Kalimèra / il y a dix sept années
Les mots de passe
Les mots de passe

La sécurité commence par de bons mots de passe, de plus en plus de nombreux services demandent un mot de passe. Quelques règles permettent de sécuriser un mot de passe par un bon choix.

La stratégie la plus fréquente des malveillants qui cherchent à prendre possession d $-1òùun système, consiste d $-1òùabord à usurper l $-1òùidentité d $-1òùun 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 $-1òùusurpation, plus rien ne peut lòùarrêter tant qu $-1òùil nòùest pas détecté. Or, le système d $-1òùauthentification par mot de passe, nòùest 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 $-1òùil 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 il sera
2. Personnel il sera
3. Souvent il changera

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 $-1òùalgorithme de codage des mots de passe, il suffit alors de lòùappliquer 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 $-1òùon a réussi à extraire au préalable. Par cette technique, on arrive à casser en moyenne plus de 20% des mots de passe d $-1òùun fichier en moins dòùune heure. La loi de composition dòùun bon mot de passe doit rendre cette technique inefficace, dòùoù la règle suivante :

Règle 1 : Un 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 $-1òùautre. Si vous le confiez à quelqu $-1òùun, même à votre étudiant, à votre ami ou encore à un proche, ce n $-1òùest plus un secret et le mot de passe ne joue plus son rôle d $-1òùauthentifiant. 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 $-1òùun rapprochement puisse être fait avec le système qu $-1òùil 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 oeuvre pour capter le couple (identifiant, mot de passe) à l $-1òùinsu des utilisateurs et administrateurs. Ces dispositifs peuvent rester en place pendant des mois avant dòùêtre découverts. Pendant ce temps, tapis à l $-1òùécoute du réseau, ils captent tous les mots de passe qui circulent.
C $-1òùest 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 $-1òùon a plusieurs mots de passe à se rappeler et qu $-1òùon applique scrupuleusement les règles ci-dessus. C $-1òùest pourquoi un mot de passe ne peut être un pur aléa. Il faut avoir une règle de constitution mnémotechnique. En voilà deux, à vous d $-1òùen trouver dòùautres si le coeur vous en dit.

1°) Méthode poétique :
Elle consiste à apprendre un vers par coeur et à constituer le mot de passe en prenant un caractère de chaque mot.
Exemple : « Tant va la cruche à l $-1òùeau quòùà 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 $-1òùalterne 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 $-1òùhabitude on sòùy 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 $-1òùattaquant connaît votre méthode de mémorisation.

2°) Méthode par substitution :
J $-1òùapprends par coeur 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 $-1òùentraînement, l $-1òùopération de composition du mot de passe se fait facilement mentalement. Les mots obtenus sont aussi très robustes.
Si l $-1òùune de ces deux méthodes vous convient, servez-vous, il n $-1òùy a pas de droits dòùauteur. Sinon, à vous d $-1òùen trouver une autre.

Kalimèra / il y a dix sept années

Re: Les mots de passe
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

© texte Copyright [illegible]

Lepigeon / il y a dix sept années

Re: Les mots de passe

Quelques précisions...

> Citation
> **Kalimèra**
> Les mots de passe
> 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).

C'était vrai sur les anciens systèmes. Les systèmes d'identification actuels en général ne souffrent plus de cette limitation.

> Citation
> **Kalimèra**
> Les mots de passe
> 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 oeuvre pour capter le couple (identifiant, mot de passe) à l $-1òùinsu des utilisateurs et administrateurs. Ces dispositifs peuvent rester en place pendant des mois avant dòùêtre découverts. Pendant ce temps, tapis à l $-1òùécoute du réseau, ils captent tous les mots de passe qui circulent.

S'il est vrai que beaucoup de mots de passe circulent en clair sur le net, de plus en plus, les transactions sont cryptées (ssh, ssl, tls,...), rendant la technique du sniffing moins efficace pour un cracker. Néanmoins, il y a encore 5 ans, c'était une approche facile et très efficace pour peu qu'on avait un accès sur une machine interne au réseau. Le courrier électronique est souvent non crypté, ce qui représentent une grosse faiblesse potentielle.