Département des Technologie de l'information et de la communication (TIC)
Filière Télécommunications
Orientation Sécurité de l'information

Travail de Bachelor

Gestionnaires de mots de passe : quelle sécurité ?

Étudiante **Noémie Plancherel**
Enseignant responsable Prof. Sylvain Pasini
Année académique 2022-2023

Yverdon-les-Bains, le 21 septembre 2022

Département des Technologie de l'information et de la communication (TIC)
Filière Télécommunications
Orientation Sécurité de l'information
Étudiante : Noémie Plancherel
Enseignant responsable : Prof. Sylvain Pasini

Travail de Bachelor 2022-2023

Gestionnaires de mots de passe : quelle sécurité ?

Résumé publiable

Dans ce travail... Ceci est le résumé publiable...

Étudiant :	Date et lieu :	Signature :
Noémie Plancherel	.....	.....
Enseignant responsable :	Date et lieu :	Signature :
Prof. Sylvain Pasini	.....	.....

Préambule

Ce travail de Bachelor (ci-après TB) est réalisé en fin de cursus d'études, en vue de l'obtention du titre de Bachelor of Science HES-SO en Ingénierie.

En tant que travail académique, son contenu, sans préjuger de sa valeur, n'engage ni la responsabilité de l'auteur, ni celles du jury du travail de Bachelor et de l'Ecole.

Toute utilisation, même partielle, de ce TB doit être faite dans le respect du droit d'auteur.

HEIG-VD

Vincent Peiris
Chef de département TIC

Yverdon-les-Bains, le 21 septembre 2022

Authentification

La soussignée, Noémie Plancherel, atteste par la présente avoir réalisé ce travail et n'avoir utilisé aucune autre source que celles expressément mentionnées.

Yverdon-les-bains, le 21 septembre 2022

Noémie Plancherel

Cahier des charges

Résumé du problème

De nos jours, les gestionnaires de mots de passe sont des outils très fréquemment utilisés. En effet, une bonne pratique est d'utiliser un mot de passe par service. De cette manière, si un service est compromis et le mot de passe divulgué, cela n'impacte pas les autres services. Il est également très important de choisir un mot de passe fort qui ne contient pas d'éléments facilement prévisibles et qui pourrait être brute-forcé rapidement.

Les gestionnaires de mots de passe permettent principalement de faciliter le stockage des mots de passe qui demandent d'être de plus en plus longs et complexes, de manière à ne pas les réutiliser. Ils permettent également d'ajouter une couche sécuritaire aux mots de passe en les stockant de manière sécurisée et en offrant la possibilité de générer des mots de passe forts.

Ces applications offrent plusieurs fonctionnalités sous la forme de différents types ; elles permettent, entre autres, l'utilisation du cloud afin de stocker les mots de passe sur les serveurs du fournisseur pour faciliter la synchronisation des données entre plusieurs devices (mobile, montre, navigateur, etc.). Certains gestionnaires de mots de passe sont également fréquemment utilisés au sein d'entreprises pour permettre le partage de données. Les entreprises vont généralement utiliser une solution self-hosted où elles auront leur propre infrastructure et stockage. Il existe des extensions de navigateur qui proposent le remplissage automatique de mots de passe dans les formulaires de connexion. Enfin, il y a également des applications en local qui vont limiter leur utilisation à un seul appareil.

Étant donné que les utilisateurs se reposent grandement sur les gestionnaires de mots de passe, il est important de s'assurer que ces logiciels satisfassent un certain nombre de principes de sécurité ainsi qu'une implémentation robuste afin d'éviter tout vol ou perte de données.

Objectifs

Ce travail de Bachelor vise à comprendre les menaces d'un gestionnaire de mots de passe, premièrement de manière générique, puis sur des produits spécifiques, sélectionnés à la suite d'une étude complète, en analysant la sécurité sous différents angles (stockage, mémoire, réseau, cryptographie, etc.).

Le travail est réalisé en deux parties distinctes ; une première partie qui est une étude approfondie et complète sur les gestionnaires de mots de passe. Elle permet d'analyser les menaces des différents type de gestionnaires de mots de passe et de présenter les exigences sécuritaires qu'il serait nécessaire de garantir. Elle va également se concentrer sur une étude de marché avec une comparaison de plusieurs gestionnaires de mots de passe existants sous différents aspects.

La deuxième partie du travail se concentrera tout d'abord sur la sélection de quelques candidats (environ 4) en fonction de critères établis au préalable. Ensuite, le but est d'évaluer la sécurité de manière complète de chaque gestionnaire de mot de passe sélectionné ; chaque élément choisi est analysé et évalué en fonction de différents critères comme les choix cryptographiques utilisés, le stockage, ou encore l'architecture de l'application.

