



ISSN 1420-7192

par Jacqueline Dousson, SIC

L'office fédéral de la culture

a octroyé un numéro ISSN – *International Standard Serial Number* (figuré par le code barre ci-dessus) au Flash Informatique. Cette reconnaissance par les autorités suisses nous prouve (mais en avons-nous vraiment besoin?) que notre revue est bien présente et occupe un créneau bien spécifique. Elle garde sa propre identité, par son côté à la fois prospectif et pratique (les trucs du Coin des Curieux par exemple).

Profitons de l'occasion pour rappeler que vous pouvez vous abonner par un simple message à fi@sic.epfl.ch, nous nous ferons un plaisir de vous envoyer nos dix numéros annuels (plus le numéro spécial été) et si vous êtes adeptes d'une *société sans papier*, n'oubliez pas que le Flash Informatique est présent sur le Web en HTML depuis **1994** et en format PDF depuis **avril 1996** (voir plus loin **Le FI sur le Net**). Soyez sûrs que dans les mois à venir, qui risquent d'être particulièrement mouvementés *informatiquement* parlant, nous allons tenter, comme toujours, de vous

donner quelques flashes pour vous aider à y voir plus clair dans ce maelstrom. Nous espérons ne pas vous décevoir et nous attendons de votre part de l'indulgence pour le côté parfois incohérent, quelquefois incomplet, du contenu. Les personnes qui écrivent dans le Flash – **vous, peut être dans un prochain numéro?** – ont bien d'autres tâches à accomplir, mais elles sont toujours animées par le désir d'informer et de partager des expériences ou des réflexions. Qu'elles soient remerciées ici pour le temps consacré à ce travail et que d'autres viennent les rejoindre ...

LE FI SUR LE NET

Depuis le numéro de janvier 1994 (il y a même quelques auteurs privilégiés de 1993 qui ont connu cet honneur), le FI est accessible sur le Web en format HTML:

<http://sawwww.epfl.ch/SIC/SA/publications/>

suite en page 9 →→

SOMMAIRE

- 1 ISSN 1420-7192
- 2 Unicos 9
Ce qui va changer par rapport à Unicos 8
- 4 Secure Shell, ou cachez ce mot de passe que je ne saurais voir
- 10 Cache Web, ou comment optimiser l'utilisation du réseau
- 12 CAPA
- 13 Un serveur de News moderne à l'EPFL
- 14 Eudora 3.0
- 15 Swiss Research Teams Index
- 15 SWITCH
- 16 Le copieur couleur Xerox Magic (Fiery-Regal) 5790
- 18 Le Coin des Curieux
- 20 Les cours de formation
- 24 Calendrier des manifestations

PROCHAINES PARUTIONS

	parution FI	délaï FI
8	22.10	03.10
9	19.11	31.10
10	17.12	28.11

Unicos 9

Ce qui va changer par rapport à Unicos 8

par Jean-Michel Chenais, SIC

INTRODUCTION

La mise en place d'une révision de système d'exploitation est traditionnellement une étape importante dans l'évolution des services d'un serveur de calcul central. Ainsi l'installation prochaine du système Unicos 9.0.2 sur Pascal, prévue depuis plusieurs mois, constituera au courant de cet automne 1996 une telle étape tant pour la communauté des usagers que pour les gestionnaires de ces ressources informatiques.

Unicos 8, maintenant en exploitation sur Pascal depuis environ 1 année et demie (installation en février 95), n'a que peu évolué entretemps, hormis des révisions mineures, surtout rendues nécessaires pour l'amélioration du logiciel système du T3D. En raison de l'évolution constante des matériels et des logiciels, il devenait temps pour le SIC d'évaluer l'opportunité d'installer la toute dernière des versions du système Unicos 9, dont la version native était déjà disponible au début 96.

Le présent article a pour but d'informer les usagers afin de leur permettre d'appréhender au mieux les quelques changements inévitables qui pourront affecter le travail quotidien sur les serveurs Pascal et T3D. Les nouveautés qui s'appliquent aux autres machines (nouvelles séries T90, J90) ne sont donc pas traitées ici. De même pour la série YMP-EL: il n'est en effet pas prévu d'installer Unicos 9 sur Nestor. Les nouveautés relatives à certains aspects internes du système sont tout au plus mentionnées, mais pas développées.

De façon générale, il sera nécessaire de se référer aux manuels en ligne (*on-line page manuals*) pour prendre connaissance des détails relatifs à chaque commande ou utilitaire. Seuls sont indiqués, et de façon non exhaustive, les principaux éléments du système qui peuvent concerner la majorité des usagers. Une liste plus complète sera annoncée et publiée par les canaux habituels.

QUELQUES CARACTÉRISTIQUES GÉNÉRIQUES D'UNICOS 9

La mise en place d'une révision majeure de système est motivée par plusieurs raisons:

- ▲ possibilité d'utiliser des matériels nouveaux ou venant en remplacement d'équipements de même nature mais moins performants. Tel est le cas pour la mise en place de postes de lecture/écriture de cassettes à haute capacité d'enregistrement (jusqu'à 50 Gigabytes, *drives* STK Redwood ou SD-3 à enregistrement hélicoïdal). Ce nouveau matériel a nécessité la mise en place sur Pascal du logiciel DMF 2.4.3 de migration automatique des fichiers, et le remplacement du logiciel de pilotage du silo à cartouches (nouvelle version ACSLS 5.1). Les cartouches actuelles resteront à disposition, mais le nouveau système offrira des possibilités complémentaires de stockage très étendues, indispensables aux besoins actuels de certains usagers.
- ▲ disparition d'un certain nombre de logiciels anciens, annoncée lors de la mise en place d'Unicos 7, et qui n'avaient été conservés par le constructeur sous Unicos 8 que par souci de compatibilité. Ces logiciels disparaissent sous Unicos 9. Tel est le cas (entre autres), de l'ancien Bourne shell (*osh*), remplacé officiellement dès

Flash informatique

Les articles de ce journal ne reflètent que l'opinion de leurs auteurs. Toute reproduction, même partielle, n'est autorisée qu'avec l'accord de la rédaction et des auteurs.

Rédacteur en chef: J. Dousson,
fi@sic.adm.epfl.ch

Comité de rédaction: J.-D. Bonjour, J.-M. Chenais,
M. Crvcnanin, L. Desimone,
J.-J. Dumont, P.-A. Haldy,
P. Lachaize, H. Le Pezennec,
F. Roulet, Ch. Simm & J.
Virchaux

Composition: A. Raposo de Barbosa
Impression: REPRO

Tirage: 4000 exemplaires
W: [http://savwww.epfl.ch/SIC/SA/
publications/](http://savwww.epfl.ch/SIC/SA/publications/)

Adresse: SIC-SA EPFL 1015 - Lausanne
☎ 021/693 22 46 & 22 47

ISSN 1420-7192



9 771420 719001

maintenant par le Korn shell (ksh), seul shell reconnu par le standard POSIX.

- ▲ adaptation des logiciels aux standards officiels tels que définis dans l'industrie. Dans ce cadre, de **très nombreuses commandes et utilitaires d'Unix ont été sous Unicos 9 modifiés pour répondre aux normes XPG4 de X/Open**. Ces standards supportent toutes les fonctionnalités de la norme POSIX. Il s'agit pour la plupart d'adjonction ou de modification de paramètres d'appel des commandes Unicos. Ces modifications sont souvent mineures, mais peuvent occasionnellement affecter le comportement de programmes et de scripts, que l'utilisateur devra adapter selon les circonstances. A titre d'exemple, des options ont été rajoutées ou modifiées dans les commandes très utilisées comme: **vi, tar, awk, make, docview, man, time, cd, bc, od, sar, pr, ps, nm, limit**.
- ▲ malgré des modifications qui se révèlent inévitables, Cray Research a le souci de garantir au mieux la compatibilité entre Unicos 8 et Unicos 9 dans les domaines suivants: commandes Unicos, syntaxe et sémantique des langages, exécution des codes absolus et relogeables des applications. A priori, le passage à Unicos 9 devrait être majoritairement transparent. Toutefois, l'utilisateur peut interpréter cette déclaration avec profit en recompilant et adaptant toutes ses applications à la première occasion.

PRINCIPAUX CHANGEMENTS

COMMANDES ET UTILITAIRES

Dès Unicos 9.x, certaines parties de l'interface utilisateur ne sont plus intégrées dans le système lui-même, mais sont livrées de façon séparée. Ainsi en est-il des **librairies Fortran** (libf, libu, libfi) qui sont intégrées dans la partie CrayLibs de l'environnement de programmation qui passe à la version PE 1.2. De même pour les utilitaires de mesure de performances (comme **atchop, atexpert, jumpview, profview**, etc.) qui sont dorénavant inclus dans le package CrayTools. Ces changements n'ont pas d'impact direct sur les applications, mais la documentation y relative se trouve réunie dans un manuel spécifique: *Tuning Guide to Parallel Vector Applications*, SG-2182.

COMMANDES UTILISATEURS ET INTERFACE DE PROGRAMMATION

- ▲ Distribution officielle de la révision majeure 19 de l'éditeur Emacs. En fait, cette version était déjà mise à disposition par le SIC peu après la mise en route de Unicos 8, évidemment sans les extensions de Cray. A noter qu'avec cette révision la façon de définir les touches de fonction doit être réadaptée dans le fichier ~/ .emacs.

- ▲ Plusieurs commandes et utilitaires disparaissent sous Unicos 9. Sont à mentionner principalement: **cl, nupdate, oawk, old, osh, pcpp, plcopy, pshell, whodo**.
- ▲ Commandes et utilitaires qui seront supprimés après Unicos 9: **Docview, xproc, xfm**, anciennes versions **obc, odc**.
- ▲ DMF: il convient de consulter les *man pages* pour les commandes **dmpu** et **dmget**.
- ▲ Gestion mémoire: toutes les fonctions précédemment documentées dans **memmgr(3)** ont été renommées sous Unicos 9 et se trouvent désormais décrites sous **malloc(3)**. La fonctionnalité des routines renommées n'est basiquement pas modifiée.
- ▲ A mentionner le support des *Threads* POSIX (**Pthreads**). La nouvelle sémantique est applicable seulement si les applications *multitaskées* sont recompilées. Une relecture soigneuse de la documentation est recommandée afin d'assimiler les quelques nouveaux concepts, comme la simple redéfinition d'un *process* dans un groupe «multitaské» pouvant contenir plusieurs *light-weight processes*.

IMPACT SUR LE T3D

Celui-ci restera mineur: le système passe de Max 1.3.0.1 à Max 1.3.0.2 avec Unicos 9, et ne concerne que la mise en place de quelques codes correctifs (pas de nouveaux *features*). La mise en place du système *I/O Phase III*, censée améliorer les performances des transferts d'entrées/sortie entre le T3D et Pascal reste réservée.

NOUVEAUX PRODUITS

Les produits (tels les compilateurs Fortran et C, assembleurs, et *Programming Environments*) en eux-mêmes sont mis à jour indépendamment des révisions des systèmes. Avec la mise en route de Unicos 9, ces produits ne changent pas. Toutefois, les utilisateurs trouveront sous la nouvelle arborescence **/opt** (récemment introduite par Cray) les nouveaux produits en cours de test, tant pour Pascal que T3D, (tel l'environnement de programmation PE 2.0). S'informer auprès des personnes de support pour l'utilisation de ces produits.

DERNIÈRES NOUVELLES

La mise en exploitation d'Unicos 9, révision 9.0.2.1 est prévue pour courant septembre. Au moment d'écrire ces lignes, restent encore à introduire les derniers codes correctifs, la configuration définitive des équipements Redwood, ainsi que quelques modifications locales du système. Selon la procédure habituelle, des tests d'exploitation d'abord restreints puis publics, sont prévus allant vers une ouverture progressive puis définitive d'Unicos 9 pour les usagers. ■

Secure Shell, ou cachez ce mot de passe que je ne saurais voir

par Martin Ouwehand, SIC

L'idée de mot de passe est connue depuis l'antiquité: Tacite nous rapporte

<http://the-tech.mit.edu/Classics/Tacitus/annals.xiii.html>

que le mot de passe de Néron était **optimae matris**, à la meilleure des mères (une forme d'humour noir puisqu'il fit tuer sa mère Agrippine). Avant lui, vers

450 av. J.-C., Euripide raconte dans sa pièce Rhesos <http://the-tech.mit.edu/Classics/Euripides/rhesus.sum.html>

comment Ulysse, l'homme aux mille ruses, extorque le mot de passe des Troyens à l'infortuné Diomède (faisant de lui l'ancêtre de nos pirates actuels). Mais il faut bien avouer que le mot de passe est une trouvaille très ingénieuse: moyennant un secret que nous pouvons emporter n'importe où dans le monde, à l'abri de notre mémoire, nous avons accès et nous seuls (espérons-nous) aux ressources qui nous ont été allouées sur nos ordinateurs. Aucun système proposé pour le remplacer n'offre tous ses avantages: impossible de se connecter par modem depuis la maison si on a oublié au bureau sa carte SecurID (qui affiche chaque trente secondes un nouveau mot de passe valable dans la tranche temporelle donnée) ! En congrès en Nouvelle-Zélande, comment utiliser sa carte à puce permettant de s'identifier si le lecteur de ladite carte se trouve à l'EPFL, aux antipodes ? (Les optimistes répondront que bientôt tous les ordinateurs disposeront d'un tel lecteur.)

