Motivation

Ce document à pour but de préciser les limites de la sécurité apportée par les mots de passe et de sensibiliser les différents acteurs (utilisateurs, administrateurs, concepteurs d'applications) sur l'importance d'une politique complète et cohérente concernant l'utilisation et la gestion des mots de passe.

Définition d'un mot de passe fort

Un mot de passe fort est un mot de passe difficile à retrouver, même à l'aide d'outils automatisés. Il dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. Un mot de passe constituée de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir.

Les différentes attaques sur les mots de passe

• Attaques par force brute. Consiste à tester toutes les combinaisons possibles d'un mot de passe.

• Attaques par dictionnaire. Consiste à tester une série de mots issus d'un dictionnaire, disponibles sur internet et pouvant êtres utilisés pour cette attaque (dictionnaire des prénoms, des noms d'auteurs, marques commerciales, etc.)

• Attaques par compromis temps / mémoire. Solutions intermédiaires permettant de retrouver un mot de passe plus rapidement qu'avec une attaque par force brute et avec moins de mémoire qu'en utilisant une attaque par dictionnaire.

• Attaques indirectes. Consiste non pas à déterminer le mot de passe par une recherche mais à le capturer au moment où il est saisi, ou encore à se le faire communiquer en usant de supercherie. Face à ces attaques, la qualité du mot de passe doit être complétées par des mesures organisationnelles (sensibilisation des utilisateurs, etc.)

Créer un bon mot de passe

Un bon mot de passe est une mot de passe fort, difficile à retrouver mais facile à retenir pour l'utilisateur pour éviter que ce dernier n'ai recours à des moyens mettant en danger la sécurité (post-it, etc.). Pour ce faire il existe des moyens mnémotechniques pour fabriquer et retenir des mots de passe forts :

- Méthode phonétique. Consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. (ex : « j'ai acheté huit cd pour cent euros cet après-midi » → « ght8CD%E7am »)
- Méthode des premières lettres. Consiste à garder les premières lettres d'une phrase. (ex : « un tiens vaut mieux que deux tu l'auras » → « 1tvmQ2tl'A »)

Gestion des mots de passe

• Politique de gestion des mots de passe. Devra à la fois être technique et organisationnelle avec, entre autres :

- Sensibilisation à l'utilisation de mots de passe forts.
- Mot de passe initial fourni sur un canal sûr par l'administrateur du système et changé dès la première connexion.
- Renouvellement des mots de passe.
- Critères prédéfinis pour les mots de passe. (longueur minimal, etc.)

- Confidentialité du mot de passe en veillant à ne pas le divulguer, ni le partager, ni le stocker dans un fichier ou sur un papier.
- Configuration des logiciels. (ex : « Ne pas retenir le mot de passe »).

• Utilisation de mots de passe différents. Il est nécessaire de changer régulièrement son mot de passe et de ne pas utiliser le même mot de passe pour tous les services vers lesquels on se connecte.

• Utilisation de mots de passe non rejouables. Il est possible d'utiliser des solutions permettant de s'authentifier à un système par le biais d'un mot de passe ne pouvant être utilisé qu'une seule fois.

• Utilisation de certificats clients et serveurs.

• Mettre en place un contrôle systématique des mots de passe. Pour s'assurer de l'absence de mots de passe faibles, il peut être intéressant pour un administrateur de réaliser des tests sur la robustesse des mots de passe.