QUI CONNAIT VOTRE MOT DE PASSE ?

Document Malveillance électronique Mot de passe Dysfonctionnement Évaluation de rendement Authentification Carte à puce Notes Chiffrement Intégrité Liste d'accès Virus Plan de relève Numéro d'employé Perte de réputation Continuité des affaires Document papier Garde barrière Canular Note Pédagogique Vers Dissuasion Cheval de Troie Prévention Fraude Réaction Disponibilité Confinement Clée Biométrie Dossier académique Identification Code source Journalisation Sabotage Antivirus Secret Vulnérabilité Numéro d'assurance sociale Vengeance Examen Incident Détection

Marc-André Drapeau
Conseiller à la sécurité de l'information

HEC MONTRÉAL

Plan de la présentation

- Contexte
- Objectif
- Introduction
- Faiblesses et attaques
- Bonnes pratiques
- Gestionnaire de mots de passe

HEC MONTRÉAL

3

Contexte

- L'École s'est dotée d'une politique de sécurité de l'information.
- Celle-ci constitue un des éléments clés à la sécurité des actifs informationnels de HEC Montréal.

HEC MONTRÉAL

4

Contexte

- La sécurité de l'information couvre plusieurs domaines notamment le « Contrôle d'accès ».
- La bonne gestion du mot de passe est un élément clé aux contrôles d'accès et touche chacun d'entre nous.

HEC MONTRÉAL

5

Contexte

- C'est avec un effort commun que les informations de HEC Montréal seront en sécurité.

HEC MONTRÉAL

6

Objectif

- **Sensibiliser** l'utilisateur d'un code d'accès **aux bonnes pratiques** entourant l'utilisation du mot de passe. Cela permet :
  - d'assurer que les informations sont consultées et modifiées seulement par les **personnes autorisées**;
  - d'identifier les bonnes pratiques à adopter.

HEC MONTRÉAL

7

Introduction

- Tout processus d'authentification réalisé par un utilisateur **engage sa responsabilité**.
- Un **mot de passe** permet de fournir une **preuve de la personne** que nous prétendons être lors de l'accès à un système.

Le **mot de passe** est donc une information personnelle et sensible et doit rester **confidentiel** et secret. Il ne faut pas divulguer son mot de passe.

HEC MONTRÉAL

8

Introduction - Saviez-vous que …

- Les principaux **risques** liés à l'utilisation du mot de passe sont sa **divulgation** et sa **faiblesse**.
- Les mots de passe sont souvent la **seule protection** pour accéder à une **station de travail** ou une **application**.

HEC MONTRÉAL

Les faiblesses et attaques

- L'entreposage
  - **Souvent trop accessible** (écrit sur un post-it, sous le clavier, dans son agenda, un fichier XLS non protégé, etc.)
- Le choix du mot de passe
  - Vulnérable aux attaques par **force brute**
    - Utilisation de toutes les possibilités.
  - Vulnérable aux attaques **hybrides**
    - Utilisation des techniques connues comme de remplacer les « 1 » par des « i », les« 0 » par des « o », les « s » par des « 5 ».
    - Utilisation de combinaisons comme date/prénom/nom/adresse.
  - Vulnérable aux attaques **dictionnaire**
    - Utilisation de mots du dictionnaire, peu importe la langue et le type de dictionnaire (dictionnaire de prénoms, de marques commerciales, de noms d'auteurs et autres.).

HEC MONTRÉAL

Les faiblesses et attaques

- Les 25 **pires** mots de passe (2012)*

password	123456	12345678	abc123	qwerty
monkey	letmein	dragon	111111	baseball
iloveyou	trustno1	1234567	sunshine	master
123123	welcome	shadow	ashley	football
jesus	michael	ninja	mustang	password1

- * http://www.quialacote.ca/2012/11/les-25-pires-mots-de-passe-cuv%C3%A9e-2012.html

HEC MONTRÉAL

11

Les faiblesses et attaques

- L'ingénierie sociale.
- L'hameçonnage.
- L'interception des communications.
- La capture des frappes au clavier.
- L'utilisation de mesure de protection désuète.

… et plusieurs autres attaques possibles …

HEC MONTRÉAL

12

Bonnes pratiques

- Savez-vous reconnaître les fausses affirmations ?
  - Un mot de passe peut être partagé à un nombre limité de personnes.

