UNIVERSITE DE LAUSANNE
CENTRE INFORMATIQUE
RTE DE CHAVANNES 33
1007 LAUSANNE
Rédaction : Jacques Guélat
Impression : Ruckstuhl, Renens

Info-Ci

Nº 20
décembre 1991

Le mot du délégué

Une grande partie de ce numéro est consacrée à la sécurité informatique. Les responsables de notre Université attachent beaucoup d'importance à ce domaine puisque actuellement un poste est réservé à cette tâche auprès de nos services informatiques.

*La sécurité de l'informatique, on devrait plutôt parler de sécurité de l'**information**, est un concept aux facettes multiples. Vous qui utilisez quotidiennement votre micro-ordinateur, vous souvenez-vous de votre dernière sauvegarde? Ne vous est-il jamais arrivé de quitter votre bureau en négligeant d'interrompre une session de travail sur un ordinateur hôte? Et le mot de passe que vous utilisez pour accéder à l'un ou l'autre des systèmes, saurait-il résister à la perspicacité d'un programme d'identification? Cette liste de questions n'est certes pas exhaustive mais illustre bien toute la complexité de la notion de sécurité.*

Dans le milieu académique, il est souvent très difficile de convaincre les utilisateurs de maintenir une discipline stricte en matière de sécurité de l'information. Il ne s'agit pas d'ériger un mur de protection infranchissable autour de toute information mémorisée sur un des nombreux supports physiques possibles, mais bien de s'assurer qu'en tout instant, cette information puisse être retrouvée et cela évidemment sans aucune altération. Notre environnement informatique actuel est devenu d'une telle complexité que seule une partie est contrôlée par les services centraux. Par conséquent, chaque utilisateur se doit d'assumer ses responsabilités afin de souder les maillons décentralisés de la sécurité de l'information.

Gervais Chapuis

Sommaire

Annexes techniques

Norton Utilities: les vertus d'une bonne installation

Philippe Ryter

Les *Norton Utilities for the Macintosh* forment un ensemble composé de plusieurs applications permettant de diagnostiquer l'état logique d'un disque, de le récupérer s'il a subi un *crash* ou une initialisation accidentelle, de récupérer également des fichiers mis à la corbeille et d'optimiser l'organisation des données enregistrées sur ce disque. Ces utilitaires font de vrais «miracles» et n'ont pas ici un réel besoin de publicité; ce qui est en revanche moins connu, c'est que l'efficacité des options *Format Recover* et *UnErase* de l'application centrale est fortement liée à l'installation correcte d'un programme résident (Init-CDev) appelé **FileSaver**.

FileSaver

Son rôle consiste à mettre à jour deux fichiers de configuration du disque ainsi qu'un fichier contenant les coordonnées des n derniers fichiers supprimés. Cette opération est effectuée automatiquement à l'arrêt de la machine ou à la demande de l'utilisateur. Ces trois fichiers installés au moyen de la procédure ci-dessous sont normalement invisibles et bien entendu inexistants sur le disque dur d'un Mac dépourvu de cet utilitaire.

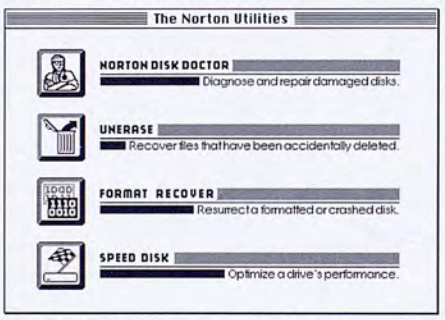
Son principe d'action peut être simplifié de la manière suivante: pour accéder à un fichier sur disque, un ordinateur doit d'abord consulter une «table des matières» lui indiquant la localisation des fichiers. Si cette table est dénaturée, l'accès aux fichiers est évidemment compromis. L'idée du concepteur des *Norton Utilities* est simple: on augmente les chances de récupération d'un disque en dupliquant périodiquement ses informations vitales. C'est le rôle de FileSaver.

Mais n'allez surtout pas en déduire que ces mesures représentent une panacée dans ce contexte de sécurité des données, car FileSaver peut dupliquer des données présentant déjà une dénaturation n'affectant pas immédiatement la bonne marche de votre Mac. Et en cas de crash «matériel» du disque dur, cette belle stratégie est évidemment inopérante; seuls les dommages «logiques» ont une chance d'être réparés.

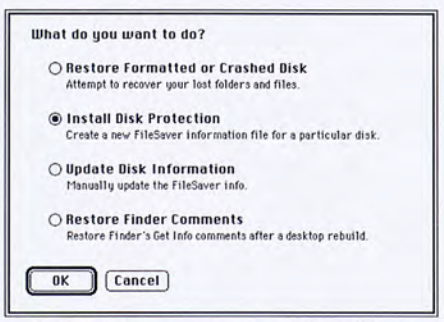
FileSaver ne peut donc en aucun cas se substituer aux mesures de sauvegardes habituelles, mais peut contribuer efficacement à l'augmentation du degré de sécurité d'accès aux données de votre Macintosh. L'auteur de ces lignes reçoit en moyenne 2-3 disques ou disquettes endommagés chaque mois, dont le contenu aurait été plus facilement récupéré si cette mesure de sécurité (objet de cet article) avait été prise à temps.

Voici la marche à suivre pour activer cet utilitaire:

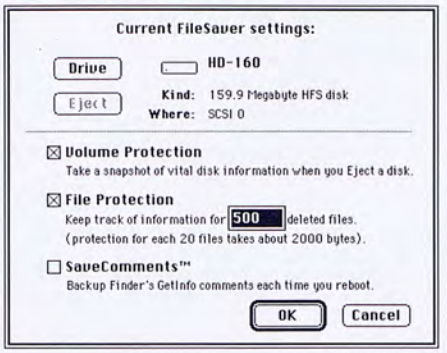
- Placer le fichier FileSaver dans le dossier système puis redémarrer votre Mac.
- Lancer l'application Norton Utilities et cliquer sur le bouton *Format Recover* du menu principal.



- Choisir l'option *Install Disk Protection*.



- Activer les cases à cocher *Volume Protection* et *File Protection* (l'option *Save comments* n'est pas absolument nécessaire).



- Choisir le nombre de fichiers dont on aimerait garder la trace une fois supprimés (prévoir un chiffre suffisamment grand, car les fichiers temporaires créés et normalement éliminés par les applications sont également comptabilisés).
- Choisir le disque-cible et cliquer sur OK. ■

Word Finder et système 7

Philippe Ryter

Dans le numéro précédent d'Info-Ci, nous avions relevé que l'accessoire de bureau Word Finder, permettant d'utiliser le dictionnaire des synonymes, ne fonctionne pas avec le système 7. Cette affirmation est correcte si on installe ce fichier directement dans le dossier menu pomme. Il existe heureusement une autre méthode d'installation permettant d'intégrer ce précieux accessoire directement au niveau de l'application Word. Les opérations suivantes peuvent être effectuées sous système 6.0x ou système 7.0:

- Charger l'utilitaire Font/DA Mover (version 4.1 sous système 7.0).
- Fermer la fenêtre présentant les fontes du fichier système.
- Ouvrer le document Word Finder®~DA dans l'une des deux fenêtres.
- En gardant la touche OPTION enfoncée, ouvrir l'application Word dans l'autre fenêtre.
- Copier l'accessoire et quitter Font/DA Mover. ■

La connectivité des PC: aussi sous Windows!

Ha Nguyen

Travail accompli

Depuis le début de cette année, les PC à l'UNIL ont pu bénéficier d'une solution au problème de connectivité (voir Info-Ci 17). Cette solution se base sur le produit *PathWay* de Wollongong et transforme le PC en un noeud TCP/IP. Elle offre sous DOS 3.3 les services suivants:

- Emulation de terminal par Telnet (client seulement).
- Service de transport pour des émulateurs tiers (par exemple Reflection 4+).
- Transfert de fichier par FTP (serveur et client).
- Partage de fichier par NFS (client seulement).
- Partage d'imprimante par LPR (serveur et client).

En plus du produit logiciel, le Centre informatique s'est occupé du financement et de la distribution des cartes Ethernet pour les PC. Actuellement deux types de cartes sont disponibles: l'un pour le bus ISA (bus qu'on trouve dans les machines du type AT et XT), l'autre pour le bus MCA (bus qu'on trouve dans les machines du type PS/2).

La nouveauté

Le support de ces services dans l'environnement Windows 3 sous DOS 3.3 est devenu une réalité!

- Une nouvelle révision du logiciel PathWay (version 2.0) se trouve déjà sur ULYS.
- Un nouveau guide d'installation sera envoyé à chaque responsable de site. Si vous ne l'avez pas reçu, veuillez téléphoner au secrétariat du Centre informatique (tél 692'23'11).
- Un complément du manuel existant est en cours de réimpression et sera disponible au secrétariat du Centre informatique.

Un certain nombre de limitations existe encore avec ce produit:

- Le serveur FTP ne doit pas être activé en mode de fond (commande "FTPD -b") si l'on utilise Windows 3.
- Le service NFS est valable pour DOS 3.3 et ne tourne pas encore sous DOS 5.0.
- Les services NFS et de partage d'imprimante doivent être complètement activés avant de démarrer Windows 3. Ce qui revient à dire qu'on doit monter les disques virtuels et rediriger les ports d'impression avant le démarrage de Windows.
- Seuls les 3 ports parallèles sont utilisables pour le service de partage d'imprimante.

Le support de DOS 5.0 sera assuré dès que le service NFS fonctionnera, probablement dès le début 92.

Enfin, dans le but d'améliorer le support pour la connectivité PC, le Centre informatique organise un cours d'initiation à ces techniques en mars 92 (voir calendrier en dernière page) et peut mettre sur pied des cours supplémentaires à la demande. En cas d'intérêt, veuillez vous adresser au secrétariat du Centre informatique ou à Jacques Guélat pour les sessions supplémentaires (tél: 692.23.93, e-mail: jguelat@ulys.unil.ch). ■

Connectique depuis le Mac: bonnes nouvelles

Pierre Küffer

Après plusieurs mois de test, le Centre informatique vient d'acquérir la licence de site, pour toute l'Université, d'un émulateur de terminal et d'un logiciel FTP (transfert de fichiers). Sans entrer dans les détails -ces deux nouveaux produits allant faire l'objet d'une présentation détaillée dans le prochain Info-Ci- disons qu'ils sont extrêmement conviviaux, résolvent beaucoup des problèmes actuels et sont particulièrement cohérents avec la stratégie de connectique réseau que le Centre informatique est en train de développer. Ce dernier point laisse augurer d'une évolution et d'une adaptabilité du produit des plus harmonieuses, ce qui est essentiel en matière de réseau, domaine en constante transformation.

Autre avantage, et non des moindres: l'utilisateur va bénéficier de ces deux nouveaux produits sans bourse délier. Conséquence indirecte, l'on peut prévoir une tendance à l'uniformisation en matière d'émulateurs à l'UNIL, ce qui va permettre d'améliorer le support aux utilisateurs. ■

Série Quadra: mise en garde

Philippe Ryter

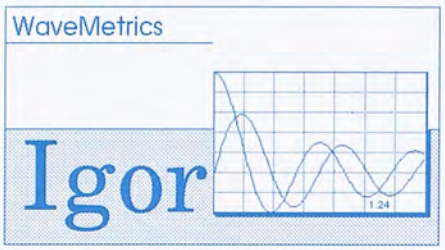
Les derniers nés de la gamme modulaire Apple (Quadra 700 et 900) offrent une puissance deux fois plus importante que celle du Macintosh fx. Ces performances accrues sont dues essentiellement à l'utilisation d'une RAM cache, intégrée au processeur 68040 et activable au moyen d'un utilitaire approprié. Pour bénéficier des atouts de l'architecture de ce nouveau processeur, les applications devront être recompilées; on pourra s'attendre alors à des vitesses de traitements encore plus grandes.

Avec la sortie des modèles si, ci et fx surtout, Apple nous a malheureusement habitué à douter de la compatibilité des programmes sur toute sa gamme de machines. Avant de passer commande d'un Quadra, renseignez-vous si vos programmes tirent réellement profit de toute cette puissance, car la RAM-cache doit être inactivée pour certains comme Excel 3.0 (pour Word 4.0 aussi, mais c'est évidemment moins grave).

On peux même se poser la question si certaines applications opérant très près du *hardware* fonctionnent tout simplement dans ce nouvel environnement. ■

IGOR, outil puissant pour la représentation et l'analyse de données sur Macintosh

Philippe Gardel



Si vous recherchez une solution pour analyser vos données et réaliser des graphiques de qualité à l'aide d'un Macintosh et que vous ne connaissez pas le logiciel IGOR, cette article vous intéressera.

Introduction

Le logiciel IGOR (*Interactive Graphical Operations for Research*) de *WaveMetrics* propose un environnement d'une grande flexibilité pour l'analyse de données et la réalisation de graphiques de précision. Le système présente une excellente intégration entre un puissant langage de commande et l'interface utilisateur du Macintosh. Chaque commande est construite à l'aide de dialogue, activé depuis la barre de menu. La commande peut également être tapée et éventuellement modifiée dans la ligne de commande au bas de la fenêtre principale. Après son exécution la commande et des résultats sont mémorisés et affichés dans la fenêtre principale. Ainsi, au fil des opérations, un historique est constitué, chacune des commandes mémorisées pouvant être facilement amenée dans la ligne d'édition de commande pour la modifier et la répéter. En plus des capacités graphiques et d'un grand nombre de fonctions mathématiques, l'utilisateur dispose d'opérateurs d'analyse sophistiqués tels que la transformée de Fourier, l'intégration, la différentielle et des possibilités d'ajustement par différents types de fonction. Le logiciel présente également des facilités intéressantes de construction de procédures de commandes. Notamment l'utilisateur peut programmer ses propres fonctions et les utiliser dans la routine d'ajustement.

