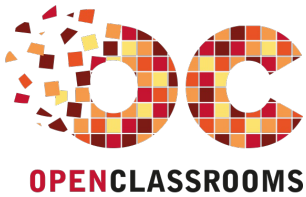
Sensibilisation sur le choix d'un mot de passe

Par Aerhus



www.openclassrooms.com

Licence Creative Commons 7 2.0
Dernière mise à jour le 2/11/2009

Sommaire

Sensibilisation sur le choix d'un mot de passe

Par  Aerhus

Mise à jour : 02/11/2009
Difficulté : Facile

(cc) BY-SA

Il existe un tas d'articles sur Internet qui traitent du choix d'un bon mot de passe. Ce qui m'a toujours gêné dans le contenu de ces articles, c'est le manque d'exemples. En effet, bien souvent, les auteurs se contentent de dire par exemple « il faut choisir un mot de passe d'au moins 8 lettres » sans dire pourquoi. Personnellement, ce type d'article ne m'a jamais fait changer mon mot de passe et je pense que c'est le cas de bon nombre de personnes.

De par ma curiosité, je me suis lancé dans un système de force brute. En étudiant les différentes façons de trouver un mot de passe, j'ai réellement été surpris de voir à quel point il peut être facile de trouver celui d'une personne.

Dans cet article, je vais principalement expliquer comment fonctionne la méthode par force brute afin de vous *sensibiliser* sur le choix de votre mot de passe.
Sommaire du tutoriel :

Méthode par force brute

J'ai choisi de présenter cette méthode car c'est principalement à cause de celle-ci qu'il faut choisir un bon mot de passe : je vais vous montrer à quel point il peut être facile de récupérer un mot de passe « simple ».
Une attaque par force brute consiste simplement à **essayer un ensemble de mots de passe** pour vérifier si l'un d'eux fonctionne. Il existe 3 types d'attaque par force brute :

- génération de tous les mots de passe possibles ;
- dictionnaire ;
- dictionnaire hybride.

Je vais vous les détailler, mais avant toute chose je vais vous présenter un pirate fictif qui se nomme *Bob Le Pirate* (ne me demandez pas pourquoi). Celui-ci va tester la méthode par force brute tout au long de l'article, et on commentera ses résultats.

Génération de tous les mots de passe possibles

Cette attaque consiste à générer tous les mots de passe possibles. Le générateur essaiera toutes les combinaisons possibles de l'alphabet en minuscules et en majuscules, qui peuvent aussi être combinées avec des chiffres (ou encore avec des caractères spéciaux tels que $ ou #). Théoriquement, aucun mot de passe ne pourrait rester caché face à ce type d'attaque car toutes les combinaisons seront essayées. En pratique, on rencontre un problème. D'ailleurs, Bob Le Pirate a fait des tests et nous a dressé un tableau. Voici donc quelques chiffres qui parlent d'eux-mêmes :

Quelques chiffres illustrant l'attaque par Force Brute

Type de caractère	Nombre de caractères	MDP à 4 caractères	MDP à 6 caractères	MDP à 8 caractères
L'alphabet minuscules (français)	26	456 976	~310 millions	~209 milliards
L'alphabet minuscules et chiffres	36	1 679 616	~2 milliards	~2800 milliards
L'alphabet minuscules, majuscules et	62	14 776 336	~57 milliards	~218 mille milliards

chiffres	62	14 770 330	~57 milliards	~218 mille milliards

Je pense que vous avez compris à quoi correspondent les 2 premières colonnes. Les 3 dernières colonnes quant à elles correspondent au nombre d'essais qu'il est possible de faire (le maximum). Le nombre d'essais augmente exponentiellement et donc devient vite énorme. C'est le point faible de cette attaque : elle peut devenir très très longue.

Pour essayer de trouver un mot de passe sur un ordinateur, cela peut prendre beaucoup de temps, voire trop de temps si le mot de passe est bien choisi (ça dépend de la puissance du processeur utilisé et de la connexion si l'attaque s'effectue à distance). Mais imaginez, pour lancer cette attaque sur un site web par exemple, en admettant que chaque tentative dure **0.2 secondes** (le temps de la connexion) et qu'on essaie de trouver un mot de passe à **6 caractères** ne contenant que des minuscules et des chiffres (**36 caractères possibles**), il faudrait environ **13 ans** pour essayer toutes les combinaisons possibles ! Et encore, là on sait que le mot de passe contient "juste" des minuscules et des chiffres et qu'il fait 6 caractères, mais si on ne sait pas… Il faut essayer minuscules, majuscules, chiffres, caractères spéciaux, le tout avec un nombre de caractères différent(s) (4 caractères, puis 5, puis 6, …).

Bref, c'est infernal et Bob Le Pirate ne s'en sort plus. C'est alors que notre pirate, qui ne manque pas d'idées, a trouvé un moyen pour diminuer considérablement le temps : le dictionnaire.

