

# Programmez!

Mensuel - Décembre 2004 - N°70 • 5,95 €

## SÉCURITÉ Êtes-vous "Indestructibles" face aux HACKERS ?

### Cryptez sous .net

## eXtreme Programming

Créez la super équipe!

## JEUX

Des effets spéciaux à la Pixar

## Le secret de la réussite

La double compétence.



Disney/Pixar



M 04319-70-F-5,95 €

Présenté en France - Imprimé en France  
 MAGAZINE DE DÉVELOPPEMENT  
 100 Boulevard de la République - 93000 Paris

### J2EE

Comparaison de JSF et Struts

### JAVA

Maniez le composant JTree

### OPEN SOURCE

Une application

### WEB

sous J2EE avec Eclipse, Tomcat et MySQL

### WINDOWS

"Hookez" votre clavier

### APPLICATIONS

Windev 9  
WinTasks

# OpenEdge 10 s'ouvre à .NET

**Avec la version 10 d'OpenEdge, une suite complète pour concevoir, déployer et administrer des applications, Progress n'abandonne pas son univers propriétaire L4G. Il l'adapte pour l'ouvrir aux nouvelles technologies, et en particulier à la plate-forme de Microsoft, .NET, en profitant au passage des nouveaux concepts d'architectures pour optimiser les développements réalisés avec OpenEdge.**

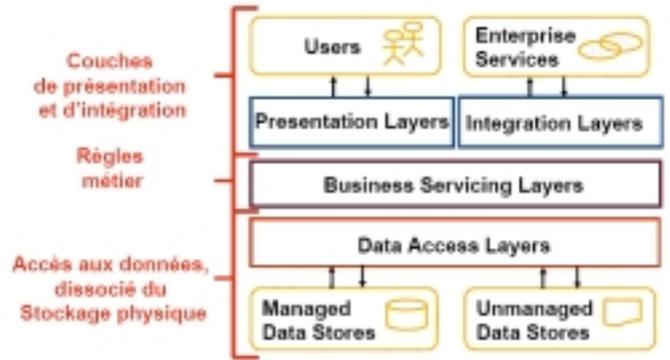
En mai dernier, Progress annonçait la commercialisation de la nouvelle version de sa suite d'outils pour le développement, le déploiement, l'administration et l'intégration d'applications. OpenEdge 10 comporte de nombreuses nouveautés, résultat d'acquisitions qui sont venues renforcer la plate-forme, mais également d'une véritable volonté de la société de s'ouvrir aux standards du marché. Au programme, intégration des Web Services, de .NET, Java, mais également adaptation au concept d'architecture SOA (Service Oriented Architecture) et même à un modèle de développement qui pourrait être du MDA (Model Driven Architecture) s'il n'était limité à la partie cliente. Le tout, sans remettre en cause le langage L4G et le cœur de la plate-forme fondée sur des technologies propriétaires.

## Une plate-forme très complète

Très fournie, la suite de Progress regroupe l'atelier de développement de type L4G OpenEdge Studio et son framework de composants Dynamics, ainsi que le stockage des données avec la base OpenEdge RDBMS déclinée en trois versions adaptées à différentes tailles d'entreprise. OpenEdge RDBMS comporte désormais un moteur SQL. En d'autres termes, les requêtes pourront désormais être indiffé-

remment écrites dans le langage L4G de Progress ou en SQL-92. La gestion des données vient également d'être renforcée par la récente acquisition (fin septembre) de Persistence, société spécialisée dans les technologies de mapping entre l'univers relationnel et le monde objet à l'aide, notamment, d'une infrastructure de cache qui optimise les performances de manière significative. Les outils de Persistence seront commercialisés par ObjectStore, filiale de Progress qui gère l'offre « gestion des données ». OpenEdge 10 comprend également un moteur d'intégration et d'orchestration des services, des outils d'administration (gamme Fathom) et même des fonctions de reporting, grâce à un accord de partenariat avec Crystal Reports et Corvu, entre autres.

## OpenEdge Reference Architecture



Similaire au concept de SOA, l'initiative OERA de Progress propose de développer et de moderniser les applications existantes en fonction du principe de la séparation des couches métier, traitements, données, interface afin de favoriser la réutilisation et la pérennité des développements.

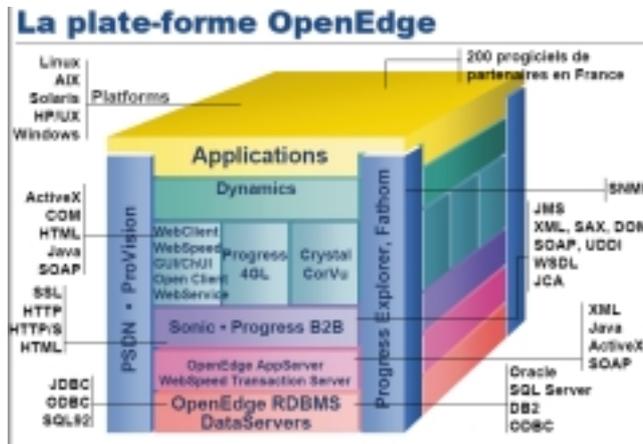
Enfin, Progress dispose de son propre serveur d'application, décliné en deux versions, pour gérer les technologies propriétaires de la société (L4G) mais également java et .NET.

## Montée en puissance sur l'intégration à .NET

Grâce à cette ouverture aux technologies tierces, OpenEdge peut gérer des clients propriétaires, mais également légers, de type HTML (WebSpeed), des smart clients ou client riches pour

Windows 32bits (WebClient). Ou encore n'importe quel type de client, à l'aide d'un proxy qui expose la logique L4G à des environnements non Progress, tels que .NET ou java (Open Client). L'éditeur adopte également les Web Services en intégrant un proxy SOAP à sa plate-forme. Les développements réalisés avec le langage maison pourront donc être exposés sous Web Service, favorisant ainsi le dialogue avec les autres applications non Progress.

Un plug-in pour l'IDE Visual Studio.NET permet également, à partir de l'environnement de développement de Microsoft, de programmer des appels en C# ou VB.NET vers des composants OpenEdge L4G. Moyennant une légère modification de la CLR (machine virtuelle de .NET), il est ainsi possible de dialoguer à partir d'un environnement .NET avec des composants placés sur l'un des serveurs d'application de Progress : AppServer pour les applications client-serveur ou WebSpeed Transaction Server pour le Web.



En quelques années, Progress est passé d'une architecture propriétaire de type L4G à une suite d'outils très riche et complètement ouverte aux nouvelles technologies.

## Des développements plus rapides quelle que soit la plate-forme cible

L'ouverture aux environnements tiers est d'autant plus réussie qu'elle s'appuie sur le framework Dynamics, lequel favorise la réutilisation des développements. Le principe est simple : l'accès aux données est séparé de la logique métier, de la gestion réseau ou encore de la gestion des sessions. L'ensemble de ces composants est stocké dans un référentiel. Ils peuvent être exploités individuellement et assemblés selon les besoins, par la suite, par d'autres développements, l'ensemble du code étant compilé à la volée, en fonction du client cible (léger, riche, HTML, etc.)

Dynamics est désormais livré en standard avec le studio de développement qui vient d'être unifié : il n'existe plus qu'une seule version que l'éditeur fait évoluer selon un modèle proche de l'open-source. Il intègre donc toutes sortes de contributions externes (pour en savoir plus : [www.possenet.org](http://www.possenet.org)).

Côté intégration, Progress n'est pas en reste non plus, avec une gamme très complète d'outils : le bus applicatif Sonic ESB qui assure le routage et la transformation, Sonic Integration Workbench, interface de développement des règles de routage et de transformation ; Sonic Orchestration Server, particulièrement adapté à la gestion complexe des processus impliquant des Web Services ; et enfin Sonic XML Server qui stocke les messages en XML dans la base

**Produit :** OpenEdge 10, plate-forme qui regroupe les outils de développement, de déploiement, d'administration et l'intégration d'applications.

**Éditeur :** Progress

**Prix :** à partir d'environ 5 000 euros pour la partie Studio de développement.

orientée objet de la société, ObjectStore. Cette dernière conserve notamment l'historique de toutes les transactions intervenues sur le bus applicatif. Les requêtes sont formulées en XQuery, langage plus adapté que le SQL à la manipulation du contenu XML. Tous les connecteurs aux applications tierces, en revanche, sont fournis par lway, société qui dispose aujourd'hui d'un des catalogues les plus fournis.

## Moderniser les applications existantes et faire évoluer les développeurs

La sortie d'OpenEdge 10 est combinée au lancement d'un programme destiné aux partenaires et clients de la société. Objectif ? Moderniser les applications existantes et faire évoluer les compétences des développeurs vers de nouvelles pratiques, plus en phase avec les nouvelles technologies et l'orientation prise par Progress. Baptisé ATG pour Application Transform Group, ce programme prévoit des méthodes documentées sur les bonnes pratiques en développement, l'utilisation des outils, ou encore des exemples de réalisation. Il bénéficie des expériences de la communauté Progress et s'appuie sur OERA (OpenEdge Reference Architecture), un modèle d'architecture préconisé par l'éditeur, très proche de celui de SOA (Service Oriented Architecture). Dans le cadre de ce programme, Progress s'engage également à assister ses partenaires dans la modernisation des applications existantes. L'éditeur compte en effet quelques 5000 applications métiers développées avec sa plate-forme par un réseau de plus de 2000 partenaires. L'enjeu étant pour Progress, qui vend essentiellement via ses partenaires, de les aider à rendre leurs applications plus compétitives.

■ Marie Varandat

# Si vous étiez leader mondial\*, que feriez-vous pour le rester?



# HASP® HL

RÉINVENTE LA PROTECTION DES LOGICIELS ET LA GESTION DES LICENCES.

Lancer HASP HL, le système matériel de protection des logiciels de nouvelle génération permettant de protéger à la fois chiffre d'affaires et propriété intellectuelle.

Implémenter une sécurité avancée et optimale fournie par le leader incontesté, Aladdin. Protégez-les une seule fois. Protégez-les bien.

Faites-vous une opinion avec "Software Protection : 1-2-3", la démo disponible en ligne ou demandez un kit de développement GRATUIT sur le site [HASP.HL.com/encore](http://HASP.HL.com/encore).

- Solution puissante de protection de logiciels axée sur des algorithmes AES et RSA
- Modèles de gestion des licences novateurs utilisés indépendamment de la protection
- Gestion des licences simples et multiples
- Outils et intégration d'API intuitifs et faciles d'emploi
- Clé de haute fiabilité petite, compacte adaptée à toute plateforme

\*Aladdin est le n°1 des clés d'authentification sur le marché de la gestion de licences logicielles en 2002 et 2003.

— Bulletin d'IDC #31 432 de 2004 —

**Aladdin**  
SECURING THE GLOBAL VILLAGE  
[eAladdin.com](http://eAladdin.com)

Tél: +33 1 41 37 70 30  
Email: [HASP.fr@eAladdin.com](mailto:HASP.fr@eAladdin.com)

# WinTasks : améliorer les performances et sécuriser

L'éditeur Leading Interactive vient de sortir une nouvelle mouture de son outil WinTasks. Il s'adresse autant aux développeurs qu'aux utilisateurs avancés.

**W**inTasks aide à maintenir un contrôle total sur les processus, vous permettant d'obtenir ainsi une maîtrise bien plus grande qu'avec le classique Task Manager livré par Microsoft. Après exécution, WinTasks présente une liste des processus tournant actuellement sur votre machine avec la date et l'heure de chaque lancement, ce qui peut s'avérer fort utile. (Fig.1)

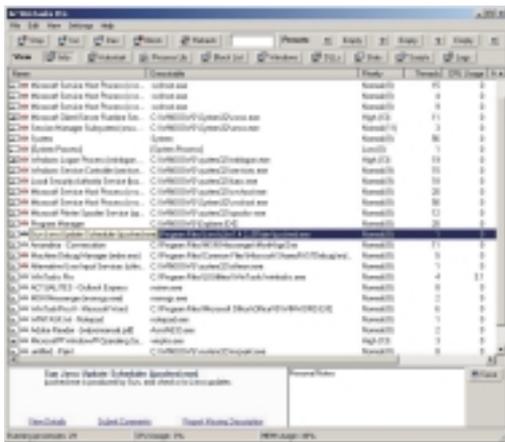


Fig. 1

Vous pouvez stopper un processus, diminuer ou augmenter sa priorité. Rien d'extraordinaire, mis à part le fait que vous pouvez sauvegarder la configuration courante en cliquant sur l'icône représentant une petite clé (menu view/toolbars/preset) : autrement dit, si vous ajustez plusieurs priorités (pour par exemple graver un DVD), ou arrêter des processus, vous pouvez rappeler cette configuration à n'importe quel moment (jusqu'à 4 configurations). Si vous cliquez sur un processus, vous pourrez en apercevoir sa description détaillée. L'utilisateur peut, en un coup d'œil, déterminer quel processus est le plus gourmand en temps CPU ou en utilisation mémoire. Des statistiques (bouton stats) de consommation mémoire et CPU sont d'ailleurs disponibles pour la dernière minute, les dernières dix minutes, les deux dernières heures ou les dernières 24 heures (vous pouvez ainsi détecter plus facilement tous les pics anormaux,

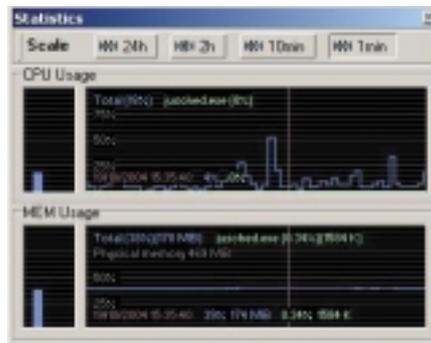


Fig. 2

lorsque par exemple un cheval de Troie s'active la nuit en votre absence). (Fig.2)

### Optimisation des ressources

En cliquant sur le bouton autostart, WinTasks vous affiche une liste des processus qui sont exécutés dès le démarrage de la machine. (Fig.3). C'est souvent à ce niveau qu'un cheval de Troie, ou un exécutable non désirable s'immiscera dans votre système (vous ne pouvez l'enlever dans ajout/suppression de programme). Si vous n'arrivez pas à déterminer la nature d'un programme, vous pouvez commencer par stopper celui-ci (vous le repêrez à l'aide du chemin d'exécution). Si votre ordinateur continue à se

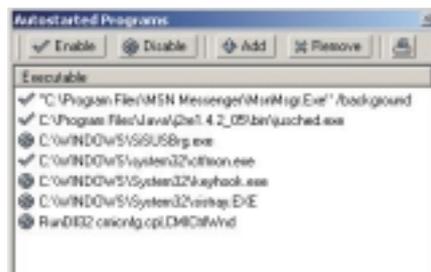


Fig. 3

comporter normalement, vous pouvez désactiver le lancement de ce processus au prochain démarrage (disable), ou tout bonnement, l'enlever de manière définitive (remove).

### Sécurité automatique

Ce n'est pas tout. WinTasks Pro possède une fiche signalétique interne d'identité des processus les plus courants (bouton Process Lib). Cette liste est mise à jour automatiquement, pour peu que vous soyez connecté à Internet. Si un exécutable indésirable tel que le SoBig tente d'infecter votre ordinateur, WinTasks Pro le bloquera. En fait, le nom de son processus (winppr32.exe) est repris dans la liste des processus connus comme étant vérolés, et

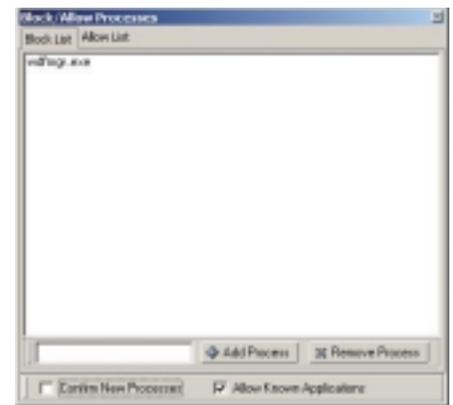


Fig. 4

WinTasks Pro empêchera son exécution. Il est aussi facile de créer sa propre liste de processus bloquants. (Fig.4)

### Journalisation

Vous pouvez aussi pister chaque processus. D'une part, WinTasks Pro tient note de chaque exécution d'un processus, et d'autre part, vous pouvez lui demander de journaliser l'activité d'un process (Settings/log process informations to file). (voit tableau ci-dessous)

### Programmation de scripts

Pour les développeurs, la crème de la crème est la programmation de scripts fonctionnant en temps réel. Par exemple avec le navigateur

Time	PID	Change	CPU	MEM	Name
19/10/2004 13:42:56	1968	Updated	1.5 %	23172 K	WinTaskPro.rtf - Microsoft Word
19/10/2004 15:08:38	1968	Updated	0 %	23276 K	WinTaskPro.rtf - Microsoft Word

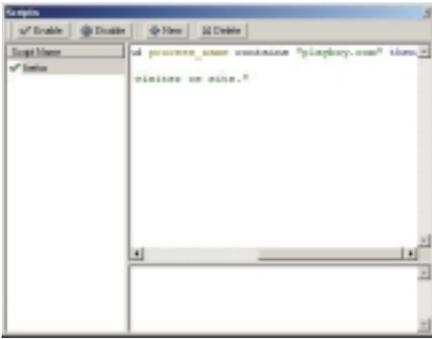


Fig. 5

Firefox (ou mettez 'iexplore.exe' pour Internet Explorer) : (Fig.5)

```
if process_file = "firefox.exe" and process_name contains "playboy.com" then
stop
alert "vous n'êtes pas autorisé à visiter ce site."
endif
```

Si l'utilisateur tente de visiter le site de playboy (c'est-à-dire, si le navigateur est Firefox, et

à condition que le nom du processus reprenne le site de playboy), le processus sera tué (stop) et un message d'avertissement s'affichera (alert).

De même si vous désirez lancer le notepad et la calculatrice :

```
If process_files contains "notepad.exe" and not
process_files contains "calc.exe" then
Start "calc.exe"
Else
If process_file = "calc.exe" and not process_files contains "notepad.exe" then
Stop
Endif
```

Et si le notepad est arrêté, la calculatrice disparaîtra également de la liste des processus actifs...

Les possibilités sont quasi infinies, car vous pouvez combiner les noms des processus avec leurs consommations CPU, si par exemple un processus accapare trop de puissance, vous pouvez diminuer sa priorité ou bien l'arrêter...

## En conclusion

L'utilisateur lambda sous Windows se soucie peu de savoir ce qui se déroule réellement sur sa machine, jusqu'au jour où celle-ci devient instable. Par contre, si en tant que professionnel vous êtes soucieux de ces problèmes de stabilité, de performance et de sécurité, vous pouvez acquérir les yeux fermés cet utilitaire. En outre, les développeurs seront contents de programmer avec WinTasks des scripts qui pourront leur faire gagner du temps, ou qui leur permettront de garder leurs applications sous un œil vigilant.

WinTasks Professionnel version 5.0 fonctionne sous Windows 98/Me/NT4/2000/XP et coûte 59,95 dollars US (vous pouvez l'acheter en ligne).

WinTasks 5 Professional : <http://www.liutilities.com>

■ **Xavier Leclercq**

[Xavier.Leclercq@programmez.com](mailto:Xavier.Leclercq@programmez.com)

Découvrez et approfondissez les technologies PHP et MySQL avec

## Direction | PHP

Actualités  
Trucs et astuces  
Alertes de sécurité  
Expertise technologique  
Dossier entreprise  
Interviews (Rasmus Lerdorf, ...)  
Dossier du mois (PHP5, XML, ...)  
Revue d'applications

**12 numéros au format PDF + les codes sources offerts = 59,90 €**

Pour commander, rendez vous sur le site : <http://www.directionphp.biz/>  
Abonnement pour particuliers et entreprises dans la section " S'abonner "  
Retrouvez tous les extraits gratuits dans la section " Extraits gratuits "

édité par **NeXen**.net

# Windev 9 et Webdev 9

**Novembre 2004 a vu la présentation conjointe de Webdev 9 et Windev 9, les deux versions étant harmonisées afin de mieux travailler ensemble. L'interopérabilité est à l'honneur, avec programmation multi cible, serveur Windows ou Linux, Pocket PC, et récupération de l'existant dans d'autres langages. Sortie officielle pour Noël.**

Plus de 200 nouveautés séparent ces nouvelles versions des précédentes. Comme toujours, une réelle simplicité facilite l'accès aux nouveautés, même si la lecture du mode d'emploi papier, et mieux encore des forums, s'avère plus que jamais nécessaire. En effet, Windev et Webdev tablent sur l'actualité, en créant des ponts vers les technologies les plus récentes. L'ouverture concerne par exemple Java, DotNet et PHP, ainsi que les composants. Un module généré en Windev ou Webdev pourra ainsi devenir du PHP ou du Java natif ! Un exploit de traduction dû à la qualité des développeurs de PCSoft, souvent anciens ingénieurs des grandes écoles.

Du côté des utilisateurs, Windev 9 et Webdev 9 leur ouvrent hors programmation, une liberté plus grande. Ils accèdent directement à la création de macro-commandes, ou encore de graphiques à partir de la sélection spontanée de leurs données, à l'aide du bouton droit de la souris. Si DirectX est installé, la visualisation s'affiche en 3D, elle pivote selon les trois axes... L'accroissement de l'ergonomie est ainsi une conséquence du langage de cinquième génération, qui facilite la souplesse des articulations, comme le faisait déjà la fonction Compile dans la version précédente. Le programmeur et l'utilisateur pouvaient alors déjà interagir.

