UNIVERSITÉ DE RENNES 1

istic Informatique Électronique

Les Gestionnaires de mots de passe

Auteur : Erwan LE CORNEC

Date : 11/12/2020

Principe et besoin ...

... d’un quelconque mot de passe

Pour expliquer la nécessité d’un gestionnaire de mot de passe, il faut comprendre le mot de passe et la raison d’en avoir plusieurs.

Tout d’abord nous savons que les mots de passe nous donnent accès aux services de ceux sans vraiment grande utilité jusqu’à ceux les plus importants pour nous, un service de divertissement une station de travail ou bien notre banque. Quelques soient ces services le mot de passe protège en général des **données personnelles**, notre travail, un environnement que nous ne partageons pas.

... d’un meilleur mot de passe

Ensuite nous pouvons nous pencher sur certaines raisons qu’un mot de passe soit connu par une autre personne. (liste non exhaustive)

1. **Brute force**

   Essais en boucle sur une base de caractères et de formats, dictionnaire français, dictionnaire de mots de passe connus...

2. **Social Engineering**

   Date de naissance, nom prénom, proches, connaissances de l’utilisateur dans des domaines fictif ou réels

3. **Fuite d’une base de donnée**

   Certaines fois des bases de données sont dévoilées elles associent un identifiant avec un mot de passe, les utilisateurs possédant la même combinaison pour un autre service pourrait se faire compromettre ce compte à leur tour.

4. **Indiscrétions**

   Avant que le mot de passe ne soit caché sur l’ordinateur un étranger de l’utilisateur peut tout à fait prendre connaissance de celui-ci, l’utilisateur, inconscient, peut également vouloir inscrire son mot de passe en dehors d’un système sécurisé tel un fichier texte ou alors un post-it.

Afin de palier aux différents problèmes évoqués ci-dessus, les solutions seraient :

1. utiliser un mot de passe plus long
2. utiliser un mot de passe aléatoire
3. utiliser des mots de passes uniques pour chaque comptes
4. ne pas les noter à la vue de tous

En effet plus le mot de passe est long avec des caractères complexe qui ne suivent aucune logique rendent le mot de passe plus compliqué à deviner, pour s’en souvenir plutôt que les écrire dans un environnement non sûr nous pouvons utiliser un gestionnaire de mots de passe.

Étant sa fonction principale avoir une multitude de mots de passe ne devrait pas déranger, et enfin s'ils sont notés dans un tel gestionnaire ils n'auraient pas besoin d'être notés à la vue de tous.

... d'un gestionnaire de mot de passe

Comme décris dans le paragraphe précédent, le principe du gestionnaire de mot de passe est de garder précieusement ses mots de passe, il peut également avoir d'autres fonctions bien utiles en rapport à une gestion bien plus poussée d'un mot de passe.

Il peut s'agir d'un **générateur de mots de passe**, cela résout alors les deux premiers points, petite description des possibilités génériques qu'un tel générateur propose :

- taille du mot de passe (12 caractères en général) jusqu'à au moins 128
- format du mot de passe : *A-Z a-z 0-9*
- présence de caractères complexes *!@#$%^&**
- mots aléatoire pour former une phrase de passe. *ex : achiness-improve-resonate*

Cela peut également être une comparaison du mot de passe avec les listes connues de mots de passe qui ont fuités par le passé ou bien la bien plus courte liste des 100 mots de passe les plus courants (password, azerty, 123456, sunshine ...). Dans tous les cas le mot de passe se verra attribué un degré de résistance face à une intrusion par brute force de nos mots de passe généralement non générés à l'aide de leur outil intégré (afin de démontrer l'utilité de celui-ci).

Ensuite ayant un mot de passe compliqué nous auront besoin de le renseigner dans l'application cible ou sur le site en question, le taper étant devenu réellement compliqué la saisie automatique ou la gestion du presse papier deviennent des atouts en quelques manœuvres nous sommes connectés et le mot de passe n'a pas été divulgué.

Une fonctionnalité quelques fois nécessaire est le partage de mot de passe, en effet partager un mot de passe en dehors de l'application reviendrai à le noter sur un papier et quiconque tombe sur ce papier peut voler le compte, c'est pourquoi l'implémentation d'un partage de mot de passe avec une autre personne au sein de l'application peut être nécessaire, cela permettrai de le garder en sécurité tout en le partageant avec une autre personne.

Accessible, un gestionnaire récolte la totalité de nos mots de passe on en a besoin absolument à tout moment et sur toute machine, c'est pourquoi l'accessibilité pour une même personne sur plusieurs appareils peut être nécessaire, toutefois nous verrons que cela n'est pas nécessaire.

