

TPE

Travaux Pratiques Encadrés

Problématique : Comment ne plus se compliquer la vie avec ses mots de passe ?



Authentification facile

Letourneur Raphaël

Sovero Kristell

Viollet Robin

Sommaire

Introduction03
Recherche03
Diagramme03
Cahier des charges04
Solutions possibles05
Les mots de passe06
Design / hardware08
Choix réalisation10
Solution existante12
Gestionnaire en ligne12
Gestionnaire hors ligne13
Biométrie14
Réalisation15
Application gestion15
Extension chrome20

Introduction :

Aujourd'hui, il existe de plus en plus de sites internet qui nécessitent une mémorisation de mots de passe. D'après des spécialistes, le nombre de compte en ligne est estimé à environ 200 par internaute.

Ces mots de passe sont de plus en plus complexes (pour des raisons de sécurité) et donc de plus en plus difficiles à retenir, ce qui pose un problème : comment peut-on retenir tous ces mots de passe sans pour autant compromettre la sécurité du compte ?

En effet, d'après une étude, 60% des français ne changent que très rarement leurs mots de passe ou bien uniquement lorsque ceci leur est demandé. De plus, 1 personne sur 2 utilise le même mot de passe pour plusieurs sites web différents.

En moyenne, un internaute perd 50 heures par ans en se connectant à ses sites favoris. Il est vrai que cela n'est pas énorme sur une période d'un an mais, si nous considérons que c'est du temps de travail, pour une personne qui serait payée au smic (~1150€ / mois) cela revient à ~410€ annuels

C'est pourquoi, nous avons décidé de proposer une solution permettant de régler ces problèmes. Le système s'occupe de retenir vos identifiants à votre place ainsi que de les saisir sur les sites qui requièrent une authentification. Nous avons donc choisi la problématique : « Comment ne plus se compliquer la vie avec ses mots de passe ? », qui illustre le fait que nous souhaitons autant améliorer la sécurité des identifiants que la simplicité de connexion.

Recherche :

Tout d'abords, nous avons réalisé un diagramme bête à corne ainsi qu'un diagramme pieuvre afin de réfléchir aux points importants du produit.

Diagramme « bête à corne »

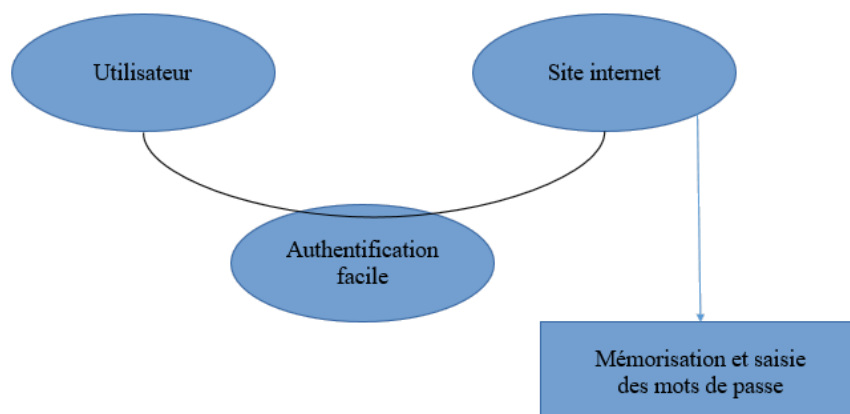
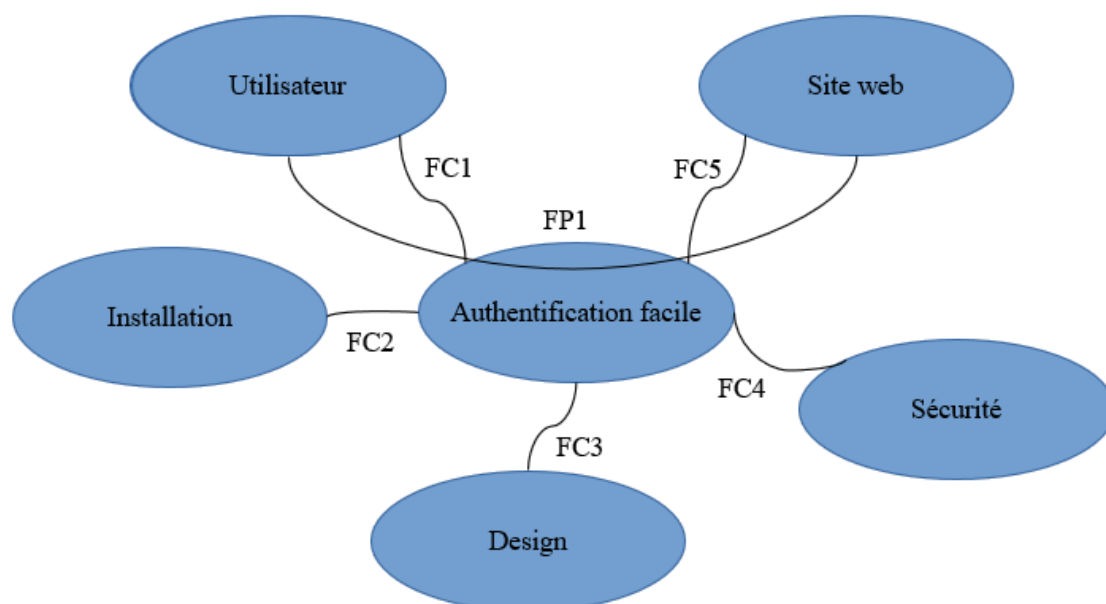


Diagramme « Pieuvre »



Pour combler ce diagramme pieuvre, nous avons réalisé le cahier des charges. Le cahier des charges permet de se donner une idée plus précise de ce que nous devons faire, pour répondre à quel besoin ainsi que l'importance de chaque tâche et une solution possible. Le nom des fonctions de service du cahier des charges correspond à ceux disponible sur le diagramme pieuvre.

