MANUEL MOTS-DE-PASSES-SÉCURISÉS

Version 1.0 FR Frédéric Jadoul

un manuel par

Moving Art Studio a.s.b.l.

Table of Contents

Mots de passe sécurisés

Un mot de passe sûr à 100% n'existe pas. Tous les mots de passe connaissent un degré de fiabilité plus ou moins élevé en rapport avec les précautions prises par leur auteur.

En pratique

Les personnes ont tendance à oublier les choses facilement lorsqu'elles ne sont pas directement connectées à leur réalité immédiate. C'est peut-être la raison pour laquelle il y a autant de gens qui emploient des mots de passe aisément identifiables pour sécuriser des données qui ne sont pas supposées être vues, sues ou utilisées par d'autres. Les considérations qui suivent s'appliquent à toutes les utilisations du mot de passe, peut importe qu'il s'agisse d'accéder à du texte dans un carnet secret, du login pour se connecter à un forum de discussion ou à un compte Unix, d'ouvrir votre machine Windows 2000 au bureau ou de transferer de l'agent depuis votre compte en banque.

Dans tous les cas, les mots de passe sont employés pour permettre l'accès à l'information aux personnes autorisées et tenir les personnes non autorisées à distance. Si votre mot de passe est utilisé à votre insu, les domages peuvent être sans limite : pertes financières, pertes de données, pertes en termes d'image de marque, etc...

Attaques du type “dictionnaire”

Tous les mots dont la liste a été dressée dans un dictionnaire sont à risques, peu importe la langue que vous employez. Il est certain que les mots d'origine anglaise ou de la langue maternelle de la victime (si elle est connue) sont plus menacés que, par exemple, des mots en Somali. Sur internet, vous pouvez trouver des dictionnaires assez spécialisés pour fournir des mots de passe à une application qui va tenter par la méthode de la “force-brute” de tester les mots de passe les uns après les autres.

Quoiqu'on puisse obtenir un degré plus élevé de sécurité en alternant les majuscules avec les minuscules (lorsqu'il est possible de changer de case), cela ne représente pas vraiment un handicape pour ce type d'attaque. en fin de compte, même “paRAPluiE” peut être découvert moyennant un nombre d'essais suffisants dans le temps.

Un dictionnaire anglais comprend à peu près 150.000 mots. Si vous ajoutez les variations de case, vous arrivez à quelque chose comme 15 millions de mots. Mais seules quelques secondes peuvent être nécessaires pour découvrir le mot de passe par la méthode “force-brute”.

En 2002, une liste de 10.000 comptes sur un serveur existant a été analysée. Après seulement 30 minutes, 30% des mots de passe étaient découverts (voir Passwords: the weakest link?).

Données personnelles

Trés prisée quoique tout aussi peu fiable est l'utilisation de données personnelles en tant que mots de passe : noms, prénoms, date d'anniversaire, numéros de téléphone, personnages de films ou de livres, passe-temps ou passions d'un utilisateur, de ses collègues, des membres de sa famille, etc... Encore plus que les mots tirés d'un dictionnaire, ces mots font sens et sont devinés plus ou moins facilement.

Dans une étude menée en 2001 auprès de1200 employés anglais, il a été établi que près de la moitié

des personnes interviewées avaient employé leurs noms, noms de leurs animaux familiés ou noms de membres de leur famille comme mots de passe. D'autres utilisaient des noms tirés de fiction célèbres comme Darth Vader ou Homer Simpson (voir Homeland Insecurity).

Chaînes de caractères

Autres mots de passe très fréquement utilisés, les chaînes de caractères du type “azerty”, "qwerty" ou "12345" qui sont très facilement tapées. Ces mots de passe sont tout aussi peu fiables car ils sont très connus (il existe même des dictionnaires qui ne comportent que ce type d'enchaînements de caractères).

