

Résumé

L'accès aux ressources informatiques doit se faire de façon nominative ou identifiée et cela pour deux raisons principales :

- empêcher l'accès aux ressources informatiques à toute personne non autorisée,
- identifier les éventuels actes malveillants ou maladroites.

Les contrôles d'accès par authentification aux systèmes informatiques font l'objet de la présente fiche.

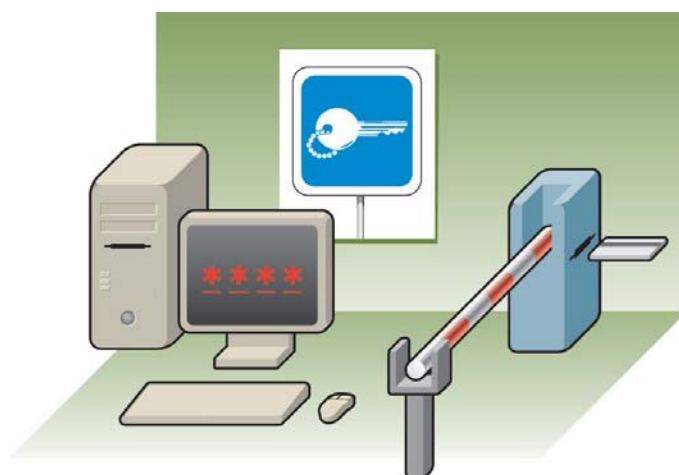
L'authentification est un mécanisme de gestion des accès, basé sur le principe d'une clé. La solution classique repose sur le couple : identifiant et mot de passe. Les diverses vulnérabilités récurrentes de cette solution sont : mots de passe peu résistants ou

inexistants, existence de comptes installés par défaut, mots de passe ayant perdu leur caractère secret, logiciels créant des utilisateurs pour usage interne, formules de chiffrement des mots de passe non fiables, mémorisation des mots de passe sur les stations de travail et absence de surveillance ou de blocage en cas de tentatives d'accès erronées. Les menaces du déchiffrement sont le « cracking » brutal, le dictionnaire ainsi que les bogues « web ». La fiche décrit comment se protéger contre les vulnérabilités et menaces énumérées.

Attention : l'accès physique aux salles informatiques et l'accès aux ordinateurs personnels n'est pas couvert par cette fiche.

Table des matières

- 1 C'est quoi ? →
- 2 Quelles sont les vulnérabilités récurrentes ? →
- 3 Quelles sont les menaces du déchiffrement ? →
- 4 Pourquoi se protéger ? →
- 5 Comment se protéger ? →



1 C'est quoi ?

L'authentification est un mécanisme de gestion des accès, basé sur le principe d'une clé. Cette clé permet de faire le lien entre la demande d'accès à l'infrastructure et une personne physique ou un autre composant du système informatique. Idéalement, cet identifiant est consolidé par un mot de passe ou tout autre élément censé être en possession unique de la personne négociant l'accès.

L'authentification n'est donc pas en tant que telle une vulnérabilité. Toutefois, la mauvaise utilisation des mécanismes d'authentification est une des vulnérabilités les plus exploitées par les pirates/crackers.

2 Quelles sont les vulnérabilités récurrentes ?

Les principes d'authentification sont applicables, au niveau de l'accès « utilisateur » et « administrateur », aux serveurs et logiciels. Il ne faut pas oublier de tenir compte des accès aux éléments physiques constituant le système informatique, tels que les routeurs, les commutateurs, ...

La solution classique = identifiant et mot de passe.

Cette solution courante base l'authentification sur une paire alliant un identifiant fourni par l'administrateur et un mot de passe que l'utilisateur final prendra soin de déterminer.

→ suite

On remarque que cette solution doit faire face à diverses vulnérabilités récurrentes :

2.1 Existence de comptes avec des mots de passe peu résistants ou inexistants

Il existe quelques critères de qualité à respecter lors de la conception d'un mot de passe et ce afin d'éviter que des logiciels spécialisés ne puissent le cracker en peu de temps. Cracker est un mot anglais signifiant déchiffrer un mot de passe. Ces critères sont abordés au chapitre 5 de la présente fiche.

