Choix.Mot.de.Passe

CHOISIR UN BON MOT DE PASSE

28 juillet 92

Jean-Luc Archimbaud CNRS/UREC

Cet article est destiné à tous les utilisateurs de systèmes informatiques qui possèdent un mot de passe. C'est le premier d'une nouvelle rubrique qui se veut régulière et sera consacrée à la sécurité informatique, des ordinateurs et des réseaux.

DE L'UTILITE D'UN BON MOT DE PASSE

Lorsque vous possédez un compte sur un ordinateur, le seul et unique contrôle d'accès à cette machine est votre mot de passe. Quelqu'un qui découvre cette clé peut ensuite travailler sur la machine sous votre nom (souvent sans que vous vous en aperceviez), lire tous vos fichiers (courriers, publications...), détruire ces fichiers ou plus insidieusement en modifier certains.
Cette fonction clé (au sens figure et au sens propre) du mot de passe est devenue encore plus importante avec l'explosion des réseaux. On peut, par exemple, considérer qu'actuellement une très grosse partie des machines dans les laboratoires sont accessibles depuis n'importe quel Minitel en France. Si l'accès n'est pas direct, il est possible avec un ou plusieurs rebonds : depuis un Minitel on fait login sur une première machine, puis depuis celle-ci on fait telnet sur une seconde machine... N'importe quel particulier peut ainsi tenter de se connecter sous votre nom et essayer de trouver votre mot de passe. Du côté de l'administrateur de la machine, il est devenu très difficile, voire impossible sans plusieurs mois d'enquête, de localiser géographiquement ses utilisateurs. Devant cette ouverture des réseaux, très utile au demeurant, le seul et unique contrôle reste le mot de passe.
Le problème du mot de passe est qu'il peut être découvert par un individu mal intentionné qui peut ensuite s'en servir avec peu de risque d'être pris.
Mais on ne peut découvrir un mot de passe que si celui-ci a été mal choisi. Pourquoi la syntaxe du mot de passe est elle importante dans la sûreté de cette clé ? Parce qu'il est actuellement impossible de trouver un mot de passe en essayant toutes les combinaisons de 7 caractères (et a fortiori plus de 7). Cela prendrait plusieurs années de temps CPU à un programme automatique. Par contre, il est très facile de découvrir un mot de passe qui est un mot d'un dictionnaire.

COMMENT PUIS-JE TROUVER VOTRE MOT DE PASSE ?

Vous connaissant, je regarderai d'abord si vous n'avez pas noté ce mot de passe. Je chercherai ainsi sur ou sous votre clavier, dans votre agenda... Puis j'essayerai comme valeur les informations personnelles vous concernant : nom de login, prénom, nom de laboratoire, numéro de téléphone, prénoms de vos enfants, date de naissance, adresse ... Si ça ne marche pas, je tenterai alors des combinaisons avec tout ça : initiales des prénoms des enfants, numéro de téléphone inverse, nom du laboratoire suivi du chiffre 1...

Si cette méthode artisanale, mais souvent efficace, échoue, j'automatiserai la recherche avec un programme pour découvrir (craquer) les mots de passe. Ce type de logiciel est du domaine public et peut être récupéré dans les news ou par ftp anonymous (cf. Microbulletin précédent, rubrique IP).
Prenons le cas d'une machine Unix. Les mots de passe chiffrés (résultat d'une fonction mathématique de chiffrement) de tous les utilisateurs sont stockés dans un fichier /etc/passwd. Tout le monde peut lire ce fichier (accès r à other), ainsi que la fonction Unix de chiffrement (fonction crypt). Je transférerai /etc/passwd de votre ordinateur sur ma propre machine. A l'abri des regards indiscrets, je pourrai faire tourner ce logiciel pour découvrir les mots de passe mal choisis de certains utilisateurs.

A noter qu'il est heureusement impossible de trouver le mot de passe en clair à partir du mot de passe chiffré, la fonction de chiffrement n'est pas inversible. Le logiciel de cracking procède par essais successifs. Il prend une suite de caractères en clair, la chiffre, et compare le résultat avec la chaîne chiffrée dans /etc/passwd. Il peut essayer :
* Les informations personnelles contenues dans /etc/passwd : nom, prénom, adresse ...
* Les mots de dictionnaires : noms communs, noms propres et prénoms. Il peut posséder des dictionnaires de plusieurs langues.
* Des variations de ce qui précède : passage en majuscule de tout ou partie, ajout d'un chiffre en début ou en fin de mot, inversion...
* Toutes les combinaisons de 1, 2, 3 , 4 , voire 5 caractères (mais pas plus).
Généralement, on découvre 1/3 des mots de passe avec ce logiciel, logiciel que les développeurs améliorent au fil du temps. De nombreux administrateurs de machines Unix font tourner ce genre de programme régulièrement sur les systèmes qu'ils gèrent et demandent aux utilisateurs dont le mot de passe a été ainsi craqué d'en changer.
Via les réseaux, cette méthode peut être utilisée depuis n'importe quel point dans le monde, par un individu que vous n'avez jamais vu.