En plus des fenêtres habituelles de dialogue, l'environnement d'IGOR est constitué des 5 types de fenêtres suivants:

- la fenêtre de travail, contient la ligne de commande et l'historique qui peut être commenté et partiellement effacé;
- la fenêtre contenant les procédures;
- les fenêtres d'édition des vecteurs;
- les fenêtres de graphique;
- les fenêtres des pages d'impression.

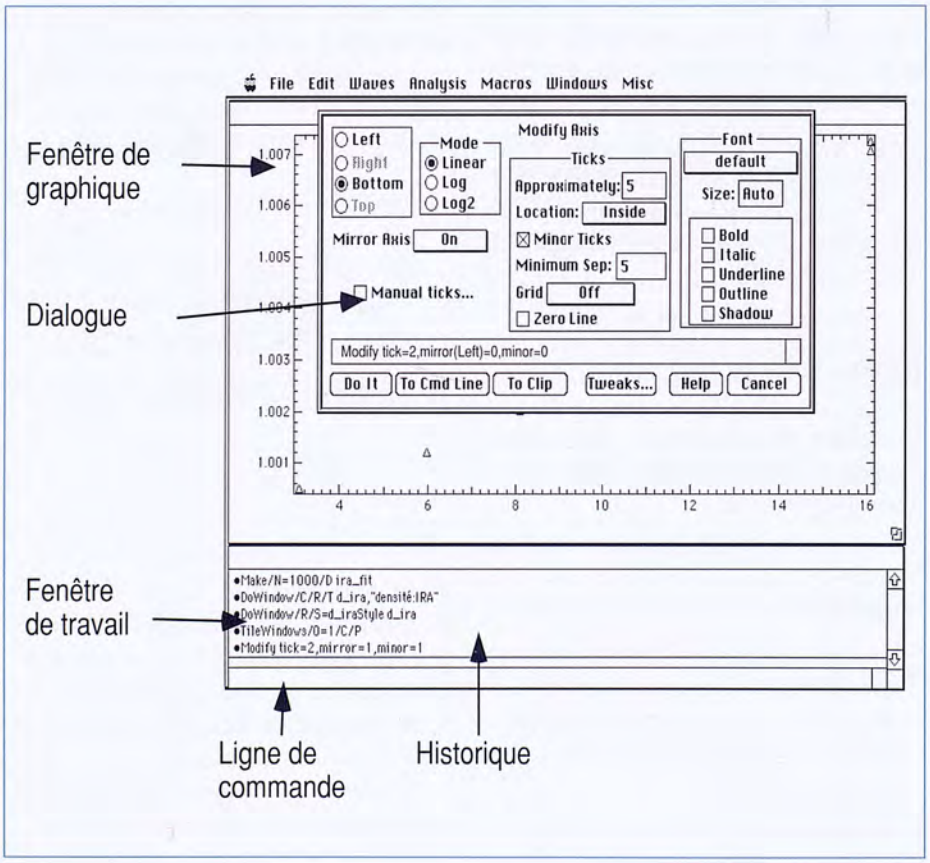
Les trois derniers types peuvent être sauvegardés sous la forme d'une commande macro apparaissant dans la fenêtre de procédure. Les éléments interdépendants sont liés de façon dynamique: après la modification d'un élément, la mise à jour des éléments dépendants est automatique.

Structure et acquisition des données

Les données sont enregistrées dans des vecteurs nommés *waves*. Ces derniers peuvent contenir des nombres réels ou complexes et comprennent une information d'échelle. Après une opération de définition, ils peuvent être entrés manuellement de la même façon que dans un tableur. L'importation de données provenant d'autres logiciels peut se faire par l'intermédiaire de fichier en format texte. Des extensions sous forme de ressources externes (XOP) permettent d'importer directement des fichiers de certains logiciels, notamment EXCEL 2.2, CRICKET, et LABVIEW.

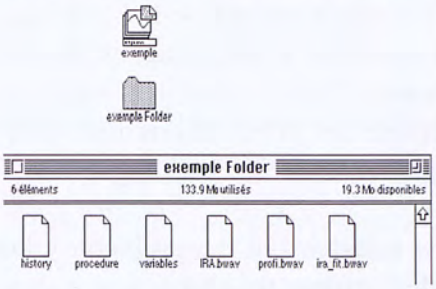
Sauvegarde d'une session

L'enregistrement d'une session de travail est possible à tout moment. Les documents sauvegardés lors de cette opération sont constitués d'un fichier texte contenant les



Environnement de travail avec le logiciel IGOR

commandes nécessaires à la reconstruction de la session et d'un dossier contenant l'historique et les procédures (fichiers texte) et les *waves* (fichiers binaires).



Structure d'une sauvegarde

Aide et documentation

En plus d'un manuel d'utilisation de bonne qualité, le logiciel offre une aide en ligne contenant quasiment tout le manuel. L'accès peut se faire soit directement à tout le fichier soit par l'intermédiaire d'un index. L'utilisateur peut également obtenir directement de l'information relative à l'opération courante.

WavesMetrics propose également de la documentation sur différents sujets, sous forme de dossier de notes. Chacune d'entre elles contient généralement un fichier de texte explicatif et une session IGOR d'exemples, source de procédures utiles.

Si ce logiciel vous intéresse...

Sachez que le logiciel IGOR, sans la boîte à outils de fonctions externes, revient à environ Frs 750.-

Si vous avez envie d'essayer ce logiciel, une version de démonstration est disponible sur le *serveur-CI* (nom *UNIL*, mot de passe *unil*), disque *UNIL*, dossier *Démos*. Après avoir ouvert le dossier *IGOR*, un double clic sur

vous permettra d'installer chez vous la version démo et l'application

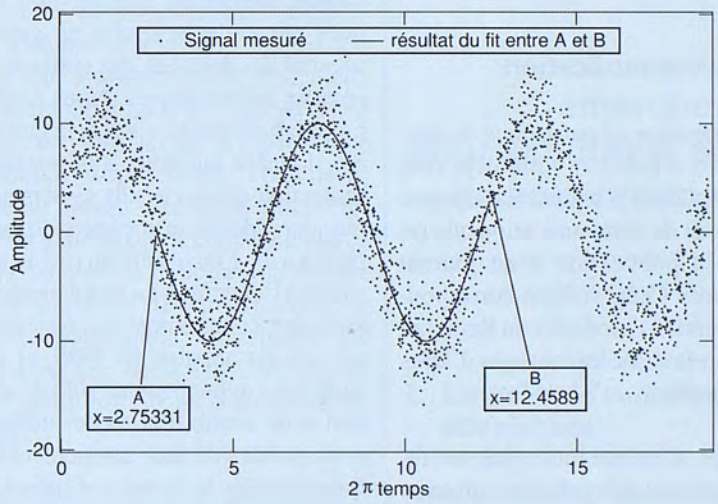
installera des notes. Prévoyez environ 2.5 MB d'espace disque pour procéder à cette installation.

Pour de plus amples informations, contactez le sussigné. ■

Exemple graphique

Pour illustrer une partie des possibilités, voici les commandes et les résultats générés par l'analyse de la mesure simulée d'un signal sinusoïdal:

```
•|ENTREE DES DONNEES
•Make/N=2048/D mesure,mesure_fit
•SetScale/I x 0,6*pi,"" mesure,mesure_fit;
•mesure=10*sin(x+pi/9)+gnoise(2.5)
•|AFFICHAGE GRAPHIQUE DES DONNEES
•Display mesure
•Modify mode=2
•|AJUSTEMENT
•CurveFit/B=700 sin mesure(xcsr(A),xcsr(B)) /D=mesure_fit
 Fit converged properly
 mesure_fit= K0+K1*sin(K2*x+K3)
 K0= -0.00532624;K1= 10.0051;K2= 1.00508;K3= 0.330095;
 V_chisq= 6252.06; V_npnts= 1055;
 V_numNaNs= 0; V_numINFs= 0;
 W_sigma={0.0792,0.113,0.0036,0.0296}
•AJOUT D'ELEMENTS GRAPHIQUES
•Append mesure_fit
•Modify lsize(mesure_fit)=0.5
•Modify tick=2,mirror=1,axThick(bottom)=0.5
•Label bottom "\[02 \F'Symbol'p\M\F]0 temps"
•Label left "Amplitude"
•Legend/J /M/A=MC "\s(mesure) Signal mesuré\t\s(mesure_fit)
résultat du fit entre A et B"
•Tag /M/L=1 mesure, xcsr(A), "\JC\Z09A\r\Mx=\OX "
•Tag /M/L=1 mesure, xcsr(B), "\JC\Z09B\r\Mx=\OX "
•DefaultFont/U "Helvetica"
```



Errata Phaser

Pierre Küffer

Une erreur typographique s'est glissée en page 4 de l'Info-Ci n°19 (septembre 1991) dans l'article intitulé: "Une nouvelle imprimante couleur !". La première ligne des paragraphes à inclure dans le fichier *Printcap* des machines UNIX doit être modifiée comme suit (remplacer ":" par "|"):

Pour un accès PostScript:

```
PhaserPS|pscolor:\
        :lp=:\
        :rm=ciphaser:
        :rp=PHASERPXPS:\
        :mx=#0:\
        :sd=/usr/spool/lpd
```

Pour un accès HPGL :

```
PhaserHPGL|HPGLcolor:\
        :lp=:\
        :rm=ciphaser:
        :rp=PHASERHPGL:\
        :mx=#0:\
        :sd=/usr/spool/lpd
```

■

DOSSIER : Sécurité

Nous abordons aujourd'hui dans le dossier un élément crucial du développement harmonieux de l'informatique à l'Université: **la sécurité**. Malgré sa consonnance rébarbative dans un milieu académique, ouvert par définition, ce terme couvre une dimension qu'on ne peut se permettre d'ignorer à l'heure actuelle. Les méfaits d'une carence de cet élément sont mesurables quotidiennement: panne de disque dur, effets malins d'un virus, perte involontaire de fichiers, piratage de logiciel, usurpation du mot de passe, ... La liste est longue.

Plusieurs mesures ont déjà été prises par le Centre informatique pour parer à certains de ces problèmes. De nombreux articles parus dans ce journal vous ont sensibilisé à cet aspect de l'informatique et le font encore aujourd'hui. Nous abordons le sujet d'une manière plus globale dans ce dossier. En complément, les annexes techniques fournissent un guide de recettes individuelles simples permettant d'augmenter significativement le niveau de sécurité.

La sécurité informatique est-elle compatible avec la liberté académique ?

Pascal Jacot-Guillarmod

Oui à la communication

Dans son message de parrainage du premier numéro d'Info-Ci, voilà déjà cinq ans, M. P. Ducrey saluait la volonté d'ouverture et de communication que représentait la publication d'un journal d'information. Cette volonté correspondait aux intentions générales du Rectorat, qui a toujours favorisé les échanges d'idées et d'informations.

Cet échange d'informations fait un recours chaque jour plus grand à l'informatique, que ce soit pour la saisie et la mise en forme des données, pour leur traitement et leur transport, ou encore pour leur sauvegarde. A chaque étape, on doit se préoccuper de sécurité, afin que les données, sur lesquelles des décisions seront prises ou des résultats publiés, soient fiables. Par données fiables, nous entendons des données disponibles en tout temps, et dont l'intégrité et la confidentialité sont garanties. La disponibilité implique des systèmes et des réseaux en exploitation continue et dont le taux de pannes tend vers zéro. L'intégrité est assurée par des mesures de sauvegarde, pour pallier à toute perte accidentelle. La confidentialité est elle garantie par un ensemble de mesures de contrôle d'accès aux niveaux réseaux, systèmes et applications.

Protection des données, des systèmes et des réseaux

Depuis longtemps, des mesures techniques ont été prises, afin de garantir la sécurité des données, des systèmes et des réseaux informatiques. Nous nous sommes d'abord préoccupés de la sauvegarde des données qui nous sont confiées. La protection des accès aux systèmes via le réseau est devenue une seconde préoccupation avec l'ouverture du réseau universitaire à l'extérieur. La problématique des virus qui contaminent les systèmes personnels est apparue en 1989, et tout de suite nous avons joué un rôle d'information et de sensibilisation des utilisateurs, responsables de leur équipement décentralisé. Enfin le Service d'informatique administrative a incorporé la sécurité comme critère de qualité primordial dans les développements d'applications au service de la gestion.

Un dossier consacré à la sécurité

La signification de la sécurité dans le domaine informatique a profondément évolué ces dernières années. Plusieurs facteurs y ont contribué.

Le développement foudroyant des réseaux transforme tout guru des systèmes, qu'il soit à son domicile à Yverdon ou devant son PC à Adélaïde, en pirate potentiel et amène ce pirate à votre porte. Le développement de l'informatique dans le domaine de la gestion a nécessité la connexion au réseau d'ordinateurs renfermant des données sensibles. Le caractère confidentiel de certaines informations rend alors les abus et le piratage plus tentants. Enfin la connaissance des utilisateurs dans le domaine des systèmes a notablement augmenté depuis l'apparition de système décentralisé qu'il faut gérer soi-même. Cela rend le travail de protection plus difficile, et un responsable système qui n'a pas eu à déplorer un abus malveillant fait office d'exception.