Avant de tempérer cet enthousiasme et d'énumérer les inconvénients de ce système, je vais décrire le fonctionnement de l'authentification par mot de passe sous Unix.

STOCKAGE ET UTILISATION DES MOTS DE PASSE SOUS UNIX

S'il est proverbialement difficile de trouver une aiguille dans une botte de foin, il est enfantin de l'y cacher: c'est en résumé le principe à la base du stockage des mots de passe sous Unix. En termes informatiques cela se traduit par l'utilisation de fonctions à sens unique (*one-way function* en anglais). En l'occurrence ce sont des procédures qui brassent de manière répétée les bits constituant le mot de passe tout en formant l'opération logique *ou exclusif* avec des états antérieurs de la suite de bits résultant de ces opérations. Le détail de cette procédure n'a pas besoin d'être tenu secret (et de fait il est publié et accessible à tous, puisqu'il s'agit de

DES, *Data Encryption Standard*)

<http://www.nist.gov/itl/div879/pubs/fip46-2.htm>

parce qu'il est pratiquement impossible de l'inverser: toute suite de bits de longueur n est le résultat du *ou exclusif* de n couples de suites de longueur n et cette opération étant appliquée de multiples fois on arrive à un nombre prohibitif de possibilités à investiguer. C'est la suite de bits ainsi obtenue et non le mot de passe lui-même qui est stockée dans un fichier. Cette méthode est jugée si sûre que sur certains systèmes les mots de passe ainsi encryptés sont accessibles à tous les utilisateurs (dans le fichier */etc/passwd*).

Pour ajouter un grain de sel à cette explication, ajoutons



que sous Unix, l'une d'entre 4096 fonctions à sens unique analogues est choisie au hasard lors de l'encryptage, le paramètre distinguant cette fonction de toutes les autres (appelé *salt* en anglais) étant stockée avec le mot de passe encrypté.

Par ailleurs une tentative de retrouver un mot de passe à partir du résultat de la fonction à sens unique en énumérant de manière exhaustive les mots de passe possibles, en les soumettant un à un à cette fonction et en comparant les résultats obtenus (une attaque *by brute force* en anglais) a très peu de chance d'aboutir: même un ordinateur capable d'encrypter un million de mots de passe par seconde (ceci doit être de l'ordre de grandeur de la capacité des plus grosses machines parallèles existant à l'heure actuelle) mettra en moyenne plusieurs siècles à réaliser ce travail.

Dans une telle attaque frontale, on pourrait éventuellement restreindre l'ensemble des mots de passe à essayer s'il y avait une corrélation entre l'argument et le résultat de la fonction à sens unique: on s'assure par tests statistiques que ce n'est pas le cas. On peut donc dire que notre fonction à sens unique est chaotique: elle est parfaitement déterministe mais ses valeurs pour différents arguments semblent être tirées au sort.

Chaque fois que le système doit vérifier l'identité d'un utilisateur, il lui demande son mot de passe, applique à celui-ci la fonction à sens unique décrite ci-dessus (en utilisant le même grain de sel) et compare le résultat avec le mot de passe encrypté qui a été stocké sur disque: s'ils sont identiques, le système considère que l'utilisateur est bien celui qu'il prétend être. Grâce à cette manière de faire, le mot de passe *en clair* n'a qu'une existence extrêmement furtive en mémoire et n'est jamais écrit sur disque.

Un dernier point de détail pour conclure ce paragraphe: nous avons parlé de mot de passe encrypté ce qui n'est pas tout à fait exact, puisqu'il est justement supposé ne plus jamais être vu en clair (c'est à dire décrypté). Les puristes parlent donc de signature ou de valeur *hashée* du mot de passe, mais cet abus de langage est assez répandu.

FAIBLESSES DU SYSTÈME DES MOTS DE PASSE

La principale faiblesse vient des utilisateurs qui choisissent des mots de passe plus ou moins faciles à deviner (noms communs, noms propres). Des millions de milliards de mots de passe possibles, ils restreignent leur choix à un ensemble qui n'en compte que quelques centaines de milliers. Outre des tentatives à l'aveugle (*le mot de passe de Dominique est sûrement Camille, ces deux-là s'aiment tellement !*), une attaque frontale telle que décrite plus haut devient possible pour un pirate ayant accès aux mots de passe encryptés.

De fait Alec Muffett a écrit l'utilitaire **Crack** qui, partant d'un dictionnaire de mots quelconques, va tester s'il l'un d'entre eux ne correspond pas à un mot de passe du fichier */etc/passwd*. Ce programme contourne même les astuces assez répandues consistant à prendre comme mot de passe un mot courant et à le soumettre à des substitutions faciles à retenir (par exemple utiliser **@**, **0** et **l** au lieu de **a**, **o** et **i**), à l'écrire à l'envers ou en alternant les minuscules et les majuscules. Même si ce programme est bien sûr populaire chez les pirates, le principe *no security through obscurity* fait qu'Alec Muffett n'est pas du tout considéré comme un scélérat: son programme est utilisé par des administrateurs dans le monde entier pour vérifier que leurs utilisateurs n'ont pas choisi de mots de passe susceptibles d'être devinés.

Une deuxième faiblesse est que sous Unix, le mot de passe comporte au maximum 8 caractères de 7 bits. Les pirates perdraient leur temps avec Crack si la longueur des mots de passe était par exemple de 50 caractères: même en utilisant des mots courants les possibilités seraient trop nombreuses.

Une troisième faiblesse est que la méthode d'encryptage est la même pour presque tous les ordinateurs Unix. Une bonne défense contre l'utilisation de Crack par les pirates serait d'étendre l'idée du grain de sel évoquée plus haut: chaque administrateur choisirait au hasard un membre parmi des millions d'une famille d'algorithmes d'encryptage, sans divulguer duquel il s'agit. Apparemment, les constructeurs n'offrent pas une telle solution parce qu'il arrive que le fichier de mots de passe soit partagé entre plusieurs machines, notamment par NIS (Network Information System).

Nous reviendrons plus loin sur le dernier point faible des mots de passe: ils passent en clair sur le réseau.

CONSEILS AUX UTILISATEURS

- ▲ Les mots courants, les prénoms, les noms de lieux, de personnages littéraires ou historiques, de héros hollywoodiens, etc. sont à proscrire absolument comme mots de passe, ainsi que leurs variations (écrire le mot à l'envers, utiliser minuscules et majuscules, substituer **a** par **@**, etc.). À éviter également, les chaînes formées de caractères voisins sur votre clavier (**qwerty**, **asdfghj**, etc.)
- ▲ Faites travailler votre imagination jusqu'à ce qu'elle produise un mot de passe qui pourrait tout aussi bien être tiré au sort.
- ▲ Utilisez pour le former toute la gamme des caractères disponibles:
 - lettres minuscules
 - lettres majuscules
 - chiffres

- autres signes: ponctuations, parenthèses, signes arithmétiques (+, >, etc.), accents, etc. sans privilégier une classe de caractères par rapport à une autre.
- ▲ Mettez au point un truc mnémotechnique pour vous en souvenir.
- ▲ N'écrivez pas vos mots de passe sur un bout de papier, un post-it collé à votre écran, etc.
- ▲ Si vous devez utiliser une liste de mots de passe parce que vous en avez trop, conservez-la comme un document précieux.
- ▲ Ne communiquez jamais votre mot de passe à autrui: il ouvre l'accès à des ressources informatiques qui vous ont été allouées à titre personnel.
- ▲ Ne laissez jamais passer votre mot de passe sur le réseau en clair, n'utilisez que des connexions encryptées (voir plus loin).

CONSEILS AUX ADMINISTRATEURS

- ▲ Si possible, activez le système des *shadow passwords*, qui empêche l'accès par les utilisateurs de votre machine aux mots de passe encryptés. Ainsi aucun d'entre eux, s'il est mal intentionné, ne pourra les soumettre à Crack.
- ▲ Ne vous laissez jamais éduquer vos utilisateurs quant au choix de bons mots de passe.
- ▲ Si vous êtes dirigeant, vous pouvez choisir un bon mot de passe pour eux et les empêcher de le changer en leur retirant le droit d'exécution à la commande `/bin/passwd`:
`/bin/chmod o-x /bin/passwd`
 Il faut naturellement bien peser le poids de cette décision: il vaut mieux des utilisateurs s'occupant spontanément de leur sécurité que des utilisateurs de mauvaise volonté parce que *brimés*.
- ▲ Installez **passwd_wrapper**, un emballage de la commande **passwd** de votre système filtrant les mauvais mots de passe suivant des critères que vous pouvez vous-même déterminer. Voir:

http://slwww.epfl.ch/SIC/SL/Securite/outils/passwd_wrapper.html

Certains constructeurs offrent une gestion de la durée de validité des mots de passe (*password aging*). Ce système force les utilisateurs à changer de mot de passe à intervalles réguliers (typiquement un ou deux mois). L'idée est de ne pas laisser le temps à un adversaire de trouver le mot de passe d'un utilisateur de votre machine. Les détracteurs de ce système font valoir qu'il vaut mieux utiliser pendant longtemps un bon mot de passe que de choisir souvent de mauvais mots de passe. De plus, disant ce système renforce la tendance des utilisateurs à écrire leur mot de passe et à abdiquer de leur responsabilité. Je n'ai pas d'opinion tranchée en la matière et je vous laisse juges.

LES BONNS MOTS DE PASSE SE LISENT SUR LE RÉSEAU

Suivant ces recommandations, vous avez choisi un mot de passe difficile à deviner, c'est bien. Mais voici qu'apparaît alors une nouvelle menace: les données échangées entre les ordinateurs passent en général telles quelles, en clair, sur le réseau. Tout ce que vous imprimez, tout votre courrier électronique, mais surtout vos mots de passe, lorsque vous vous connectez d'un ordinateur à un autre (par **telnet**, **rlogin**, **rsh** ou **ftp**), transitent sur le réseau sans qu'aucune disposition spéciale ne soit prise pour les cacher. Or la plupart des machines Unix offre la possibilité de lire tous les paquets passant sur le brin Ethernet auquel ils sont connectés et il va sans dire que les pirates informatiques y ont largement recours pour étendre leur emprise sur un site (cette activité de reniflage, ou *sniffing* en anglais, leur permet de multiplier les machines auxquels ils ont accès, en lisant les mots de passe sur le réseau).

Que les données passant sur le réseau ne soient pas mieux protégées (par exemple en les encryptant) peut être considéré comme un défaut de TCP/IP et de fait, plusieurs propositions sont en cours de discussion pour y remédier. Citons SKIP

<http://skip.incog.com>

et d'autres procédés d'encryptage au niveau de la couche IP

<http://www.ietf.org/html.charters/ipsec-charter.html>

ou TCPcrypt (encryptage au niveau de la couche TCP),

<http://nic.merit.edu/routing.arbiter/RA/security/>

En attendant que de telles solutions soient plus généralement disponibles, on peut, pour se protéger des renifleurs:

- ▲ ne jamais laisser passer de mots de passe sur le réseau,
- ▲ utiliser des mots de passe *jetables*, valables une seule fois,
- ▲ cacher les mots de passe en utilisant des connexions encryptées.

Nous allons expliquer comment réaliser chacune de ces trois possibilités.

DU BON USAGE DES FICHIERS .RHOSTS

La première se base sur l'utilisation des fichiers **.rhosts**. Comme on le sait, si la ligne

```
machine1.epfl.ch user1
```

figure dans le fichier **\$HOME/.rhosts** de l'utilisateur **user2** sur l'ordinateur **machine2** (généralement, **user1** et **user2** sont identiques) alors **user1** pourra démarrer une session sur la machine **machine2** sous le compte

user2, par la commande **rlogin**, sans entrer le mot de passe de **user2** et a fortiori, sans que celui-ci ne transite sur le réseau. Cette manière de faire est particulièrement adaptée aux utilisateurs *sédentaires* qui travaillent (physiquement) toujours depuis le même ordinateur: ils ouvrent des sessions interactives sur la console (et le mot de passe ne passe donc pas par le réseau) et de là ils lanceront leurs programmes sur d'autres machines du réseau sans mot de passe, par l'utilisation judicieuse de fichiers **.rhosts**.

