Project Specification

Working Title

Lukasz’s Password Manager.

Project Aim

This project is to create a free and open-source password manager for the privacy focused user.

Project Expectations

This is a product focused security project. The main expectation is to create a password manager. The main expectations for the password manager are:

- Create a cryptographic container for the password data based on previous works and own research, like Linux LUKS (cryptsetup, 2020). This would allow for:
  - A way to recover the encrypted data without a password by using a recovery phrase.
  - A way to distribute the secret recovery data into pieces, with thresholds by implementing Shamir’s scheme (Adi Shamir, 1979).
  - Multiple passwords to be used to open the container.

- Make a password manager that:
  - Implements the container described with all of its features.
  - Implements basic password manager features:
    - Add/Remove/Update passwords.
    - Allow exporting passwords.
    - Change encryption specific settings.
    - Generate secure passwords.

- Implement code unit tests that:
  - Verify the password manager is encrypting and decrypting correctly.
  - Verify data can be recovered with:
    - A password.
    - Another different password.
    - A recovery phrase.
    - Shamir’s scheme.

The secondary project expectation is to explore different encryption methods and choose the best encryption method or methods for the password manager.

Good practice

Good practice will be shown by using design patterns and unit testing.

Git version control should also be used as git provides better workflow. It allows room for collaboration in the future. It also doubles as a diary of changes to the program.

Cryptographic Container and Research

The container will be the bulk of the research. The container will be able to recover the encrypted data without a password by using a recovery phrase, generate the secret recovery data into pieces and allow multiple passwords to be used to open the container.

The research will find the best techniques in terms of security and performance to allow the container to exist. Similar approaches like LUKS (cryptsetup, 2020) exist. In summary, the best encryption methods will also be researched and considered.

Features and Evaluation

Because this is a project focused on the product, most of the marks should come from number of planned features in the password manager that are implemented and working. Other metrics like security of data and performance of the program should be considered when marking.

Some marks should come from the research and decisions made while developing the password manager. Marks should be awarded given the extensiveness of the research and own experimentation.

Bibliography

Adi Shamir (1979) ‘How to Share a Secret’, *Massachusetts Institute of Technology*, 22(11), pp. 612–613.

cryptsetup (2020) ‘Cryptsetup and LUKS - open-source disk encryption’, *What the ...?*, 21 December. Available at: https://gitlab.com/cryptsetup/cryptsetup (Accessed: 14 January 2021).

Mark Scheme

REPORT	*70% +*	*50-69%*	*40-49%*	*Weighting* *(should add up to 100)*
Introduction (aims and objectives) *(10%)*	*Well written + critical overview of topic, concisely summarising key point. Purpose and issues clearly defined*	*Good introduction to content of the report. Key points identified.*	*Basic introduction with brief summary of points which the project will address. Key points are possibly incomplete or lacking in details on how they interrelate*	*10*
Research/Investigation *(max 50%)*	*Well written/practical investigation into different kinds of encryption methods, comparing different characteristics of each method.* *Well reasoned justification of chosen encryption method for each component of the program.* *Appropriate evaluation of encryption methods chosen – explaining why they are subtile.*	*Identified different kind of encryption methods and characteristics.* *Justification for the encryption method chosen for each component of the program.* *Appropriate evaluation of encryption methods chosen.*	*Show basic understanding of encryption methods.* *Selected and discussed an encryption method for each part of the program.* *Evaluate the performance of the method of encryption chosen.*	*5*

