CHAPITRE 2 : ETUDE PREALABLE

Introduction

Le présent chapitre sera consacré à repérer les principales caractéristiques de l'existant Ainsi que nous prêtons attention à la solution proposée par Paceword.

Nous présentons alors une analyse de quelques systèmes existants tels que : « Lastpass » et « 1Password » dans le but de dégager leurs limites et de justifier le développement du futur système : « Paceword ».

Nous définissons aussi toutes les fonctionnalités de notre futur système, et ceci en déterminant les besoins fonctionnels et d'appréhender la liste des exigences traduites par les besoins non fonctionnels.

Pour ce faire, un diagramme de cas d'utilisation global a été bien modélisé pour exprimer les besoins et identifier les acteurs.

I – Analyse de l'existant

I.1 – Présentation de l'existant

Il existe plusieurs solutions dans le marché, mais ces solutions poses beaucoup de problèmes.

Parmi les solutions les plus répandus nous trouvons :

LastPass qui est un gestionnaire de mots de passe qui permet à l'utilisateur de se connecter automatiquement aux sites préférés, génère de nouveaux mots de passe forts et complexes en un clic, ou rempli les formulaires en ligne. [3]

1Password qui est un logiciel développé par Agile Web Solutions. Ce logiciel est un gestionnaire de mots de passe qui permet de conserver (ou générer) des mots de passe de façon sécurisée (sites web, applications, numéro de sécurité sociale, cartes bancaires…), mais aussi des notes, et de les protéger par un seul et unique mot de passe. [4]

Ces deux produits sont les leaders sur le marché et compatibles avec tous les systèmes d'exploitation.

I.2 – Critiques de l'existant

Notre analyse comparative est basée sur les forces et les faiblesses de chacune des outils Lastpass et 1Password.

I.2.A – Critères d'évaluation

CRITÈRE	1Password	Lastpass

EXECUTION	1Password offre seulement la possibilité d'enregistrer les informations d'identification d'un site web.	Lastpass nécessite plusieurs étapes pour valider l'authentification.
COUT DES SOLUTIONS	une licence chez 1Password est à (39.99$ /Licence).	Un abonnement chez LastPass est à (12$ / An).
SECURITE DE SOLUTIONS	1Password utilise un système appelé "PBKDF2" qui est utilisé pour ralentir les attaques par force brute en offrant un délai entre chaque tentative, alors qu'ils font ces attaques plus chères.	La même chose.
UTILISATION D'UN CLAVIER VIRTUEL	1Password offre aux utilisateurs un clavier virtuel pour échapper aux programmes malveillants uniquement sur Windows, et à l'exception de Google Chrome navigateur Web.	Pour se défendre contre les enregistreurs de frappe, Lastpass offre aux utilisateurs un clavier virtuel pour échapper aux programmes malveillants sur tout la plates-formes.
PROTECTION	1Password peut protéger les utilisateurs contre les intrus, mais il n'offre pas aux utilisateurs des informations sur les assaillants.	La même chose.

Table 1 Critère d'évaluation de l'existant

I.2.B – Techniques de piratage

ATTAQUE	1Password	Lastpass

FORCE BRUTE	Une attaque par force brute peut être contré par plusieurs mécanismes, 1Password utilise une version plus forte que PBKDF2 (Touche Fonction Dérivation de passe-Based). 1Password utilise la fonction de PBKDF2 mis en œuvre avec SHA-256 pour transformer le mot de passe maître dans la clé de chiffrement.	LastPass utilise une version plus forte que PBKDF2 (Touche Fonction Dérivation de passe-Based). LastPass a choisi d'utiliser SHA-256, un algorithme de hachage lent qui fournit plus de protection contre les attaques par force brute. LastPass effectue x nombre de tours de la fonction pour créer la clé de cryptage, devant un seul tour supplémentaire de PBKDF2 est fait pour créer votre connexion hachage.
INGENIERIE SOCIALE	L'ingénierie sociale consiste à utiliser un type de confiance astuce pour obtenir un mot de passe à la place de la fissuration d'un système, si elle est utilisée dans un système de fraude complexe, il peut être nocif pour tout utilisateur. Les pirates peuvent parfois usurper une identité pour obtenir une information secrète à l'aide d'un appel téléphonique. 1Password ne peut pas se permettre une protection contre ces techniques, ils ne peuvent alerter les utilisateurs de ne jamais révéler leur information à quiconque.	La même chose.

