

Intervention de M.Journault

# Atelier sur les mots de passe

Anthony Journault est expert en cryptologie à l'Agence Nationale de la Sécurité des Systèmes d'Information. Il a effectué sa scolarité dans les écoles, le collège et le lycée de La Châtre.

Un hacker cherche à déterminer le nombre de tentatives qu'il lui faudra pour deviner le mot de passe d'une victime.



1. « Pour se mettre en jambes »
  - (a) Imaginons que le mot de passe n'est constitué que de deux caractères (0 ou 1) et qu'il est de taille 2. Lister toutes les possibilités : .....
  - .....
  - (b) Maintenant, supposons que le mot de passe n'est constitué que de deux caractères (0 ou 1) et qu'il est de taille 3. Lister toutes les possibilités : .....
  - .....
  - (c) Calculer le nombre de mots de passe possibles, à deux caractères et de taille 8. ....
  - .....
2. Observons le nombre de mots de passe possibles lorsque nous changeons le nombre de caractère :
  - (a) Calculer le nombre de mots de passe possibles de taille 8 et dont les caractères peuvent être des lettres minuscules ou majuscules. ....
  - .....
  - (b) Calculer le nombre de mots de passe possibles de taille 8 et dont les caractères peuvent être des lettres minuscules, majuscules, des chiffres ou des caractères spéciaux (en tout 90). ....
  - .....
  - (c) Par combien faut-il multiplier pour passer de la réponse a) à la réponse b) ? .....
  - .....
3. Observons le nombre de mots de passe possibles lorsque nous changeons la taille :
  - (a) Rappeler le nombre de mots de passe possibles de taille 8 et dont les caractères peuvent être des lettres minuscules ou majuscules. ....
  - (b) Calculer le nombre de mots de passe possibles de taille 12 et dont les caractères peuvent être des lettres minuscules ou majuscules. ....
  - .....
  - (c) Par combien faut-il multiplier pour passer de la réponse a) à la réponse b) ? .....
  - .....

4. Quelle méthode a le plus d'impact par rapport à la sécurité d'un mot de passe? .....
- .....
5. Le hacker sait que le mot de passe de sa victime fait 8 caractères qui peuvent être des lettres minuscules, majuscules ou des chiffres.
- (a) Calculer le nombre de mots de passe possibles. ....
- .....
- (b) Une stratégie d'attaque naïve consiste à essayer tous les mots de passe possibles (brute-force). Quelle est la probabilité de trouver le mot de passe correct si on essaye des mots de passe au hasard? .....
- .....
- (c) Combien faudrait-il tester de mots de passe pour avoir une probabilité de succès d'au moins 50%? .....
- .....
- (d) Sachant qu'un attaquant peut tester 1 000 000 mots de passe par secondes, combien de temps lui faudrait-il pour être sûr de retrouver le mot de passe?.....
- .....
6. En pratique, une très faible proportion des mots de passe est utilisée. En effet, les utilisateurs utilisent très (très) souvent des mots de passe provenant de mots du dictionnaire. Il y a environ 30 000 mots de 8 lettres en français.
- (a) En combien de temps un attaquant testera cette liste? .....
- .....
- (b) Comparer par rapport à tester tous les mots de passe possibles. ....
- .....

**Conclusion**

*(quelques conseils)*

.....

.....

.....

.....

 La journée internationale du mot de passe est le 6 mai.