Nycom
Informatique
Rue St-Jean 20 - 1260 Nyon
Tél. 022 / 362 59 54
Fax 022 / 362 60 45
www.nycom-informatique.ch

1991 25 2016

La problématique des mots de passe

Moyen simple d'authentifier l'utilisateur, les mots de passe sont devenus omniprésents. Conséquence négative : il est nécessaire d'en retenir un nombre toujours croissant. Comment se souvenir de mots de passe toujours plus nombreux ? Comment concilier la confidentialité, l'unicité, la complexité, la longueur et la fréquence de renouvellement de ses mots de passe ? La solution existe et c'est ce que nous allons voir ensemble.

Qualité des mots de passe

En premier lieu, qu'est-ce qu'un bon mot de passe ? Un mot de passe est fiable lorsqu'il tient compte des contraintes de sécurité suivantes :

- longueur (nombre de caractères élevé)
- diversité dans les caractères (minuscules, majuscules, chiffres et caractères spéciaux)
- unicité (un mot de passe ne sert qu'une fois)
- confidentialité (un mot de passe est personnel : il n'est jamais communiqué à des tiers)
- renouvellement fréquent du mot de passe (bonne pratique)
- absent des dictionnaires (ce n'est pas un mot ayant sens dans une langue)

Pourquoi ? Car si ces contraintes sont réunies dans un mot de passe, il est dit "robuste" : on ne peut pas le deviner ou le casser facilement.

En effet, un nombre de caractères élevé, allié à la diversité des caractères employés et l'absence des dictionnaires garantit un allongement de la durée nécessaire à la découverte du mot de passe par une attaque consistant à tester toutes les possibilités une à une (attaque par force brute).

En outre, l'unicité, tout comme la fréquence de renouvellement, permettent de prévenir les risques relatifs à un vol de base de données (par exemple la base de données d'un serveur internet) contenant le mot de passe. En effet, le mot de passe découvert ne sert alors qu'à un usage unique et/ou n'est plus valable au moment d'être exploité par l'attaquant ou une tierce partie. Garder un mot de passe pour soi permet aussi de réduire les risques : n'est digne de confiance que la personne à l'origine du mot de passe.

Premier constat : toutes ces contraintes sont opposées à la mémorisation. Retenir des mots de passe longs, complexes, jamais utilisés plus d'une fois, non partagés, continuellement renouvelés et n'ayant pas de signification particulière peut s'avérer ardu. Si le nombre de mots de passe devient important rapidement, la tâche tient de l'impossible.

La réaction habituelle consiste à choisir et réutiliser un mot de passe simple (car facilement mémorisable), ou à créer des variantes basées sur un mot de passe unique, ce qui n'est bien entendu absolument pas sûr. Cette problématique a donc naturellement donné naissance à la nécessité de trouver une solution.

Les gestionnaires de mots de passe

Les gestionnaires de mots de passe sont de simples programmes (gratuits ou payants) dont le but consiste à décharger l'utilisateur des contraintes de gestion des mots de passe. Certains logiciels antivirus proposent également des fonctions de gestion de mots de passe, par exemple BitDefender ou Kaspersky. Il en existe un nombre important, quelques exemples tirés d'internet :

- keepass
- 1password
- keeper
- lastpass
- roboform
- password safe
- pins
- sticky password
- efficient password manager
- ipassman
- clipperz
- anypassword
- …

Keepass

L'un des plus réputés se nomme keepass et permet de tenir compte de toutes les contraintes de sécurité. Si vous disposez d'un nombre important de mots de passe, ce logiciel changera grandement votre quotidien numérique.

Keepass offre les avantages suivants :

- multiplateforme (Windows, Mac OS, Linux, Android et IOS)
- multilingue (fichiers de langues téléchargeables)
- mémorisation d'un unique mot de passe (ouverture de la base de données)
- possibilité de ne plus jamais utiliser un mot de passe à double (unicité)
- planification des échéances (renouvellement)
- sécurité en cas de vol (chiffrement AES : meilleure méthode de cryptage symétrique connue à ce jour)
- possibilité de partager la base de données sur différents terminaux (ordinateur, tablettes et smartphones)
- évaluation de la robustesse des mots de passe
- génération automatique de mots de passe selon des critères personnalisables (taille, complexité, etc…)
- mesures réduisant l'efficacité des attaques par force brute
- certification pour usage bancaire
- gestion des mots de passe à usage unique (TAN [Transaction Authentication Numbers])

Presque tout est parfait avec un bon gestionnaire de mots de passe. Cependant, quelques inconvénients demeurent :

- il est toujours nécessaire de retenir un mot de passe (ouverture de la base de données)
- la perte/corruption du fichier de base de données entraine la perte de toutes les données
- vulnérabilité au *shoulder surfing* (vue par-dessus l'épaule de l'utilisateur)
- vulnérabilité aux *keyloggers* (enregistrement de la frappe au clavier)

Situation obtenue

Un gestionnaire de mots de passe permet donc d'obtenir la situation idéale suivante : en ne retenant qu'un seul mot de passe, il est possible de disposer de mots de passe robustes et uniques sans avoir à les mémoriser, lesquels sont accessibles sur tous les périphériques et renouvelés régulièrement. Il s'agit là de la meilleure réponse à la problématique de gestion des mots de passe.