Criterion E: Evaluation

Product Evaluation

After consultation with my client (Appendix II), we concluded that I had accomplished all the success criteria. All requirements were met based on my test plan, as shown in the Criterion D video. Discussions with my advisor and father also resulted in positive reviews, with them saying they would consider using it.

Success Criteria	Met?	Client Review (Appendix II - not in word count)
I. A master password is required to access the main menu; the user can create one if one does not exist.	Yes - it will show a separate window if a master password is needed. Otherwise, there is a login page.	"I was able to create a master password when I started the program, which gave me peace of mind knowing that my passwords are secure. Perhaps include information on how to choose a strong password, but otherwise, well done."
II. There are limited login attempts with an incorrect master password.	Yes - there is a limit of 3 attempts before the program closes.	"I like that there are limited login attempts with an incorrect master password. It makes me feel more secure knowing someone can't keep guessing my password indefinitely. However, I believe it would be more secure to block them from trying again for a certain amount of time, not just having the pain of having to constantly re-open the application."
III. An account list, retrieved from an XML file and displayed in the main menu, is sorted in descending order, with the most-used accounts at the top.	Yes - the account list is sorted in descending order based on usage.	"A great feature that works perfectly. It makes it easy to access accounts quickly."
IV. Users can add, remove, and filter/search items from the account list.	Yes - users can add, remove, and filter/search items in the account list.	"The program gives me complete control over my passwords and accounts, which is very useful. At times on my laptop, I have to move around the adding account window for it to fit on my screen, so maybe make that a bit smaller."
V. When adding an account, users can generate strong, randomized passwords that meet standard password complexity requirements.	Yes - users can generate strong passwords that meet common complexity requirements.	"I'm really glad you added this feature. This was one of the main things that I struggled with, and I believe one of the main motivators of this project. Now I don't have to worry about creating a secure password myself. Thank you."
VI. Users can select a	Yes - users can select a	"The renewal period feature is great. It helps me

renewal period for a password when adding an account. The program will display a message when a password is about to expire.	renewal period for passwords and receive expiration reminders.	keep track of when my passwords need to be changed. As someone who likes to procrastinate, though, it might be best to notify me of the renewal deadlines as soon as I log in - maybe run the password scan feature automatically, although I'm not sure if I would like that."
VII. The data is secure and encrypted with AES-256 using a password-based encryption key.	Yes - data is encrypted with AES-256 using a password-based encryption key.	"I have no idea what AES-256 means, but I feel confident my information is secure. I opened the XML file and saw that everything was scrambled, so good job."
VIII. The client, my mother, considers the program easy to use.	Yes - my mother is satisfied with the program.	"I'm very thankful for this program and will definitely be using it for a while. [...] There are some very small changes you can make with spelling. Also, the icon color makes it blend into my windows bar, if you could change that? But other than that, I figured out how to use it quickly, so I think everyone else will be able to as well. Thank you very much; I like that I can quickly access all my passwords in one place."

Future Improvements

I enjoyed this project and plan to continue developing it in the future. Extensibility ideas are listed in Appendix IV.

Recommendation for Improvement	**Benefits**	**How?**
Ability to export unencrypted passwords	Useful for backup purposes or migration to another password manager.	A secure export function that requires the user to enter their master password again, decrypt the accounts.xml file, and then export it as a separate file. This IA has given me a lot of experience with decryption and writing files.
Prompt user about expired/expiring passwords as soon as they log in	Helps users quickly identify passwords that need to be changed. This can increase the security of their accounts and reduce the risk of password-related breaches by mitigating the risk of them forgetting to renew them.	A reminder function that iterates through the expiration date of passwords upon login and prompts the user to change them if necessary OR open the password scan window along with the main menu. This would be a change that could be done in less than an hour.

Add a login time restriction after 3 incorrect logins	Can prevent unauthorized access to the account list by drastically increasing the time it would take to crack.	Implement a time restriction feature that locks the program for a set amount of time after three incorrect login attempts. This can be done by having an encrypted text file with login attempt timestamps and a function to check if multiple login attempts have occurred within a certain period. This would be a large but feasible project.

Word Count: 252