UNIVERSITY OF BUEA

P.O Box 63,
Buea South West Region
CAMEROON
Tel: (237) 3332 21 34/3332 26 90
Fax: (237) 3332 2272

REPUBLIC OF CAMEROON

PEACE-WORKFATHERLAND

FACULTY OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER ENGINEERING

Security of Information Systems and Cyber Security (CEF 451)

PASSWORD MANAGEMENT AND DATA ENCRYPTION

By:

KAMCHE YANN ARNAUD, FE21A208

Option: Software Engineering

Academic Supervisor
Dr. TSAGUE
University of Buea
Academic Year: 2023/24

TABLE OF CONTENTS

INTRODUCTION

In an era dominated by digital landscapes and interconnected systems, the paramount importance of safeguarding sensitive information has never been more evident. As we navigate the intricate realms of cyberspace, the security of our digital assets, ranging from confidential passwords to critical data, becomes a pressing concern. This report delves into the realm of digital security, presenting a comprehensive guide on two essential aspects: password management and data encryption.

The report focuses on the utilization of two robust tools, KeePassX for securing passwords and VeraCrypt for encrypting data. Both selected for their open-source nature, strong community trust, and proven encryption algorithms, these tools stand as pillars in fortifying the digital defenses of individuals and organizations alike. The exploration encompasses their selection criteria, download and installation processes, key functionalities, and practical examples, offering a hands-on approach to implementing enhanced security measures.

As we delve into the intricacies of KeePassX and VeraCrypt, the report aims to empower users with the knowledge and tools necessary to navigate the dynamic landscape of digital security. Through the adoption of best practices in password management and data encryption, individuals and organizations can proactively mitigate potential threats, contributing to a more secure and resilient digital environment.

1- Securing Passwords using KeePassX

1.1 Why Securing Passwords?

In the digital landscape, the security of passwords is paramount. Password managers are instrumental in fortifying this security aspect by offering a systematic approach to password management. For this task, KeePassX, an open-source password manager, has been chosen for its robust features, cross-platform compatibility, and community trust.

1.2 Password Manager Selection

KeePassX stands out due to its open-source nature, which fosters transparency and community scrutiny. Its cross-platform compatibility ensures accessibility across various devices, and it boasts strong security features to protect sensitive information.

1.3 Download and Installation

To begin, download KeePassX from the official website, [1] and follow the installation instructions tailored to your operating system. The installation process is straightforward and user-friendly.

1.4 Functionality and Features

KeePassX operates on the principle of securely storing and managing passwords. The master password and/or key file act as the primary access keys. The application utilizes robust encryption algorithms to safeguard the stored data, ensuring a high level of protection.

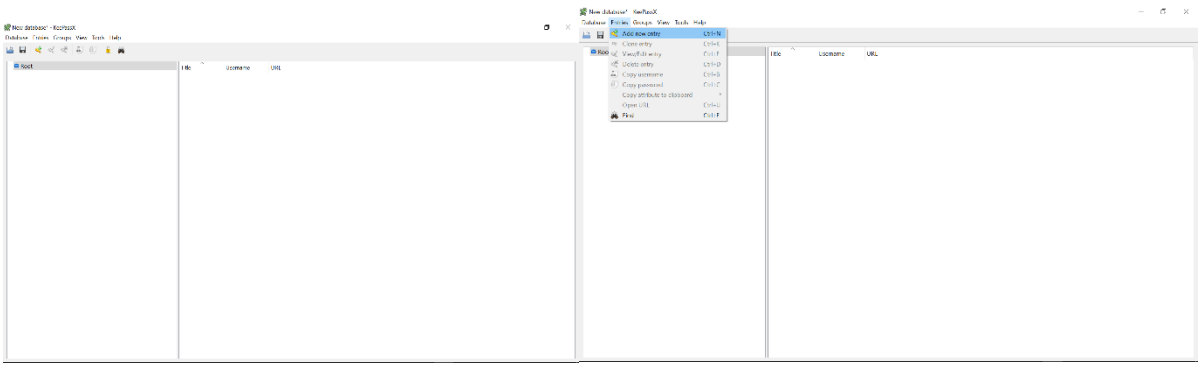
1.5 Examples and Illustrations

To exemplify the process of creating a new entry in KeePassX and subsequently securing a password:

Creating a New Entry:

- **Open KeePassX:**
  After installation, launch KeePassX from your desktop or applications folder.