## Refactoring et centres de contrôles

On nomme 'refactoring' l'action qui consiste à propager les modifications à travers les diverticules d'un programme. Par exemple lorsqu'une zone de texte change de nom, elle apparaît probablement plusieurs fois dans le code de sa fenêtre d'origine, et également dans les états et autres documents utilisant les données concernées. Il en résulte qu'il est plus que facile d'oublier l'une ou l'autre des occurrences, et de le payer par la suite, en terme de dysfonctionnement et débogage. Désormais, on modifie si on le désire, l'ensemble des mentions présentes dans le projet,

progrès, le code conditionnel permet d'attribuer des traitements spécifiques, selon qu'on est sur un PC, sur Internet, ou encore sur un Pocket PC.

## L'ingénierie de la connaissance

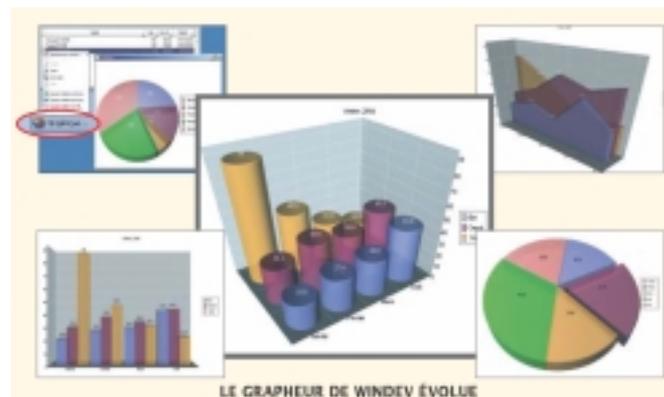
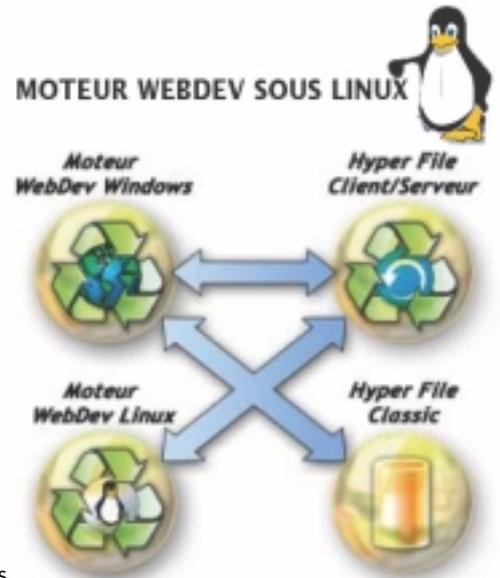
Afin de ne pas négliger le domaine de la représentation de la pensée, préalable au codage, PCSoft a intégré différentes technologies, au-delà de Merise, d'ULM et des différents RAD (ceux-ci fonctionnant désormais également pour générer du Java ou du PHP). Ainsi, le Real Rad permet de générer des

suggérer des idées, par exemple, l'intégration d'un composant tout fait, dont on ignorait l'existence. L'AAP aide à l'amélioration des performances, également à travers des suggestions documentées. Plus important pour l'utilisateur, le MCU ou micro code utilisateur automatise des actions répétitives sous un nom de macro. Le responsable réseau n'est pas oublié. Il bénéficie du MABD, qui met à jour les bases de données sur le réseau, notamment lorsqu'une définition a été ajoutée, modifiée ou supprimée.

## Conclusions

Face à tant de bien belles choses, on pourra cependant objecter que cette version 9 est trop intelligente, trop ambitieuse, trop complexe, en bref, trop riche. Il existe cependant un pare-feu à la confusion entre richesse fonctionnelle et complexité. Il s'agit des forums gratuits dans lesquels les utilisateurs posent et résolvent les problèmes rencontrés. On trouve même des spécialistes qui s'efforcent de rester au Top Ten des incollables. De par notre expérience personnelle, là se trouve probablement l'une des richesses rarement mentionnées de l'environnement Windev et Webdev.

■ Jacques De Schryver



jusque, et y compris, dans les requêtes. Les Centres de Contrôles faciliteront la synthèse des événements rencontrés lors du développement en équipe. Ils documentent et centralisent automatiquement les difficultés, afin, par exemple, d'affecter leur résolution à un programmeur ou à une équipe. Autre

applications complexes, tandis que l'AAA ou Architecture Automatique d'Application, facilite la création de modèles de génération de codes et de fenêtres. Le GCV gère le cycle de vie complet du projet, avec sa maintenance et son évolution. L'AAD ou aide au développement, ira jusqu'à

# Fotovista

## 50 000 lignes de code modifiées en PHP 4

**Le numéro un en ligne de la distribution de matériel photo, vidéo et son en France a décidé de migré le code de PIXMANIA.COM en objet le tout sous MySQL 4.021 et PHP4. Objectif : passer d'une modélisation de données structurée vers une modélisation objet pour gagner en rapidité de développement et en maintenance.**

**F**otovista (236 millions d'euros de chiffre d'affaires pour un effectif de 1200 personnes) est connue pour son site de commerce en ligne Pixmania.com. Le site est la clé de voûte de l'activité de Fotovista avec 3 millions de visiteurs uniques par mois au niveau mondial. Pixmania.com a été développé entièrement par l'équipe interne en PHP. « 90 % de nos applications sont en Open Source, un choix stratégique pour répondre aux problématiques de performance, de fiabilité et de rapidité d'évolution des logiciels » déclare Thibaud Cainne, DSI de Fotovista. Début 2004, la direction informatique mène une réflexion pour migrer son modèle de données MySQL version 4.021 de son site e-commerce, sous PHP 4. « Nous étions confrontés à un code de plus en plus complexe. Il fallait trouver une solution pour diminuer les temps de développement. La version 5 de PHP n'étant pas encore stabilisée, nous avons décidé de rester sous la version 4 » précise Thibaud Cainne. Le système de gestion de commandes du site est sophistiqué. En effet, il prend en compte non seulement les commandes, mais aussi la gestion physique des colis, des articles, des factures, etc, le tout,

en multi-devises et en multilingues, soit 50 000 lignes de code à modifier, ainsi que plusieurs centaines de fichiers. Une refonte en profondeur qui a impliqué 10 mois de développement homme.

### Organiser les équipes

La direction informatique de Fotovista intègre plusieurs équipes : celles dédiées au front-office, au back-office et aux comparateurs/ partenaires, toutes impactées par la migration. Les « comparateurs/ partenaires » comme par exemple, Kelkoo, permet aux usagers de comparer directement le prix du matériel photo sur le Net. Il faut donc qu'il



puisse posséder un extrait de la base de données de Fotovista. « La plus grande difficulté explique Pierre Cailleux responsable Web chez Fotovista a été de synchroniser les équipes. Il a fallu planifier longtemps à l'avance la migration. La réflexion initiale est importante pour comprendre tous les impacts d'une migration objet. » Première phase : réunir les équipes et expliquer le nouveau concept de données objet. Objectif : rendre le développement le plus souple possible en définissant les normes afin que n'importe quel développeur en interne puisse retrouver les méthodes classiques d'exécution de requête, etc. « Nous avons travaillé avec le ges-

tionnaire de sources CVS qui permet à plusieurs développeurs de travailler en même temps sur un même objet » précise le responsable Web.

Pendant quatre mois, 18 développeurs se sont mis à la tâche. « Ils ont réinjecté l'ancien modèle de données soit 3,5 Go dans le nouveau modèle avec à titre indicatif, une trentaine de tables à transformer et à réorganiser de manière différente » ajoute Pierre Cailleux. Deuxième phase : les tests. « Avant la migration nous avons testé pendant trois semaines les modifications du modèle de données. A ce niveau, le département « business intelligence », a commencé sa refonte pour accueillir la refonte de PIXMANIA. Il fallait remplir notre datawarehouse pour prendre en compte la nouvelle structure dans le décisionnel » note le responsable Web. Après une nuit blanche, la migration a été finalement réalisée sans rupture d'activité. « Aujourd'hui nous bénéficions d'un code simplifié, moins de lignes, un affichage des pages Web plus rapide. Et nous pouvons rajouter du code sans que cela deviennent désormais une usine à gaz » conclut avec satisfaction Thibaud Cainne.

■ Annie Lichtner



# Sécurité

## Nouvelles menaces, nouvelles parades



La sécurité demeure une préoccupation forte des utilisateurs et des entreprises. La menace est de plus en plus vicieuse. On ne recenserait pas moins de 5000 virus, vers, ou spywares apparus depuis le début de l'année 2004. On pointe aussi du doigt une autre menace : le cheval de Troie. Les conséquences sont très diverses : vol de données confidentielles, ralentissement de son ordinateur, usurpation d'identité. D'où une perte de productivité, débits illégaux sur des comptes bancaires, écroulement de réseau, etc. Dans ce dossier, vous lirez aussi une section plus pratique, orientée développeur, notamment en listant les failles et vulnérabilités qu'une application web possède et comment les combler afin d'être "secure".

Pour les amateurs de cryptographie, nous vous proposons un exercice sympathique

sur le cryptage du framework .NET. Bien entendu, nous n'oublions pas le côté concret : comment définir une politique de sécurité, les nouvelles techniques de protection (biométrie, les applications mobiles, les clés USB, l'authentification forte, etc.). Vous comprendrez pourquoi, le mot de passe statique que l'on utilise tous les jours devient une passoire

■ François Tonic

### 3000 attaques par jour à la MAAF

Le Pdg des assurances MAAF-Groupe MMA, Jean-Claude Seys, expliquait le 12 novembre sur la radio BFM qu'une de ses principales hantises, en terme de sinistre, après les risques de santé publique, étaient "le terrorisme et les attaques informatiques". Et d'ajouter : "notre société subit 3000 attaques par jour, nous les arrêtons, mais on ne sait pas jusqu'à quand".

# Le hacking a-t-il changé ?

D'abord si on parle de hacking, c'est par abus de langage. En effet si on doit désigner par ce terme l'introduction illégale, à distance, dans des systèmes informatiques, il faudrait plutôt parler de crac-



king. La différence fondamentale est la suivante : les hackers construisent des systèmes tandis que les crackers les cassent. Cette citation d'Eric S. RAYMOND en dit long : "Les vrais hackers pensent que les crackers sont des gens paresseux, irresponsables et pas très brillants".

**I**l faut bien prendre conscience que des systèmes informatiques entiers sont rendus inutilisables (et donc, ne trouvent pas acquéreur) du seul fait qu'ils n'offrent pas un degré de protection suffisant. La question de la sécurité est donc primordiale pour tous : les développeurs aussi bien que les utilisateurs. En outre, les techniques de cracking, du parfait pirate, évoluent en permanence, parallèlement à la technologie (\*). Il faut donc régulièrement mettre à jour les logiciels de protection pour qu'ils restent efficaces. Pas question donc de les figer, et une mise à jour régulière d'un nombre indéterminé de logiciels est toujours coûteuse en temps et en argent.

## Quelles sont les nouvelles méthodes d'attaque, les nouvelles techniques ?

Nous prendrons comme référence la liste des vulnérabilités produites par le SAN. Cet organisme international (System Administration Networking and Security Institute) en collaboration avec le FBI dresse depuis quelques années une liste des faiblesses les plus courantes en matière de sécurité. La dernière en date (version 5) a été mise à jour au mois d'octobre 2004.

### TOP 10 des vulnérabilités sous Windows

- W1 Web Servers et Services
- W2 Workstation Service
- W3 Windows Remote Access Services
- W4 Microsoft SQL Server (MSSQL)
- W5 Windows Authentication
- W6 Web Browsers
- W7 File-Sharing Applications
- W8 LSAS Exposures
- W9 Mail Client
- W10 Instant Messaging

### TOP 10 vulnérabilités sous Linux/Unix

- U1 BIND Domain Name System
- U2 Web Server
- U3 Authentication
- U4 Version Control Systems
- U5 Mail Transport Service
- U6 Simple Network Management Protocol (SNMP)
- U7 Open Secure Sockets Layer (SSL)
- U8 Misconfiguration of Enterprise Services NIS/NFS
- U9 Databases
- U10 Kernel

Le SAN sépare le risque Windows de celui d'Unix. Ensuite, des nouvelles failles sont apparues, comme celle de la messagerie instantanée (W10), ou celle relative au navigateur (W6). Au sujet de cette dernière vulnérabilité, il faut savoir que L'US-CERT, un organisme indépendant du ministère américain de la sécurité intérieure, a récemment publié une note préconisant plusieurs mesures pour faire face aux multiples problèmes de brèches ouvertes, rencontrés par Internet Explorer (IE). D'abord, désactiver l'Active Scripting et les

contrôles ActiveX, ensuite mettre à jour son navigateur, ne pas cliquer sur les liens reçus, et enfin... changer de navigateur.

### [W1] Vulnérabilité des services et serveurs Web

Au sujet des serveurs Web, il ne faut pas remonter bien loin dans le temps pour trouver un exemple. En effet, récemment une vulnérabilité a été découverte dans les mécanismes d'authentification de ASP.NET 1.0 et 1.1 sur IIS 5.0 sous Windows XP (et Windows 2000).

Pour s'en protéger il faut ajouter le code suivant au fichier global.asax :

```
Sub Application_BeginRequest(ByVal sender As Object, ByVal e As EventArgs)
    Dim rPath As String = Request.RawUrl
    rPath = rPath.Replace("\", "/")
    Context.RewritePath(rPath)
End Sub
```

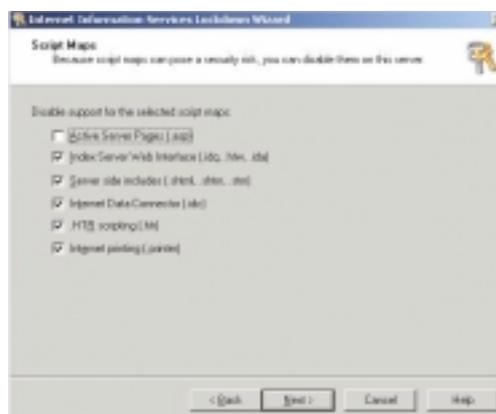
Cela dit, Microsoft fournit deux outils gratuits, appelés IISLockDown et URLScan, pour essayer de minimiser les risques. IISLockDown permet d'automatiser certaines phases de sécurisation. Suivant le modèle de sécurisation adopté (serveur http uniquement, serveur de base de données, etc.), ce logiciel désactivera certaines fonctionnalités du serveur, ou les sécurisera si nécessaire. URLScan (installé par IISLockDown) possède comme caractéristique de restreindre l'accès à certains types de requêtes HTTP auquel le serveur est habilité à répondre. Les requêtes malveillantes seront ainsi repoussées.

IISLockDown et URLScan : <http://www.microsoft.com/technet/security/tools/locktool.mspx>

Une machine Windows expose par défaut toute une gamme de services au monde extérieur.

Depuis Windows 2003, Microsoft a radicalement modifié cette politique, partant du principe qu'un service ne doit être actif qu'en connaissance de cause. Sous XP, vous devez installer le service pack 2 pour profiter d'une protection minimale.

Il faut donc désactiver les services inutiles (comme Messenger et Telnet) et les protocoles non utilisés (NetBIOS, WebDAV, SMB, FTP, NNTP, etc.) et renforcer la pile TCP/IP en configurant divers paramètres au niveau de la base des registres pour contrer les attaques par refus de services (\*).



[W2] Vulnérabilité du service station de travail  
C'est ici la gestion à distance du service workstation qui est visée. En effet, les différentes fonctions d'administration de Windows sont accessibles, via des fichiers spéciaux appelés tubes nommés, et regroupés dans le partage IPC\$. Les fonctions d'administration qui sont proposées par les API de Windows font appel à ces tubes nommés, en utilisant le protocole SMB pour, par exemple, ouvrir un fichier. Le cracker peut de cette manière s'infiltrer à distance.

**En voici une liste :**

\pipe\eventlog :  
pour la gestion à distance des journaux

\pipe\lsarpc :  
pour la gestion à distance de la LSA

\pipe\samr :  
pour l'administration de la base SAM

\pipe\spoolss :  
concerne les imprimantes partagées

\pipe\svrsvc :  
le service serveur

\pipe\svcsctl :  
les services gérés à distance

\pipe\winreg :  
l'accès à distance à la base de registres

\pipe\wkssvc :  
l'accès à distance du service workstation

L'outil pipelist permet de lister tous les tubes nommés ouverts sur une machine locale : <http://www.sysinternals.com/ntw2k/info/tips.shtml>  
Le remède ? Microsoft propose son propre outil d'analyse de failles, le Baseline Security Analyzer (MBSA). Celui-ci s'utilise, via une interface graphique, ou une console d'administration. Il est possible avec cet utilitaire d'indiquer une plage d'adresses IP pour sonder un réseau local ou distant. Le rapport final vous indique les failles potentielles en vous proposant des rustines ou des actions de réparation adéquates. Pour un cracker il s'agit de renseignements très utiles, car les articles

issus de la base de connaissance de Microsoft indiquent souvent comment répéter une faille ou un bug. Dans la plus part des cas, quand une nouvelle vulnérabilité du système est découverte, le mode d'emploi pour exploiter cette vulnérabilité est lui aussi publié dans les heures qui suivent. Il faut donc patcher et mettre à jour le plus souvent possible : le service pack 2 automatise cette mise à jour.

### **Faut-il penser et réfléchir comme un hacker pour le contrer ? Autrement dit, faut-il en connaître autant que l'attaquant pour se protéger correctement ?**

Cette question est primordiale. Un fournisseur d'un service sécuritaire peut-il offrir un logiciel ou un dispositif hardware contre quelque chose dont il ignore l'existence ? Un utilisateur peut-il être efficacement protégé contre une attaque dont il ignore les implications techniques ? L'actualité de ces dernières années l'a démontré à maintes reprises : à moins d'être au courant quasi en temps réel d'une attaque (d'un ver par exemple), vous serez toujours en retard d'une guerre lorsque celle-ci se produira effectivement.

Pour y remédier il n'y a pas trente-six mille possibilités : les fournisseurs de sécurité doivent pratiquer de la veille technologique. Concrètement, les veilleurs devront commencer par rechercher sur Internet des bonnes sources d'information. Il faut savoir que la plupart de celles-ci ne proviendront pas des moteurs de recherches traditionnels. En effet, un moteur comme Google est très mal adapté à l'indexation de documents récents ou de qualité (selon la verticalité de la recherche sécuritaire effectuée). Google s'attarde beaucoup plus sur le contenu superficiel, que l'on peut visualiser comme étant le sommet d'un iceberg. Selon une étude menée par l'univer-

sité de Berkeley, l'ensemble des informations produites par un homme, une femme ou un enfant vivant sur terre est de 250 Mega bytes par personne (source : <http://www.sims.berkeley.edu/research/projects/how-much-info/>). Et ceci, chaque année... Par exemple, l'équipe de veille technologique de Symantec scanne régulièrement des dizaines de milliers de sites Internet de la zone grise (crackers et hackers) pour tenter d'y découvrir une nouvelle technique, jamais répertoriée auparavant. De ce fait, et même si aucun microbe logiciel ne l'exploite encore, il y a moyen de définir une nouvelle règle pour contrer un virus qui n'apparaîtra en définitive que quelques mois ou quelques années plus tard. Concrètement, le système Deep Sight mis au point par Symantec permet de comparer les informations récoltées aux 30 terabytes de données historiques disponibles.

Du côté du client/utilisateur il faut s'informer continuellement, appliquer les patches et adopter autant que possible des outils proactifs. C'est-à-dire qu'il ne faut pas se protéger en tenant compte seulement des attaques passées, qui sont disponibles sous la forme d'une définition (d'une règle de sécurité). Reconnaître une signature stable d'une attaque réseau ou d'un virus informatique représente un travail complexe et périlleux en raison de la sa nature potentiellement changeante. C'est pourquoi, l'antivirus ou le détecteur de rootkits, essaiera aussi de repérer des caractéristiques globales plutôt que des détails (c'est-à-dire des signatures uniques). Malheureusement, les attaquants ont trouvé des parades anti-heuristiques parfois très efficaces, dont le corollaire est le risque de déclencher un nombre anormalement élevé de fausses alarmes.

### **Quelles seront les futures menaces ?**

Info ou intox commerciale, les principaux fournisseurs d'antivirus prétendent recevoir quotidiennement plus de 10 microbes jamais vus auparavant...

