UQAC
Université du Québec
à Chicoutimi

Complément d'information technique :

Encodage des phrases de passe

Prenons la phrase TropSimple composée d'un mot de 4 lettres et 6 lettres. Donc facilement décodable avec un ordinateur de puissance moyenne.

Il existe plusieurs algorithmes de cryptage, mais pour fin d'exemple nous utiliserons le MD5, qui est une méthode de « hachage » de base. Une méthode telle le MD5 est une méthode ne possédant pas d'algorithme permettant de retrouver un mot à partir de sa version encodée.

Vérifions pour nos deux mots et notre phrase

Mot	MD5
Trop	8e8f3538a7a9cbc71f3d4af0265257da
trop	8b2495cd99bfa227d9c973cc0f3593fa
Simple	1fbb1e3943c2c6c560247ac8f9289780
simple	8dbdda48fb8748d6746f1965824e966a
TropSimple	4f556f553a48047221235327373f2c30
tropsimple	1a934838574a718ed9136d806da33ab4

En fait un « hash » MD5 est une signature. On peut voir que la signature de la phrase n'a aucune correspondance avec la signature des deux mots qui la compose et que même l'utilisation de majuscules change la signature.

Afin de trouver une signature, on peut utiliser la force brute qui consiste à générer des signatures jusqu'à trouver celle correspondant à celle de notre mot ou phrase. Donc, pour trouver le premier mot, on utilisera au maximum la combinaison de 4 caractères dont 26 lettres minuscules + 26 majuscules + 10 chiffres (oublions les caractères spéciaux…).

8 ou 10 caractères

un mot de passe de 8 lettres majuscules, minuscules et chiffre
nombre de différents symboles : 26 + 26 + 10
longueur du code : 8
combinaisons : 62 Exposant 8 = 218 340 105 584 896
longueur du code : 10
combinaisons : 62 Exposant 10 = 839 299 365 868 340 224

Si nous utilisons un processeur Intel Core I5 (1 134 418.21 kps) pour essayer de trouver la signature d'un mot de passe en utilisant les combinaisons de caractères possibles:

Trop	4 caractères	Moins de 2 secondes
TropF	5	34 secondes
TropFa	6	29 minutes
TropFac	7	1 journée et 1 heure
TropFaci	8	Presque 2 mois
TropFacil	9	7 ans 9 mois
TropFacile	10	4 siècles 3 ans 9 mois 2 semaines et 8 heures
PrTropFacile	12	726 millénaires 7 siècles 5 ans et 10 mois

Ce tableau n'est qu'une estimation et un processeur I5 est loin d'être le processeur le plus rapide, sans compter que certaines cartes graphiques possèdent plusieurs milliers de processeurs. C'est pourquoi un mot de passe de 8 caractères n'est plus jugé comme très sécuritaire, car si on peut diviser le « travail » de décodage par, disons 5000 nous pourrions décoder un mot de passe en quelques minutes (2 cartes graphiques GeForce GTX 1080 = 2560 x 2 – 5120 cores).

Kps : milliers d'opérations par seconde

Autres méthodes

Il existe d'autres méthodes pouvant être utilisées pour retrouver un mot à partir d'une signature. Une de ces méthodes est l'utilisation de « Rainbow tables » qui consiste en une liste de mots et leur signature correspondante. Ce sont des mots extraits de différents dictionnaires. C'est pourquoi l'utilisation d'un mot « commun » comme mot de passe n'est pas recommandée.

Même si ces tables contiennent des millions d'entrées, c'est une méthode beaucoup plus rapide que la force brute. Les fraudeurs misent sur le fait que beaucoup d'utilisateurs utilisent un mot du dictionnaire comme mot de passe.