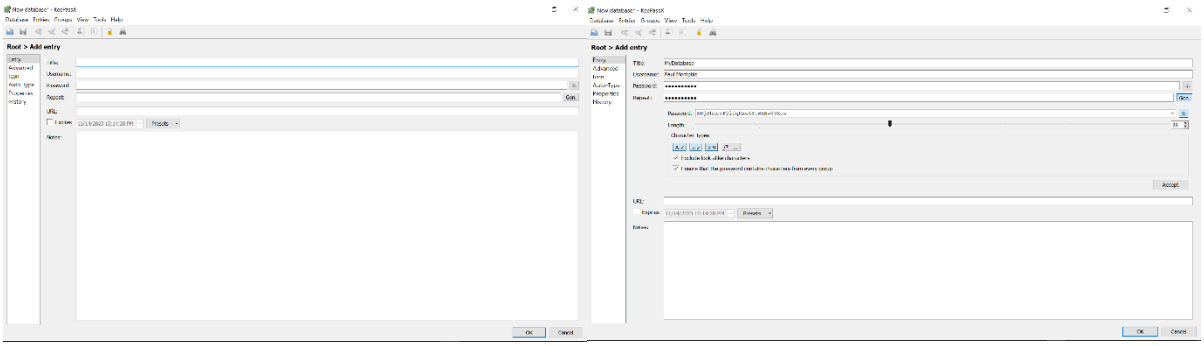
- **Navigate to "Add Entry":**
  Once inside the KeePassX interface, locate and click on the "Add Entry" button. This initiates the process of creating a new password entry.



- **Populate Required Fields:**

- A new window will appear, prompting you to fill in various fields such as Title, Username, and Password.

- Ensure the use of a strong, unique password, and consider utilizing the built-in password generation feature for enhanced security.



- **Save the Entry:**

- After filling in the necessary information, click on the "OK" or "Save" button to save the new entry.

- KeePassX will encrypt and store the information securely.

- **Verify Entry Creation:**

- Navigate to the password list within KeePassX to confirm the successful creation of the new entry.

1.6 Conclusion

In conclusion, KeePassX emerges as a reliable solution for enhancing password security. Its features, coupled with an intuitive interface, make it a valuable asset in the ongoing effort to fortify digital defenses.

2- Encryption Software using Veracrypt

2.1 Why encryption

Encryption serves as a crucial layer in the protection of sensitive data and hard disk drives. Veracrypt, an open-source encryption software, has been selected for its stellar reputation, open nature, and robust encryption algorithms.

2.2 Encryption Software Selection

Veracrypt's reputation in the cybersecurity community, coupled with its open-source nature, makes it a compelling choice for securing data. Its reliance on well-established encryption algorithms ensures a high level of data protection.

2.3 Download and Installation

Commence the process by downloading Veracrypt from the official website, [2]. The installation instructions, tailored for different operating systems, guide users through a seamless installation process.

2.4 Functionality and Features

Veracrypt operates by creating encrypted containers, be it file-based or encompassing entire drives. The encryption algorithms, including AES, contribute to a robust security framework, shielding data from unauthorized access.

