Que dois-je contrôler pour assurer la sécurité de mes données?

Différentes sources de danger peuvent être identifiées en matière de sécurité. De base, la sécurité d'un appareil peut être atteinte par une personne de bon aloi ou quelqu'un ayant de véritables mauvaises intentions. Cette première page résume les techniques disponibles pour prévenir les accidents de parcours. S'il s'agit d'un cas de mauvaises intentions, les intrusions peuvent être tentées selon deux scénarios: la machine elle-même est accessible et permet l'accès à des ressources; la machine est reliée à un réseau et partage quelques ressources communes. Plusieurs solutions existent pour chacun des cas. Les trois autres pages de cet aide-mémoire traitent de la protection contre ces intrusions.

1. Techniques de protection contre les gestes accidentels

Un accident est si vite arrivé. Tout fichier dans sa forme finale ne devrait être accessible qu'en mode lecture seulement ou même masqué pour les personnes inexpérimentées. Pour ce faire, plusieurs moyens peuvent être envisagés, que ce soit par le logiciel d'application que vous utilisez quotidiennement (voir la dernière section de ce document) ou par le système.

Chaque fichier sous l'environnement IBM possède des caractéristiques appelées attributs. Ces caractéristiques protègent les fichiers contre les manipulations accidentelles des utilisateurs.

L'une de ces caractéristiques est l'attribut lecture seule qui protège un fichier en empêchant sa modification ou sa suppression. Lorsqu'un fichier possède cet attribut, vous pouvez le lire mais vous ne pouvez plus le supprimer, le renommer ou le modifier.

Une autre de ces caractéristiques en matière de protection est l'attribut caché qui masque un fichier aux yeux de l'utilisateur. Lorsqu'un fichier possède cet attribut, les commandes régulières de gestion de fichiers ne peuvent l'atteindre.

DOS

Le système DOS offre une commande de protection appelée ATTRIB.

La commande ATTRIB est une commande standard du DOS et s'utilise de la façon suivante:

```
ATTRIB +R FICHIER.DOS  (Mise en lecture seule)
ATTRIB -R FICHIER.DOS  (Mise en lecture-écriture)

ATTRIB +H FICHIER.DOS  (Masquage du fichier)
ATTRIB -H FICHIER.DOS  (Réaffichage du fichier)
```

Notez cependant que la commande ATTRIB protège vos fichiers seulement contre les manipulations accidentelles et que toute personne peut enlever à son gré l'attribut d'un fichier s'il en connaît le nom.

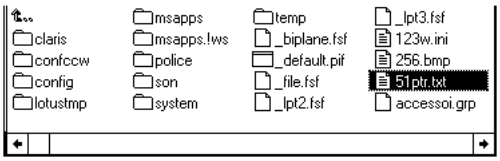
Windows

Sous Windows, le gestionnaire de fichier offre la même protection par sa commande Propriétés. Cette commande est le pendant de la commande ATTRIB du système DOS.

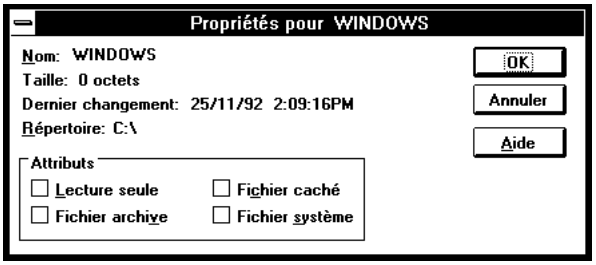
Pour placer un attribut à un fichier, il suffit de:

1. Ouvrir le gestionnaire de fichiers en double-cliquant son icône;

2. sélectionner le fichier à protéger en cliquant le fichier (figure ci-dessous);



3. choisir la commande Propriété du menu Fichier: la boîte de dialogue suivante est alors présentée;



4. cocher les attributs appropriés.

Il faut noter que si on masque un fichier sous Windows, le gestionnaire de fichiers ne peut plus voir ce fichier. L'utilisateur doit alors passer par la commande ATTRIB du DOS pour effectuer la commande de réaffichage.

