Introduction à la Sécurité Informatique

Titre du Rapport : Rapport sur le Gestionnaire de Mots de Passe

Mehdi Oudghiri

Sommaire

I. Introduction

A. Présentation du projet

Dans un écosystème numérique où la gestion de multiples identifiants et mots de passe devient un défi quotidien, l'importance d'une gestion sûre et efficace de ces clés d'accès est indéniable. Ce rapport est consacré à la présentation d'un projet de fin d'études : le développement d'un gestionnaire de mots de passe. Ce projet vise à concevoir un outil capable d'assurer une gestion sécurisée et centralisée des mots de passe. Il se veut être une réponse aux défis posés par la sécurité des informations d'identification dans le contexte actuel de menaces cybernétiques en constante évolution.

B. Importance des gestionnaires de mots de passe

L'adoption de gestionnaires de mots de passe est devenue une nécessité dans notre quotidien numérique. Cela est dû à l'augmentation exponentielle des comptes en ligne par utilisateur et des exigences de sécurité complexes pour les mots de passe. Les individus se retrouvent souvent à jongler avec de nombreux mots de passe, ce qui peut conduire à des pratiques peu sûres comme la réutilisation des mêmes mots de passe ou l'utilisation de mots de passe trop simples et prévisibles.

Les gestionnaires de mots de passe offrent une solution à ces problèmes. Ils permettent de stocker de façon sécurisée l'ensemble des mots de passe sous une forme chiffrée, réduisant ainsi considérablement le risque de violations de données dues aux attaques par force brute ou à d'autres méthodes d'effraction. En facilitant la création et la gestion de mots de passe forts et uniques pour chaque service, ces outils jouent un rôle crucial dans l'amélioration de la posture de sécurité globale des utilisateurs.

II. Présentation

A. Objectif et fonctionnalités du gestionnaire de mots de passe

Le gestionnaire de mots de passe que nous avons développé vise à offrir une solution sécurisée pour le stockage et la gestion des identifiants et mots de

passe. Il permet aux utilisateurs de conserver leurs informations de connexion dans un coffre-fort numérique sécurisé, accessible uniquement via une authentification forte. Les fonctionnalités clés incluent la génération de mots de passe forts, le stockage crypté, l'auto-remplissage des formulaires de connexion, et la possibilité de changer rapidement les mots de passe sur les sites web pris en charge.

B. Architecture et technologies utilisées

Notre gestionnaire de mots de passe s'appuie sur une architecture légère et efficace, conçue pour garantir à la fois la facilité d'utilisation et la sécurité. Ci-dessous, nous décrivons les composants clés de notre système :

- **Architecture Simplifiée** : Le système est structuré autour d'une application de bureau autonome, éliminant la nécessité de communications complexes entre le client et le serveur, ce qui réduit les surfaces d'attaque potentielles.
- **Langage de Programmation** : Nous avons opté pour [Python, réputé pour sa robustesse et sa facilité de maintenance, permettant une mise en œuvre efficace de l'interface utilisateur et des algorithmes de cryptage.
- **Bibliothèque de Chiffrement** : Le choix de la bibliothèque [Nom de la bibliothèque de cryptage] nous permet d'implémenter les algorithmes de chiffrement standards de l'industrie sans avoir à les concevoir de zéro, réduisant ainsi le risque d'erreurs dans la gestion des données sensibles.
- **Stockage des Données** : Les données sont stockées localement sur la machine de l'utilisateur dans une base de données dans un fichier texte qui est cryptée à l'aide de l'algorithme Fernet pour assurer la sécurité des données en repos.
- **Interface Utilisateur** : L'interface utilisateur est construite avec une approche minimaliste, en utilisant Tkinter, ce qui permet une navigation intuitive et une gestion facile des mots de passe.

C. Chiffrement des mots de passe

Algorithmes de chiffrement utilisés

Pour garantir la confidentialité des mots de passe stockés, nous utilisons Fernet, une implémentation de cryptage symétrique qui repose sur l'AES en mode CBC. Cela assure un haut niveau de sécurité en combinant le cryptage AES pour la confidentialité et HMAC avec SHA256 pour l'intégrité des données.

Gestion des clés de chiffrement

La clé de chiffrement Fernet est générée de manière sécurisée et stockée séparément des données cryptées. Nous utilisons également un système de rotation des clés qui permet de changer régulièrement la clé de chiffrement sans compromettre la sécurité des données précédemment cryptées.

