République Tunisienne

Ministère des Technologies de la Communication

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Bien choisir un mot de passe

Public Cible	Date de Publication	Date de Révision	Version
Simple Utilisateur	Mai 2008	Mai 2009	02

Introduction

Qu'est ce qu'un mot de passe ?

Un mot de passe (en anglais password) est l'une des plus anciennes techniques de sécurité. Par exemple, pour accéder à un système informatique, un identifiant unique (login ou username) et un mot de passe vous sont, en général, demandés. Ceci permettrait de s'assurer de votre identité et vous permettrait d'accéder au système. Cette technique reste toujours fortement utilisée pour l'authentification et est considérée comme sûre à condition que certaines règles fondamentales soient respectées.

On peut distinguer :

- Des mots de passe relatifs à l'utilisation d'Internet : mot de passe de connexion, mot de passe de messagerie (mail ou MSN), mot de passe d'accès à des forums, à son compte bancaire, etc.
- Des mots de passe relatifs à l'utilisation de son système : mot de passe d'accès à la session d'utilisateur.

Quelles sont les attaques possibles ?

Attaque par force brute (brute force cracking):

Cette méthode consiste à deviner un mot de passe en testant tous les mots de passe possibles. Plusieurs outils permettent de réaliser ce type d'attaque et ce, pour chaque système d'exploitation. De tels outils ont pour première vocation de permettre aux administrateurs de tester la robustesse des mots de passe de leurs utilisateurs. Seulement, certains pirates informatiques les utilisent pour s'introduire illicitement dans les systèmes informatiques d'autrui.

- **Attaque par dictionnaire:**

La plupart du temps les utilisateurs choisissent des mots de passe significatifs de peur de les oublier. Ceci constitue une aubaine pour les pirates informatiques qui essaient donc toutes les combinaisons de mots significatifs, d'où le nom "Attaque par

dictionnaire". Ainsi, un pirate peut deviner un tel mot de passe en seulement quelques minutes.

- **Attaque hybride:**

Cette attaque est une combinaison d'attaque par force brute et d'attaque par dictionnaire qui permet au pirate de retrouver les mots de passe constitués d'un nom significatif suivi d'une lettre ou d'un chiffre.

- **Autres attaques**

- Les key loggers : permettent d'enregistrer tout ce que l'utilisateur saisit sur son clavier.
- L'ingénierie sociale: consiste à obtenir le mot de passe d'un individu en abusant de sa naïveté par exemple, en se faisant passer pour un administrateur réseau ou bien en appelant l'équipe de support pour leur demander de réinitialiser en urgence le mot de passe.
- L'espionnage: est la méthode la plus rudimentaire pour deviner le mot de passe de quelqu'un, il suffit de regarder discrètement au dessus de son épaule ou en fouillant dans certains papiers sur son bureau.

Comment choisir un bon mot de passe ?

Voici quelques règles d'or pour obtenir un mot de passe fort :

- Créez un mot de passe sûr dont vous pourrez vous souvenir sans devoir le noter quelque part,

- Un mot de passe ne doit pas pouvoir être trouvé dans un dictionnaire (anglais, français et espagnol),

- Composez un mot de passe d'au moins 8 caractères. En fait plus un mot de passe est long, plus il est difficile à deviner.

- Choisissez une combinaison de minuscules et majuscules, de chiffres, de lettres et de caractères spéciaux (¬+ ! § %, ...).

Exemple illustratif :

Si nous prenons le mot "asselema" (ce qui veut dire salut en arabe), il s'agit d'un mot de 8 lettres facile à retenir et qui n'existe dans aucun dictionnaire. Seulement, tel que présenté, il ne constitue pas un mot de passe fort car il ne contient aucun chiffre, aucune majuscule et aucun caractère spécial. Seulement, avec quelques manipulations, nous pourrons aboutir à un mot de passe plus robuste:

- ajouter des chiffres : par exemple, en ajoutant un "3" en tête de mot et en remplaçant le "s" par un "5", nous obtenons au mot "3a55elema",

- ajouter des majuscules : aussi, en remplaçant certaines lettres minuscules en majuscules, nous pourrons obtenir le mot "3a55eleMA",

- ajouter des caractères spéciaux : enfin, nous pouvons remplacer le "l" par un point d'exclamation "!" et le "a" par "@" ce qui permettrait d'aboutir à un bon mot de passe : "3@55e!eMA".

Quelles sont les bonnes manières pour gérer votre mot de passe ?

- Ne divulguez jamais votre mot de passe et surtout pas en l'envoyant par courrier électronique.

- Évitez de noter votre mot de passe quelque part ou de le laisser exposé (sur écran, sous le clavier, dans un fichier non protégé, ...)

- Changez votre mot de passe sur incident ou bien périodiquement (au moins tout les trois mois),

- Choisir plusieurs mots de passe par catégorie d'usage (par exemple, le mot de passe de votre carte bancaire ne doit pas être le même que pour votre compte mail).