Cahier des Charges du projet StickPass : un gestionnaire de mots de passe matériel alimenté via USB

Version 1.0

Table des matières

1. Sommaire exécutif

1.1 Sommaire

L'objectif de ce projet est de concevoir et fabriquer un gestionnaire de mots de passe matériel alimenté via USB. Ce projet est développé dans le cadre du cours ELE792 Projet de fin d'études en génie électrique.

1.2 Objectif et cadre du cahier des charges

L'objectif du document de cahier des charges est de décrire le travail à accomplir et d'identifier les différentes contraintes reliées au projet. Le cahier des charge fournit aussi la liste des livrables ainsi que la planification du projet.

2. Description du projet

Cette section décrit les facteurs ayant un impact sur le projet et ses requis.

2.1 Contexte du projet

Le projet est développé dans le cadre du cours ELE792 – Projet de fin d'études en génie Électrique de la session hiver 2016 à l'École de Technologie Supérieure de Montréal.

2.2 Détails sur le projet

Le gestionnaire de mots de passe matériel alimenté via USB (nommé StickPass) est un gadget électronique ayant pour fonction de stocker des identités (combinaisons usager/mot de passe) afin de faciliter l'utilisation d'une multitude d'identités pour un utilisateur. Avec l'augmentation du nombre d'applications et de services utilisés dans le quotidien, il devient de plus en plus difficile de gérer plusieurs identités tout en satisfaisant les contraintes de sécurité, c'est à dire d'utiliser des mots de passe différents et complexes pour chaque service ou application.

StickPass permet à l'usager d'utiliser ces identités sans avoir le besoin de connaître les mots de passe. Cela permet l'utilisation de longs mots de passe à entropie très élevée ce qui améliore grandement la sécurité. StickPass agit en tant que dispositif à interface humaine au même titre qu'un clavier ou une souris. De cette façon, l'appareil est peut être détecté sur la plupart des ordinateurs modernes sans nécessiter l'installation d'un pilote propre. StickPass est utilisé à l'aide de deux boutons, un servant à la navigation parmi les identités et un servant à injecter le mot de passe.

2.3 Caractéristiques usager du projet

L'utilisateur typique du gestionnaire de mots de passes matériel alimenté via USB est l'individu qui utilise plusieurs applications ou services informatiques requérant une authentification avec mot de passe. Ci-dessous est présenté une liste de cas d'application typiques:

- Utilisation de plusieurs boites de courriel.
- Utilisation d'applications web pour le média (Netflix, youtube).
- Utilisation d'applications bancaires sur le web.
- Utilisation d'applications d'entreprise (professionnels).
- Utilisation d'application académiques (étudiants).
- Utilisation de quelconque service protégé via un mot de passe.

2.4 Suppositions et contraintes

Ce document suppose que l'usager utilisera l'appareil dans un ordinateur possédant des ports USB supportant le protocole USB 1.X ou USB 2.0. Les contraintes suivantes ont été identifiées :

- L'utilisateur devra posséder les privilèges nécessaires pour utiliser le port USB.
- Le système d'exploitation devra posséder par défaut des pilotes pour les appareils de type HID (human interface device). (voir annexe pour définition des acronymes et détails)
- L'ordinateur devra fournir de la puissance au port USB en respect avec la spécification USB (5V @ 1A).
- Les combinaisons usager/mot de passe sont des caractères encodé en UTF-8 représentables selon la table ASCII. Ceci assume donc que 1 char = 1 byte.

3. Exigences du système

Cette section décrit les exigences du système avec assez de détails pour que le concepteur puisse concevoir le système tout en répondant aux exigences et que le testeur puisse vérifier que le système conçu réponde aux exigences.

Définitions des priorités

- Les définitions suivantes sont données à titre indicatif afin de prioriser les requis :
- Priorité 1 – Le requis est absolument nécessaire pour la fonctionnalité de base du système.
- Priorité 2 – Le requis entraîne des avantages immédiats et augmente la performance du système, mais n'est pas nécessaire pour la fonctionnalité de base.
- Priorité 3 – Le requis serait agréable à satisfaire et est un bonus (nice to have).