L'avenir ne s'annonce pas rose, et voici un échantillon des perspectives :

- Les éditeurs d'antivirus s'inquiètent qu'un futur composant de Longhorn, le Microsoft Shell (nom de code Monad) permette de créer des scripts pour contrôler le système d'exploitation ;

#### **(\*) Dans l'éditeur de la base des registres, recherchez l'entrée :**

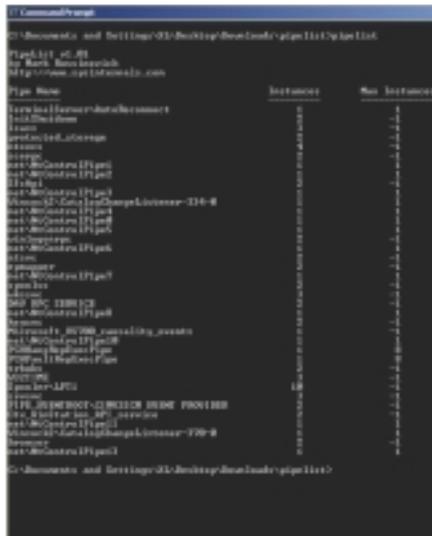
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Et modifiez les valeurs suivantes :

EnableDeadGWDetect = "0" (défaut = 1)  
 EnableCMPIRedirect = "0" (défaut = 1)  
 EnablePMTUDiscovery = "0" (défaut = 1)  
 KeepAliveTime = "300,000" (défaut = 7,200,000)  
 NoNameReleaseOnDemand = "1" (défaut = 0)  
 PerformRouterDiscovery = "0" (défaut = 1)  
 SynAttackProtect = "2" (défaut = 0)

- Tous les systèmes d'exploitation sont concernés par des problèmes de sécurité, même Linux (et Unix) quoique relativement préservé jusqu'à maintenant. Ainsi, Mac OS X a été touché récemment par le virus Opener, volant les mots de passe et désactivant les protections du système en ouvrant des portes dérobées. Malheureusement, son code est simple à modifier ce qui pourrait engendrer pas mal de variantes ;
- La messagerie instantanée (risque SAN W10) est à son tour touchée. Récemment, un nouveau microbe du nom de Funner a infecté des postes, via MSN, en provoquant des redirections intempestives sur un site chinois (www.78p.com) ;
- D'après McAfee, 20 % des e-mails seraient infectés ;
- La grave faille JPEG provoquant la prise de contrôle d'un poste par simple affichage d'une image (par le biais d'un débordement de tampon) n'est sans doute que le sommet de l'iceberg de problèmes futurs. En effet, le code source de Windows ayant été diffusé (illégalement) sur Internet, la probabilité est forte que d'autres failles soient découvertes par des crackers (les crackers sont des opportunistes).

Si le système d'exploitation est fermé, le colmatage d'une brèche dépend du propriétaire de ce code qui ne peut être lu ou modifié par une tierce personne. Malheureusement, la mise à disposition de ce correctif pourra se



faire attendre, car le bout de code défaillant sera, par exemple, jugé impossible à corriger, trop cher à produire, peu dangereux ou ne touchant qu'une partie infime des utilisateurs. Comme tous les programmes sont bogués, l'utilisateur est au bout du compte pris en otage. Sans entrer dans une polémique sans



fin, il faut reconnaître que les utilisateurs de logiciels open source évitent ces écueils.

## Conclusion ?

Vouloir sécuriser une machine isolée ou un réseau d'entreprise a un coût. Cependant, il est clair qu'il ne sert strictement à rien d'investir dans du matériel ou des logiciels coûteux, sans réfléchir à une politique globale de sécurité. Si vous achetez un pare-feu, mais que vous l'installez par défaut, ou si vous investissez dans un système de détection d'intrusion, ou un antivirus sans mettre à jour les règles de définitions ou les signatures, ou si personne ne lit les messages d'avertissements produits par vos logiciels, cela ne sert à rien. Que les logiciels soient fermés ou bien Open Source n'y change rien. L'idéal serait d'installer des systèmes sécuritaires, puis de les oublier. Actuellement, c'est impossible. La solution miracle n'a pas encore été inventée. Il faut donc que les utilisateurs finaux acceptent que leurs logiciels soient moins conviviaux, mais plus sécurisés, que les développeurs tiennent compte de la sécurité au niveau de leurs développements, et que les entreprises prévoient un budget conséquent en matériels, logiciels et conseils... Bref tout un programme... que tout le monde n'est pas encore prêt à accepter.

■ **Xavier.Leclercq**  
Xavier.Leclercq@programmez.com

## Dictionnaire de l'insécurité

	C'est quoi ?	Quelques mesures
<b>Spam</b>	Mails publicitaires, la plupart sont des arnaques	Filtres mail au niveau serveur ou de la messagerie, outils d'anti-spamming
<b>Virus</b>	Petit programme s'exécutant sur un ordinateur. Existe plusieurs types de virus dangereux ou non. Se propage grâce à l'utilisateur	Firewall, filtres, antivirus (sur l'ordinateur ou en réseau)
<b>Ver</b>	Se propage sans l'aide de l'utilisateur. Variante du virus	Idem que pour les virus
<b>Cheval de Troie (ou Troyen, ou Trojan)</b>	Code malicieux capable d'exploiter plusieurs failles d'un logiciel, d'un système. Dangereux (prise de contrôle d'un PC, vol de données...)	Seuls les Troyens connus sont détruits. Bloquer les accès au périmètre avec du firewall, filtres, etc. Outil anti-intrusion.
<b>Spyware (logiciel espion)</b>	À l'origine, avait un but commercial afin de récupérer des informations sur l'utilisateur. Petit logiciel actif à l'insu ou non de l'utilisateur.	Anti spyware
<b>Malware</b>	Généralité. Tout programme pouvant nuire à l'ordinateur, à une application, à l'utilisateur (virus, ver...)	
<b>Phishing</b>	Une technique d'usurpation d'identité. Permet de récupérer des informations confidentielles en trompant l'utilisateur et des sites marchands ou non.	Infrastructure de confiance, signature, etc.
<b>Spoofing</b>	Technique d'usurpation d'identité afin de tromper un serveur, un réseau. Ex. : spoofing d'IP pour pénétrer dans un réseau.	Système d'identification, anti-intrusion...
<b>Sniffing</b>	Écoute d'une communication, d'une session pour repérer les paquets pour les voler, les corrompre ou pour ensuite attaquer (ex. : vol de mot de passe).	Cryptage, sessions sécurisés
<b>Key logger</b>	Logiciel enregistrant toute frappe du clavier. C'est une sorte de Troyen	Firewall, filtre, contrôle des flux

Mini-bibliographie : C. Camborde, *sécurisez vos applications internet*, Dunod, 2004 - Collectif, *Sécurité des architectures web*, Dunod, 2004 - Collectif, *écriture du code sécurisé 2e édition*, Microsoft press, 2003

# Spywares : ils n'ont pas dit leur dernier mot !

**D'abord il y a eu les virus, puis il y a eu les vers, puis les Spam sont venus compliquer l'utilisation des emails. Au fur et à mesure que les menaces apparaissent, les éditeurs organisent la défense. Des antivirus sont développés pour protéger les postes de travail, les serveurs et les réseaux ; des systèmes anti-intrusion et des firewalls bloquent les vers; et des solutions antispam tentent de bloquer le harcèlement publicitaire des fournisseurs de Viagra.**



La dernière menace des pirates du Web est le spyware. L'éditeur Webroot définit le spyware comme un logiciel qui s'installe sans le consentement de l'utilisateur selon une grande variété de modes d'intrusion. Parmi eux on trouve le changement de la page de démarrage pour une page indésirable, la redirection forcée de recherches faites sur le net vers un site non choisi, l'apparition de pop up indésirables et même la surveillance étroite d'un utilisateur permettant de prendre le contrôle de son PC. Des pirates utilisent même à leur insu le modem de certains utilisateurs pour établir régulièrement des communications téléphoniques longue distance à peu de frais ! Beaucoup d'utilisateurs ne savent même pas qu'ils sont infectés de logiciels espions jusqu'à ce que les performances de leur PC se dégradent nettement. Une récente étude menée par Webroot en collaboration avec la société américaine ISP EarthLink, a mis en évidence que 90 % des internautes connectés à Internet étaient infectés et qu'en moyenne chacun de ces postes utilisateurs grand public était infecté de 28 spywares.

## Spywares et virus agissent de concert

Les spywares se définissent par ce qu'ils font, tandis que les virus et les vers se définissent plutôt par les modifications de fonctionnement qu'ils introduisent. Il est de plus en plus difficile de distinguer les spywares des virus, car

les deux sont souvent imbriqués pour agir simultanément. Un virus tel que Bagle ou MyDoom, ou un ver tel que Funner peut, par exemple, installer un spyware sur un ordinateur, mais l'installation d'un spyware se fait le plus souvent à l'occasion d'un téléchargement de logiciel. Ainsi KaZaa, le logiciel, s'installe avec plusieurs spywares, tout comme les économiseurs d'écran et les jeux qui sont aussi souvent l'occasion d'installer ces espions en même temps. La plupart du temps, les utilisateurs se trouvent infectés pendant qu'ils vont sur des sites qui installent des spywares utilisant des contrôles ActiveX ou Java. La raison qui fait que les Spywares constituent une très grande menace pour les internautes est le fait qu'ils rapportent énormément d'argent à leurs auteurs et à ceux qui se chargent de les propager. En effet, les auteurs et les distributeurs sont rémunérés proportionnellement au nombre d'internautes qu'ils redirigent vers des sites complices qui font appel à ces méthodes de détournement, sachant que chaque fenêtre pop up qui s'ouvre leur génère encore un peu plus de chiffre d'affaires. Le plus dangereux des spywares surveille les utilisateurs. Il est mis en place par des escrocs pour intercepter ses noms d'utilisateurs, ses mots de passe et ses informations bancaires afin de détourner l'argent de son compte en banque.

Richard Stiennon, VP de WebRoot, éditeur de Spysweeper précise : " Il y a de nombreuses mesures à prendre pour éviter les spywares : toujours utiliser les dernières mises à jour des

outils Microsoft ; ne jamais télécharger de logiciel d'une source inconnue et ne jamais cliquer sur les bouton "no" d'une fenêtre "pop up" demandant si l'on souhaite installer un logiciel et quand une fenêtre "pop up" indésirable apparaît il faut la fermer en cliquant sur la croix de fermeture de la fenêtre et non sur le bouton "no". Beaucoup de spécialistes de la sécurité sur Internet conseillent aux utilisateurs de se tourner vers des navigateurs tels que safari ou Fire Box 1.0 qui ne sont pas perméables aux spywares actuels. Alors que ces navigateurs alternatifs deviennent de plus en plus répandus chez les internautes, de nouveaux spywares vont être créés pour les infiltrer.

Tout comme les virus, les spywares sont continuellement modifiés et mis à jour par leurs auteurs afin de déjouer les nouvelles protections.

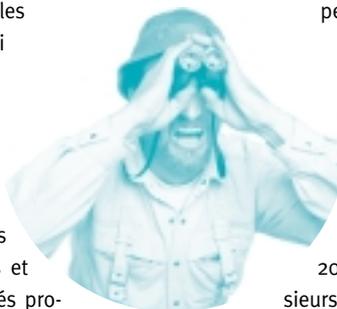
Peut-on prévoir la fin de l'expansion des espions et autres menaces Internet ? Pour

M. Stiennon, le cycle du développement des nouvelles menaces et des nouvelles protections n'est pas prêt de se terminer. Pour enrayer ce cycle, il faudrait rendre les outils Microsoft moins vulnérables. Microsoft prévoit de sortir le prochain Windows en

2006 et il faudra ensuite plusieurs années pour que les utilisateurs migrent tous dessus.

La plupart des analystes et experts en matière de sécurité estiment qu'un nouveau système d'exploitation ne changera rien et que les pirates trouveront rapidement le moyen de contourner ses protections.

Dans les 6 ou 12 mois qui viennent, on peut s'attendre à une formidable montée en puissance des dommages causés par les spywares. On s'attend, en particulier, à un spyware qui utiliserait la faille d'un outil Microsoft en infectant un PC par le biais d'une image, un fichier jpeg reçu par mail, ou chargé à partir d'un site Web. Cette vulnérabilité des produits Microsoft est une aubaine pour les pirates du net. C'est





une manière parfaite pour injecter un nouveau spyware dans un PC comme M. Stiennon. De plus, les différents types de menaces vont se faire la courte échelle. Ainsi, des vers et des virus seront créés pour se propager sur Internet et installer des spywares. Ils utiliseront comme vecteurs la transmission de messages instantanée (IM), les emails, les dossiers partagés, et même les nouveaux messages d'information RSS en XML. Comme il va être de plus en plus difficile de séparer les différents types de menaces, il va être de plus en plus difficile de lutter contre les menaces visant le PC, les comptes bancaires ou la vie privée. C'est pourquoi, les outils qui ont pour vocation de protéger l'utilisateur devront être de plus en plus vigilants. Comme le dit M. Stiennon : " si nous voulons continuer à apprécier les avantages de la communication facile d'Internet, nous devons lutter en parallèle de toute notre force contre les auteurs de spywares.

### Lutter contre les spywares ?

1. Télécharger un outil de détection et de nettoyage de spywares,
2. Utiliser un antispyware pour empêcher les futures infections,
3. Employer un navigateur alternatif à Microsoft Internet Explorer tel que Mozilla Firefox, ou mettre à jour régulièrement sa version d'IE,
4. Ne jamais installer un logiciel sans examiner soigneusement son origine et être soupçonneux !

■ *Propos recueillis par François Tonic*

# Le mode de propagation des vers évolue

## Entretien avec Eyal Dotan

(Directeur R&D de TEGAM, éditeur de la solution antivirus ViGuard)

*Programmez : existe-t-il une nouvelle génération de virus ?*

**Eyal Dotan :** Le ver ne change pas. Ce qui évolue, à l'image d'un Blaster, c'est son mode de propagation. Quand il y a une faille critique, le ver s'y engouffre. Il y a encore plus de vers diffusés par mail que par faille. Cependant, ce type d'infection augmente, la propagation est plus rapide avec des failles Windows. Le ver en lui-même ne fait que se propager. Ce qui serait catastrophique, c'est s'il détruisait des fichiers systèmes ou personnels. Cela pourrait arriver dans l'avenir, certaines variantes de vers le feraient. Mais, les menaces peuvent être plus subtiles. Il peut faire plus de choses. Le virus pourrait ouvrir un port et transmettre des données confidentielles, via un cheval de Troie ou un helper. On constate la création de groupes d'auteurs de virus.

*Programmez : La prise de conscience est-elle réelle ou non ? L'utilisateur est-il plus conscient du problème de la sécurité ?*

**ED :** Oui, il y a de plus en plus d'utilisateurs au courant du problème. Si on regarde les statistiques, le nombre d'infections a doublé. Il y a une prise de conscience, mais les systèmes de protection ne sont pas imparables. Le virus arrive de plus en plus rapidement. Un autre danger est le ver ouvrant des ports sur son système. Cela demeure une minorité des vers, mais en 2004, ce type de ver a connu une progression. Il s'agit maintenant de ver / virus, à but lucratif.



*Programmez : Constatez-vous une évolution de la mentalité et de la motivation des hackers, du hacking ? La méthode d'attaque a-t-elle changé ?*

**ED :** La réponse est plutôt oui. La motivation a changé. Le hacking n'est plus aussi "noble" qu'auparavant. Avec le Web, les hackers ne sont plus réellement de "vrais" hackers. Pour les virus, ils reprennent souvent les bases existantes, ils partent moins de zéro. Il faut comprendre techniquement et les méthodes qu'ils utilisent pour tromper l'utilisateur. Il faut connaître les techniques de hacking. Sur les attaques directes dans un contact direct avec Internet. Il faut mettre à jour les outils et bien configurer applications et serveurs. De plus en plus d'outils arrivent bien fermés par défaut. L'attaque indirecte se fait par un virus, un ver, un cheval de Troie, on rentre par l'utilisateur. Firewall ou non, rien ne peut l'arrêter. Il faut déjà détecter les chevaux de Troie connus. Les chevaux de Troie spécifiques ou inconnus sont très difficiles à détecter.

■ F.T.

## Conseils pratiques de sécurité

Nous avons glané quelques conseils sur le site [www.viguard.com](http://www.viguard.com).

*La sécurité informatique repose sur trois éléments indissociables :*

### 1. Le comportement de l'utilisateur

- Un utilisateur mal informé ou négligent peut réduire à néant n'importe quelle protection. Miser sur l'information et la formation.
- Vous pouvez prendre l'habitude de demander à vos interlocuteurs d'avoir eux aussi un comportement responsable : ils veulent vous envoyer un message avec pièce jointe ? Qu'ils vous préviennent avant par e-mail séparé et vous annoncent d'abord précisément le nom de la pièce jointe qui sera attachée à leur e-mail suivant.

### 2. Les correctifs (patches)

Appliquez les correctifs (patches) de sécurité critiques de Microsoft pour ne pas laisser ouvertes des brèches de sécurité. Après diagnostic en ligne, ils sont délivrés via la fonction Windows Update de votre machine ou téléchargeables depuis le site de Microsoft.

### 3. Les protections logicielles nécessaires :

- Protection antivirale contre les virus, vers et chevaux de Troie
- Les pare-feu constituent une brique de sécurité complémentaire.

# Chevaux de Troie : le vrai danger !

On aurait tendance à l'oublier un peu rapidement, le " Cheval de Troie " est pourtant en passe de demeurer la véritable menace du monde informatique. Vieux et perfectionné, il constitue un défi pour les utilisateurs, les développeurs, les entreprises. Entretien avec Joachim Krause, consultant sécurité Telindus, SSII orientée réseaux et sécurité.

**Programmez ! : Comment jugez-vous la menace informatique aujourd'hui ? On parle beaucoup de phishing, de spam, de spyware, est-ce la réalité ou une petite partie des menaces réelles ?**



**Joachim Krause :** Il y a un déplacement de la menace, avant elle était sur l'infrastructure, le réseau, maintenant, elle s'oriente sur les utilisateurs. Le phishing n'est que l'aspect le plus visible du problème. Il y a quelque chose de bien plus grave, le Cheval de Troie. Le phishing reste encore très anglo-saxon, comme le spam. On est suspicieux envers un mail en Anglais. Or, maintenant, l'utilisateur fait face aux Troyens. Il n'est pas protégé. Les statistiques des éditeurs d'antivirus montrent qu'il y a autant de nouveaux Troyens que de nouveaux virus !

**Programmez ! : Faut-il distinguer différents niveaux dans la dangerosité, entre un cheval de Troie, un spyware, un spam, etc. ?**

**Joachim Krause :** Il y a en effet d'importantes différences. Intrinsèquement, le ver ou le virus n'est pas aussi dangereux que cela. On a pu le constater avec Blaster. Il est " inoffensif ". Il produit un DoS, mais n'atteint pas la vie privée. Sasser avait fait parler de lui, mais les dommages furent quasi nuls. Le spyware est un outil commercial. Certains sont très agressifs, comme le spyware Gator. Il écrit dans la base registre. Il attend donc à l'intégrité du système et à la vie privée. En haut de l'échelle de la menace se situe le cheval de Troie. Il pose de gros soucis techniques. Il est d'une technicité élevée, car capable d'exploiter 3 ou 4 vulnérabilités ! Un de ses objectifs est la cyber criminalité ! Le code malicieux est une arme servant à gagner de l'argent. Il est donc à but lucratif, en volant les informations confidentielles nécessaires. On constate qu'un grand nombre de Troyens sont orientés "banque", comme le key logger.

**Programmez ! : Le cheval de Troie est-il réellement aussi présent que cela ? Peut-on décortiquer un Troyen ?**

**Joachim Krause :** Dans des statistiques sur les 10 premiers jours du mois d'octobre dernier, un client a recensé 77 Troyens " banque ", 10 Troyens divers, 28 spams et phishings, 14 jokes et 21 vers / virus.

La menace est claire, c'est le cheval de Troie ! Décortiquer un cheval de Troie est compliqué et prend du temps. Il est souvent écrit en C, C++ ou en assembleur, pas en Java. Java peut, par contre, servir à télécharger un Troyen sur un ordinateur, via une page Web trafiquée. L'accès distant est une autre pratique commune.

Elle permet notamment de se servir d'un ordinateur comme d'un relais de spam. Il faut savoir que c'est très lucratif, certains pirates vendent du relais de spam ! Quand une machine est "black listée", le pirate passe à une autre... Une autre tendance est le PC zombie. Il sert à lancer des attaques. Je pense que ce type d'attaques va augmenter.

**Programmez ! : Comment le Troyen se propage-t-il ?**

**Joachim Krause :** Encore aujourd'hui, on a

beaucoup de difficulté à répondre à cette question. La première hypothèse, c'est l'exploitation de vulnérabilités que l'on connaît, mais qui ne sont pas corrigées, exemple, celles d'Internet Explorer. La 2e hypothèse est d'utiliser des vers pour installer un Troyen. C'est une bonne idée. On écrit un ver, on le diffuse, il contamine un poste. On passe alors un antivirus qui détruit la partie vérolée, mais le Troyen, lui demeure ! Une autre technique consiste à utiliser le ver pour ouvrir des ports sur l'ordinateur que le pirate utilise ensuite pour installer son Troyen.

**Programmez ! : À vous écouter, le Troyen est une bête terrible, peut-on néanmoins limiter sa présence ?**

**Joachim Krause :** Oui, il existe des parades, mais on est en retard entre la découverte d'un Troyen et les mécanismes de blocage. Pour rattraper ce retard, il faut mettre en place du bon sens, faire du safe computing, par exemple, ne pas aller sur des sites douteux, ne pas utiliser des outils de P2P ou de télécharger des MP3, etc.

■ *Propos recueillis par François Tonic*

## Description du Troyen SCOB

Le pirate compromet un site Web s'appuyant sur Microsoft Web IIS (hébergé en règle générale par Windows 2000 ou 2003). Pour cela, il utilise une faille de ce produit qui semble être la faille " PCT " déjà utilisée dans le passé par de nombreux vers et chevaux de Troie. Il n'est pas exclu non plus que la vulnérabilité utilisée soit une nouvelle faille du produit Microsoft. Plusieurs jours après l'alerte, cette information n'est toujours pas fiable.

Le pirate exécute un VBScript sur le serveur Web IIS. Ce code malicieux ajoute un code JavaScript en bas des pages web (Footer) du site hébergé par le serveur. Ce cheval de Troie JS/Scob sera alors téléchargé par tous les postes de travail qui consulteront une page infectée.