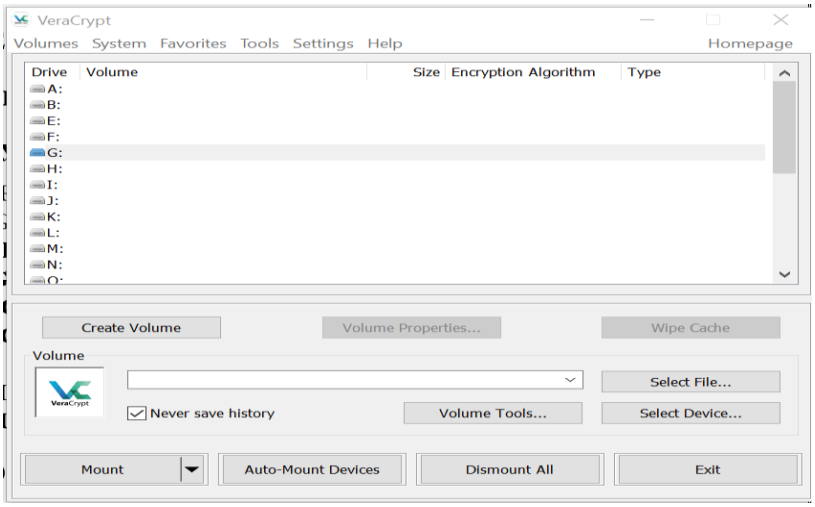
2.5 Examples and Illustrations

To elucidate the process of creating an encrypted container using Veracrypt:

Creating an Encrypted Container:

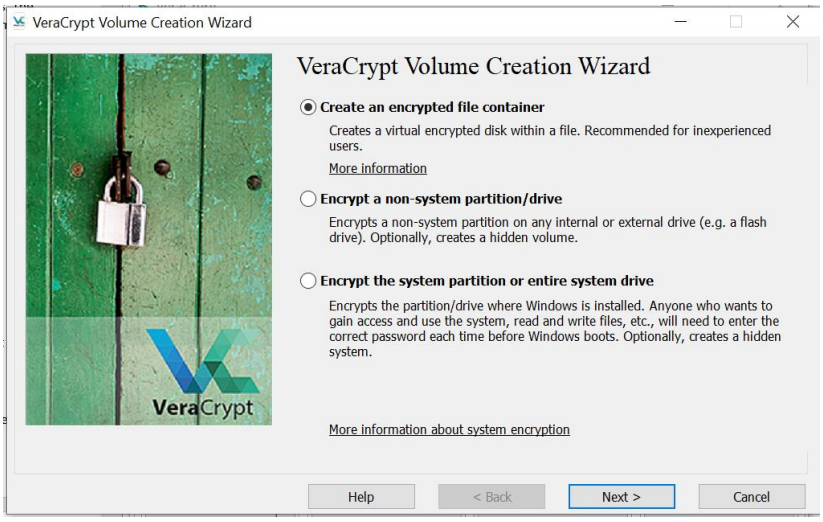
- **Launch Veracrypt:**

- Open the Veracrypt application after installation. The main interface will display various options related to volume creation and management.



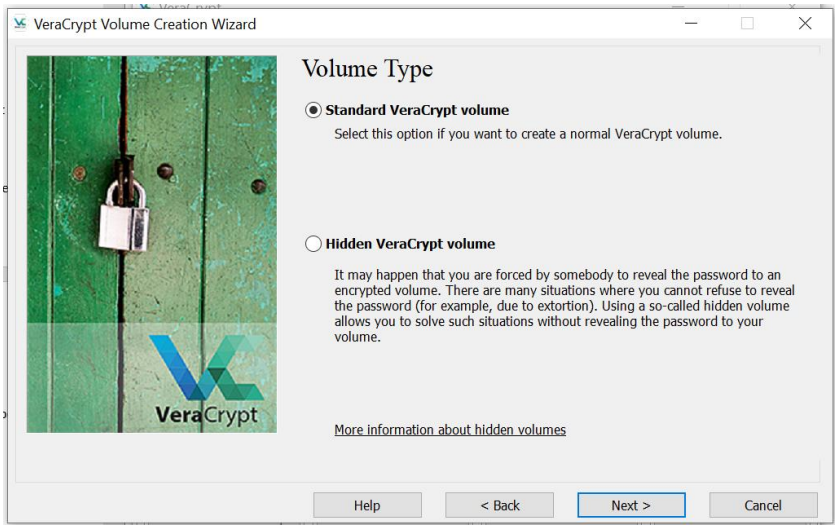
- **Select "Create Volume":**

- Within the Veracrypt interface, click on the "Create Volume" button. This begins the process of creating a new encrypted container.



