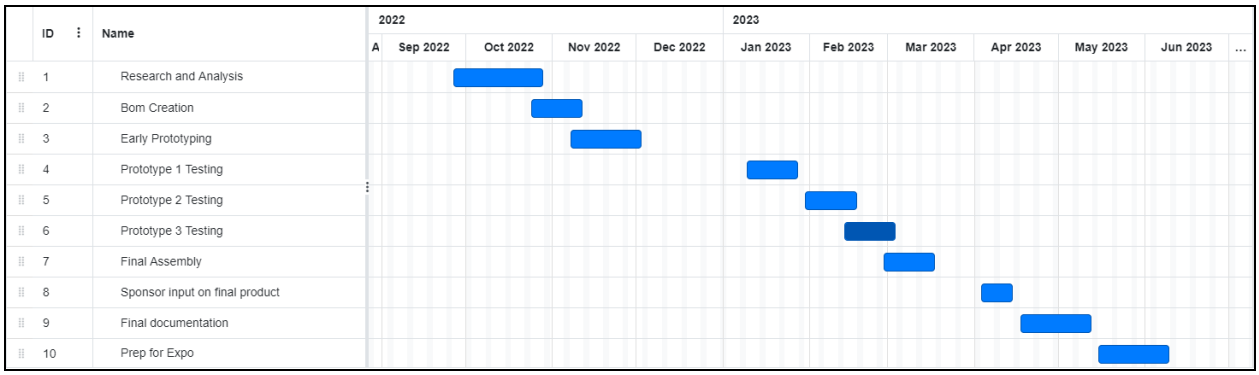
ECE44X Security of Electronic Safe Locks Executive Summary

The purpose of this project is to analyze a LAGARD Combogard Pro 39E electronic combination safe lock in order to discover and characterize the potential vulnerabilities for the purpose of opening the safe lock without knowledge of the pin.

This project started in the research phase where the project group was given the choice between different locks and decided to choose the LAGARD 39E as it has some challenging features to overcome and no previous research beyond pointers given by the project sponsor professor Vincent Immler. During this phase, the team worked on applying different hardware security techniques such as side channel analysis, timing analysis, and power supply vulnerability. Side channel analysis is the technique of analyzing the digital waveforms coming in and out of the lock in order to determine if there is an exploitation within the signal in order to guess at the pin or open the lock. Timing analysis looks at the timing between the output waveforms to try and tell if certain keypad inputs give a different output timing, helping guess at the correct pin. Lastly, power supply vulnerability is commonly used to shut down the power to the lock in order to stop the lockout process, leading to an infinite number of attempts of unlocking the device. During this research phase the team determined that there existed only two vulnerabilities, one that the power supply could be interrupted to stop the lockout and second, that there existed some sort of timing delay between the correct and incorrect pin combinations.

After vulnerabilities were identified in the lock's structure the team decided to build three main modules: one was the analog keypad input that allowed a microcontroller to emulate the keypad on the lock in order to automatically try different keypad combinations, the next was the brown-out circuit that would cut power if a wrong input was detected, and the last was a photo-LED circuit that could read the output LED and try to guess the timing difference between the output signals. Additional support modules were created such as a user interface using a touch screen that allowed readout of the found pin, a loading bar to show timing, and a restart button to use on multiple locks. The other support module was the power supply so that the system could be powered independently of a laptop or bench supply. This lines up with the timeline given below.



One major turning point of the development phase was finding out that a random seed generator was used within the firmware of the lock that randomized the timing of the output, making it almost impossible to tell if the correct input had been given to the lock. Further research on this is needed, as doing a probabilistic analysis on the output timing could detect the seed used and therefore allow future students to decode the correct pin using the photo-LED. This led the team to scrapping the photo-LED as the vulnerability had been patched. The other major turning point that was identified was that the brown-out could only be done before the output LED and buzzer was triggered, making it so the only way to successfully brown-out would not yield a right or wrong output. The only way to tell if the device had successfully opened was if you tested every pin twice, leading to double the time necessary to open the lock.

Current work includes continuing the timing analysis and dumping the firmware of the lock. If the team is able to determine the random seed and capture it, a mathematical formula can be created within the microcontroller that can then decode the timing and give a successful guess on the pin. Additionally, project sponsor Vincent Immler is working with his graduate students to dump the firmware of the lock, allowing the team to see inside and know the vulnerabilities that are contained within for sure. The drawback of dumping the firmware is that it takes too long and will not be completed before the end of the project, so it will be for the next set of students to complete.

Overall, the project was mainly built upon research of the lock and potential vulnerabilities, not opening the lock. But, because the team worked so hard we were able to create a device that opens the lock, just not in a small amount of time. Learning that in a research project, there might not be a right answer, is very tough as the objective of the capstone is to create a product that works. This sets this project apart from some of the others such as the wearable device as it cannot be marketed or sold. Another valuable lesson learned from this project is how to work with team members in an ever stressful environment. Meeting deadlines and self-motivating the team in order to complete the project is hard but fulfilling when you go to the final check-off and your system works. Teaching yourself how to keep on schedule and meet the deadlines per the timeline above is a skill that will be necessary in the engineering industry as there are no assignment deadlines or teachers assistants to keep you on track. The last and most important lesson for any engineer is how to collaborate with others on projects. This is something everyone in the group had to work towards as each member worked with each other on not only their own blocks but on their peers in order to help each other succeed. This is a valuable skill for industry as you will not only have your own assignments, but group assignments that you will have to work on with other engineers.