<u>Fonctions de service</u>	<u>Critères d'appréciation</u>	<u>Niveaux d'appréciation</u>	<u>Flexibilité</u>
FP1 : Faciliter l'authentification	Site sur internet	Auto-complétion	Nombre d'utilisateurs limité à 20 ou 200 pour le moment
FC1 : Facile d'utilisation	Simple / Basique	Interface simple	
FC2 : Pas d'installation complexe	Plug and play	autorun	Temps de démarrage d'1 minute
FC3 : Doit plaire à l'utilisateur	Compact, esthétique et ergonomique	Imprimante 3D (Boîtier adapté à la taille)	Moins de 10cm
FC4 : Doit être sécurisé	Cryptage	Aes-258	
FC5 : Associer le bon mot de passe au bon site	Identifier le site	Reconnaissance URL	Associer bon identifiant à bon site

Nous avons donc réfléchi sur les différentes méthodes répondant à la problématique. Pour cela, nous avons cherché les avantages ainsi que les défauts de chaque solution qui nous passait par la tête.

Solution possible

<u>Solutions</u>	<u>Points positifs</u>	<u>Points négatifs</u>
Mot de passe maitre	+ Portabilité + Protège contre phishing + Rapidité	- Obligation de retenir un mot de passe très complexe - Peut se faire pirater à distance facilement - Protège pas totalement des Keylogger
Papier stylo / fichier texte	+ Sécurisé à distance	- Peut sécuriser, mots de passe écrit en toute lettre - Nécessité d'avoir la feuille partout, tout le temps - Perte de temps - Protège pas des phishing, / Keylogger
Via d'autre appareil (Double authentification)	+ Sécurisé	- Avoir toujours son smartphone a porté de main - Difficulté en cas de panne - Long, saisi pour chaque site - Protège des Keylogger / Phishing
Physique / avec clé USB	+ Rapide + Facile + Portabilité + Sécurisé à distance + Sécurise des keylogger et des phishing	- Peut sécuriser avec un accès à la clé USB - Difficulté en cas de panne
Biométrique	+ Sécurisé aussi bien à distance qu'avec un accès à l'ordinateur + Rapide, pression de doigt + Toujours son doigt a porté de main + Rien à retenir, ni identifiant, ni mot de passe + Protège contre Keylogger / Phishing	- Difficulté en cas de panne - Portabilité

Keylogger = Virus qui enregistre ce qui est tapé au clavier. Evité par le fait que l'utilisateur n'utilise pas son clavier

Phishing = Méthode de piratage qui consiste à créer un site ressemblant à un site célèbre afin de convaincre la victime d'entrer ses identifiants qui sont retransmis au hacker. Evité par un contrôle de l'URL

Pour notre projet de TPE, nous avons donc choisi de travailler sur un gestionnaire de mots de passe biométrique. Nous avons fait ce choix car la solution par reconnaissance biométrique est une solution encore très peu utilisée alors que cette technologie à un énorme potentiel. Cette solution dispose d'énormément d'avantage tel que la sécurité et la facilité d'utilisation. De plus, nous avons réussi à trouver diverses techniques permettant de diminuer voire supprimer les inconvénients comme en prévoyant les pannes éventuelles ou bien la portabilité du produit.

Pour revenir sur le cahier des charges, on peut voir dans la catégorie « Niveaux d'appréciation » que nous avons choisi de faire un logiciel autorun. Cela signifie qu'il s'exécute tout seul au branchement de notre périphérique sans que l'utilisateur doive procéder à une installation. Cela est pour nous une continuité dans notre quête pour la simplification maximale de notre produit afin de le rendre vraiment accessible à un maximum de monde.

Il ne faut pas confondre sécuriser et crypter qui selon moi sont deux choses bien différentes. Crypter signifie que la donnée est modifiée afin d'avoir une forme différente de la sienne afin que la personne se retrouve avec une chaîne de caractère qui n'est pas le mot de passe par exemple puisqu'un algorithme aura été appliqué dessus. Alors que sécuriser signifie selon moi une protection d'accès. Sécuriser signifie donc qu'il ne peut pas accéder à vos données alors que crypter qu'il ne peut pas utiliser les données qu'il aurait éventuellement pu obtenir.

Les mots de passe

Nous avons également parlé d'un cryptage nommé AES-258. Il s'agit d'un cryptage qui se constitue de 258 bits. C'est actuellement le meilleur. Pour se donner un ordre d'idée, il y'a $1,1 \times 10^{77}$ possibilités pour décrypter un seul mot de passe ce qui, toujours pour décrypter un seul mot de passe prendrait des milliers d'années avec notre technologie actuelle (je ne parle pas d'informatique quantique).

Attention tout de même à ne pas confondre cryptage et hashage. La grande différence est que le cryptage est réversible contrairement au hashage qui lui ne fonctionne que dans un sens : il est irréversible. Etant donné que nous devons pouvoir lire les mots de passe pour pouvoir les utiliser avec notre logiciel, nous étions obligés d'utiliser une sécurité cryptographique réversible. Le hashage est lui souvent utilisé pour se connecter sur les sites internet. Son fonctionnement est simple. L'utilisateur entre son mot de passe, puis sa saisie est hashée et c'est le hash du mot de passe qui est comparé à celui de la base de données pour voir s'il correspond ou pas.

Pour continuer sur les mots de passe et leurs sécurités, nous avons également étudié les différents moyens de les stocker. Bien que nous avions que 2 possibilité, le choix a tout de même été difficile.

Recherche Stockage mots de passe

<u>Solutions</u>	<u>Points positifs</u>	<u>Points négatifs</u>
Mémoire interne	+ Portabilité + Sécurisé	- Impossibilité de récupération en cas de panne
Base de donnés	+ Portabilité + Possibilité de récupération en cas de panne	- Nécessite connexion internet - Moins sécurisé à distance

Nous nous sommes donc tournés sur un stockage en base de données. Nous avons choisi cette solution pour sa capacité de récupération en cas de panne ce qui contre en grande partie les problèmes liés à une panne du capteur. Étant donné qu'une empreinte peut être réenregistrée, une récupération de tous les identifiants est potentiellement envisageable bien que celle-ci doit rester exceptionnelle afin d'éviter le vol de la totalité des identifiants via usurpation d'identité par exemple.