2. Notions de protection reliées aux réseaux sous Vines

Lorsqu'on parle de mise en réseau, notre appareil nous ouvre une porte sur le monde. La contrepartie malheureusement incontournable de cette opportunité est que les portes de notre appareil sont à leur tour ouvertes au monde entier... Heureusement, plusieurs types de protection sont disponibles lorsque l'on utilise un réseau institutionnel comme celui de l'Université. Outre les mots de passe nécessaires à l'accession au réseau, ce même réseau offre un contrôle sur les destinataires en permettant plusieurs lieux d'entreposage selon les personnes avec lesquelles on a besoin de partager l'information.

2.1 Protéger en choisissant le lieu d'entreposage

La protection d'un document créé et modifié par une personne va avec la définition qu'on fait de ceux à qui le document est destiné. Il est donc important de bien qualifier l'information et de bien choisir le répertoire dans lequel on dépose un document afin de s'assurer qu'il ne sera accessible qu'aux personnes qu'il vise. On peut qualifier l'information selon trois catégories: privé, semi-privé et public. Chaque serveur renferme habituellement les répertoires nécessaires pour permettre ces types de partage d'information.

Privé

Certaines portions de l'information contenue sur un disque ou véhiculée sur les réseaux peuvent être qualifiées de privées. Elles ne doivent être accessibles que par l'auteur et, lorsque c'est le cas, par la personne à laquelle on destine l'information.

Bien qu'on l'utilise pour plusieurs personnes à la fois, le courrier est, par définition, privé. Il s'agit d'une communication par réseau de personne à personne.

Il en est de même de l'information généralement contenue sur un poste de travail dédié à une seule personne. Elle ne doit être accessible en tout temps que par cette personne. Il est possible que ce même type d'information soit placé sur un disque commun accessible via un réseau. Bien que le disque soit commun, on peut restreindre l'accès au propriétaire de l'information seulement. Le disque E: de plusieurs serveurs Vines du campus sert explicitement à cette fin. Chaque répertoire y est privé.

Semi-privé

À un second niveau, certaines informations peuvent être d'intérêt pour un groupe particulier. Ce groupe peut alors réserver des plages communes protégées contre l'accès par des personnes non-concernées. Ces plages communes sont accessibles sur un disque partagé sur un serveur. Le disque F: de plusieurs serveurs Vines du campus est dédié à cette tâche de partage. Les répertoires s'y trouvant sont accessibles à tout le groupe partageant le serveur et non accessible au reste du monde.

Au niveau du courrier, c'est par des listes de distribution que l'utilisateur du courrier peut envoyer une information privée à plus d'un lecteur à la fois. Souvent, les administrateurs créent une liste permettant de rejoindre tout le groupe rattaché à un serveur en plus de placer des listes d'adresses selon les domaines d'intérêts.

Public

Finalement, un document jugé d'intérêt public peut être placé sur un support physique que tous peuvent consulter. À ce moment, le problème n'est plus du ressort de la confidentialité mais bien de l'intégrité des données. Comment faire pour préserver les contenus des modifications lorsque c'est nécessaire et comment empêcher le disque partagé de tourner à l'anarchie? La solution consiste souvent à mettre en lecture seulement le dossier partagé.

Le lecteur Y: accessible sur Vines sert à cette fin. Il est en lecture seulement, ce qui veut dire que l'on ne peut y déposer de fichiers ni en modifier le contenu.

On doit éviter d'utiliser le courrier pour diffuser l'information d'intérêt public puisqu'il est peu approprié pour ce genre de situation. On doit plutôt privilégier les babillards électroniques et les services de nouvelles tel Usenet.

Comment savoir?

Si la structure des disques réseaux de votre serveur ne correspond pas aux descriptions ci-haut, on peut connaître les attributions de confidentialité des disques du serveur que l'on utilise en s'adressant à l'administrateur de réseau. Dans certaines circonstances, celui-ci peut même les modifier.

2.2 Changer son mot de passe sur Vines

Lorsque l'on se trouve au niveau du DOS, la commande Password déclenche le processus qui s'enchaîne avec les demandes et messages suivants (*l'italique* correspond à ce qui est entré par l'utilisateur).