KEYLOGGERS	Pour se défendre contre les enregistreurs de frappe, 1Password a ajouté un clavier virtuel pour éviter les keyloggers, malheureusement ce gestionnaire ne fournit pas cette fonctionnalité sur toutes les plateformes qui exposent l'utilisateur à un risque élevé d'être victime de keyloggers.	Pour se défendre contre les enregistreurs de frappe, Lastpass a ajouté un clavier virtuel pour éviter les keyloggers classiques.
SNIFFERS	Sniffers ou man-in-the-middle attack (MITM) est une attaque utilisée par les pirates pour capturer tous les paquets lors de l'envoi des données dans un réseau public ou non protégé.	LastPass crypte les données pour protéger l'utilisateur, si un pirate veut capturer les données, ces derniers ne peuvent pas être décryptés.
PHISHING	Phishing est la tentative d'acquisition de données sensibles en trompant l'utilisateur vers un faux site Web ou en envoyant un courriel à récupérer des données sensibles. Toute entreprise peut être ciblée d'une attaque de phishing, il y'a des histoires bien connues où le phishing avait conduit la société à une grande perte, par exemple des cibles (magasins) ont exposé des informations de 110.000.000 utilisateurs, et le directeur général et personnel de sécurité étaient tiré à cause des dégâts. 1Password ne dispose pas de solution contre ce type d'attaque, ils peuvent acheter un certificat HTTPS et dire à l'utilisateur de faire attention au site Web qu'ils visitent, car les pirates peuvent imiter n'importe quel site Web et par exemple au lieu d'utiliser www.1Password.com ils peuvent utiliser www.1Password.us (ce site est actuellement disponible).	La même chose.

RAINBOW TABLES	Rainbow Tables sont des tables précompilés d'inverser les fonctions de hachage, créés par Philippe Oechslin, ils sont utilisés pour casser les mots de passe des tables de hachage pour récupérer un mot de passe initial, certains pirates ont une énorme base de données des résultats pré-haché, et ils regardent le hash du mot de passe puis regardent les résultats pré-haché pour inverser la fonctionnalité de hachage. Beaucoup d'entreprises utilisent MD5 ou SHA-1 en ajoutant un sel pour rendre les résultats moins efficace, par exemple Playstation Network ou Adobe a été piraté et tout le hachage des utilisateurs ont été exposés, alors ils ont demandé à chaque utilisateur de changer leurs mots de passe. 1Password sûrement utilise la même technique pour stocker les données des utilisateurs.	La même chose.
RECUPERATION DE MOT DE PASSE	1Password n'envoie pas une reprise parce que l'utilisateur ne doit jamais oublier le mot de passe maître, il peut se produire, mais ils conseillent à l'utilisateur de rappeler le seul mot de passe, il ne l'oubliera pas.	La même chose.

LE CLONAGE DE TELEPHONE (SIM)	LastPass est le seul gestionnaire de mot de passe qui utilise un double système d'authentification, l'utilisateur reçoit un message texte ou un appel téléphonique qui génère un OTP (One Time Password) qui laisse l'utilisateur s'authentifie, ou en utilisant un YubiKey qui est une clé USB pour authentifier l'utilisateur mais cette solution a besoin d'un matériel spécial. Il y a un problème sur les systèmes doubles d'authentification, une carte SIM peut être cloné, tout pirate peut le faire et il peut répondre à l'appel avant l'utilisateur, et il peut recevoir un message texte au même moment que l'utilisateur le reçoit.	
LES SCANNERS DE VULNERABILITÉS	Les scanners de vulnérabilités sont des logiciels conçus pour les systèmes d'exploitation pen-test, ils utilisent une base de données et vérifie si la victime n'est pas protégée. Si un utilisateur ne met pas à jour son OS, il peut être exposé à un risque de ces scanners, et malheureusement, il n'y a pas un gestionnaire de mot de passe qui peut protéger un utilisateur à ce niveau si le système d'exploitation ne protège pas l'utilisateur, les mots de passe des gestionnaires peuvent être mis à jour après la découverte d'une vulnérabilité critique avec des protocoles utilisés, tels que SSL, TLS.	