D. Stockage sécurisé des données

Base de données cryptée

Toutes les données sensibles, y compris les mots de passe et les notes sécurisées, sont stockées dans une base de données cryptée avec Fernet. Cela signifie que même en cas d'accès non autorisé à la base de données, les données restent protégées et illisibles sans la clé de chiffrement.

III. Interface utilisateur

A. Gestion de l'interface L'interface graphique de notre gestionnaire de mots de passe, construite avec Tkinter, fournit une expérience utilisateur fluide et conviviale. Les éléments de l'interface ont été disposés de manière à assurer une navigation intuitive et un accès rapide aux différentes fonctionnalités.

- **Disposition ergonomique :** L'interface est organisée en panneaux clairement délimités, permettant aux utilisateurs de localiser rapidement la fonctionnalité requise, que ce soit l'ajout d'un nouveau mot de passe, la recherche d'une entrée existante ou la configuration des paramètres de sécurité.
- **Thème et personnalisation :** Le thème visuel de l'interface peut être adapté aux préférences de l'utilisateur, offrant un choix de couleurs et

de polices pour une expérience personnalisée tout en préservant la lisibilité et l'accessibilité.

B. Fonctionnalités accessibles aux utilisateurs Le programme offre plusieurs fonctionnalités directement accessibles depuis l'interface principale, toutes conçues pour faciliter la gestion sécurisée des mots de passe.

- **Ajout et édition de mots de passe :** Les utilisateurs peuvent ajouter de nouveaux mots de passe ou éditer des entrées existantes à travers des dialogues modaux qui sollicitent les informations nécessaires tout en masquant les entrées sensibles.
- **Recherche et organisation :** Une barre de recherche dynamique permet aux utilisaires de filtrer et de retrouver rapidement les entrées spécifiques. De plus, les mots de passe peuvent être catégorisés, offrant une méthode d'organisation personnalisée.
- **Alertes et confirmations :** Des notifications contextuelles fournissent des retours immédiats sur les actions effectuées, comme la confirmation de l'enregistrement d'un nouveau mot de passe ou des alertes lors de tentatives de saisie incorrectes.

IV. Conclusion

A. Bilan du projet Ce projet de gestionnaire de mots de passe représente une avancée significative en termes de sécurité et d'accessibilité pour la gestion des données sensibles. En utilisant Tkinter pour l'interface utilisateur, nous avons réussi à créer un outil qui est non seulement fonctionnel mais aussi agréable à utiliser. Les algorithmes de chiffrement Fernet assurent la sécurité des informations de nos utilisateurs, tandis que la structure du programme et sa logique de programmation assurent une grande réactivité et fiabilité.

B. Perspectives d'évolution et améliorations possibles Bien que le gestionnaire de mots de passe actuel soit robuste, l'évolution continue des menaces de sécurité sur Internet nécessite une amélioration continue de nos outils de sécurité. Les pistes d'amélioration incluent :

- **Implémentation de l'authentification multi-facteurs (MFA) :** Pour renforcer la sécurité, il serait judicieux d'intégrer un système d'authentification multi-facteurs, offrant une couche supplémentaire de protection contre les accès non autorisés.

- **Synchronisation entre appareils :** Permettre aux utilisateurs de synchroniser leurs mots de passe entre différents appareils sécuriserait encore plus l'utilisation multiplateforme tout en maintenant la facilité d'accès.
- A**udit de sécurité régulier** : Mettre en place un audit de sécurité régulier du logiciel pour s'assurer que toutes les vulnérabilités sont identifiées et traitées rapidement.
- **Amélioration de l'interface utilisateur** : Continuer à améliorer l'expérience utilisateur sur Tkinter, peut-être en ajoutant la possibilité de personnalisation plus poussée de l'interface, ainsi que l'amélioration de l'accessibilité pour les utilisateurs ayant des besoins spéciaux.

En conclusion, le gestionnaire de mots de passe a réussi à atteindre ses objectifs initiaux de fournir un outil sécurisé, fiable et facile à utiliser. Les bases solides sur lesquelles le projet a été construit permettent d'envisager un avenir prometteur avec des améliorations continues répondant aux besoins changeants de la cybersécurité et de l'expérience utilisateur.