Tant qu'à garder des données sensibles telles que nos mots de passe plusieurs gestionnaires se proposent de conserver également toute note sous différents formats, une note texte, une carte bancaire, ou même nos informations personnelles depuis que la saisie automatique est intégrée et notre identité changeant rarement ces informations peuvent également être saisie automatiquement dans le formulaire.

Différentes Solutions

Plusieurs solutions ont alors été imaginées depuis le succès de ces premières solutions bien d'autres ont été produis depuis. Je vais lister ici les solutions intéressantes et décrire ensuite leur processus de sécurisation des mots de passes. Ici trois logiciels Lastpass Keepass et Bitwarden mais plusieurs autres auraient également pu faire partie de cette liste tel Dashlane, Nordpass, Roboform...

Lastpass[1]

Un des premiers gestionnaires vraiment connus (sorti en 2009) il a démocratisé l'utilisation d'un gestionnaire. Les mots de passes sont destinés à être stockés sur un compte de l'entreprise, malheureusement dans une telle situation le piratage de leur base de donnée exposerait tous les mots de passes de leurs clients en même temps ce qui serait contre productif. Et cela a été le cas en 2015.

Keepass[2]

Le gestionnaire open source le plus connu, en effet « standalone » il fonctionne uniquement à l'aide d'un simple fichier où nos mots de passes sont enregistrés, à nous d'en prendre soin. Par dessus cela dans ce logiciel on peut ajouter des plugins afin de modifier le comportement, ajouter des fonctionnalités et au final personnaliser suffisamment le logiciel pour le rendre unique à un tel point qu'on peut également modifier le système de chiffrement du fichier de sauvegarde, les attaquants passeront plus de temps à comprendre cela plutôt que connaître le fonctionnement global de l'application et s'attaquer à ses faiblesses.

En effet on peut lister parmi les plugins certains proposant d'utiliser d'autres fonctions de « ciphers » pour les mots de passe (Twofish, serpent, salsa et même multi cipher qui permet d'en combiner plusieurs). Pour continuer sur la liste des plugins on remarque les différents moyens proposés pour accéder à l'application : **une carte et un lecteur RFID**, une clé usb U2F divers autres modules ou bien même de le transformer en serveur sécurisé personnel (accessible sur internet donc mais par nos propres moyens pas dans une base de donnée connue).

Ce logiciel est recommandé par l'état français et certifié par l'ANSSI.

Bitwarden[3]

Un autre gestionnaire bien connu open source également et sorti en 2016. Cependant plus facile à mettre en place en effet le logiciel se base sur un serveur que l'entreprise se propose d'héberger pour nous mais que nous pouvons également choisir de garder sur nos serveurs, que nous soyons un particulier ou une entreprise. La solution est simple donc une application ou une interface web qui chiffre le mot de passe avant même de quitter notre machine tel que décris mot pour mot sur leur site internet. Le chiffrement se base sur une clé AES-256, un hash salé et la clé de dérivation à base de mot de passe PBKDF2 SHA-256 afin de vérifier le mot de passe général de notre compte.

Ce logiciel parmi d'autre intègre la gestion des clé TOTP (timebased one time password), un second facteur d'authentification dont les 6 chiffres qui le composent changent régulièrement.

---

[1] https://www.lastpass.com/fr/

[2] https://keepass.info/

[3] https://bitwarden.com/

Étant lié à un compte puisque ce nombre étant le fruit du calcul (dont l'algorithme est gardé secret) de la tranche horaire avec une clé générée et fournie par le site où on veut se connecter. Cela veut donc dire que le code est lié au seul compte pour lequel le code est fourni et à aucun autre et prouve la nécessité de le garder sécurisé auprès des autres enregistrements pour ce compte, tant que la sécurité dans ce coffre est bonne.

A propos de cette solution il se peut que j'en ai parlé en des termes plus élogieux ou décrit des fonctionnalités non nécessaire et cela s'explique par le fait que j'ai moi-même installé ce système chez moi à l'aide d'un portage en container docker du serveur.

Les hardware password manager

Un petit outil[4] se faisant passer pour un simple clavier et qui possède une entrée physique, des boutons avec lesquels on sélectionne notre mot de passe qui sera ensuite tapé directement dans l'ordinateur.

Du coté de l'ordinateur l'entrée du mot de passe se fait de la même façon que lors d'une saisie habituelle de la part de l'utilisateur seulement cette fois-ci le clavier est virtuel et est programmé pour écrire n'importe quel mot préenregistré. Derrière ce fonctionnement de clavier on retrouve un ordinateur miniature gérant une mémoire, le chiffrement/déchiffrement et l'interface utilisateur.

