Reflection

The course aimed to offer practical, hands-on learning in computer hardware security. It was designed to give us an experience in "ethical hacking" into a computer system at various levels, helping us understand and protect against security vulnerabilities in hardware. The course successfully developed and utilized a custom-designed hardware platform called HaHa (Hardware Hacking board). This platform supported over a dozen experiments to teach hardware security fundamentals, attacks, and countermeasures. It enabled us to perform experiments without the need for additional benchtop electrical measurement units, making it suitable for online learning. My accomplishments include learning about how the hardware works and how several methods can be used to go around it to access the information or data provided. Visualizing that in a real-world scenario from the manufacturer's perspective and the hacker's perspective was really interesting. There were several challenges faced while doing certain experiments like compiling the .hex file or figuring out how to compile to generate the .fs file was confusing. The instructions were provided in the PowerPoint but they were not understandable when it came to usefulness. Several things were just playing around with the software to figure out if the process being done would result in anything or not. There were several challenges in the coding process too where a chunk of code and information were provided and we had to understand it ourselves with no external information or help. The tools were cool but some information provided on the PowerPoint might have been outdated where the option they told us to choose did not work at all and alternatives did. In the end, it was a huge learning curve for me. The experiments were engaging to learn more about ethical hacking and hardware security. My proudest success was definitely being able to run the experiment without any trouble. There were problems in every step taken forward in the experiments. Being able to understand and run the programs was my proudest moment. Some of the interesting ones were the ciphers about how the specific bytes play a specific role in it and how it can mess up the decryptions. The other one was a Bus Snooping attack using Ground pins, MISO and CLK in the Haha Board.

Expanding the range of experiments and topics covered to include emerging threats and countermeasures in hardware security would really be interesting. Working this as my future job would be really fun if it had experiments that align with the latest developments in hardware security and if the documentation were actually helpful where if someone as basic level as us were to start. Other improvements could include topics like quantum computing security, advanced persistent threats in hardware, and firmware analysis. Integrating more advanced tools and techniques for hardware analysis and security testing. Collaborating with industry partners to provide real-world case studies and examples would be the best. Going out in the real world to solve several problems would be great. This project highlights the importance of hands-on learning in technical education, especially in fields like hardware security where practical skills are crucial. It demonstrates the effectiveness of custom-designed educational tools in enhancing the learning experience. The project's success in making complex topics accessible and engaging can be a valuable experience for future educational and training program designs. Going out in the hardware side or even the documentation process could be helpful in the future with these experiments. The ability to

adapt and provide meaningful online learning experiences in hardware security is particularly relevant in the current educational landscape. Working on such a project deepens the understanding of hardware security, a critical and ever-evolving field. This expertise is valuable in numerous technology sectors, including IT, cybersecurity, and embedded systems developments. Designing and implementing course materials and experiments hones your problem-solving skills. We learn to address complex technical challenges, which is a highly transferable skill applicable in various professional situations. Conducting research and analysis for the course strengthens the ability to gather, interpret, and utilize data. These skills are crucial for decision-making and strategy development in any technical role. Focusing on ethical hacking and the responsible use of technology raises our awareness of the social and ethical implications of technology. This perspective is increasingly important in a world where technology impacts almost every aspect of our lives.

-Experiment 0: completed; Missing steps of using Gowin Analyzer Oscilloscope using Waveforms (was not working properly).
-Experiment 1: completed; updated documentation, added source code used.
-Experiment 2: completed; updated documentation; added source code used.
-Experiment 3: completed; updated documentation
-Experiment 4: partially completed; could not progress beyond part 1 because the Gowin Analyzer Oscilloscope was not functioning; added sample source code used
-Experiment 6: completed; updated documentation; not sure if the BOM and schematic are correct
-Experiment 8: partially completed; updated documentation; added .hex compiled that was compiled; could not run it through programmer in GOWIN at last