The project my team and I have chosen for our year-long senior design project is Microarchitecture Attacks Capture the Flag. To provide a brief background on what this may contain within, microarchitecture refers to the internal design of central processing units, or CPUs for short. Just like how threat actors in the cyber space may execute attacks through methods such as DDoS or cross-site scripting, they can also attack at this microarchitecture level and target vulnerabilities at one of the deepest layers available. This is a much less known or talked about method of attack, but also an effective and undermined method. We believe that it is very important to show those in the cyber space just how dangerous these attacks can be as well as teach them how to perform them themself in order to know how to defend against them. Our planned format is to provide three different microarchitecture attacks, being spectre, cache, and data analysis (not as much of an attack but usually paired with an attack to gain sensitive data when paired with other attacks). Users will be able to log into the site, explore the different challenges and take a crack at them themself with the guidance of the documents and tutorials we will provide. The users also have the option to use hints that will guide them in the right direction but this will decrease their potential score points that they can gain by completing that challenge. The whole basis of the “capture the flag” is that once they complete each challenge, they will obtain a phrase, or the “flag”, which can then be entered and reward them points for completing the challenge.

My designated role in the project is the Testing Lead, although our entire team has been contributing towards getting everything running and learning about these attacks, as well as how we will incorporate them. So far, I have learned a lot through this project, mostly about microarchitecture attacks themself but also how to run organized educational events that will lead to a beneficial experience to many who wish to participate. The specific attack that I learned the most about was cache attacks as it is the one I will be working on along with another group member to incorporate. This has been a very educational experience for me so far and I have very high hopes for how much more I will achieve over the course of the following year.

As far as resources go, we have been outsourcing a lot of them. This includes the use of multiple web servers that we will use to run and execute code as well as run the website that our challenges will be held on. Our “client” has been very helpful when it comes to this as he provided us with a very powerful web server that we will utilize to perform a lot of the heavy lifting when it comes to the needed compute power. I also reached out to ETG, an Iowa State resource, to obtain another web server that we will be using for some of the smaller components such as handling authentication, relaying code, retrieving results, and displaying data about the competition as it goes on. Other resources we have been utilizing have been many different microarchitecture learning resources such as textbooks and websites that are teaching us the basis of how these attacks we are incorporating works.