COMBIEN DE TEMPS POUR PARCOURIR L'ENSEMBLE DES MOTS DE PASSE ?

1

Pour qu'un mot de passe soit difficile à trouver, il faut le choisir uniformément dans un grand espace de possibilités. Selon la longueur A de la liste de caractères autorisés pour le composer et selon le nombre N de symboles qui composent le mot de passe, la taille $T = A^N$ de cet espace varie considérablement. Voici cinq exemples.

Dans chacun des exemples, on précise A, N, T et le nombre D d'heures qu'il faut pour explorer l'espace des possibilités, suivi du nombre X d'années qu'il faudrait attendre, en supposant que la loi de Moore (« doublement de capacité de calcul tous les deux ans ») reste toujours valide, pour que cet espace devienne explorable en moins de une heure. On prend comme point de départ l'hypothèse qu'en 2018 votre machine explore un milliard de possibilités par seconde. On a donc :

$T = A^N$, $D = T/(10^9 \times 3\,600)$, $X = 2 \log_2[T/(10^9 \times 3\,600)]$.

$A = 26$, $N = 6$
$T = 308\,915\,776$
$D = 0{,}000\,085\,8$ heure de calcul
$X = 0$ année d'attente

$A = 26$, $N = 12$
$T = 9{,}5 \times 10^{16}$
$D = 26\,508$ heures de calcul
$X = 29$ années d'attente

$A = 100$, $N = 10$
$T = 10^{20}$
$D = 27\,777\,777$ heures de calcul
$X = 49$ années d'attente

$A = 100$, $N = 15$
$T = 10^{30}$
$D = 2{,}7 \times 10^{17}$ heures de calcul
$X = 115$ années d'attente

$A = 200$, $N = 20$
$T = 1{,}05 \times 10^{46}$
$D = 2{,}7 \times 10^{33}$ heures de calcul
$X = 222$ années d'attente

© Wutzkohphoto/Shutterstock.com

du nombre N de possibilités. Ce nombre est donné par la formule 1+partie entière($\log_2(N)$). Pour le premier exemple, la mesure donne 29 bits, et pour le second 75 bits. On parle aussi d'entropie de 29 bits, ou de 75 bits.

L'Agence nationale de la sécurité des systèmes d'information (Anssi) formule des conseils sur ces questions. Quand il s'agit des mots de passe ou de clés secrètes pour des systèmes de chiffrage dont on veut absolument assurer la sécurité, elle conseille de n'utiliser que des espaces de 100 bits au moins. Il est même recommandé une taille d'au moins 128 bits si l'on souhaite que la sécurité soit assurée pour plusieurs années. L'Anssi précise qu'il faut considérer comme très faibles les espaces de moins de 64 bits, comme faibles ceux entre 64 et 80 bits, comme moyens ceux entre 80 et 100. La différence entre la sécurité instantanée et la sécurité à long terme provient de la loi de Moore, selon laquelle la puissance de calcul d'un ordinateur d'un prix donné double tous les deux ans environ. Même si cette loi de Moore semble voir son rythme >