Toutefois ce procédé présente plusieurs inconvénients: tout d'abord, un pirate pénétrant sur une machine aura du coup également accès, sans effort, à toutes les machines dont les fichiers **.rhosts** ouvrent l'accès à la machine piratée. Ensuite, tout le trafic entre ordinateurs continue à être lisible sur le réseau, y compris les mots de passe entrés sur la machine *remote* (**machine2** dans l'exemple ci-dessus). Il est donc dangereux d'y devenir **root** en utilisant la commande **su**. De plus, cette solution ne s'applique pas aux connexions par **ftp**, pour lesquelles le mot de passe continue à être visible. Enfin, l'utilisation des fichiers **.rhosts** se basant en fin de compte sur l'adresse IP des machines, des attaques par usurpation d'adresse IP (*IP spoofing* en anglais)

http://nic.switch.ch/network/security/cert_advisories/CA-95:01.IP.spoofing

deviennent possibles.

MOTS DE PASSE JETABLES, VALABLES UNE SEULE FOIS

Le logiciel OPIE (One-time Passwords In Everything,

<ftp://ftp.nrl.navy.mil/pub/security/opie/>)

est mis à la disposition d'Internet par le laboratoire de recherche de la Marine Américaine (NRL) qui a repris et étendu le logiciel S/Key

<http://www.bellcore.com/SECURITY/skey.html>

de Bellcore.

Le principe à la base de OPIE est de rendre le reniflage du réseau impraticable, par le biais de mots de passe *jetables* (*one-time passwords* en anglais): un pirate aura beau en avoir lu un sur le réseau, celui-ci ne sera plus valable. Dans la pratique, OPIE utilise de multiples avatars d'un mot de passe de base, en répétant simplement la procédure habituelle d'encryptage du mot de passe décrite ci-dessus, chaque résultat de l'encryptage constituant une autre version du mot de passe. OPIE utilise ces versions différentes dans le sens inverse du nombre d'itérations: d'abord le mot de passe encrypté 100 fois, puis 99 fois, etc. puisque c'est dans ce sens qu'il est difficile de *remonter*. Ces mots de passe sont lus ou écrits dans un *alphabet* de 2048 mots anglais assez court, par ensemble de 6 mots (ceci correspond donc

à 66 bits d'information, dont 64 sont effectivement utilisés, ce qui est un peu mieux que les mots de passe de 56 bits d'Unix). Par exemple:

```
LISA OIL SILT KEEN DARE HARK
```

OPIE est constitué de nouvelles versions des programmes identifiant les utilisateurs par mot de passe (**login**, **ftpd** et **su**) ainsi que de programmes propres gérant les mots de passe (**opiekey** et **opiepasswd**, l'analogue de **passwd**). Là où les versions Unix traditionnelles de ces programmes demandaient à l'utilisateur son mot de passe, les programmes d'OPIE lui lance un *défi*, en affichant un numéro de génération de mot de passe (99 dans l'exemple) ainsi qu'un *germe* (*seed* en anglais, ici *se1433*):

```
login: user1
otp-md5 99 se1433
Response or Password:
```

(Le rôle de ce germe est de rendre plus difficile les attaques frontales qui sont décrites ci-dessus). Se basant sur ces deux éléments, l'utilisateur peut retrouver la version du mot de passe qu'attend OPIE par la commande **opiekey** qui la lui donnera après qu'il aura entré son mot de passe *de base* (celui qu'OPIE encrypte plusieurs fois pour en obtenir différents avatars):

```
$ opiekey 99 se1433
Using the MD5 algorithm to compute
response.
Reminder: Don't use opiekey from
telnet or dial-in sessions.
Enter secret pass phrase: (l'utili-
sateur entre le mot de passe de
base)
MAUL NUMB MOTH FRET BARK CARR
(Affichage de opiekey)
```

Dans la plupart des cas, le défi proviendra d'une machine distante mais on invoquera **opiekey** depuis la console de la machine sur laquelle on travaille, de manière que le mot de passe de base ne soit pas lisible sur le réseau. Si besoin est (séjour dans un site sans **opiekey**, etc.), on peut demander à **opiekey** d'afficher un certain nombre d'avatars du mot de passe de base, par exemple pour les vingt prochains défis, et les noter, ou les imprimer si on dispose d'une imprimante directement attachée à un ordinateur (une imprimante accédée par le réseau rendrait bien sûr illusoire la fiabilité du système.)

Dans ce contexte, notons qu'il existe des versions de **opiekey** pour PC (Windows 3.11, Windows 95 et Windows NT) et Macintosh. Dans le cas de tels ordinateurs personnels coupés du réseau, on a un gain de sécurité certain, l'idéal restant une calculatrice programmable, facile à emporter avec soi (mais le programme équivalent à **opiekey** reste à écrire !)

Vous trouverez des indications plus précises quant à l'installation d'OPIE sous **W**:

<http://slwww.epfl.ch/SIC/SL/Securite/outils/opie-install.html>

SSH (SECURE SHELL)

SSH <http://www.cs.hut.fi/ssh/> est un logiciel écrit par le Finlandais Tatu Ylönen <http://www.cs.hut.fi/~ylo/> offrant des fonctionnalités semblables à **rlogin**, **rsh** et **rpcp** mais dont les connexions entre les machines cliente et serveur sont encryptées. On obtient le nom de la version SSH des commandes mentionnées en remplaçant le **r** initial par **s** (pour **secure**): **slogin**, **ssh**, **sshd** et **scp**. Il y a en outre quelques commandes nouvelles servant à gérer les clés utilisées pour l'encryptage. En effet, comme PGP (Pretty Good Privacy), SSH utilise un système d'encryptage hybride à clés publiques et à clés secrètes. L'encryptage à clés publiques utilisé est RSA, dont le lecteur se souviendra (cf. l'article de mon collègue Claude Lecommandeur paru dans le FI7/95:

<http://sawwww.epfl.ch/SIC/SA/publications/FI95/fi-7-95/7-95-page3.html>)

qu'il permet l'échange confidentiel de données entre deux entités (personne, ordinateur) sans que celles-ci n'aient eu auparavant à partager par un canal sûr une quelconque clé secrète: chacun possède une clé privée et une clé publique et encrypte en utilisant sa clé privée et la clé publique de son correspondant, le système étant conçu (à travers une relation arithmétique spécifique entre les clés de chacune de ces paires) pour que ce dernier puisse décrypter par sa propre clé privée et la clé publique de l'expéditeur. Comme cette méthode est assez lente (elle implique des calculs arithmétiques sur de très grands entiers, typiquement 1024 bits), elle sert principalement à l'échange de clés lors de la mise en œuvre de méthodes d'encryptage traditionnelles à clé secrète (on a le choix entre RC4, DES, IDEA et DES triple, du plus rapide au plus lent) que SSH utilise pour le gros du trafic entre machine cliente et serveur.

De plus, SSH se sert des possibilités d'authentification de RSA

http://www.rsa.com/rsalabs/faq/faq_rsa.html#rsa.1

pour s'assurer que les acteurs impliqués (utilisateur, machines cliente et serveur) sont bien ceux qu'ils prétendent être: SSH n'est donc pas susceptible comme **rsh/rshd** à des attaques par usurpation d'adresse IP.

SSH est également capable d'établir des connexions encryptées entre une machine cliente et une machine serveur pour n'importe quel port TCP, par transmission de port (*port forwarding* en anglais.) Ceci est particulièrement important pour le système X Window: très souvent en effet, on utilisera **rsh** pour lancer sur une autre machine un processus client du serveur X depuis lequel on travaille (par exemple **xterm**). Dans ce cas, remplacer **rsh** par **ssh**

n'apporterait pas grand chose, puisque les caractères tapés au clavier (mot de passe, entre autres) transitent entre les deux machines par une connexion X Window, différente de la connexion encryptée de **ssh**. C'est pourquoi Tatu Ylönen a pensé à établir automatiquement avec chaque connexion par **ssh** une connexion X Window encryptée, en utilisant ce système de transmission de port.

SSH est un excellent logiciel qui résoud de manière satisfaisante le grave problème des données lisibles lorsqu'elles transitent par le réseau. Il est de plus assez simple à utiliser et je recommande donc vivement de l'installer sur vos ordinateurs. Vous trouverez des indications plus précises quant à l'installation de SSH sous **W**:

<http://slwww.epfl.ch/SIC/SL/Securite/outils/ssh-install.html>

OFFRE D'EMPLOI

DEUX POSTES D'INGÉNIEURS EPF

en informatique, microtechnique, mécanique ou électricité pour un mandat d'une durée de un à trois ans portant sur un projet intitulé

ARCHITECTURE LOGICIELLE POUR DES MACHINES DE PRODUCTION

Il s'agit d'un projet pluridisciplinaire de l'Institut de Microtechnique et du Laboratoire de génie logiciel. Le projet vise à concevoir une architecture du logiciel, produire des composants paramétrés et des mécanismes d'assemblage de ces composants (framework), le tout pour des machines de production multi-axes numériques. La première phase du projet consiste en l'étude de l'existant et une analyse de ses forces et faiblesses. Le travail se fera en étroite collaboration avec des entreprises qui produisent ou utilisent de telles machines. Il nécessitera des déplacements fréquents et des séjours de courtes durées dans ces entreprises.

Les deux employés devront travailler en étroite collaboration. Leurs compétences seront complémentaires, couvrant aussi bien l'informatique que la technologie des machines de production multi-axes numériques. La langue de travail est le français. Des connaissances de l'allemand sont un atout.

L'entrée en fonction souhaitée est fixée au 1er octobre 1996, ou à une date à convenir. La durée du contrat d'engagement sera de 12 mois, renouvelable. Les candidats doivent être de nationalité suisse ou au profit d'un permis de séjour/travail. Les candidatures féminines sont particulièrement bienvenues.

Pour plus d'informations sur le projet et les conditions d'engagement, veuillez vous adresser aux professeurs Alfred Strohmeier et Jacques Jacot. Les candidatures, accompagnées des pièces usuelles, doivent leur être envoyées aux adresses ci-dessous.

Prof Alfred Strohmeier,
Laboratoire de génie logiciel, EPFL-DI-LGL,
CH-1015 Lausanne
✉ alfred.strohmeier@di.epfl.ch, ☎ 021 693 42 31
W <http://lgwww.epfl.ch/>

Prof Jacques Jacot
Institut de Microtechnique, EPFL-DMT-IMT
CH-1015 Lausanne
✉ jacques.jacoteimt.dmt.epfl.ch, ☎ 021 693 59 08



→→ Suite de la première page

Depuis quelques numéros, notre *claviste*, comme elle aime à s'appeler, n'a pas résisté au plaisir de tester des nouvelles possibilités et de vous en faire profiter puisque maintenant le FI est aussi accessible en format PDF (Portable Document Format) sur le Web. La création du format PDF se fait depuis PageMaker 6.0 qui offre cette possibilité (voir *Clavitudes ou les affres de PageMaker 6.0* paru dans FI2/96 :

<http://sawwww.epfl.ch/SIC/SA/publications/FI96/fi-2-96/2-96-page20.html>).

Pour en savoir plus sur PDF, reportez-vous à l'article de François Roulet *Acrobat, jonglez avec vos fichiers* paru dans le FI1/96 :

<http://sawwww.epfl.ch/SIC/SA/publications/FI96/fi-1-96/1-96-page10.html> .

Pour lire des fichiers au format PDF, sachez qu'il existe différents outils *Acrobat Reader*.

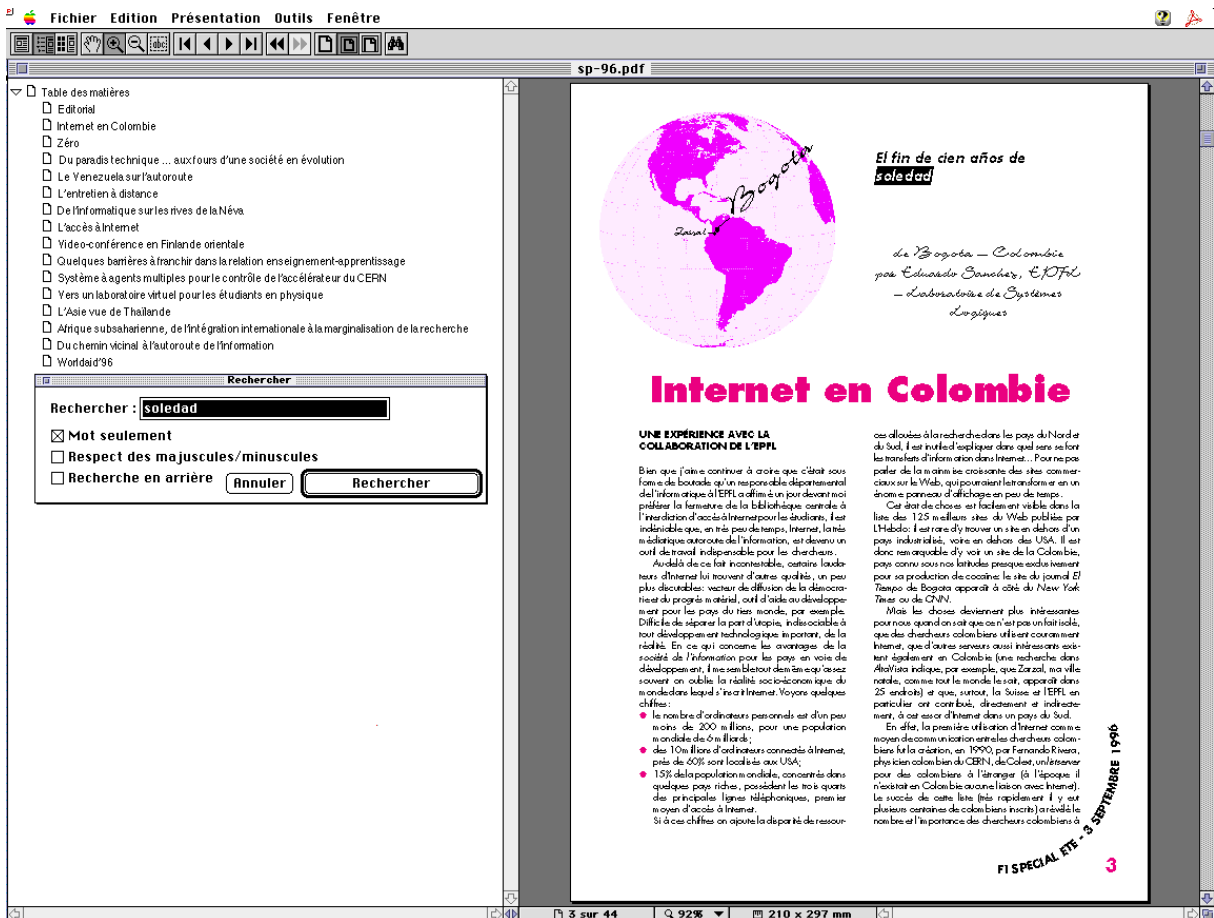
▲ sous forme d'applications externes appelées par votre navigateur si votre configuration est à jour. Si vous utilisez Netscape (depuis la version 2): Menu **Options/General Preferences/Helpers**,