Cette nouvelle situation dans le domaine de la sécurité informatique fait que les mesures techniques ne sont plus suffisantes. Comme réponse à ce nouveau problème, des mesures organisationnelles et une sensibilisation accrue des utilisateurs sont indispensables.

L'ouverture: la responsabilité de chacun

Toute personne qui a besoin de l'accès aux ressources informatiques dans son travail possède une clef d'accès aux systèmes d'information scientifiques ou administratifs. De l'usage qu'il sera fait de ces clefs dépendra le degré d'ouverture qu'il sera possible de maintenir. Il est dans l'intérêt de chacun que cette ouverture soit la plus large possible, afin de garantir les échanges nécessaires à la vitalité de notre domaine académique. ■

La vulnérabilité de l'information

Anik Bossuat

L'évolution de l'informatique, principalement dans les domaines des communications et de la micro-informatique, offre la possibilité à toute entreprise (petite, moyenne ou grande), depuis une quinzaine années, d'accéder à l'information, de la traiter et de la véhiculer. Par information on entend ici logiciels, données, messages, documents informatisés.

L'information sur un site universitaire ou dans une entreprise passe au travers d'outils de création, de traitement, de stockage et de transport. Par là même, l'information devient vulnérable. C'est en portant un regard sur les notions de qualité, de temps, de valeur et d'éthique que nous comprendrons mieux ce qu'est en réalité la vulnérabilité de l'information.

Notion de qualité

La qualité de l'information découle des trois critères de *disponibilité* (accessible en tout temps), *d'intégrité* (référence à l'état de l'information qui se doit d'être complet, correct et inchangé depuis sa dernière vérification) et de *confidentialité* (accessible uniquement par une personne ou un groupe de personnes prédéfinies).

Notion de temps

La notion de temps intervient dans le cas d'incidents et elle se concrétise par la question: «combien de temps puis-je supporter de ne pouvoir accéder à mon information (reconstitution de données suite à un effacement malheureux, une panne de réseau ou du système, une surcharge du système, du réseau, etc...) sans que mon travail en soit perturbé?»

Notion de valeur

La valeur de l'information va orienter notre stratégie en matière de sécurité. En effet dès que notre information ne répond plus aux critères de qualité (intégrité, disponibilité, confidentialité), des conséquences plus ou moins graves peuvent apparaître. Le tableau ci-dessous nous montre le rapport entre la valeur de l'information et les conséquences qui en résultent:

Valeur	*Conséquence*
Stratégique?	➨ Projet en péril
Critique?	➨ Perte inacceptable.
Sensible?	➨ Seuil critique.
Faible?	➨ Petites nuisances.
Nulle?	➨ Perte insignifiante.

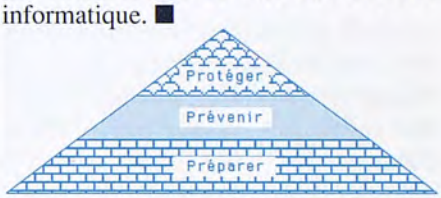
Notion d'éthique

La création de règlements est un frein à la liberté et constitue une lourde charge administrative. Seul le comportement de chacun d'entre nous peut éviter cette entrave. A ce titre, on peut mentionner la confidentialité du mot de passe ou du code de la carte permettant l'accès au réseau depuis un téléphone personnel, la connexion de matériel au réseau effectuée exclusivement par le Centre informatique, la fermeture correcte de vos accès aux ressources informatiques (applications, systèmes et réseaux), la signalisation de tout fonctionnement défectueux d'un équipement ou d'un logiciel. Pour terminer, on pourrait citer la copie illicite de logiciel, trop souvent considérée comme un moyen normal de réduire les coûts. En général on ne considère pas ce piratage comme un délit dans la mesure où un exemplaire a été dûment acquis; or ceci n'est valable que si l'exemplaire a été acquis avec une licence de site ou une licence multi-utilisateurs (voir encart ci-dessous).

C'est en fonction de la prise de conscience de toutes ces «notions» et du comportement de chacun que se construit la sécurité. Le petit Larousse définit la sécurité comme suit :

"Confiance, tranquillité d'esprit résultant de la pensée qu'il n'y a pas de péril à redouter".

Que nous soyons du monde "académique" ou du monde "administratif", nous sommes tributaires de la vulnérabilité de l'information. La variété des risques nécessite une approche globale et systémique. Cette nécessité d'une analyse globale, cohérente et très structurée devient primordiale, fondant ainsi les bases d'une discipline nouvelle: la sécurité informatique. ■



Penser sécurité c'est...

Préparer, Prévenir pour Protéger

Protection du logiciel

La directive européenne relative à la protection du logiciel a été votée le 14 mai dernier. Les ministres des Douze ont opté pour l'application du droit d'auteur au logiciel. Cette couverture s'appliquera dans l'ensemble des pays de la communauté dès le 1er janvier 1993. La décompilation (reverse engineering) ne sera autorisée que sous certaines conditions pour assurer l'intéropérabilité (interfonctionnement) de diverses applications.

Démarche pour assurer la sécurité de son information

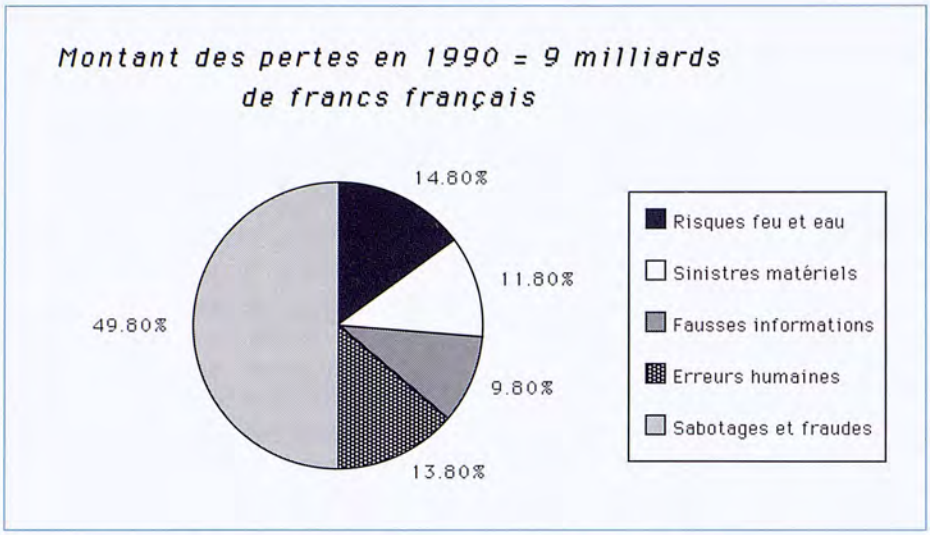
Anik Bossuat

1. La prise de conscience des risques

Alors que plus de 50% des données vitales pour les entreprises sont stockées sur ordinateur, on constate que la sécurité informatique est défaillante: soit nous sommes inconscients des risques, soit nous refusons de les envisager.

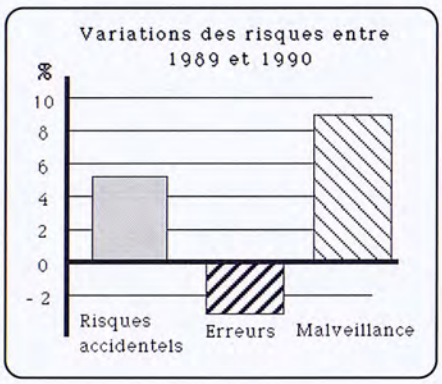
Pourtant les risques sont présents: pertes ou modifications de données, panne du matériel ou du logiciel, destruction du matériel ou du logiciel, négligence du personnel informatique ou de l'utilisateur, piratages, virus etc...

Les graphes ci-après en provenance de l'APSAD (Assemblée Plénière des Sociétés d'Assurance Dommages) nous



Répartition des pertes subies en France en 1990

montrent la répartition des pertes subies dans le domaine informatique au cours de l'année 1990 en France, ainsi que l'évolution des risques majeurs entre 1989 et 1990.



L'évolution des risques majeurs entre 1989 et 1990

Il est à noter qu'en Allemagne ces chiffres sont équivalents. Malheureusement, en Suisse aucun organisme n'a pu établir de statistique.

2. La volonté d'agir

Avec l'explosion de la télématique, la nécessité de protéger les systèmes d'informations a fait naître des standards de sécurité, des lois et des méthodes (Marion, Melisa, Incas, Arome, etc...). Gouvernements puis constructeurs ont manifesté leur volonté d'agir.

Certaines entreprises gèrent encore les sinistres au fur et à mesure qu'ils se produisent... D'autres par contre, ont pris conscience de l'existence de risques potentiels et ont la volonté d'agir pour maîtriser ces risques de manière objective et cohérente. Celles-ci considèrent que l'étude de sécurité doit être gérée comme un projet. Ce projet ne peut être mené avec profit que s'il a été décidé par la Direction de l'entreprise, si celle-ci s'implique véritablement et si l'ensemble du personnel y collabore.

Le choix des décisions qui assure le développement de l'entreprise, en évitant que ne surviennent des sinistres, doit être fait en connaissance de cause; c'est le rôle des méthodes quantitatives de gestion des risques défini sous le terme de méthodologie.

3. La mise en oeuvre d'une méthodologie

La méthodologie choisie doit préserver la qualité de l'information en conservant sa disponibilité, son intégrité, sa confidentialité.

Les niveaux de l'*Orange book*

Huit niveaux de sécurité, adoptés universellement, ont été définis par NCSC(*National Computer Security Center*, branche du département de la défense américaine) dans un ouvrage intitulé *"Department of Defense Trusted Computer System Evaluation Criteria"* plus communément connu sous le nom de ***"Orange book"***. La liste établie va de l'absence de sécurité à la protection totale:

D Protection inexistante; on trouve ici tous les systèmes qui ne réussissent pas à se faire agréer aux niveaux supérieurs.

C Le système possède des fonctions permettant de contrôler l'accès aux données, mais l'utilisateur est libre de les utiliser, toutes ou certaines, ou d'en négliger l'usage: c'est la protection «à discrétion».

C1 L'accès aux données et aux programmes est limité à certains utilisateurs, ceux-ci étant parfaitement identifiés.

C2 La séparation totale est exigée entre le système de sécurité et les données et programmes accessibles par les utilisateurs; le contrôle des accès est strict, et le travail des opérateurs est enregistré; à ce stade, un administrateur de système devient indispensable.

B1 Toute connexion au système fait, obligatoirement, l'objet d'un contrôle; hiérarchisation de la confidentialité des fichiers accessibles (programmes et données); Impossibilité, pour les utilisateurs, de définir ou redéfinir eux-mêmes les autorisations d'accès.

B2 Le système de sécurité doit être modulaire; analyse systématique des flux de données; tests de sécurité «en grandeur naturelle»; formulation mathématique du système de sécurité; contrôle total de l'élaboration de système de sécurité; morcellement de la fonction d'administrateur-système.

B3 Le système de sécurité est distillé: d'un côté, les procédures courantes, de l'autre, le noyau «sensible», facilement contrôlable.

A Le système de sécurité doit être mathématiquement certifié (ce n'était pas encore le cas en mai 1989)

Référence: "Safe and secure?" par Patrik Wood, BYTE, mai 1989, pp 253-258

La mise en oeuvre de la sécurité pour les systèmes d'informations se traduit par un certain nombre d'actions qui touchent aux domaines de :

- la sécurité physique
- la sécurité d'exploitation
- la sécurité du développement des applications
- la sécurité d'organisation
- la sécurité des sauvegardes avec plan de secours

Les études spécialisées dans chacun de ces domaines suivent la démarche d'un schéma directeur de sécurité des systèmes d'informations. L'objectif du schéma directeur est de proposer une liste de mesures assurant la hiérarchie de la *protection* (degré de protection optimale du petit risque au grand risque) et l'homogénéité de la *prévention* (diminution des petits risques à fréquence élevée). Ces deux types de mesures doivent tenir compte des contraintes techniques et financières, ainsi que du rapport qualité/coût des facteurs sélectionnés.

La méthodologie se compose:

- d'un **audit de sécurité**.

  L'audit consiste à radiographier, à un temps t, l'état d'un domaine. Le rapport de l'audit répertorie les points vulnérables et propose des recommandations pour que des actions (les plus urgentes) puissent être effectuées.

- d'un **catalogue**.

  Le catalogue est créé à partir du rapport de l'audit. Chaque point vulnérable décelé à l'audit, ainsi que chacune des recommandations sont l'objet d'une étude qui doit aboutir à des mesures de prévention et de protection. Celles-ci seront proposées à la Direction qui prendra éventuellement la décision d'engager leurs réalisations.

- d'un **modèle**.

  Le catalogue final va permettre la création d'un modèle (consolidation des mesures par leurs actualisations périodiques).

Prévoir et non subir,

tel est finalement l'objectif de cette démarche quantitative et structurée. ■

Etat d'avancement des travaux de sécurité à l'Université

Anik Bossuat

A l'Université, les deux premières démarches, la «prise de conscience des risques» et la «volonté d'agir» sont des faits établis, si nous nous référons au travail effectué au cours des années 1989-1990. Des documents de sensibilisation ont été adressés au Rectorat, ce qui a eu pour conséquence la création d'un poste d'*ingénieur sécurité*. Suite à cela, un *Comité de sécurité* a été créé (voir ci-après) et des directives ont été entérinées par ce même comité. Les règles d'utilisation des serveurs données plus loin en fournissent un exemple concret.