Un serveur compromis présente les caractéristiques suivantes :

- Dans le répertoire %Systemroot%\System32, la présence des fichiers Agent.exe, et Ftpcmd.txt, Download\_Ject\_Symantec.doc, ipaddress.txt, issue.csv, et security\_log.rtf.
- L'option " Enable document footer " est activée et référence des fichiers de type %Systemroot%\Winnt\System32\Inetsrv\lis<3 nombres aléatoires>.dll

# Check list de sécurité du développeur

L'application est le maillon faible de la sécurité. Les développeurs d'application pour le Web, ne sont pas ou peu informés. Les pressions sur les délais empêchent généralement la prise en compte sérieuse des risques. Les pirates exploitent alors facilement ces faiblesses.

Est-ce que l'application exige une authentification ? Nous allons d'abord répertorier les différentes attaques possibles. Puis nous évoquerons les

autres vulnérabilités rencontrées fréquemment dans les applications WEB.

Avant de publier votre application sur le Net, imaginez toutes les utilisations détournées possibles. Si le risque est important, faites auditer votre application par des professionnels.

■ **Philippe Prados** [www.philippe.prados.name](http://www.philippe.prados.name)

## Les attaques les plus fréquentes

-  **Attaque : Soumettre très rapidement des authentifications, avec différents mots de passe tirés de dictionnaires, ou produits par force brute.**

 Solution : Limiter le nombre de tentatives d'identification avant de bloquer un compte. Proposer un test, que seul un humain, dans l'état actuel des technologies, est capable de résoudre (image avec texte).
-  **Dénis de service en grillant tous les comptes.**

 Ne pas bloquer le compte, mais imposer un délai d'attente de plus en plus long avant une nouvelle tentative d'authentification.
-  **À la longue pourtant, un mot de passe est vulnérable.**

 Imposer un changement de celui-ci régulièrement.
-  **Approche inverse, chercher un compte possédant un mot de passe particulier. Si les identifiants sont prédictibles les uns des autres (numéro de compte bancaire, prénom suivi du nom, etc.) il est possible de chercher s'il n'existe pas un compte ayant un mot de passe simple.**

 Mémoriser les mots de passe en échec pendant une période, et, si un seuil est dépassé, refuser les authentifications avec ce mot de passe, même s'il est valide.
-  **Exploiter le temps mis par le serveur pour détecter l'échec d'un mot de passe. En chronométrant le temps mis par le serveur pour refuser un mot de passe, il est possible de découvrir un à un les différents caractères du mot de passe.**

 Utiliser un algorithme à temps constant pour qualifier un mot de passe.
-  **Le mot de passe initial d'ouverture du compte peut être toujours valide.**

 Celui-ci doit être immédiatement modifié après la première connexion et l'usage limité dans le temps.
-  **Si un compte est découvert, il permet de prolonger l'attaque.**

 Limiter le nombre de connexions par jour et par compte, limiter à certaines tranches horaires pour certains jours.
-  **Dénis de service par demande de reset d'un compte toutes les cinq minutes.**

 Limiter le délai avant un nouveau reset de compte.
-  **Regarder un utilisateur taper le mot de passe**

 Ajouter une contrainte biométrique, permettant de garantir qu'il s'agit bien de la bonne personne qui saisit le mot de passe. Une analyse du rythme de la saisie peut être un critère discriminant.
-  **Découvrir les astuces mnémotechniques utilisées par les utilisateurs pour mémoriser les mots de passe.**

 Analyser la complexité des mots de passe avant de les accepter dans l'application. Cette analyse va au-delà des contraintes typographiques généralement imposées aux mots de passe.
-  **Découvrir des informations par analyse des messages d'erreur.**

 Un message générique doit être diffusé, quelles que soient les causes de l'erreur (compte inexistant, mot de passe erroné, compte bloqué, utilisation hors délais, etc.).
-  **Voler le cookie de session d'un utilisateur.**

 Associer à la session la version du navigateur utilisé et l'adresse IP source.
-  **Découvrir les attaques**

 Une fois que l'utilisateur est authentifié correctement, il est pertinent de lui communiquer :

  - le nombre d'échecs avant son authentification ; cela lui permet de découvrir une tentative de connexion ;
  - la date et l'heure de la connexion précédente ; Si cette information est inhabituelle, il peut prévenir l'administrateur ;
  - son obligation de changer rapidement de mot de passe (d'initialisation ou standard).

## Applications Web

☹ La technologie http, permet à l'internaute de **naviguer** comme il le souhaite sur un site. Il peut voyager de page en page en suivant des liens, mais il peut également aller directement à une page, sans suivre le cheminement prévu par le développeur.

Cela permet à des pirates, dans certaines situations, d'abuser des services du site. Par exemple, imaginez un site de commerce avec le processus suivant :

- Remplissage du panier,
- Ouverture du processus de commande,
- Demande des informations bancaires,
- Validation de la commande.

Si le site n'est pas protégé suffisamment, le pirate peut tenter de remplir le panier après la saisie des informations bancaires ou de sauter cette étape pour confirmer sa commande.

😊 Pour contrer cela, il faut suivre précisément le cheminement de l'utilisateur, et interdire toutes déviations.

☹ Naïvement, les développeurs pensent que **les valeurs données dans les différents champs de l'application** sont bonnes. Les pirates exploitent cela pour :

- Injecter du code SQL, permettant de consulter toute la base, de la modifier, voire de la détruire.
- Injecter du code LDAP, permettant de contourner les authentifications ou de voler des informations personnelles.
- Injecter du code HTML, permettant le vol du cookie de session d'un utilisateur.
- Injecter des valeurs hors limite, permettant l'exécution de code arbitraire par débordement de tampon, la modification des prix d'une commande, la modification des champs cachés,
- Injecter des paramètres entraînant des traitements excessivement gourmands en CPU (via des expressions régulières mal écrites, des requêtes à la base de données trop complexes, ...)

😊 Il faut vérifier précisément, et systématiquement, tous les paramètres manipulables. Cela concerne, bien entendu, les champs des formulaires, mais également les champs cachés, les valeurs des cookies, les en-têtes du navigateur, etc.

☹ **Injection de traitement dans les valeurs.**

😊 Les informations venant de l'utilisateur sont utilisées pour générer. Avant de les exploiter, il faut éventuellement les encoder pour respecter les contraintes d'intégration. Trop souvent, les développeurs

imaginent que les données sont saines, car elles ont été nettoyées au début du traitement. C'est possible, mais comme il existe tellement de possibilités d'utiliser une même donnée, il est probable que le nettoyage ne soit pas suffisant dans tous les cas. Sauf si l'application n'accepte que des valeurs alphanumériques, sans espaces, sans accents, sans caractères de ponctuations. Cela n'est concrètement pas possible. Les données utilisateur sont généralement exploitées pour générer des requêtes SQL, LDAP, pour des expressions régulières, des fichiers XML, XSL, produire des pages HTML, etc. Suivant les cas, il faut modifier les données pour éviter une mauvaise interprétation par ces différents autres langages. Certains caractères doivent être présentés avec un encodage particulier, des mots-clefs doivent être systématiquement supprimés, etc. Par exemple, pour injecter une donnée dans une page HTML, il existe six encodages différents, suivant la localisation de la donnée dans la page.

☹ **Condition de course.**

😊 Les applications WEB sont, par nature, multitâches. Les développeurs imaginent qu'un utilisateur particulier ne peut faire qu'une seule chose à la fois. L'application est alors écrite comme si elle était mono tâche. Un pirate peut exploiter cela pour demander simultanément plusieurs traitements, dont l'inconsistance permet de casser la base de données ou de contourner des protections. C'est ce que l'on appelle des " conditions de course " (race condition).

L'application doit garantir que l'exécution simultanée de plusieurs traitements pour un même compte n'aura pas d'impact sur la qualité des données manipulées. Il faut également qu'une seule transaction soit ouverte lors du calcul d'une page. Si l'application utilise plusieurs petites transactions, il y a un risque d'inconsistance des données.

☹ **Les erreurs peuvent révéler de nombreuses informations à l'utilisateur.**

😊 Il est important de qualifier précisément les erreurs pouvant être transmises à l'utilisateur de celles ne le pouvant pas. À défaut, il est préférable d'afficher un message générique que de transmettre la requête SQL ayant échoué.

# L'arsenal des protections

Il existe une multitude de solutions pour sécuriser son poste, ses applications, ses données, un réseau. Il y a même une hiérarchie des technologies, chacune correspondant à un besoin, à un critère de sécurité précis. Contrairement à d'autres outils, dans le domaine de la sécurité, n'espérez pas réaliser des économies. À vous de bien définir les besoins et les réponses à apporter. C'est avec ce problème d'audit que l'on ajuste au mieux son budget sécurité.

Aujourd'hui, comme vous le verrez ci-dessous, tout ou presque est susceptible d'être une faille de sécurité. Si on privilégie encore le poste de travail et le réseau, désormais c'est l'infrastructure même d'identification qui occupe le terrain pour le business, c'est la protection des données, la sécurisation des accès aux applications ou encore la protection des terminaux / applications mobiles et les sessions.

## Antivirus, firewall, DMZ

Le périmètre est votre barrière entourant votre réseau ou poste de travail. C'est là que vous devez arrêter les attaques. Une fois rentrées et installées, les attaques les plus malicieuses sont difficilement délogeables. C'est pour cela que vous devez tout d'abord mettre en place les outils de base : antivirus et firewall. Les systèmes embarquent au moins un firewall logiciel (qu'il faut activer par défaut). Le prochain Longhorn aura son propre antivirus en standard. À cela, s'ajoutent maintenant les antispams, les antispywares, les anti-intrusions, les scanners de ports, les filtres Web et de messageries. Selon que vous protégez un poste personnel, un poste de travail, un réseau entier, les outils changent de taille. Pour un réseau, vous pouvez à la fois installer sur le poste de travail et le serveur. Pour les plus exigeants ou les très gros parcs, optez plutôt pour des solutions "matériels" : les gateways (firewalls, filtres divers, etc.). L'avantage est de centraliser son administration. Vous pouvez aussi mettre en place des outils anti-intrusion, des filtres d'utilisation, etc. Dans certains cas, vous pouvez implémenter une DMZ permettant de séparer le réseau (" serveur public " et accessible à partir du Web) en contact avec le Web, du réseau privé. Bref, il faut agir dès le périmètre contre tous les malwares possibles.

Quelques éditeurs d'anti malware (uniquement logiciel) : Sophos, CA, Symantec, McAfee, Panda Software, F-Secure, Square, TrendMicro, Kaspersky, BitDefender, Sybari Software, Tegam.

## La biométrie

On parle de plus en plus souvent de biométrie. Il s'agit surtout d'une méthode d'authentification, via une partie du corps : rétine ou empreinte digitale (ou autre). La deuxième solution est la plus utilisée dans le monde informatique. Cependant, ce type de solution demeure encore onéreux, malgré les multiples annonces. La biométrie peut servir d'authentification dans des sessions, des transactions, pour l'accès à un terminal, à une application. Son usage est très large. Pour les applications et terminaux (PC et autres), les périphériques disponibles sont nombreux : souris, lecteur biométrique USB, PC Card, clavier. Comme dit plus haut, le prix est souvent un facteur négatif, surtout si on souhaite équiper un parc conséquent. Cependant, à vous de juger le risk



tent de capturer le " bio-paramètre ", de l'analyser et de le stocker. Lors de la procédure d'authentification, l'application procède à la comparaison entre l'empreinte " maître ", de l'empreinte fraîchement scannée. Selon les solutions, les SDK supportent C/C++, VB. L'autre souci de la biométrie est le support parfois limité des systèmes. Souvent, Windows est supporté, mais Linux et MacOS X, le sont plus rarement. La société Xelios propose, pour ses propres solutions, un SDK dédié aux applications Web. Pour Linux, on peut citer l'apparition en été 2004 du SDK Veridicom (support limité au sensor FPS 200 pour le moment). Cependant, pour certaines solutions packagées et limitées à un usage, comme la protection de données sur un clé USB, cela fonctionne aussi bien sur MacOS X que Windows (Ex. : clé de stockage USB avec Biometrie intégrée de Trek.



Des firewalls, antivirus matériels, ici le Gate Defender de Panda Software

management et le bénéfice qu'une telle solution peut vous apporter. Les constructeurs de solutions de biométrie proposent des SDK, afin d'implémenter au mieux la biométrie dans son application. Ainsi, la société Identix a divers SDK, selon le type de biométrie et de contrôle voulu. Pour l'empreinte, on prendra BioEngine Fingerprint SDK. Les SDK permet-

Bien entendu, la biométrie pour être efficace doit être couplée à d'autres technologies, notamment dans le cas d'une application de commerce électronique, avec la mise en place d'une infrastructure de confiance et des sessions sécurisées. La biométrie peut remplacer le mot de passe classique.

**Pour :** l'usage d'un biomètre est en principe



Trek biometrie : les clés USB biométrie

plus sécurisant, la fiabilité, idéal pour les accès aux applications, PC...

**Contre :** prix, difficilement généralisable, peu d'offres pour les terminaux mobiles (hors ordinateur portable et TabletPC).

**Quelques constructeurs, distributeurs :** Xelios, Zefyr, Zalix, Sagem, Identix, Actronix.

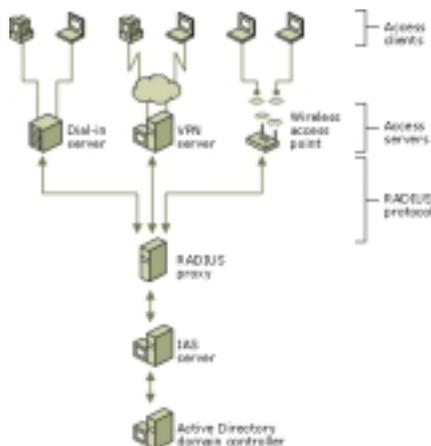
## Mobilités : prévention et protection à tous les niveaux !

La mobilité accrue des applications et des terminaux pose un réel souci de sécurité pour les données, les applications et le réseau. La sécurité, la protection d'un PocketPC ou d'un PDA en général se fait tout d'abord, comme sur PC, par l'antivirus. Des éditeurs comme F-Secure ou McAfee proposent ce type d'outils. Cependant, les risques viraux y sont très minces. Sur smartphone, très récemment, Nokia a annoncé un antivirus F-Secure dans son nouveau modèle, le 6670. Ce dernier n'est, cependant, pas installé par défaut. Il faudra le télécharger.

Le cryptage de données est sans doute le meilleur choix sur des terminaux de type PDA. Utilisez mot de passe et outils de cryptages (ex. FileCrypto de F-Secure). L'usage de cryptage est une contrainte, mais cela permet de limiter les conséquences d'une perte ou du vol de son PDA. Pour les applications mobiles, le développeur devra utiliser des bibliothèques dédiées, afin de stocker les données sensibles sous forme cryptée. Pour toute session distante avec un service, on pourra mettre en place du VPN, une session sécurisée avec https et SSL. Cela est indispensable quand on fait de la synchronisation et/ou réplique de données entre l'application serveur et l'application mobile. Dans tous les cas, le terminal (et l'application) mobile doit être intégré dans la politique de sécurité de l'entreprise. Le couple VPN - SSL (à la place d'IPSec) est une solution de plus en plus utilisée pour les sessions mobiles.

Côté Wifi, la sécurité s'améliore enfin avec l'arrivée du WPA 2. Cette nouvelle norme Wifi s'appuie sur la norme 802.11i et implémente AES (advanced encryption standard) à la place du TKIP. Si l'implémentation du 802.11i était attendue, le revers de la médaille est une incompatibilité de nombreux matériels (WPA 2 nécessite une puce de cryptographie dédiée). Cependant, WPA 2 est compatible avec le WPA 1, donc inutile de tout remplacer d'un coup même si la sécurité devient bancal.

Pour une gestion centralisation des authentifications des utilisateurs (avec autorisation d'accès aux ressources), qu'ils soient nomades ou



Une architecture de sécurité globale selon Check Point

non, vous pouvez mettre en place une architecture utilisant du serveur RADIUS (Remote Authentication Dial-In User Server). RADIUS est un protocole ouvert. Dans le cadre d'un réseau Wifi, le RADIUS peut améliorer la sécurité et éviter l'intrusion d'un vrai faux utilisateur.

## Authentification forte

Tout ce qui est sécurité de l'identité, ou plutôt l'identification de l'utilisateur, devient une pièce maîtresse des applications business ou critiques (ex. : banque, finance, accès aux applications / données, etc.). L'authentification forte fournit un niveau élevé d'identification. Bref, l'authentification forte remplace le mot de passe statique, via un accès à génération dynamique logicielle ou matérielle, par diverses technologies : token, biométrie, carte à puce, etc. L'authentification forte fournit uniquement le mot de passe généré à la volée, qui complète l'identification d'un utilisateur. Il s'agit d'une technologie très en vogue actuel-

lement. L'offre sur ce domaine est assez vaste. Par exemple, RSA Security propose depuis longtemps de telles solutions (SecureID). Cela peut servir au niveau du poste (accès) ou sur des applications ou données (dans le cadre de RSA Security il s'agira des RSA Agents). Au-delà de cela, l'infrastructure de confiance (avec par exemple un PKI) s'avérera indispensable pour le eBusiness. Le monde bancaire met en place un couplage fort entre infrastructure de confiance et authentification forte. Le but est de mieux identifier l'utilisateur et éviter le vol de données et d'argent sur les comptes bancaires !

## Protéger vos applications

Aujourd'hui, le dongle est revenu à la mode pour certaines applications et entreprises. Que la clé soit parallèle ou USB, son implémentation dans une application ne pose guère de problème. Le constructeur fournissant les API nécessaires. Ainsi, l'offre Sentinel de SafeNet fonctionne sur Windows, MacOS et Linux. Il est possible de les implémenter avec les langages courants du marché. Les clés Sentinel incluent un cryptage AES de 128 bits. Un kit de développement est disponible. Deux grandes méthodes sont utilisées : encapsulation d'un .exe ou d'une DLL. Son avantage est la rapidité d'implémentation. La seconde solution consiste à implémenter dans le code source. L'application dialoguera alors avec la clé, selon les fonctions demandées. Cette solution peut être utilisée par les éditeurs de logiciels, les entreprises, le développeur indépendant.

SafeNet n'est pas le seul constructeur à proposer ce genre de technologies. Aladdin propose aussi ce type de possibilités, via la gamme HASP. Cette gamme, comme pour SafeNet, permet une protection matérielle ou logicielle. Plusieurs niveaux de clés USB sont disponibles, notamment sur la mémoire disponible. On dispose d'un cryptage 128 bits AES, une API de développement, le support de Windows Update. Fonctionne sous Windows, MacOS X ou Linux. Et est compatible avec de multiples langages utilisables pour l'implémentation.

Si une telle solution fonctionne bien, attention tout de même au coût. Il faudra bien choisir le type de licence à mettre en œuvre.

■ François Tonic



# La sécurité doit apporter du service !

Faire prendre conscience que la sécurité est aussi une question de productivité, d'ergonomie et de services aux utilisateurs. Voilà les préoccupations de Pierre Herbelot, directeur EMEA Identify Management Solutions de SafeNet, fabricant de la clé de protection Sentinel et de logiciels de sécurité et de cryptage.



**Programmez ! : Quelles sont les nouvelles menaces que l'on rencontre au quotidien ?**

**Pierre Herbelot :** L'usurpation d'identité demeure la première

menace, récemment des banques en ont subi. Les attaques de type Denied of Service existent toujours, ainsi que le spam pour les mails. Le phishing n'est qu'une variante d'usurpation. Il s'agit en réalité d'une double attaque. On fait croire à un utilisateur qu'il reçoit un message de confiance. La seconde attaque consiste à usurper l'identité de cet utilisateur et de récupérer des données confidentielles afin de tromper un organisme bancaire (ou autre). Il s'agit d'un type d'attaque ciblée et marginale, mais cela va sans aucun doute prendre de plus en plus d'importance, car les mesures de sécurité nécessaires ne sont pas prises. Le phishing, c'est (aussi) la faute aux organismes et entreprises qui ne mettent pas en place les structures nécessaires. On tombe ici dans le risk management.

**PH :** Comment éviter le phishing ?

Il faut mettre une infrastructure de confiance, comme un PKI. C'est simple et parfois gratuit. Cela ne suffit pas. On demeure avec une identité logicielle, du niveau d'un login. Il faut ajouter une authentification forte, avec un support physique.

**PH :** Faut-il faire de la veille ?

Si on ne fait pas de veille, on regarde le navire couler. Cependant, il faut un passage à l'acte après la veille. Il faut mettre en place de

la prévention en premier puis surveiller ce qui se passe. Si on ne fait rien, on peut perdre beaucoup !

**PH :** La sécurité passe aussi par le développeur, afin de bétonner le code et l'application. Faut-il centrer la sécurité sur le développeur ?

Tout d'abord, il faut que l'entreprise soit sensibilisée au problème de sécurité. Le développeur développe pour les utilisateurs. Si l'entreprise ne prend pas en compte la sécurité, le développeur ne le fera sûrement pas. Il faut un plan d'action, avec des applications sécurisées.



**PH :** Avec les terminaux mobiles, les applications et les données deviennent mobiles. Le problème de sécurité est-il identique ?

Le problème est le même que sur le desktop. Avec le PDA, il y a le problème du vol, il s'oublie plus facilement qu'un PC ! Nous avons des systèmes pour PDA mais la demande est très faible. Actuellement, bien souvent, sur le desktop, on reste encore avec du mot de passe, alors la sécurité sur PDA, cela pourra prendre plusieurs années. Sur le téléphone le

problème est encore autre. Là, le coût est important et la sécurité renchérit ce coût.

