La sécurité commence par un bon mot de passe

La sécurité de tous dépend de la prudence de chacun.

La stratégie la plus fréquente des malveillants qui cherchent à prendre possession d'un système, consiste d'abord à usurper l'identité d'un utilisateur ; puis, dans un deuxième temps, à utiliser les failles connues du système pour devenir super administrateur sur une machine. Dans la plupart des systèmes, en particulier sous Windows NT et UNIX, lorsque le pirate a réussi la première étape d'usurpation, plus rien ne peut l'arrêter tant qu'il n'est pas détecté. Or, le système d'authentification par mot de passe, n'est efficace que dans la mesure où chacun a conscience que celui-ci constitue un secret précieux. La sécurité de tous repose sur la capacité de chacun à conserver consciencieusement cet important secret. Les trois lois fondamentales qu'il faut connaître et appliquer pour que ce secret ne tombe jamais entre des mains « qui ne vous veulent que du mal », sont à graver dans le marbre.

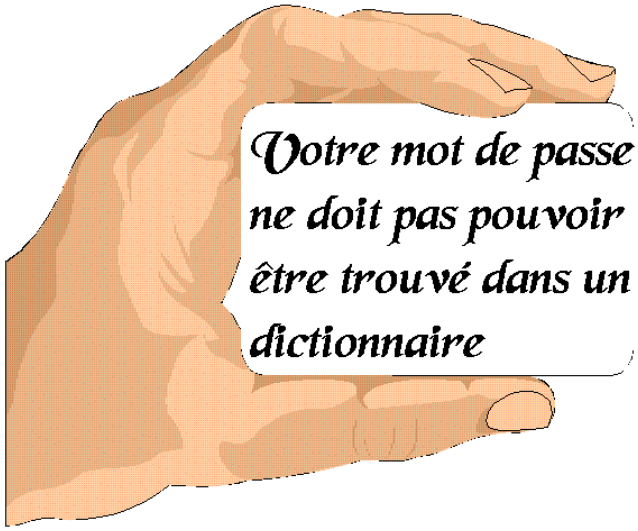
Un mot de passe :

1. **Solide tu le choisiras**
2. **Jamais tu ne le partageras**
3. **Souvent tu en changeras**

Un mot de passe solide :

Des techniques existent pour tenter de casser les mots de passe. La plus utilisée consiste à faire des essais systématiques à partir de dictionnaires : on connaît l'algorithme de codage des mots de passe, il suffit alors de l'appliquer à des dictionnaires choisis astucieuse-ment - sur internet, il y en a en de nombreuses langues - et de comparer le résultat à chacune des entrées du fichier système contenant les mots de passe, qu'on a réussi à extraire au préalable. Par cette technique, on arrive à casser en moyenne plus de 20% des mots de passe d'un fichier en moins d'une heure. La loi de composition d'un bon mot de passe doit rendre cette technique inefficace, d'où la règle suivante :

Règle 1 : Votre mot de passe ne doit pas pouvoir être trouvé dans un dictionnaire



Les deux autres techniques utilisées, consistent à essayer toutes les combinaisons possibles, soit sur un jeu réduit de caractères, soit en cherchant une chaîne de caractères de petite longueur. Pour faire échouer ces tentatives, il faut élargir au maximum le champ des combinaisons possibles, ce qui conduit à énoncer les deux règles suivantes :

Règle 2 : Votre mot de passe doit contenir un mélange de caractères alphanumériques et de caractères spéciaux (- + ! § %, ...),

Règle 3 : Votre mot de passe doit faire au moins 8 caractères
(sur les systèmes Unix, seuls les 8 premiers caractères sont pris en considération).

Il ne faut pas prêter son mot de passe

Un mot de passe est un secret entre vous et votre machine qui ne doit être partagé par personne d'autre. Si vous le confiez à quelqu'un, même à votre étudiant, à votre ami ou encore à un proche, ce n'est plus un secret et le mot de passe ne joue plus son rôle d'authentifiant. Vous mettez en échec la sécurité du système dans son fondement ; dès lors, toutes les mesures que vous pourriez prendre par ailleurs, ne servent plus à rien. Il ne faut pas non plus écrire votre mot de passe sur un support, à proximité de la machine ou de manière qu'un rapprochement puisse être fait avec le système qu'il est censé protéger. Les « stickers » sous le clavier ou le tapis de la souris, ne sont pas une bonne idée !

Il faut changer régulièrement le mot de passe :

Les mots de passe circulent en clair sur les réseaux. Des techniques simples (sniffers, espions, chevaux de Troie ...), peuvent être mises en œuvre pour capter le couple (identifiant, mot de passe) à l'insu des utilisateurs et administrateurs. Ces dispositifs peuvent rester en place pendant des mois avant d'être découverts. Pendant ce temps, tapis à l'écoute du réseau, ils captent tous les mots de passe qui circulent. C'est pourquoi, même robuste, un mot de passe doit être modifié régulièrement - au moins tous les trois mois. Mais cette exigence pose un problème de mémorisation, qui devient insurmontable lorsqu'on a plusieurs mots de passe à se rappeler et qu'on applique scrupuleusement les règles ci-dessus. C'est pourquoi un mot de passe ne peut être un pur aléa. Il faut avoir une règle de constitution mnémotechnique. Je vous en proposerais deux, à vous d'en trouver d'autres si le cœur vous en dit.

1°) Méthode poétique :

Elle consiste à apprendre un vers par cœur et à constituer le mot de passe en prenant un caractère de chaque mot. Exemple : « ***Tant va la cruche à l'eau qu'à la fin elle se casse*** ». Pour chaque mot du vers qui possède plus de trois caractères, je prends le premier caractère. Les autres mots sont ignorés. J'alterne 1 minuscule, une virgule, 2 majuscules, un point-virgule, 2 minuscules, 1 majuscule, pour que la chaîne fasse 8 caractères. **Résultat : t,CE;feC**.

Certes, la méthode peut paraître compliquée au premier abord, mais, avec un peu d'habitude on s'y fait très bien. Une version simplifiée, consistant à ne prendre que les premiers caractères de chaque mot du vers, est souvent utilisée. Mais le résultat est considéré comme faible, dès lors que l'attaquant connaît votre méthode de mémorisation.

2°) Méthode par substitution :

J'apprends par cœur une chaîne **{C}** de caractères spéciaux. Par exemple : **{* + $ / ? £}.** Je prends un mot ou un nom que je peux retenir facilement. Par exemple : Robert. Je remplace les voyelles par les caractères successifs de la chaîne **{C}**. Je mets une majuscule à chaque bout du mot et je le complète, si nécessaire, à 8 caractères avec le reste de la chaîne **{C}**. **Résultat : R*b+rT$/**. Quand je change mon mot de passe, je ne change que la « graine » (ici Robert) et je garde toujours la même chaîne **{C}** que je mémorise définitivement. Personnellement, cette méthode me plaît plus que la précédente. Avec un peu d'entraînement, l'opération de composition du mot de passe se fait facilement mentalement. Les mots obtenus sont aussi très robustes.

Si l'une de ces deux méthodes vous convient, servez-vous, il n'y a pas de droits d'auteur. Sinon, à vous d'en trouver une autre. Mais dans tous les cas, rappelez-vous que « **la sécurité** » ne vous appartient pas, vous la partagez avec l'ensemble de la communauté scientifique. Si vous êtes laxiste dans ce domaine ou si, simplement « vous vous laissez aller », vous portez tort à tous vos collègues, y compris à ceux qui acceptent - eux ! - de faire les efforts nécessaires.