0 (Critical)	2 (Hard)	--	--
TP-Link Archer A7 AC1750	CVE-2020-10888	--	5 (Cheap)	9.8 (Critical)	2 (Hard)	--	--
Eques Elf Smart Plug	CVE-2019-15745	3	5 (Cheap)	8.8 (High)	3 (Medium)	3 (Somewhat Intregratable)	22.8
XIAOMI XIAOAI speaker Pro LX06	CVE-2020-10263	3	5 (Cheap)	6.8 (Medium)	--	2 (Barely Intregratable)	--

3.3 Proposed Design

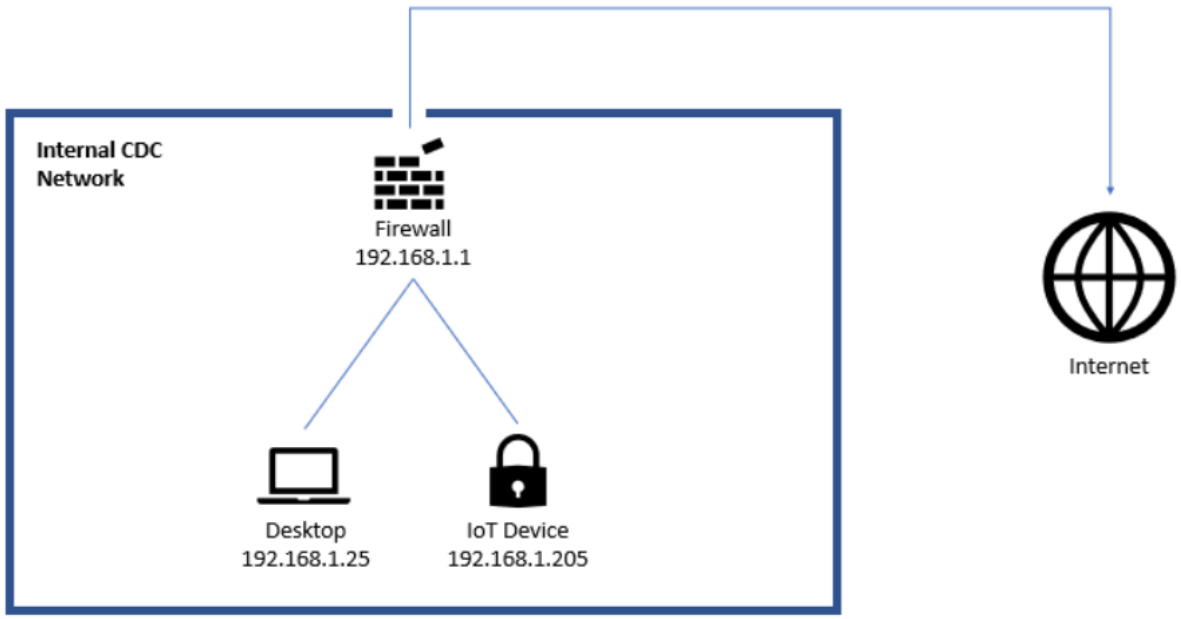
Discuss what you have done so far – what have you tried/implemented/tested?

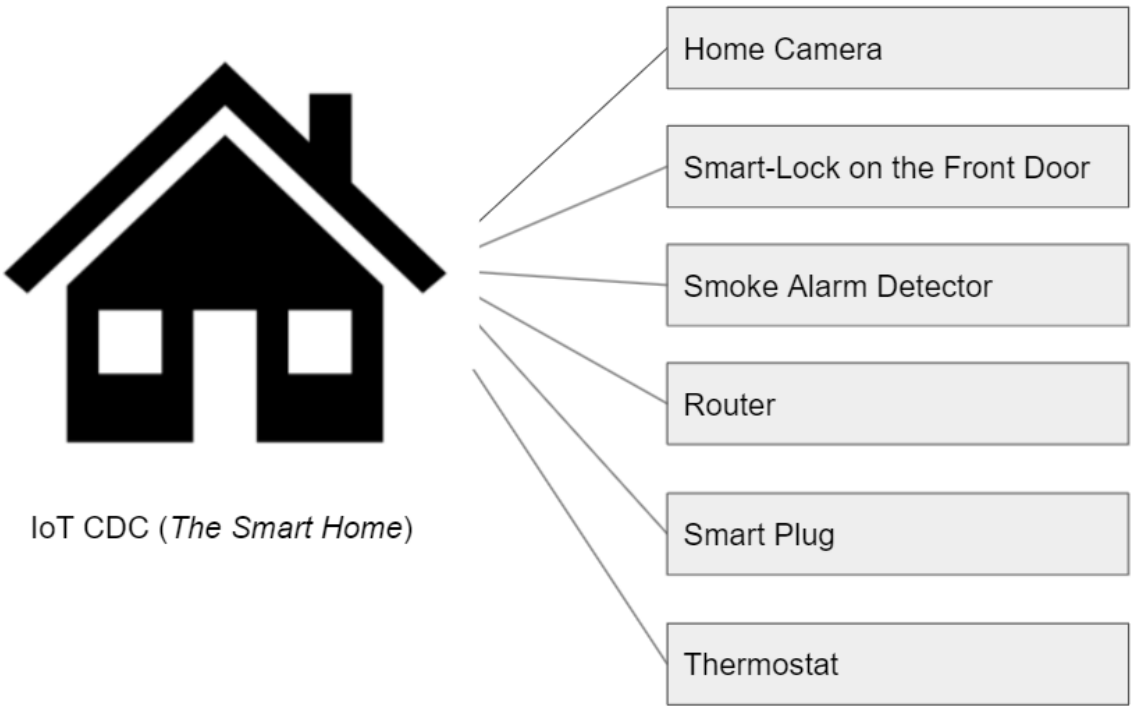
One of our initial designs that was meant to accomplish creating a "downloadable and easily distributable CDC" consisted of a very simple initial design. We created 3 separate VM's acting together as a virtual LAN: a pfSense firewall, a "Blueteam" desktop, and an IoT device (which is a Linux server). The idea was to have any single person be able to download and import a .OVA file, and once they had their CDC VM imported into VirtualBox, they wouldn't have to do any, or at least do very little, network configurations to have a fully functioning personal CDC.