De plus, ce produit étant destiné aux mots de passe de nos comptes en ligne, la nécessité de disposer d'une connexion internet reste négligeable bien qu'il peut arriver de vouloir consulter nos identifiants cela reste tout de même très rare.

En ce qui concerne la sécurité, une base de données bien gérée est sûrement aussi sécurisée que le serait la sécurité du capteur avec les mots de passes stockés en interne si un attaquant disposais d'un accès physique au module.

La dernière partie des recherches était l'intégration hardware de notre module.

Design / Hardware

Recherche Intégration

<u>Solutions</u>	<u>Points positifs</u>	<u>Points négatifs</u>
Clé USB	+ Portabilité + Possibilité de crypter des fichiers + Utilisation courante	- Se perd facilement - Clé USB assez volumineuse
Boîtier	+ Portabilité	- Objet supplémentaire
Souris	+ Pratique / utilisé couramment	- Portabilité

Comme vous pouvez le voir depuis quelques tableaux de recherche déjà, la portabilité est un des critères les plus présents dans nos recherches. Bien que dans l'objectif final, ce critère aurait une place moins importante puisqu'une solution enlèverait le besoin de se promener avec son capteur pour avoir accès à ses comptes

Pour finir, nous avons donc choisi de commencer à travailler sur un boîtier. Nous avons commencé le travail en voulant mettre le prototype dans un clic de souris mais en y réfléchissant, il est préférable d'utiliser un objet plus passe-partout afin de pouvoir se déplacer avec ses identifiants et surtout ne pas ajouter des obligations aux potentiels utilisateurs qui souhaiteraient peut-être une autre souris que celle que nous aurions proposé. Il est évident que certaines personnes auraient préféré avoir le choix de leur souris plutôt que disposer de notre module.

Ensuite, la clé USB est une excellente idée. Surtout qu'elle permet d'héberger le logiciel afin de l'exécuter en autorun ainsi que de sécuriser quelques fichiers par reconnaissance biométrique. Nous pensons faire ceci si nous continuons le projet hors lycée car c'est sûrement la meilleure solution surtout avec le changement de capteur puisque sa taille pourrait correspondre. Cependant, disposant de peu de temps, nous avons essayé de finir d'abord un produit fonctionnel mais nous avons réfléchi à plusieurs évolutions telle que celle-ci.

Enfin, pour revenir sur notre boîtier, nous avons à notre disposition une imprimante 3D ce qui nous a permis de faire des pièces très précises et variées contrairement à ce qu'on aurait pu faire avec des planches de bois ou de PVC. Ceci nous a permis d'améliorer la portabilité en minimisant la taille.

À propos de l'ergonomie, nous avons choisi de faire une forme arrondie en forme de gouttière sur le dessus dans le but de rendre plus naturel et améliorer la pose du doigt sur le capteur. En effet, cela permet au doigt de glisser directement dans la bonne position c'est-à-dire la même que lors de l'inscription. En plus de rendre l'identification plus agréable, cela augmente également les performances

puisque si la position du doigt est toujours très similaire à l'empreinte enregistrée, la vitesse d'identification sera supérieure. Le risque d'une non-identification est également très réduit au point de devenir négligeable puisque les tests d'identification se lançant à la suite, si l'un échoue, le suivant devrait trouver le résultat.

Pour finir avec le boîtier, nous sommes encore en train de réfléchir à une solution permettant un meilleur maintien de celui-ci sur le support sur lequel il est situé. Le problème étant que son faible poids (qui est un avantage pour sa portabilité) peut provoquer un soulèvement du capteur lorsqu'on souhaite retirer notre doigt. De plus, si l'on ne fait pas attention au moment de la pose, le capteur peut glisser ce qui n'est pas forcément agréable.

Recherche Stabilité

<u>Solutions</u>	<u>Points positifs</u>	<u>Points négatifs</u>
Sable	+ Diminue le soulèvement ainsi que la glissade	- Lourd - Portabilité
Socle aimanté	+ Diminue le soulèvement et la glissade pour une certaine force + Rajoute peu de poids	- Dégrade les composants électroniques
Ventouse	+ Assez efficace + Portable	- Difficile à décrocher
Grip	+ Leger + Diminue la glissade + pas cher / Facile à faire + Portabilité	- Non efficace sur le soulèvement
Face inférieure auto-collante	+ Diminue glissade / soulèvement	- Portabilité - Usure
Scratch	+ Diminue glissade / soulèvement + Portabilité + Changement possible de position + Rend pas le décrochage trop difficile	- Modification de l'espace de travail. Solution pour moyenne / longue durée

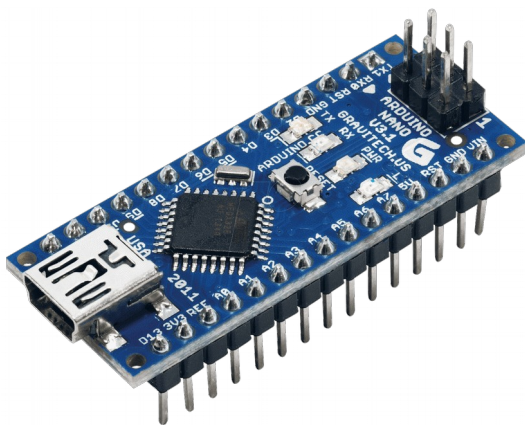
Choix pour la réalisation

Choix langage de programmation

Pour finir sur la phase recherche, le dernier choix que nous avons dû faire est le choix du langage de programmation. L'arduino et le javascript étaient obligatoire pour la partie biométrie et l'extension web, seul le langage de l'application de gestion restait à déterminer. J'ai choisi d'utiliser, d'apprendre le C# (le langage de programmation développé par Microsoft, se prononce C sharp) car c'est un langage assez facile comparé au C ou au C++ qui aurait été impossible à apprendre en si peu de temps. De plus, Visual Studio comporte un concepteur graphique intégré ce qui m'a permis de vraiment me concentrer sur la programmation fonctionnelle et ne pas perdre du temps sur l'esthétisme de l'application. De plus, la communauté du C# est très active sur les forums comme Stackoverflow par exemple ce qui peut grandement aider en cas de problème que nous n'arrivons pas à résoudre seul. Etant dérivé du C et du C++, le langage C# a énormément de possibilité et de fonction conçu de base ce qui permet de gagner du temps.

