Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . N
Direction centrale de la sécurité des systèmes d'information
CERTA

Paris, le 12 avril 2007
N° CERTA-2005-INF-001

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Les mots de passe

Conditions d'utilisation de ce document : `http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document : `http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001`

Gestion du document

Référence	CERTA-2005-INF-001
Titre	Les mots de passe
Date de la première version	15 mars 2005
Date de la dernière version	12 avril 2007

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Introduction

L'utilisation de mots de passe forts est l'une des briques de base dans la sécurisation d'un système d'information. Malheureusement cette première étape est souvent absente dans la politique de sécurité. Il est par conséquent assez fréquent de trouver des comptes avec des mots de passe triviaux, sans mot de passe ou avec des mots de passe par défaut. Cette note a pour but :

- de sensibiliser les utilisateurs de système d'information sur l'intérêt d'avoir des mots de passe forts ;
- de sensibiliser les administrateurs sur l'intérêt de mettre en place un contrôle systématique de la qualité des mots de passe ;
- de sensibiliser les concepteurs d'application sur l'importance d'une politique complète et cohérente concernant l'utilisation et la gestion des mots de passe.
- de préciser les limites de la sécurité apportée par les mots de passe.

2 Définition d'un mot de passe fort

Un mot de passe fort est un mot de passe qui est difficile à retrouver, même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules.

3 Les différentes attaques sur les mots de passe

Afin d'éviter qu'un mot de passe ne soit facilement retrouvé par un outil conçu à cet effet, il peut être intéressant de connaître les différentes méthodes utilisées par les outils automatisés pour découvrir les mots de passe. Dans la plupart des cas, ce sont les empreintes (valeur de sortie d'une fonction de hachage) des mots de passe qui seront stockés sur le système. Les attaques sur les mots de passe consistent donc à calculer des empreintes et à les comparer à celles contenues dans les fichiers de mots de passe.

3.1 Attaques par force brute

Cette attaque consiste à tester toutes les combinaisons possibles d'un mot de passe. Plus il existe de combinaisons possibles pour former un mot de passe, plus le temps moyen nécessaire pour retrouver ce mot de passe sera long.

Un mot de passe fort, d'une longueur minimale de dix caractères et constitué d'au moins trois des quatre groupes de caractères enoncés ci-dessus (minuscules, majuscules, caractères spéciaux et chiffres), ne pourra être découvert par cette attaque dans un temps raisonnable, avec les moyens dont on dispose au moment de la rédaction de cette note d'information.

3.2 Attaques par dictionnaires

Cette attaque consiste à tester une série de mots issus d'un dictionnaire. Il existe toutes sortes de dictionnaires disponibles sur l'Internet pouvant être utilisés pour cette attaque (dictionnaire des prénoms, dictionnaire des noms d'auteurs, dictionnaire des marques commerciales...). En utilisant un mot de passe n'ayant aucune signification cette attaque ne donnera aucun résultat.

Cependant, plusieurs règles de transformation des mots du dictionnaire sont utilisées par les outils automatisés pour augmenter le nombre de combinaisons possibles. Citons par exemple :

- le remplacement d'un ou de plusieurs caractères du mot du dictionnaire par une majuscule (`bUreAU`) ;
- le remplacement de certains caractères par des chiffres comme par exemple le `S` en `5` (`mai5on`) ;
- l'ajout d'un chiffre au début ou à la fin d'un mot (`arbre9`) ;
- l'ajout des mots de passe déjà découverts.

Il est possible d'utiliser les dictionnaires précalculés contenant une liste de mots de passe et leur empreinte associée. Même si cette possibilité accélère le temps nécessaire pour retrouver un mot de passe, elle nécessite une place plus importante en mémoire.

La solution idéale pour un individu malintentionné qui souhaiterait retrouver des mots de passe le plus rapidement possible serait d'avoir une liste exhaustive de tous les mots de passe possibles et de leur empreinte associée. Un tel dictionnaire n'est pas enviseageable car il nécessiterait une place en mémoire bien trop importante. Cependant sur les algorithmes de chiffrement faibles (par exemple le chiffrement `LM` sur les systèmes Microsoft Windows), il est possible d'utiliser les attaques par compromis temps/mémoire (voir bibliographie).

