Our senior design project will be focused on the creation of covert channels. We intend to create guidelines that one can follow to create covert channels on various devices and sites. Our original intent was to prove their effectiveness using a website that we will set up. However, if that proves to be too much of a challenge, we may just show that it works on an operating system level of a computer as a proof of concept. Many papers have been made about detecting covert channels, but not many have been made about building them. Because of this, we hope that our guide will help teach analysts to learn and understand covert channels.

The primary courses that I have taken that will be useful in this project are EECE 4029: Operating Systems/Systems Programming, CS 5155: Cyber Defense Overview, and CS 4065: Computer Networks. EECE 4029 first introduced me to Linux and VirtualBox, which we will likely be using for the project. It also taught me quite a bit about operating system commands and structure, which will be all but required for the creation of any covert channel. CS 4065: Computer Networks will be very useful for the interactions required if we were to create the channel in any sort of remote fashion, which was our original intent. It also gave me an introduction to cryptography, which CS 5155 will expand on this semester. Cyber Defense Overview will almost certainly be the most useful out of these courses, because a covert channel is a cybersecurity concept; our group even chose the professor who teaches the course to help us as a faculty advisor.

Working with GIRD Systems as a Firmware Developer will admittedly not help me much in this project; it mostly just served as an introduction to the working world, and allowed me to develop my programming skills in a few languages. While working there, I did learn Batch, and after leaving, I was proficient in the windows CMD language, but not quite fluent. However, my second Co-op, with ITI International Technegroup, will help me greatly during this project. The primary language I worked in was CMD, and I now know it well enough that I would call myself fully fluent. Our group does not yet know if we want to use a windows system as well as a Linux system, but my experience in making these CMD will absolutely help me in both, since Linux’s Bash has quite a few similarities to it. I also learned to work in an agile environment, as a part of a group, using a task board, which is the same process that our group intends to use to keep ourselves on track. I also managed a mercurial repository, which is similar enough to git (what our group will be using) that it will significantly help me throughout this semester.

The idea behind this project was created by one of our member’s research into covert channels out of curiosity. He discovered that there weren’t many resources on how covert channels were made, but there were resources about detecting them. When I saw his idea on the discussion board, I immediately messaged him, because I have an interest in cybersecurity as a field, and this would be an amazing opportunity to help me learn a great deal about it. The fact that we will be focusing primarily on creating a covert channel will help me much more than if we were studying how to defend against them, since the job I currently have my eye on for after graduation is a penetration testing position. Many of the skills I have mentioned so far will be tested throughout this, especially agile development and working in a linux environment. I hope that this process will improve these existing skills, and that it will allow me to develop new ones that will help me grow as a programmer.

Our approach to this project will be to first gather as much information about covert channels as we can, and familiarize ourselves with them. Then, we will begin to work on creating one as a proof of concept. We hope to eventually be able to make a paper showcasing a great deal of information surrounding the creation of covert channels, through both first-hand experimentation, and second-hand research from other sources that we will have gathered. At a minimum, in order to consider ourselves done, we will have to make an example based on our paper, to show that it works. Hopefully, we will be able to show multiple examples on different systems. Personally, I think that our team will have done a “good job” if we are successful in our demonstration, and if our paper is able to contribute meaningfully to the field of cybersecurity.