En aucune circonstance, un mot de passe ne peut être partagé

HEC MONTRÉAL

13

Bonnes pratiques

- Utilisez un **logiciel de gestion des mots de passe** afin de ne pas enregistrer ceux-ci sous une forme non protégée.
- Ce logiciel :
  - **Garde vos mots de passe** de façon sécuritaire.
  - Génère pour vous des **mots de passe robustes**.
  - Facilite l'utilisation de **mots de passe différents** pour tous les sites.

HEC MONTRÉAL

14

Bonnes pratiques

- **Dissociez** vos mots de passe pour le **travail** de ceux de vos services **personnels**.

La robustesse d'une sécurité se définit par le maillon le plus faible.

HEC MONTRÉAL

15

Bonnes pratiques

- Lorsque vous recevez un mot de passe **temporaire**, changez-le dès la première utilisation. Par la suite, **changez** votre mot de passe **régulièrement**.

HEC MONTRÉAL

16

Bonnes pratiques

- Choisir un mot de passe de **qualité**.
  - Facile à mémoriser et difficile à deviner,
  - Méthode phonétique
    - « J'ai du bon fromage au lait acheté à sept îles » devient **Gdbfmgolhta7i**
  - Méthode des premières lettres (citation, paroles d'une chanson, extrait d'un livre, …)
    - « Être ou ne pas être, là est la question ! » devient **Êonpê,lel?!**

HEC MONTRÉAL

17

Bonnes pratiques

- Un mot de passe de qualité est :
  - **Composé** d'un minimum de 8 caractères et comprenant minimalement : minuscule, majuscule et chiffre.
  - **Indépendant** de toutes **informations personnelles** faciles à deviner ou à obtenir. Éviter d'utiliser un nom, numéro de téléphone et date d'anniversaire.
  - **Blindé d'une attaque** par dictionnaire (éviter d'utiliser un mot de passe figurant dans un dictionnaire).

HEC MONTRÉAL

18

Bonnes pratiques - Savez-vous choisir votre mot de passe ?

- Lesquels de ces mots de passe vous paraissent de qualité
  1. Madrapeau2005/09/17
     - Ce mot de passe est composé d'un code utilisateur et d'une date.
  2. trustno1
     - Ce mot de passe est donné en exemple dans cette présentation et fait partie du « top 25 » des pires mots de passe de 2012.
  3. %D/r5$d
     - Mot de passe trop court, il ne compte que 7 caractères.
  4. App114t1ons
     - Mot du dictionnaire avec quelques caractères modifiés.
  5. Xàc-thu'c
     - Mot du dictionnaire « Tieng Viêt »
  6. Alice:4506047i3i
     - Prénom et numéro de téléphone avec le « 1 » remplacé par un « i » et le « 0 » par un « o »
  7. admin@gouv.qc.ca
     - Ce mot de passe est une adresse courriel.

HEC MONTRÉAL

19

Gestionnaire de mots de passe

- Un **gestionnaire de mots de passe** est un type de logiciel qui permet à un utilisateur de centraliser l'ensemble de ses identifiants et mots de passe dans une base de données accessible par un mot de passe unique, afin de n'en avoir plus qu'un seul à retenir.

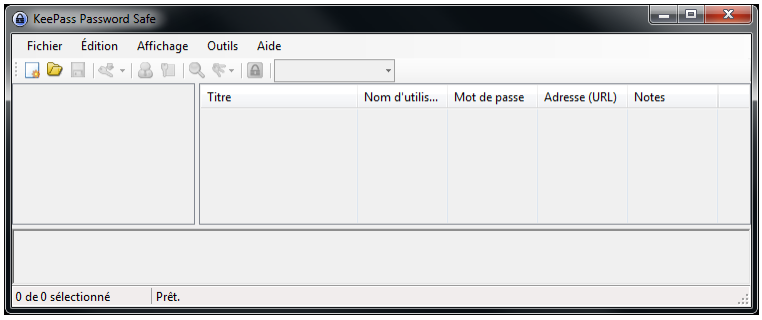
Réf : http://fr.wikipedia.org/wiki/Gestionnaire_de_mots_de_passe