**PH :** La biométrie est souvent mise en avant. Mais finalement, est-ce une solution miracle et faut-il y croire ?

La biométrie peut remplacer le code PIM mais il faut lui associer une technologie. Il faut aussi penser à l'ergonomie. On avait réfléchi à un concept mélangeant de la biométrie et un token USB, mais là aussi, le problème est le prix. Je pense qu'il y a pas mal d'effets d'annonces dans ce domaine. Je n'ai pas encore vu de déploiement d'envergure de ce genre de solution sur PC et sur réseaux.

**PH :** Quand on pense sécurité, on pense immédiatement aux coûts. Faut-il encore raisonner ainsi ?

Aujourd'hui, on peut apporter du service autour de la sécurité, par exemple avec les clés USB contenant des applications. On essaie de le présenter ainsi. Cela commence à être bien compris. De plus, l'ergonomie est aussi un point important pour l'utilisateur en lui facilitant l'accès. On ne pense jamais à l'utilisateur, mais uniquement au niveau technique ! Pourtant, l'utilisateur a une demande simple. Il s'agit d'offrir du service pour améliorer l'accès et la productivité. Il faut ne pas oublier les coûts cachés, par exemple, un utilisateur, à son arrivée le matin, oublie son mot de passe et doit contacter le responsable... Prenez le mot de passe statique. Il a aussi un coût. Imaginez que l'on ait à gérer 1 000 postes avec 9 applications dont les mots de passe changent tous les mois !

■ F.T.



des mises à jour des éditeurs.

Les risques liés au navigateur Web découlent des techniques suivantes :

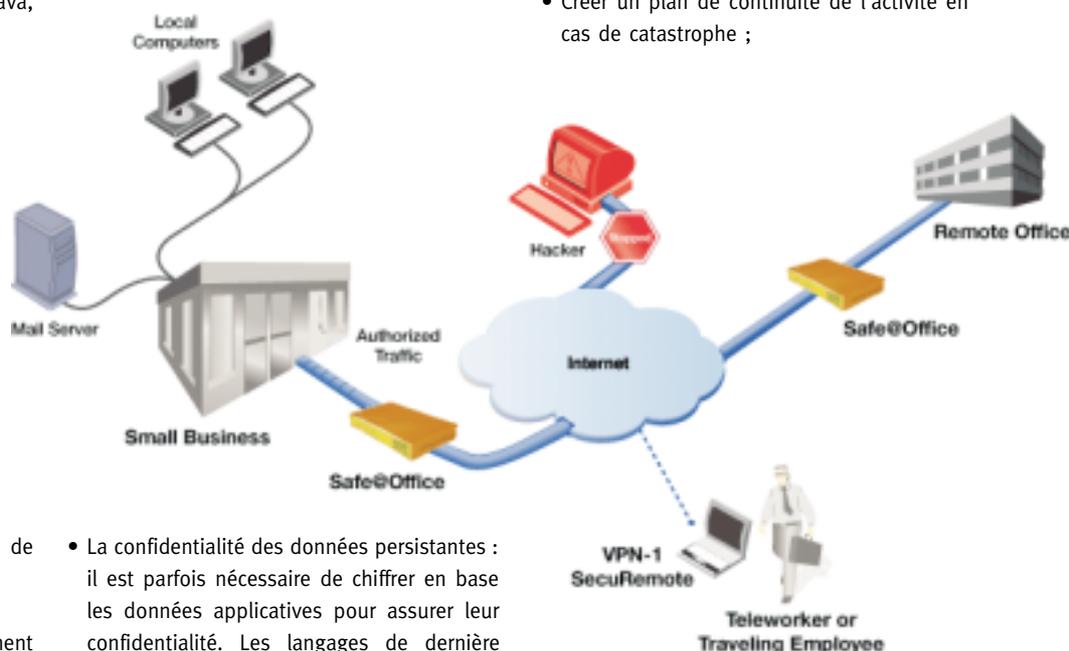
- Les cookies : ils permettent de tracer le comportement des utilisateurs.
- Les scripts Java Script : ils permettent de prendre le contrôle de certaines fonctions du navigateur.
- Les composants " managés " (Applets Java, .NET WinForms) : ces programmes interactifs sont exécutés sur des machines virtuelles (Java ou .NET). ils présentent un risque faible, car ils sont isolés du système d'exploitation par des barrières ad hoc.
- Les " plug-ins " (Flash, Shockwave, etc.) : ces programmes interactifs sont exécutés directement par le système d'exploitation. ils présentent donc un risque fort, exploitable par des " hackers ".
- Le navigateur lui-même : ses éventuels bugs présentent un risque fort et sont largement exploités par les " hackers ". Il doit donc faire l'objet de mises à jour régulières par les équipes de maintenance informatique.

Les problématiques de sécurité qui concernent les développeurs d'applications Web sont les suivantes :

- Le contrôle des paramètres HTTP : il est indispensable de bien contrôler les paramètres transmis au serveur dans les requêtes http, afin de se prémunir contre les buffers overflows (saturation du serveur par envoi massif de données), les injections de commandes (envoi de commande SQL ou commande système au travers des paramètres HTTP) et le cross-site scripting (utilisation de Java Script pour déclencher la transmission d'informations confidentielles par le serveur).
- La gestion des erreurs : les erreurs applicatives (exemple : mauvais typage des données) peuvent être utilisées pour faire dysfonctionner le serveur.
- L'authentification et les habilitations des utilisateurs : il convient d'utiliser un bon niveau d'authentification avant de donner aux utilisateurs accès à l'application. Ces authentifications peuvent utiliser des mots de passe simples, des certificats numériques, des annuaires LDAP, etc. Les langages de dernière génération proposent des

composants d'authentification packagés de très bon niveau.

- La confidentialité des échanges : il est souvent nécessaire de chiffrer les échanges HTTP pour assurer leur confidentialité, tout particulièrement lors d'échanges de mots de passe. Les protocoles SSL et IPSEC peuvent assurer cette confidentialité.



- La confidentialité des données persistantes : il est parfois nécessaire de chiffrer en base les données applicatives pour assurer leur confidentialité. Les langages de dernière génération proposent des composants cryptographiques pour assurer ce chiffrement.

Il est essentiel, pour le développeur, d'utiliser les mécanismes standard proposés par les environnements technologiques (J2EE et .NET), plutôt que de développer des systèmes spécifiques de sécurité qui seront nécessairement moins sécurisés.

## Conclusion

Au-delà de la sécurité des infrastructures et des applications Web, il est aujourd'hui recommandé d'organiser la sécurité de manière globale. Les entreprises qui suivent cette approche disposent d'un département sécurité dirigé par le RSSI, Responsable de la Sécurité du Système d'Information. Ce RSSI est en charge de créer la " politique de sécurité " du SI et de veiller à son application.

Pour créer cette politique de sécurité, le RSSI peut s'appuyer sur des normes comme MEHARI, MARION ou ISO 17799, etc. Ces normes proposent des méthodologies pour :

- Définir ce qu'il faut protéger ;
- Sensibiliser l'ensemble des acteurs de l'entreprise ;

- Évaluer les investissements à consentir ;
- Étudier les différentes solutions de sécurité ;
- Assurer la mise en place des solutions retenues ;
- Auditer régulièrement le système d'information ;
- Assurer une veille technologique et réglementaire active ;
- Créer un plan de continuité de l'activité en cas de catastrophe ;

Un des rôles du RSSI est de sensibiliser les populations de l'entreprise aux normes de sécurité. Il s'attachera en particulier à suivre les équipes de développement afin que ces dernières prennent en compte la politique de sécurité tout au long des phases de projets. Il peut d'appuyer pour cela sur un référent sécurité pour chaque projet, que nous appellerons " Responsable Assurance Sécurité " par analogie avec le Responsable Assurance Qualité.

■ **Guillaume Plouin**  
Conseil  
technologique SQLI

Co-auteur de  
**"Sécurité  
des architectures  
Web"**,  
ouvrage paru  
chez Dunod



# L'open source offre-t-il une meilleure sécurité ?

**La sécurité informatique est devenue un sujet clé des entreprises du 21<sup>e</sup> siècle. La délinquance électronique est en perpétuelle évolution ces derniers mois. D'après l'éditeur SYMANTEC, spécialisé dans les logiciels antivirus, le nombre de nouveaux virus et de vers destinés au système d'exploitation Windows a augmenté de 400 % entre janvier et juin, par rapport à la même période de 2003. Selon l'éditeur NORTON, environ 5000 nouveaux virus et vers ont été répertoriés au premier semestre 2004, contre seulement 1000 au premier semestre 2003.**

**L**es systèmes d'exploitation open source de type LINUX sont-ils à l'abri de ces funestes statistiques ? Oui et non.

Tout d'abord, il est clair que Windows représentant plus de 90 % du marché des systèmes d'exploitation, les délinquants en attente de publicité, voire de gloire, sont plus tentés de s'attaquer au plus grand nombre. De plus, Microsoft et les éditeurs propriétaires en général ont depuis longtemps, jalousement gardé les secrets du code source de leurs produits. Pour des raisons psychologiques évidentes, les pirates sont là aussi, tentés de s'attaquer à ces produits fermés, car violer leurs secrets relève du défi personnel et de la victoire de David face à Goliath.

Il n'est cependant pas objectif de dire que l'approche open source et l'adoption de systèmes comme LINUX sont les vaccins absolus. Les premiers vers informatiques sont apparus sur des architectures UNIX, bien avant l'avènement de Windows et une explication à l'absence quasi totale de virus pour les systèmes open source est aussi la relative faible diffusion de ceux-ci, surtout auprès d'utilisateurs peu avertis donc peu méfiants.

Techniquement parlant, LINUX et l'architecture UNIX en général sont cependant mieux armés contre les attaques virales, car depuis toujours, les utilisateurs sont classés en catégories, chaque utilisateur ayant alors des droits d'accès limités. De même, la multiplicité des distributions LINUX, des modes d'installation et des applications utilisées limite la stricte compatibilité binaire nécessaire à la propagation du virus. Un grand nombre de virus et vers sous Windows profite du fait que la quasi-totalité des clients finaux utilise les applications de l'éditeur (IE comme navigateur,

Outlook comme client de courrier électronique, Office pour la rédaction des documents). Une attaque à travers une de ces applications est donc systématiquement vouée à un " succès " planétaire. Un utilisateur Windows faisant le choix de composants open source, tout en restant dans l'environnement Windows (Mozilla, Firefox, Thunderbird, Open Office, etc.) donnera déjà du fil à retordre aux pirates.

Bien entendu, la disponibilité du code source, parfois rendue obligatoire dans le cas de certaines licences, comme la GPL (General Public Licence, une des plus répandues dans le monde open source) facilite la détection des failles de sécurité, car le nombre de bêta-testeurs et de contributeurs à l'amélioration des sources n'est plus limité à l'éditeur lui-même. Au siècle de l'Internet rapide, une correction de faille sérieuse est donc très rapidement disponible.

De plus, l'identification d'un composant open source est beaucoup plus précise que celle d'un composant classique : les auteurs sont clairement nommés, et leur style de programmation est appréciable pour tout œil averti. Aucun développeur open source ne se risquerait à intégrer une portion de code suspect,

sous peine de perdre sa légitimité auprès de la communauté. Plus concrètement, la distribution de composants open source officiels est systématiquement accompagnée d'une clé, permettant de valider l'identification de la provenance du paquetage (le plus souvent la clé PGP de l'auteur du paquetage).

Pour revenir au côté psychologique, il est beaucoup moins excitant pour le pirate de violer des secrets qui n'en sont pas – puisque rien n'est secret dans l'open source - et de par le mode de distribution décrit précédemment, il y a peu de chances que le délinquant arrive à ses fins.

Il convient cependant de rester prudent, car il n'existe pas de solution miracle et outre l'adoption de composants plus ouverts, la maîtrise des outils et le bon sens sont des conditions également nécessaires.

■ **Pierre FICHEUX**

*pierre.ficheux@openwide.fr*  
 Directeur Technique Open Wide  
 (<http://www.openwide.fr>)



## Bibliographie :

- Article " Linux est épargné par le virus I LOVE YOU, pourquoi ? " sur <http://www.aful.org/presse/pr-virus.html>
- Statistiques sur l'évolution des virus Windows sur <http://2607.blogs.com>
- Portail sur l'open source sur <http://www.opensource.org>
- CERT coordination center sur <http://www.cert.org>
- Portail sécurité LINUX sur <http://www.linuxsecurity.com>
- Projet Mozilla (Thunderbird, Firefox) sur <http://www.mozilla.org>
- Projet Open Office sur <http://www.openoffice.org>
- Portail sécurité en français <http://www.securite.org>

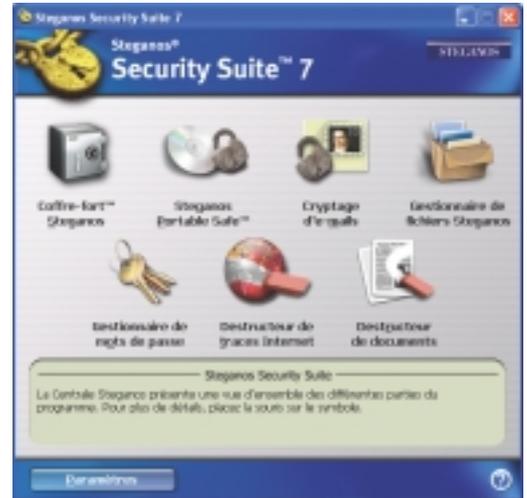
# Gardez votre précieux code à l'abri des regards

CRYPTAGE

**Steganos Security Suite et DriveCrypt de SecurStar sont des logiciels de cryptage, efficaces et simples d'emploi. Ils sont indispensables au chef de projet qui tient à garder son code source à l'abri de toute attaque**

Le code source est précieux et il court de nombreux dangers. Le plus grave est de tomber entre de mauvaises mains. On pense bien sûr à la concurrence, mais il peut aussi exister en interne des personnes malveillantes. La seule solution c'est de crypter les données. Il faut toutefois se méfier des logiciels téléchargeables gratuitement sur le Web. Beaucoup d'entre eux sont basés sur les algorithmes élémentaires, comme le " ou exclusif " qui n'offrent aucune protection. D'autres ne publient pas les algorithmes utilisés. Il est par conséquent impossible de savoir s'ils sont sérieux et surtout, s'ils ne contiennent pas une " porte

Steganos Security Suite 7 et DriveCrypt 4.2 de SecurStar. Tous deux tournent sous Windows et permettent de créer des fichiers cryptés qui se transforment en disques logiques lorsqu'ils sont ouverts avec le mot de passe correspondant. Ces disques apparaissent dans tous les logiciels comme des partitions logiques, sur lesquelles il est possible de transférer des fichiers comme avec une partition standard. Lors de ces transferts, les données sont cryptées/décryptées à la volée, d'une manière transparente pour l'utilisateur. Lorsque le travail est terminé, il suffit de démonter les lecteurs, pour que les données qu'ils contiennent deviennent inaccessibles. En cas de crash de l'ordinateur, les lecteurs se ferment automatiquement sans perte de données. Steganos Security Suite 7 est plutôt orienté grand public. Il ne coûte que 40 € et contient toute une suite logicielle. En premier, un destructeur de documents. Chacun sait que l'effacement d'un fichier ne le détruit pas, mais efface seulement quelques octets dans la table d'allocation. Viennent ensuite, un destructeur de traces Internet, un gestionnaire de mots de passe, un gestionnaire de fichiers, un module de cryptage des e-mails, et enfin les deux modules Portable Safe et le Coffre-fort. Le premier permet de transporter des données cryptées sur des supports amovibles tels que des CD, des DVD ou même des clés USB. Ces supports peuvent ensuite être distribués facilement, car ils contiennent également le logiciel de déchiffrement. Le module de cryptage enfin est le Coffre-fort. Basé sur l'algorithme AES 128



Steganos Security Suite 7 comprend de nombreux outils destinés à assurer la sécurité du poste de travail.



DriveCrypt 4.2 offre un grand choix d'algorithmes de chiffement aux utilisateurs.

dérobée " permettant de casser facilement la clé. Il faut ensuite bien choisir son algorithme de chiffement. Pour une protection réellement efficace, il est préférable de se tourner vers l'AES ou d'autres algorithmes considérés comme sûrs, tels que FEAL, REDOC, LOKI, RC2, IDEA, GOST, RC5 ou encore BlowFish.

## Créer des disques cryptés

Nous avons sélectionné deux produits qui nous semblent bien sécurisés. Il s'agit de

Clé de chiffement	Sécurité offerte
toto	Ce mot de passe n'offre aucune protection
jean K	Ce mot de passe peut être deviné
alain 0354	Ce mot de passe peut être déchiffré à l'aide d'un logiciel spécifique
M28kypl-wW	Ce mot de passe ne peut pas être déchiffré à l'aide d'ordinateur mis en réseau
M28kypl-wW*9H?mX<	Ce mot de passe ne peut pas être déchiffré à l'aide de nombreux ordinateurs mis en réseau
M28kypl-wW*9H?mX<4tvN	Ce mot de passe ne peut pas être déchiffré par les services secrets

La sécurité des données dépend de la qualité des mots de passe choisis

bits, il permet de créer jusqu'à 4 disques d'une capacité maximale de 64 Go. Son point fort est d'indiquer à l'utilisateur la qualité de son mot de passe, au fur et à mesure qu'il le saisit.

## Un produit adapté aux équipes

DriveCrypt 4.2 coûte 60 \$ et ne comprend que la fonction de cryptage de disque, ainsi qu'un module de stéganographie qui ne fonctionne qu'avec des fichiers musicaux. Il autorise le cryptage de partitions entières, dont la taille n'est limitée que par le système de fichiers utilisé, mais son point fort est la possibilité de placer deux mots de passe sur un même disque. Chaque développeur pourra, par exemple, avoir son propre mot de passe sur son disque, mais le chef de projet possèdera un mot de passe maître, permettant d'ouvrir tous les disques. Ce responsable pourra également restreindre l'ouverture des disques à certaines plages horaires. Ainsi, si un développeur est absent, ou a quitté l'équipe, il sera toujours possible au chef de projet de récupérer les données de son disque crypté. DriveCrypt permet enfin de cacher des données dans un disque, en donnant deux mots de passe. Le premier l'ouvre sur des données banales et le second sur les données confidentielles. Cette fonction est censée protéger l'utilisateur contre les agressions, mais elle semble un peu gadget, car connue de tous.

■ Alain COUPEL

# Cryptographie : l'exemple .NET

Aujourd'hui, les principaux langages proposent des API, classes, bibliothèques de cryptologies. Microsoft a fait un gros effort sur la sécurité à l'intérieur de .NET (pour tout ce qui concerne le code managé). Dans le framework 1.1, on dispose du namespace System.Security.Cryptography. Il fournit les services cryptographiques nécessaires (codage, décodage, hachage, génération aléatoire de nombre, authentification de messages...). Pour la partie non managée, on passera par CryptoAPI (des wrappers sont présents dans le namespace de cryptographie). Mais là attention, on sort d'un cadre strictement contrôlé par l'environnement .NET, on est donc susceptible d'être moins "secure".

Une nouvelle instance d'une classe d'algorithme de cryptage génère automatiquement les clés nécessaires. Par défaut, .NET fournit plusieurs algorithmes de cryptographie. Le modèle cryptographique du framework se caractérise par trois éléments :

- héritage d'objet : classe de type d'algorithme (niveau abstrait), la classe d'algorithme hérite de la précédente (niveau abstrait), implémentation d'une classe algorithme (hérite d'une classe d'algorithme, niveau implémenté).
  - Design de flux : utilisé par le CLR pour implémenter les algorithmes symétriques et de hachage. Le core design est la classe CryptaStream (dérivant de la classe Stream). On bénéficie d'une seule interface.
  - Configuration cryptographique : permet d'ajouter sa propre implémentation logicielle/matérielle d'un algorithme.
- Le framework étant extensible, on peut alors créer ses propres classes et implémenter des algorithmes non présents. Par exemple, pour le hachage, il est possible de faire un hachage MD5. Bien entendu, pour une bonne crypto-

graphie, il faut utiliser les signatures, afin de vérifier et d'authentifier les données et l'utilisateur, voici les étapes :

- génération de signatures : nouvelle instance de RSACryptoServiceProvider pour générer des clés publiques et privées. La clé privée va à RSAPKCS1SignatureFormatter, classe effectuant la signature numérique. Dans le cas d'un hachage, on spécifie l'algorithme de hachage à utiliser (ex. SHA1). On appelle la méthode RSAPKCS1SignatureFormatter.CreateSignature pour signer.
- Vérification de signatures : si on veut vérifier qu'une application / utilisateur spécifique ait signé des données, on doit d'abord posséder la clé publique qui a servi à signer, la signature numérique, les données signées et l'algorithme de hachage utilisé par la partie ayant été signée. La vérification de la signature appliquée par RSAPKCS1SignatureFormatter se réalise par RSAPKCS1SignatureDeformatter. Cette classe est fournie par la clé publique de la partie ayant signé. Ensuite, on crée un objet RSACryptoServiceProvider (stockage de la clé publique). On initialise ensuite une structure RSAParameters avec les valeurs citées ci-dessus. On initialise une nouvelle instance de RSACryptoService Provider (avec les valeurs du RSAParameters).

Très brièvement, abordons le cas ASP.NET. Une application ASP.NET embarque un fichier web.config, contenant des données appSettings. Ce sont donc des informations sensibles et facilement piratables. Pour éviter cela, il faut les crypter. Pour en savoir plus, un exemple complet et très concret : <http://www.bewise.fr/download/articles/CodeArticle19.zip>.