Les attaques en “force-brute”

Les ordinateurs actuels sont très puissants. En ce moment, des systèmes facilement abordables sont capables de tester plus de 10 millions de clés en une seconde pour cracker, par exemple, l'algoritme d'encodage RC5 (qui est pourtant réputé fiable). Si l'on confronte ce chiffre avec des mots de passe d'une longueur de 6 caractères (incluant des majuscules et des minuscules), vous pouvez aisément calculer le temps que cela prend pour découvrir un mot de passe par la méthode dite de “force-brute” :

52 caractères possibles élevés à la puissance 6 (longueur du mot de passe) = about 20 millards de combinaisons
20 millards / 10 millions = 2.000 secondes = à peu près une demi-heure.

Deux conséquences dérivent de ce simple calcul :

- les mots de passe courts ne sont pas fiables
- les mots de passes tirés d'un nombre restreint de caractères (juste des chiffres ou juste des minuscules) sont plus fragiles que ceux tirés d'un éventail de caractères plus large (chiffres, majuscules, minuscules, caractères spéciaux).

Conclusion

Récapitulons. Les mots de passe doivent comporter les attibuts suivants pour offrir un taux de sécurité relativement acceptable :

- Les mots de passe doivent être longs (au moins 8 caractères)
- Les mots de passe doivent contenir une combinaison de lettres/chiffres/caractères spéciaux
- Les mots de passe ne doivent pas faire sens

Les méthodes suivantes vous aideront à trouver des mots de passe avec un taux de sécurité adéquat dont vous pourrez vous souvenir plus facilement qu'une suite aléatoire de caractères :

- Joindre deux mots (en mélangeant minuscules et majuscules) par un caractère spécial (exemple : "4aT&hOme", "b1G#seCreT", "zEIt+f0rM")
- Les premières lettres d'une phrase en conjonction avec des caractères spéciaux et des nombres
  (exemple : "Spau2rP!" pour "Some people are unable to remember passwords!")
- Des mots sans signification qui sont constitués de syllables articulables combinées à des caractères spéciaux et des chiffres

(exemple : "dOsil?Ar0n")

 N'employez pas ces exemples, trouvez vous-même votre mot de passe!

Pourquoi mêmes ces précautions ne sont pas suffisantes

Les mots de passe compliqués sont plus difficiles à retenir que les simples. Même s'il est tentant de les noter et de les conserver dans son porte-feuille ou de les coller sous l'écran, il vaut mieux ne les tenir enregistrés que dans votre mémoire. Même si vous avez choisi votre mot de passe précautioneusement, les autres s'épargeront beaucoup d'efforts s'ils peuvent simplement le lire sur un mot accroché à votre écran et beaucoup d'ennuis peuvent être ainsi évités si jamais votre porte-feuille se retrouve par hasard entre les mains de quelqu'un d'inconnu qui détient des informations à propos des moyens d'accès aux données de votre société.

Un autre bon moyen de disséminer son mot de passe est d'employer toujours le même pour sécuriser des comptes différents. Si le gestionnaire d'un site de discussion connaît votre mot de passe, il peut espérer (pour peu qu'il soit suffisament mal intentionné) que vous employez également le même mot de passe pour vous connecter sur le réseau de votre société. C'est pourquoi les mots de passe ne doivent être employés qu'une seule fois et être changés fréquement.

Notez aussi que les mots de passe sont parfois envoyés de manière non protégée via internet ou sur le réseau interne de votre société. Ils voyagent alors en claire et peuvent être interceptés tout au long de la ligne de communication. N'employez jamais ces mots de passe deux fois !

En la matière, il est vivement conseillé de ne faire confiance à personne. Ne confiez donc pas non plus votre mot de passe à un ami au cas où vous l'oublieriez ou pour partager l'accès à certaines données.

Versions

Version number	Modifications	Author
1.0 NL	Original version	Frédéric Jadoul
1.0 FR	Traduction	Frédéric Jadoul
1.0 FR	Conversion sxw => odt	Patrick Brunswyck
1.0 EN	Translation pdf NL-> odt EN	Patrick Brunswyck

page	**Modifications**
first	Added Cover all2all GNU Free Documentation License
last	Versions and Modifications
4	Warning sign in table