Les mots de passe : sentiment et réalité

Atelier LoLiGrUB du 18 février 2012 (animation : Didier Villers)

Emails, ordinateurs, connexion wifi, sites web, réseaux sociaux, banques en ligne,... autant d'applications qui demandent à vous authentifier, à indiquer un mot de passe. Mais que faire pour concilier la nécessaire sécurité de ces accès et les difficultés à mémoriser un grand nombre de codes parfois tarabiscottés ?

Un mot de passe, comment ça marche ?

Mot de passe bien connu de "Ali Baba et les 40 voleurs" : Sésame, ouvre-toi ! ... ce n'est pas très sûr, ce n'est plus un secret pour personne !

Un mot de passe :

- moyen d'authentification pour utiliser une ressource ou un service dont l'accès est limité et protégé.
- Authentification = identification + autorisation : l'identité est vérifiée
- Identification : l'identité est connue mais non vérifiée
- Les mots de passe sont à garder secret : par l'utilisateur, le fournisseur de service, et lors de la transmission !
- Références
  - http://fr.wikipedia.org/wiki/Mot_de_passe
  - http://en.wikipedia.org/wiki/Password

Quelqu'un connaît-il mon mot de passe ?

En pratique, dans la plupart des cas, les sites web, les fournisseurs de service chiffrent le mot de passe (*cf.* cryptographie)

Cela se fait à l'aide de fonctions de hachage : fonctions mathématiques non symétriques fournissant une valeur courte (par exemple 16 bytes ou 128 bits) à partir d'un "gros" fichier, ou simplement d'un mot de passe.

L'administrateur système de votre ordinateur, du fournisseur de service ne devraient jamais connaître les mots de passe. Ils peuvent éventuellement les réinitialiser. Méfiez vous des sites qui vous renvoie votre mot de passe actuel, cela veut dire qu'il est stocké "en clair" ! C'est acceptable pour des services peu sensibles comme des listes de diffusion ou des abonnements, mais il est important d'éviter l'utilisation de mêmes mots de passe que pour des utilisations plus sensibles.

Procédures en cas d'oubli du mot de passe. Réinitialisation via email. Attention aux questions secrètes !

Divulgation non désirée du mot de passe : chez l'utilisateur, chez le fournisseur de service, ou lors de la transmission.

Problèmes supplémentaires : s'il y a perte, on pourrait ne pas le savoir, ce qui peut avoir des conséquences pires : quelqu'un "lit dans votre dos" sans que vous le sachiez !

Les risques sont augmentés si d'autres personnes peuvent accéder physiquement à l'ordinateur.

C’est quoi, un mot de passe sûr ?

Une référence :
http://www.commentcamarche.net/faq/29818-choisir-securiser-et-gerer-ses-mots-de-passe

conseils de base :

- prendre des mots de passe long
- utiliser toutes les possibilités du clavier
- recourir à la mnémotechnique
- un mot de passe pour chaque compte d'utilisateur
- changer fréquemment de mots de passe

Pièges à éviter

- éviter les mots de passe qui utilisent des données d'identification trop évidentes
- éviter de divulguer des informations personnelles sur les réseaux sociaux
- éviter l'utilisation de chaînes de caractères linéaires : 123456, azertyuiop
- ne pas écrire ses mots de passe sur papier libre

Idéalement, un mot de passe est long, imprévisible (pas de mots “dictionnaires”), avec des chiffres, majuscules/minuscules et caractères spéciaux.

Utiliser des mots de passes différents suivants les risques, le type d’accès ou de données à protéger, la possibilité de devoir révéler le mot de passe,…

Si écriture sur papier, répartir plusieurs morceaux du code et d’autres non utilisés sur une grille et retenir un parcours de cases

Mon navigateur enregistre mes mots de passe. Est-ce bien sûr ?

Réponse : pas vraiment si on peut accéder à l'ordinateur !

Des programmes stockent les mots de passe “en clair” sur les ordinateurs :

- Firefox, si on ne prévoit pas une “clé globale” (cf. préférence - sécurité - mot de passe principal) et si on laisse le navigateur ouvert alors qu'on quitte son ordinateur
- client FTP Filezilla
- certains fichiers de configuration de certains serveurs, par exemple pour les accès des databases pour des CMS

Comment font les pirates pour obtenir les mots de passe ?

Risques : “vol” du mot de passe, ou attaques qui cherchent à découvrir le mot de passe.

- attaque dictionnaire
- attaque par force brute (combinatoire dans le nombre d'essai à faire suivant le nombre de caractères possibles)
- intrusion chez l’utilisateur
- intrusion chez le fournisseur de service

- écoute du réseau (sniffer)
- extorsion via un faux site intermédiaire (techniques "man in the middle")

Dictionnaires : une langue usuelle fait de l'ordre de 20 000 mots courants, 200 000 max. Pour un ordinateur c'est peu !

La force brute peut utiliser des ordinateurs en réseaux, les puces graphiques avec des algorithmes massivement parallèles. Spécialement pour des fichiers protégés par des mots de passes (pas de limite en nombre de tentatives)

Attention aux keylogger, au réseau wifi inconnu, spécialement en déplacement. Solution : caractères générés avec la souris, des copier/coller de caractères. Usage d'un VPN (sécurisant une partie de la transmission, pas son entièreté).

Des outils existent pour écouter le trafic réseau pour détecter des insécurités de texte en clair, dont des mots de passe (dsniff)

Comment faire pour ne pas perdre mes mots de passe ?

Malettes ou boites à mots de passe, elle-même chiffrées et protégées par un mot de passe (qui doit être très sûr).

Outils Intégrés à l'OS ou au gestionnaire de bureau (GNOME, KDE,...). Ne pas oublier de sauvegarder le fichier avant migration...

Logiciel spécifique indépendant : keepass (windows), keepassx (Linux, Windows, OS X)

Est-ce sûr d'écrire les mots de passe ? oui dans certains cas, si le vol n'intéresserait absolument pas les personnes à proximité du papier où c'est écrit ! Sinon, c'est évidemment dangereux, sauf utilisation de coffres-forts réels ou de grilles sur papier comportant des parties de mots de passe dans le désordre, pas tous utilisés.

Liens divers

Articles, billets :

- http://www.davidtan.org/how-to-manage-and-save-passwords/
- http://www.artduweb.com/linux/recovery-passwd (en cas de perte de mot de passe Linux !)

Programmes :

- http://www.openwall.com/john/ john the ripper (crack)
- http://www.artduweb.com/tutoriels/jtr (test de crackage de mot de passe)