CE QU'IL NE FAUT PAS FAIRE

Il ne faut pas noter son mot de passe. Pour cela, il faut qu'il soit mnémonique.
Il ne faut pas le confier à quelqu'un, ni le partager avec d'autres. Il doit toujours être personnel. Si l'on désire travailler à plusieurs sur les mêmes fichiers, ceci est possible dans tous les systèmes d'exploitation avec un mot de passe différent pour chacun (possibilité des groupes sous Unix par exemple).
Il ne faut pas choisir comme mot de passe une information personnelle telle que son nom; celui de son laboratoire, de son projet ou de ses proches; son numéro de voiture... Les noms communs, noms propres ou prénoms présents dans un dictionnaire français ou étranger sont à proscrire. Est à éviter aussi, toute variation de ce qui précède, telle que l'inversion, les initiales, ou l'ajout de chiffres.

LE BON CHOIX

Prenez tout d'abord un temps de réflexion pour choisir votre mot de passe. Si l'on vous presse lors de l'ouverture de votre compte sur une machine d'un centre de calcul par exemple, donnez en un simple et changez le à tête reposée lors de votre premier login.
Il faut choisir une suite d'au moins 7 caractères, avec des majuscules, chiffres et/ou caractères de ponctuation. Cette suite doit être difficile à découvrir par les pirates avec les méthodes décrites avant mais facile à mémoriser. Une première méthode est de combiner des mots en introduisant des chiffres ou des caractères de ponctuation (BaD!beurk, PC3rpr5). Une autre consiste à utiliser des mots avec de la phonétique (7touMuch, uneCtion). Vous pouvez aussi prendre les premiers lettres d'une phrase, expression... que vous aimez (JvAlPaLl pour "Je vais à la pèche à la ligne"). Et pour finir, vous pouvez mixer tout ca (c'est1KO).
Il faut faire marcher votre imagination pour trouver des suites de signes apparemment aléatoires qui n'ont un sens que pour vous. Mais il faut que ça vous soit facile à mémoriser.
Dernière recommandation, il faut changer son mot de passe régulièrement, même s'il est très bon, à cause principalement de l'écoute qui peut être faite sur les réseaux. La périodicité de changement dépend de l'utilisation que vous faites de l'informatique et de votre environnement. Changer son mot de passe avant de partir en vacances est souvent une sage attitude à condition de s'en souvenir en revenant. A noter qu'il ne faut pas reprendre d'anciens mots de passe que vous avez déjà utilisés.

ET LE RESEAU ?

Le réseau peut amener deux problèmes que sont les tentatives d'accès en provenance du monde entier et la possibilité d'écoute des liaisons.
Etre connecté sur un réseau international, amène une ouverture internationale qui permet à des individus d'essayer votre mot de passe depuis le bout du monde. Le risque de piratage n'est donc plus uniquement local mais international. Il faut prendre en compte cette nouvelle donnée. Mais pour l'instant, si l'on regarde de l'autre côté de l'Atlantique, en avance de plusieurs années dans la pratique des télécommunications entre chercheurs, il y a eu très peu de piratage à travers les réseaux de la recherche.
Si entre votre clavier et la machine où vous faites login vous traversez un réseau, votre mot de passe circule en clair sur les fils. Des logiciels existent pour récupérer, depuis un PC, les identités et les mots de passe qui circulent sur un réseau à diffusion tel que Ethernet. Ceci est imparable. Mais ce danger est à relativiser. Si vous communiquez entre deux laboratoires à travers un réseau international, le risque d'écoute se situe aux extrémités, sur les deux réseaux locaux des laboratoires. Entre ceux-ci, les réseaux peuvent être considérés comme sûrs en ce qui concerne le risque d'écoute. En effet, avec la quantité de données qui circulent sur ces réseaux d'interconnexion, il est très difficile d'extraire le couple nom-mot de passe. De plus, les uniques personnes qui ont accès à ces réseaux sont des professionnels des télécommunications plus dignes de confiance que les étudiants sur les réseaux locaux aux 2 extrémités.

POURQUOI CETTE RUBRIQUE ?