Exemple code C# d'un hachage SHA1 (exemple Microsoft – MSDN)

```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;

class Class1
{
    static void Main(string[] args)
    {
        byte[] HashValue;

        string MessageString = "This is the original message!";

        // création une nouvelle instance de la
        // classe UnicodeEncoding pour
        // convertir le string dans les bytes Unicode
        UnicodeEncoding UE = new UnicodeEncoding();

        //// Conversion du string
        byte[] MessageBytes = UE.GetBytes(MessageString);

        // Création d'une nouvelle instance de la
        // classe SHA1Manager pour créer la valeur du
        // hash
        SHA1Managed SHhash = new SHA1Managed();

        // Création de la valeur hash
        HashValue = SHhash.ComputeHash(MessageBytes);

        // Affichage de la valeur dans la console
        foreach(byte b in HashValue)
        {
            Console.Write("{0} ", b);
        }
    }
}
```

■ F.T.

# Conservez vos secrets avec .NET

N'importe quel programmeur est, un jour ou l'autre, confronté au besoin de stocker un mot de passe. Le framework .NET peut lui venir en aide.

## Vision globale des possibilités du framework

Commençons par dresser un résumé des espaces de noms dédiés à la sécurité : [System.Security.Cryptography](#)

Fournit des services cryptographiques ainsi que l'authentification de messages et la génération de nombres aléatoires (le générateur de nombre pseudo aléatoire `System.Security.Cryptography.RNGCryptoServiceProvider` est bien plus fiable que `System.Random`).

[System.Security.Cryptography.X509Certificates](#)

Implémente un certificat Authenticode X.509 v.3. Celui-ci est signé avec une clé privée permettant d'identifier de manière unique son détenteur.

[System.Security.Cryptography.Xml](#)

Fournit le service de signature numérique d'objets XML.

[System.Security.Permissions](#)

Définit des classes contrôlant l'accès aux opérations et aux ressources en fonction de la stratégie implémentée.

[System.Security.Policy](#)

Définit des règles qui seront appliquées par le système de stratégie de sécurité en fonction des groupes de codes, des conditions d'appartenance et des preuves.

[System.Security.Principal](#)

Définit un objet Principal qui représente le contexte de sécurité dans lequel le code sera exécuté.

## Trois familles d'algorithmes

Comme on le voit, un namespace complet est dédié au chiffrement dans .NET : `System.Security.Cryptography`. Trois grands types de classes sont ici implémentées : les algorithmes de hachages, les algorithmes symétriques et les asymétriques. Un système à clé symétrique utilise une clé secrète pour chiffrer et déchiffrer un seul message secret (DES, triple DES, RC2, Rijndael), tandis qu'un système à clés asymétriques emploie une clé privée et une clé publique (RSA et DSA).

Dans ces systèmes asymétriques, la première opération consiste en un chiffrement et une génération de signature avec la clé privée de l'émetteur. Le second traitement a pour but de déchiffrer et de vérifier la signature par le récepteur avec la clé publique. Les systèmes asymétriques sont plus lents, mais offrent une gestion des clés simplifiée.

## Le hachage en pratique

Le hachage est un traitement cryptographique non réversible (MD5, SHA1, etc.). Vous pouvez crypter une donnée, mais non effectuer l'opération inverse, c'est-à-dire qu'à partir de la donnée cryptée vous ne pouvez pas retrouver la donnée originale. C'est évidemment idéal pour crypter des mots de passe afin de stocker leurs signatures. Lorsqu'un utilisateur voudra s'identifier, il suffira de vérifier que le résultat du hachage est identique à la signature stockée.

À l'aide de cette technique, une seule modification de la chaîne du mot de passe produira un résultat de hachage différent.

```
using System;
using System.Security.Cryptography;
namespace MD5
```

```
{
    class Class1
    {
        public static string MD5(string Text)
        {
            byte[] tampon = System.Text.Encoding.UTF8.GetBytes(Text);
            try
            {
                MD5CryptoServiceProvider check;
                check = new MD5CryptoServiceProvider();
                byte[] somme = check.ComputeHash (tampon);
                check.Clear();
                string ret = "";
                foreach (byte a in somme)
                {
                    if (a<16)
                        ret += "0" + a.ToString ("X");
                    else
                        ret += a.ToString ("X");
                }
                return ret ;
            }
            catch
            {
                throw;
            }
        }

        static void Main(string[] args)
        {
            string chaine1 = "somme de contrôle";
            string chaine2 = "somme de controle";
            string chaine3 = "Somme de controle";

            string Ctrl_1;
            Ctrl_1 = MD5(chaine1);
            string Ctrl_2;
            Ctrl_2 = MD5(chaine2);
            string Ctrl_3;
            Ctrl_3 = MD5(chaine3);

            Console.WriteLine("La somme MD5 de " + chaine1 + " = " + Ctrl_1);
            Console.WriteLine("La somme MD5 de " + chaine2 + " = " + Ctrl_2);
            Console.WriteLine("La somme MD5 de " + chaine3 + " = " + Ctrl_3);

            Console.ReadLine();
        }
    }
}
```

```
// Ce qui donne :
// La somme MD5 de 'somme de contrôle' = CECBDC21042391CAB
C402F208BFA9998
// La somme MD5 de 'somme de controle' = 4C0E5F87C5C9A45E649
133919063684C
// La somme MD5 de 'Somme de controle' = 3B278D3FB13A2B62C5
6F85D112C6AA25
```

Nous créons d'abord un tableau d'octets (byte[]) contenant la chaîne d'origine qui sera hachée. Ce tableau (tampon) sera garni en utilisant la méthode : System.Text.Encoding.UTF8.GetBytes(). Nous avons sélectionné le fournisseur de service MD5CryptoServiceProvider et calculons le hachage à partir de cette chaîne, à l'aide de la méthode ComputeHash() de ce fournisseur. Cette méthode renvoie un tableau d'octets de la chaîne au format crypté. Attention, à ce stade il y a un choix à effectuer : vous pouvez retenir cette chaîne cryptée, via une ligne du style ret = Convert.ToBase64 String(somme) ; cette méthode convertissant le tableau d'octets en une chaîne codée en base 64. Ou bien vous pouvez rentrer dans une itérative ayant pour but de transformer chaque octet en son équivalent hexadécimal sur deux positions. Vous devez employer l'une ou l'autre de ces techniques, car sinon, certains caractères ASCII risquent de ne pas s'afficher. Il est très simple de changer d'algorithme :

```
SHA1CryptoServiceProvider check;
check = new SHA1CryptoServiceProvider();
```

La différence d'un algorithme à l'autre est la taille de la clé servant à hacher. L'algorithme SHA1 utilise une clé de cryptage de 160 bits, tandis que MD5 emploie une clé de 128 bits. SHA1 est par conséquent plus robuste, car il présentera moins de collisions, c'est-à-dire moins de risque de produire deux résultats de hachage identiques. D'ailleurs, pour écarter tout risque de ce type vous pouvez programmer du 'sel'. Ce sel consiste à ajouter une valeur unique à la chaîne avant de la hacher. Cette valeur unique sera par exemple un nombre aléatoire, qu'il faudra évidemment aussi stocker. Il existe d'autres algorithmes à notre disposition : vous pouvez choisir MD5CryptoServiceProvider(), SHA1CryptoServiceProvider(), SHA256Managed(), SHA384Managed(), SHA512Managed() et enfin MD5CryptoServiceProvider(). Comme il est recommandé par Microsoft nous effaçons la variable de hachage par un appel à la méthode Clear, une fois que celle-ci a rempli son rôle.

### Le chiffrement en pratique

Plusieurs algorithmes de cryptage/décryptage sont disponibles avec .NET Framework et comme dans le cas des algorithmes de hachage, il est d'abord nécessaire d'effectuer un choix (DES, RC2, Rijndael ou TripleDES).

```
DESCryptoServiceProvider encode = new DESCryptoServiceProvider();
```

Vous devez ensuite générer un vecteur d'initialisation (IV) qui permettra de démarrer le cryptage du premier bloc. Sans celui-ci, les données communes d'une chaîne à l'autre hériteront d'un modèle identique pour la même clé... Ce vecteur IV est employé comme variable aléatoire pour crypter les données (évitant ainsi que deux textes ne génèrent les mêmes données cryptées).

```
encode.IV = ASCIIEncoding.ASCII.GetBytes("A1C2D3E4");
encode.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEXYZ");
```

La clé doit rester secrète, sinon n'importe qui pourra décrypter le messa-

ge et le lire. Il est par conséquent préférable de la demander à l'utilisateur plutôt que de l'encoder en dur (mais vous pouvez toujours la hacher). Nous allons créer un flux crStream vers lequel nous enverrons les octets cryptés. Nous avons indiqué une constante énumérée, décrivant le mode dans lequel nous voulons créer cette classe (write pour écriture).

```
CryptoStream crStream = new CryptoStream(stream, encode.CreateEncryptor(),CryptoStreamMode.Write);
```

Une fois que l'objet CryptoStream, crStream, est créé, vous pouvez écrire les données dans le flux fichier (ou mémoire selon l'utilisation) en appelant la méthode Write de l'objet CryptoStream. C'est elle qui exécute le cryptage en envoyant au fur et à mesure chaque bloc de données.

```
byte[] données = ASCIIEncoding.ASCII.GetBytes("Ce message est secret.");
crStream.Write(données,0,données.Length);
```

Voici le code récapitulatif de cryptage :

```
using System;
using System.IO;
using System.Text;
using System.Security.Cryptography;

namespace CryptoStream_Encrypte
{
    class Class1
    {
        static void Main(string[] args)
        {
            FileStream stream = new FileStream("C:\\test.txt", FileMode.
OpenOrCreate,FileAccess.Write);

            DESCryptoServiceProvider encode = new DESCryptoService
Provider();

            encode.IV = ASCIIEncoding.ASCII.GetBytes("A1C2D3E4");
            encode.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEXYZ");

            CryptoStream crStream = new CryptoStream(stream, encode.
CreateEncryptor(),CryptoStreamMode.Write);

            byte[] données = ASCIIEncoding.ASCII.GetBytes("Ce message
est secret.");

            crStream.Write(données,0,données.Length);

            crStream.Close();
            stream.Close();
        }
    }
}
```

Le décryptage suit un schéma relativement semblable au cryptage. Vous devez d'abord obligatoirement faire appel au fournisseur de service cryptographique adéquat (ici DES) :

```
DESCryptoServiceProvider decode = new DESCryptoServiceProvider();
```

Il est aussi évidemment nécessaire de fournir la même clé et le même

vecteur d'initialisation que ceux employés pour le cryptage :

```
decode.IV = ASCIIEncoding.ASCII.GetBytes("A1C2D3E4");
decode.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEXYZ");
```

Nous créons le flux `crStream` à partir duquel sont lus les octets cryptés et le mode dans lequel nous voulons créer cette classe est ici placé sur `read` pour lecture.

```
CryptoStream crStream = new CryptoStream(stream, decode.CreateDecryption(), CryptoStreamMode.Read);
```

Nous pouvons maintenant lire les données en appelant la méthode `ReadToEnd()` :

```
string donnees = reader.ReadToEnd();
```

L'application vous affichera au final un magnifique «Ce message est secret.». Voici le code récapitulatif de décryptage :

```
using System;
using System.IO;
using System.Text;
using System.Security.Cryptography;

namespace CryptoStream_Decrypte
{
    class Class1
    {
        static void Main(string[] args)
        {
            FileStream stream = new FileStream("C:\\test.txt", FileMode.Open, FileAccess.Read);

            DESCryptoServiceProvider decode = new DESCryptoServiceProvider();

            decode.IV = ASCIIEncoding.ASCII.GetBytes("A1C2D3E4");
            decode.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEXYZ");

            CryptoStream crStream = new CryptoStream(stream, decode.CreateDecryption(), CryptoStreamMode.Read);

            StreamReader reader = new StreamReader(crStream);

            string donnees = reader.ReadToEnd();

            System.Console.WriteLine(donnees);
            System.Console.ReadLine();

            reader.Close();
            stream.Close();
        }
    }
}
```

Remarquez que pour générer la clé privée il est possible de faire appel à une méthode `GenerateKey`. Celle-ci fait appel à un générateur de nombre aléatoire (RNG : Random Number Generator).

```
encode.GenerateKey();
```

```
Console.WriteLine(Convert.ToBase64String(encode.Key));
```

La taille de la clé dépend du fournisseur choisi : 64 bits pour une clé DES, mais 192 bits pour une clé TripleDES... C'est la propriété `KeySize` qui renvoie la taille de la clé utilisée pour générer la clé secrète. De même, vous pouvez générer un vecteur d'initialisation avec la méthode `GenerateIV()` comme ceci :

```
encode.GenerateIV();
Console.WriteLine(Convert.ToBase64String(encode.Key));
```

Pour terminer, si vous désirez crypter/décrypter en mémoire (et non en stockant dans un fichier comme nous l'avons fait) vous devez créer un flux de type `MemoryStream`.

Voici le bout de code nécessaire :

```
...
ICryptoTransform ct;
MemoryStream ms;
CryptoStream cs;

DESCryptoServiceProvider encode = new DESCryptoServiceProvider();

encode.IV = ASCIIEncoding.ASCII.GetBytes("A1C2D3E4");
encode.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEXYZ");

byte[] donnees = ASCIIEncoding.ASCII.GetBytes("Ce message est secret.");
ct = encode.CreateEncryptor(encode.Key, encode.IV);
ms = new MemoryStream();
cs = new CryptoStream(ms, ct, CryptoStreamMode.Write);
cs.Write(donnees, 0, donnees.Length);
cs.FlushFinalBlock();
Console.WriteLine(Convert.ToBase64String(ms.ToArray()));
Console.ReadLine();
...
```

L'espace de noms `System.Security.Cryptography` de .NET répondra aux besoins les plus courants. Cependant, si vos besoins algorithmiques s'étendent au-delà des possibilités de ce qu'offre .net, par exemple, si vous désirez absolument utiliser un algorithme tel que le Blowfish, vous devrez recourir à une ressource externe. Cyfer est une bibliothèque qui répondra à vos besoins pour les langages C, C++, Java, C#, Perl, PHP (\*1) et Python.

Une autre possibilité est d'écrire vos applications .net sous Mono qui comporte son propre espace de nom (Mono.Security).

(\*1) Test de hachage en PHP avec Cyfer :

```
function test_hash()
{
    $a = cyfer_hash_init("RIPEMD-160");
    cyfer_hash_update($a, "Hello World");
    $res = bin2hex(cyfer_hash_finish($a));
    if ($res == "a830d7beb04eb7549ce990fb7dc962e499a27230")
        return true;
    return false;
}
```

Cyfer : <http://software.senko.net/projects/cyfer/>

■ Xavier Leclercq - [Xavier.Leclercq@programmez.com](mailto:Xavier.Leclercq@programmez.com)

# Double compétence : le secret de la réussite ?

Sur le marché du travail, on recherche des employés éclectiques et compétents, capables de dialoguer, de répondre aux besoins et de s'adapter à de multiples situations. Les informaticiens n'échappent pas à ces règles. Désormais, comme nous l'évoquions dans un précédent article, les entreprises utilisatrices, les SSII et les éditeurs sont à la recherche d'informaticiens disposant d'une double, voire d'une triple compétence : technique bien sûr, mais aussi métier et/ou fonctionnel.



" C'est le lot commun de la majorité des entreprises depuis un peu plus d'un an ", confirme Christine Grevé, Thales IS. De plus en plus d'entreprises externalisent leur informatique, mais souhaitent dialoguer avec des interlocuteurs qui connaissent bien le secteur d'activité ou plus exactement la fonction pour laquelle l'outil informatique est dévolu. Marie-Aude Firmin, consultante en recrutement chez Aedian, SSII spécialisée dans le tertiaire financier, rappelle ce que certains ont eu tendance à oublier au fil des ans : " l'informatique doit répondre aux besoins de l'utilisateur final ". D'où l'intérêt, voire la nécessité de comprendre ses besoins et ses contraintes. Une notion " un peu oubliée dans les années d'euphorie ", ironise Didier Neyrat, directeur géné-

ral de Cadextan, spécialisée dans la finance de marché et qui ne recrute à ce titre que des profils doubles compétences.

Les secteurs d'activité les plus sensibles à la connaissance métier semblent actuellement être la banque et l'assurance (voir notre focus ci-dessous), les télécoms, l'aéronautique, l'industrie en général et la santé.

Pour un développeur, la maîtrise d'une double compétence fonctionnelle ou métier en plus de la technique est devenue un élément fort d'employabilité et de résistance à l'offshore : difficile et coûteux en effet de transférer à des ingénieurs indiens, dont le turn-over est de plus particulièrement élevé, des compétences très spécifiques sur les spécificités de la comptabilité ou de la paye française...

## Métiers, fonctions et doubles compétences

"Les entreprises ne recherchent pas la connaissance d'un métier et de l'informatique, mais bel et bien celle d'une fonction (ressources humaines, comptabilité...), au sein d'une entreprise ou d'un secteur d'activité donné ", prévient Eric Patrux pour Iorga, une société de services informatiques spécialisée dans le conseil, l'intégration et la communication. " Il est nécessaire de bien distinguer la compétence métier de la compétence technique. Nous serons ainsi très intéressés par un profil ayant une connaissance parfaite d'un métier, et qui sera capable de rédiger un cahier des charges fonctionnel permettant des développements informatiques", poursuit Eric

## Les éditeurs aussi

Cette recherche de double compétence n'est toutefois pas la caractéristique des seules SSII. Pascal Guillemin, directeur des ressources humaines de Cegid, principal éditeur français dans le domaine de l'informatique de gestion avec le rachat de CCMX, souligne également la nécessaire double compétence métier et technique ". Au sein de ses équipes de développement, des spécialistes de la comptabilité, de la trésorerie, et de métiers comme ceux de la mode, du BTP ou des cafés hôtel-restaurant. Pour concevoir un progiciel à l'attention de ces secteurs il est en effet indispensable de les connaître... une évidence qui ne l'a pas toujours été. Sur le marché historique de Cegid, celui des experts comptables, la double compétence était " naturelle ", indique

Pascal Guillemin. Au fil du développement de la société, le profil des collaborateurs a évolué et la double compétence est plus ou moins forte selon les secteurs d'activité et la fonction. Christophe Raymond directeur technique de Cegid, souligne qu'un développeur travaillant sur les outils de paye doit pouvoir dialoguer avec un DRH, celui qui travaille sur la partie immobilisation doit connaître les normes IAS y afférant... Des compétences qui, souligne-t-il, ne se trouvent pas facilement. D'où les investissements forts sur la formation dans ces domaines, qui deviennent en outre un élément de motivation, les développeurs étant ainsi à même de voir l'implication finale de leurs réalisations.

Patrux. Il sera apte à dialoguer avec l'entreprise et à comprendre ses attentes. Il identifiera les liens et saura comment construire le système d'information en fonction des flux métiers. " En revanche, dans le cadre de doubles compétences, nous recherchons des profils connaissant à la fois une fonction et l'informatique ", explique Eric Patrux.

La double compétence peut être informatique/métier (banque, assurance, aéronautique), informatique fonction (finance, contrôle de gestion, gestion des risques, achats, etc.) ou encore... informatique/informatique. Patrick Bénichou, directeur général d'Open Wide cite ce dernier cas pour des profils d'architectes, qui doivent à la fois savoir conseiller le client sur les briques à utiliser, en ayant donc capacité à les évaluer, puis les intégrer en étant capable " d'aller dans le code ". Le terme de double compétence technique peut s'avérer flou. Les demandes peuvent aussi bien concerner les nouvelles technologies (Java et .net par exemple) que des technos de génération différentes (MVS Pacbase+ Java ou encore Java+ Grands systèmes).

## Des cursus spécifiques

Pour atteindre un tel niveau d'aptitude, il est souvent nécessaire de suivre parallèlement ou successivement deux cycles d'études. Dans le cadre d'une double compétence finance/informatique un DESS finance et un diplôme d'ingénieur en informatique s'avèrent très souvent nécessaires. Depuis une vingtaine d'années, des DESS double compétence ont fait leur apparition. Ainsi, l'Université Henri Poincaré de Nancy propose depuis 1984 un DESS compétences complémentaires en informatique (ancien DESS double compétence) dont l'objectif est " d'ajouter à la formation initiale de scientifiques non-informaticiens (biologistes, géologues, mathématiciens, physiciens...), une solide culture générale en informatique les conduisant à des postes d'ingénieurs, soit pour conjuguer leur première compétence et l'outil informatique, soit pour se convertir à l'informatique ". D'autres universités de l'hexagone préparent également à des diplômes similaires. Les " Miage " étaient censés répondre à ce type de besoin : Les connaissances des diplômés en gestion demeurent néanmoins souvent un peu trop théoriques aux yeux des futurs employeurs.

Les doubles formations se généralisent aussi dans les écoles d'ingénieurs qui, depuis

## Khodr Arnaout, Micropole Univers : De l'informatique à la finance



Aujourd'hui directeur de l'offre finance au sein de Micropole Univers, Khodr Arnaout est un exemple de profil informatique ayant évolué vers un domaine fonctionnel, en l'occurrence celui de la finance. Diplômé de l'ISIM, mais déjà intéressé par les problématiques financières, il rejoint Univers informatique (avant la fusion avec Micropole), comme ingénieur. Il commence à mettre en place des outils de reporting financier, puis s'intéresse à l'élaboration budgétaire. Après l'évolution classique, chef de projet et directeur de projet, il est désormais " directeur Management et Pilotage Financier " de Micropole Univers.