Choix matériel

Notre choix de matériel a beaucoup été basé sur la miniaturisation de notre prototype. Nous avons donc essayé d'utiliser les composants le plus petit possible ainsi que le moins de composants possible sans pour autant négliger les performances. Pour cela, nous avons utilisé (hormis résistance et câble) uniquement deux composant.





Arduino nano



Capteur GT511C3

Nous avons utilisé un Arduino nano car c'est l'arduino le plus petit qu'il existe et ses performances sont suffisantes, c'est pourquoi il nous serait paru totalement absurde d'en choisir un autre.

Pour ce qui concerne le capteur, nous avons peu de choix. En effet, il n'existe que 2 capteurs différents bien que le capteur choisi dispose de plusieurs variante modifiant le nombre d'empreinte maximal par exemple.

	<u>Capteur ADH-tech</u>	<u>Capteur Adafruit 751</u>
Photo		
Dimension	36 x 18 x 8 mm	56 x 21 x 21 mm
Temps de réponse / d'identification	Environ 1,5 seconde	< 1 seconde
Taux d'erreur bonne empreinte	<0,1 %	<1.0 %
Taux d'erreur mauvaise empreinte	<0,001 %	<0,001 %
Nombre empreinte	Max 20 ou 200	162 max
Prix approximatif	~ 50 ou 60€	~ 65€

En plus du fait que le capteur ADH-tech est mieux que le capteur Adafruit à propos des taux d'erreur ainsi que moins cher, il est surtout beaucoup plus petit car il n'est pas dans une « coque » contrairement au capteur adafruit ce qui nous laisse une marge de main d'œuvre beaucoup plus restreinte comparé au capteur ADH-tech qui peut plus facilement être incluse dans un projet petit.

De plus, le lycée disposant du capteur Adafruit, nous avons commencé à travailler avec celui-ci qui très vite nous a posé problème à cause de plusieurs erreurs auquel nous n'avons pas trouvé de solution ni même d'explication. C'est pourquoi nous avons été obligé de changer de capteur si nous souhaitions avancer ce qui, au final est une très bonne chose.

Solution existante

Les gestionnaires de mot de passe ne sont pas des solutions nouvelles. Bien que ceux-ci existent depuis déjà quelques années, ils restent encore très rares et peu utilisés. Pourtant, il en existe de nombreux disponibles gratuitement sur internet ainsi que certains déjà liés à la reconnaissance biométrique. Ils sont très rares et leur présence étant très faible, ceux-ci sont (les gestionnaires biométriques) davantage des gadgets que des outils vraiment fonctionnels. Notre produit reste tout de même innovant car comme vous le verrez plus tard, il reste supérieur aux autres en proposant un fonctionnement unique et jamais vu.

Les gestionnaires en ligne

Tout d'abord, sans doute les plus connus ainsi que les plus répandus, il s'agit des gestionnaires de compte en ligne. Ce n'est pas des sites internet mais des logiciels sur lesquels vous devez disposer d'un compte pour stocker vos mots de passe en ligne. C'est le système de mots de passe maître qui est utilisé. Je ne reviendrais pas en détails sur les défauts de ce système tel que la possibilité de se faire voler son mot de passe maître mais il a l'avantage d'être gratuit et d'avoir une incroyable portabilité. Disponible sur tous les ordinateurs après une installation sans obligation de rajouter un module complémentaire externe.



Dashlane est le numéro un dans ce domaine. Il dispose d'énormément de fonctionnalités. C'est d'ailleurs de lui que nous nous sommes beaucoup inspirés pour concevoir notre projet.

Parmi ses gros points forts, on peut voir qu'il est vraiment extrêmement portable

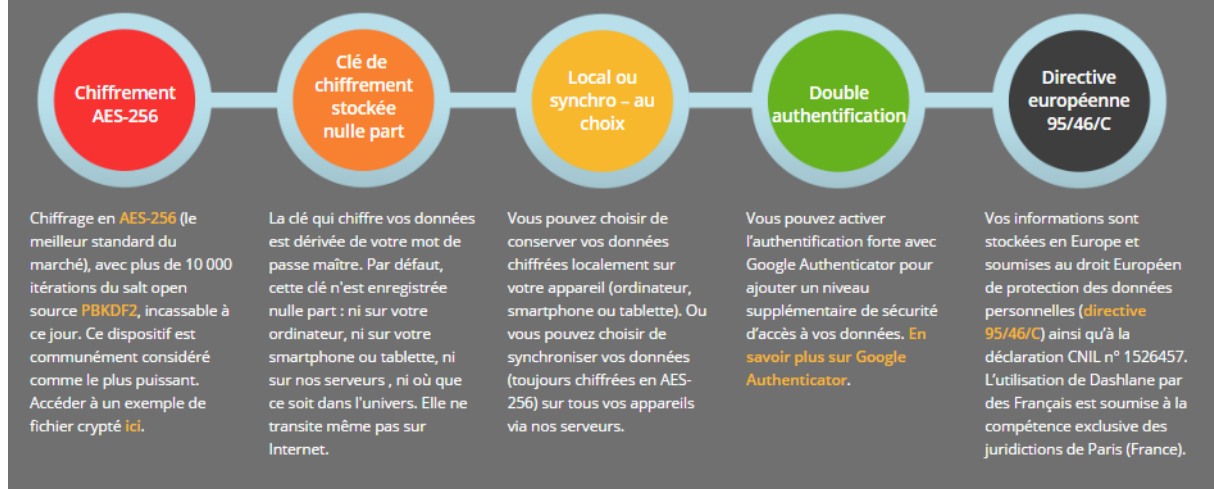
Dashlane fonctionne où que vous soyez

Utilisez vos mots de passe dans vos navigateurs préférés.