2.2 Existence de comptes installés par défaut lors de la mise en place de logiciels

Lors de l'installation de logiciels tels que les systèmes d'exploitation, il y a création de comptes par défaut. Ces comptes utilisent un mot de passe connu de tous les pirates/crackers. Il est évident que ces comptes sont les premières cibles des personnes mal intentionnées. Il est donc nécessaire de protéger ce compte par un mot de passe fiable.

2.3 Mots de passe ayant perdu leur caractère secret

Un mot de passe est l'artifice permettant d'identifier l'utilisateur d'un compte. Il s'inscrit dans la même logique qu'un numéro de code pour les retraits aux guichets automatiques. Malheureusement, on voit trop souvent des mots de passe affichés sur les écrans ou connus de multiples personnes.

2.4 Logiciels créant des utilisateurs pour usage interne

Certains logiciels, telles que les bases de données ou autres, vont créer des comptes utilisés en interne pour converser avec les autres composantes du système informatique. Ces identifiants

et leur mot de passe, souvent faibles ou même inexistants, sont documentés et évidemment connus de tous les pirate/crackers.

2.5 Formules de chiffrement des mots de passe non fiables

Le transport ou le stockage des mots de passe est chiffré dans la plupart des systèmes informatiques. Toutefois il est bon de s'assurer que le paramétrage par défaut n'utilise pas un chiffrement faible facile à décrypter. On peut être certain que les chiffrements faibles sont connus du monde des pirates/crackers

2.6 Mémorisation des mots de passe sur les stations de travail

De nombreux logiciels utilisant des mots de passe offrent la possibilité de les stocker de manière à ne plus devoir les saisir la prochaine fois. Il est évident que, malgré son aspect pratique, cette possibilité est vivement déconseillée, car cela revient à ne pas avoir de mot de passe.

2.7 Absence de surveillance ou de blocage en cas de tentatives d'accès erronées

L'apparition de multiples tentatives d'introductions erronées de mots de passe pour un même compte représente évidemment un signal d'alarme très important pour un responsable de l'administration.

Alors que la plupart des systèmes informatiques permettent le blocage d'un compte après un certain nombre de tentatives erronées, il n'est pas rare que cela ne soit pas utilisé, ouvrant de ce fait la porte aux logiciels de « cracking » décrits dans ce document.

3

Quelles sont les menaces du déchiffrement ?

A la consultation du « Top20 » des vulnérabilités publié par le SANS (System Administration, Audit, Network, Security institute - www.sans.org), on remarque que la vulnérabilité des mécanismes d'authentification demeure depuis plus d'un an dans le « Top10 » des vulnérabilités les plus exploitées.

Pour perpétrer ce genre d'attaques, les pirates/crackers/hackers utilisent des logiciels de déchiffrement spécialisés et se basant sur deux technologies distinctes :

3.1 Le « cracking » brutal (Brute Force Cracking)

Ce type de logiciel va essayer toutes les combinaisons contenant aussi bien des caractères hybrides qu'alphanumériques. Cette solution est efficace mais demande énormément de temps pour permettre une découverte de chaînes de caractère complexes.

Certains de ces outils sont dédiés à des logiciels spécifiques tels que Microsoft Word, ou autres.

→ suite

3.2 Le dictionnaire

Ce logiciel va essayer tous les termes stockés dans un dictionnaire qui reprend les mots de passe habituellement utilisés. Cette méthode un peu plus rapide ne permet pas de donner les mêmes résultats que la méthode brutale.

3.3 Les bogues « web »

Une autre méthode, malheureusement en pleine expansion, est l'usage de certains «web bugs» qui ont pour but d'écouter tout l'encodage clavier et de les transmettre à une adresse particulière. La fiche relative aux «Bogues - Bugs» donne plus d'informations sur les contre-mesures.

4 Pourquoi se protéger ?

Les impacts des vulnérabilités décrites dans le chapitre 2 sont assez faciles à imaginer, puisque qu'ils équivalent à rendre public un système de traitement d'informations, les logiciels et toutes les données qui le constituent (voir aussi la fiche «Les impacts des incidents informatiques»).

Dans un scénario catastrophique, on peut imaginer la perte complète du contrôle du système de traitement d'information, sans autre solution que de tout recommencer à zéro.

