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 >

> diminuer, il est sage de la prendre en compte pour des mots de passe qu'on veut sécuriser durablement.

Pour un mot de passe vraiment robuste au sens de l'Anssi, il faudrait par exemple demander une suite de 16 caractères pris chacun dans un ensemble de 200 caractères. Cela ferait un espace de 123 bits.

Ce n'est guère envisageable, aussi les concepteurs de systèmes sont-ils moins exigeants et se contentent-ils d'espaces de mots de passe faibles ou moyens; ils n'appliquent l'exigence de clés longues que lorsque l'utilisateur n'a pas à la mémoriser lui-même, car elle est gérée automatiquement par le système.

D'autres procédés sont mis en œuvre pour empêcher l'exploration de l'espace des possibilités et casser les mots de passe. Le plus simple est bien connu et utilisé par les cartes bancaires: au bout de trois essais infructueux, la carte est bloquée. D'autres idées ont été proposées comme doubler les temps d'attente entre deux essais à chaque nouvelle erreur, sauf s'il s'est passé un long moment, 24 heures par exemple, auquel cas le système se remet à zéro.

Ces méthodes sont cependant inopérantes quand l'attaquant du système peut travailler hors ligne et mener des essais secrètement de manière isolée, ou que le système ne peut pas être configuré pour arrêter et freiner les essais infructueux.

Assez souvent, un attaquant réussit à se procurer le mot de passe chiffré ou l'empreinte du mot de passe (nous allons voir ce qu'est une empreinte) en accédant à des données du système qu'il attaque. Il peut alors, en toute tranquillité, pendant des jours entiers ou même des semaines, mener toutes les tentatives qu'il souhaite pour casser les mots de passe dont il s'est emparé sous forme chiffrée.

Avant d'expliquer les subtils procédés utilisés par de tels attaquants, revenons sur la taille de l'espace des possibilités.

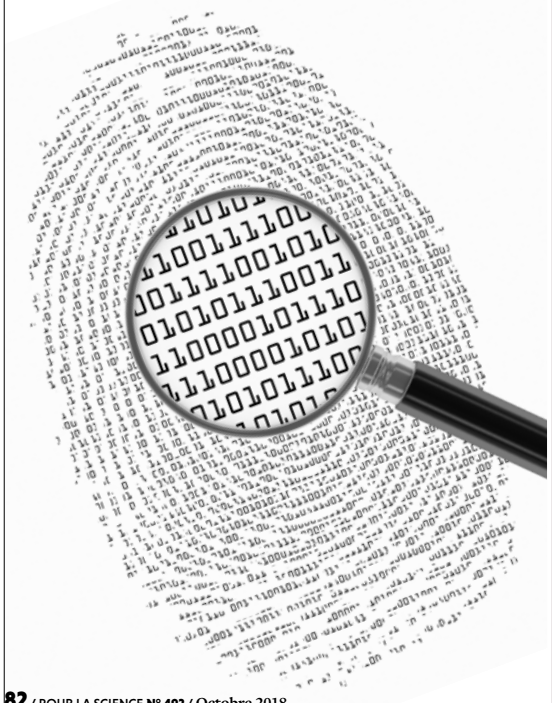
Quand nous avons évalué la taille en bits d'un espace de clés ou mots de passe, dénommée entropie, nous avons implicitement supposé que l'utilisateur choisit au hasard uniformément son mot de passe dans cet espace. Le plus souvent, ce n'est pas le cas, car pour mémoriser un mot de passe on préférera un mot courant, par exemple «locomotive», à un mot vraiment quelconque, par exemple «xdichqewax».

DES DICTIONNAIRES POUR ATTAQUER

C'est là un grave problème qui donne lieu aux attaques par dictionnaires. Des listes de mots de passe couramment utilisés ont été collectées et classées en fonction de la fréquence avec laquelle ces mots de passe sont utilisés. Un attaquant tentera des essais en prenant l'une de ces listes et en l'utilisant dans l'ordre.

2

LES PIRATES DÉÇUS PAR LES FONCTIONS DE HACHAGE



Les fonctions de hachage cryptographique sont des procédés soigneusement mis au point qui transforment un fichier informatique F, aussi long soit-il, en une suite *h*(F) de petite taille appelée empreinte de F. Par exemple, la fonction notée SHA256 transforme la phrase « Il fait beau » en :
316FF650DC5FFC6F8B9CFF25069942F4AA5088
78930A1410D81D5F1DD8C71077
(64 caractères hexadécimaux qui sont équivalents à 256 bits).

Changer un seul caractère du fichier change totalement son empreinte. Par exemple, pour « il fait beau », la fonction SHA256 donne l'empreinte :
D66D08EC93EBA6ACCDD552E2A38EBE6474285
E0D4F2370A87E206553E29AB93C.

Vous pouvez refaire et vérifier ces calculs à l'adresse :
https://passwordsgenerator.net/sha256-hash-generator/
ou https://www.xorbin.com/tools/sha256-hash-calculator.

Les bonnes fonctions de hachage produisent des résultats analogues à ceux qui seraient obtenus s'ils étaient tirés uniformément au hasard. Surtout, pour un résultat possible arbitraire (une suite de 64 caractères hexadécimaux), il est impossible de trouver en un temps raisonnable un fichier F ayant cette empreinte.

Il existe plusieurs générations de fonctions de hachage. Les générations SHA0 et SHA1 sont considérées comme obsolètes et déconseillées. La génération SHA2, à laquelle appartient SHA256, est considérée comme sûre.

Au lieu de mémoriser les mots de passe de leur client, les serveurs internet doivent mémoriser les empreintes de ces mots de passe. En cas d'intrusion, il sera alors impossible ou très difficile au pirate informatique d'exploiter ce qu'il trouve.