Table 2 Description des techniques de piratage

II – Paceword : la solution proposée

Introduction

D'après les études qu'on a effectuées la solution appelée Paceword que nous proposons, vise à combler les problèmes cités auparavant, cette solution est le seul moyen d'authentification en une seule étape qui n'utilise pas un matériel supplémentaire.

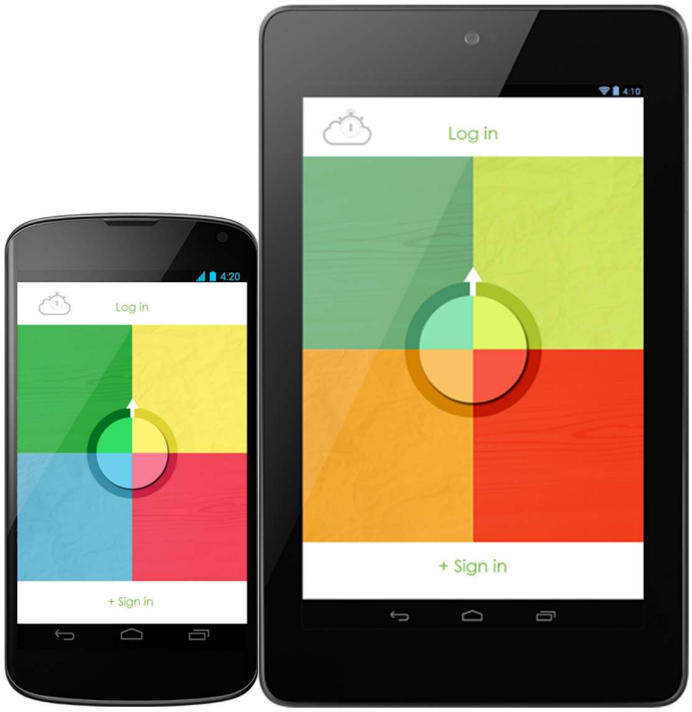

Figure 5 Paceword sur Téléphone et Tablette

II.1 – Etude théorique du Paceword

II.1.A – Spécificités algorithmiques

Il faudrait utiliser deux types de compte à rebours pour assurer l'authentification de l'utilisateur :

1- Le chronomètre de l'application démarre lorsque l'utilisateur touche un carreau, on doit autoriser un décalage de 300ms par touche.
2- Un toucher est considéré un appui long si la couleur touchée dure plus que 400 ms.
3- Un long appui autorise 250ms de décalage entre le moment du toucher et l'instant où l'utilisateur retire son doigt.

II.1.B – Exemples des scénarios

Scénario A :

L'utilisateur tape une fois chaque carreau rapidement (sans appui long), la moyenne du temps qu'il met pour toucher chaque carreau est enregistré comme le suivant (0.000s, 0.150s, 0.500s, 0.750s).

La valeur que l'utilisateur ne doit pas dépasser est de (0.000s, 0.450s, 0.800s, 1.050s).

Scénario B :

L'utilisateur tape une fois chaque carreau rapidement, cependant le dernier carreau est un appui long, la moyenne de temps qu'il met est (0.000s, 0.400s, 0.600s, 0.700s-1.000s).

La valeur que l'utilisateur ne doit pas dépasser (0.000s, 0.700s, 0.900s, 1.000s-1.250s).

II.2 – Etude technique du Paceword

II.2.A – Critères d'évaluation

- Exécution

Paceword offrira la possibilité d'enregistrer toutes les informations d'identification, (cartes de crédit, ou des formules de signe-up, APS, FTP, iTunes), l'utilisateur peut choisir le compte que qu'il souhait pour se connecter,

Il faut seulement deux étapes pour valider l'authentification.

Paceword est plus sûr, plus rapide et plus intuitive.