Livrables

Les délivrables seront les suivants :

1. Une documentation contenant :
   - Présentation des différents types de gestionnaires de mots de passe
   - Étude de marché
   - Une analyse de menaces de différents types de gestionnaires de mots de passe
   - Spécification des exigences sécuritaires à garantir

   (a) Analyse sécuritaire des quelques candidats représentatifs (environ 4) :
   - Sélection de candidats pour la suite du travail

   chaque analyse se décomposera ainsi :
   - Sélection de critères d'analyse
   - Analyse complète de chaque aspect
   - Rapport des faiblesses trouvées au fabricant

   (b) Synthèse des résultats
2. Comparaison entre chaque candidat

Déroulement

En se référant aux dates validées par M.Donini, le travail de Bachelor débute le 20 septembre 2022 et se termine au plus tard le 10 février 2023. Il y a 3 dates clés incluant des rendus :

- **14 octobre 2022** - rendu du rapport intermédiaire
- **14 décembre 2022** - rendu du rapport final
- **23 janvier au 10 février 2023** - soutenance du travail de bachelor

Etant donné, que la soutenance du travail implique l'intervention d'un expert, la date doit être définie entre tous les intervenants.

Le volume du travail de bachelor est de 15 crédit ECTS, soit 450 heures. Le rapport intermédiaire représente 150 heures de travail.

Au niveau de la répartition de la charge de travail, cela représente environ 45h/semaine jusqu'au rendu, soit le 14 décembre, car le travail se fait à 100%.

Planning

Le travail de bachelor sera séparé en plusieurs tâches et sous-tâches différentes qui permettront de répartir plus facilement le travail sur des périodes de plusieurs semaines. Ci-dessous, le planning détaillé avec toutes les tâches :

1. Préparation
   - Rédaction du cahier des charges
   - Planification
   - Recherches initiales et introduction
2. Étude de marché
   - Recherches et explication des différents types de gestionnaires de mots de passe
   - Comparaison des fonctionnalités
3. Étude sécuritaire
   - Identification et analyse des menaces potentielles
   - Rédaction des exigences sécuritaires
4. Sélection
   - Mise en place des critères de sélection des candidats
   - Sélection des candidats
5. Analyse sécuritaire (pour chaque candidat)
   - Identification et rédaction des critères d'analyse
   - Analyse sécuritaire de chaque aspect
6. Synthèse (pour chaque candidat)
   - Synthèse des résultats
   - Rapport des faiblesses au fabricant
7. Synthèse générale
   - Comparaison de tous les résultats
   - Conclusion du travail

8. Documentation
    - Rédaction du rapport
    - Lecture / visualisation de documents
    - Tenue d'un journal de travail

Un diagramme de Gantt a également été effectué afin de pouvoir visualiser le planning et ajouter des périodes de temps :

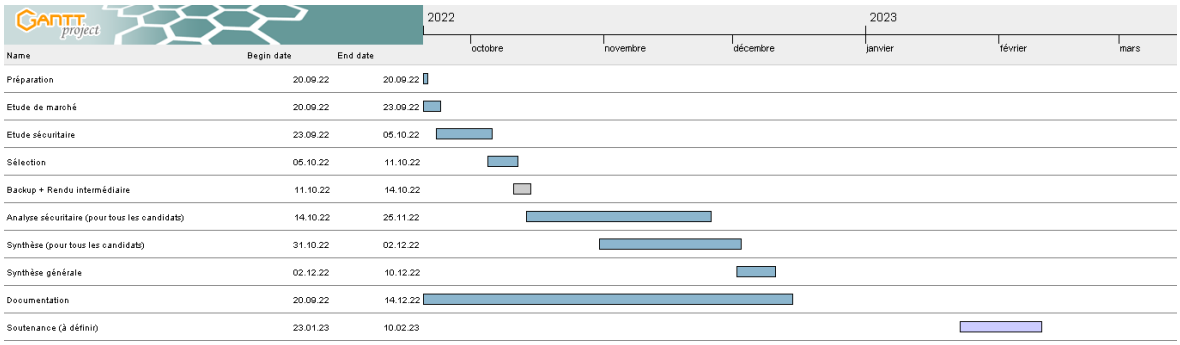

Table des matières

Chapitre 1

Introduction

Pour un utilisateur lambda, il peut être difficile de se souvenir de tous ses mots de passe tout en s'assurant d'en utiliser un différent pour chaque service afin d'éviter tout vol de données. Typiquement dans ces situations, nous allons naturellement utiliser des mots de passe simples, qui sont facilement mémorisables. Comme, par exemple, utiliser son prénom et sa date de naissance, "123456" ou encore "qwerty". De plus, il est plus simple d'utiliser le même mot de passe pour chacun de ses comptes, afin d'en mémoriser uniquement un seul.