On retiendra que pour contrer ce type d'attaque, il y a 2 choses :

1. le mot de passe doit contenir un grand nombre de caractères (on conseille toujours au moins 8 caractères).
2. Il doit contenir plusieurs « types » de caractères (minuscules, majuscules, chiffres et caractères spéciaux).

Force brute par dictionnaire

L'attaque précédente consistait en une génération de tous les mots de passe possibles. L'attaque par dictionnaire va utiliser un dictionnaire de mots, c'est-à-dire un fichier qui contient beaucoup de mots tels que « mouchoir » ou « maxime ». Cela permet au pirate de n'essayer que des mots de passe qui ont un sens : eh oui, des études montrent que beaucoup de gens utilisent des mots communs pour leurs mots de passe.

Quand je parle de mots communs, je regroupe également les noms propres.

Citation : Burçin Gerçek

> Une autre étude, menée cette fois-ci par l'université de Hertfordshire en Grande Bretagne, donne des résultats inquiétants : 47 % des utilisateurs choisissent le prénom d'un membre de leur famille, le nom de leur animal ou leur date de naissance comme mot de passe. 32 % préfèrent les stars du showbiz, 11 % des mots à connotation sexuelle. Or, tous ces mots sont recensés par les logiciels de craquage. Un pirate les tentera en premier lieu pour s'introduire dans votre système informatique.
>
> source (au passage, c'est un article intéressant qui traite du même sujet)

Il y a donc de grandes chances pour que votre mot de passe (s'il s'agit d'un mot commun) soit recensé dans les dictionnaires des pirates.
À titre de comparaison, le *Petit Robert* contient environ 60 000 mots (et donc autant de tentatives). Cela vous donne une petite idée du temps gagné par rapport à l'ancienne méthode (pour le chiffre, il suffirait de **3 heures et 20 minutes** avec 0.2 secondes par tentative pour tester les **60 000 mots**).

Cependant, notre petit Bob s'est rendu compte qu'un certain nombre de mots de passe rajoutent des chiffres en plus (comme « maxime78 ») ou encore qu'ils associent plusieurs mots (par exemple « maximedu78 »). Pour pallier ce problème, il utilise une *attaque hybride*.

On ne va donc retenir qu'une chose pour cette attaque :

1. le mot de passe ne doit pas être un mot commun.

Force brute hybride

Ce type d'attaque n'est qu'une sorte d'amélioration de la précédente attaque. Elle va combiner plusieurs mots d'un dictionnaire ou encore ajouter des chiffres à celui-ci, ce qui permet de recouvrir un plus grand nombre de mots de passe potentiels. Pour reprendre l'exemple précédent, cela pourrait permettre de retrouver un mot de passe du type « maximedu78 ». Avec cette attaque, en supposant que notre Bob possède un excellent dictionnaire et que le mot de passe ne soit composé que de mots communs (avec des chiffres ou pas), même s'il doit mettre plus de temps, il finira par trouver le mot de passe.

Pas grand-chose à dire de plus sur cette attaque, donc :

1. Le mot de passe ne doit pas être composé que de mots communs (+chiffres).

Finalement, après avoir laissé tourner son ordinateur pendant 7 jours, Bob Le Pirate n'a pas réussi à trouver le mot de passe et il sait qu'il ne lui reste que 2 options : soit il attend des années en essayant absolument toutes les combinaisons possibles sur le site en question (premier type d'attaque qu'on a vu), soit il abandonne. Et comme c'est une *feignasse*, il abandonne.

(Il faut savoir qu'un pirate, s'il est assez fort, arrive toujours à ses fins mais cela peut prendre du temps et donc on essaie de lui barrer la route le plus possible pour qu'il finisse par abandonner.)

J'aimerais dire une dernière chose sur les chiffres donnés sur la durée de chaque attaque : ce n'est qu'à titre d'information. En effet, cela peut être largement variable (selon si l'attaque se fait par Internet ou pas). Il y a beaucoup de facteurs à prendre en compte. De plus, je pense qu'il est possible de diviser le temps en faisant plusieurs attaques à la fois qui vont tester différentes combinaisons chacune.

Conclusion

En récapitulant tout, il faut choisir votre mot de passe selon ces quatre règles :

1. le mot de passe doit contenir un grand nombre de caractères (on conseille toujours au moins 8 caractères).
2. *Il doit contenir plusieurs « types » de caractères (minuscules, majuscules, chiffres et caractères spéciaux).
3. Le mot de passe ne doit pas être un mot commun.
4. Le mot de passe ne doit pas être composé que de mots communs (+chiffres).