Etant donné l'envergure de la mise en oeuvre de la sécurité des systèmes d'information au sein de l'Université, il était important, dans le cadre de la troisième démarche (la «méthodologie»), de cerner dans l'immédiat les degrés de vulnérabilité dans les domaines dits «vitaux» (matériels informatiques et réseaux). Ces domaines ont fait l'objet d'un audit réalisé avec la collaboration de Digital Equipment Corporation.

Ce travail représente la première étape de cette troisième démarche. Il s'est déroulé durant le premier semestre 1991. La deuxième étape, étude détaillée de l'ensemble des risques à l'Université, ouvrira un chantier début 1992.

Résultats de l'étape 1

Les conclusions de l'audit prouvent que le niveau de sécurité des domaines «radiographiés» est élevé, le Centre informatique ayant déjà effectué un travail considérable dans le cadre de la sécurité. Elles relèvent aussi la qualité des connaissances et du travail du personnel de ce département.

Néanmoins quelques points faibles restent à améliorer. En particulier, l'audit a fait ressortir deux lacunes importantes pour assurer la **qualité** de la sécurité:

- le manque de personnel et d'outils pour gérer, surveiller l'énorme infrastructure informatique (systèmes et réseaux).
- le manque de sensibilisation des utilisateurs aux problèmes liés à la sécurité.

D'autre part, des mesures techniques complémentaires permettent l'amélioration de la sécurité et peuvent être envisagées à court terme par les responsables des systèmes et du réseau ou à plus long terme, impliquant alors une étude pour leur réalisation. Ces dernières ont fait l'objet de recommandations dans l'audit. Le comité de sécurité les a étudiées dans le détail, puis les a soumises au Rectorat pour décision.

En conclusion j'aimerai exprimer l'espoir de voir chacun des membres de l'Université participer spontanément au vaste projet qu'est la sécurité informatique. Paul Béraud, président de l'APSAIRD (Assemblée Plénière des Sociétés d'Assurances contre l'Incendie et les Risques Divers), a dit: *«Les risques informatiques constituent indéniablement un important thème de réflexion dès lors que l'on s'interroge sur le fonctionnement de la société de demain»*. ■

Les 7 du comité de sécurité

Jacqueline Reigner

L'Université est sensible à l'importance de son informatique. Dans la recherche ou dans l'administration, nous sommes tous également vulnérables face à une épidémie de virus informatiques, à une panne d'ordinateur ou à la perte de données précieuses. L'ordinateur et les télécommunications sont devenus les outils indispensables à grand nombre d'activités quotidiennes. Les pannes accidentelles, les erreurs et les actions malveillantes visant le système d'information constituent un danger permanent que l'Université doit maîtriser.

La sécurité est de moins en moins une affaire de spécialistes. La décentralisation, l'intégration des micro-ordinateurs et les réseaux sont autant de facteurs impliquant des modalités nouvelles de gestion

de la sécurité. L'Université a pris conscience que la sécurité est un sujet sérieux qui doit préoccuper chacun dans des situations aussi différentes que l'engagement de personnel, la construction des bâtiments ou l'accès à un ordinateur, par exemple. La sécurité n'est plus seulement l'affaire de la salle des machines, mais elle est bel et bien celle de tous les membres de l'Université.

Afin de disposer en tout temps d'une structure compétente, un *comité de sécurité* a été constitué. Son rôle est de veiller sur l'ensemble des facteurs dont dépend la sécurité informatique. Animé par Jacqueline Reigner, responsable du Service d'informatique administratif, le comité est constitué d'Anik Bossuat, ingénieur sécurité, du professeur Gervais Chapuis, délégué du rectorat à l'informatique, de Claude Cuendet, chef de la chancellerie du Rectorat, de Solange Ghernaouti, professeur d'informatique en HEC, d'Edith Huber, concepteur-analyste et de Pascal Jacot-Guillarmod, chef du Centre informatique. Le comité de *sécurité* est chargé d'évaluer la situation actuelle et d'élaborer un plan d'action pour que la sécurité du système d'information de l'Université réponde aux exigences actuelles. ■

UNIVERSITE DE LAUSANNE
DELEGUE DU RECTORAT A L'INFORMATIQUE

Règles d'utilisation des serveurs dédiés à l'informatique académique des domaines scientifique et administratif.

L'université de Lausanne dispose de deux serveurs informatiques centraux, l'un dédié au domaine scientifique et l'autre à la gestion administrative. Ces deux serveurs sont gérés par le Centre informatique.

1 - **En signant les formulaires** «Demande de création d'un username pour l'utilisation des ressources du Centre informatique» **ou** «Demande d'accès au système d'information», **tout utilisateur s'engage à ne travailler sur les serveurs gérés par le Centre informatique (Ci) que dans les conditions décrites ci-dessous:**

2 - Responsabilité de l'utilisateur
Bien que le Centre informatique fasse tous ses efforts pour assurer la sécurité des données, notamment au travers des changements de version du système d'exploitation ou de pannes, l'utilisateur fera des copies de sécurité de ses fichiers critiques sur supports externes (bandes magnétiques, cassettes, etc...). **Tout utilisateur est responsable de la sécurité et de la confidentialité de ses données et de son ou ses mots de passe**.

3 - Mot de passe
L'utilisateur veillera à ce que son mot de passe ne soit pas identique à son Username, à son nom ou son prénom ou un nom qui pourrait être facilement connu de quelqu'un d'autre. L'utilisateur ne l'écrira sur aucun support matériel. **Il est intransmissible à des tiers.**

4 - Username
Le **Username** transmis à l'utilisateur qui en a fait la demande en bonne et due forme, **est unique et intransmissible à des tiers.**

5 - Réseaux
a) - Afin de garantir une protection de nos moyens informatiques contre les abus par des tiers, **tous les accès**, - entre ordinateurs et réseaux de l'Université et les réseaux externes publics ou autres- , **doivent impérativement être effectués avec du matériel distribué par le Centre informatique qui fixe les normes d'accès et de sécurité.**
b) - La carte «Passkey» reçue pour accéder aux réseaux de l'Université depuis les réseaux publics des PTT est personnelle. Son code d'accès (no d'identification) est confidentiel.

6 - Fonctionnement défectueux
Le fonctionnement défectueux d'un équipement ou d'un logiciel doit être annoncé le plus rapidement au Centre informatique.

7 - Droit du Centre informatique
a) Le Centre informatique se réserve le droit d'empêcher l'accès sur ses installations à tout utilisateur potentiellement susceptible de mettre en péril la sécurité des systèmes.
b) Toute personne utilisant de manière abusive des mots de passe, données ou programmes appartenant à d'autres utilisateurs ou aux exploitants des installations, s'expose à des poursuites.

Nous remercions nos collègues de l'EPFL de leur conseil.

UNIX: prévention de base contre les intrus

Michel Müller

Le développement des moyens de télécommunication permet aujourd'hui à l'utilisateur UNIX d'accéder de manière simple et quasi-instantanée à toute machine distante connectée au réseau sous TCP/IP: il lui suffit pour cela de connaître le nom ou l'adresse IP de la machine qu'il désire atteindre. Cette facilité fort appréciée exige en contrepartie un minimum de sécurité sur les ordinateurs afin de prévenir toute tentative d'intrusion de la part d'utilisateurs non-autorisés.

En guise de préambule, relevons que le système UNIX a été développé en partie dans le universités américaines sur un concept alliant ouverture et simplicité d'utilisation: cela fait d'UNIX un système qui est «par défaut» relativement peu sécurisé. UNIX est en revanche hautement configurable, et c'est au responsable de la machine qu'il appartient d'ajouter au système le minimum de sécurité requis. Les aspects de la sécurité d'un système informatique étant multiples, nous nous bornerons à donner ici quelques recommandations permettant de maintenir une sécurité minimale sur les machines UNIX.

Sécurité côté utilisateur

Chemin d'accès - La référence au répertoire courant (.) doit toujours apparaître comme dernier élément du *pathname* . On gagne ainsi l'assurance que ce sont bien les commandes UNIX originales qui sont exécutées et non pas une version piégée introduite par un intrus qui souhaite s'approprier les mots de passe. Pour root , la référence au répertoire courant est à bannir **absolument** du *pathname* .

Protection des fichiers - Il appartient à l'utilisateur de protéger lui-même ses informations en choisissant un code de protection approprié. Ceci peut être réalisé de manière automatique au moyen de la commande *umask* qui définit le code par défaut utilisé à la création de fichiers et de répertoires. La valeur de *umask* fixée à 022 assure une protection minimale.

Mots de passe - Il s'agit de la voie d'intrusion privilégiée des *hackers*, donc celle qui, sur tout système, doit faire l'objet des plus grandes précautions. Sous UNIX les mots de passe sont encryptés par une fonction non inversible liée au nom de code de l'utilisateur. Malheureusement, le fichier contenant ces mots de passe encryptés peut être lu par tout utilisateur déclaré. Sur les systèmes SUN et HP il est toutefois possible de masquer ces informations en implémentant le niveau de sécurité C2 (voir *Orange book* en page 8).

On trouve aujourd'hui, pratiquement dans le domaine public, des programmes qui tentent de "casser" le mot de passe en comparant les versions encryptées de mots probables avec celles du fichier /etc/passwd. Il importe donc que le mot de passe soit convenablement choisi. Les quelques règles simples données en annexe technique sont valables pour le monde UNIX et sont à respecter absolument.

Sécurité côté système

Comme mentionné plus haut, des lacunes de sécurité existent de manière native dans la majorité des systèmes UNIX et c'est au responsable-système qu'il appartient de les combler en appliquant les recommandations suivantes:

Accès root distants - Les UNIX de type BSD permettent de limiter les accès distants en mode *superuser*. Pour ce faire, réduire au minimum les connexions du type *secure* dans le fichier */etc/ttytab* (il est possible de les supprimer toutes, même pour la console). Ceci contraint toute personne à utiliser la commande *su* pour travailler en mode privilégié, et laisse une trace de son passage dans le fichier d'audit.

Fichiers /.rhosts et /etc/hosts.equiv - L'existence de tels fichiers constituent un danger permanent sous UNIX et leur usage doit être limité au minimum. En particulier, ne jamais utiliser l'option «+» qui ouvre complètement le système.

Fichiers spéciaux - Les droits d'accès et de propriété des fichiers spéciaux (répertoire */dev*) doivent être définis correctement. Ceci est particulièrement important pour les devices *kmem* et *mem* qui représentent la portion de mémoire réservée au noyau, respectivement la totalité de la mémoire. La lecture de ces fichiers est limitée à *root*, leur propriétaire, et au groupe *kmem* uniquement.

Programmes privilégiés - Ces programmes, exécutables par tout utilisateur, doivent pouvoir disposer de privilèges particuliers pendant leur exécution. Ils bénéficient à cet effet d'un statut spécial, dénommé *setuid* : c'est le cas, par exemple, du programme d'impression *lpr*. Précautions: vérifier régulièrement le nombre et l'emplacement des programmes *setuid* qui ne doivent jamais apparaître dans une zone d'accès public. Ne jamais utiliser de *shell script* ayant le statut *setuid*, trop faciles à piéger.

Démons non-surveillés - Historiquement, les implémentations traditionnelles d'UNIX comprennent un certain nombre de *daemons* présentant de grandes lacunes de sécurité. Ces *daemons* étant souvent peu, voire pas du tout utilisés il est recommandé de les désactiver. Pour ce faire commenter dans le fichier /etc/inetd.conf les lignes correspondant à *tftp* , *rexec* , *uucp*, *systat* , *netstat* et *rusers*. Relancer ensuite le procès *inetd* pour valider les modifications.

Mise à jour - Les systèmes livrés par les divers constructeurs ne cessent de s'améliorer, notamment sur le plan de la sécurité. Il est donc recommandé d'installer au plus tôt toute nouvelle release et surtout les *patches* liés à la sécurité lorsqu'ils sont documentés.

Pour terminer ...

La sécurité absolue n'existe pas. Cependant en appliquant les recommandations précitées, il est possible d'améliorer de manière sensible la sécurité d'UNIX. Notons par ailleurs une évolution (réjouissante ?) vers un système mieux protégé puisque que tant Open Software Foundation avec OSF/1 que ATT avec System V Release 4/ES (= *Enhanced Security*) annoncent pour bientôt un UNIX certifié aux niveaux B et C de l'*Orange Book* (voir dossier pour des informations à ce sujet). ■

Aide aux utilisateurs de système UNIX

Michel Müller

Les personnes de l'Université qui désirent soumettre au Centre informatique leurs questions relatives à l'utilisation ou l'exploitation de systèmes UNIX peuvent le faire actuellement en utilisant les canaux suivants:

- Les personnes possédant une station UNIX ou ayant un accès aux ressources centrales peuvent envoyer un message à ASSIST sur les machines centrales à l'adresse:

  `assist@ulys.unil.ch`

  Au Centre informatique, les messages sont redirigés vers les collaborateurs concernés qui s'efforcent d'y répondre dans les meilleurs délais.