"La sécurité informatique, c'est le problème des entreprises privées ! La recherche fondamentale doit être totalement ouverte. Elle est universelle et ne supporte aucune contrainte ! ". Ce discours très souvent entendu porterait à croire que la sécurité informatique ne touche pas les chercheurs.
Voici quelques exemples vécus dans des unités du CNRS et qui prouvent que les laboratoires ne sont pas épargnés par ces risques :
* Un chercheur fait régulièrement de la simulation sur un gros calculateur scientifique. Il dispose chaque année d'un certain quota d'heures d'unité centrale réservées sur cette machine. Mais cette année, lors de son premier login au mois de mai, son crédit est déjà épuisé alors qu'il n'a jamais travaillé sur l'ordinateur. Apres enquête, on s'aperçoit que quelqu'un a utilisé le compte du chercheur pour faire tourner ses propres programmes. Le mot de passe du chercheur avait été découvert par un individu sans scrupule, en mal de temps machine. Il faut dire que c'était son nom de login.
* Un thésard saisit sa thèse sur un PC, partagé par plusieurs personnes. Après un vendredi 13, tout le contenu du disque du PC est détruit par un virus. Sans sauvegarde, adieu le fichier Word de la thèse, le thésard doit tout retaper : bonnes nuits blanches. Un des utilisateurs du PC amenait régulièrement des disquettes de jeux qu'il avait copiées et qu'il essayait...
* Un Directeur de laboratoire reçoit un coup de téléphone d'un laboratoire de recherche de la NASA lui demandant d'intervenir pour interdire à M. Dupont sur la machine ZEUS de son laboratoire de se livrer à des tentatives de piratage sur les machines américaines. En effet, l'étudiant Dupont essayait de récupérer des fichiers de mots de passe par ftp anonymous, pour s'amuser...
* Un laboratoire allait signer un contrat de recherche avec une grosse société industrielle. Au dernier moment, celle-ci refuse. L'industriel avait pris des renseignements sur les méthodes de travail dans le laboratoire. Malgré la grande renommée scientifique internationale du laboratoire, c'était une vraie passoire en matière de confidentialité informatique des recherches. Ce domaine de recherche intéressant la concurrence, l'industriel a préféré choisir un autre partenaire moins bon scientifiquement mais plus sûr.
* Un laboratoire sur un campus se fait voler les 15 micros qui constituent l'ensemble de son parc informatique. Question matériel c'est une perte sèche, le matériel de l'état n'est jamais assuré. Les disques qui contiennent les résultats des expériences se sont aussi envolés. Combien d'argent et de jours de travail ont été perdus ?

Parallèlement à ces exemples de la vie de tous les jours (j'espère que ce n'est pas tous les jours), un Centre National de Recherche doit veiller à une certaine confidentialité de ses recherches. Dans notre monde, la guerre industrielle entraîne une compétition effrénée à l'innovation. Or toute nouveauté est issue, de près ou de loin, d'une recherche fondamentale. La Recherche se trouve ainsi, souvent malgré elle, prise dans cette course ou tous les moyens sont bons pour être les premiers. Les résultats de recherche peuvent devenir des enjeux économiques ou stratégiques. Il convient donc de contrôler l'accès à ces informations. Etant de plus en plus stocké sur des supports informatiques, ceci est à traiter par la sécurité informatique.
Faire quelque chose dans ce domaine au CNRS, c'est essayer d'éviter tous les ennuis ci-dessus. La méthode ne vise pas à transformer les laboratoires en blockhaus, ni à mettre un gendarme à chaque porte; mais à sensibiliser l'ensemble des personnels des laboratoires pour qu'ils adoptent certaines habitudes de travail qui limitent les risques.
Cette rubrique du microbulletin va essayer d'aller dans ce sens, en donnant certains conseils souvent de simple bon sens. Son but n'est pas de gendarmer ou de sanctionner, mais d'informer et de conseiller.
Si vous avez eu, par exemple, des expériences heureuses ou malheureuses dans ce domaine, n'hésitez pas me proposer un article qui paraîtra dans cette rubrique.

CHARGE DE MISSION SECURITE INFORMATIQUE

Je suis charge de mission sécurité informatique et réseau au CNRS. Un prochain article de cette rubrique décrira mon rôle et mes actions. Mais dès à présent, vous pouvez me contacter pour toute aide et conseil dont vous auriez besoin dans ce domaine.

PETITE MAXIME DE SECURITE

La sécurité est un compromis.

Ceci est vrai en général. C'est d'autant plus vrai en informatique ou plusieurs individus partagent souvent la même machine, et en réseau dont le but est l'ouverture.
C'est un compromis humainement et techniquement.
Humainement, car il ne faut pas imposer des contraintes draconiennes dans ce domaine, inadaptées à l'environnement de travail et à l'esprit de la maison. Ceci est d'autant plus vrai au CNRS où il y a une forte tradition libérale hostile à toute contrainte. Des mesures militaires provoqueraient une attitude de rejet complet et un essai de contournement systématique (un chercheur est toujours très imaginatif). La sécurité n'est pas un but en soi.
Compromis aussi technique. Il n'y a jamais de "0 défaut" avec un produit de sécurité informatique. Le seul ordinateur totalement sécurisé est l'ordinateur éteint (sic). Toutes les mesures de sécurité, les outils ou les conseils ont des failles. Ils réduisent les risques, mais sans jamais arriver à tous les éliminer. Il y aura toujours des esprits négatifs qui diront : "Oui, mais si le pirate fait... alors il contourne votre truc et ça ne marche pas".
Face à ce postulat, il convient d'éviter le choix du tout ou rien qui conduit à ne rien faire. Au contraire, il convient de prendre quelques mesures adaptées (des bonnes habitudes de travail ...) et acceptées par tous, sans ambition sécuritaire démesurée.
Ce n'est pas parce que vous savez qu'un voleur professionnel peut très facilement forcer la serrure de votre voiture, casser le neiman et s'envoler avec votre véhicule, que vous laissez toujours les portes ouvertes avec la clé de contact au volant.