Cependant, même si l'unique mot de passe qu'on utilise est fort et aléatoire, il n'est pas garanti à 100% qu'on soit la cible d'aucun attaquant et si une attaque est réalisée, toutes nos données personnelles sont exposées.

Ainsi, dans ce genre de cas, les gestionnaires de mots de passe interviennent et peuvent faciliter le quotidien de la plupart des utilisateurs.

1.1 Fonctionnement général

Les gestionnaires de mots de passe sont des applications multi-plateformes qui vont permettre de stocker des informations sensibles telles que des mots de passe, numéros de carte de crédit ou encore des fichiers confidentiels. On peut les comparer à des coffres forts.

Ces derniers proposent un *master password* ou une *master key* qui va permettre d'accéder à l'ensemble des données secrètes. En conséquence, la sécurité repose sur un seul mot de passe principal, ce qui est très bénéfique pour les utilisateurs car ils n'ont qu'un mot de passe à retenir. Une fois l'accès à l'application, l'utilisateur a la possibilité de stocker des données, générer des mots de passe ainsi que se connecter à des services en ligne (remplissage de formulaire d'identification automatique).

Les gestionnaires de mots de passe sont disponibles en plusieurs types différents en fonction

du besoin de l'utilisateur et des fonctionnalités proposées.

1.2 Types

1.2.1 Cloud

Les gestionnaires de mots de passe dans le cloud sont proposés pour un usage personnel ainsi qu'un usage professionnel. Les mots de passe entrés dans le coffre fort vont directement être stockés sur les serveurs du constructeur et ils seront également chiffrés sur ces derniers. Aucun stockage n'est effectué en local.

Le cloud va permettre aux utilisateurs d'avoir accès à leurs données sur n'importe quel device (ordinateur, mobile, montre) et à tout moment. De plus, toutes les données vont être synchronisées sur tous les devices connectés.

À propos de la sécurité, elle repose entièrement sur le provider de l'application car toutes les informations sont stockées sur leurs propres serveurs.

1.2.2 Local

Les applications en local s'installent sur le desktop ou sur le mobile de l'utilisateur. Ces gestionnaires de mots de passe fonctionnent indépendamment et sont offline. Ces produits en peuvent donc être utilisés sur une seule machine, par conséquence la synchronisation n'est pas proposée pour ce type de password manager.

Toutes les données sensibles sont directement stockées et chiffrées sur le device. La sécurité est plutôt bonne comparé à la solution cloud car c'est du offline, cependant si on récupère / vole le device, la sécurité devient plus faible car il y aurait la possibilité d'avoir accès aux informations sensibles du gestionnaire de mots de passe.

Il y a également une solution *on-premise* (ou *self-host*) qui permet d'utiliser sa propre infrastructure locale pour héberger toutes les données du gestionnaire de mots de passe. Les fonctionnalités offertes sont les mêmes que pour les solutions cloud mais le prix est en général plus cher et l'application plus orientée professionnelle.

1.2.3 Extension de navigateur

Le dernier type de gestionnaire de mots de passe sont les extensions de navigateur. Elles vont faciliter la gestion et la sauvegarde de mots de passe de comptes de sites web. Il y a également la possibilité de synchroniser toutes les données stockées entre tous les devices qui supportent le navigateur en question (Chrome, Firefox, Safari, etc.).

Toutes les informations sont stockées et chiffrées sur les serveurs du vendeur. En terme de sécurité, en cas de vol ou dégât du device, le risque de perdre les données est minime, cependant étant donné que les mots de passe sont stockés sur des serveurs externes, il faut leur faire confiance.

Chapitre 2

Étude de marché

Ce chapitre vise à étudier les différentes fonctionnalités offertes par les gestionnaires de mots de passe en les comparant entre plusieurs produits sélectionnés et en établissant un tableau afin d'avoir une meilleure vue d'ensemble.

Nous allons également analyser les différents prix des applications ainsi que présenter où en est le marché actuel afin d'étudier la popularité de ces dernières.

Pour l'étude de marché, les gestionnaires de mots de passe sélectionnés seront : *LastPass*[1], *Dashlane*[2], *1Password*[3], *KeePass*[4], *Bitwarden*[5], *NordPass*[6], *RoboForm*[7], *Keeper*[8].