Il est très sécurisé (bien que le mot de passe maître peut encore être volé)

Notre modèle de sécurité en quelques mots :



Dashlane est largement en avance sur les concurrents

Dashlane	Les Concurrents*
Connexion intelligente et mémorisation des mots de passe automatique, et qui fonctionne partout	Vérification nécessaire pour s'assurer que les informations ont été correctement enregistrées
Notification à chaque fois qu'une brèche de sécurité est détectée sur l'un de vos comptes	Notification qui arrive de temps en temps, voire pas du tout
Tableau de Bord de Sécurité intelligent expliquant concrètement comment améliorer sa sécurité	Score et évaluations qui ne veulent pas dire grand-chose
Prix global pour sauvegarde illimitée quel que soit le nombre d'appareils	Facturation par appareil
Aucune barre d'outils dérangeante dans le navigateur ou de manipulations peu intuitives	Barre d'outils nécessaire avec guide d'installation et procédure de débogage
Fonctionnalités sans restrictions	Fonctionnalités limitées ou mode consultation seulement

Les gestionnaires hors ligne

Les gestionnaires dit hors ligne repose eux sur un tout autre principe dont je n'ai toujours pas parlé. Il s'agit en fait de stocker les mots de passe dans un fichier crypter que seul l'application peut ouvrir. Le problème de ceux-ci étant que pour l'instant, les peu utilisant encore ce système ne sont pas correctement finaliser. En effet, très souvent ce sont juste des gestionnaires mais ne s'occupe pas de l'autosaisi ou de vérifier la sécurité. De plus, parfois, comme c'est le cas sur keepass, un mot de passe maître reste demandé afin d'éviter le vol de ce fichier.



Les gestionnaires biométriques

Enfin, pour terminer, nous allons étudier la partie la plus intéressantes des solutions existantes. Il s'agit des solutions biométriques.

La société HP (« Hewlett-Packard ») commercialise depuis plusieurs années des ordinateurs portables possédant un lecteur d'empreinte digital intégré. De base, ce capteur sert de base uniquement à l'accès à la session Windows mais, grâce à un logiciel non intégré (nommé « SimplePass ») qu'ils ont développé, il est possible de mémoriser des identifiants web avec nos empreintes digitales via ce capteur.

Le système biométrique des téléphones portables est exactement le même. Il permet de base uniquement à déverrouiller l'appareil mais peut être configuré pour mémoriser des identifiants de site web.

Cependant, la méthode utilisé est peu adaptée. En effet, le capteur ne fait pas la différence entre 2 empreinte. Il reconnaît uniquement si l'empreinte est enregistrée ou non mais ne peut pas différencier 2 personne ce qui pose problème si plusieurs personnes souhaitent utiliser le capteur biométrique pour se connecter ou bien si comme le cas des smartphones, vous voulez bien donné accès à quelqu'un à votre téléphone sans pour autant qu'il puisse se connecter sur tous vos sites sans problème.

On peut encore ajouter que même si la faible portabilité vous oblige à ne pas oublier vos mots de passe, ces logiciels ne vous permette de récupérer vos identifiants d'aucune façon en cas de panne.



Remarques :

Le biométrie étant encore peut développer sur les ordinateur portable (uniquement HP) et pas du tout sur les ordinateurs fixes dit de bureau, le déploiement de cette technologie aux ordinateurs de bureau ou non HP pourrais permettre de créer des réseaux afin d'avoir vraiment des capteurs d'empreinte partout pour qu'au final, nos empreintes digitales remplacent totalement nos mots de passe où que l'on soit avec n'importe quel appareil.

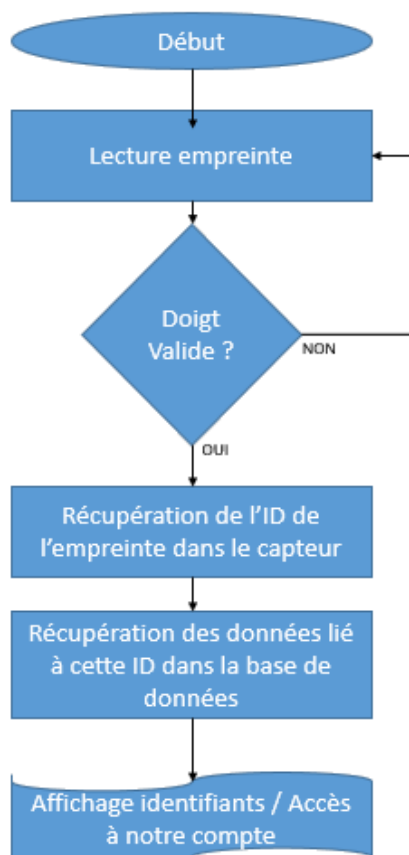
Réalisation

Une fois la phase de réflexion achevée, nous avons enfin pu commencer la réalisation. Nous avons réparti les rôles de la façon suivante :

Raphaël Letourneur	<ul style="list-style-type: none"> • Programmation application gestion (en C#) : Utilisation de Visual Studio • Programmation capteur biométrique (en Arduino) • Gestion de la base de données (MySQL, PhpMyAdmin) • Réflexion des problèmes éventuel ainsi que solution
Kristell Sovero	<ul style="list-style-type: none"> • Design, boîtier extérieur (solidworks)
Robin Violet	<ul style="list-style-type: none"> • Programmation extension Web (javascript) • Aide conception Boîtier

Application de gestion (Raphaël Letourneur)

Connexion :