▲ sous forme de **plug-in**, c'est-à-dire complètement intégrés au navigateur, ce qui est possible sur certaines plates-formes (tous les détails sur le site d'ADOBE: <http://www.adobe.com/>).

Le format PDF offre la possibilité de *feuilleter* le journal à l'écran, d'accéder directement à un article depuis le sommaire ou de faire une recherche dans le numéro. ■



Le premier FI sur le Web



Le spécial été 96 «Terra informatica» vu par Acrobat Reader

Cache Web, ou comment optimiser l'utilisation du réseau

par Jacqueline Dousson & Claude Lecommandeur, EPFL-SIC

LE PRINCIPE DU CACHE WEB

Deux motivations principales peuvent conduire à réfléchir à une technologie *cache*:

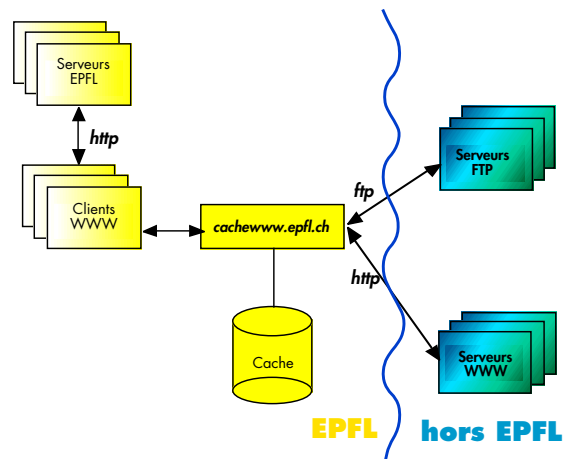
- ▲ augmenter la qualité du service à l'utilisateur, en diminuant le temps d'attente pour obtenir l'information désirée
- ▲ mieux gérer son porte-monnaie, c'est-à-dire réduire les coûts inhérents au trafic réseau.

La situation d'engorgement du réseau à certaines heures et les augmentations des factures de SWITCH, ont donc naturellement amené le SIC à mettre en place cette technologie.

Après une phase expérimentale, le cache WEB devient officiel à l'EPFL et son efficacité sera d'autant plus grande que vous serez plus nombreux à l'utiliser... en effet, il est naturel de penser que les pages Web qui nous intéressent ont de grandes chances d'en intéresser d'autres!

Le principe en est très simple. Une machine est configurée pour recevoir les requêtes qui proviennent de l'intérieur du site EPFL et qui demandent des informations sur le WEB à l'extérieur du domaine. Cette machine examine si le document a été demandé précédemment:

- ▲ il se trouve déjà sur la machine cache. Une *mini* requête est envoyée vers le serveur où il est censé résider, pour savoir s'il a été modifié entre temps. En cas de modification, on va rechercher ce document et c'est cette nouvelle version qui sera gardée à son tour sur la machine cache; sinon, c'est la page stockée sur la machine cache qui est envoyée au client **W**. Dans ce dernier cas, le gain sur le trafic extérieur à l'école est très important.
- ▲ c'est la première fois que cette page est demandée, la requête est envoyée à l'extérieur, on se retrouve dans le cas classique; mais le document est stocké sur la machine cache en vue d'éventuelles requêtes ultérieures.



Pour les requêtes s'adressant à des serveurs internes à l'EPFL, il est bien sûr inutile de passer par la machine cache puisqu'elles ne provoquent aucun trafic externe, ce que permettent les configurations actuelles des navigateurs.

Important: il ne faut pas confondre le cache dont il est question ici avec les possibilités qu'offrent les navigateurs comme Netscape d'utiliser un cache au niveau *local* sur votre machine: celui-ci est un cache disque ou mémoire que vous configurez à travers Options/Network Preferences/Cache.

Plusieurs logiciels proxy-cache sont disponibles sur le marché. Nous avons choisi celui développé au départ par l'Université du Colorado (Harvest); en effet, ce logiciel gratuit a beaucoup de succès dans la communauté internaute et offre la possibilité de travailler hiérarchiquement (voir plus loin le paragraphe: **Des caches au niveau de la Suisse**). Comme il arrive souvent dans le monde Internet, l'équipe d'universitaires a éclaté; une partie a fondé une société privée qui commercialise les nouvelles versions d'Harvest (**netcache**); les développements de la version universitaire gratuite ont été repris par le National Laboratory for Applied Network Research sous le nom de Squid.

La configuration actuelle à l'EPFL mais qui peut évoluer selon les besoins, dispose d'un disque de 1GB. Les fichiers de type scripts (cgi-bin) ne sont pas stockés. Les documents demandés par le protocole ftp depuis une page Web sont stockés. La gestion de l'espace cache se fait selon le principe suivant: c'est le document dont l'accès est le plus ancien qui disparaît le premier. La machine sur lequel est installé le logiciel cache porte le nom de: cachewww.epfl.ch.

COMMENT L'UTILISER

Si vous utilisez le navigateur NETSCAPE (à partir de la version 2), sous Options/Network Preferences/Proxies, cocher **Automatic Proxy Configuration**, et entrer l'URL suivante:

<http://cachewww/netscape.proxy>

dans le champ libre. Ce passage par une configuration automatique offre l'avantage de pouvoir jouer sur différents paramètres; il est notamment prévu que les requêtes qui s'adressent à des serveurs de l'EPFL ne passent pas par le cache.

Si vous utilisez le navigateur Mosaic, il faut mettre dans le fichier de ressources, les lignes suivantes:

**Mosaic*httpProxy:<http://cachewww.epfl.ch:3128/>
Mosaic*ftpProxy:<http://cachewww.epfl.ch:3128/>**

Si vous utiliser le navigateur MS Internet Explorer 3.0, sous le menu **Options/Connection**, cochez **Connect through a proxy server** et sous **Settings** entrez dans les champs HTTP et FTP: **cachewww** et **3128** pour le port.

DES CACHES AU NIVEAU DE LA SUISSE

Switch qui est notre prestataire pour nous relier à Internet étudie également la mise en place d'une telle technologie. Leur choix s'est d'ailleurs porté sur le même logiciel (Squid). Actuellement nous fonctionnons en *voisins* avec Switch, l'ETHZ et l'Université de Berne; ceci signifie que si le document demandé n'est pas trouvé dans le cache EPFL, une requête est envoyée vers les *voisins* pour voir s'ils l'ont stocké, avant d'envoyer la requête au serveur originel. Ce fonctionnement n'est envisageable qu'avec un petit nombre de *voisins*. Dans une deuxième phase, la machine Switch travaillera comme *parent* des autres caches locaux, ce mode hiérarchique est en effet prévu dans le logiciel; il a été mis en place avec succès dans différents pays.

QUELQUES STATISTIQUES

L'analyse des chiffres dont on dispose montre que malgré un nombre encore assez restreint d'utilisateurs le passage par le cache a permis d'économiser sur le

dernier mois au moins 2.6 GB calculé ainsi: un volume de documents trouvés dans le cache en moyenne par jour ouvrable de 130MB pendant 20 jours...

Evidemment ce chiffre ne peut qu'augmenter avec le nombre d'utilisateurs du cache, puisqu'en élargissant le spectre des documents recherchés à travers le cache, on augmente la probabilité de «hits» (1 «hit» par document demandé et trouvé dans le cache), qui tourne aujourd'hui autour de 30%.

N.B. les termes *pris chez les voisins* qui apparaissent dans les tableaux de statistiques (voir l'URL plus bas) signifient que le document n'était pas résident sur le cache de l'Ecole mais sur un cache d'un de nos voisins (voir plus haut **Des caches au niveau de la Suisse**). Evidemment en termes de coût, cela ne change rien puisqu'un byte qui provient de Berne nous revient aussi cher qu'un byte de Palo-Alto, avec les grilles de facturation actuelles, mais en termes d'efficacité et d'encombrement du réseau international, le gain est évident.

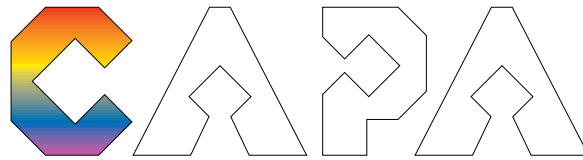
QUELQUES PROBLÈMES QUE VOUS POUVEZ RENCONTRER

Vous serez vite séduits par la rapidité avec laquelle vous proviennent la plupart des pages que vous demanderez. Evidemment, cela n'aura pas d'effet pour des pages destinées à un public plus restreint, ou qui font appel à des scripts.

Comme le cache garde en mémoire pendant un certain temps l'état des documents demandés et du serveur appelé, vous pouvez forcer, si vous l'estimez nécessaire, une connexion au serveur originel par un **Reload** ou **Maj-Reload**.

QUELQUES ADRESSES POUR CEUX QUI VEULENT EN SAVOIR PLUS

- ▲ la home page de Squid
<http://www.nlanr.net/Squid/>
- ▲ les configurations des différents navigateurs pour une bonne utilisation du cache qui décrit les fonctionnalités de Squid
<http://slwww.epfl.ch/SIC/SL/servdist/cacheWWW.html>
et comment configurer son browser
<http://slwww.epfl.ch/SIC/SL/servdist/cacheWWWconfig.html>
- ▲ les statistiques de l'utilisation du cache à l'Ecole, chaque jour, et par département
<http://slwww.epfl.ch/cgi-bin/cachestats.pl/>
- ▲ les chiffres de la consommation SWITCH par protocole, par jour, par unité, de l'EPFL
<http://stiwww.epfl.ch/conso/epfl/> ■



L'informatique parallèle: outil de base pour l'ingénieur

MARDI 8 OCTOBRE 1996 À 14H00, SALLE CO3, EPFL - ECUBLENS

Qu'il s'agisse de construction en génie civil, de mise au point de machines d'usinage, d'écoulement dans une turbine ou d'autres exemples, les ingénieurs doivent faire face aujourd'hui à des problèmes de plus en plus complexes et pluridisciplinaires.

Ceux-ci trouvent des solutions grâce aux progrès de l'informatique, dont les plus récents développements offrent de meilleures performances –notamment grâce au calcul parallèle–, un partage plus aisé des informations et des outils de visualisation conviviaux. C'est pour répondre aux besoins industriels en services informatiques adaptés à la résolution de tels problèmes complexes pluridisciplinaires qu'a récemment été créé CAPA, le Centre pour les Applications Parallèles et Avancées, à l'EPFL.

Ce centre, ses activités et des exemples de projets seront présentés lors de cette Rencontre EPFL-Economie, qui sera retransmise en vidéo-conférence au Centre suisse de calcul scientifique (CSCS/SCSC) à Manno (Tessin).