3.3 Attaques par compromis temps/mémoire

Les attaques par compromis temps/mémoire sont des solutions intermédiaires permettant de retrouver un mot de passe plus rapidement qu'avec une attaque par force brute et avec moins de mémoire qu'en utilisant une attaque par dictionnaire. Ces compromis sont réalisés à partir de chaînes construites à l'aide de fonctions de hachage et de fonctions de réduction. Pour retrouver un mot de passe, il faudra d'abord retrouver à quelle chaîne appartient l'empreinte recherchée. Une fois que la chaîne aura été retrouvée il sera alors facile de retrouver le mot de passe, à partir du début de cette chaîne.

3.4 Attaques indirectes

D'autres attaques assez connues car très pratiquées (en particulier le filoutage et les logiciels de captures des frappes au clavier) consistent non pas à déterminer le mot de passe par une recherche technique mais à le capturer au moment où il est saisi, ou encore à se le faire communiquer en usant de supercherie. Face à ces attaques, la qualité (ou « force ») du mot de passe doit être complétées par des mesures organisationnelles essentielles :

- procédures robustes d'ouverture de compte (initialisation et première fourniture du mot de passe) ;
- sensibilisation et bonne information des utilisateurs afin qu'ils détectent les tentatives pour leur soutirer leur mot de passe ;

– procédures robustes de réinitialisation en cas d'oubli ou perte du mot de passe par un utilisateur.
– ne pas réutiliser les mots de passe et en particulier, pas d'utilisation pour une application peu protégée du même mot de passe que pour une application sensible ;

4 Créer un bon mot de passe

Un bon mot de passe est un mot de passe fort, qui sera donc difficile à retrouver même à l'aide d'outils automatisés mais facile à retenir. En effet, si un mot de passe est trop compliqué à retenir, l'utilisateur mettra en place des moyens mettant en danger la sécurité du SI, comme par exemple l'inscription du mot de passe sur un papier collé sur l'écran ou sous le clavier où l'utilisateur doit s'authentifier. Pour ce faire, il existe des moyens mnémotechniques pour fabriquer et retenir des mots de passe forts.

4.1 Méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple la phrase « *J'ai acheté huit cd pour cent euros cet après midi* » deviendra `ght8CD%E7am`.

4.2 Méthode des premières lettres

Cette méthode consiste à garder les premières lettres d'une phrase (citation, paroles de chanson...) en veillant à ne pas utiliser que des minuscules. Par exemple, la citation « `un tiens vaut mieux que deux tu l'auras` » donnera `1tvmQ2tl'A`.

5 Gestion des mots de passe

Les mots de passe sont souvent la seule protection d'une station de travail. Il est donc indispensable de mettre en œuvre une politique de gestion des mots de passe intégrée à la politique de sécurité du système d'information.

5.1 Politique de gestion des mots de passe

La politique de gestion de mots de passe devra être à la fois technique et organisationelle. Les éléments suivants pourront, entre autres, être inscrits dans cette politique :

5.1.1 Sensibilisation à l'utilisation de mots de passe forts

Les utilisateurs d'un système d'information doivent être sensibilisés à l'utilisation de mots de passe forts afin de comprendre pourquoi le risque d'utiliser des mots de passe faibles peut entraîner une vulnérabilité sur le système d'information dans son ensemble et non pas sur leur poste uniquement.

5.1.2 Mot de passe initial

Le mot de passe initial doit être de préférence fourni sur un canal sûr. Lorsque ce mot de passe initial est fourni par l'administrateur du système ou lorsqu'il est communiqué sur un canal non confidentiel, il doit être changé dès la première connexion de l'utilisateur.

L'administrateur qui a fourni un mot de passe sur un canal non sûr doit avoir une vigilance plus soutenue afin de s'assurer que le mot de passe n'est pas utilisé par un tiers.

5.1.3 Renouvellement des mots de passe

Les mots de passe doivent avoir une date de validité maximale. A partir de cette date l'utilisateur ne doit plus pouvoir s'authentifier sur le système si le mot de passe n'a pas été changé. Ceci permet de s'assurer qu'un mot de passe découvert par un utilisateur mal intentionné, ne sera pas utilisable indéfiniment dans le temps.