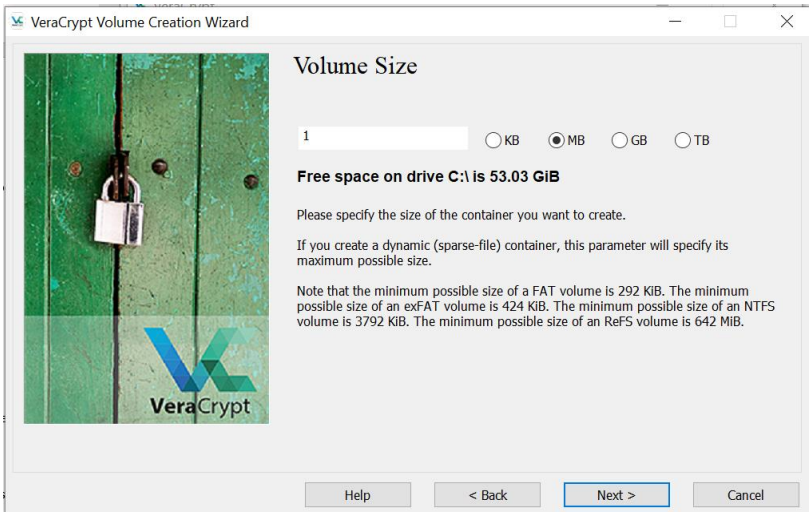
- **Choose Volume Type:**

- Veracrypt offers different volume types, including a standard volume or a hidden volume. Select the appropriate option based on your security requirements.



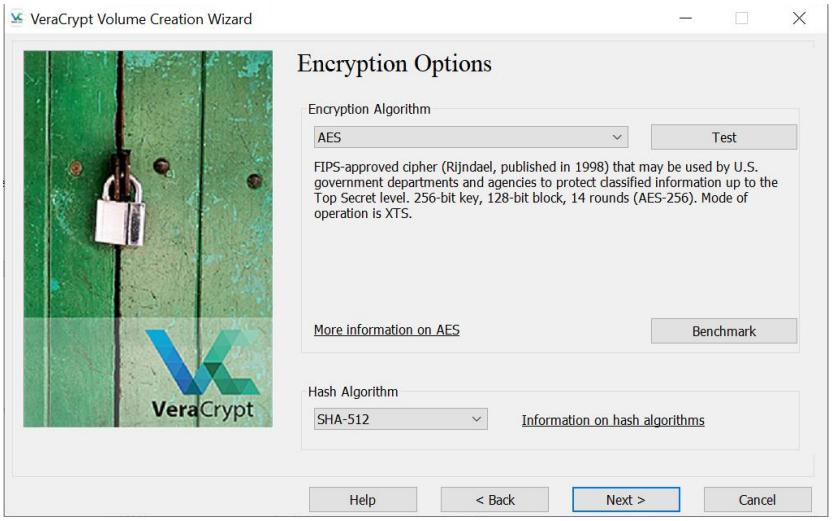
- **Specify Location and Size:**

- Indicate the location where the encrypted container will be stored. Define its size, ensuring it meets your storage needs.