- 14h00** Le calcul parallèle bientôt à la portée de tous
Prof. Michel Deville, Institut de machines hydrauliques et de mécanique des fluides, EPFL
- 14h20** Coopérations industrielles et interdisciplinaires au CSCS/SCSC: un succès continu
M. Jean-Pierre Therre, Centre suisse de calcul scientifique (CSCS/SCSC), Manno
- 14h40** The ABB-CSCS/SCSC collaborative R&D project on the ESP Electrofilter
MM. Ulrich Kogelschatz et Walter Egli, ABB, Baden; M. Edgar Gerteisen, CSCS/SCSC, Manno
- 15h00** CAPA: la réponse aux problèmes interdisciplinaires
Mme Marie-Christine Sawley et M. Ralf Gruber, Service informatique central, EPFL
- 15h30** Pause café
Présentation de posters sur des projets interdisciplinaires
- 16h15** La modélisation du chauffage par induction: un exemple réussi de collaboration
M. Marek Swierskosz, Calcom SA, Lausanne
- 16h35** Increased demand for computational fluid dynamics at Sulzer Hydro
M. Helmut Keck, Sulzer Hydro AG, Zurich
- 16h55** Questions et discussion
- 17h30** Apéritif

Gratuit pour les membres cotisants de l'APLE (Association pour la promotion des liaisons EPFL-Economie), Fr 50.- pour les membres correspondants, Fr 90.- pour les non-membres (y. c. documentation), payables sur place. Entrée libre pour les collaborateurs et étudiants de l'EPFL.

Inscriptions et renseignements, **avant le vendredi 4 octobre 1996**, au

CAST - EPFL, 1015 Lausanne, tél. +41 21 693 35 75, fax: +41 21 693 47 47

Un serveur de News moderne à l'EPFL

par Franck Perrot, SIC, ✉ perrot@sic.epfl.ch

Depuis le 1er août 1996, nous utilisons à l'EPFL un serveur de News de nouvelle génération dont le principe est le *dynamic sucking*. Une entrée sur le Web vous permettra de régler certains des problèmes rencontrés et satisfaire les plus curieux d'entre vous:

<http://sasun4.epfl.ch/News/Dnews.html>

La principale motivation à ce changement est la réduction de notre trafic réseau. Mais d'autres considérations le favorisent également dont les moindres seraient sa modernité et son intelligence.

HISTORIQUE

Depuis leurs débuts, les News ont eu pour tâche principale de résoudre l'épineux problème qu'entraînait l'utilisation des *mailing-list*, la surabondance de *mails* inutiles. Abonné à plusieurs *mailing-lists* traitant de sujets d'intérêts divers, un utilisateur connecté contemplant, impuissant, le remplissage de sa boîte aux lettres électroniques alors que seule une infime partie de ce courrier l'interpellait. Avec le temps et l'augmentation du nombre de connectés, l'utilisateur arriva à la conclusion radicale qu'il valait mieux se désabonner de tout plutôt que de persister à lire sur écran un tas d'*âneries*. Le temps des *mailing-lists* était compté lorsque surgit des profondeurs d'Internet un nouveau concept informatique nommé Usenet.

Miracle! s'écria notre utilisateur tout à sa joie de pouvoir communiquer à nouveau. Usenet, en effet, permit une lecture intelligente des courriers toujours triés par centre d'intérêt, et ne remplissait plus les boîtes aux lettres de milliers d'utilisateurs. Coût réseau réduit, lecture sélective, centralisation du service, centres d'intérêt multipliés à l'infini, accès immédiat, logiciels clients efficaces et agréables, etc. Comment ne pas être satisfaits? L'évolution constante des logiciels serveur et client a fait la gloire internationalement reconnue d'Usenet et a grandement participé à celle d'Internet. Trop de gloire et de joie devaient à l'évidence et à raison attirer tous ceux qui s'en trouvaient exclus. Aussi Usenet commença à connaître ses premières faiblesses conceptuelles.

Le moindre serveur régional ou d'entreprise ne fut plus que faire pour freiner l'invasion des nombreux

enthousiastes d'Usenet qui déversaient leurs joies sous formes de textes, de logiciels ou d'images de plus en plus imposantes. Les pauvres serveurs s'en montraient fort marris et se trouvèrent vite sur les genoux. Par fierté, ceux-ci firent des miracles pour satisfaire autant que faire se peut leurs nombreux utilisateurs dont le bonheur ne faisait qu'empirer. Pour cela, les serveurs allèrent jusqu'à accepter les pires idioties dont la dernière fut sans doute fatale. Elle consistait à tout recevoir, coûte que coûte, pour détruire aussitôt de peur de sombrer dans le chaos. Par ailleurs, le coût du trafic réseau ne fit qu'augmenter. La fin était proche; la nouvelle génération aussi, avec une solution de nouveau miraculeuse comme il sied à cet univers.

LA NOUVELLE GÉNÉRATION: DNEWS

Dnews apporte la solution idéale à notre problème. Il s'appuie sur les précédents concepts d'Usenet, en intègre le nouveau, soit le *dynamic sucking*, et offre le tout en un ensemble homogène, plus autonome, plus intelligent et avec de nouvelles fonctionnalités. Lui aussi est déjà en constante évolution.

Le principe du *dynamic sucking* est d'aller chercher seulement ce que les utilisateurs lisent. Ainsi, la fierté des serveurs redevient réelle puisque tout peut être de nouveau reçu et ainsi satisfaire le plus grand nombre d'utilisateurs, tout en diminuant conséquemment le trafic réseau. L'honneur est sauf.

Voilà pour le conte. Notre nouveau serveur a évidemment ses faiblesses, mais cette fois-ci de jeunesse. Veuillez les lui pardonner le temps qu'il s'habitue à son nouvel environnement.

Quant au bénéfice principal escompté, à savoir la réduction des coûts du trafic réseaux, il est *a priori* certain. Avant de tirer un premier bilan, il faudra laisser la première phase de réglage se dérouler.

Nous faisons partie des premiers à nous engager dans ce nouveau procédé, mais soyez certains que d'autres nous emboîteront le pas dans les mois qui viennent.

Par ailleurs, sachez aussi que nous avons upgradé notre serveur (physique cette fois) d'information (News, **W**...).

Me contacter si besoin. ■

Eudora 3.0

par Pierre Collinet (*postmaster@epfl.ch*)

You have new mail.



Voilà la nouvelle version d'Eudora prête à l'emploi sur Cyclope pour les utilisateurs de Macintosh. Les versions Windows 3.11, Win95, WinNT et Newton sont en bêta test actuellement chez Qualcomm. Il faut donc attendre un peu encore.

Sur Cyclope, dans la partition Système, dossier Messagerie/Eudora, choisissez le dossier qui convient: 680x0 ou PowerPC, suivant le type de processeur de votre Mac, ou FAT si vous voulez éviter de réfléchir (ça prend plus de place sur le disque).

Notez que cette version est distribuée en ANGLAIS !, oui en anglais: la langue d'origine d'Eudora en fait. J'ai craqué devant la tâche de traduction cette fois à cause des trois versions (processeurs) qu'il n'y avait pas avant et devant la complexité croissante de l'application (sans compter que le support est d'autant plus lourd ensuite). Si vous insistez, je traduirai une des trois versions (seulement les textes des menus), celle qui conviendra le mieux à la majorité.

De toute façon, désormais les fichiers du Dossier Eudora auront le nom d'origine en anglais (donc ce sera **Eudora Folder** etc.), contrairement aux précédentes versions.

Pour ceux dont les notions d'anglais sont tellement rudimentaires, il reste la version précédente sur Cyclope: Eudora F2.1.3.

Compte tenu de ce qui précède, l'installation d'Eudora 3.0 doit se faire depuis une «copie propre» du serveur sur votre disque local, à laquelle on peut ajouter ses anciens classeurs personnels (fichiers avec une icône d'enveloppe AVEC adresse) et quelques autres fichiers comme les fichiers *Signature*, les Surnoms qu'il faut renommer en *Nicknames*...

Comme d'habitude, Eudora pour Mac est préconfiguré, tout est en place, sauf les trois champs

individualisant votre environnement : *POP Account*, *Real Name* et *Sender Address*). Eudora doit être lancé par un alias sur le fichier *Eudora Settings* (qui s'appelait Paramètres Eudora) et non pas sur l'application.

Un fichier d'aide à l'installation (détails) est disponible avec le programme sur Cyclope.

Eudora 3.0 offre un certain nombre de fonctions supplémentaires à la version précédente, mais seuls ceux qui utilisent le mail comme un *outil de travail* vont vraiment apprécier. Les améliorations sont listées dans Eudora 3.0, dans le menu d'aide (les bulles), rubrique *About this version*.

En très gros, il y a:

- ▲ filtres plus puissants pour: transmettre, rediriger, répondre, laisser sur le serveur, effacer du serveur ou rapatrier, sauter au suivant... tout ça pour classer et gérer vos messages sélectivement et automatiquement !
- ▲ l'interaction avec le serveur POP permet de gérer les messages sur le serveur sans nécessairement les rapatrier (option *Leave on server* à cocher dans la configuration habituelle et détails en pressant la touche Option et menu *File/Check Mail Specially...*).
- ▲ le texte peut contenir des mises en évidence (gras, italique, taille, styles, couleurs, etc) conformes à MIME (richtext). URL actives et cliquables (il faut configurer l'application à ouvrir en pressant la touche Option et double cliquer sur l'URL...).
- ▲ les annexes peuvent être posées simplement sur la feuille du message au lieu de passer par le menu habituel (Drag & Drop).
- ▲ la liste des Surnoms (ou *Nicknames*) est devenue un vrai *Address book* avec des champs pour plein d'infos, triables à souhait...
- ▲ les messages dépassant les 32 k ne sont PLUS saucissonnés en morceaux (c'était dû à la limitation de TeachText qui est maintenant remplacé par Writeswell Jr., applescriptable).
- ▲ création et gestion de *modèles* de réponse ou d'envois.

Je ne vous dis pas les autres, comme la barre d'outils et le *look* modulable, voyez vous-même dans le menu *Special/Settings*...

Utilisez les bulles d'aide (*balloons help*) autant que possible. Elles sont très bien faites. ■

Swiss Research Teams Index

par Martin Berli – Switch, E-mail: berli@chx400.switch.ch

Récemment, SWITCH a mis un nouveau service à disposition de la communauté du Cyberspace, le **Swiss Research Teams Index**:

http://www.switch.ch/edu/research_index.html

Cet index est une base d'information sur des équipes de recherche suisses actives dans de nombreux domaines. L'index contient une courte description de chaque équipe ainsi qu'un ensemble de mots-clés y relatifs. Ces derniers sont rassemblés en une liste que l'on peut interroger.

Des informations détaillées sur les équipes de recherche et leurs projets se trouvent dans leurs propres pages web. L'index permet donc avant tout de localiser les équipes de recherche.

SWITCH a pris plusieurs mesures afin de garantir une certaine qualité de l'index:

- ▲ les nouvelles entrées sont contrôlées par SWITCH avant d'être ajoutées à l'index. Ainsi, il est possible d'éviter l'utilisation abusive de l'index.
- ▲ les adresses électroniques sont vérifiées par l'envoi d'un message à celles-ci.
- ▲ chaque lien (URL) sur les pages entretenues par les équipes est vérifié hebdomadairement et corrigé le cas échéant.
- ▲ les équipes de recherche enregistrées sont contactées périodiquement par courrier électronique pour contrôler leurs données et signaler les corrections le cas échéant.

Néanmoins, la mise à jour continue de l'index ne représente qu'un des critères d'utilité d'un tel index. Encore faut-il qu'il soit complet. Dans cette optique, SWITCH s'efforce de faire connaître l'existence de cet index au plus grand nombre possible d'équipes de recherche à travers la Suisse. Ce court article fait partie de la campagne d'information entreprise par SWITCH.

Si vous-mêmes faites partie d'une équipe de recherche mettant à disposition de l'information via des pages web, ou avez connaissance d'une telle équipe, n'hésitez pas à prendre contact pour la faire enregistrer dans l'index.

SWITCH vous remercie d'avance de votre collaboration, au nom de tous les futurs utilisateurs (parmi ces derniers un nombre croissant d'utilisateurs étrangers s'intéresse à la recherche en Suisse). ■

SWITCH

SWITCH est le prestataire de services et d'accès à Internet pour le monde académique suisse. Sous la forme d'une fondation dont les membres sont les Hautes Ecoles (EPF et Universités), depuis 1990 SWITCH nous apporte bon nombre de services.

SWITCHlan est le premier réseau académique suisse qui relie entre elles les Hautes Ecoles et les Ecoles d'ingénieur. Cette année une connexion directe avec les USA a été mise en service (2 lignes à 1,5 Mbits/s), en plus de l'accès à Europanet (le réseau académique européen). Le réseau ATM de l'OFI (KOMBV) est actuellement utilisé pour permettre, à terme, de supprimer des lignes louées coûteuses.

D'autres services comme la distribution des News, le serveur de noms (DNS) sont parfois oubliés ou considérés comme tout à fait naturels. Le serveur FTP ([ftp.switch.ch](ftp://ftp.switch.ch)) offre un service dit miroir qui est une copie des fichiers d'autres sites. Des logiciels shareware et freeware sont à disposition et ainsi évitent de surcharger inutilement les lignes internationales.

SWITCH 111 est l'annuaire électronique des PTT. Actuellement, un CD-ROM permet un accès très rapide aux données, avec cependant l'inconvénient de n'être à jour qu'au changement de CD.