Ils ont été sélectionnés en se basant sur leur popularité sur le marché ainsi qu'à la suite de lecture d'articles concernant les meilleurs gestionnaires de mots de passe [2][3][5][4].

2.1 Fonctionnalités

Ci-après, une liste des fonctionnalités disponibles dans les gestionnaires de mots de passe. Cette énumération se base sur toutes les fonctionnalités citées sur les websites des différents des *password manager*.

1. Stockage d'informations personnelles (cartes de crédit, passeport, contrats, etc.)

1. https://www.lastpass.com/
2. https://www.dashlane.com/
3. https://1password.com/
4. https://keepass.info/
5. https://bitwarden.com/
6. https://nordpass.com/
7. https://www.roboform.com/
8. https://www.keepersecurity.com/

2. Remplissage automatique des formulaires en ligne (auto-complétion)
3. Partage de données entre plusieurs utilisateurs (par exemple, partage d'informations d'identifications entre une famille)
4. Générateur de mots de passe forts
5. Surveillance de la fuite de données ou données compromises
6. Alerte en cas de données compromises
7. Synchronisation de données entre devices (cloud)
8. Authentification à double facteurs
9. Self-hosting
10. Support prioritaire
11. Connexion à l'aide de facteurs biométriques (*fingerprint* ou *facial recognition*) ou d'un pin
12. Possibilité de stockage des secrets en local

Ci-dessous un tableau récapitulatif qui indique quels gestionnaires de mots de passe offre quelles fonctionnalités.

Application	1	2	3	4	5	6	7	8	9	10	11	12
LastPass	×	×	×!	×*	×*	×*	×	×		×*	×*	×
Dashlane	×*	×	×!	×	×*	×	×*	×!				×
1Password [9]	×*	×*	×*	×*		×*	×*	×*		×*		×*
KeePass [10]	×	×		×	×			×	×		×	×
Bitwarden		×	×!	×	×*	×*	×	×!	×*	×*	×!	×
NordPass	×	×	×*	×	×*		×	×	×*	×*	×	×
RoboForm	×	×	×*	×		×	×*	×*	×*	×*		×
Keeper [11]	×*	×* [12]	×*	×*	×*	×*	×*	×*	×*	×*	×*	×*

TABLE 2.1 – Fonctionnalités proposées par les candidats

× : L'application propose cette fonctionnalités
***** : Fonctionnalité proposée mais avec un version premium (payante)
! : Limitations avec une version gratuite

Sur tous les candidats sélectionnés, nous remarquons que la plupart offre la majorité des

9. L'application est totalement payante et différents abonnements sont proposés
10. En général, nécessite l'installation de plugins supplémentaires afin de profiter de toutes les fonctionnalités
11. Se référer à la note de bas de page 9
12. Extension *KeeperFill*

fonctionnalités énumérées plus haut. Nous constatons que l'offre des constructeurs de gestionnaires de mots de passe est assez variée et répond à la demande des particuliers et des entreprises.

2.2 Plateformes

Cette partie va permettre de visualiser sur quelles plateformes les gestionnaires de mots de passe sélectionnés sont supportés.

Application	Windows	MacOS	Linux	Android	iOS	Navigateur
LastPass	×	×	×	×	×	×
Dashlane	×	×	×!	×	×	×
1Password	×	×	×	×	×	
KeePass	×	×*	×*	×*	×*	×*
Bitwarden	×	×	×	×	×	×
NordPass	×	×	×	×	×	
RoboForm	×	×	×!	×		×
Keeper	×	×	×	×	×	×

TABLE 2.2 – Plateformes supportées par les différentes applications

× : L'application est supportée sur ces plateformes
***** : Des applications (ou des paquets) compatibles avec KeePass Password Safe non-officielles mais contribuées existent
! : Utilisation via des extensions de navigateur

Même si un gestionnaire supporte toutes les plateformes indiquées, il est nécessaire d'aller vérifier les conditions d'utilisation du système, c'est-à-dire les versions des plateformes afin de s'assurer que l'application fonctionnera quand même.

Cependant, nous constatons que la majorité des applications sont disponibles sur les plateformes les plus courantes, et même si elles ne le sont pas, il y a souvent une solution non-officielle (notamment pour KeePass) ou via le navigateur qui existe.

2.3 Prix

Nous allons passer brièvement en revue les prix proposés par les gestionnaires de mots de passe. Chaque application propose leurs propres gammes de prix avec également des abon-

nements possibles pour les particuliers, familles ou entreprises.