- Cout Des Solutions

Paceword est gratuit avec un abonnement de 9,99$ /An, 6,99$/6Mois, ou 3.99$ /3Mois, un compte gratuit n'offre pas la fonctionnalité de synchronisation des données, et propose seulement 10 pouvoirs gratuitement.

- Sécurité De Solutions

Paceword ne nécessite aucun système supplémentaire pour protéger les utilisateurs contre les attaques par force brute, disant qu'un pirate a trouvé la clé pour s'authentifier, il ne peut pas reproduire le même rythme de l'utilisateur, car il y'a des possibilités infinies avec des rythmes, donc une attaque par force brute sur Paceword coûte beaucoup plus que 1Password et LastPass.

➢ Utilisation D'un Clavier Virtuel

Ces types de programmes malveillants deviennent désuets contre Paceword qui n'utilise pas un clavier pour que les utilisateurs puissent s'authentifier, ce qui rend Paceword plus efficace et sécurisé pour l'information la plus ciblée par les programmes malveillants qui est le mot de passe. Paceword efface le concept de mot de passe.

➢ Protection

Tout en utilisant Paceword, si un intrus a obtenu le mauvais tempo, une image sera envoyé au compte DropBox et être notifié sur les périphériques d'utilisateur.

Contre les concurrents, Paceword aide l'utilisateur à détecter qui lui vise.

II.2.B – Techniques de piratage

➢ Force Brute

Paceword peut connecter uniquement les appareils enregistrés, essentiellement une attaque par force brute ne peut pas travailler tout simplement moins que l'attaquant ait en sa possession l'appareil. L'utilisateur peut supprimer ses données de téléphone lorsque son appareil est volé.

➢ Ingénierie Sociale

Paceword peut être efficace contre ce type d'attaques, car la valeur du rythme ne peut être communiquée entre les utilisateurs, il n'y a pas moyen de communication pour partager une information abstraite comme le rythme.

➢ Keyloggers

Paceword ne nécessite pas d'un clavier virtuel et ne n'utilise pas des caractères pour que les utilisateurs puissent se connecter, certains pirates peuvent capturer l'écran du Smartphone de l'utilisateur lors de l'authentification, mais ce scénario peut être facilement contré par l'ajout d'une caractéristique technique pour éviter toute capture d'écran en faisant complètement l'écran noir tout en prenant les captures d'écran.

➢ Sniffers

Paceword va également crypter les données avant tout envoi pour protéger l'utilisateur contre cette attaque.

➢ Phishing

Espérons que, Paceword peut contrer cette attaque en effectuant une vérification de l'adresse IP, en utilisant les statistiques des utilisateurs, nous pouvons empêcher les utilisateurs d'être victimes en leur disant par exemple: "L'adresse IP de paceword.us est 66.66.666.888 et il nes'est pas garanti ».

Avec un pop-up de confirmation, nous pouvons les rediriger vers le site correct, si le pop-up apparaît trois fois l'un après l'autre, nous pouvons les informer que le réseau est compromis et le besoin d'utiliser un VPN ou modifier le réseau.

➢ Rainbow Tables

Paceword possède une autre approche pour résoudre ce problème.

Appart l'authentification à l'aide de chiffres et de mots de passe, les pirates ne peuvent pas générés le hachage des valeurs de rythme, ce qui rend la base de données plus complexe à comprendre.

Disant une entreprise utilise notre API pour authentifier leurs utilisateurs, afin de voler les données des utilisateurs, les attaquants peuvent pirater à la fois la société ciblée et notre base de données, et parce que on stocke seulement les valeurs de rythme ce scénario peut être prédit et nous pouvons utiliser des règles de pare-feu pour refuser toute connexion externe et la construction d'une base de données de réseau sécurisé, pas même de l'entreprise ou le personnel peut lire le rythme en valeurs de hashage, une fois les données stockées, personne ne peut le déchiffrer.

Si la base de données de l'entreprise est piratée, ils sont partiellement protégés jusqu'à ce qu'ils demandent aux utilisateurs de changer leurs mots de passe, en attendant, nous allons faire en sorte de bloquer toute authentification qui ne correspond pas le rythme de l'utilisateur.