Les accès aux bibliothèques, le transport d'ETHICS entre l'ETHZ et l'EPFL, la coordination avec les entités académiques d'Europe sont encore de nombreux services offerts pour la bonne marche de services de télécommunications.

SWITCH possède aussi sa vitrine sur le Web (www.switch.ch) où l'ensemble de ses services est décrit. La coordination des services reste un élément prépondérant pour les Ecoles avec la garantie d'une compétence de haut niveau.

Jacques Virchaux SIC-STI

L'atelier Repro présente...

Le copieur couleur

Xerox Magic (Fiery-Regal) 5790

par Roland Chaboz, Atelier de Reprographie EPFL

L'atelier Repro de l'Avenue de Provence vient de s'équiper d'un copieur couleur *haut de gamme*; comme d'habitude, les intéressés peuvent faire des copies (analogiques) à partir d'originaux papier, mais aussi, innovation, des copies à partir de leur fichier informatique. Ce copieur est un *Xerox-Magic 5790* piloté par un interpréteur/RIP *Fiery Regal 5790*.



CE QUE VOUS POUVEZ RÉALISER

Des affiches, des couvertures, des publications, des transparents pour présentation, voilà entre autres ce que vous pouvez sortir de ce copieur.

CE QUE VOUS POUVEZ OBTENIR

Vous pouvez obtenir vos travaux sur papier normal ou cartonné jusqu'à 160 gr au maximum en A3 ou A4 ainsi que sur transparent en A4 seulement.

D'après le constructeur Xerox, il est possible de faire du recto-verso, mais la Repro le déconseille après avoir effectué des tests peu concluants (bourrage papier dans le copieur). Les utilisateurs exigeant tout de même du recto-verso sont priés de nous téléphoner avant la création du fichier PostScript pour la compatibilité de la machine et de ses magasins.

CE QUE VOUS DEVEZ FOURNIR

En principe, seuls les fichiers PostScript seront acceptés par la Repro. Néanmoins, moyennant une participation de frs. 50.-/heure, la Repro pourra éventuellement accepter des fichiers source Illustrator, Photoshop, PageMaker et X-Press (sur Macintosh uniquement) pour quelques retouches, ou adaptations de résolution.

SCANNAGE DES ILLUSTRATIONS

La résolution du copieur est de 400 dpi; par conséquent, la numérisation optimale de vos illustrations devra se faire à 150 dpi maximum dans le cas d'une impression à 100 %.

COMMENT FABRIQUER VOS FICHIERS

FICHIERS POSTSCRIPT MULTI-PLATEFORMES

Vous pouvez vous référer au mode d'emploi pour la génération de fichiers PostScript depuis un Macintosh, paru en page 8 du FI3/96 du 26 mars 96 :

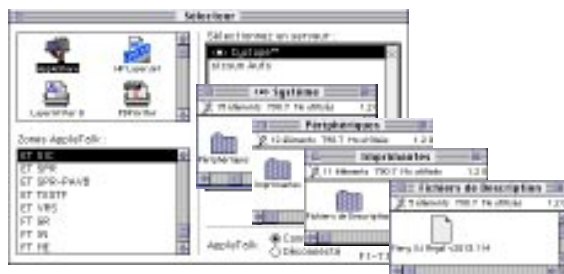
<http://sawwww.epfl.ch/SIC/SA/publications/FI96/fi-3-96/3-96-page8.html>

et depuis un PC, paru en page 19 du FI6/96 du 2 juillet 96:

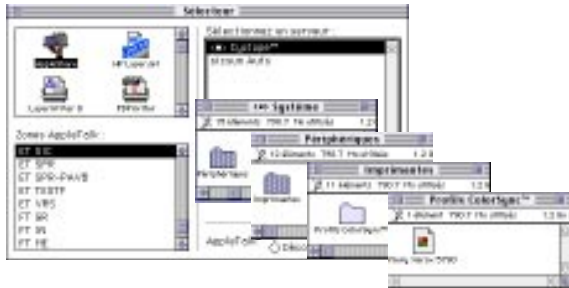
<http://sawwww.epfl.ch/SIC/SA/publications/FI96/fi-6-96/6-96-page19.html>

Les fichiers Post-Script MAC seront générés avec le driver *Fiery XJ Régal v2013.114* disponible sur serveur Mac:

<•>Cyclope/<•>Système/Périphériques/
Imprimantes/Fichiers de Description/Fiery XJ
Regal v2013.114



Pour les *fondus*, un profil ColorSync **Fiery Xerox 5790** est aussi disponible sur le serveur Mac:
**<•>Cyclope/<•>Système/Périphériques/
 Imprimantes/Profils ColorSync™/Fiery Xerox
 5790**



Les fichiers PostScript PC seront générés avec le driver **Fiery XJ Régal v2013.114** qui est disponible sur le serveur Olympe:

**\\OLYMPE\olympesys_w95\english\
 Drivers2\Printers\Xerox\FieryReg**

Pour les fichiers PostScript Unix, veuillez nous téléphoner au préalable.

TIRAGE

Important: lors de la création du fichier PostScript, sous la rubrique nombre de copies: **indiquer 1 copie**. Ne mentionner le nombre de copies désiré que sur la réquisition.

DRIVER: SÉLECTION DES MAGASINS

Lors de la génération du fichier PostScript soyez attentifs au choix du magasin:

- Tray 1** = A3 papier 90 gr.
- Tray 2** = A4 standard papier 90 gr./recto seul, c'est en général ce magasin que vous choisirez.
- Tray 3** = A4 oblong, ne pas l'utiliser, car en général, les logiciels gèrent l'oblong sur l'A4 standard.
- Manuel** = A3 cartonné, A4 cartonné (160 gr. au maximum) et transparents.

Important:

nous vous rappelons qu'en cas de nécessité d'une impression recto/verso, il faut prendre contact préalablement avec nous pour le choix des magasins.

PRIX

Le prix des copies, qu'elles soient faites à partir d'un original papier ou d'un fichier PostScript est de

- frs. 1.00 — la copie A4
- frs. 1.50 — la copie A3
- frs. 2.00 — la copie A4 sur transparent

auquel s'ajoutera, dans le cas des copies faites à partir d'un fichier PostScript, les frais de prise en

charge du fichier calculés ainsi:
 frs. 10.00 par fichier dont on tirera de 1 à 10 copies
 frs. 7.00 par fichier dont on tirera de 11 à 20 copies
 frs. 5.00 par fichier dont on tirera de 21 à 29 copies
 frs. 0.00 par fichier dont on tirera 30 copies ou plus

Pour toute création ou intervention sur un fichier source (Mac) une participation de fr. 50.-/heure sera demandée (ne pas oublier de joindre les polices non-standard et les images/scans avec le fichier source).

TRANSPORTS DES FICHIERS

La Repro est encore en pleine mutation (réseau, serveur, etc.); c'est la raison pour laquelle il n'est pas possible de transférer aujourd'hui vos fichiers par le réseau.

La Repro est équipée de Macintosh seulement, en attendant le réseau, faites-nous parvenir vos fichiers PostScript sur disquette ou SyQuest 5" 1/4 (lire aussi les FI 3 et 6/96) .

REQUISITION

Avec les travaux couleur, vous joindrez comme d'habitude une réquisition OCFIM, avec le numéro de compte **et** le Centre de Frais.

Exercice comptable	
Druckprogramm-/Budget-Position	
Position: Progr. d'impression/budget	
Projekt-Nr.	Kredit-Code
N° de projet	Code de crédit
Fremdkredit/Rückvergütung	(Ankreuzen) <input type="checkbox"/>
Réimputation	(Croix) <input type="checkbox"/>
Konto	
Compte	
Text Texte	

EN CONCLUSION

Le temps de se *faire la main* et d'acquérir plus d'expérience sur le système, nous permettra de vous donner des renseignements supplémentaires par l'intermédiaire de ce même journal.

DES PROBLEMES?

En cas de problème, vous pouvez toujours atteindre

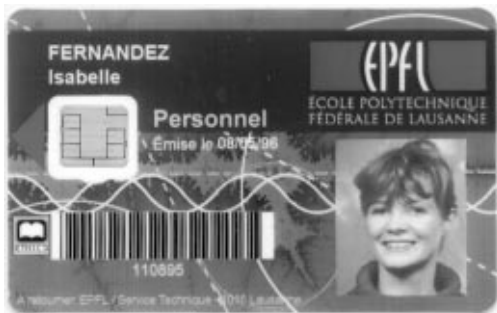
Roland Chabloz
 Atelier de Reprographie EPFL
 ☎ 625 74 72. ■

Le Coin des Curieux

par Isabelle Fernandez - Arob@sqe

X-Files

L'AVENTURE CONTINUE



1ÈRE PARTIE

Service Informatique Central de
l'EPFL - Lausanne
le 1er février 1996 - 18h45

Un nouvel envahisseur s'empare des sites Macintosh et Windows de l'EPFL. Les agents très spéciaux d'Arob@sqe sont appelés afin de tester, analyser et trouver un plan d'action pour informer la population de ce nouveau programme, nom de Code: FileMaker Pro 3.0.

Arob@sqe, salle d'autopsie -
Lausanne
le 2 février 1996 - 0h15

«Lausanne, le 2 février 1996. Il est exactement 0h15. Nous allons pratiquer l'autopsie de ce nouveau FileMaker Pro 3.0. Afin d'éviter tous risques d'épidémie, nous avons préalablement fait une copie de sauvegarde des fichiers FileMaker Pro 2.1.

Le sujet se présente sous forme de trois disquettes et ne semble âgé que de quelques mois. L'installation du programme se déroule bien. Aucun virus, ni erreur système n'est à relever. La taille HD est de 2.2 MB pour le programme et de 8 MB pour l'installation complète. La taille RAM souhaitée est de 5 MB. Ah, la mutation de la créature est déjà apparente au niveau de son icône:



FileMaker Pro

Nous démarrons maintenant le programme... Une nouvelle fenêtre est apparue permettant la création d'un nouveau fichier basé sur un modèle vierge ou encore l'ouverture d'un fichier existant. Nous portons notre choix sur l'ouverture d'un fichier et choisissons d'un clic ferme et assuré notre ancien fichier d'adresses.

Une fenêtre de sécurité demande de renommer la nouvelle version du fichier afin de générer automatiquement la copie de secours.

Le fichier est maintenant ouvert. Tout semble normal, toutefois nous constatons déjà des modifications au niveau des menus. Un nouveau menu **Mode** fait son apparition, tandis que les menus **Sélection**, **Modèle** et **Objet** ont disparu dans l'espace-temps.

Notre autopsie commence par le menu **Mode**: nous y trouvons les différents niveaux tels que **Utilisation**, **Recherche**, **Modèle** et **Prévisualisation**. En poursuivant notre dissection, nous découvrons les articles indispensables concernant la gestion des fiches. Ils ont donc passé du menu **Edition** au menu **Mode**.

Afin de faire une analyse complète, nous restons dans le niveau **Utilisation**. L'aspect général de l'écran est normal, aucun changement physique n'est intervenu dans ce niveau. Rappelons juste que les articles de création de fiches, duplication

ou suppression se trouvent dans le menu **Mode**. Nous tentons maintenant une modification de la fiche en cours. Tout se passe normalement. Tant que la fiche n'est pas validée (avec la touche **ENTER** ou **ENTREE** ou en cliquant à l'extérieur des rubriques), nous pouvons annuler toutes les corrections grâce à l'article **Rétablir la fiche** du menu **Mode**.

En poussant plus loin notre inspection des rubriques de type Texte, il s'avère que nous pouvons y insérer des marques de tabulations au moyen des touches **OPTION-TABULATEUR** (Macintosh) et **CTRL-TABULATEUR** (Windows). Une règle de texte est disponible dans le menu **Format** et permet ainsi de placer des taquets de tabulation, ou de réaliser des retraits ou indentations (voir figure 1).

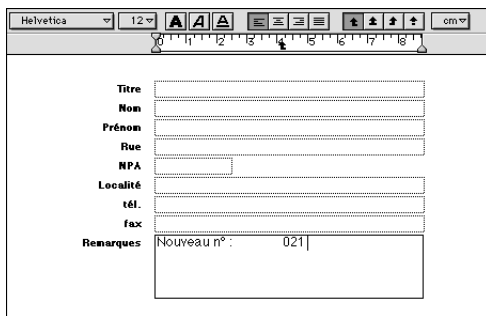


Figure 1

Nous tentons maintenant une recherche au moyen de l'article **Recherche** du menu **Mode**. Aucune particularité n'est à relever. Tout semble stable et conforme à l'ancienne version. La liste des symboles est identique. Toutefois, nous constatons que la gestion des recherches se pratique maintenant sous le menu **Mode**, tout comme la gestion des fiches.

Les articles de sélection suite à une recherche, **Tout rechercher**, **Rechercher les fiches ignorées**,... se trouvent dans le menu **Sélection**. Aucun point supplémentaire ne se dégage de ce premier examen. Nous activons donc à l'instant le mode **Modèle**. Notre attention se porte immédiatement sur la zone des outils. Deux boutons ont été ajoutés à la liste précédente. Nous cliquons donc le premier et dessinons dans le corps de la fiche un rectangle qui s'apparente à un bouton. Une fenêtre s'ouvre et permet de choisir le rôle de l'objet (voir figure 2).

