My individual contribution to this project was completing our OS channel, and creating the first draft of the receiver portion of the Network Channel. The OS channel was based on an exploit discovered in 2017 known as Meltdown. The skills I learned in EECE 4029 wound up being the most useful, as a large portion of the code I wrote for the OS channel required a deep understanding of how operating systems accessed kernel memory. Cryptography wound up not being very important in the OS channel, as the concept behind the covert channel mostly involved hiding data, rather than encoding it. I did wind up creating it on Linux, so my previous Linux command knowledge did come in handy.

The biggest obstacles I wound up facing were the knowledge barrier required to make any of my code, and finding out that the initial plan of making meltdown wouldn’t work. The OS channel required me to understand fully how memory is structured, how out of order execution works, and how to manage the cache with flush+reload. Meltdown wound up also not working, because since its discovery, it seems to have been patched; I was unable to get it to work with the sample meltdown experiment from seed labs. In the end, though, I was able to get flush+reload working more consistently than the seed labs sample code, and I was able to fully explain the code with comments, and explain how it would function differently if meltdown was still functional.