Une molette cliquable sur la droite permet de naviguer parmi les options et mots de passe, et une carte renseigne une clé secrète débloquant le portefeuille de mots de passe avec celle-ci l'outil peut recueillir des comptes de la part de différents utilisateurs chacun possède sa carte et le boîtier peut rester connecté sans aucun problème.

Une alternative peut être envisagée en effet des applications sur téléphones peuvent le transformer en ce boîtier ou bien un bricolage à base de carte raspberry pi zero et autres peuvent faire l'affaire et coûter bien moins cher.

Le problème de genre de solution physique externe est qu'il prend du temps à l'utilisation c'est pourquoi ce n'est pas énormément répandu.

[4] Description sur la base de Mooltipass https://www.themooltipass.com/

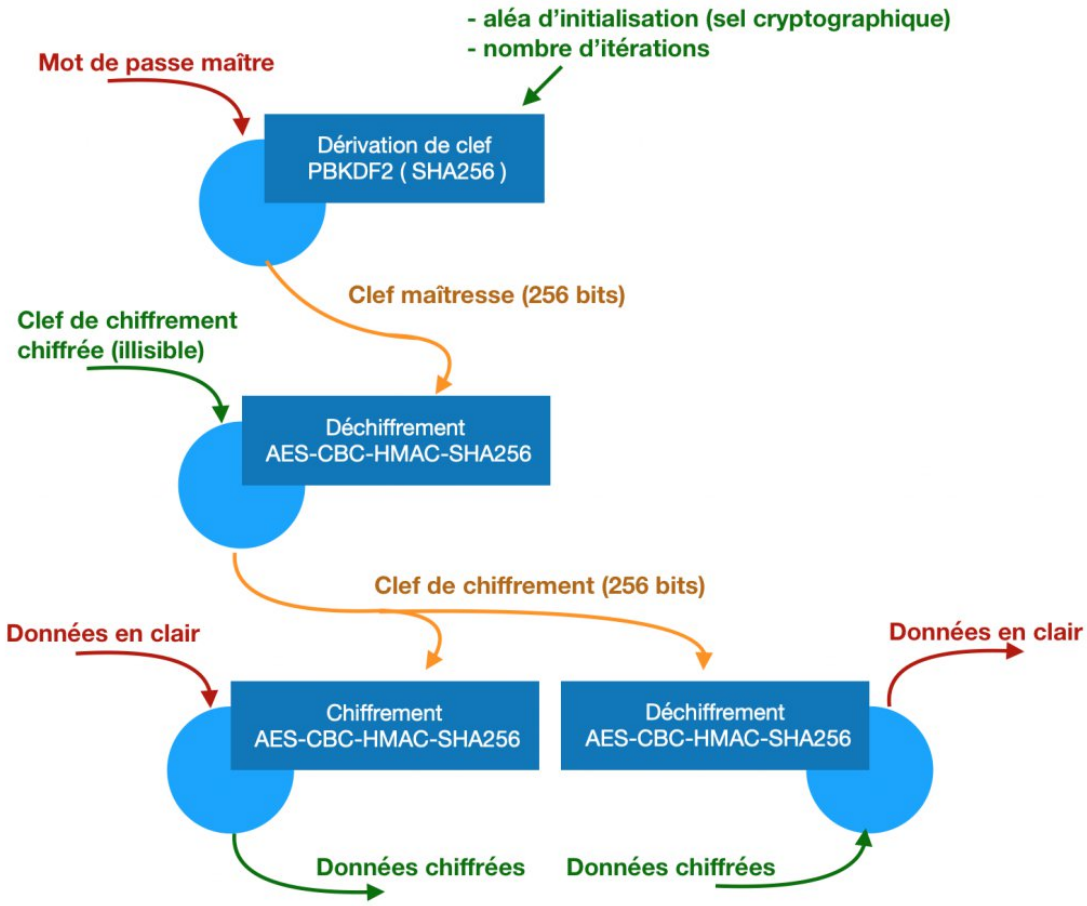
Fonctionnement Interne

Le « fonctionnement » à proprement parler est toujours décris comme utilisant un chiffrement AES-256[5] débloqué par un mot de passe, en effet le mot de passe traverse un processus de hash comme vu précédemment en partie Bitwarden et qui se trouve être la solution générique d'usage.

Le détail du fonctionnement est très bien décrit sur le blog d'Eric « edaspet »[6].

Le fonctionnement de keepass est passé au crible : le mot de passe « maître » est directement utilisé pour déchiffrer nos mots de passe c'est à dire dans le cas du changement du mot de passe principal le logiciel doit déchiffrer absolument tous les mots de passes et le chiffrer à nouveau avec le nouveau.

Pour pallier à ce problème Bitwarden par exemple -et comme expliqué dans l'article- utilise l'algorithme dessiné ci dessous.