Nous pouvons dès lors certifier que ce nouvel outil permet la création rapide et aisée de boutons. Il suffit de choisir l'action désirée et valider OK.

Le deuxième bouton inconnu permet de réaliser des **tables externes**. Ce phénomène certainement lié à la notion relationnelle attire notre attention. Nous allons donc pousser plus loin notre recherche.»

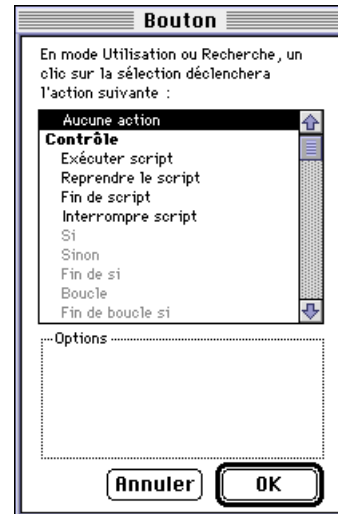


Figure 2

Arob@sqe - Lausanne
le 2 février 1996 - 23h11

C'est alors que le 4ème agent d'Arob@sqe, retenu jusqu'alors par une affaire non classée de réseaux, entre dans la salle d'autopsie et interrompt les investigations. Avec un enthousiasme non dissimulé, ses trois autres collègues lui relatent alors leurs fabuleuses découvertes.

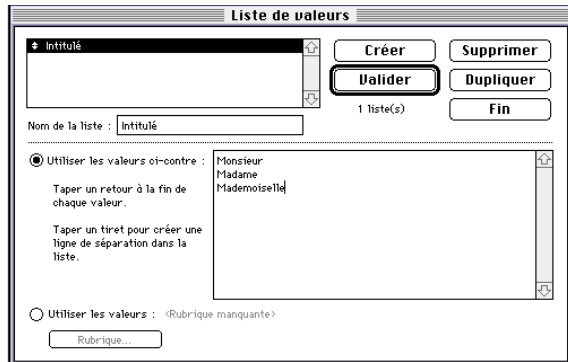
Arob@sqe - Lausanne
le 3 février 1996 - 1h15

«Après une courte interruption, nous reprenons l'autopsie de FileMaker Pro 3.0. Nous sommes maintenant le 3 février; il est 1h15. Le sujet se trouve toujours en mode **Modèle**. Nous laissons provisoirement la notion de tables externes car elles demandent une recherche plus poussée dans les fenêtres de **Définir des liens...** et **Définir les rubriques...**

De nombreux articles sont disposés différemment dans les menus adaptés au mode **Modèle**. L'article **Ordre des modèles...** sous le menu **Modèle** attire notre attention: il permet de redéfinir l'ordre d'apparition et également d'estomper certains modèles dans le menu de la barre d'état. L'article **Format de modèle...** quant à lui nous permet de constater que des marges peuvent être choisies pour chaque modèle.

Format de rubrique... du menu **Modèle** retient notre attention. Après avoir sélectionné la rubrique **Intitulé** dans le modèle, nous activons cet article. Un cercle d'option **Liste** est offert. Nous l'activons et ouvrons le menu local ci-après. Nous activons l'article **Liste de valeurs** et découvrons une nouvelle fenêtre. Elle permet la saisie du nom de la liste. Après avoir exécuté cette opération nous confirmons la création, puis saisissons les valeurs désirées

(Monsieur, Madame, Mademoiselle) et validons la fenêtre. Pour s'assurer que notre sentiment est bien fondé, nous glissons dans le mode Utilisation: Oh ... un clic sur la rubrique Intitulé et nous découvrons notre liste de valeurs. Nous pouvons donc affirmer qu'il n'est plus obligatoire de créer les listes de valeurs depuis la fenêtre **Définir les rubriques...** Quel gain de temps extraordinaire !



Afin que notre première analyse soit complète, nous avons **Définir les rubriques...** disposé dans le menu **Fichier**. La mutation continue aussi dans cet environnement: un format de rubrique

Global est apparu; avec prudence, nous créons une rubrique appelée logo à laquelle nous attribuons ce format. Dès la validation, nous devons choisir le type (texte, nombre, date, ...). Nous optons pour le format multimédia et validons notre choix. Dès notre retour en Utilisation, nous collons une image dans cette nouvelle rubrique... Elle est dès lors apparue dans toutes les fiches présentes dans notre fichier. Ce nouveau format global permet donc d'utiliser la même information pour toutes les fiches.»

C'est alors que le natel sonne et interrompt l'autopsie en cours.

Liaison téléphonique entre le Service Informatique Central de l'EPFL et Arob@sque - Lausanne le 3 février 1996 - 08h03

Un plan d'action est mis en œuvre. Des cours d'introduction, avancés et de transition sont immédiatement organisés et publiés dans le Flash Informatique.

(à suivre...) ■

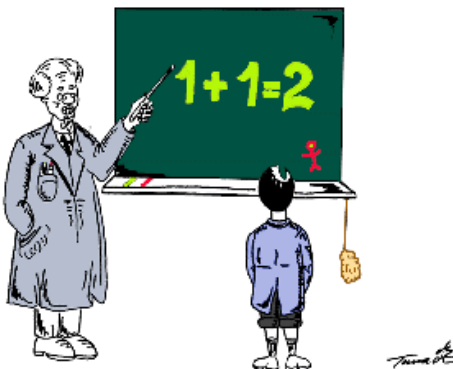
Les cours de formation

Les cours ci-dessous sont ouverts à tous, membres ou non de l'EPFL. Pour le personnel de l'EPFL, le SIC se charge des frais de cours.

Inscriptions et renseignements (matin uniquement):
Josiane Scalfo, SIC-EPFL, CP 121, 1015 Lausanne
☎ 693.2244 – Fax: 021 693 22 20
QuickMail ou E-mail: scalfo@sic.adm.epfl.ch

Pour tout changement, consultez aussi les News, ou le serveur WWW : <http://sawwww.epfl.ch/SIC/SA/cours/cours.html>

COURS SUR MACINTOSH



Cycle de base complet A + B (12 demi-jours)

N° 1771 A 08, 10, 15, 17, 22 & 24.10.96 13h30 - 17h15
Introduction au Macintosh, à ClarisDraw 1.0, Word 6.0, Excel 5.0, FileMaker Pro 3.0.

N° 1771 B 05, 07, 12, 14, 19 & 21.11.96 13h30 - 17h15
Introduction à l'utilisation des réseaux, Internet, Messagerie & Astuces pratiques du système.

N° 1772 A 12, 14, 19, 21, 26 & 28.11.96 08h15 - 12h00
Introduction au Macintosh, à ClarisDraw 1.0, Word 6.0, Excel 5.0, FileMaker Pro 3.0.

N° 1772 B 02, 04, 06, 09, 11 & 13.12.96 08h15 - 12h00
Introduction à l'utilisation des réseaux, Internet, Messagerie & Astuces pratiques du système.

BASE DE DONNÉES

FileMaker Pro transition 2.1 à 3.0 (2 demi-jours)
N° 1783 29 & 31.10.96 13h30 - 17h15

FileMaker Pro 3.0 avancé (5 demi-jours)
N° 1778 21, 23, 28, 30.10 & 04.11.96 08h15 - 12h00

METTEUR EN PAGE

PageMaker 6.0 (3 demi-jours)
 N° 1774 04, 06 & 11.11.96 13h30 - 17h15
 Prérequis: connaissances approfondies de Word et d'un logiciel de dessin!

PRÉSENTATION

PowerPoint 4.0 avancé, niv. 1 (2 demi-jours)
 N° 1769 14 & 16.10.96 13h30 - 17h15
 Prérequis: connaissances de base d'un logiciel de dessin et d'un traitement de texte !

PowerPoint 4.0 avancé, niv. 2 (2 demi-jours)
 N° 1757 30.09 & 03.10.96 08h15 - 12h00
 N° 1770 09 & 11.12.96 13h30 - 17h15
 Prérequis: connaissances de PowerPoint !

TABLEUR

Excel 5.0 avancé, niv. 1 (3 demi-jours)
 N° 1766 31.10, 05 & 07.11.96 08h15 - 12h00

Excel 5.0 avancé, niv. 2 (2 demi-jours)
 N° 1767 25 & 28.11.96 13h30 - 17h15

Excel 5.0 macros (2 demi-jours)
 N° 1768 03 & 05.12.96 08h15 - 12h00

TRAITEMENT D'IMAGES

MacroMind Director (3 demi-jours)
 N° 1790 08, 15 & 22.11.96 08h15 - 12h00

PhotoShop (3 demi-jours)
 N° 1788 15, 17 & 22.10.96 08h15 - 12h00

Premiere (2 demi-jours)
 N° 1789 25 & 29.10.96 08h15 - 12h00

TRAITEMENT DE TEXTE

Introduction à ClarisWorks 4.0 (4 demi-jours)
 N° 1779 07, 09, 14 & 16.10.96 08h15 - 12h00
 Introduction au Macintosh et à ClarisWorks 4.0.

FrameMaker 5.1 introduction (3 demi-jours)
 N° 1784 20, 27.11 & 04.12.96 13h30 - 17h15

Mailing (Word - FileMaker) (1 demi-jour)
 N° 1777 06.11.96 08h15 - 12h00
 Prérequis: connaissances de base de Word et FileMaker Pro!

Word 6.0 avancé (5 demi-jours)
 N° 1773 11, 13, 18, 20 & 25.11.96 08h15 - 12h00

Word 6.0 gestion de longs documents (2 demi-jours)
 N° 1775 21 & 23.10.96 13h30 - 17h15
 Les longs documents, tels que Thèses, rapports, livres, ... demandent une certaine rigueur tant dans la conception du document que dans sa mise en page. Cette rigueur permet de rendre le document homogène et offre des fonctions automatiques par exemple pour les tables des matières et index, ...

Ce cours de deux demi-journées est destiné à toute personne qui doit, est en train ou mieux encore planifié de réaliser d'importants documents avec Word 6.0.

Contenu du cours :

- Les marges (paires et impaires) • Les en-tête et pied de page (pairs, impairs, première page, ...)
 - Les numérotation des pages • Les notes de bas de page • Les signets et renvois • Les sections • Les légendes • Les styles et N° des titres • Le mode plan • Les documents maîtres (liaisons de plusieurs documents Word) • L'index • Les tables d'illustrations, matières, ...
- Prérequis: connaissances de base de Word 6.0.

Word 6.0 formulaires (1 demi-jour)
 N° 1776 28.10.96 13h30 - 17h15

Word permet de réaliser des formulaires - modèle tels que lettres types, en-tête de fax, ... - avec saisie à l'écran des informations variables. Cela vous évite de devoir sans arrêt placer votre curseur d'insertion au bon niveau, rechercher la zone de l'adresse ou du début de la lettre avant la frappe.

Cette fonction vous permet également de réaliser facilement et rapidement des questionnaires avec cases à cocher - de type bulletin d'inscription, questionnaires, ... - dans le but d'obtenir un résultat papier. Il ne vous offre cependant pas la possibilité de traiter les données variables d'un questionnaire afin d'en tirer des statistiques directement dans Word, mais offre un «export» en vue d'un traitement dans FileMaker Pro par exemple.

Contenu du cours :

- la création de champs de type : texte, nombre, date et heure • La création de champs avec cases à cocher et liste de valeur • Le réglage des options de champs • La création de texte d'Aide • L'insertion de caractères spéciaux (ciseaux, téléphone, ...)
- La protection des sections • L'enregistrement sous forme de modèle • L'utilisation des formulaires • L'enregistrement des données variables en vue d'un traitement

Prérequis: notions de base et la gestion des tableaux de Word 6.0

Word 6.0 trucs + astuces (1 demi-jour)
 N° 1787 01.11.96 08h15 - 12h00

WEB

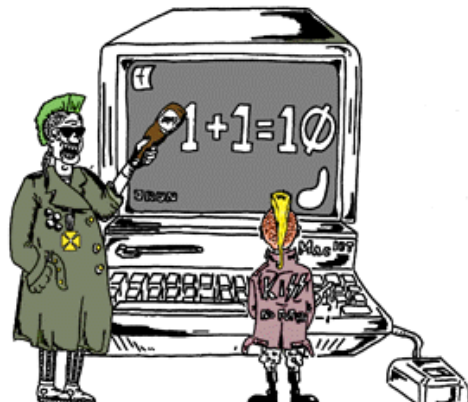
HTML (2 demi-jours)

Ce cours est destiné aux secrétaires qui devront mettre de l'information sur les serveurs **W** de l'Ecole.