* Je le précise ici, ajouter des caractères spéciaux participe grandement à la sécurité : il en existe beaucoup (des « connus » comme +,"%&/ et des moins connus comme ¢©Ø¶ […]) et le pirate ne peut pas deviner lesquels vous avez pu utiliser, ce qui implique qu'il doit prendre en compte un nombre bien plus grand de caractères possibles… Bien évidemment, le problème qui se pose est l'accessibilité sur les différents types de clavier.

Voici un exemple de bon mot de passe : Qoaua,oaasb!. Ça fait peur hein ? Mais sachez que je n'ai pas écrit ce mot de passe par hasard, c'est tout simplement les premières lettres d'une phrase que je connais bien : Quand On Aime Un Arbre, On Aime Aussi Ses Branches !. Joli proverbe, vous ne trouvez pas ?
C'est donc un très bon moyen mnémotechnique pour avoir un mot de passe correct (le tout en remplaçant certains mots par des caractères spéciaux, comme le mot « et » par « & »).
Je vous donne un second exemple : 4gf/ki-2KL@[23](mot de passe repris du tutoriel d'ebola sur l'anti brute-force). Ce mot de passe est encore mieux : alternance entre chiffres, lettres (minuscules et majuscules) et caractères spéciaux. Cependant il est plus difficile à retenir. Vous pouvez facilement obtenir ce genre de mot de passe avec des générateurs de mot de passe (merci hyperion66).
Sinon, il existe beaucoup d'autres façons de créer un mot de passe complexe qui se retienne facilement ; allez lire les commentaires, certains membres nous livrent des méthodes intéressantes

Pour terminer, je vous donne quelques conseils qui n'ont pas de rapport direct avec le choix du mot de passe :

- Apprenez votre mot de passe par cœur (ne l'écrivez pas sur un post-it ou sur un fichier que vous conservez sur votre ordinateur), ça serait bête que quelqu'un le voie.
- Attention avec les caractères spéciaux. Si vous choisissez un caractère qui n'existe pas sur un clavier d'un autre pays et que vous vous retrouvez devant celui-ci, vous êtes mal ! (bien qu'il *peut* y avoir la présence d'une table de caractères selon le système sur lequel vous vous trouvez).
- Changer votre mot de passe de temps en temps est aussi une manière de vous protéger (tous les 2 jours, toutes les semaines ou encore tous les mois… C'est à vous de voir).
- Si vous pouvez choisir un mot de passe différent selon les sites, c'est aussi un plus (imaginez qu'un des sites sur lequel vous êtes se fasse pirater, hop le pirate peut accéder à votre compte sur tous les autres sites !);
- Certains sites proposent un identifiant différent du pseudonyme sous lequel tout le monde vous voit : profitez-en ! C'est un peu comme si vous aviez deux mots de passe, sauf que l'identifiant n'a pas besoin d'être aussi complexe que le mot de

passe.

Hum, attends là ! J'ai pas bronché jusque là, mais t'as pas l'impression d'en demander un peu trop là ? Le mot de passe compliqué, c'est déjà… compliqué à gérer.

Oui, tout ça c'est très contraignant. Mais vous n'êtes pas obligé de suivre à la lettre ce que je vous dis. Tout dépend de ce que vous devez protéger : si c'est un projet top-secret qui concerne la sécurité interplanétaire, alors il faudra effectivement être très vigilant (même si c'est contraignant), dans le cas contraire si le mot de passe ne protège « que » vos données personnelles et que vous n'êtes pas une personne connue mondialement, pas la peine de suivre toutes ces procédures (un bon mot de passe que vous connaissez par cœur suffit).
J'espère vous avoir fait comprendre grâce à cet article pourquoi il y a ces « règles » pour faire un bon mot de passe.

Toutefois, sachez que de nos jours les systèmes sur lesquels vous vous enregistrez sont plutôt sécurisés : au-delà de 3 tentatives de connexion, le système bloque l'utilisateur (ce qui évite l'attaque par force brute) ou encore tous les mots de passe ne sont pas acceptés (parfois, ils obligent à avoir au minimum 8 caractères). Mais par mesure de sécurité et parce que tous les systèmes ne sont pas protégés, mieux vaut éviter de prendre n'importe quel mot de passe.

Aujourd'hui, les mots de passe suffisent encore à protéger nos systèmes. Mais demain, qu'arrivera-t-il ? La puissance des ordinateurs augmente de jour en jour, ce qui rend la méthode par force brute plus rapide. La connexion elle aussi devient plus « puissante », avec les futurs câbles optiques qui permettent d'atteindre des taux de transfert énormes… Les mots de passe constitueront-ils toujours une sécurité suffisante ? Seul l'avenir nous le dira.

Je tiens à remercier les membres pour leurs critiques. Je n'ai pas ajouté les détails que les membres ont pu apporter à ce sujet afin de ne pas rendre l'article trop lourd. C'est pourquoi je vous invite, lecteurs, à aller lire les commentaires : les informations peuvent vous intéresser

Partager

Ce tutoriel a été corrigé par les zCorrecteurs.