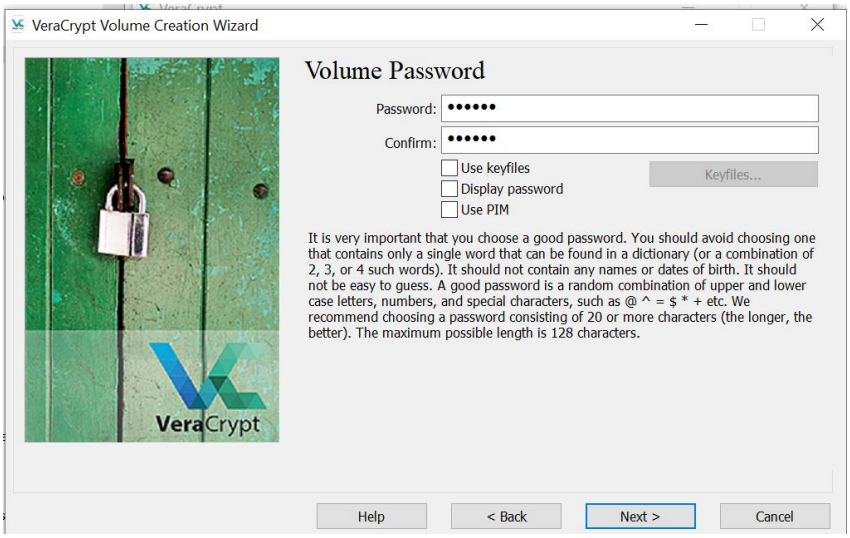
- **Set Encryption Options:**

- Choose the encryption algorithm and hash algorithm based on your preferences. Veracrypt supports robust algorithms such as AES for encryption.



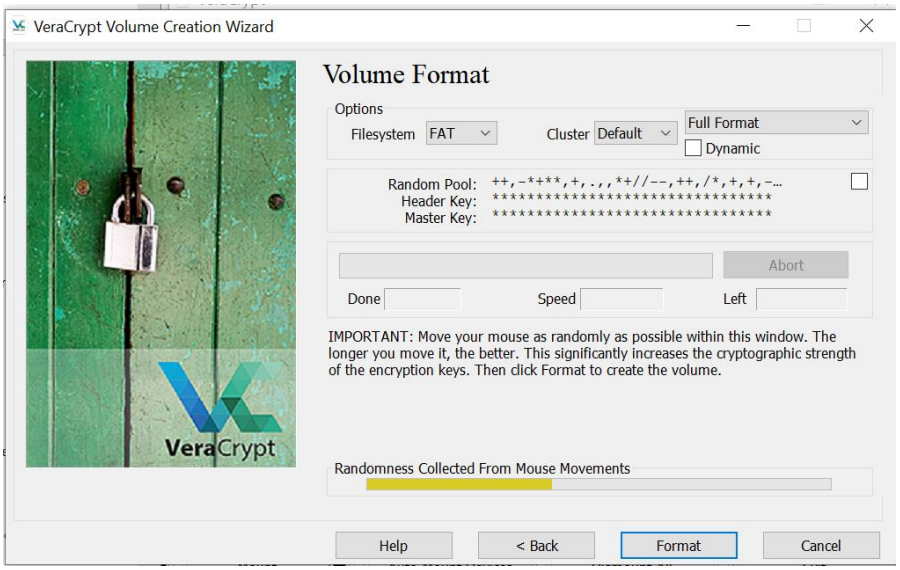
- **Set Strong Password:**

- Define a strong and unique password for the encrypted container. Utilize Veracrypt's built-in password strength indicator to enhance security.



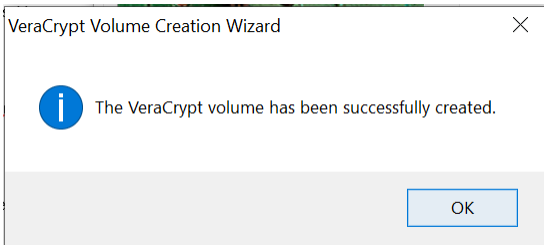
- **Complete the Process:**

- Follow the on-screen prompts to finalize the creation of the encrypted container. Veracrypt will encrypt the container, making it accessible only with the specified password.



- **Mount the Encrypted Container:**

- Once created, use Veracrypt to mount the encrypted container. This process establishes a secure connection and allows you to access the encrypted data.



2.6 Conclusion

Veracrypt proves to be an indispensable tool for encrypting sensitive data, providing users with a secure and efficient mechanism to protect their files and drives. Its comprehensive features and user-friendly interface make it a standout choice in the realm of encryption tools.

REFERENCES

[1] KeePassX Official website, [https://www.keepassx.org/downloads]

[2] Veracrypt Official website (https://www.veracrypt.fr/en/Downloads.html)