- les principes de base de **W** (modèle client-serveur, Internet, hypertexte, URL)
- les commandes HTML les plus importantes
- les différentes méthodes pour créer/récupérer des textes pour un serveur **W**

N° 1785 08 & 10.10.96 08h15 - 12h00
 N° 1786 27 & 29.11.96 08h15 - 12h00

Prérequis: avoir déjà utilisé un logiciel **W** (Mosaic ou Netscape)



COURS SUR PC - WINDOWS'95

Cycle de base complet A + B (12 demi-jours)

N° 2568 A 14, 16, 21, 23, 28 & 30.10.96 13h30 - 17h15
Introduction à Windows 95, PowerPoint 7.0, Word 7.0, Excel 7.0, FileMaker Pro 3.0.

N° 2568 B 04, 06, 11, 13, 18 & 20.11.96 13h30 - 17h15
Introduction à l'utilisation des réseaux, Internet, Messagerie & Astuces pratiques de Windows 95

BASES DE DONNÉES

Access 7.0 introduction (2 demi-jours)
N° 2565 22 & 24.10.96 08h15 - 12h00

Access 7.0 avancé (4 demi-jours)
N° 2566 18, 22, 25 & 29.11.96 08h15 - 12h00

Access 7.0 / VisualBasic 4.0 (2 demi-jours)
N° 2567 19 & 21.11.96 08h15 - 12h00

DESSIN

Designer 6.0 (2 demi-jours)
N° 2575 05 & 07.11.96 13h30 - 17h15

LANGAGE DE PROGRAMMATION

VisualBasic 4.0 introduction (2 demi-jours)
N° 2558 29 & 31.10.96 13h30 - 17h15

VisualBasic 4.0 avancé (4 demi-jours)
N° 2559 19, 21, 26 & 28.11.96 13h30 - 17h15

PRÉSENTATION

PowerPoint 7.0 avancé, niv. 1 (2 demi-jours)
N° 2564 04 & 07.11.96 08h15 - 12h00
Prérequis: connaissances de base d'un logiciel de dessin et d'un traitement de texte !

TABLEUR

Excel 7.0 avancé, niv. 1 (3 demi-jours)
N° 2560 14, 16 & 18.10.96 08h15 - 12h00

Excel 7.0 avancé, niv. 2 (2 demi-jours)
N° 2561 29 & 31.10.96 08h15 - 12h00

Excel 7.0 macros (2 demi-jours)
N° 2563 22 & 24.10.96 13h30 - 17h15

TRAITEMENT DE TEXTE

Word 7.0 avancé (5 demi-jours)
N° 2571 17, 21, 23, 28 & 30.10.96 08h15 - 12h00

Word 7.0 gestion de longs documents (2 demi-jours)
idem que le cours Word 6.0 gestion de longs documents sur Macintosh.
N° 2572 11 & 13.11.96 08h15 - 12h00

Word 7.0 formulaires (1 demi-jour)
idem que le cours Word 6.0 formulaires sur Macintosh.
N° 2573 20.11.96 08h15 - 12h00

Word 7.0 mailing (1 demi-jour)
N° 2574 25.11.96 13h30 - 17h15
Prérequis: connaissances de base de Word.

Word 7.0 trucs + astuces (1 demi-jour)
N° 2578 05.11.96 08h15 - 12h00
Prérequis: connaissances de base de Word.

WEB

HTML (2 demi-jours)
idem que le cours HTML sur Macintosh
N° 2576 06 & 08.11.96 08h15 - 12h00

COURS SUR PC - WINDOWS NT

Windows NT Workstation V4.0 (4 jours)
No 6001 22 au 25.10.96 08h15-17h15

Le but de ce cours est de familiariser les participants avec la gestion, l'installation et la configuration des stations de travail Windows NT, Workstation.

Prérequis

Expérience de l'installation et configuration de Windows 3.1 dans un environnement réseau. Connaître la gestion des périphériques d'entrée-sortie.

Contenu

- Environnement • Installation et configuration de Windows NT Workstation • Gestion des comptes • Système de fichiers
- Protection des ressources locales • Sécurité du système
- Environnement réseau • Service d'accès distant • Gestion des impressions • Optimisation des performances • Diagnostique et dépannage

Windows NT Server V4.0 (4 jours et demi)
No 6002 4 au 7.11.96 08h15-17h15
et 8.11.96 08h15-12h00

Le but de ce cours est de permettre aux participants de se familiariser avec l'installation, la configuration et la gestion de Windows NT Server dans un environnement réseau.

Prérequis

Avoir suivi le cours Windows NT Workstation ou posséder les connaissances équivalentes.

Contenu

- Installation et configuration de Windows NT Server • Gestion des domaines • Mécanisme de réplication • Protection des données • Relation d'approbation • Gestion et utilisation des groupes • Interopérabilité DOS/Windows • Implémentation de TCP/IP • Le service Browser • Optimisation des performances
- Services pour Macintosh

Microsoft System Management Server (4 jours et demi)

No 6003 16 au 19.12.96 08h15-17h15
 et 20.12.96 08h15-12h00

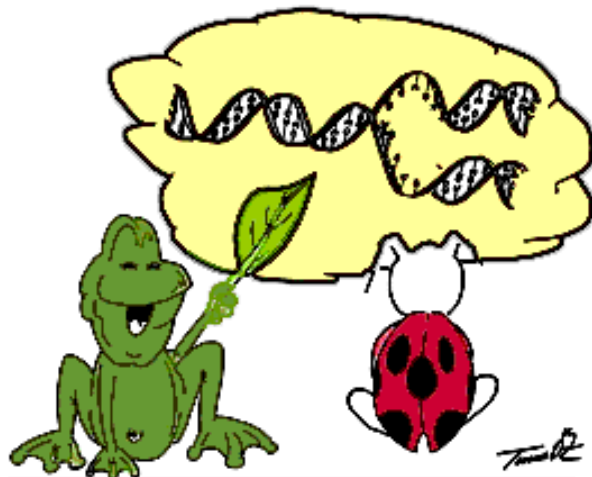
Le but de ce cours est de permettre aux participants de se familiariser avec l'installation, la configuration et l'administration de SMS.

Prérequis

Avoir suivi le cours Windows NT Server ou posséder les connaissances équivalentes.

Contenu

- Fonctionnalités et environnement de SMS
- Gestion de site SM
- Administration de l'inventaire
- Interrogation de la base SQL
- Distribution de logiciels sur les stations de travail
- Gestion des applications partagées
- Support et surveillance à distance



COURS SUR STATIONS DE TRAVAIL

Unix introduction (1 demi-jour)
 N° 3136 18.11.96 13h30 - 17h30

Unix et les 1ers éléments d'administration (5 jours)
 N° 3128 28.10 au 01.11.96 09h00 - 17h30

A l'issue de ce cours, le stagiaire pourra maîtriser le système UNIX (SunOs 4.x, Solaris 2.x, ...) pour une utilisation avancée.

Ce cours est destiné aux développeurs et administrateurs. Une bonne connaissance d'un système d'exploitation ainsi qu'une habitude des éditeurs sont indispensables. La connaissance de quelques commandes UNIX serait un plus. Les sujets suivants seront développés:

- Les principales caractéristiques UNIX (utilisateur, tâche, fichier).
- Etude rapide des commandes de base.
- L'arborescence UNIX (organisation, protections).
- Etude de vi.
- Les expressions régulières et les commandes concernées.
- Les outils sed et awk.
- Gestion mémoire (swapping, pagination). Les processus UNIX.
- Administration premier niveau. Le réseau local.
- Modèle client serveur.
- Terminologies et concepts NFS.
- Connexion et soumission de commandes à distance.
- Les outils de développement de programmes.
- Gestions des compilations et des sources: make et sccs.
- Aspects interactifs du C-shell. Etude avancée du C-shell.

Configuration réseau des machines Unix (1 jour)
 N° 3129 19.11.96 09h00 - 17h30

Ce cours d'une journée est destiné aux «managers» de stations de travail sur le site.

Les caractéristiques principales du réseau sont passées en revue. Les principes de TCP/IP sont abordés afin d'expliquer comment nous configurons les machines sur le site. Les protocoles les plus utilisés sur IP sont brièvement étudiés.

Nous parlons un peu du passé (Ethernet avant le recablage). Beaucoup du présent (Ethernet et FDDI aujourd'hui). Et aussi un peu de l'avenir (Fast-Ethernet FDDI ATM).

Les outils disponibles sur le site pour :

- configurer une machine,
 - diagnostiquer un problème,
 - dialoguer avec la section téléinformatique,
- sont mis en application.

Langage C (5 jours)

N° 3125 30.09 au 04.10.96 09h00 - 17h30

Ce cours est complet. Vous pouvez vous inscrire auprès de Josiane Scalfò afin d'être en liste d'attente pour ce cours et/ou avoir priorité sur le prochain.

Programmation C++ (5 jours)

N° 3126 14 au 18.10.96 09h00 - 17h30

Ce cours est complet. Vous pouvez vous inscrire auprès de Josiane Scalfò afin d'être en liste d'attente pour ce cours et/ou avoir priorité sur le prochain.

Pour toute information concernant les cours Unix: Franck Perrot, ☎ 693.2255, ✉ perrot@sic.epfl.ch

TCL / TK (4 demi-jours + 1 jour)

N° 3127 04 au 07.11.96 13h30 - 17h30
 & 08.11.96 09h00 - 17h30

Description

Tcl/Tk (développé par J. Ousterhout) permet d'écrire rapidement des applications avec interface graphique (GUI) pour l'environnement Xwindows.

Tcl est un langage de script, interprété. Tk est la boîte à outils pour la partie graphique X. Les applications écrites en Tcl/Tk ont l'aspect Motif tout en étant créées très rapidement grâce à l'interface de haut niveau et à la nature interprétée du langage.

Connaissances préalables exigées

Aucune en particulier, mais une connaissance de Unix, d'un langage de scripts comme sh, csh... et une vision globale de Xwindows seront des atouts précieux.

Objectifs et contenu

A l'issue du cours, les participants seront capables d'écrire la plupart des applications en Tcl/Tk sans se référer trop souvent à la documentation et de construire des interfaces graphiques agréables à utiliser.

Pour plus de renseignements, voir le serveur http://slwww.epfl.ch/SIC/SL/logiciels/TclTk/TclTk_announce.html.

CONDITIONS D'INSCRIPTION

En cas d'empêchement à suivre le(s) cours, l'élève avertira le Service informatique central au minimum une semaine à l'avance (sauf cas exceptionnel), faute de quoi le SIC se réserve le droit de facturer à son unité les frais occasionnés pour le cours.

Une confirmation parviendra à l'élève environ deux semaines avant le cours. S'il est déjà complet, l'élève sera informé de suite et son nom placé en liste d'attente. Dès qu'un cours identique sera fixé, il recevra un nouveau formulaire d'inscription.

Le SIC se réserve le droit d'annuler un cours si le nombre minimum de 4 participants n'est pas atteint ou pour des raisons indépendantes de sa volonté. Aucune compensation ne sera due par le SIC.

Calendrier des manifestations

OCTOBRE 1996

- Mardi 1er 14h15 Salle Conférences SIC **CTI** — Commission Technique Informatique
M. Reymond, ☎ 693.2210, ✉ reymond@sic.adm.epfl.ch
- Mardi 8 14h00 Salle C03 - EPFL-Ecublens **CAPA** — L'informatique parallèle (lire en page 12)
CAST-EPFL, ☎ 693.3575, fax: 693 47 47
- Judi 17 14h15 Salle Conférences SIC **PolyPC** — Groupe des utilisateurs d'IBM PC et compatibles
Ch. Zufferey, ☎ 693.4598, ✉ zufferey@sic.adm.epfl.ch
Info sur **WWW**: <http://pcline.epfl.ch/pc/grp/home.htm>
- Vendredi 18 10h00 Salle Conférences SIC **SUNLine** — Groupe des utilisateurs de stations SUN
Ordre du jour: • Solaris 2.5.X • autres nouveautés
concernant l'administration • présentation par SUN de
nouvelles annonces.
Krassimir Todorov, ☎ 693.2241, ✉ todorov@sic.epfl.ch

NOVEMBRE 1996

- Mardi 5 14h15 Salle Conférences SIC **CTI** — Commission Technique Informatique
M. Reymond, ☎ 693.2210, ✉ reymond@sic.adm.epfl.ch
- Mardi 12 08h30 Salle polyvalente du SIC **Comité de rédaction du FI**

INSCRIPTION POUR LES COURS ORGANISÉS PAR LE SIC

Remplir une inscription par type de cours (Mac, PC, Unix, ...) et retourner à Josiane Scalfo, SIC-EPFL, 1015 Lausanne

Je, soussigné(e) Nom: Prénom:

☎: E-Mail: Fonction:

Institut: Dépt: Adresse:

m'engage à suivre le(s) cours dans son (leur) intégralité et à respecter l'horaire selon les conditions d'inscription:

N° du cours	Nom du cours	N° cours de remplacement	Date du cours
.....

Date: Signature:

Autorisation du chef hiérarchique (nom lisible et signature):

INTÉRÊT ET SOUHAIT POUR D'AUTRES COURS

Description ou titre des cours que je souhaite voir organiser par le SIC:

.....

.....

.....