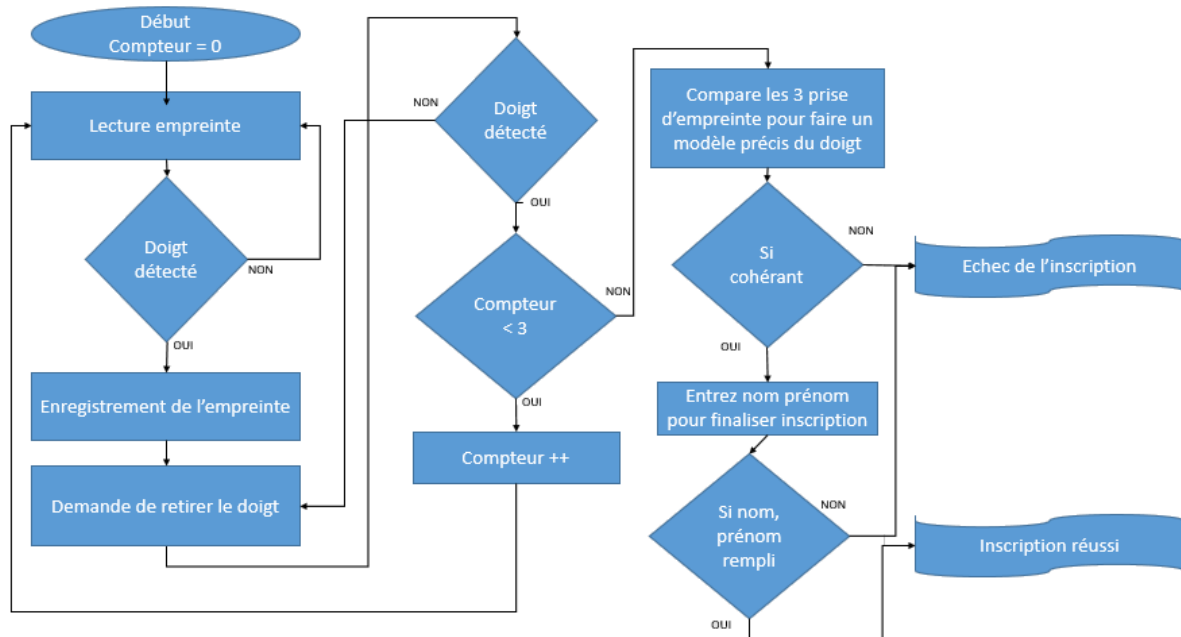
Ceci est un schéma simplifié de l'algorithme de connexion.

A ce moment-là, voici ce que nous avons en face de nous.



La textBox en dessous du bouton ouvrir s'actualise toute seule pour indiquer à l'utilisateur ce qu'il doit faire.

Inscription :



Le procédé d'inscription est quant à lui légèrement plus complexe. Le programme procède à plusieurs captures afin de faire un modèle précis et plus sécurisé de votre empreinte digitale. Il s'assure également que votre Nom, Prénom soit saisi.

Nous nous trouvons actuellement en face de cette fenêtre.

The screenshot shows a window titled 'Veuillez suivre les instructions d'inscription'. On the left is a large fingerprint icon. Below it are input fields for 'Nom' and 'Prenom', followed by a 'S'inscrire' button. On the right, under the heading 'Ports:', there is a dropdown menu showing 'COM5' and an 'Ouvrir' button. Below these is a text box containing the instruction: 'Veuillez poser votre doigt une première fois !'.

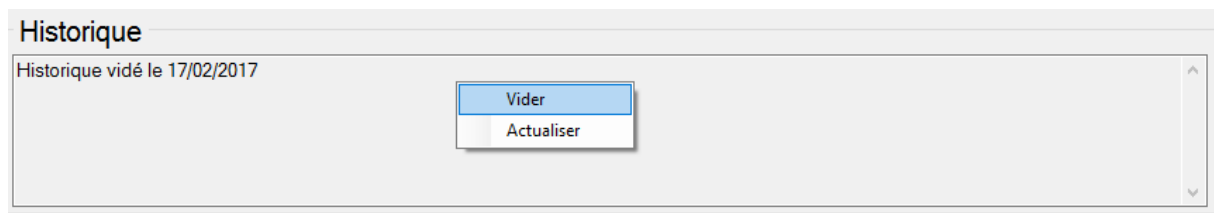
Après la connexion :



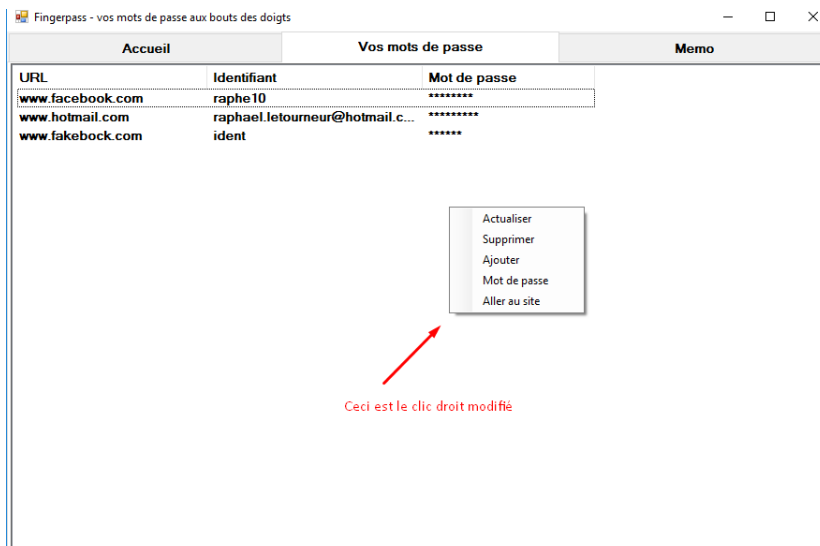
Après la connexion, l'utilisateur a donc accès à son espace perso. On peut voir sur l'accueil un historique des actions effectuées. Cette historique affiche les sites pour lesquels les identifiants ont été supprimés, ajoutés ou bien visionnés avec la date et l'heure de l'action. Dans l'exemple ci-dessus, j'ai tenté de faire planter le logiciel c'est pourquoi les noms de sites peuvent paraître inappropriés. Il s'agissait en fait, de tester tant bien en lecture qu'en écriture, la réaction de la base de données face à des caractères interdits en SQL tel que les « ' » ou bien les « " ».

On peut voir que le logiciel a très bien réagi en supprimant ce caractère plutôt que de créer la célèbre faille SQL donnant un accès total à la base de données.