Product Development ***(max 50%)***	***Produce a secure password manager with password manager features.*** ***Implemented all recovery and export features for the password manager.*** ***Discuss good practice techniques that were used while developing the password manager as well as their positive impact on the project.*** ***Show the clear use of design patterns for good coding.***	***Produce a secure password manager with some standard password manager features.*** ***Implemented most recovery and export features.*** ***Discuss good practice techniques that were used while developing the password manager.*** ***Show some use of design patterns.***	***A basic password manager without any encryption, security or additional features.*** ***Implement export features.*** ***Show understanding of good practice techniques that were used while developing the password manager.*** ***Design pattern implementation attempted.***	***50***
Evaluation + Conclusions (to include research and development where applicable) ***(max 25%)***	***Summary describing the chosen encryption method detailing the specific numbers in regards to performance and security, with data to back up claims.*** ***Scaling recommendations are presented if this were to be used in a bigger context.*** ***Critical review of the whole project.***	***Summary briefly describing the chosen encryption method and show some metrics in regard to the performance.*** ***The reflection is not critical, but still reflects on the project as a whole.***	***Summary describes performance of the chosen encryption method with little data to back it.*** ***There should be some reflection on the word done on the project.***	***20***
Professional Practice (Project Management and Evaluation of Professional Skills) ***(10%)***	***Critical evaluation of the overall project with excellent analysis of the methodologies involved. Project limitations covered***	***Good evaluation of the project and methodologies. Project management techniques used***	***Limited or partial evaluation of project and project management techniques.***	***10***
Presentation, Layout and Referencing ***(5%)***	***Excellent standard of appearance. Report is well structured and organised. Free (or minimal) spelling or grammatical errors – if any, it does not detract from the reading of the report. Sources fully cited. Correct use of 3rd person***	***Good standard of appearance with a logical flow. Sources cited. 3rd person used throughout or in majority.***	***Report conveys across the intended message. There may be sections that impact on the logical flow and structure. Sources cited but possible inconsistent or lacking correct referencing back to the main document. Grammar and/or spelling impacting on readability.***	***5***

				100
PRODUCT + PRESENTATION	***70% +***	***50-69%***	***40-49%***	***Weighting***
Quality of Product – define a set of metrics for product ***(80 marks)***	***Standard password manager features present (5+).*** ***All recovery options (3) working and demonstrated.*** ***Password unlocks the password manager's data in a fast and efficient manner.*** ***Will demonstrate that the user will not run out of password storage.*** ***Will demonstrate that the program will not slow down with a large database.***	***Standard password manager features present (3+).*** ***Most recovery options (2+) working and demonstrated.*** ***Password unlocks the password manager's data.*** ***Will demonstrate that the user will not run out of password storage.***	***Password manager missing standard features (3-).*** ***Recovery options (1-) missing from password manager.*** ***Password unlocks the password manager's data.***	***80***
Presentation/QA ***(20 marks)***	***Presentation contains an accurate overview of all aspects of project management implementation and evaluation. Supported and demonstrated well through QA***	***Presentation contains an overview of most aspects of project management implementation and evaluation. Supported and demonstrated through QA***	***Presentation contains a limited overview of aspects of project management implementation and evaluation. QA is limited to specific point.***	***20***
				100

Risk Register

ID	Risk Description	Likelihood	Impact	Impact Description	Severity	Severity Description	Owner	Mitigation	Status
Equipment During Development									
e1	Multiple Screen failures	Unlikely	None		Medium	There are only two screens on the developmental machine. If both fail, the development would have to be carried out on a different machine or a new screen would have to be bought.	Lukasz	Continue project on another device until a replacement screen arrives.	Open
e2	PC backup HDD fail	Likely			Low	If the HDD that is used for backups of the HDD is very old and might fail. Since this is only a backup, it should not hinder the project.	Lukasz	Find another backup solution	Open
e3	SSD fail	Unlikely			High	As the SSD is the primary location for the operating system in the configuration, the computer would no longer boot and the data would be lost until the most recent backup/commit.	Lukasz	Reinstall the operating system onto a HDD	Open
e4	PC power supply fail	Unlikely			High	The computer would be unable to turn on, potentially slowing the development of the project	Lukasz	Continue project on another device until a replacement power supply arrives.	Open
e5	No wired internet access	Unlikely			Medium	There is a high dependency on the internet for documentation and.	Lukasz	Continue project by using mobile data.	Open
e6	No wired internet access (ID:e6) and no mobile data	Unlikely			High		Lukasz	Continue project without internet access and push changes to the server when possible.	Open
e7	Peripheral failures.	Unlikely			High	Without a mouse or a keyboard, it's impossible to continue to work on the project.	Lukasz	Continue project on another device until the replacement peripheral arrives.	Open
Resources Related Issues									
r1	Illness, specifically COVID-19	Likely	None		High	The implications of getting COVID-19 are that work could be delayed by at least a week or more, depending on the severity.	Lukasz	Rest and wait till the illness goes away and continue to work where possible.	Open
r2	Generic illness or other health problems	Likely			High	The implications of illnesses and health problems vary but they're never good. There is a good chance that the work will be delayed by some time and that during the effect of the illness/health problem, productivity will be at least decreased.	Lukasz		Open