➢ Récupération De Mot De Passe

Paceword ne repose pas sur un mot de passe, la probabilité d'oublier le rythme est moins que d'oublier le mot de passe, mais nous avons obtenu une solution pour les utilisateurs qui ont besoin d'au moins deux périphériques authentifiés.

Lorsque l'utilisateur utilise Paceword sur un nouveau dispositif, il doit enregistrer l'appareil en utilisant son e-mail, donc si il a oublié le rythme de dispositif «A», il peut utiliser le dispositif "B" pour supprimer le périphérique "A", puis enregistrer son nouveau dispositif, la synchronisation sera pour partager les données sur les deux appareils.

➢ Le Clonage De Téléphone (Sim)

Paceword est un système d'authentification de double contrôle basé sur le motif de carrés et le rythme de l'utilisateur, ce qui rend les systèmes d'authentification doubles tels que Google Authenticator ou 3DS (conçus

par le réseau Lyra et utilisés par Visa) moins efficaces que Paceword si on compare la vitesse d'exécution des deux systèmes.

➢ Résumé

Nous pouvons présenter la liste des techniques de piratage que notre solution Paceword peut se défendre sous le tableau suivant :

ATTAQUES	PACEWORD	LASTPASS	1PASSWORD
Brute force	✓	✓	✓
Social engineering	✓	×	×
Keyloggers	✓	✓	×
Sniffers	✓	✓	✓
Phishing	✓	×	×
Rainbow Table	✓	×	×
Password recovery	✓	×	×
Phone cloning (SIM)	✓	×	×
Vulnerability scan	×	×	×
Virus/Trojan/Worm	×	×	×

Table 3 résumé des techniques de piratage que Paceword peut se défendre

III - Capture des besoins

III.1 – Identification des acteurs

En principe deux types d'utilisateur ont été identifiés:

- Utilisateur : qui est l'utilisateur du Paceword.

- Administrateur : qui est l'administrateur du Paceword.

III.2 – Les besoins fonctionnels

Le futur système doit permettre à l'utilisateur « Client Paceword » de :

- S'enregistrer
- Changer le schéma rythmique des doigts
- Consulter les statistiques
- Contacter l'administration
- Laisser son avis sur Google Play
- Consulter la page official du Paceword sur Facebook

Le futur système doit permettre à l'utilisateur « Admin Paceword » de :

- Générer des graphes et des rapports
- Gérer les emails

III.3 – Les besoins non fonctionnels

III.3.A – Contraintes ergonomiques

L'interface de notre future application doit respecter la charte graphique d'une application qui ressemble à un **Screen locker**, elle doit donc permettre :

- verrouiller le téléphone,
- désactiver le bouton Home, □

- l'ouverture au démarrage du téléphone,
- désactiver toutes les activités,
- recevoir des appels,
- inclure un design simple,
- L'utilisateur doit être guidé lors de la première utilisation.

III.3.B – Contraintes techniques

- L'application doit garantir la sécurité à travers la gestion des droits d'accès,
- L'accès à la base de données doit être souple et rapide,
- L'application doit être toujours fonctionnelle,
- Espace de stockage des données suffisant,
- L'application doit détecter la présence d'une connexion internet,
- Temps de réponse minimum,

III.4 – Diagramme de cas d'utilisation

Les diagrammes des cas d'utilisation identifient les fonctionnalités fournies par le système (cas d'utilisation), les utilisateurs qui interagissent avec le système (acteurs), et les interactions entre ces derniers. Les cas d'utilisation sont utilisés dans la phase d'analyse pour définir les besoins de "haut niveau" du système. Les objectifs principaux des diagrammes des cas d'utilisation sont:

- fournir une vue de haut-niveau sur ce que fait le système

- Identifier les utilisateurs ("acteurs") du système

- Déterminer des secteurs nécessitant des interfaces homme-machine. (IHM)

Les cas d'utilisation se prolongent au delà des diagrammes imagés. En fait, des descriptions textuelles des cas d'utilisation sont souvent employées pour les compléter et représenter leurs fonctionnalités plus en détail.

