Jacob Braddock

Cybersecurity

Dr. Michael O’Neil

May 2025

**Senior Project Design: Problem Statement**

The data and files that people have on their personal computers have become less and less safe within the modern age. The user’s personal computer should be able to keep safe the information stored upon it without risk of possible data theft, leaks, or other means of said file tampering that should put the information on the terminal at risk. This of course is a dream rather than the actual case.

As the worldwide web grows more and more, this problem exasperates to higher and higher degrees. In a study performed by the Identity Theft Resource Center (ITRC), from January 2023 to September 2023, tracked 2,116 data compromises, a 17 percent increase from 2022’s 1802 (Q3 2023 Data Breach Report: Identity Theft Resource Center Reports Data Compromise Record with Three Months Left in the Year, 2023). This was a result in the combination of the increase in phishing attempts, zero-day exploits (targets software vulnerability to which there is no patch), ransomware attacks, and other various malware attacks. There is no shortage of these attacks, and the drastic uptick has been increasing, and increasing with the fast passage of time.

There is one solution in my mind, that is an attempt to rectify this problem, or at least create a source of protection against these attacks. The creation of file-encryption software to protect files from such attacks. If a terminal were to contain private pieces of information, information that would be so detrimental if compromised, there needs to be a system in place to protect those files from such malicious means. The use of encryption is almost a sure-fire way to prevent access to said files except to the user itself, to make only the information readable to the owner of said computer. The use of keys to access and file encoding turns most vulnerable PCs into much more secure pieces of tech with almost unreadable files.

In a world with an ever-expanding web, there is no shortage of the number of nefarious deeds that come along with it. Accounts to our favorite websites, our most precious files, and even our computers are never truly safe in this age. This problem only grows more and more as the years tick on and the black hats of the cyberworld get better and smarter. There are means to attempt to protect the masses however, to try and protect those who need it. With the usage of something like an easy-to-use file encryption software, there is a chance that people can help protect themselves from the dangers lurking on the web.

The language I would propose in the creation of this program would be C++ or C# as both would be a more professional code to use, so to speak, in the coding world. In terms of possible libraries, packages, etc. I will be using in the development of my program; I am undecided but open-minded in terms of what will be used. However, I have investigated using Crypto++ given that it is a free and open-source C++ library that dabbles into the field of what I am doing. In terms of other needed software or equipment, it is currently unknown what I would need. As I progress into this project, I would most likely have a greater idea of what would be necessary for use.

I personally want to develop this program for a couple of different reasons, though in summary I want to provide something useful to people. I switched my major from kinesiology to cybersecurity out of my pursuit to chase something that would make me happy to do in life, and ever since entering the program I have never felt more at home in the field. This project is perhaps my way of not only helping people but being able to give something back and make a mark on the field in the process. I think being able to protect people and show off what I can do with everything I have learned so far, it would be such a huge honor to do such a thing. In terms of my major though, I think learning computer safety in a physical manner becomes very important as a cybersecurity major. I need to know how to protect computers of all kinds from other people who need assistance with myself, as if I become compromised in my own safety then how could I ever hope to protect anyone else.

I plan on completing the project by mostly following the turn in date guide as my basis for pacing myself along with the belief I cannot just do this entire project at the last minute. There are expected turn in dates to hit with physical, actual files and documents to turn in that must be hit so I will be turning in everything from those requirements and the syllabus. I have already agreed and set up to meet my advisor every Wednesday for questioning, project check in progress, and anything else I may need assistance with. I also plan and will contact him any time I need help or assistance with the code should it stump me, be it information, recommendations, or help in problem solving with the code. Submitted along with this is a WBS which contains various dates that I would wish to use as the checkpoints for certain points of the project.

Reference

Identity Theft Resource Center. (2023, October 3). *Q3 2023 data breach report: Identity Theft Resource Center reports data compromise record with three months left in the year*. ITRC. <https://www.idtheftcenter.org/post/q3-2023-data-breach-report-itrc-reports-data-compromise-record-with-three-months-left-in-year/>