A l'aide de cette méthode seule la clé de chiffrement est déchiffrée par l'ancien mot de passe maître et rechiffré avec le nouveau encore une fois. Ce système est je trouve plus propre et est moins sujet aux erreurs de manipulations mais avant tout un gain de ressource et de temps non négligeable.

[5] mis à part Pass un logiciel linux utilisant GnuPG soit une paire de clés asymétriques

[6] https://n.survol.fr/n/dis-tonton-comment-ca-fonctionne-la-securite-dun-gestionnaire-de-mots-de-passe-introduction-cryptographique

En élargissant ce nouvel algorithme et c'est certainement le cas pour le plugin MultiCipher évoqué page 4, nous pouvons répéter ce système de chiffrement de clé en plusieurs étages puis disposer les différentes clés sur plusieurs -et différents- supports physiques.

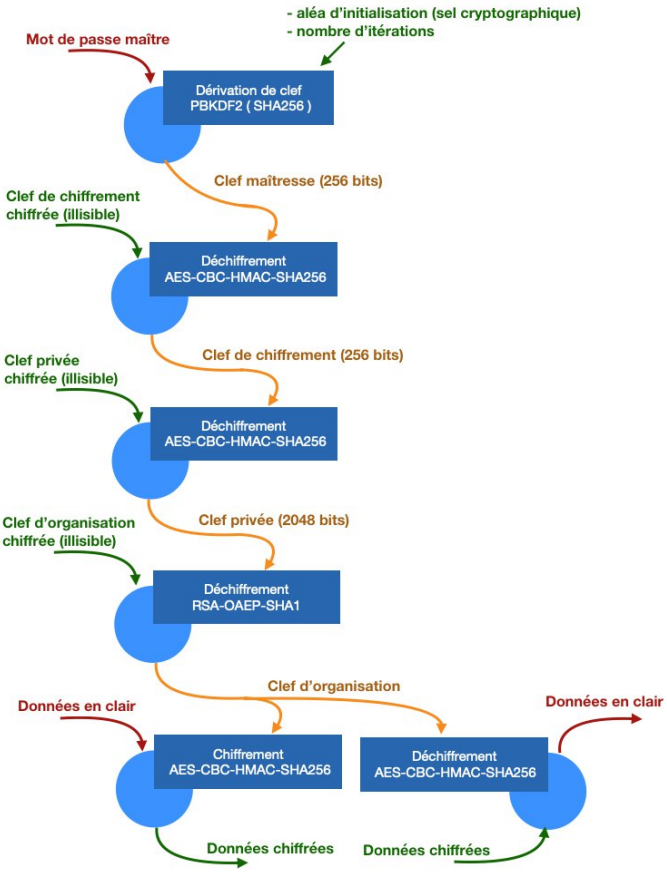
Par la suite dans le blog, l'auteur nous présente la gestion du mot de passe dans le cas d'une information partagée. Pour cela il prend une nouvelle fois pour exemple Bitwarden et son système d'organisation.

Lors de la création de l'organisation une nouvelle clé symétrique est créée et le partage de cette clé doit se faire de manière sécurisée, c'est alors qu'une paire de clé asymétrique est générée, en effet rien de mieux pour partager une information :

- le destinataire envoi sa clé publique
- l'administrateur de l'organisation chiffre la clé AES de l'organisation avec cette clé publique
- l'administrateur l'envoi à l'utilisateur faisant partie de l'organisation ou appelé ci dessus le destinataire
- cet utilisateur peut alors déchiffrer la clé d'organisation avec sa clé privée
- et enfin déchiffrer le mot de passe partagé avec la clé d'organisation

La dernière étape est de sécuriser la clé privée de l'utilisateur, le logiciel n'a plus qu'à réutiliser la base de mots de passe personnels déjà utilisée la clé privée étant tout autant personnelle.

Au final pour ce qui s'agit du partage au sein d'un groupe/d'une organisation le schéma[7] ci-dessous résume très bien tout le processus.



Je me demandais cependant si c'est toujours le cas lors de l'utilisation à plusieurs reprises des mots de passe de l'organisation si la clef d'organisation est stockée toujours chiffrée par la clé asymétrique ou bien si elle est inscrite aux cotés de celle-ci et des autres mots de passe.

Pour conclure, je dirais que l'utilisation d'un gestionnaire de mots de passe est grandement conseillée pour les plus sceptiques ne voulant confier de telles informations à des entreprises d'autres solutions existent malheureusement elles restent compliqués à mettre en place d'après une étude techadvisor[8].

[7] issu du blog d'Eric une nouvelle fois

[8] https://www.techadvisor.fr/banc-essai/ordinateurs/meilleur-gestionnaire-de-mot-de-passe-3666137/