Ci-dessous le diagramme de cas d'utilisation général de notre système :

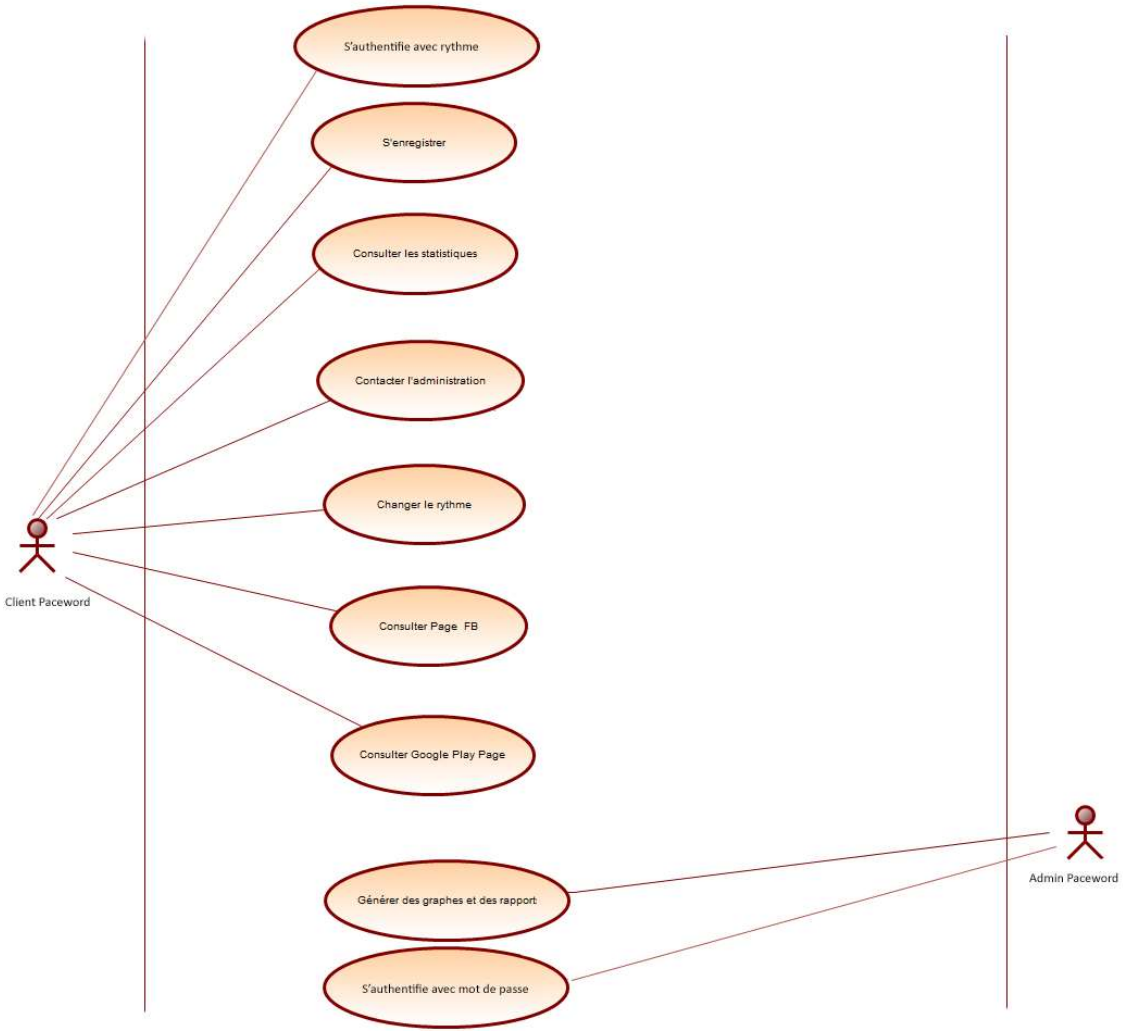

Diagramme 2 Diagramme de cas d'utilisation général

Conclusion

Ce chapitre nous a permis de dégager les limites des solutions existantes actuellement et les comparer avec la solution Paceword.

On a pu faire aussi un découpage fonctionnel de notre système par le biais du diagramme de cas d'utilisation et de consacrer les contraintes ergonomiques et techniques.

Dans le chapitre qui suive, une analyse bien détaillée pour les cas d'utilisation globale de notre système sera présentée.