Cahier des charges
Face Key

Matthieu Vilain, Quentin Gerard, Louis L'Haridon

I. Situation initiale

Problème des mots de passe

De nos jours on observe une augmentation du nombre de sites qui nécessite la création d'un compte : réseaux sociaux, diffèrent compte mail, opérateur téléphonique, journaux en ligne … Il devient difficile d'avoir un mot de passe différent par site, qu'il soit assez complexe pour être sécurisé et qu'on n'ait pas besoin de la noter quelque part. La plupart des utilisateurs utilise donc un seul mot de passe, souvent très simple, en dépit de la sécurité. Leur compte et informations qu'ils contiennent deviennent donc facilement hackable et comme les comptes sont souvent liés, on risque un hackage en chaine de beaucoup de ses comptes.

Une solution développée pour pallier ce problème est le gestionnaire de mot de passe (GMDP). Le principe est simple : l'utilisateur n'a qu'un seul gros mot de passe à connaitre et c'est le GMDP qui s'occupe des combinaisons login/mot de passe sécurisé pour chaque site. L'un des problèmes de cette solution est qu'il faut toujours retenir un mot de passe compliquer pour déverrouiller le GMDP et donc ce déverrouillage peut prendre plus de temps. Avec cette méthode il peut aussi être fastidieux, non intuitif et peu sécurisé de partager l'accès à un compte (partager son compteur d'opérateur téléphonique avec son conjoint par exemple).

Maturation de la technologie

Avec l'émergence du deeplearning et d'autres technique de traitement d'image et de machine learning, les techniques de reconnaissance faciale deviennent de plus en plus performante. Certain algorithme arrive même à battre l'humain dans certaines conditions (Chaochao Lu et Xiaou Tang 2014). De plus beaucoup de grands acteurs économiques s'attaquent au problème, obtiennent d'excellents résultats et en sortent des applications, par exemple Facebook avec deepFace en 2014, Microsoft avec Hello en 2015 et enfin très récemment Apple avec FaceID (en 2017).

Il a également été prouvé que la reconnaissance faciale pouvait être plus difficilement hackable que des mots de passe de par la complexité et l'unicité du visage humain.

II. Notre solution : Face Key

Présentation

Notre idée est de combiner les technologies émergentes avec un gestionnaire de mot de passe traditionnel afin de supprimer le mot de passe fastidieux à apprendre et long à taper afin de rendre instantanée et sécurisée la connexion à nos sites préférés.

Fonctionnement

Notre application se présentera sous forme d'un plug-in web, il suffira de se présenter sur la page du site où l'on veut se connecter et cliquer sur le plug-in en haut à droite du navigateur. L'application va alors prendre une photo avec la webcam du l'ordinateur, l'envoyer sur l'application Face Key qui tourne sur l'ordinateur de l'utilisateur ; un algorithme va trouver le visage présent d'en l'image et l'identifier. Si il s'agit bien du visage de l'utilisateur une requête sera faites aux bases de données des serveurs Face Key afin d'obtenir les identifiants pour la page visitée. La page s'actualise avec les identifiants du compte et d'un coup d'œil vous êtes connecté.

Nous proposons également un système de partage de compte. L'utilisateur peut choisir de partager certains de ses comptes avec d'autres utilisateurs Face Key. Il choisira alors quel personne est autorisé à utiliser quel compte et de la même manière l'autre utilisateur pourra accéder uniquement avec son visage au compte du premier.

Organisation des différents projets

Le projet Face Key s'intègre dans le projet d'intégration et recoupe donc les projets de base de données, de réseau, de développement d'application mobile et potentiellement celle de système d'exploitation.

Base de données

Nous utiliserons une base de données pour stocker différentes informations et paramètres de nos utilisateurs. Par exemple les informations de connexion à la plateforme, les couples login/password pour se connecter aux différents sites, différents paramètre de préférence de l'utilisateur, des données utilisateur collecter sur chaque site (heure moyenne de connexion, fréquence de connexion …), des données sur l'utilisation de notre application(date de création, fréquence d'utilisation …).

Un des objectif est de rendre la base de données ''anonyme'', c'est-à-dire qu'on ne demande pas de nom, prénom à notre utilisateur, uniquement une adresse mail, afin que si quelqu'un à accès aux données que nous collectons il ne puisse pas remonter à l'identité de nos utilisateurs.

Les images nécessaires pour l'apprentissage des visages ne seront pas stockées dans une base de données sql, après quelques recherche nous pensons que cet outil n'est pas adapté.

Pour plus d'informations sur la partie base de données, consultez le schéma relationnel ci joint.

Réseau

La partie réseau de l'application est décomposée en 3 parties :

- Le Plugin Web
- Un Client local (tournant sur la machine de l'utilisateur)
- Un Serveur Distant relié à une Base de Donnée

Le Plugin Web communiquera avec le serveur local et lui transmettra toutes les entrées de l'utilisateur. Le client local lui s'occupera de traiter toutes les demandes de l'utilisateur en effectuant les taches nécessaires quant à la résolution du problème donné par l'utilisateur. Le client local communiquera avec le serveur distant (lui-même relié à une base de données) pour obtenir les données nécessaires à la résolution du problème.

La connexion entre le client et le serveur sera assuré par le protocole TCP permettant un transport des informations fiable et en mode connecté.

Les informations transitant sur le réseau seront de plusieurs natures : Images, textes, fichiers, etc …

Développement d'application mobile

Nous n'avons pas encore demandé à Monsieur Dimitrios si l'idée est en accord avec ce qu'il demande, mais voici l'idée :

A partir de l'application Face Key, l'utilisateur pourrai gérer les différents accès à ses comptes : autoriser d'autres utilisateurs à se connecter sur ses comptes, faire des mises à jour de ses mots de passe … Il pourrait également prendre des photos de son visage pour augmenter la précision de la reconnaissance.

Cette idée regroupe les spécifications demandées pour le projet mais est-elle trop ambitieuse ?

Système d'exploitation

Nous ne pouvons pas encore définir clairement dans quelle mesure le projet de système d'exploitation sera intégrer à notre projet. (Optimisation de la forward/back propagation dans le réseau de neurones en multithreadant les multiplications de matrice ?)

Projet de synthèse

Pour la partie projet de synthèse, nous apportons chacun un plus au projet en y incorporant nos domaines préférés :

- Louis l'Haridon : plug-in web/interface utilisateur
- Quentin Gerard : cryptographie/sécurité réseau
- Matthieu Vilain : machine learning/reconnaissance faciale

III. Nos ambitions, nos limites

Tout ce qui a été présenté précédemment est la vision idéale du projet. Dans un premier temps nous nous concentrerons sur le gestionnaire de mot de passe avec reconnaissance faciale sans implémenter le partage de compte mais en concevant l'architecture du logiciel pour que le partage soit possible.

En revanche si nous arrivons à tout finir en temps et en heure, nous nous laissons libre d'ajouter des fonctionnalités comme analyse de l'émotion de l'utilisateur lorsqu'il déverrouille l'application ou autre.

L'idéal initial était de pousser le projet à fond en développent un protocole d'installation, une documentation détaillé ect afin de proposer le logiciel final en open source. Cet objectif ne pourra pas être réalisé au court du projet de L3 par manque de temps.