QU'EST-CE QUE LA « FORCE » D'UN MOT DE PASSE ?

Par abus de langage, on parle souvent de « force » d'un mot de passe pour désigner sa capacité à résister à une énumération de tous les mots de passe possibles.

Cette « force » dépend de la longueur L du mot de passe et du nombre N de caractères possibles. Elle suppose que le mot de passe est choisi de façon aléatoire. Elle se calcule aisément par la formule N^L. Mais il est plus difficile d'estimer si la valeur ainsi obtenue est suffisante ou pas.

COMMENT ESTIMER LA « FORCE » D'UN MOT DE PASSE ?

La force d'un mot de passe peut être estimée par comparaison avec les techniques cryptographiques. Une taille de clé cryptographique de 64 bits est aujourd'hui considérée comme non sûre car les capacités de calcul modernes permettent de retrouver cette clé en énumérant toutes les clés possibles. Or une telle clé peut être vue comme un mot de passe de 64 caractères où les seuls caractères possibles sont 0 et 1. La « force » d'un tel mot de passe est donc 2^{64}.

Les règles édictées par l'ANSSI en matière de mécanismes cryptographiques imposent par exemple une taille de clé minimale de 100 bits. Il est même recommandé une taille de clé de 128 bits pour des clés dont l'usage présumé est de longue durée. Il est par ailleurs communément admis que des tailles de clé de 80 bits sont désormais exposées à des attaques utilisant des moyens techniques conséquents.

Ces chiffres permettent de calibrer la « force » d'un mot de passe.

Taille de clé équivalente	Force d'un mot de passe
64	très faible
64<80	faible
80<100	moyen
> 100	fort

COMMENT RENFORCER MON MOT DE PASSE ?

Une question qui se pose fréquemment est : mais quels critères dois-je employer pour mes mots de passe ? Huit caractères, dix caractères, des chiffres, des majuscules, etc ?
Une première règle à savoir est qu'il est souvent plus efficace d'allonger un mot de passe que de chercher à le rendre plus complexe. Mais pour s'en rendre compte, le mieux est d'utiliser le petit calculateur ci-dessous :

Longueur : 10 caractères.

Alphabet : 62 symboles 0 à 9, A à Z et a à z

Calculer la force

Un mot de passe avec ces caractéristiques est à peu près équivalent à une clé de ? bits.

QUELQUES RÉSULTATS TYPIQUES

Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour des mots de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots de passe plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l'algorithme de chiffrement standard AES (128 bits).