**Computer Science**

| Contract | Term | Course | Contract Title | Description |
|---|---|---|---|---|
| 379082 | Spring 2018 | CPSC 4160 | Bluetooth LE and Predictable Random Numbers | In this project, I will use the theories of cryptography taught in class and analyze their importance in modern, in-use protocols and applications. Specifically, I will delve into Psuedo-Random-Number-Generators (PRNGs) found in Low Energy Bluetooth devices. The cryptographic significance of random numbers is evident - they play an essential role in establishing secure connections, both in confidentiality and authentication between two parties. PRNGs can be found inside Bluetooth devices, but there are often limitations of each device with regards to generating large quantities of random numbers; as a result, we seek to use external Bluetooth adapters for our research instead of commercial Bluetooth devices (the Bluetooth adapters still utilize the same or similar Bluetooth technology, so there is no differentiation in using one or the other in terms of final results). Bluetooth LE dongles can be found online, and they are often combined with a USB adapter, making analysis of devices relatively straightforward. I will analyze the PRNG numbers given by each compatible device used, which may be 1-3 dongles, against the NIST statistical test suite (STS), which tests for randomness in given values. If time permits, I may also test against multiple test suites for randomness. The project, essentially, is an in-depth analysis of one security aspect: random numbers; the objective is to report the security level (e.g. low-security, high-security) of each Bluetooth dongle. |