- Les utilisateurs qui ne possèdent aucun accès à une messagerie électronique (VMS-MAIL ou SMTP) peuvent appeler aux numéros de téléphone suivants:

  Michel Müller 692'23'38
  Alexandre Roy 692'23'10

D'une manière générale il est préférable d'utiliser en priorité le courrier électronique pour poser vos questions. Cela facilite d'une part l'organisation du travail des personnes chargées d'y répondre et d'autre part, ne dit-on pas qu'un problème bien posé est déjà à moitié résolu? ■

Résultats de l'enquête UNIX

Jacques Guélat

L'évolution exponentielle du nombre stations de travail UNIX sur le campus a incité le Centre informatique à prendre dès 1989 des mesures destinées à étoffer de manière significative ses prestations dans ce domaine. Le dossier du numéro 18 d'Info-Ci a été consacré à la description de ces mesures. Dans le présent article, nous exposons les résultats de l'enquête qui a été effectuée au mois d'août dernier auprès de tous les responsables de sites équipés de machines UNIX. Le but de cette enquête consistait à mieux cerner les besoins réels des utilisateurs de l'Université et à maximiser la pertinence des moyens mis en oeuvre par le Centre informatique.

L'enquête

Le questionnaire distribué contenait une première partie descriptive qui a permis d'établir un état de la distribution des machines UNIX à l'UNIL. Une deuxième partie proposait une liste de prestations pouvant être offertes par le Centre informatique. Chaque responsable avait alors la possibilité d'indiquer ses priorités et de signaler tout service qu'il jugeait important d'obtenir.

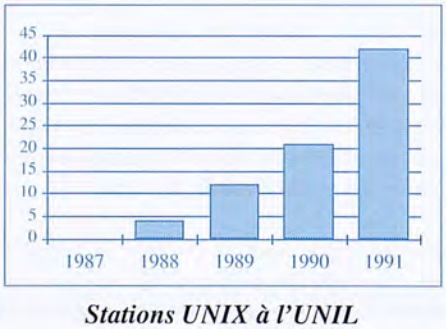
La récolte des réponses

Afin de préciser si nécessaire les besoins exprimés, une visite a été effectuée par Michel Müller, responsable au Centre informatique des systèmes décentralisés, auprès de toutes les personnes contactées.

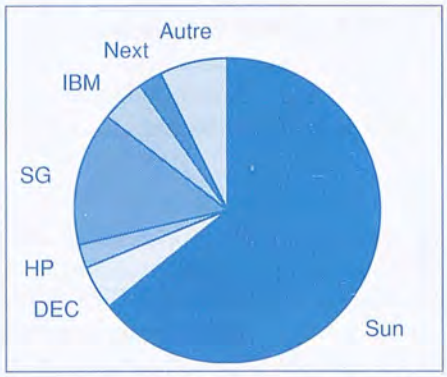
Début septembre, 11 questionnaires étaient rentrés permettant de procéder à un premier dépouillement. Ces 11 questionnaires représentent 11 sites différents pour un nombre total d'une centaine d'utilisateurs UNIX potentiels. Fin septembre l'enquête a été considérée comme terminée, 14 questionnaires ayant été récupérés. Les trois derniers relevés n'ont pas modifié sensiblement les premiers résultats.

Les résultats

La partie statistique du questionnaire nous a permis d'établir une "carte" de la distribution des machines UNIX à l'UNIL. Les figures ci-contre montrent l'évolution du parc de ces machines depuis 1988 et la répartition du parc actuel selon les constructeurs.



Stations UNIX à l'UNIL



Répartition des machines UNIX selon les constructeurs (septembre 1991)

Afin de pouvoir faire ressortir les points importants parmi les demandes des utilisateurs, une pondération a été établie de la manière suivante:

Poids= 10 x (nombre de sites)
+ (nombre d'utilisateurs potentiels)

Le poids maximal s'élève ainsi à 201.

Trois classes de résultats ont alors été définies:

P) Sujets **prioritaires** ($P \in [140,201]$)
I) Sujets **importants** ($P \in [90,140[$)
A) Sujets **annexes** ($P \in [0,90[$)

Le tableau ci-contre liste les résultats.

Les actions

Dès réception des réponses, plusieurs actions ont été entreprises par le Centre informatique. Nous signalons ici les plus importantes.

P6 - Une des concrétisations majeures a eu lieu le 25 novembre dernier par le tenue de la première réunion du GOUROU, le tout nouveau *GrOupe d'UtilisateuRs d'Ordinateurs Unix*. Ce groupe, animé par MM. Müller et Roy du Centre informatique, représente l'occasion pour tous les responsables de machines UNIX de soumettre leurs problèmes et aussi peut-être leurs solutions à la discussion. Il servira de canal privilégié à l'information dispensée par le Centre informatique en matière UNIX.

N°	Sujet	Pts
Sujets prioritaires		
P1	Réponse aux questions	189
P2	Partage de fichiers sous NFS	189
P3	Imprimante couleur PostScript A4	173
P4	Messagerie internationale	170
P5	Utilisation de logiciels standards	158
P6	Participation à un User's Group	154
P7	Maintenance gérée par le Ci	141
Sujets importants		
I1	Cours d'introduction à UNIX	124
I2	Serveur de logiciel	115
I3	Administration système	106
I4	Démos + tests de logiciels au Ci	106
I5	Puissance CPU	102
I6	Espace disque permanent	102
I7	Serveur news	97
Sujets annexes		
A1	Fichiers de configuration standard	83
A2	Cours shell et commandes	79
A3	Aide à la mise à jour de système	66
A4	Environnement de test au CI	64
A5	Cours langage C	64
A6	Cours Network File System	64
A7	Espace-disque scratch	60
A8	Network Information Service	56
A9	Aide à l'installation de système	44
A10	Cours NIS	30
A11	Outils de maintenance make,sccs	25

Table des sujets triés

P4 - Depuis le rapatriement de la passerelle GW à l'UNIL, la messagerie internationale est accessible depuis toute machine UNIX.

P3 - Dans le dernier Info-Ci, la nouvelle imprimante couleur A4 du Centre informatique vous était présentée. La correction donnée en page 5 permettra à tout utilisateur UNIX de profiter de cette imprimante directement depuis sa station de travail.

P1 - Plusieurs manières d'établir un service de réponse aux questions ont été examinées lors du premier GOUROU. L'article ci-contre précise les canaux à utiliser pour soumettre les problèmes.

P7 - Le Centre informatique propose un contrat type de maintenance des stations UNIX pour les machines DEC, SUN et SGI.

I1, I3 - Le programme des cours du Ci contient une introduction à UNIX, où l'on apprend les premières manipulations de ce système et un cours avancé plus axé sur l'automatisation des tâches de gestion d'une machine UNIX (scripts). Un cours d'administration système sera mis sur pied bientôt.

I5, I6 - Depuis l'installation du serveur SUN ULCI20, plusieurs personnes ont pu profiter de cette machine pour des fins de tests, d'exercices, ou même de production (restreinte).

Cette série de mesures couvre déjà une bonne partie des demandes formulées par les utilisateurs. Grâce à cette enquête et aux réunions régulières des utilisateurs UNIX, nous saurons où mettre nos efforts dans la suite. ■

Le système 7 à coeur ouvert

Par Philippe Ryter

Deux opportunités de découvrir les nouveautés apportées par cette version tant attendue:

les 27 janvier ou 14 février, de 14 à 16 h

au Centre informatique
Salle des Macintosh

Inscriptions au 692.23.11 (nombre de places limité)

Réseaux

Achèvement du réseau en pharmacie

Antoine Péclard

Le réseau informatique du BEP, le Bâtiment de l'Ecole de Pharmacie, a été mis en service dès ce printemps, les bureaux étant raccordés dès l'installation des personnes dans leur nouvel environnement de travail.

Ce qui distingue cette installation de celles effectuées dans les autres bâtiments est que, dans ce cas, un précâblage a été installé lors de la construction. Ce précâblage est mixte: différents types de câble peuvent être utilisés suivant l'information à transporter.

- Une *fibre optique* relie le bâtiment au réseau LUNET. Cette liaison entre le BEP et le BSP possède la réserve nécessaire pour passer à une technologie FDDI (réseau à haut débit).

- Les différentes plate-formes d'étages sont reliées entre elles également par *fibre optique*. Ce câblage "vertical" permettra plus tard d'envisager une interconnexion plus rapide également.

- Des armoires d'étages partent 3 types de câblage:
  1. câbles en paires cuivres de type *OpenLink*™ pour les connexions série (voir Info-Ci n°19);
  2. câbles coaxiaux de type *Ethernet fin* pour la connexion des PC et des stations;
  3. câbles *Phonenet* pour la connexion des Macintosh.

Ce câblage «horizontal» est distribué dans tous les canaux et permet d'ajouter des prises si nécessaire. Actuellement le bâtiment est équipé de 135 prises sérielles, 23 prises Phonenet et 120 prises Ethernet fin. ■

Politique de sauvegarde des disques au Centre informatique

Jacques C. Wenger

Dans le contexte de ce numéro "spécial sécurité", il nous a semblé nécessaire de rappeler aux utilisateurs du système central de l'Université les principes qui gouvernent le sauvetage du contenu des disques de ce système et leurs implications pratiques pour l'utilisateur. Ces principes avaient été exposés il y a un peu plus de trois ans dans ce journal, et semblent avoir été quelque peu oubliés.

Politique suivie

Pour permettre de faire face à une éventuelle destruction du contenu des disques, accidentelle ou autre, le Centre informatique procède régulièrement au sauvetage des fichiers (opération de BACKUP).

Trois types d'opérations sont actuellement en vigueur:

Sauvetage mensuel

Un sauvetage complet du contenu de tous les disques est fait au début de chaque mois, sur cassette magnétique. Depuis l'introduction de la technique du "*volume shadowing*" (disques miroirs), cette opération est possible sans devoir arrêter le système, ni perturber le travail des utilisateurs. Les cassettes magnétiques sont conservées pendant deux mois au minimum.

Sauvetage quotidien

Un sauvetage quotidien des seuls fichiers qui ont été modifiés ou créés depuis le dernier sauvetage, pour autant qu'ils existent encore au moment où le sauvetage se fait, bien entendu. Ceci se passe entre 1 et 2 heures du matin, du dimanche au vendredi. Ces fichiers sont conservés sur bande magnétique au moins jusqu'au prochain sauvetage hebdomadaire.

Sauvetage hebdomadaire

Un sauvetage hebdomadaire, le samedi entre 1 et 2 heures du matin, qui est le résumé des six sauvetages quotidiens précédents, c'est à dire de tous les fichiers, encore présents à ce moment, qui ont été modifiés ou créés dans le cours de la semaine écoulée. Les bandes sont conservées pendant deux semaines environ.

Conséquences

Avec une telle stratégie, il est possible en tout temps, à partir du dernier sauvetage complet et des sauvetages incrémentaux qui le suivent, de reconstituer un disque dans l'état où il était au moment du dernier sauvetage incrémental. Ainsi la perte possible d'information se limite à l'équivalent d'une journée de travail.

Cette stratégie assure donc une disponibilité et une intégrité quasi totale des informations stockées sur les disques du site central.

Et vos fichiers perdus ?

Il ne faut cependant pas confondre cette opération avec l'archivage des données personnelles. A ce sujet, quelques points sont à relever:

• Un fichier supprimé le jour où il a été créé n'est, évidement, pas récupérable.

• Les sauvetages périodiques des disques sont faits sur un jeu "tournant" de bandes ou de cassettes. Il s'ensuit que les sauvetages anciens (plus de 2 en arrière) n'existent plus. Le processus mis en place est destiné avant tout à assurer la sécurité du système et des données qui y résident.

• Il est quand même possible de récupérer des fichiers perdus à la suite d'une fausse manoeuvre. Il est indispensable que la demande en soit faite au plus vite, que vous connaissiez le nom et si possible la date de création des fichiers perdus, et que ceux-ci aient été l'objet de l'un au moins des sauvetages décrits plus haut. On réservera ces demandes aux cas graves, où les fichiers perdus ne sont pas reconstituables ou lorsque les pertes sont massives.

• Le Centre informatique n'offre actuellement aucun service d'archivage à court ou à long terme; cette opération est laissée à la responsabilité des utilisateurs. Un cours d'une demi-journée de formation à cette technique est dispensé par le Centre informatique et apparaît dans la grille des cours réguliers sous le nom de "Sauvegarde des données sur VAX" (voir Info-Ci nº19).

• En cas de fermeture de compte, un archivage complet des fichiers est effectué et conservé aussi longtemps que la bande magnétique utilisée reste lisible. ■

SGBD

Sauvegardes INGRES

Jacques Guélat

Les bases de données INGRES développées sur UL9000 sont désormais doublement sauvegardées. En plus du backup régulier des fichiers sur disques (voir l'article ci-contre), une procédure a été développée ces derniers mois permettant à l'opérateur d'effectuer un sauvetage quasi-automatique de toutes les bases de données développées sous INGRES (opération *unloaddb*) et la récupération d'une ou de toutes ces bases à partir de la bande magnétique contenant la sauvegarde. Cette manière de procéder assure la consistance des bases récupérées en cas de crash disque.

L'introduction de cette nouvelle procédure de sauvegarde augmente la disponibilité et l'intégrité des bases de données développées par les utilisateurs d'INGRES. Elle ne remplace toutefois pas les mesures immédiates de sécurité propres au bases de données (*checkpoint*, *journaling*) qui sont toujours du ressort des utilisateurs désirant une fiabilité de haut niveau. ■

Sécurité Télépac

Daniel Henchoz

Possibilités d'accès

L'accès au réseau X25 Télépac des PTT, aussi appelé réseau de paquets commutés, est possible depuis les machines VAX du Centre informatique. Il est réalisé à l'aide du logiciel P.S.I. (*Packet System Interface*) fourni par DEC. Cet accès permet à chaque utilisateur de se connecter sur bon nombre de machines en Suisse et à travers le monde. Il ne doit cependant être utilisé que dans le cas où la connexion par le réseau Internet n'est pas possible! En effet, les coûts d'exploitation sont très élevés en raison des fortes taxes prélevées par les PTT.

