Trent Walraven

Tina Prouty

CPRE 494

10 November 2023

A Reflective Journey: Navigating Your Cumulative Experience at Iowa State University

Two weeks late to start, but here I am now, only a short distance from graduating. My path to where I am now, has been a long and varied one, but I have enjoyed it all. Stepping all the way back to my senior year of high school, I had only recently learned about the entire field of cyber security, and had fallen in love. I knew it was what I wanted to do for a career, but that quickly led to me questioning how do I even get into the field, as it is still extraordinarily new.

While I could have gone to school for an adjacent field and specialized after, like computer engineering, that is not what I wanted to do. I knew I wanted to spend my time and money working directly to get into the field. This already severely limited my options for colleges that had a program, and while Iowa State was on that short list, had you asked me in January of my senior year, I would not have called it serious consideration. That all changed when COVID started to ramp up, just as I was getting tours of potential colleges. My tour at Engineering Day in February 2020 is by far the best tour I had of them all though. While the general tour was very generic, what I was impressed with was the major breakout session. We were given a presentation by current students about their experience with the, at the time, brand new program, and the field as a whole. Then after the presentation I got to spend time talking with students, and the professors of the program, all of whom clearly had a passion for the field, and were clearly knowledgeable about how quickly the field is changing, making it clear that I would not be learning about changing tools, but transferable concepts. In contrast, most of my

other visits consisted of cyber security barely being a footnote, or talking about classes to learn tools and exploits that 4 years later are obsolete. Then after seeing how Iowa State handled COVID rather well, that April of my senior year, I made the decision to come to Iowa State for my degree.

That August, just a day before I was supposed to move into my dorm, my father tested positive for COVID, and my plans to start my college career were just pushed back two weeks while I was quartining. I missed moving in, Destination Iowa State, meeting my dorm floor, and starting classes. I was at home in my room having my first day online instead. This rather rapidly led me to getting involved with clubs here at Iowa State, as those were one the few things that for the first few weeks I could actually participate in. From the cyber security club, the Information Assurance Student Group (IASG) to the Culinary Science Club. Being a part of these clubs has been an absolutely incredible experience here at Iowa State. From the Culinary Science Club where I have had the chance to experience foods I have never tried before, and getting that chance to build things like knife skills at a salsa workshop that was held. The culinary arts have always been an interest, and being able to explore and learn about it has been so joyful.

I do not know where to start with IASG. It has been a major part of my time in college in so many different ways. Freshman year it was a place where I got to regularly interact with other cyber security interested folks, and just generally make friends in this entirely new environment to me, many of which are still good friends to this day. This support network built from other cyber security is indescribably important. These peers that have been through many of those same things as I was actively going through are able to provide support about class material, degree requirements, and just generally being someone that can empathize with your struggles. The club also was able to help me explore my areas of passion, in a number of ways like

bringing professionals in the field currently, to purchasing for student use hardware that would otherwise be prohibitively expensive for a one-off side project, and unparalleled levels of networking. The networking with prior students because you interacted regularly, led to my last internship offer after a former student handed my resume to their manager. It does not stop at students though, I have also met individuals from every level in companies, hiring managers, engineers, and C suite executives. The most memorable though is the time that as a club we had the opportunity to volunteer and support the National Association of Secretaries of State, who held a security awareness event for the secretaries in Des Moines. There I had the chance to meet with secretaries from across the country, all of whom brought rather interesting ideas to the table about security and policies around it. It also resulted in getting the chance to talk with Pual Pate, the Iowa Secretary of State, and receiving a handwritten letter in mail after the event. I know that the cabinet of the club is what really opened these doors for the other members by bringing in the companies, and working to manage the events. After having gained so much from the club, I wanted to give back to all the students in the club, and have held numerous positions including Social Chair, YouTube Chair, Treasurer, Vice President, and currently President of the club. In all of these positions, helping be that mentor and leader opening those doors, and giving advice and assistance when possible.