5 Comment se protéger ?

Les conseils donnés ci-après, traitent de l'usage de l'authentification par compte/mot de passe. Ces règles sont à configurer par vous dans le logiciel d'administration, de manière à ce qu'elles soient automatiquement applicables à tous les comptes créés.

5.1 Assurez vous que les mots de passe sont solides

Si les mots de passe répondent à la description suivante, vous pourrez considérer que les outils de cracking prendront tellement de temps que les éventuels pirates/crackers perdront courage :

- Ne pas contenir de partie du nom de l'utilisateur.
- Avoir minimum 6 à 8 caractères de longueur.
- Contenir des caractères de minimum trois de ces familles :
 - > alphabétique minuscule,
 - > alphabétique majuscule,
 - > numérique de 0 à 9,
 - > non alphanumérique (!,*,#, ...).

5.2 Conservez un historique des mots de passe

- Conservez les mots de passe utilisés. Il est donc impossible aux utilisateurs de toujours utiliser les mêmes deux ou trois mots de passe.
- Donnez une durée de validité maximale au mot de passe. De cette manière, une fois la date de validité atteinte, l'utilisateur devra impérativement changer de mot de passe.
- Donnez une durée de validité minimale au mot de passe. Cela peut sembler étonnant, mais si vous ne veillez pas à cette durée minimale, l'utilisation de l'historique ne sert à rien car il suffira à un utilisateur de changer dix fois de mot de passe en une minute pour pouvoir réutiliser le mot de passe initial.

5.3 Trucs et astuces

Pour éviter que l'absence d'un responsable informatique ne cause le blocage complet d'un système informatique, il peut parfois être nécessaire de donner un accès de secours à une personne. Toutefois, il vaut mieux éviter que cette personne ne puisse utiliser cet accès sans raison. Pour cela, il est toujours possible de stocker le mot de passe sous enveloppe scellée dans un coffre ou de créer un mot de passe composé de deux parties distinctes dont deux personnes connaissent la moitié.

Pour créer un mot de passe complexe mais facile à retenir, vous pourrez utiliser la méthode des initiales, par exemple : «Je suis né le 13 juillet 61 à Luxembourg» > «Jsnl13j61aL».

[→ suite](#)

5.4 Contrôlez l'architecture informatique

Il est très important d'analyser périodiquement les logs afin de détecter les éventuelles tentatives d'accès frauduleux. De même, il est indispensable de mettre à jour la liste des utilisateurs, leurs profils et leurs droits sur le système informatique.

5.5 Limitez les comptes « administrateur »

Les comptes de type « administrateur », bénéficiant de beaucoup de droits, sont la cible privilégiée des pirates, crackers. Il est conseillé de ne pas partager pas ce compte avec toute l'équipe informatique, mais de créer des profils correspondant aux besoins exacts de chacun des membres de l'équipe.

Sur la plate-forme Microsoft Windows, il peut même être intéressant de limiter tous les pouvoirs du compte « administrateur » et de lui attribuer un mot de passe très complexe. Il suffit ensuite de redistribuer les tâches à d'autres comptes moins visibles. De cette manière, l'éventuel pirate / cracker passera son temps sur un leurre puisque ce compte ne lui permettra rien. Malheureusement, cela n'est pas possible sur la plate-forme Unix avec le compte root.

5.6 Utilisez des logiciels de validation de mots de passe

Il existe sur le marché divers logiciels de validation de la solidité des mots de passe. Ces logiciels étant malheureusement assez onéreux, il peut s'avérer plus économique pour vous de demander à des entreprises externes de procéder à ce genre de test.

⚠ Attention : Avant de vous lancer dans toute tentative d'évaluation des mots de passe il faut que vous en informiez le responsable des accès et que vous analysiez les impacts possibles. En effet, l'utilisation de ce genre de logiciels pourrait mener au blocage pur et simple de tous les comptes.

5.7 Solutions alternatives

De nouvelles solutions d'authentification, telles que la PKI (Public Key Infrastructure), la biométrie et les cartes à puces, sont en train de faire leur apparition sur le marché. Ces solutions font l'objet de fiches séparées.

L'avantage de ces solutions est de supprimer le problème de la divulgation des mots de passe ou de la transmission de données critiques au travers du réseau. Malheureusement, elles restent encore coûteuses et complexes à mettre en place.