Définir un mot de passe pour NOM@GR@ULAVAL —
Tapez votre mot de passe actuel: *ancien_mot_de_passe*
Saisissez un nouveau mot de passe: *nouveau_mot_de_passe*
Veuillez le retaper: *nouveau_mot_de_passe*
Nouveau mot de passe pour NOM@GR@ULAVAL en vigueur

3. Protection contre l'intrusion

Protéger son ordinateur correspond en plusieurs points à la protection de sa propriété. Les mots de passe constituent autant de clés pour restreindre l'accès à votre appareil. En quoi la comparaison est-elle si proche? De la même façon que vous ne confieriez pas vos clés à un étranger, il ne faut pas révéler votre mot de passe. Pour les mêmes raisons qu'il n'est pas recommandé de laisser une clé sous le tapis du portique, on ne doit pas choisir un mot de passe facile à découvrir ni le "coller" sous le bureau, là où tout bon pirate saura chercher. Toutefois, les mots de passe ne sont pas la seule méthode permettant de protéger un appareil.

3.1 Protection machine

La meilleure protection reste encore un appareil éteint dans un local fermé à clé. Personne ne peut accéder à un appareil qu'il est impossible d'atteindre ou d'ouvrir.

Physique

Au niveau physique, les machines de type IBM et compatibles sont souvent munies d'une clé qui empêche le fonctionnement de l'appareil. Barrer le mécanisme et enlever cette clé assure que l'appareil sera inutilisable.

Système

Au niveau système, chaque machine dispose de fonctionnalités permettant d'exiger un mot de passe à l'ouverture de l'appareil. Les techniques varient exigeant parfois l'utilisation d'une disquette de lancement. Parfois, des appareils de même marque utilisent des techniques différentes!

Le moment où l'utilisateur doit s'identifier varie aussi. Dans certains cas, il ne le fait qu'à l'ouverture de l'appareil; dans d'autres, il le fait systématiquement à chaque redémarrage. Encore une fois, ces différences sont fondées sur la marque de l'appareil.

Pour plus de précisions, consultez les spécialistes de l'informatique qui pourront vous guider.

Mise en veille

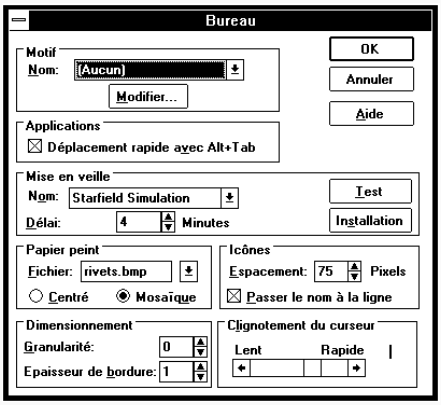
Un appareil temporairement délaissé est exposé aux regards indiscrets des visiteurs. Les outils de mise en veille sont une bonne façon de protéger les renseignements confidentiels. Toutefois, s'il s'agit d'une mise en veille sans mot de passe, il est possible, d'un coup de souris, de faire apparaître ce qui devait rester caché. C'est pourquoi certains outils de mise en veille sont munis de mots de passe.

Windows offre une telle mise en veille. Il devient donc pratiquement impossible de visualiser le contenu de l'appareil. Sitôt qu'un mouvement est détecté, le mot de passe est demandé avant le réaffichage de l'écran. Pour placer un tel mot de passe, voici la marche à suivre.

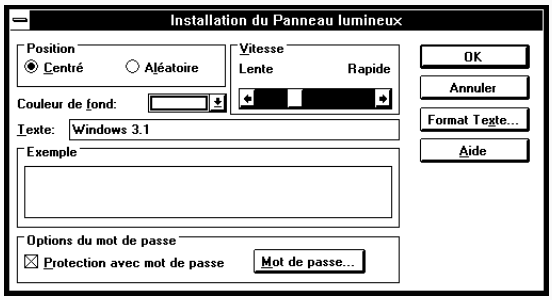
1- Double-cliquer l'icône du groupe principal;

2- double-cliquer l'icône du Panneau de configuration;

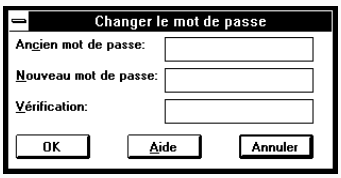
3- double-cliquer l'icône Bureau, la fenêtre suivante apparaît;



4- choisir un modèle de mise en veille puis cliquer sur le bouton Installation, la boîte de dialogue suivante apparaît alors;



5- demander l'utilisation d'un mot de passe en cochant la case située au bas de la boîte de dialogue, la boîte de dialogue suivante apparaît alors;



6- donner le mot de passe désiré;

7- terminer en cliquant le bouton OK pour chacune des boîtes de dialogue.