HEC MONTRÉAL

20

Gestionnaire de mots de passe

- Page d'accueil de Keepass

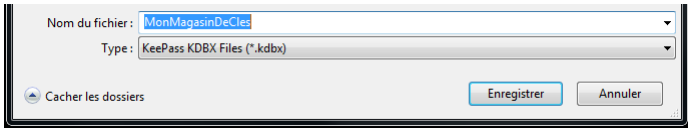


HEC MONTRÉAL

21

Gestionnaire de mots de passe

- Création de votre magasin de clés
  - Fichier / Nouvelle…



HEC MONTRÉAL

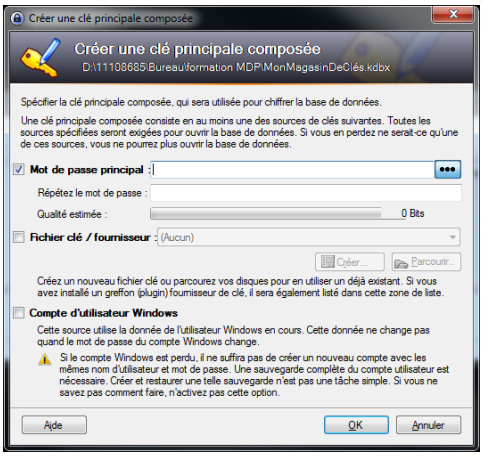
22

Gestionnaire de mots de passe

- Vous devez créer votre clé maître.

Une clé maître est une composition de trois choix.

- Mot de passe
- (et/ou) Fichier clé
- (et/ou) Compte Windows

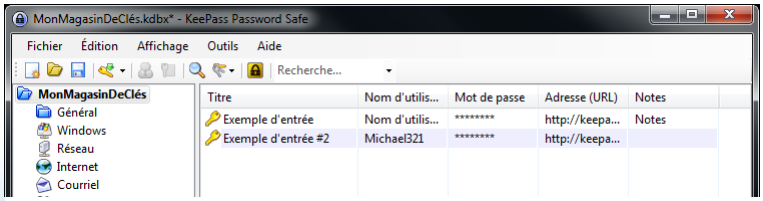


HEC MONTRÉAL

23

Gestionnaire de mots de passe

- Une fois la clé maître créée, vous pouvez saisir vos mots de passe, et les organiser par catégorie.



HEC MONTRÉAL

24

Gestionnaire de mots de passe

- Avertissement

Si vous oubliez votre clé maître, vous perdez également l'accès à tous les mots de passe dans votre magasin de clés. Il n'existe aucun moyen de contournement.

HEC MONTRÉAL

25

Des questions ?

HEC MONTRÉAL

26

Complément

- Options de composition de votre clé maître
- Guide d'utilisation de Keepass

HEC MONTRÉAL

27

Options de composition de votre clé maître (1/3)

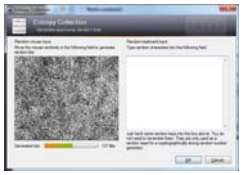
- Premier choix (mot de passe)
  - Protéger votre magasin avec un **mot de passe**
    - Vous devez choisir un mot de passe de qualité ou une phrase de passe. Un indicateur de qualité de votre mot de passe est affiché afin de vous aider à choisir.

HEC MONTRÉAL

28

Options de composition de votre clé maître (2/3)

- Deuxième choix (fichier)



  - Option 1
    - Choisir un fichier.
  - Option 2
    - Générer un fichier. Pour cela, soit :
      - générer du bruit en déplaçant la souris au-dessus du carré poivre et sel.
      - Utiliser l'espace d'édition pour saisir des données aléatoires.

HEC MONTRÉAL

29

Options de composition de votre clé maître (3/3)

- Dernier choix (Authentification Windows)
  - Utiliser votre **authentification Windows**. Pour cela, vous devez vous authentifier toujours avec le même compte Windows pour ouvrir votre magasin de clés.

HEC MONTRÉAL

30

Guide d'utilisation de Keepass (1/9)

Installation de Keepass

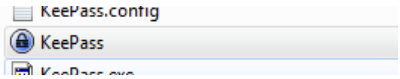
1. Télécharger le fichier « KeePass-2.20.1.zip » à l'adresse suivante : (http://downloads.sourceforge.net/keepass/KeePass-2.20.1.zip)
2. Une fois téléchargée, « décompresser » le fichier .ZIP dans le répertoire de votre choix. C'est à partir de ce répertoire que vous allez par la suite démarrer le logiciel KeePass.