Aujourd'hui, l'offre finance de Micropole Univers regroupe jusqu'à 100 personnes : " des profils fonctionnels, techniques et mixtes ", explique Khodr Arnaout. Selon lui, le challenge aujourd'hui, sur un projet est de " constituer une équipe mixte technique et fonctionnelle ", capable de communiquer, ce qui suppose de " donner un bon vernis technique aux fonctionnels, et inversement ", avec une proportion d'environ deux tiers de profils techniques et un tiers de fonctionnels. Le travail se fait régulièrement en binôme, afin que les spécifications tiennent compte des aspects fonctionnels et techniques, avec une solution proposée répondant aux besoins du client, sans remettre à plat son système d'information. Et ce, sur un métier qui évolue rapidement, entre normes IAS/IFRS et lois de sécurité financière, et qui, nouvelle organisation oblige, information centralisée et saisie de l'information décentralisée, évolue technologiquement, avec les architectures Web et une conception qui est passée en quelques années de la mise en place de briques applicatives à des solutions progicielisées, de plus en plus sophistiquées, et dont la couverture fonctionnelle a beaucoup évolué, pour passer de la simple remontée d'information à une plate-forme financière complète, avec outils décisionnels pointus, pour participer à l'élaboration budgétaire.

Pour répondre à ces besoins, Micropole Univers assure une formation fonctionnelle à ses ingénieurs : au programme, l'élaboration d'un compte de résultats, des notions de cash flow, d'analyse des coûts. Khodr Arnaout note qu'il y a " de moins en moins de frontières entre les profils techniques et fonctionnels ".

quelques années, proposent soit des options double compétence dans le cycle ingénieur ou en troisième cycle, et dans ce dernier cas, souvent en collaboration avec une école de commerce ou une université. Ainsi, l'EISTI à Cergy, école très orientée informatique, a créé une option " ingénierie financière ", en anglais en plus. Elle propose également à ses diplômés une formation complémentaire pour être actuaire. Syntec Informatique s'est récemment dit, via son président Jean Mounet " très préoccupé par la désaffection des études scientifiques ", et a souligné à cette occasion la nécessité de " redéfinir le contenu pédagogique ", ce qui fait l'objet de la création d'un observatoire. Un des éléments précisés par Jean Mounet est la double formation, indispensable pour donner naissance à une génération des techniciens qui soient également " très compétents dans les métiers des clients ".

## Un plan de formation et d'accompagnement

Ces profils sont très recherchés, donc sollicités par d'autres sociétés que la leur.... Une fois que les sociétés les ont attirés, elles cherchent donc à les fidéliser. Experian poursuit deux objectifs : continuer à former ses collaborateurs et les fidéliser. Dans un premier temps, un bilan individuel dressé chaque année permet d'identifier tous les profils atypiques. " Un formulaire recense toutes les compétences de l'intéressé, avec à la fois, celles qui ont été mises en œuvre dans d'autres entreprises, et celles qui n'ont pas été exploitées ", explique Didier Croyet. Le plan de formation permet ensuite d'accompagner le collaborateur en travaillant sur ses points faibles. " Un petit nombre de nos ingénieurs ou chefs de projets a intégré des équipes avant-vente où la technique est omniprésente, mais où le commercial est très important. Il

s'agit de profils de double compétence, particulièrement atypiques ", confie Didier Croyet. Ils sont d'une aide précieuse dans le cadre de projets d'externalisation, où les équipes avant-vente doivent s'adapter et intégrer rapidement les particularités de chaque client pour répondre à leurs besoins.

## Focus : Banque et assurance, des segments porteurs

La banque est le secteur le plus spontanément cité lorsqu'on parle de double compétence informatique métier. Et pour cause : ce secteur sera dans les années qui viennent l'un des plus touchés par le papy-boom, avec le départ à la retraite chaque année de 3,3 % de ses collaborateurs entre 2005 et 2010, contre 0,9 % actuellement. Des départs qui touchent les équipes informatiques d'une part, d'où un recours plus important aux prestataires de services informatiques, mais qui amène aussi les banques à vouloir revoir un certain nombre de process, ou à se concentrer sur certaines activités, donc à rechercher des technologies pour compenser ces départs, a récemment indiqué Jean Mounet, président de Syntec Informatique. Unilog a, par exemple, construit une offre dédiée, via Unilog management, dont l'un des axes est de " travailler sur l'automatisation des processus métiers et la mutualisation des systèmes d'information, afin de réaliser des gains de productivité et de faciliter la capitalisation et la transmission des savoir-faire qui sont deux enjeux majeurs pour relever le défi du papy-boom. "

## Trois types de demandes

Dans l'univers de la banque et de l'assurance, les doubles compétences finance/informatique et monétique/informatique seront les plus recherchées. La publication de " Bâle II " suscite aujourd'hui des demandes de la part des banques. Selon Syntec Informatique, les experts sur Bâle II sont un des profils qui manquent actuellement. Côté monétique, EMV qui ouvre la porte au multi applicatif et à la



généralisation de la carte à puce dans le monde, devrait procurer du travail pour les années qui viennent.

**Didier Neyrat**, directeur général de Cadextan, SSII spé-

## Double diplôme, cinq ans d'expérience : le Top

Le profil idéal aujourd'hui est être diplômé d'une grande école d'ingénieur (Centrale Paris et Supélec sont assez appréciées), d'avoir un diplôme supplémentaire en finance (DESS par exemple) et deux à cinq années d'expérience dans le secteur, idéalement dans la banque, voire dans une banque pour le compte de SSII. Avec ce profil, vous serez accueillis à bras ouvert dans quasiment toutes les SSII, et demandés, en même temps par trois ou quatre clients de ces sociétés, ce qui est toujours flatteur...

cialisée sur le secteur de la finance, distingue trois types de demandes, correspondant à trois métiers bancaires différents : la banque de détail, à réseau, recherche des profils ayant déjà travaillé dans la banque, la compétence métier y est essentielle. Deuxième métier : la niche de la monétique. Troisième métier : la gestion d'actifs et la banque d'investissement, " un milieu où les clients sont assez élitistes et recherchent des profils ayant une double compétence informatique et finance ", avec en plus une connaissance de produits financiers particuliers (produits dérivés, Swap par exemple). Marie-Aude Firmin, consultante en recrutement chez Aedian, souligne que ces doubles compétences sont recherchées aussi bien pour des missions d'ingénierie que de conseil. Lorsque l'on consulte les offres d'emploi sur les sites spécialisés, sont principalement recherchées, des compétences en mathématiques financières (très souvent mentionnées), Bâle II, gestion des risques, contrôle de gestion. Côté informatique pure, les demandes des banques sont assez classiques et assez larges, compte tenu de systèmes d'information assez anciens et donc hétérogènes. Au programme, encore beaucoup de grands systèmes, du cobol encore et toujours, mais dans des proportions qui diminuent au profit de technologies et langages un peu plus récents, comme C++, Java, voire J2EE.

## Un parcours professionnel formateur

Très souvent cependant, une double compétence s'acquiert au cours d'un parcours professionnel. " Nos collaborateurs qui possèdent une double compétence ne sont pas issus d'un cursus d'études spécifiques, mais l'ont acquise auprès d'autres sociétés ", confirme Didier Croyet, responsable recrutement chez Experian. Société de services aux entreprises, Experian génère près de la moitié de son



chiffre d'affaires avec le monde bancaire (Image chèque, monétique, sécurisation des moyens de paiement, gestion de la relation client, externalisation...). " Nous

ne recrutons pas de jeunes diplômés, hormis ceux qui ont effectué leur stage d'étude chez Experian, mais du personnel confirmé justifiant de cinq à six années d'expérience", poursuit **Didier Croyet**. Certains collaborateurs ont d'ailleurs évolué dans le monde bancaire et ont suivi le cycle de formation interbancaire. Ils sont diplômés de l'institut de technique de banque (ITB) et/ou du centre d'études supérieures de banque (CESB). " La connaissance des process et des contraintes du monde bancaire, notamment dans le cadre de solutions monétiques, vient renforcer la pertinence des produits proposés par Experian ", indique Didier Croyet. Les doubles compétences ne sont pas des phénomènes nouveaux chez Experian. Elles sont inscrites dans la culture de l'entreprise.

Les collaborateurs titulaires d'un tel profil sont pour la plupart ingénieurs d'études, ingénieurs de projet ou chefs de projet.

Même soin apporté à la formation continue chez Cadextan. " Chaque année nous essayons de favoriser l'obtention de compétences complémentaires dans le domaine de la finance des marchés ", explique Didier Neyrat. Cela peut passer par un DESS spécialisé de la CNAM, pour lequel la société finance l'inscription et l'achat des ouvrages nécessaires. Cette année, Cadextan a également inscrit une quinzaine de collaborateurs pour l'obtention d'une certification.

■ **Carole Pitrás et Pascal Thuot**

# Rennes : destination sécurité informatique

**L**a technopole de Rennes Atalante a créé au fil des ans un véritable écosystème dans le domaine de la sécurité des systèmes d'information (SSI). L'école Nationale des télécoms Bretagne, sise à Brest, y dispose d'un pôle de recherche en SSI, qui s'intègre dans le tissu économique local, avec notamment la proximité du CELAR (centre électronique de l'armement) et de nombreuses SSII, dont Silicomp AQL, spécialisée dans la sécurité des systèmes d'information.

## Une longue tradition à l'ENST Bretagne

L'entité rennaise de l'ENST Bretagne travaille sur la SSI depuis plus de dix ans, avec plusieurs axes : les modèles et politiques de sécurité, les mécanismes de protection, la détection d'intrusion, l'évaluation de protocoles cryptographiques, des techniques d'analyse de programmes Java, etc. Parmi les nouveaux axes de recherche, dans le cadre des réseaux RNTL et RNRT, l'ENST participe aux projets MP6 (définition et mise en œuvre de politiques de sécurité dans les domaines de la santé et du social) et VTHD++, et à plusieurs autres projets dans le cadre de l'action coordonnée incitative, Système d'information du ministère de la Recherche.

## Un mastère SSI initié par le tissu économique local

L'enseignement de la SSI à l'ENST Bretagne commence en deuxième année du cycle ingénieur, avec deux UV consacrées à la "programmation réseau et sécurité" et aux "méthodes et concepts dans la sécurité des réseaux". En troisième année, plusieurs options intègrent des enseignements en sécurité : option "réseaux informatiques et système d'information multimédia", option réseaux et services mobiles, option réseaux et système d'information pour la finance ou encore, la plus spécialisée, l'option sécurité des systèmes d'information, ouverte en septembre 2004. D'autres options comportent également un enseignement en la matière.

De plus, l'école a créé il y a quelques années, avec Supelec, un mastère Sécurité des systèmes d'information. Une initiative, explique Sylvain Gombault, répondant notamment à une demande forte du secteur de la défense. Dès 1995 le

CELAR et AQL (devenu Silicomp AQL) réfléchissaient à la création d'un club SSI à Rennes, et en 2000, à l'opportunité d'un enseignement dédié. En 2001 ce projet a débouché sur la création du mastère SSI, dont la première promotion a été diplômée en 2003. Ce mastère vise à former des responsables sécurité, des concepteurs d'applications, des "évaluateurs" et des experts en sécurité. Les initiateurs de ce diplôme, comme le Celar ou Aql, participent également à l'enseignement, de même que la DCSII.

Au programme de ce troisième cycle, une formation de 135 heures sur l'aspect générique "réseaux et informatique", une formation de 100 h à l'analyse de risque et à l'évaluation, 150 heures sur la sécurité informatique, avec mini-projet à la clé, un cours théorique de 50h sur la SSI, quelques heures sur la cryptographie. Objectif : leur donner une capacité à structurer les problématiques SSI rencontrées, et apporter une expertise technique aux entreprises autant sur des aspects cryptographie qu'architecture. Il s'agit de petites promotions (15 personnes environ), alors que la demande est importante souligne Sylvain Gombault : jusqu'à 45 candidats se présentent à l'entrée. Cette formation mixte jeunes diplômés (60 %) et ingénieurs expérimentés (40 %).

En complément de ces formations et pour compléter son "catalogue", l'ENST a récemment développé une offre de formation continue sur la SSI, avec neuf stages proposés, disponibles pour des formations intra-entreprises, en partenariat avec AQL.

## Celar : le pôle sécurité informatique de la DGA

Implanté près de Rennes, le Celar compte 700 personnes, dont 40 % d'ingénieurs (10 % de militaires et 30 % de civils). Son rôle est notamment d'apporter son expertise technique à la DGA, par exemple d'évaluer des produits, de bâtir une cryptographie de défense, depuis la conception des algorithmes de chiffrement gouvernementaux à leur intégration. Un "centre d'expertise des techniques de la guerre de l'information", résume Arnaud Miguel, directeur du Celar "La SSI doit être considé-



rée comme une composante défensive dans la guerre de l'information", souligne-t-on au Celar. Objectif : assurer la "préservation, la confidentialité, l'intégrité l'authenticité et la disponibilité" des données informatiques, support de tous les systèmes militaires. Par exemple, le Celar travaille avec le CNES sur les projets Hélios (I et II) dans sa composante sol utilisateur (CSU). Ce projet d'imagerie spatiale compte, dans la dimension CSU quelque quatre millions de lignes de code, soit un projet de quelque 45 MEuros... Le Celar réalise au profit du CSU des missions de maquettage, d'assistance pour les spécifications techniques des besoins, de suivi du développement technique ou encore de qualification et ceci, tant dans la dimension informatique, de sécurité, de qualité des logiciels ou de technologie des composants.

## Silicomp-AQL : de la SSI militaire à la SSI des entreprises

Créée en 1988 à Rennes, AQL (Alliance qualité logicielle) a fait de nombreuses évaluations pour le Celar à partir de 1991. Jusqu'en 1997, la société réalise son chiffre d'affaires dans le secteur de la défense. Il n'est plus que de 12 % désormais, le marché "civil" de la sécurité informatique s'étant largement développé. La société réalise 57 % de son CA en conseil, 20 % via ses labos (Cesti, centre d'évaluation de la sécurité des technologies de l'information et Lesti pour l'homologation des cartes à puce et lecteur de carte), le reste, au travers de prestations d'audit dans le domaine de la sécurité. En 2000, AQL a été racheté par Silicomp, SSII d'origine grenobloise. Le groupe compte 600 personnes, dont 170 à Rennes et réalise un chiffre d'affaires de 45 M€.

■ Carole Pitras

# eXtreme Programming : DEVENEZ SUPER-DEVELOPPEUR



## Méthodes agiles, faire moins, mais mieux

**D'après le Gartner, 20 % des budgets informatiques sont gaspillés sur des projets qui seront purement et simplement abandonnés !**

**Les méthodes de conduite de projet utilisées sont-elles indaptées aux besoins, ou bien incorrectement mises en œuvre ?**

Les méthodes de développement ne sont certainement pas les seules incriminées, mais cette situation a conduit à une remise en cause des approches traditionnelles au profit de nouvelles méthodes plus légères et pragmatiques offrant une meilleure gestion des risques : les méthodes agiles. Parmi celles-ci, la plus célèbre et la plus utilisée est l'Extreme Programming (XP).

XP est une méthode de conduite de projet mise au point à la fin des années 90 par Kent Beck, Ward Cunningham et Ron Jeffries. Elle est centrée sur les fonctionnalités, les ressources humaines, la gestion des relations MOA/MOE et la gestion du changement, contrairement aux méthodes traditionnelles qui sont basées sur la planification, les processus et la documentation. XP repose sur un postulat simple : la gestion des risques doit rester en permanence au cœur du projet.

### 4 facteurs clés

Il existe 4 facteurs clés qui influencent le déroulement (et le succès ou non) d'un projet informatique :

- Le coût : un budget plus ou moins élevé permet d'influencer notablement le cours du projet. Mais attention, trop ou pas assez de moyens peuvent nuire à son bon déroulement ;
- Le temps : en accordant plus ou moins de temps à un projet, on influence directement

le coût et la qualité du produit final ;

- La qualité : le facteur le plus simple à réduire, avec le résultat que tout le monde connaît ;
- Le périmètre fonctionnel : moins il faut développer de fonctionnalités, meilleure devrait être la qualité (du moins en théorie).

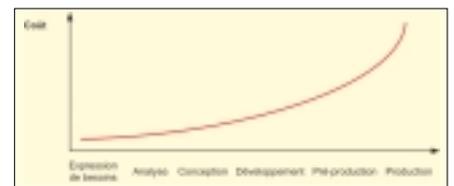
Toute l'alchimie d'un projet réussi repose sur une pondération adéquate de ces facteurs clés. XP recommande d'utiliser au maximum le périmètre fonctionnel comme variable d'ajustement. En clair, cela consiste à en faire moins, mais avec un meilleur niveau de qualité. Il faut donc, dès le démarrage du projet, faire le tri entre les besoins exprimés et les besoins réels, et associer de façon étroite la maîtrise d'ouvrage (le client) au processus de développement. Le coût d'une modification dans le cahier des charges d'une application varie d'une façon à peu près exponentielle avec l'avancement du projet. La modification d'une fonctionnalité lors des phases d'expression de besoins ou d'analyse est peu coûteuse, mais plus on avance dans le déroulement du projet plus le coût est élevé. Il est donc très important de partir sur des expressions de besoins solides si l'on veut éviter toute explosion des coûts.

### 4 valeurs fondamentales

Contrairement aux méthodologies traditionnelles qui reposent sur les processus, la plani-

fication et la documentation, XP repositionne les hommes au cœur du projet informatique. L'équipe projet XP comprend à la fois les développeurs (MOE) et un ou plusieurs clients (MOA). Plutôt que de spécifier des workflows et des documents types pour les échanges entre les participants, XP met en avant un certain nombre de comportements et de qualités humaines indispensables :

- La communication est une valeur incontournable, car, sans elle, les risques s'amoncellent sur le projet. La résolution des problèmes ne peut se faire sans des échanges constructifs et sincères entre les participants.
- La simplicité est un gage de la robustesse de la solution construite. Combien de projets ne se sont pas transformés en " usines à gaz "



Le coût du changement.

à cause d'un modèle de conception très sophistiqué (et très valorisant pour ses auteurs), mais parfaitement inutile. C'est aussi une preuve d'humilité de la part des concepteurs.

- Le feedback doit être à la base de toutes les actions dans un projet qui met en œuvre XP. Il concerne les relations entre les intervenants, mais aussi entre les développeurs et leur code (les tests).

- Le courage consiste à reconnaître les erreurs dès qu'elles apparaissent et à les traiter sans attendre, plutôt que de tenter de les dissimuler.

L'expérience montre malheureusement que peu d'organisations (en particulier celles de taille importante) s'attachent à promouvoir ces valeurs. Bien souvent, les considérations politiques prennent le pas sur le bon sens.