2.3.1 Particuliers

Pour la plupart des applications, nous pouvons retrouver 3 gammes de prix ; Gratuit, Premium, Famille. L'offre familiale va être plus cher car les gestionnaires de mots de passe sont conçus pour pouvoir avoir plusieurs gestionnaires chiffrés individuels différents. Les tarifs ci-dessous sont exprimés en mensualités.

Application	Gratuit	Premium	Famille
LastPass	$0	$3	$4
Dashlane	$0	$3.99	$5.99 n
1Password	non	$2.99	$4.99
KeePass [13]	$0	non	non
Bitwarden	$0	<$1	$3.33
NordPass	$0	$1.84	$4.99
RoboForm	$0	$1.99	$3.99
Keeper	non	$2.92	$6.25

TABLE 2.3 – 2.3 Tarifs pour particuliers

2.3.2 Entreprises

Les entreprises ont quant à elle des prix différents dû à leurs besoins spécifiques où ils pourraient avoir besoin d'un devis personnel afin de choisir l'abonnement qui convient au mieux à leur infrastructure.

Application	Gratuit	Premium	Famille
LastPass	$0	$3	$4
Dashlane	$0	$3.99	$5.99 n
1Password	non	$2.99	$4.99
KeePass [14]	$0	non	non
Bitwarden	$0	<$1	$3.33
NordPass	$0	$1.84	$4.99
RoboForm	$0	$1.99	$3.99
Keeper	non	$2.92	$6.25

TABLE 2.4 – 2.3 Tarifs pour particuliers

13. gratuit et open-source
14. gratuit et open-source

2.4 Marché actuel

prix sur le marché, popularité, lier l'augmentation des cyberattaques avec le covid-19 + peur de perdre ses données

2.5 Récapitualtif de l'étude

Chapitre 3

Étude sécuritaire

Ce chapitre est dédié à toute l'analyse sécuritaire des gestionnaires de mots de passes en général. Nous allons dans un premier temps décrire comment ces applications sont sécurisées, puis justifier l'importance d'une forte sécurité suite à l'augmentation de la demande des entreprises et des particuliers.

Dans un second temps, nous allons lister et analyser toutes les menaces existantes et / ou potentielles des *password manager* en mettant en avant les failles actuellement connues des constructeurs et les conséquences de ces dernières ou de faiblesses qui pourraient survenir à tout moment (par exemple des cyberattaques).

Finalement, nous allons rédiger toutes les exigences sécuritaires que doivent respecter les gestionnaires de mots de passe afin que ces dernières garantissent une utilisation sûre qui évite des pertes ou vol de données.

3.1 Sécurité dans les gestionnaires de mots de passe

Dans cette section, afin de se baser sur des gestionnaires de mots de passe déjà existants et de pouvoir comparer les différentes sécurités implémentées, nous allons reprendre les 8 candidats sélectionnés dans la partie *étude de marché*, c'est-à-dire ; *LastPass*, *Dashlane*, *1Password*, *KeePass*, *Bitwarden*, *NordPass*, *RoboForm* et *Keeper*.

3.1.1 Fonctionnement de la sécurité

3.1.2 L'importance d'une forte sécurité

3.2 Menaces

3.2.1 Failles connues des constructeur

3.2.2 Conséquences d'une quelconque faiblesse

3.3 Exigences sécuritaires à respecter

Chapitre 4

Sélection des candidats

Chapitre 5

Conclusion

Bibliographie

[1] Gildas Avoine, Pascal Junod, Philippe Oechslin, and Sylvain Pasini. *Sécurité informatique, cours et exercices corrigés*. Vuibert, 2015.

[2] Clifford Colby, Rae Hodge, and Attila Tomaschek. Best password manager to use for 2022, 2022.

[3] Elizabeth A. Gallagher. Choosing the right password manager. *Serials Review*, 45 :1–2, 84–87, 2019.

[4] Michael Kurko. Best password managers, 2022.

[5] Paulius Masiliauskas. Most secure password managers in 2022, 2022.

Table des figures

Liste des tableaux

Liste des listings

Annexe A

Outils utilisés pour la compilation

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Annexe B

Journal de travail

Table B.1 – Journal de travail

Date	Description	Rech. [h]	Dev. [h]	Rapport [h]	Admin [h]
> 20.09.22	Discussion avec le professeur responsable, établissement du cahier des charges, introduction	7	0	10	4
20.09.2022	Update + organisation du TB, planing, relire le début du TB déjà commencé, avancement de l'étude du marché (fonctionnalités, plateformes, prix), lecture d'articles	2	0	5	1
12.03.2020		4	0	0	0
19.03.2020		0	7	1	0
25.03.2020		0	0	4	0
25.03.2020		0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0