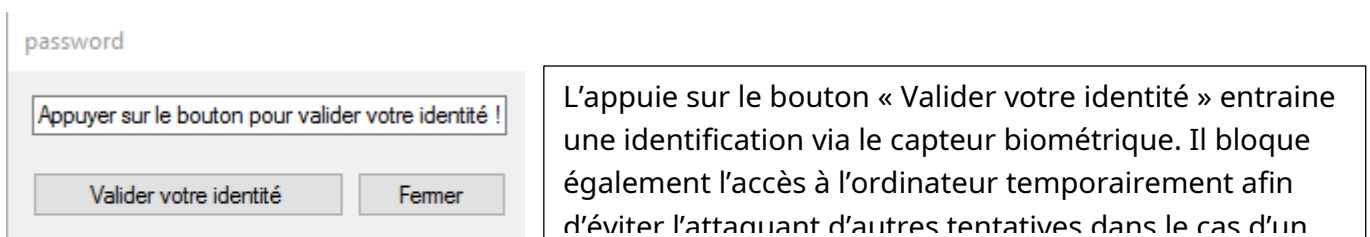
Cet historique peut être vidé avec un clic droit dessus puis vider. Cependant, en plus de la trace qui reste temporairement dans notre base de données, la date du dernier vidage est écrite.



De plus, pour la fonction « mot de passe » si une intrusion est détectée par une empreinte connue du capteur, le nom, prénom associé ainsi que la date et l'IP de l'attaquant sont inscrits dans l'historique.

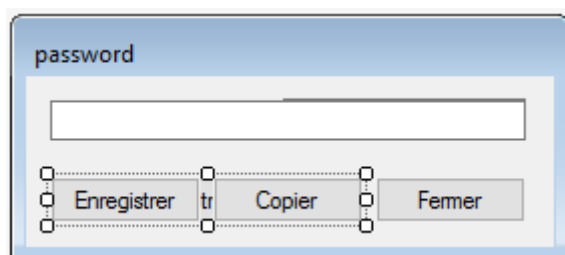


Dans la catégorie « Vos mots de passe », les identifiants associés à l’empreinte sont affichés. Les mots de passes sont remplacés par des « * ». La fonction mot de passe est la plus intéressante.



Comme cité plus haut, si une autre empreinte connue est détectée, ses informations sont stockées ainsi que l’ip afin de prévenir l’utilisateur.

Une fois la vérification d’identité terminée, la fenêtre des mots de passe ressemble à ça :

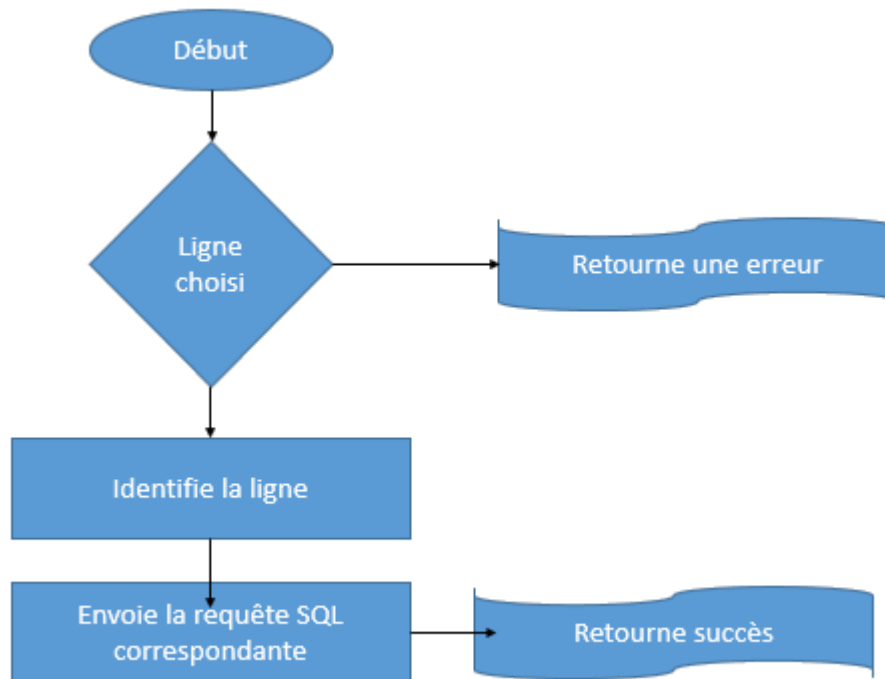


Dans la textbox, le mot de passe est affiché et peut être modifié afin d’être réenregistrer dans la base de données. Il peut également être copier dans le presse papier en un clic avec le bouton copier.

La fonction « Aller au site » ouvre le lien dans le navigateur par défaut. Pour cela, nous avons utilisé le gestionnaire de processus de Windows

Fonction supprimer / accéder / mot de passe :

Ces 3 fonctions ont un point commun. Elle nécessite toute les 3 d'une identification de la ligne sélectionnée et on la même architecture.



En effet, dans leurs fonctionnements généraux, uniquement la case « Envoie la requête SQL » varie. Cette case devient lance le processus d'ouverture de lien dans la fonction accéder, et ouvre la fenêtre de mot de passe pour la fonction « mot de passe ».

La fonction ajout reste elle très banale. Elle utilise une fenêtre qui est celle-ci :

The screenshot shows a window titled 'Ajout' (Add). It contains three input fields: 'URL', 'Identifiant' (Identifier), and 'Mots de passe' (Passwords). Below these fields are two buttons: 'Ajouter' (Add) and 'Annuler' (Cancel).

Extension chrome (Viollet Robin)

J'ai, pour ce projet, créé une extension pour le navigateur Google Chrome permettant de compléter directement sur le formulaire de connexion les nom d'utilisateur et mot de passe sur le site nécessitant une connexion, le tout de façon automatique. À la demande de l'utilisateur, l'extension récupère auprès de l'application développée par Raphaël en C#, les identifiants liés au site et les insère dans le formulaire de connexion. J'ai aussi aider à la fin Kristell à finaliser le boîtier pour qu'il soit plus confortable et que le capteur biométrique s'ajuste mieux dans le boîtier.

L'extension complète le formulaire de connexion du site nécessitant une connexion après l'avoir récupéré et l'envoi au site ce qui permet une connexion automatique. L'extension récupère auprès de l'application les identifiants correspondant à l'empreinte de l'utilisateur pour le site web visité et complète ensuite le formulaire avec ces données.