3.1 Tableau des exigences du système

Le tableau ci-dessous liste les exigences du système et utilise la nomenclature suivante :

RXXX_## où ## est le numéro du requis et RXXX représente le type de requis selon la formule ci-dessous:

- RFUN = requis fonctionnel : affecte la fonctionnalité du système
- RAPP = requis de l'application usager
- RSEC = requis de sécurité

Requis#	Exigence	Commentaires	Priorité
RFUN_01	Le système doit s'allumer lorsque branché dans un port USB	La mise sous tension initie le fonctionnement du système.	1
RFUN_02	Le système doit être détecté en tant que HID.	Le système d'exploitation de l'hôte détecte le système et l'énumère comme un HID.	1
RSEC_01	La mémoire du système est protégée.	Seul l'usager approprié peut accéder au contenu de la mémoire interne du système qui contient les mots de passe.	2
RFUN_03	Le système doit être en mesure d'injecter de l'information dans l'hôte.	L'utilisation normale du système implique que le système envoie des informations relatives à l'utilisateur et au mot de passe respectif vers l'hôte. Cette interaction émule le fonctionnement d'un clavier : le mot de passe est injecté dans un champ de texte comme s'il avait été tapé au clavier par l'utilisateur.	1
RSEC_02	La mémoire du système est encryptée.	La mémoire interne doit être décryptée avant la lecture. Ceci protège l'information en cas de pénétration.	2
RFUN_04	Le système peut emmagasiner au moins 10 combinaisons usager/mot de passe.	On alloue une taille moyenne de 64 bytes par combinaison soit approximativement 32 bytes pour le nom d'usager et 32 bytes pour le mot de passe.	2
RAPP_01	Le système peut générer des mots de passe à entropie élevée.	L'utilisateur peut décider d'emmagasiner un mot de passe généré par le système afin de maximiser la complexité du mot de passe.	3
RFUN_05	Le système permet de naviguer dans la liste de combinaisons usager/mot de passe.	L'utilisateur peut naviguer la liste de combinaison et choisir quelle identité qu'il veut utiliser.	1
RFUN_06	Le système supporte les mise à jour.	Si nécessaire, l'usager peut effectuer une mise à jour du microprogramme via le port USB.	3
RSEC_03	Le système utilise 2FA.	L'usager doit utiliser une combinaison de deux éléments pour débloquer le système avant utilisation.	3
RAPP_02	Le système peut être géré à partir d'une application usager CLI.	L'application permet d'ajouter et de retirer des combinaisons, générer des mots de passe etc	2
RFUN_07	Le système fonctionne sous Linux.	Environnement de test principal.	1
RFUN_08	Le système fonctionne sous OSX.		2
RFUN_09	Le système fonctionne sous Windows.	Requiert une implémentation supplémentaire de l'application usager	3
RAPP_03	L'application usager contient un manuel d'instructions complet.	Sous forme de manpage	1

Requis#	Exigence	Commentaires	Priorité
RFUN_10	La durée de vie du système doit être d'au moins 5 ans.	Choisir une mémoire flash qui peut supporter le nombre requis de cycles d'écriture/lecture.	2

Tableau 1: Tableau des requis fonctionnels

3.2 Exigence supplémentaire

Cette section identifie une exigence particulière qui n'a pas d'impact sur la fonctionnalité du système comme tel. C'est une exigence optionnelle qui est en lien avec la méthodologie employée et qui peut être catégorisé comme : « agréable à avoir ».

L'exigence est de rendre le projet open source (libre) dans sa totalité. Cela veut dire que le matériel, le logiciel ainsi que la méthodologie sera open source.

3.2.1 Logiciel open source

Cela signifie le code source original du projet est librement accessible et peut être redistribué et modifié par quiconque le désire.

3.2.2 Matériel open source

Cela signifie que les schémas électriques et mécaniques originaux du projet sont librement accessibles et peuvent être modifiés par quiconque le désire.

3.2.3 Méthodologie open source

Cela signifie que tous les outils logiciels utilisés dans ce projet seront des outils gratuits (gratuit dans le sens libre, c'est à dire qu'ils sont open source eux même, mais pas nécessairement sans coût monétaire). Cela s'applique également aux logiciels utilisés pour la documentation et la planification de projet.