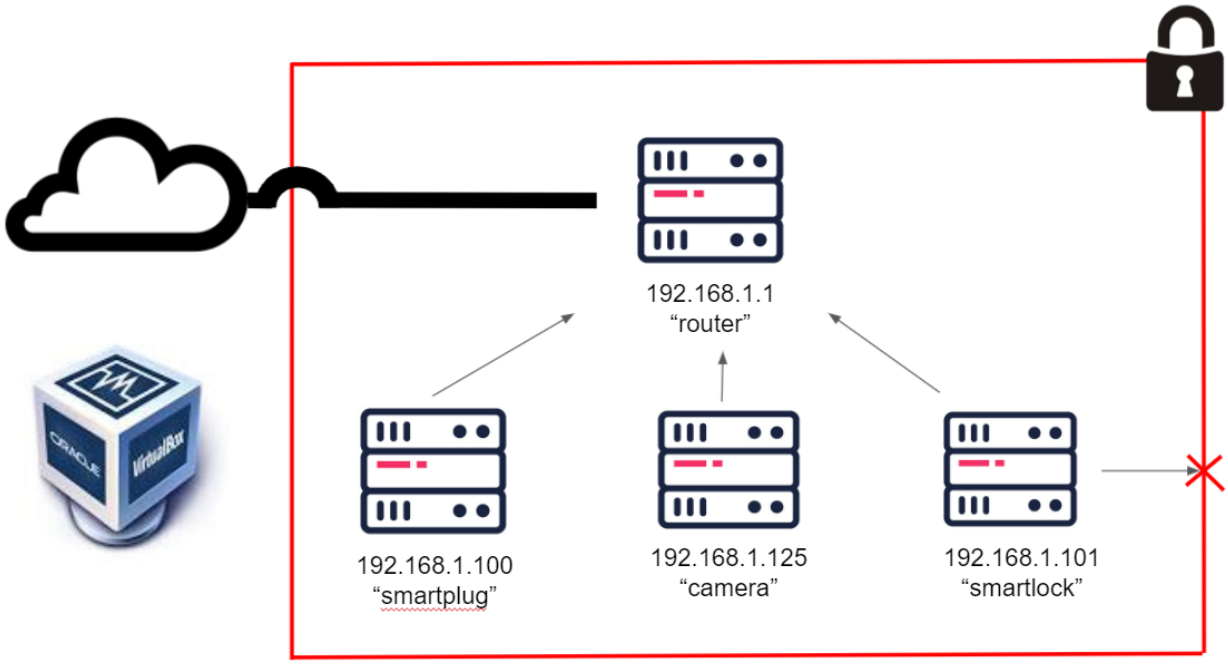
After a few meetings and discussions with our client, we are now moving to a different approach, which is integrating a virtual IoT VM directly into the ISEAGE environment. This IoT VM will be involved with the overarching CDC scenario in the Spring. We also will be creating a physical IoT device that will be included in the Spring CDC, but as an anomaly. It will take time to have ISEAGE 2.0 allocate space for our VM. In the meantime we will create services that our VM will use and create scripts to automatically setup the VM once we get access.

3.3.1 Design Visual and Description

Include a visual depiction of your current design. Different visual types may be relevant to different types of projects. You may include: a block diagram of individual components or subsystems and their interconnections, a circuit diagram, a sketch of physical components and their operation, etc.







Describe your current design, referencing the visual. This design description should be in sufficient detail that another team of engineers can look through it and implement it.

3.3.2 Functionality

Describe how your design is intended to operate in its user and/or real-world context. This description can be supplemented by a visual, such as a timeline, storyboard, or sketch.

How well does the current design satisfy functional and non-functional requirements?

Our design will be deployed as a virtual machine for Cyber Security Students and people competing in the Cyber Defence Competition. These people will then be tasked with finding and mitigating all the vulnerabilities that we have implemented without affecting the functionality of the device. They will then be graded on how well they secured the device. Our design has met much of the functional requirements, but our current implementation lacks non-functional requirements. We have a functional network with a virtualized IoT device, which renders itself as functional. However, we have not implemented this within ISERink, and so the design is currently lacking in the non-functional requirements. With our prototype and proof of concept done, we have enabled our team to successfully replicate our process within ISERink.

3.3.3 Areas of Concern and Development

Based on your current design, what are your primary concerns for delivering a product/system that addresses requirements and meets user and client needs?

We are concerned that the task of modifying the previous Senior Design work in addition to implementing our own device will result in neither product being usable.

What are your immediate plans for developing the solution to address those concerns? What questions do you have for clients, TAs, and faculty advisers?

We plan to put our full effort into developing our own virtual device and only modifying the previous team's work if we have time. This way we guarantee that we have a deliverable to our client and users.