Qu’est-ce qu’un bon mot de passe ?



Un bon mot de passe est un mot de passe que seul vous connaissez.

Si vous vous mettez dans la peau d'un infâme pirate informatique, pour découvrir un mot de passe, **deux solutions sont préconisées** :

- **espionner la personne**, en regardant discrètement derrière son épaule lorsqu’elle le tape, par exemple.
- **le *bruteforce*** *:* c’est **essayer toutes les combinaisons à la suite jusqu’à trouver la bonne**, comme on ferait tourner les roues d’un cadenas une à une jusqu’à trouver la position de déverrouillage.

Pour éviter le *bruteforce*, il faut multiplier le nombre et le type de caractères du mot de passe.

Par exemple, si vous choisissez un mot de passe contenant deux lettres, alors le nombre de possibilités est de 26 pour la première, 26 pour la deuxième. Il faudra alors 26 * 26 essais pour être sûr de découvrir la bonne combinaison, soit 676 essais. Autrement dit, moins d’une seconde pour un ordinateur.

En utilisant majuscules, chiffres et caractères spéciaux, vous augmentez le nombre de caractères disponibles (aux alentours de 70). Nous sommes donc à 70 * 70, soit 4 900 essais.

À chaque caractère que vous ajoutez, vous multipliez le nombre d’essai à réaliser par le nombre de caractères disponibles, ici par 70. Donc un mot de passe à trois chiffres sera compris dans un ensemble de 70 * 70 * 70 essais, soit 343 000 .

Un mot de passe à 15 chiffres demandera 70^15 (70 puissance 15) essais, soit : 4.7475615e+27 essais. C’est pas mal !

Pour accélérer les recherches, **les pirates commencent en fait par les combinaisons les plus probables**, c’est-à-dire contenant des dates de naissances, des prénoms, des mots. **Utilisez si possible des suite aléatoires de frappes de clavier**, en mémorisant le mot de passe comme une comptine pour enfant, et en utilisant la mémoire musculaire plutôt que la mémoire des lettres.

Pour évitez l’espionnage, rappelez-vous qu’un mot de passe est personnel, il n’a pas vocation à être communiqué. Le temps de le mémoriser, vous pouvez le noter dans un carnet anodin, qui restera dissimulé.

Enfin, même si cela nécessite de mémoriser plus d'informations, **évitez d'utiliser deux fois le même mot de passe pour deux sites différents**. Si l'un des deux sites est attaqué, et que l'attaquant récupère votre mot de passe, il possède alors le mot de passe pour les deux sites.

Révision #1
Créé 2023-08-08 12:43:20 CEST par Rachelle
Mis à jour 2023-08-08 12:44:22 CEST par Rachelle