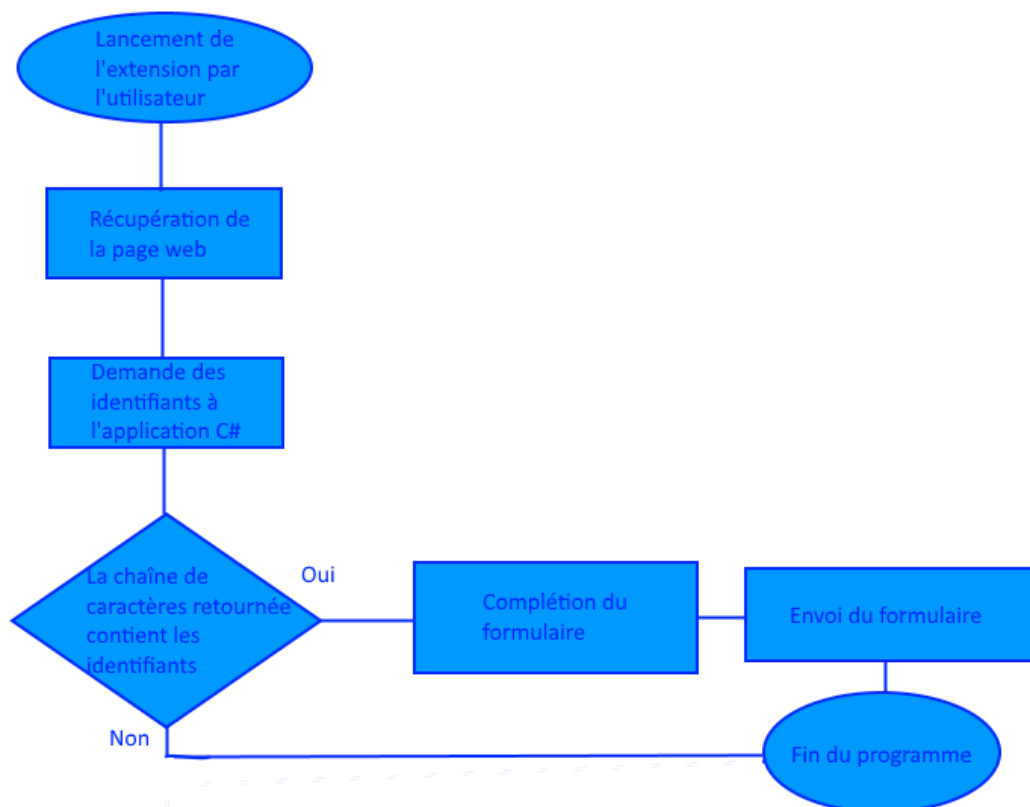


Diagramme de fonctionnement de l'extension Google Chrome

Boîtier par Kristell Sovero

Réalisation (SOVERO Kristell):

Pour l'Authentification biométrique j'ai dû travailler sur l'interface graphique du capteur (travailler sur le boîtier).

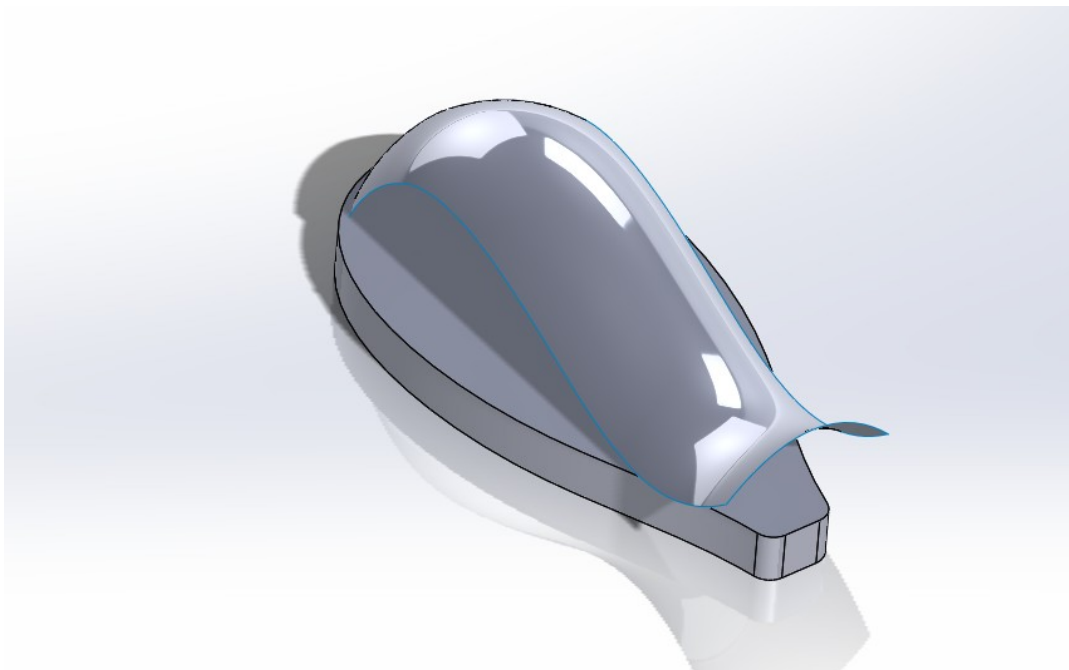
Pour la réalisation du boîtier c'était nécessaire d'utiliser solidworks pour créer quelque chose facile à rapporter et qui puisse plaire à l'utilisateur.

Au début j'avais trouvé 2 idées :

*Une boîte de Clé USB

*Une souris

Après d'avoir réfléchi j'ai trouvé que la souris était l'idée plus précise pour réaliser parce que quand nous utilisons internet avec l'ordinateur et la plupart des gens utilisent une souris donc c'est un objet utilisé normalement pour tout le monde et c'est facile à installer (y a besoin que d'un ordinateur et d'un porte clé USB) et donc j'ai commencé mon travail en solidworks.



La partie difficile de cette réalisation c'était le câblage de la souris pour qu'elle puisse fonctionner avec une petite boîte à cote qui contient le capteur mais finalement je devrais changer d'idée parce que n'y a pas tout le monde qui porte une souris avec elle.

Donc après j'ai retourné a mon idée principal, la boîte de clé USB, mais avec un petit changement que c'était de porter que le capteur.