4. Scénarios client (User stories)

Cette section liste une variété de scénarios clients (plus connu sous le nom anglais : user story). Les scénarios clients servent à clarifier les requis en décrivant un exemple concret d'utilisation typique du système.

1. En tant qu'utilisateur, je peux emmagasiner mes noms d'utilisateur et mots de passe sur le StickPass.
2. En tant qu'utilisateur, je peux utiliser le StickPass afin d'éviter d'avoir à taper mes noms d'utilisateur et mots de passe dans les services que j'utilise.
3. En tant qu'utilisateur, de je peux générer des mots de passe complexes avec le StickPass.
4. En tant qu'utilisateur, je veux que mes identités soient emmagasinées dans un emplacement sécuritaire et difficile à pénétrer.
5. En tant qu'utilisateur, je veux que le StickPass soit facile à configurer et à utiliser.

5. Livrables

Cette section couvre la liste des livrables à remettre dans le cadre du projet.

Livrable	**Description**
Rapport d'étape	Document servant à faire le point sur le projet.
Rapport technique final	Rapport de conception du projet.
Code source	Code source intégral du projet et application usager en mode exécutable.
Schémas de conception	Schémas électroniques (et mécaniques s'il y a lieu) de conception.
Prototype	Prototype fonctionnel de l'appareil.
Autres documents	BOM, diagrammes fonctionnels, schémas systèmes et autres documents pertinents

6. Plan du projet

Le tableau ci-dessous présente les tâches à compléter durant le projet et le temps estimé qui y est associé.

Planification des tâches	Temps estimé (h)
Documentation	**21**
Rédaction du rapport d'étape	5
Rédaction du rapport technique final	8
Préparation de la présentation orale	8
Fabrication du circuit électronique (prototype)	**25**
Sélection du microcontrolleur	4
Conception du circuit	6
Approvisionnement des composantes	3
Assemblage du circuit	2
Test de la programmation du microprogramme	6
Sanity check du circuit	4
Conception logiciel	**60**
Implémentation du pilote HID sur le microcontrolleur	4
Implémentation du protocole USB virtuel sur le microcontrolleur	8
Implémentation des requis fonctionnels du système	24
Implémentation des requis de sécurité du système	12
Implémentation de l'application usager	12
Test du logiciel	**44**
Test des communications	6
Test du protocol USB	12
Test du pilote HID	6
Test des requis fonctionnels	8
Test des requis de sécurité	4
Test de l'application usager	6
Test de performance	2
Fabriquation du prototype final	**29**
Conception du PCB	8
Révision du PCB	2
Approvisionnement des composantes	3
Fabrication du PCB	4
Assemblage PCB	4
Test PCB	8
TOTAL	**179**

ANNEXE

Annexe A. Définitions, Acronymes et Abréviations

Ci-dessous une liste des acronymes utilisés dans ce document :

- **HID**: Human Interface Device (dispositif d'interface humain)
  En informatique, la classe de dispositif d'interface humaine USB (de classe USB HID) est une partie de la spécification USB pour les périphériques informatiques: il spécifie une classe d'unité (un type de matériel informatique) pour des périphériques d'interface tels que les claviers, les souris, les manettes de jeu et dispositifs d'affichage alphanumérique.
- **2FA**: Two-Factor Authentication (authentification à deux étapes)
  Authentification à deux facteurs (aussi connu comme 2FA ou 2 -Step vérification) est une technologie qui fournit l'identification des utilisateurs par le biais de la combinaison de deux éléments différents. Ces composants peuvent être quelque chose que l'utilisateur sait, quelque chose que l'utilisateur possède ou quelque chose qui est inséparable de l'utilisateur. Un bon exemple de la vie quotidienne est le retrait d'argent d'un guichet automatique. Seule la combinaison correcte d'une carte bancaire (quelque chose que l'utilisateur possède) et un code NIP (numéro d'identification personnel, soit quelque chose que l'utilisateur connaît) permet à la transaction à effectuer.
- **CLI**: Command line interface (interface de ligne de commande)
  Une interface en ligne de commande est une interface homme-machine dans laquelle la communication entre l'utilisateur et l'ordinateur s'effectue en mode texte.