3.2 Protection contre les intrusions externes

Quelques outils permettent de consulter un fichier sans avoir en main l'application qui l'a créé. Ces intrusions d'origine externe sont un autre niveau d'atteinte à la confidentialité. Pour palier à ce genre d'intrusions, un recours est offert dans certains cas: l'encryptage. Bien que les machines IBM et compatibles soient peu équipées pour protéger les informations sous cette dimension, d'autres opportunités sont souvent offertes par divers logiciels.

Protection logicielle*

Si la machine ne peut répondre à un besoin de sécurité, certains logiciels de protection sur le marché ou même le logiciel d'application que vous utilisez quotidiennement peuvent offrir des mécanismes de protection.

Logiciels de protection

Sur un appareil de type IBM ou compatibles, peu de logiciels spécialisés de protection sont disponibles pour renforcer la protection Il en existe tout de même quelques-uns.

Dans cette catégorie, on peut citer comme exemple DiskLock. Il s'agit d'un logiciel commercial qui empêche l'accès à un appareil, à un disque ou à un fichier particulier grâce à différentes clés d'accès et ce, peu importe la technique utilisée pour démarrer l'appareil. Il permet aussi de faire l'encryptage des données d'un fichier afin de les rendre inaccessibles par d'autres moyens. Ce logiciel permet également de bloquer l'appareil ouvert en l'absence de son propriétaire en noircissant l'écran et en exigeant un mot de passe pour visualiser le contenu de l'écran.

D'autres logiciels offrent des possibilités différentes pour d'autres besoins. Il faut noter que ce type de logiciel ne pardonne pas si on oublie son mot de passe.

Logiciels courants offrant de la protection

Quelques logiciels d'application courante offrent une certaine forme de protection se limitant, dans la plupart des cas, à l'enregistrement des fichiers.

Parmi les logiciels les plus connus qui offrent des capacités de protection, nommons Excel, FileMaker Pro et WordPerfect. Voici un court tableau résumant à quel niveau se situent les protections.

Logiciel	Protection d'une partie du contenu	Mise en lecture seulement sans mot de passe	Mise en lecture seulement avec mot de passe	Protection contre l'ouverture	Encryptage
WordPerfect		s		s	s
Excel	m	s	s	s	
FileMaker Pro	m		m	m	

Dans ce tableau, la lettre *s* signifie que ce type de mot de passe est spécifié lors de l'enregistrement du fichier alors que la lettre *m* indique que ces types de protection sont disponibles via l'un des menus de l'application.

* L'identification d'un logiciel dans cette section ne signifie aucunement que le SIT ou toute autre instance à l'Université en fait le support. Les logiciels nommés ici le sont uniquement à titre d'exemple.

4. Les qualités d'un bon mot de passe

1- Changer son mot de passe régulièrement.

2- Ne pas choisir comme mot de passe le nom du conjoint, de l'enfant, de l'animal domestique ni la marque de l'auto, le numéro de téléphone, le numéro civique, l'âge ou tout autre nom, numéro ou date identifiant soi-même ou un proche.

3- Privilégier plutôt: tout mot de passe de six caractères au minimum, composé d'un mélange de chiffres, de lettres et, lorsque c'est permis, de caractères spéciaux suivant une logique facile à retenir mais impossible à découvrir. Exemple: **2ouppi**. Ce mot provient de youppi avec la lettre Y remplacée par un 2 puisqu'elle est la deuxième lettre de l'alphabet en commençant par la fin.

5. Gestes à éviter

Machine ouverte jour et nuit

Depuis quelques années, la tendance en matière de prévention des bris de machine incite plusieurs personnes à garder en permanence leurs machines ouvertes. Bien que ce soit favorable au strict point de vue de la fiabilité des pièces électroniques, au point de vue sécurité, un poste ne devrait jamais rester ouvert en permanence. Encore moins s'il est connecté à des disques partagés en réseau.

Telnet et mode FTP serveur

L'outil Telnet permet la connexion à une machine distante. Bien que ce soit sa fonction principale, ce n'est pas la seule. Il peut également rendre votre machine accessible aux utilisateurs externes si on permet l'accès en mode FTP et que l'on possède un numéro IP. La plupart des logiciels de type Telnet ont leur façon propre de spécifier cette option. Bien que par défaut le logiciel ne soit pas placé en mode FTP serveur, il peut être important de s'en assurer.