Notre liaison avec Télépac nous permet aussi d'être atteints par des correspondants appelant depuis Télépac ou depuis d'autres réseaux X25 étrangers (France: Transpac, Etats-Unis: Tymnet, ...).

Sécurisation des accès

Avec le logiciel P.S.I., un module de sécurité est également fourni. Nous avons activé ce module pour contrôler d'une part les accès des utilisateurs de l'UNIL vers l'extérieur et d'autre part filtrer les appels venant du monde extérieur.

Procédure d'autorisation

En conséquence, si vous voulez vous connecter à une machine en utilisant le réseau Télépac ou si vous devez vous connecter vers notre site depuis un site extérieur, vous devez en faire la demande écrite au Centre informatique en utilisant le même formulaire que le celui utilisé pour une demande d'ouverture de compte (ces formulaires se trouvent chez votre responsable d'unité budgétaire). Dans les deux cas, veuillez préciser sur la formule le nom du site ou de la machine avec laquelle la connexion doit être réalisée ainsi que son numéro DTE (sorte de numéro de téléphone propre aux réseaux X25). Vous serez averti par messagerie dès que les accès auront été libérés pour vous.

Utilisation

Après réception du message d'autorisation, vous devrez ajouter la ligne:

```
@UNIL$LIBRARY:TELEPAC_LOGIN
```

dans votre fichier **LOGIN.COM**, afin que toutes les définitions nécessaires à l'utilisation de Télépac soient faites automatiquement pour vous. Pour vous connecter à une ressource X25, tapez ensuite simplement la commande:

```
UL9000$ TELEPAC <nom_de_la_ressource>
      ou:
UL9000$ TELEPAC
```

qui vous retournera la liste des noms des ressources auxquelles vous avez le droit de vous connecter.

Accès public

Certains services sont accessibles par Télépac sans passer par la procédure d'autorisation décrite ci-dessus. C'est le cas du service ATE (Annuaire Téléphonique Electronique) des PTT qui est ouvert à toute personne qui aura ajouté la ligne

```
@UNIL$LIBRARY:TELEPAC_LOGIN
```

dans son fichier **LOGIN.COM.** L'appel à ATE se fait en tapant:

```
UL9000$ TELEPAC ATE ■
```

Suite, mais pas fin ...

Daniel Henchoz

Afin d'élargir l'accès et d'augmenter la fiabilité de la connexion vers SIBIL, nous avons procédé à quelques petites modifications dans la manière de s'y connecter. Les nouveautés annoncées dans le dernier numéro d'Info-Ci restent valables.

Il est actuellement possible de se connecter à SIBIL en utilisant l'une des méthodes présentées ci-après:

Depuis un DECserver:

```
Local> Connect SIBIL
```

Depuis un NIU:

```
>> Connect SIBIL
```

NOUVEAU:

Depuis une source TCP/IP:

```
TELNET> open SIBIL
```

L'accès à SIBIL par le protocole TCP/IP est réservé aux machines du réseau de l'UNIL. Ce nouvel accès rend SIBIL disponible aux personnes travaillant à partir d'un émulateur de terminal supportant TCP/IP (par exemple MAC240 avec MacTCP via une passerelle FastPath) ou de n'importe quelle machine pouvant générer une connexion de type TELNET.

Lorsque la connexion aura été établie, vous obtiendrez le message suivant:

```
****************************************
* Pour acceder au Reseau Romand        *
*      des bibliotheques               *
*  Utilisez le Username «SIBIL»        *
****************************************

Unauthorized access prohibited

Username:
```

Dans tous les cas tapez le nom d'utilisateur SIBIL. Le système ne vous demandera pas de mot de passe et vous connectera directement à l'IBM de Rero pour autant qu'il reste encore une ligne disponible ... Si toutes les lignes sont déjà occupées (il n'y en a que quatre pour le moment), vous obtiendrez le message suivant :

```
%SNATERM-E-FAIESTSES, failed to
establish session
-SNA-E-SESINUNAC, session address
already in use or not activated

Toutes les lignes vers SIBIL sont
occupees ...
Veuillez reessayer plus tard s'il-
vous-plait !

SIBIL  logged out at 18-NOV-1991
11:18:31.37
```

La commande SIBIL depuis une session utilisateur est toujours valable:

```
UL9000$ SIBIL ■
```

Première expérience sur le NEC plus ultra

Alexandre Roy

Introduction

Le projet d'acquisition d'un superordinateur national est en voie d'achèvement. Le 9 septembre dernier, la machine choisie, une NEC SX3, est arrivée à Manno au Tessin dans 110 caisses pesant au total environ 46 tonnes. L'installation s'est terminée le 30 septembre et, depuis, l'ordinateur est en période de test jusqu'au mois de mars 92, date prévue pour le début de la production.

J'ai eu le privilège de faire partie du groupe d'utilisateurs pilotes chargés d'effectuer les premiers tests utilisateurs sur cette machine. Ce groupe a été invité à Manno au début octobre. Chacun avait pour mission d'installer un ou plusieurs programmes sur le SX3 afin d'apprécier la valeur du compilateur Fortran et les performances de la machine. Cet article résume mes premières impressions.

Le CSCS

Le CSCS (*Centro Svizzero di Calcolo Scientifico*) est une unité dépendant directement du centre de calcul de l'Ecole Polytechnique Fédérale de Zürich. Il est situé à Manno (TI), près de Lugano. Le CSCS est composé d'un groupe d'exploitation et du GASS (*Gruppo Applicazioni Scientifiche su Supercomputer*). Le groupe d'exploitation réunit 19 postes de spécialistes. Il est responsable de la maintenance matérielle et logicielle ainsi que de l'assistance directe aux utilisateurs. Ces personnes sont appuyées par cinq spécialistes de la firme NEC travaillant en permanence à Manno. Le GASS quant à lui s'occupe de l'aide aux programmeurs, afin d'assurer l'utilisation optimale des processeurs vectoriels. Ce groupe se composera de 15 personnes environ, dont 5 seront en permanence à Manno. Les autres personnes seront disséminées dans les Universités et Ecoles Polytechniques. Le GASS aimerait commencer ses activités par l'établissement d'une antenne dans chaque Université et EPF. Pour l'Université de Lausanne, cette antenne est initialement constituée de Isabelle Moullet (Section de physique) et de moi-même (Centre informatique).

L'infrastructure

Les locaux du CSCS sont situés dans une zone industrielle près de Manno. L'ensemble du centre occupe 4200 m^2 d'un bâtiment appartenant aux CFF; 1400 m^2 sont au sous-sol pour le refroidissement des machines, la climatisation et l'infrastructure électrique. Au rez-de-chaussée, les 2800 m^2 restant se divisent en trois zones de sécurité: la salle des machines, au coeur du bâtiment (environ 1000 m^2), les bureaux des collaborateurs internes et finalement la zone d'accueil. Cette troisième zone comprend l'administration, une cafétéria, trois bureaux équipés de stations de travail pour les visiteurs, deux salles de conférences, une bibliothèque et une salle de cours avec treize stations de travail. Un laboratoire graphique équipé d'un matériel graphique haut de gamme est également disponible; il est attenant à la salle des machines. Cette dernière contient non seulement le SX3, mais également divers serveurs de fichiers pour les stations de travail et toute l'infrastructure nécessaire aux télécommunications et au réseau.

Le réseau lui-même a été conçu par la section de communication du service informatique de l'ETHZ. Il est constitué de deux boucles FDDI (*Fiber Distributed Data Interface*) ayant chacune une capacité de transport de 100 Mbits/s. Un routeur de type CISCO relie ces deux boucles. De la première partent les lignes reliant les écoles polytechniques. Ces deux lignes offrent pour l'instant un transport à 2 Mbits/s, pouvant être ultérieurement porté à 34 Mbits/s. La deuxième boucle FDDI est interne au CSCS; elle relie une ou deux stations graphiques, un serveur de fichiers et divers brins Ethernet sur lesquels sonts connectés les stations du centre et le SX3.

Le superordinateur SX3

La série SX3 comporte 8 modèles. Le modèle SX3/11 monoprocesseur est le modèle de base; tout en haut de la gamme on trouve le SX3/44. Le premier chiffre 4 dans le nom du modèle indique le nombre de processeurs et le deuxième le nombre de *pipelines/sets* par processeur. Un *pipeline/set* peut produire, en théorie, 4 résultats de calcul en virgule flottante par temps d'horloge, ce dernier étant de 2.9 nanosecondes. Le modèle installé à Manno est un SX3/22 ayant un performance théorique maximum de 5.5 Gflops (milliards d'opérations par seconde). L'upgrade à 4 processeurs est prévu pour 1993.

La mémoire centrale, partagée entre les deux processeurs, est de 1 Goctets et va passer, dès le mois de janvier prochain, à 2 Goctets. Une mémoire étendue de 4 Goctets est également installée (équivalent de la SSD de CRAY); c'est une zone de stockage d'accès plus rapide que les disques, mais plus lente que la mémoire centrale. Les disques offrent un espace de 70 Goctets, dont 20 sont répartis sur des disques haute vitesse. Quant au système d'archivage, il est constitué d'une unité de cartouche robotisée totalisant une capacité de 1 Toctets (10^{12} octets).

Les logiciels et systèmes d'exploitation

Le système d'exploitation est un Unix basé sur le système V avec des extensions de BSD 4.3. Son nom est Super-UX; il intègre des améliorations spécifiques aux superordinateurs. Comme sur les CRAYs, le traitement batch est géré par NQS. Concernant le réseau, le SX3 utilise TCP/IP (telnet, ftp, NFS, ...) à travers Ethernet et dans un proche avenir la connexion au réseau FDDI sera directe.

Le compilateur Fortran est évidemment le plus optimisé parmi les compilateurs disponibles. Il offre une vectorisation automatique du code et fait usage de plusieurs techniques semblables à celles qui sont utilisées sur CRAY. Les autres compilateurs disponibles sont C et C++. Le système offre également des outils pour ana-

lyser les performances d'un code (ANALYSER/SX et PARALLELIZER/SX). Une bibliothèque mathématique optimisée (ASL/SX) est fournie afin de faciliter le portage de programmes d'un CRAY sur le SX3. La bibliothèque NAG est aussi installée.

Programmation sur le SX3

L'architecture du SX3 est très semblable à celle du CRAY 2 et, en principe, les programmes favorables à ce dernier offre de bonnes performances. Deux faiblesses du SX3 sont à relever. Premièrement, l'accès mémoire est lent relativement à la rapidité du CPU. Il faut être très soigneux dans le dimensionement des tableaux; la vitesse d'exécution d'une boucle peut varier d'un facteur 100 uniquement en changeant la première dimension d'un tableau à deux dimensions. Ceci est bien connu sur le CRAY 2, mais dans une mesure moins importante. Deuxièmement, les entrées/sorties sont pénalisantes, mais il est possible de les améliorer en utilisant les disques rapides ou la mémoire étendue.

5 fois plus rapide que le Cray 2

Applications pilotes sur le SX3

Un groupe de 12 utilisateurs a été invité à Manno au mois d'octobre, pour installer chacun une ou plusieurs applications sur le SX3. Le PSI (Paul Scherrer Institute), ainsi que les Universités et EPF étaient représentés. Les programmes appartenaient aux domaines suivants: chimie quantique, dynamique moléculaire, physique du solide, diffusion de neutrons, physique des plasmas, phénomènes de transport. D'une manière générale, les résultats sont très bons. En moyenne, les programmes sont 5 fois plus rapides que sur le CRAY 2 et 2 fois plus rapides que sur le CRAY YMP. Les programmes écrits en Fortran standard n'ont montré aucun problème de migration. Les problèmes sont apparus principalement avec des programmes faisant un usage intensif de la représentation en nombres complexes et avec la bibliothèque ASL/SX qui s'est avérée très peu performante.

L'accueil à Manno

Le 7 octobre, je me suis retrouvé en compagnie des 11 autres utilisateurs pilotes au CSCS à Manno. Le centre est très facilement accessible; il se trouve tout près de la sortie d'autoroute Lugano-Nord. Il se situe dans un grand bâtiment administratif flambant neuf et encore à moitié vide. Nous avons été accueuilli par le Dr. F. Scaroni, directeur du centre, et durant les trois journées passées à Manno, j'ai eu l'occasion de rencontrer plusieurs membres du CSCS.

Durant la première demi-journée, un consultant de la firme NEC nous a dispensé un cours; il nous a présenté le superordinateur SX3 en général et nous a décrit en détail l'utilisation du compilateur Fortran et de l'analyseur de performance. Dès le second jour, nous avons pu nous connecter à la machine pour commencer l'installation de nos programmes respectifs. Le CSCS dispose à cet effet d'une salle de stations Unix équipée de 13 DECstations 5000.