5.1.4 Les critères prédéfinis pour les mots de passe

Plusieurs critères peuvent être définis et mis en œuvre dans de nombreux systèmes pour s'assurer de la qualité des mots de passe. Ces critères sont, par exemple :

- une longueur minimum prédéfinie (au minimum 10 caractères) ;
- l'impossibilité de réutiliser les *n* derniers mots de passe ;
- le nombre de tentatives possibles ;
- la manière de déverrouiller un compte qui a été bloqué (pour éviter les dénis de service liés au blocage de tous les comptes sur un système d'information, il peut être intéressant que le déblocage des comptes se fasse de manière automatique après un certain délai) ;
- l'utilisation sur le poste de travail ou sur une application particulière de la mise en veille automatique avec un déblocage par un mot de passe.

5.1.5 Confidentialité du mot de passe

Un mot de passe sert à s'authentifier sur un système. Dans ce but il est important de veiller à ne pas divulguer son mot de passe. Un mot de passe ne doit jamais être partagé ni stocké dans un fichier ni sur papier. Cependant, il est possible que la politique de sécurité demande aux utilisateurs d'un système d'information de stocker les mots de passe sur papier dans un lieu sûr (enveloppe cachetée dans un coffre ignifugé) pour le cas ou un problème surviendrait.

5.1.6 Configuration des logiciels

Une large majorité de logiciels comme par exemple les logiciels de navigation Internet proposent d'enregistrer les mots de passe, par le biais d'une petite case à cocher « `retenir le mot de passe` », pour éviter à l'utilisateur la peine d'avoir à les ressaisir. Ceci pose plusieurs problèmes de sécurité notamment lorsqu'une personne mal intentionnée prend le contrôle de l'ordinateur d'un utilisateur, il lui suffit de récupérer le fichier contenant la liste des mots de passe enregistrés pour pouvoir se connecter sur des sites à accès protégé.

5.2 Utilisation de mots de passe différents

Il est important de garder à l'esprit qu'un mot de passe n'est pas inviolable dans le temps. C'est pour cette raison qu'il est nécessaire de changer régulièrement son mot de passe et qu'il est important de ne pas utiliser le même mot de passe pour tous les services vers lesquels on se connecte.

En effet, si le poste de travail est compromis et qu'un renifleur de clavier est installé, il sera possible pour un utilisateur mal intentionné de récupérer tous les mots de passe entrés au clavier (même si ces mots de passe sont des mots de passe forts). L'utilisateur mal intentionné pourra seulement accéder aux services dont il connaîtra le ou les mots de passe capturés durant la période pendant laquelle le renifleur de clavier était installé. Tant que les mots de passe capturés ne sont pas changés, des accès malveillants sont possibles, l'impact de l'attaque est durable.

C'est pourquoi changer régulièrement de mots de passe, *à partir de machines saines*, permet de diminuer la durée de l'impact de l'attaque.

5.3 Utilisation de mots de passe non rejouables (`One Time Password`)

Il est possible d'utiliser des solutions permettant de s'authentifier à un système par le biais d'un mot de passe ne pouvant être utilisé qu'une seule fois. Cette solution présente l'avantage que lorsqu'un mot de passe est découvert, il ne pourra pas être réutilisé. Cette technique reste toutefois vulnérable aux attaques de l'intercepteur (*man in the middle*).

5.4 Utilisation de certificats clients et serveurs

L'utilisation de certificats de clés publiques sur les postes clients et serveurs permet de détecter l'intercepteur (*man in the middle*), mais reste vulnérable au vol sur le poste de travail du code porteur ou de la clé privée si elle n'est pas protégée dans un matériel adéquat (par exemple une carte à puce). Si le client dispose d'un certificat d'authentification et d'une clef privée bien protégée, alors il est préférable d'utiliser cette clef plutôt qu'un mot de passe pour l'authentification.

5.5 Mettre en place un contrôle systématique des mots de passe

Pour s'assurer de l'absence de mots de passe faibles, il peut être intéressant pour un administrateur, s'il y est autorisé, de réaliser des tests sur la robustesse des mots de passe utilisés sur son système d'information. Des outils commerciaux ou gratuits sont disponibles sur l'Internet. Le choix de l'outil le plus adapté dépend du type de mots de passe que l'on désire analyser.

6 Bibliographie

– Les mots de passe Windows à la merci des compromis temps-mémoire :
http://lasecwww.epfl.ch/ oechslin/publications/sstic04.pdf

Gestion détaillée du document

21 février 2005 version initiale.

1 septembre 2006 corrections diverses.

12 avril 2007 rendre plus explicite les risques d'attaques indirectes, développer le propos sur la politique de mots de passe, corrections diverses.