HEC MONTRÉAL

Guide d'utilisation de Keepass (2/9)

Changez la langue pour le français (1/2)

1. Pour changer la langue à français, il suffit de télécharger le fichier « French-2.20f.zip » à l'adresse suivante : (http://downloads.sourceforge.net/keepass/French-2.20f.zip)
2. Une fois téléchargée, « décompresser » le fichier .ZIP suivant dans le répertoire de KeePass.
3. Démarrer le logiciel KeePass en double cliquant sur le fichier KeePass

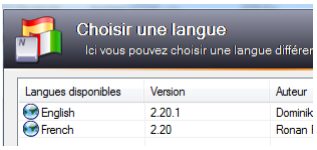


HEC MONTRÉAL

Guide d'utilisation de Keepass (3/9)

Changez la langue pour le français (2/2)

1. Cliquer sur le menu « *View* ».
2. Choisir l'option « *Change Langage* ». Cette action fera apparaître la fenêtre suivante :



3. Cliquer sur « French ». Une fois fait, KeePass redémarre automatiquement et voilà, le tout est en français.

HEC MONTRÉAL

33

Guide d'utilisation de Keepass (4/9)

Créer un magasin de clés (1/3)

1. Cliquer sur le menu Fichier.
2. Cliquer sur l'option « Nouvelle ».
3. Saisir le nom de votre magasin de clés. Cela se fait en écrasant le texte « NouvelleBaseDeDonnées » inscrit à l'emplacement « Nom du fichier : »

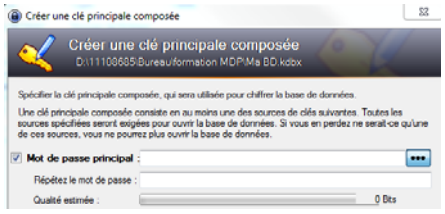
HEC MONTRÉAL

34

Guide d'utilisation de Keepass (5/9)

Créer un magasin de clés (2/3)

- Choisir l'emplacement de sauvegarde
- Cliquer sur le bouton « Enregistrer ». Cela fera apparaître une fenêtre vous demandant de créer votre clé maître.



HEC MONTRÉAL

35

Guide d'utilisation de Keepass (6/9)

Créer un magasin de clés (3/3)

1. Saisir un mot de passe principal
2. Cliquer sur le bouton « OK ». Cela fera apparaître une fenêtre vous permettant de modifier les paramètres.
3. Laisser les paramètres par défaut et cliquer sur le bouton « OK ».

Note: votre magasin de clés est maintenant créé. KeePass vous propose une structure de répertoire par défaut pour classer vos mots de passe. Ceux-ci peuvent être supprimés s'ils ne vous conviennent pas.

HEC MONTRÉAL

36

Guide d'utilisation de Keepass (7/9)

Ajouter un mot de passe dans votre magasin de clés.

1. Cliquer sur l'icône « ajouter une entrée ». Cela fera apparaître une fenêtre vous permettant de saisir l'information concernant votre nouvelle entrée.

2. Saisir le nom d'utilisateur et le mot de passe que vous voulez sauvegarder dans Keepass. Minimalement les champs suivants doivent être complétés : (Titre, nom d'utilisateur et mot de passe)

HEC MONTRÉAL

37

Guide d'utilisation de Keepass (8/9)

Installer le manuel d'utilisation en français pour une aide complète (1/2).

1. Télécharger le manuel d'utilisation à l'adresse suivante : (http://downloads.sourceforge.net/keepass/French-1.06-Manual.zip)
2. « Décompresser » ce fichier .ZIP dans le répertoire de KeePass. Une fenêtre apparaître vous demandant si vous voulez écraser le fichier KeePass.chm. Cela est normal, car le fichier original est une aide en « anglais ». Répondez de remplacer ce fichier par celui qui provient du fichier .ZIP.

HEC MONTRÉAL

38

Guide d'utilisation de Keepass (9/9)

Installer le manuel d'utilisation en français pour une aide complète (2/2).

1. Ouvrir le logiciel KeePass
2. Cliquer sur le menu « Aide »
3. Cliquer sur l'option « Source de l'Aide… ». Cela fera apparaître une fenêtre vous permettant de choisir votre source d'aide.
4. Sélectionner « Fichier d'aide locale ».
5. Cliquer sur le bouton « OK ». Vous pouvez maintenant appuyer en tout temps sur la touche « F1 » de votre clavier pour consulter l'aide.

HEC MONTRÉAL

Pour davantage d'information ou pour de l'assistance, demander au centre d'assistance technique.

Téléphone : 514 340-6063
Courriel : gti.info@hec.ca
Bureau : Comptoir au 3.820 (édifice 3000 ch. de la Côte-Ste-Catherine ascenseur sud 3e étage)

HEC MONTRÉAL