Mon expérience sur le SX3

La première étape du portage de nos programmes consistait à transférer les fichiers sources. Le réseau du CSCS utilise le protocole TCP/IP; il est connecté au Universités et EPF par SWITCH. La connexion avec ULYS à Lausanne s'est effectuée sans problème avec telnet et ftp aussi bien depuis la station DEC que depuis le SX3. **Le temps de réponse et la vitesse de transfert sont les mêmes qu'entre ULYS et une station Sun du Centre informatique. La distance ne joue aucun rôle.**

L'utilisation du SX3 ne pose aucun problème pour une personne connaissant Unix. Il y a bien sûr toujours des variations minimes entre les différentes implémentations d'Unix, comme entre une station Silicon Graphics et une station Sun.

Le programme, que j'ai installé sur le SX3, est un code de simulation 2D, appelé CLIO; il permet de calculer l'équilibre MagnétoHydroDynamique d'un plasma dans un Tokamak. La compilation du programme n'a présenté aucun problème; ceci n'était pas le cas pour les codes comportant beaucoup d'extensions propres à un constructeur (VAX ou IBM). L'utilisation de bibliothèques mathématiques a également posé quelques problèmes à plusieurs utilisateurs pilotes, à cause d'une documentation insuffisante et d'un manque de maturité de ces bibliothèques. Quant au programme CLIO, il utilise une dizaine de routines propres au CRAY; j'ai par conséquent dû fournir moi-même ces routines. Parmi celles-ci, quelques unes sont des routines BLAS, dont je n'ai pas trouvé facilement l'équivalent dans la bibliothèque ASL du SX3.

Une fois le programme CLIO compilé, l'exécution s'est déroulée sans difficulté et a produit un résultat correct. Suivant la taille de l'équilibre calculé, **le SX3 s'est avéré 6 à 16 fois plus rapide que le CRAY2**. Le Dr Gruber nous a appris qu'il s'agissait d'un record parmi les expériences des utilisateurs pilotes. De plus, un consultant de NEC m'a assuré que, en jouant sur les différentes options du compilateur, la vitesse d'exécution pourrait être doublée. L'analyseur de performance m'a facilement permis de trouver les portions de code critiques.

Et la suite...

Suite à cette expérience personnelle, j'aimerais encourager les personnes ayant besoin de temps calcul à utiliser cette machine qui offre des possibilités remarquables. Contrairement à la crainte exprimée par plusieurs personnes, son éloignement physique n'est pas un handicap et la machine est tout aussi facile d'accès, si ce n'est plus facile (pas de Securid), que le CRAY 2 voisin.

Concernant les divers problèmes qui subsistent, en particulier ceux touchant aux nombres complexes et aux bibliothèques mathématiques, je désire rappeler que le SX3 de Manno est la seconde machine de ce type installée dans le monde, qu'elle en est à ses tout premiers débuts et que l'on peut s'attendre à une nette amélioration dans un avenir immédiat. Ceci nous a été confirmé par le Dr. Friedli: durant les deux mois qui ont suivi l'installation, des problèmes hardware et software ont été rapidement réglés par les ingénieurs de NEC et parmi les problèmes observés durant le mois d'octobre, certains sont déjà résolus. ■

Nouveaux visages

Jacques Guélat

C'est devenu une coutume au Centre informatique: le bizutage des nouveaux collaborateurs passe par un autoportrait dans l'Info-Ci. Voici les tableaux de ceux qui ont récemment intégré le Centre.

Vous l'aurez certainement au bout du fil

Pour assister Pierre Magnenat dans ses tâches administratives, la vivacité des réactions de *trader* de **Nécia Benjamin** n'est pas de trop. Il est sûr qu'avec elle vos commandes ne traînent pas!

De droite à gauche: Philippe Gardel, Pierre Küffer et Nécia Benjamin

En 1980, je suis venue en Suisse pour passer un mois de vacances... 11 ans plus tard, j'y suis toujours.

Pendant tout ce temps, j'ai travaillé dans le commerce international du café, comme coffee-trader, ce qui m'a permis de garder le contact avec le Brésil, mon pays d'origine.

Le monde du business-bourse-décalage horaire et tutti quanti étant lassant après tant d'années, je cherchais à mettre mes connaissances commerciales et administratives au profit d'un job me permettant d'avoir un autre regard sur les mots budget, rentabilité, bénéfice, et j'en passe.

Me voilà donc au Groupe Gestion du Centre informatique.

L'efficacité tranquille

Philippe Gardel ne fait pas beaucoup de bruit, mais il a toujours la solution au problème qu'on lui pose. Au sein du groupe assistance, il s'occupe de tout ce qui touche aux statistiques sur grands et petits systèmes, en passant par la représentation graphique des données. C'est aussi lui qui veille au bon fonctionnement des systèmes de bases de données sur ULYS. Ses multiples talents sont mis à contribution pour les cours du Centre informatique puisque c'est lui qui enseigne, entre autres, le cours Excel dès la rentrée.

Originaire de Ste Croix, lointain descendant de huguenot français, je suis né à Lausanne. C'est dans cette même ville que j'ai terminé mes études de physicien à l'EPFL en 1985. Intéressé par le domaine de la physique médicale, j'ai entrepris un travail de recherche à l'Institut de Radiophysique Appliquée (IRA), dans le domaine de la dosimétrie des faisceaux de rayonnement ionisants de haute énergie utilisés en radiothérapie. Durant ce travail, faisant l'objet d'une thèse, j'ai été amené à utiliser différents outils informatiques allant de gros systèmes à la micro, confronté tour à tour aux problèmes liés aux calculs de simulations statistiques, à l'acquisition de données expérimentales, à l'analyse et à la représentation de données.

Durant ces années j'ai fréquemment été conduit à aider et à conseiller des collaborateurs de l'Institut dans le cas de problèmes informatiques. Actuellement, j'exerce cette activité au Centre informatique de l'Université, où j'ai rejoint les rangs du groupe assistance en mai 1991 pour m'occuper plus particulièrement des problèmes statistiques et de SGBD.

Un nouvel ancien

Après un congé sabbatique, Pierre Küffer a réintégré l'équipe d'assistance pour y reprendre ses préoccupations d'antan pour une part (graphique) et s'employer pour une autre à l'occupation stratégique qui consiste à diffuser au grand public les nouveautés de connectique développées par l'équipe réseau.

Biologiste de formation, je suis entré au Centre informatique en 1985, époque à laquelle le bâtiment de biologie, ainsi que bien d'autres, possédait ses propres machines, des minis Norsk-Data. Lorsque le Centre informatique centralisa ses ressources, j'émigrai vers l'ouest au BSP. Transhumance prémonitoire. Je m'occupai alors des ressources graphiques.

En mai 1989, je donnai quelque ampleur à ce mouvement vers l'ouest et, franchissant plusieurs longitudes, j'échouai à Boston Massachusett. Inscrit à la Berklee school of music, je me plongeai avec délice dans les interactions luxuriantes de la musique et de l'informatique. En été 1991, j'en réémerge muni du Bachelor of Arts in Music.

Les vents migratoires soufflent à nouveau, et j'atterris à Vidy, un poil plus à l'est qu'à mon départ. Je m'y emploie, comme précédemment au graphique, ainsi qu'aux multiples aspects de la connectivité sur le réseau de l'Université. Et qui sait, peut-être que certaines images voudront du son. ■

Les cours du Ci

Jacques Guélat

Le programme des cours du semestre d'hiver bat son plein. Le cap des 500 participants a été allègrement franchi au début novembre, preuve d'un attrait toujours aussi grand dans la communauté universitaire. J'aimerais relever ici quelques ajouts intéressants ou modification au programme, dont le calendrier est donné comme à l'accoutumée en dernière page de ce journal. Les descriptifs des cours ont paru dans Info-Ci 19, numéro dont on peut toujours se procurer une copie au Centre informatique.

Cours sécurité

Dans un numéro consacré à la sécurité, je me dois de faire tout d'abord ressortir les possibilité de formation dans ce sujet que contient le programme. Deux cours sont spécialement orientés dans cette direction: le cours de *Sécurité des données sur Mac* aborde la liste des problèmes courants et inventorie les méthodes de protection, aussi bien au niveau de la prévention que de la récupération en cas de crash. En une journée, les participants font le tour de la question et savent efficacement sécuriser leurs données à la sortie du cours. Le cours *Sauvegarde des données sur VAX* montre en une demi-journée comment effectuer une sauvegarde de ses données personnelles sur le système central, opération qui n'est pas assumée par le Centre informatique (voir l'article à ce sujet dans ce journal). Divers aspects de sécurité sont en outre présentés dans les cours *Gérer et utiliser un serveur sur Mac*, *Cours avancé sur le système Mac*, et dans les cours d'introduction au Macintosh, à VAX/VMS et aux réseaux.

Du nouveau dans la salle des Macintosh

Pour répondre à de fréquentes critiques des participants aux cours à propos de la lenteur des MacSE utilisés dans cette salle et pour préparer la venue du système 7 et des futures versions de logiciels toujours plus gourmandes en mémoire, une mise à jour matérielle a été réalisée en novembre faisant passer les appareils à la classe supérieure du SE/30 et à une mémoire plus que confortable de 5 MB. Fini les attentes lors d'un exercice de calcul dans le cours Excel!

Cours connectivité

Le cours *Utiliser le réseau depuis son micro* a pour but d'apprendre à ses participants la manière d'installer et d'utiliser sur son micro-ordinateur les logiciels de connectique proposés par le Centre informatique. Les responsables de site ont déjà reçu l'information nécessaire à l'installation de ces produits. Cependant, ces responsables ne sont pas forcément à portée de main et ils ne vous apprendront en aucun cas comment utiliser ces produits. Ce cours d'une journée vous l'apprendra.

Suite à l'expérience passée, il s'avère difficile d'aborder deux types de matériels dans un même cours, à savoir des micro-ordinateurs Macintosh et PC. Le cours annoncé au programme pour janvier 91 sera donc dispensé sur du matériel Macintosh uniquement alors que celui de mars 91 se fera sur PC. Des cours supplémentaires peuvent organisés sur demande.

Nouvelles sessions spéciales

Suite à l'engouement observé l'été dernier pour les séminaires bureautique (9 demi-journées consécutives consacrées à la résolution d'un problème complexe et complet), nous avons décidé de réitérer l'expérience en 1992 avec un premier rendez-vous en avril. Le succès des premiers séminaires a généré dès l'été passé une liste d'intéressés qui n'ont pu trouver satisfaction alors. C'est pour ces personnes que ce premier séminaire est d'ores et déjà réservé. Que les autres se rassurent: l'expérience sera certainement reconduite l'été prochain.

Toujours pour essayer de répondre aux propositions émise par les participants lors des cours, une autre expérience sera tentée prochainement: des séances de réponses aux questions seront organisées au Centre informatique et animées par deux spécialistes «incollables» (Messieurs Ryter et Lalieu) qui vous donneront des solutions à vos problèmes les plus corsés. Plus de détails dans l'annonce ci-dessous. ■

Spécial Session *Pilori*

Venez poser vos **questions** Mac
et obtenir des **solutions** à vos problèmes!

Deux spécialistes sont à votre diposition pour résoudre avec vous vos problèmes concernant l'un ou plusieurs des logiciels suivants:

Word4, Excel2.2, FileMakerPro, Illustrator.

séance 1:	21 février 1992, de 9h à 12h
séance 2:	21 février 1992, de 14h à 17h
séance 3:	18 mars 1992, de 9h à 12h
séance 4:	18 mars 1992, de 14h à 17h

Toutes les séances ont lieu au Centre informatique, salle des Macintosh.

Règles de participation:

1. Avoir un ou plusieurs problèmes à soumettre relatifs à l'utilisation des logiciels sus-mentionnés **et ceux-là seulement!**
2. S'inscrire au secrétariat du Ci (692.23.11).
3. Indiquer brièvement lors de votre inscription le contenu du(des) problème(s) que vous désirez voir traiter.
4. Apporter votre matériel sur disquette lors de la séance.

Calendrier des cours de janvier à mars 1992

Cours	Durée	Horaire	Janvier	Février	Mars
INITIATION					
Introduction au Macintosh	1 jour	9-12h, 14-17h	13	4	4
Introduction à VAX/VMS	1 jour	9-12h, 14-17h	14	4	5
Introduction à UNIX	1 jour	9-12h, 14-17h	-	6	4
Introduction aux réseaux	1 jour	9-12h, 14-17h	28	27	-
Introduction à Word 4	2x 1/2 jour	9-12h	21	17	11
		14-17h	22	18	12
Introduction à FileMakerPro	2x 1/2 jour	14-17h	21	-	10
		9-12h	22	-	13
Introduction à Excel 2.2	1 jour	9-12h, 14-17h	16	28	-
Introduction à HyperCard	1 jour	9-12h, 14-17h	31	-	3
Dessiner avec le Mac	1 jour	9-12h, 14-17h	29	-	5
Présentation assistée sur Mac	1 jour	9-12h, 14-17h	30	26	24
APPROFONDISSEMENT					
Cours avancé sur le système Mac	2 jours	9-12h, 14-17h	-	5	-
		9-12h, 14-17h	-	12	-
VMS II	1 jour	9-12h, 14-17h	22	-	19
UNIX II	1 jour	9-12h, 14-17h	24	-	24
Tout Word 4	4x 1/2 jour	9-12h	-	11	10
		9-12h	-	13	12
		9-12h	-	18	17
		9-12h	-	20	19
Représentation des données sur Mac	1 jour	9-12h, 14-17h	-	6	25
Utiliser le réseau depuis son micro	1 jour	9-12h, 14-17h	14 (Mac)	-	9 (PC)
SPECIALISATION					
Sécurité des données sur Mac	1 jour	9-12h, 14-17h	17	25	-
Sauvegarde des données sur VAX	1/2 jour	9-12h	30	-	10
Programmer sur VAX	1 jour	9-12h, 14-17h	16	-	17
Messagerie électronique	1/2 jour	9-12h	15	3	6
Word 4 - secrétariat	2x 1/2 jour	9-12h	23	19	-
		14-17h	24	20	-
Word 4 - académique	2x 1/2 jour	14-17h	23	-	-
		9-12h	24	-	-
Gérer et utiliser un serveur sur Mac	1/2 jour	9-12h	-	7	-

Sur demande (min. 5 personnes), cours d'introduction à BASIS, INGRES, SAS, UNIRAS, VAXSET.