That advice when talking about classes usually revolves around cyber classes, but there is a single notable expectation Computer Engineering 381. I have described this class as one of the most enjoyable classes that I would never take again. This class is teaching about computer architecture, as a whole, covering everything from assembly, all the way down to the actual design of individual components like a cache. Every single second I was amazed at the amount of detail in a processor, and how all of this came together to build the highly complex unit that is

a modern day computer. At the same time, there was such a large amount of material that studying for the class alone took up the allotted credit hour time, before even beginning to look at the lab work to go with it. These labs were both amazing and terrible. We started the semester using a hardware description language where we literally described physical components like an AND gate, and built them in the base components of a processor. The time spent learning this new coding language, and debugging the simulated hardware output to figure out where my component design was wrong, was immense, but so rewarding to see these pieces of "hardware" I made function properly.

That is not where the class ended, the final group project of the lab was using these components, and new ones that you made to build a fully functional MIPS processor. While the idea of what makes a processor was understood from class at a conceptual level, making that work in hardware was something entirely new. My team spent significant time planning out what our current components did, and where they could be, alongside unique ways that these components could be used, so they performed a different functional requirement that was needed. One of those unique ways that still stands out to me is how we implemented a counter for the current location we were executing. We needed to increment a given amount each clock, except in a number of special scenarios. We took a pair of 2 adders, the first getting the current value of the counter, and an optional switch between the hard coded increment, or the inverse of the current value. The second got the output from the first, and another input that was zero, or what was needed in special cases. When a special case arrived, it automatically switched the input of the first, resulting in a zero from the first adder, and the output of the second value only ever being the needed value. This unique thought pattern of working around problems with what you have is not the only thing that I took away from the project.

My major contribution to the project was final integration, after we had each of these logical segments that we had tested separately, I was responsible for bringing them all together, and completing the processor. This compilation of the components resulted in the minor edge cases that were not caught before to spring up, and propagate to a much larger scale. I still remember the hours I spent in Coover Hall looking at the waveform output from our processor. Starting with that final output that was wrong, I had to walk it backwards, debugging where the issue arose, and creating the needed fix. Starting from that output, and the expected value, I would formulate the potential locations that could have caused the problem, and what their expected inputs and outputs would be. Then following that digital wire we created, a single step at time verifying the inputs, outputs, and making sure that step functioned properly, until I had stepped far enough back to find the issue. Where I would then have to implement a fix, sometimes simple, sometimes complex and with the help of teammates. This idea of being able to work backwards from an output and reverse engineer the problem from the outside-in, is invaluable in the security field, where those tiny mistakes that propagate can cause major flaws.

This fixing of flaws in a system is not just an idea either, but something I have the chance to practice and use at the Cyber Defense Competitions put on. For these competitions, the cabinet of IASG puts together a team, both to compete, but also help other participants by offering help, and working through issues with them. When we are given these virtual machines, they are typically in a non-working, and incredibly poor security state. Starting with getting the intended service functioning properly, and reliably, is digging into new programming languages, parsing errors, reading documentation, and making changes until it is running in a stable state. Then comes the challenge of building the defenses against the professional attackers that are brought in. Combing through a system to find mis-configurations, backdoors, and open doors is a

good start, and fixing them is significant improvement. There are often issues that are much more embedded in the system, and are less easy to remove. The first piece of code that executes in a computer is called a “kernel”, and is that base core that the rest of the computer assumes to remain true. Often we are given old systems without updates, and that kernel itself is one of the security problems, and a fix needs to be applied in place without breaking the currently functional system.

I take on this task whole-heartedly, I begin by analyzing what I know the kernel is currently doing, and then building a new configuration that can be used to replicate the same functions in a newer kernel. At which point, I will get and compile that newer kernel with this initial configuration. Rarely does it work first, resulting in warnings and errors, both at compile time, and after putting that new kernel in the system replacing the current one. At which point I have to go back through an execution chain similar to CPRE381, and understand what went wrong and where. At which point, I can make changes to fix them and test again. Going through this process for my team has proven to be wildly successful for the team. In the last competition, our team had logging on our servers, helping us learn where attackers got in. Another thing that we also saw was the failed attempts to break in. Each time the attackers thought they had a foothold, they would execute this attack, which was fixed by replacing the kernel, and get no further. As a result my team placed first in the competition, and got our ticket to the national competition in February.

Hopefully my team and I can secure our systems well for nationals, and I can end up winning my final national competition. I have gained so much from Iowa State immeasurable experiences, knowledge, skills, networking, with that win being a perfect cap for my time here.

After which, I will be able to bring all these tools I have gained into the industry, and help improve the security of the world for everyone.