Inscriptions et renseignements au 692.23.11. Descriptifs des cours dans Info-Ci nº19

Les gens qui font le Centre informatique

Direction Pascal Jacot-Guillarmod
ULYS::PJACOT 692 23 01

Secrétariat Marianne Jaquier
692 23 11
FAX 692 22 40

Gestion, achats, usernames

Responsable Pierre Magnenat
ULYS::PMAGNENA 692 23 12

Adjointe Nécia Benjamin
ULA::NBENJAMI 692 23 12

Réseaux informatiques, maintenance micro-ordinateurs

Responsable Jean-Paul Longchamp
ULYS::JLONGCHA 692 23 03

Spécialiste réseau Ha Nguyen
ULYS::HNGUYEN 692 23 37

Spécialiste réseau Antoine Péclard
ULYS::APECLARD 692 23 87

Opérateur Nino Petrillo
ULYS::NPETRILL 692 23 09

Système et exploitation

Chef d'exploitation Daniel Henchoz
ULYS::DHENCHOZ 692 23 13

Responsable système Jacques Wenger
ULYS::JWENGER 692 23 14

Systèmes décentralisés Michel Müller
ULYS::MMULLER 692 23 38

Pupitreur Roger Pernoux
ULYS::RPERNOUX 692 23 06

Assistance logiciels

Responsable Jacques Guélat
ULYS::JGUELAT 692 23 93

Micro-informatique Philippe Ryter
ULYS::PRYTER 692 23 02

Bureautique Marie-France Pernet
ULYS::MPERNET 692 23 05

Statistiques et SGBD Philippe Gardel
ULYS::PGARDEL 692 23 96

Graphique et connectique Pierre Küffer
ULYS::PKUFFER 692 22 42

Programmation et bibliothèques scientifiques Alexandre Roy
ULYS::AROY 692 23 10

UNIVERSITE DE LAUSANNE
CENTRE INFORMATIQUE
RTE DE CHAVANNES 33
1007 LAUSANNE
Rédaction : Jacques Guélat
Impression : Ruckstuhl, Renens

Info-Ci Nº20
décembre 1991

Annexes techniques

Sommaire

Recettes de sécurité

par

Anik Bossuat

Informatique administrative
Université de Lausanne

Nous abordons dans cet article divers aspects particuliers de la sécurité touchant aussi bien à l'accès aux ressources centrales qu'aux ordinateurs personnels. Les recettes mentionnées, bien qu'elles ne forment qu'un sous-ensemble des mesures envisageables pour augmenter le niveau et la qualité de la sécurité, ont le mérite d'être simples et immédiates à appliquer.

Les mots de passe

L'accès aux ressources informatiques s'effectue au moyen de mots de passe. Un mot de passe vous sera en règle générale demandé lors de chaque connexion à un ordinateur ou à une application.

Qu'est-ce qu'un mot de passe informatique ?

• Un mot de passe est une chaîne de caractères.

• Votre mot de passe vous permet d'accéder à un ordinateur ou à une application informatique. Certaines applications utilisent le terme de code d'accès qui est synonyme de mot de passe.

Un mot de passe est invisible.

• Pour des raisons de sécurité, les caractères qui composent le mot de passe n'apparaissent jamais à l'écran lorsqu'on le tape.

Un mot de passe est INTRANSMISSIBLE.

• En recevant l'autorisation d'exploiter des ressources informatiques, vous êtes désormais responsable de la **fiabilité**, de la **confidentialité** des informations et aussi, dans certains cas, de l'augmentation des **frais informatiques**. Pour ces raisons, la clé d'accès que constitue un mot de passe est intransmissible à des tiers (voir l'article *Règles d'utilisation des serveurs dédiés à l'informatique académique des domaines scientifique et administratif* dans le journal).

EXEMPLES

Défaut de fiabilité.

• Un utilisateur habilité à entrer des informations dans une application transmet son *username* et son mot de passe à un "ami". Celui-ci pourra entrer des données erronées, même involontairement en s'amusant avec l'application. Certaines erreurs pourront être détectées immédiatement, d'autres des jours, des semaines, voire des mois plus tard.

• *Remarque*: Le Centre informatique garde une trace de chaque connexion. Dans cette situation, elle s'effectue sous le nom du propriétaire du username et non de celui de l'ami!

MPLES EXEMPLES EXEMPL

Défaut de confidentialité.

• Il se peut qu'une information sélectionnée dans une application ne soit pas confidentielle. Mais, juxtaposée à d'autres informations sélectionnées à partir de la même application ou à partir d'autres applications , elle peut le devenir.

• Des utilisateurs, autorisés à consulter des informations, transmettent leur username et leur mot de passe à un **même** "ami", celui-ci peut exploiter en tout impunité les informations. Seul le nom des propriétaires des usernames est enregistré.

Augmentation des frais informatiques.

• Les coûts d'exploitation ne sont pas toujours apparents pour l'utilisateur, en particulier les coûts d'accès au réseau Télépac (X25): un responsable d'une petite entreprise a besoin d'informations sur des bases de données publiques à l'étranger. Il trouve un utilisateur autorisé à utiliser les réseaux, qui lui transmet son username et son mot de passe. Pendant des heures ce responsable peut utiliser les réseaux internationaux (frais de transmissions payés par l'Université).

• Remarque: le Centre informatique garde un accounting des frais Télépac lié au username.

Longueur du mot de passe.

• La longueur du mot de passe varie selon les ordinateurs et les applications. Pour les ordinateurs, la longueur varie entre 6 et 256 caractères. Pour les applications, la longueur est mentionnée dans le manuel d'utilisation.

• Plus le mot de passe est long, plus il est difficile à deviner.

Mots de passe déconseillés.

• La sécurité conseille de ne pas utiliser un mot de passe ou code d'accès facile à découvrir. Sont **déconseillés** tous les mots pouvant provenir d'un dictionnaire, de votre environnement privé ou professionnel par exemple :

- Votre nom, prénom, username ou toute combinaison de ceux-ci.
- Le nom ou prénom d'un membre de votre famille ou de vos amis très proches, même s'ils vous sont chers.
- Le nom de la ville où vous habitez.
- Le nom de votre animal, de votre voiture, de votre bateau.
- Le nom de votre compagnie, de votre projet préféré.
- Vos numéros de plaques de voiture, de téléphone.
- Votre date de naissance.

• Inutile d'alterner majuscules et minuscules ou de préfixer ou suffixer le mot par un chiffre.

Comment trouver un bon mot de passe facile à retenir.

• Créez votre mot de passe en pensant à un mot, à une courte phrase et en l'écrivant avec votre phonétique. Exemple:
La vie est courte ——> **laviaikurt**

• Vous pouvez y insérer un chiffre ou un symbole pour augmenter la sécurité (évitez toutefois les caractères de contrôle!). Exemple:
La vie est courte ——> **lavi_ai_kurt**

• Vous pouvez inverser les syllabes d'un mot et écrire phonétiquement. Exemple:
bouquin ——> **kinbou**

• Vous pouvez prendre la première lettre de chaque mot d'une phrase. Exemple:
Il est temps de changer les pneux d'été ——> **ietdclpde**

• Vous pouvez prendre le milieu d'une phrase. Exemple:
Le nez de Cléopâtre ——> **ezdecleo**

Comment trouver plusieurs mots de passe facile à retenir.

• Si vous avez à gérer plusieurs mot de passe, *vous pouvez utiliser un seul mot de passe de base* et ajouter la première lettre de l'application suivie de 1 ou 2 chiffres. Exemple:
J'ai l'autorisation de travailler avec Gadmine et Reshus. J'ai choisi pour mot de passe de base: gesmor (Morges)
Mon mot de passe d'accès
à l'ordinateur VAX sera ——> **V09GESMOR**
à Gadmine sera ——> **G09GESMOR**
à Reshus sera ——> **R09GESMOR**

Changement du mot de passe.

• Le mot de passe peut avoir une durée de vie limitée. Eventuellement, l'ordinateur vous demandera d'effectuer un changement quelques jours avant son expiration pour vous laisser choisir le moment opportun. Passé ce temps limite, votre mot de passe devient *pré-expiré*.

• Prenez l'habitude de changer vos mots de passe régulièrement avant que l'ordinateur ne vous le demande, tous les 5 de chaque mois par exemple.

• Changez tous vos mots de passe en même temps.

• Pour des raisons de sécurité, lorsque vous mettez trop de temps pour entrer ou changer votre mot de passe, apparaît à l'écran le message "TIME-OUT" qui interromp votre session. Vous n'avez plus qu'à recommencer. Donc, avant d'engager la procédure de changement, définissez votre nouveau mot de passe.

➨ N'oubliez pas :

Vos mots de passe sont intransmissibles.

Quitter les ressources informatiques

Très souvent, en se promenant dans les couloirs de l'Université, on aperçoit des écrans allumés et abandonnés temporairement par leur utilisateur. Jusque-là, rien de très dangereux. Cela le devient lorsqu'on s'aperçoit que non seulement l'écran est allumé, mais que la session de travail sur l'ordinateur hôte est en cours! Tous les accès propres à l'utilisateur sont ainsi offerts à tout venant. Il ne faut pas beaucoup de temps pour effectuer des opérations aux conséquences catastrophiques...

La fonction de quitter les ressources informatiques est donc primordiale et doit s'effectuer correctement. Elle est constituée des étapes suivantes:

1 - Quitter l'application

2 - Quitter l'ordinateur hôte

☞ Les ressources informatiques, bien que très importantes, ont des limites d'absorption d'utilisateurs.

• Evitez de rester connecté inutilement.

• Pratiquez les étapes 1 et 2 aussitôt votre travail terminé.

3 - Si vous utilisez un émulateur de terminal, quittez-le!

☞ Vos transactions peuvent être confidentielles comme par exemple la lecture d'un message électronique.

• Toutes vos transactions informatiques et leur contenu, à l'exclusion de votre mot de passe, sont mémorisées dans le MAC. Elles seront détruites ou gardées selon votre choix, dès que vous aurez terminé l'étape no 3.

• Un tiers peut visualiser et imprimer l'ensemble de votre travail!

4 - Quitter le poste de travail

☞ En votre absence, vous ne savez pas qui passe près de votre bureau.

• Si vous quittez votre poste de travail temporairement, protégez l'accès à l'écran par un mot de passe (avec un outil comme *After Dark* par exemple).

• Si vous quittez votre poste de travail définitivement, éteignez-le complètement et fermez votre bureau.

Récupération du papier ...

La récupération du papier implique un minimun de sécurité.

C'est dans les poubelles que l'on trouve les trésors.

En jetant dans les poubelles nos brouillons de documents comptables, de publications scientifiques, de documents des immatriculations, etc... nous donnons notre information à qui désire la prendre...

Il est donc nécessaire de séparer les brouillons des documents confidentiels, des autres brouillons (les chutes d'imprimante dans de nombreux cas sont confidentiels).

Le Comité de sécurité engage chaque service, institut, faculté à acquérir une déchiqueteuse.

Sécurité de l'information sur Macintosh

Nous réunissons ici quelques consignes édictées par Philippe Ryter dans des numéros précédents d'Info-Ci (nos 17, 16, 15 et 10) permettant d'élever le niveau de sécurité de l'information sur Macintosh.

SAUVEGARDES

Sauvegardez vos données.

☞ Par copie à l'aide du Finder ou avec FASTBACK II.

Conservez vos programmes originaux en lieu sûr.

☞ A l'abri de la poussière, de l'humidité, de la chaleur et des champs magnétiques, et dans un local autre que votre bureau. Ces critères de stokage sont identiques pour les sauvetages de vos informations.

Conservez plusieurs copies de vos fichiers importants.

☞ Par copieà l'aide du Finder ou avec FASTBACK II sur des supports physiques (disques ou disquettes) distincts.

VIRUS

Examinez toute nouvelle disquette introduite dans le lecteur ou tout fichier importé par le réseau à l'aide d'un détecteur de virus.

☞ Avec SAM, Virex, Disinfectant, Virus Détective, etc...

RUS VIRUS VIRUS

Verrouillez vos disquettes en lecture.

☞ Poussez le taquet vers le bord de la disquette.

Verrouillez vos applications sur le disque dur.

☞ Case à cocher dans l'article *Lire les informations* du menu *Fichier*.

Examinez régulièrement votre disque dur.

☞ Avec SAM, Virex, Disinfectant, Virus Détective, etc...

PRECAUTIONS

Initialisez les disquettes à recycler; jetez-les au message *l'initialisation a échoué.*

☞ Avec l'article *Initialiser le disque* du menu *Rangement*.

Utilisez les outils de protection du disque.

☞ Avec FileSaver (voir article dans ce journal).

Bloquez votre écran lorsque vous devez vous absenter momentanément.

☞ Avec After Dark ou Pyro et un mot de passe.

Votre MAC peut acquérir un bon niveau de sécurité.