#### 4 activités seulement

Une fois fixées les valeurs que les intervenants doivent partager, comment gérer concrètement la réalisation du projet ? XP recommande d'organiser le travail autour de 4 activités :

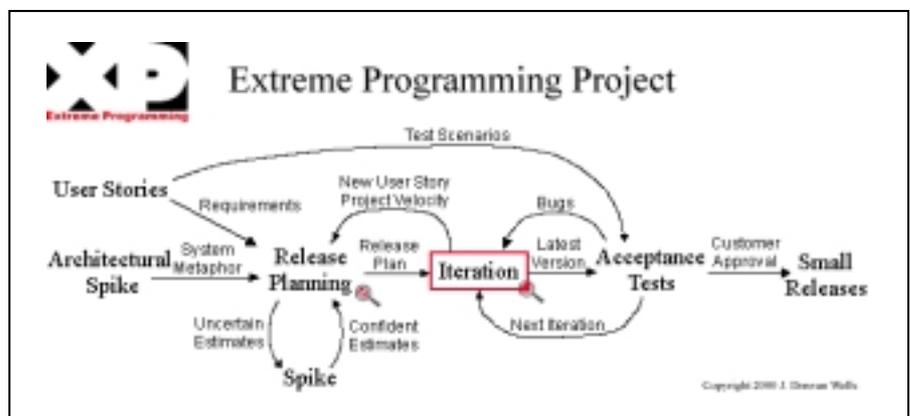
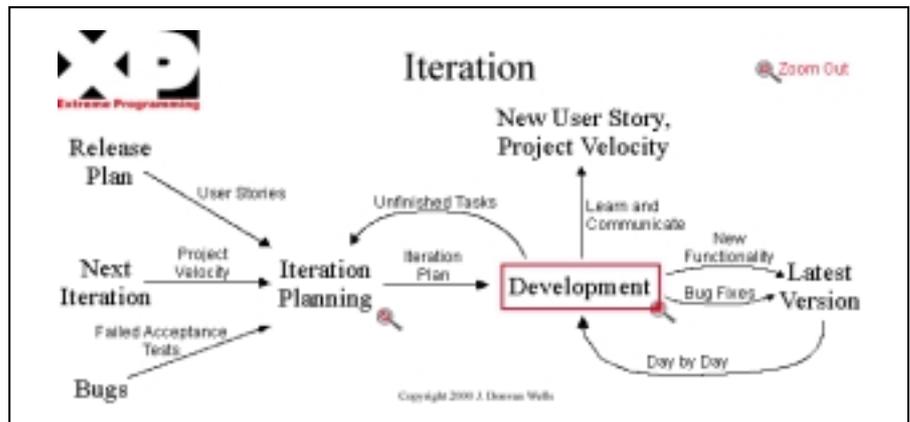
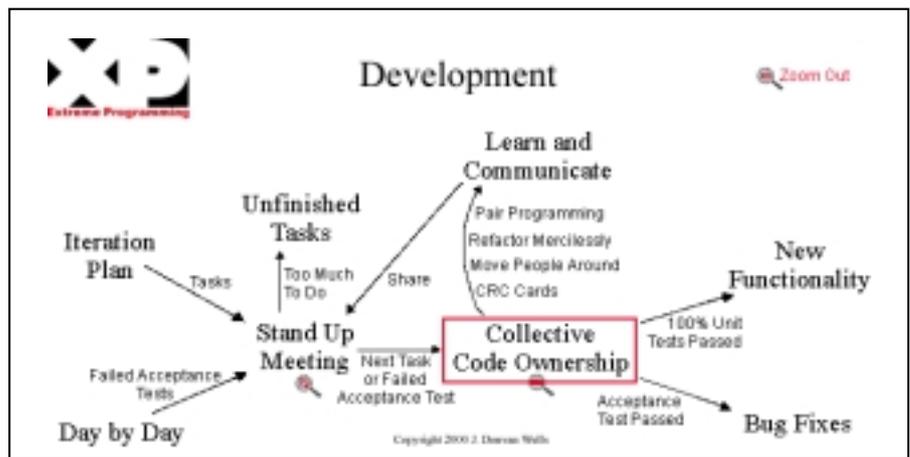
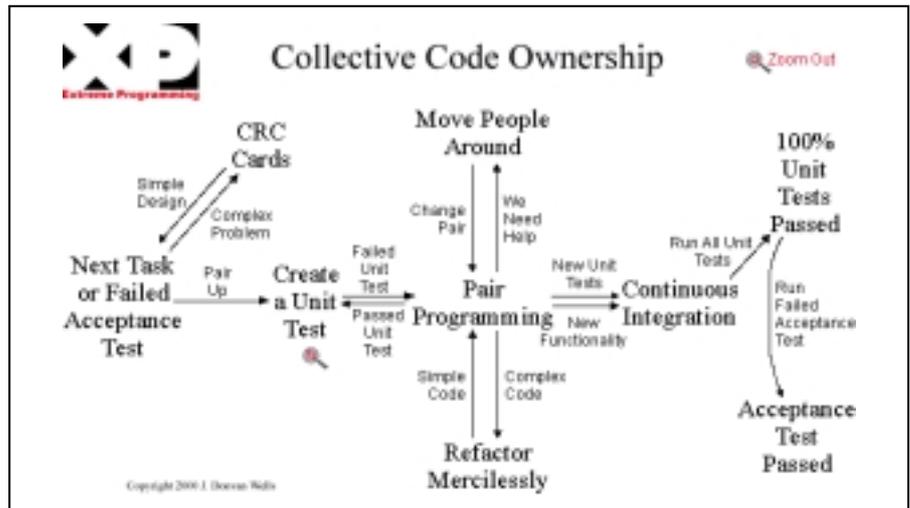
- Le codage est la tâche fondamentale de tout projet informatique. Le code doit être clair, simple et correctement commenté. Avec XP, le codage s'effectue de telle façon que les morceaux (objets, composants, procédures stockées ...) puissent être évalués le plus rapidement possible (idéalement tous les jours).
- Les tests doivent immédiatement suivre les opérations de codage. Qu'il s'agisse de tests unitaires ou de tests fonctionnels plus complexes, XP requiert que l'ensemble du code soit testé tout au long du projet. D'une manière générale, avec XP, les scénarios de tests sont élaborés dès l'expression des besoins. Les tests sont au cœur de la démarche XP, car ils contribuent activement au contrôle des risques.
- L'écoute est une activité à part entière, car les membres de l'équipe ne maîtrisent pas aussi bien les aspects fonctionnels que le client. Ils doivent donc rester à l'écoute des besoins et prendre correctement en compte les feedbacks utilisateurs.
- La conception est un pré requis indispensable. Il n'est pas possible de commencer le codage de l'application sans une réflexion sur son architecture de l'application. Même si XP désacralise la phase de conception, elle n'en reste pas moins importante.

En résumé, XP c'est un peu de conception, pas mal de code, de l'écoute et beaucoup de tests.

#### XP en pratique

Sur le plan pratique, les projets qui mettent en oeuvre l'eXtreme Programming se caractérisent par des pratiques originales, en particulier :

- Le pair programming (programmation en binôme) consiste à mettre deux développeurs par poste de travail. Le premier contrôle le clavier et tape le code tandis que



le second s'occupe de la cohérence des objets en cours de développement avec l'ensemble de l'application et apporte son point de vue sur le code. Bien entendu il est possible (et même souhaitable) de permuer les rôles et de changer régulièrement la composition des binômes.

- L'intégration en continu. Avec XP, le code doit être intégré dans le référentiel commun le plus vite possible pour pouvoir être testé rapidement. L'intégration se fait généralement sur un poste dédié à cette tâche.
- La propriété collective du code est un principe absolu. Aucune portion du code n'est la propriété d'aucun membre de l'équipe. Tout le monde peut intervenir sur n'importe quel objet ou méthode. Le pair programming facilite ce principe dans la mesure où les développeurs tournent sur les différentes parties de l'application.

On le voit, l'Extreme Programming remet profondément en cause l'organisation pratique des développements tels qu'ils sont conduits aujourd'hui dans de nombreuses organisations.

### XP or not XP ?

Alors faut-il adopter sans réserve l'Extreme Programming ? Cela dépend du projet, du

contexte et des ressources disponibles. En effet, autant XP convient parfaitement pour des petits ou moyens projets informatiques réalisés par des équipes réduites, mais performantes, autant il n'est pas du tout adapté à des projets de grandes tailles, car la souplesse qu'il apporte risque de semer la pagaille en désorganisant les équipes. Concernant les projets de petites ou moyennes tailles, il existe également deux pré requis importants qu'il faut absolument valider avant de se lancer :

- la réelle volonté (et la capacité effective) du client de s'impliquer tout au long de la phase de réalisation ;
  - la présence dans l'équipe de développement d'un noyau dur de développeurs senior aguerris, capables de maîtriser les subtilités de cycles de développements très courts et de pratiquer effectivement le pair programming ;
- Si ces deux conditions ne sont pas remplies, il est préférable d'utiliser une méthode de gestion de projet classique.

### Conclusion

XP est une méthodologie supplémentaire. Elle vient s'ajouter à la longue liste des techniques de gestion de projet qui jalonnent la courte histoire de l'informatique. XP va à contre-cou-

rant de la tendance qui consiste à transférer la responsabilité du projet sur des processus, des plannings et de la documentation normalisée. Cette approche qui nous vient de l'industrie (aéronautique, automobile, bâtiment) où elle a largement fait ses preuves, n'est pas du tout adaptée au monde du service où le contexte et les besoins évoluent constamment. Le succès d'XP est là pour le prouver.

On pourra néanmoins regretter le nom choisi pour cette méthodologie qui par son caractère "extreme", rend plus difficile sa promotion et son acceptation par un large public de développeurs et de clients.

En 1974, dans "Le mythe du mois-homme", Frederick Brooks, le père de l'IBM System 360, soulignait déjà les insuffisances des techniques de gestion de projet et la spécificité de l'informatique dans ce domaine. Force est de constater que 30 ans plus tard, l'informatique n'a pas terminé sa quête de la méthodologie universelle.

### ■ Médéric Morel

Directeur technique de Neoxia, cabinet de conseil en architecture des systèmes d'information.  
mederic.morel@neoxia.com



## Comment devenir eXtreme programmeur ?

**Le lieu :** une zone dite « technologique » dans la banlieue d'une métropole de province, cet été. Une salle de réunion où il fait très chaud.

**Les gens :** une équipe un peu inhabituelle, puisqu'on y retrouve la plupart des ingénieurs qui développent le produit, mais également le chef de projet, le responsable qualité, le directeur marketing, la direction Produits et même le PDG.

**L'action :** tout le monde est assis autour d'une table et travaille avec enthousiasme à... gonfler des ballons. Pas tout à fait une réunion comme les autres ! C'est l'une des premières étapes d'un processus qui prendra certainement plusieurs mois, mais qui est porteur, pour ceux qui sont là, de promesses et d'inquiétudes à la fois ; c'est le début, pour cette équipe, d'une transition vers une nouvelle méthode de développement et de gestion des projets. Mais quel rapport avec les ballons ?

### Une décision longuement réfléchie

Retour en arrière de quelques mois. Nous sommes dans la même salle, mais c'est d'une réunion plus classique qu'il s'agit, et l'ambiance est moins joyeuse. À l'ordre du jour, le bilan du développement de la version la plus récente du produit phare de l'entreprise. Sur

un budget initial de 200 jours-homme, un dépassement constaté. - 500 jours ; et un retard de plusieurs mois.

Le cas étudié est celui d'une entreprise industrielle du secteur de l'instrumentation de mesure, que nous appellerons "I.M."; son métier consiste à fabriquer les boîtiers per-

mettant l'acquisition de données en temps réel, mais également le logiciel d'analyse qui fonctionne sur un PC, ainsi que "l'intelligence" embarquée dans les instruments.

Les performances décevantes du précédent projet n'ont pas été une surprise totale, et ne



Disney/Pixar

sont pas réellement hors normes dans une industrie du logiciel où dépassements de budgets et de délais, problèmes de qualité et mauvaise compréhension des besoins de l'utilisateur sont considérés par beaucoup comme une fatalité.

Pourtant, depuis quelque temps, on parle dans les couloirs d'I.M. d'un espoir possible. Aperçue sur le Web, croisée à nouveau dans un livre, puis dans les pages d'un magazine spécialisé, Extreme Programming ressemble tellement peu à l'image d'Épinal du projet logiciel "proprement" géré, qu'on a peur d'y croire. Mais des idées comme l'automatisation du test ou l'implication des clients font mouche, notamment dans l'esprit des ingénieurs.

Pour la direction, pas question d'avoir une confiance aveugle dans une méthode quelle qu'elle soit. Mais il faut bien reconnaître qu'un problème existe, et la décision de le régler a été prise. Puisqu'une solution semble à portée de main, il faut passer à l'action. C'est sur la base des résultats qu'on jugera.

## Comment s'y prendre ?

La difficulté, c'est que personne chez I.M. ne maîtrise, ou n'a pratiqué la méthode. Chacun sent bien qu'il faudra redéfinir les rôles – que fait un "testeur" en XP, qu'attend-on du "client" – et prendre de nouvelles habitudes – comment s'organise une "itération", comment mesure-t-on la "vélocité" ? Enfin, par où commencer ?

Avant d'être un ensemble de techniques, XP est surtout une façon différente de voir et de concevoir les projets de développement et leurs problèmes. Une équipe qui verrait XP comme quelque chose de "facile" ou "naturel" serait probablement en train de passer à côté de l'essentiel. Il faut donc commencer par mettre au point une stratégie. C'est dans ce but que la direction d'I.M. fait initialement appel à mes services.

Il n'existe pas une "recette" unique et garantie pour adopter XP et en retirer de bons résultats. Chaque contexte est différent. Chaque entreprise rencontre des difficultés particulières lors de ses projets logiciels, selon son secteur d'activité - la finance ou l'électronique - sa taille - équipes de 10 ou de 100 personnes - son mode de fonctionnement - éditeur ou SSII. Il faut considérer le passage à XP comme

un projet à part entière. Le recours à un consultant externe expert dans la méthode, capable d'appréhender rapidement et de façon synthétique les particularités du terrain, mais voyant la situation avec plus de recul que les membres de l'équipe, peut accélérer un tel projet.

## Comment apprendre ?

Il y a trois difficultés majeures dans XP.

Dans le désordre : changer la façon de planifier. Mettre les gens autour de la table pour maximiser la communication. Et augmenter radicalement la qualité du code par les tests. Dans chaque cas, la difficulté ne consiste pas à faire quelque chose de nouveau, à acquérir des connaissances, ou à disposer des "bons" documents types pour tel ou tel type de livrable. Elle consiste à mieux comprendre la dynamique d'ensemble d'un projet ; à comprendre les raisons pour lesquelles un projet peut prendre 200 % de retard sans que personne ne s'en aperçoive, par exemple.

Dès lors qu'il s'agit de changer le point de vue des gens sur les projets, une "formation" classique ne peut pas faire l'affaire. XP est constituée d'un certain nombre de techniques, qu'il est possible d'apprendre à pratiquer dans un premier temps, de perfectionner ensuite. Mais cet apprentissage risque d'être inutile si on n'a pas pris conscience de la nature du problème. C'est le talon d'Achille de toutes les techniques, par exemple, UML ou les langages objet. Le danger est de ne réaliser des diagrammes UML que parce qu'ils sont obligatoires, ou de croire qu'il suffit de programmer en Java pour "faire de l'objet".

Pour éviter ces écueils, l'apprentissage d'une méthode doit réunir trois éléments :

- Mettre au même niveau de connaissance les développeurs, leurs managers et clients, et éviter tout contresens ; un bon moyen d'y parvenir est une présentation générale de la méthode devant un public le plus large possible.
- Laisser s'exprimer toutes les inquiétudes ou résistances, par exemple lors d'une ou plusieurs "tables rondes" à la suite de ces présentations générales. En définitive, lors de

certaines formations, je passe plus de temps à écouter les gens qu'à parler – et plus j'écoute, plus mon intervention est efficace.

- Laisser les personnes les plus proches du terrain construire leur propre façon d'aborder et de comprendre la méthode - de la même façon, je considère qu'ils seront les mieux à même de formuler une stratégie pour la mettre en oeuvre.

Ce dernier point est le plus délicat, et le type d'intervention que je préfère utiliser dans mes prestations, et que je recommande à ceux qui cherchent à mettre en place XP "en interne", est l'apprentissage en situation – par exemple, l'atelier de simulation de projet.

Ce qui nous ramène aux ballons.



## Comprendre XP en trois heures

L'atelier "XP Game" est un excellent exemple. C'est un atelier efficace et ludique qui permet de placer l'équipe en situation : l'objectif est de planifier, réaliser et tester un certain nombre de "fonctionnalités", qui représentent un projet de développement logiciel. Mais il ne s'agit pas d'écrire du code - l'implémentation d'une de ces "fonctionnalités" exigera, par exemple, de gonfler cinq ballons, de réaliser un château de cartes de deux étages ou de réaliser un score minimum en lançant trois dés. "XP Game" est l'invention de deux consultants XP belges, Vera Peeters et Pascal van Cauwenberghé – <http://www.xp.be/xpgame/>.

Un certain nombre d'hypothèses propres à Extreme Programming font partie de la structure du jeu : ainsi, l'équipe reçoit un "cahier des charges" sous la forme d'un certain nombre de fiches de jeu, indépendantes les unes des autres. Chaque fiche comporte une très courte description de la tâche à réaliser, par exemple "Gonfler 5 ballons à un diamètre de 40 centimètres". Chaque fiche porte également une indication de la "valeur métier" de la fonctionnalité décrite - sa valeur pour le client, indépendamment de la difficulté à la réaliser. L'équipe doit estimer les charges en termes de temps - de 5 à 60 secondes. Le projet est découpé en "itérations" de trois minutes chacune. Ce "temps du projet" est matérialisé

par un simple sablier, ce qui permet de ménager des arrêts de jeu pour répondre à diverses questions. En tenant compte du temps nécessaire pour expliquer les règles du jeu, des divers arrêts de jeu, du temps nécessaire à réaliser les plannings, un atelier d'une après-midi - trois à quatre heures - permet de réaliser trois itérations.

Plusieurs équipes sont en général mises en concurrence - là aussi, il s'agit de refléter la réalité des projets - et chacune a pour objectif de réaliser, à chaque itération, un ensemble de fonctionnalités apportant une valeur la plus élevée possible. Mais une certaine liberté est laissée à l'équipe dans la façon de s'organiser, la stratégie à adopter, et ainsi de suite. En tant que modérateur et arbitre du jeu, je sais par avance quels « tests » je compte réaliser pour accepter ou non une fonctionnalité livrée par l'équipe - par exemple une ficelle de la longueur appropriée pour mesurer le diamètre des ballons. Si l'équipe oublie de me demander par avance quels seront ces tests, elle peut s'attendre à de mauvaises surprises au moment de la livraison. C'est une façon très efficace de démontrer l'intérêt de placer les tests le plus tôt possible dans le cycle de développement !

### Les effets

L'intérêt de ce type d'atelier est multiple. Il permet de présenter les concepts et la terminologie du mode XP de planification des projets, de façon ludique, donc mémorable. Il met les participants dans une situation de résolution de problème, où ils peuvent utiliser non seulement ces concepts, mais également leur propre expérience, et intégrer les deux. J'ai pu ainsi observer plusieurs personnes maîtrisant des techniques "classiques" de modélisation et de planification, qui ont rendu leur équipe plus efficace. Ces équipes ont appris quelque chose d'important : non seulement, XP est compatible avec ces compétences classiques, mais les deux approches peuvent se renforcer en se combinant ! Cet apprentissage en situation réserve toujours des surprises ; certaines équipes se trouvent en échec, d'autres ont plus de succès, mais tout le monde apprend des échecs autant que des succès. Surtout, cet apprentissage actif porte sur la dynamique globale du projet : en quelques heures, on peut tirer des bilans sur les mécanismes de contrôle ou de dérapage des délais de projets qui se



Disney/Pixar

déroulent normalement sur des périodes de plusieurs semaines ou plusieurs mois. Le retour sur investissement, en termes d'idées nouvelles par heure de temps investi, est très élevé. Le debriefing » qui suit l'atelier va donner de nombreuses pistes pour savoir quelle place le mode de planification d'XP doit occuper dans la stratégie de mise en oeuvre de la méthode.

### Les résultats

Retournons chez I.M., six semaines après la session "XP Game". Celle-ci s'inscrivait dans le cadre d'une prestation plus complète de formation et de conseil, comportant notamment d'autres ateliers de simulation (par exemple sur les effets de différentes stratégies de « bêta test » sur la qualité et les délais) et d'autres formations pratiques et interactives, notamment à la programmation par les tests. Mais les premières réunions avaient indiqué que la question la plus urgente était celle de la maîtrise des délais. Dans le cadre d'une nouvelle version à paraître dans quelques mois, la « feuille

de route » de l'équipe posait comme prioritaire le passage à une planification itérative.

Le bilan est largement positif, bien qu'incomplet. L'équipe a déjà réalisé trois itérations dans le mode XP ; elle estime que sa vélocité est bien maîtrisée. Les responsables du marketing et de la stratégie produit, qui avaient initialement une inquiétude quant aux sollicitations sur leur temps, générées par leur rôle de "client sur site", sont finalement très demandeurs d'une collaboration plus étroite avec l'équipe de développement, et plutôt satisfaits du niveau de qualité désormais fourni. L'équipe a adopté, de façon très spontanée et sans heurts, la programmation en binôme. Celle-ci contribue à améliorer la qualité et réduire certains problèmes liés à la sur-spécialisation des ingénieurs.

Il reste encore du travail à accomplir. Notamment, l'utilisation systématique des tests, pourtant un pilier d'XP, n'est pas encore au rendez-vous. Mais c'est encourageant après seulement six semaines ; ce qui compte surtout, c'est que l'équipe soit pleinement aux commandes et responsable de sa propre stratégie d'amélioration.

### À votre tour

Il n'existe pas une manière unique de devenir ou de construire une équipe de programmeurs extrêmes, mais certains principes peuvent vous guider de manière fiable dans un tel projet : l'apprentissage par la pratique, la réflexion d'ensemble sur la réalité du terrain, l'autonomie et la responsabilité de chaque membre de l'équipe. Ces principes augmenteront vos chances de succès dans la mise en place d'une nouvelle méthode de développement, que ce soit Extreme Programming ou une autre.

■ Laurent Bossavit - [lbossavit@exoftware.com](mailto:lbossavit@exoftware.com)



**Laurent Bossavit** est consultant-formateur indépendant ; co-auteur de "L'Extreme Programming", aux éditions Eyrolles, il se spécialise dans les méthodes agiles de développement et de gestion de projet ; il intervient également pour Exoftware, pionniers en Europe sur ce secteur.



TEMOIGNAGES :

# L'eXtreme Programming plaît !

**Nous avons été voir comment cela se passe dans la "vie réelle" avec de "vrais" développeurs et chef de projets ! Nous avons constaté que XP est plutôt bien perçu. Même si le "pur XP" n'existe quasiment pas, pour des soucis pratiques et de réalisme technique et humain. Mais, l'impact du XP sur le projet est fort, avec à la clé, une qualité de code supérieure et une productivité visiblement accrue !**

## David Barth, directeur technique IdealX Marier XP à d'autres méthodes



**Programmez ! : De quelle manière IdealX utilise-t-il la méthode XP dans les projets ?**

**David Barth :** Globalement, l'idée est que l'on ne fait pas du pur XP. D'ailleurs, j'ai rarement rencontré cela. En interne, on peut sans doute faire du 100 % XP. Chez IdealX, nous marions XP à la méthode RUP / UP.

UP est un bon compromis entre une méthode classique et une méthode agile. XP nous sert au développement à l'intérieur de la méthode UP. Ce qui fonctionne bien, c'est le "outside customer", le client qui réagit. Il faut un

contact chez le client. C'est très précieux pour un projet itératif. XP étant itératif, il permet l'intégration en continu, et de réaliser du test unitaire. On a une approche test / recettes comme le définit RUP.

**Programmez ! : XP intervient-il très tôt dans un projet ?**

**David Barth :** On commence à coder en XP dès la phase d'élaboration, afin de rôder les équipes, le planning... Pour le développement, on essaie de faire le plus possible de XP, même si "de loin", le client ne verra que RUP / UP.

**Programmez ! : Le fait d'avoir un binôme de développeur est-il un handicap ou contraire un "plus" ?**

**David Barth :** Dans un duo XP, il faut un "papa" et un "enfant". Sur ce point, on est classique. Le binôme est très difficile à faire fonctionner parfaitement. Je l'ai rarement vu bien marcher. Il faut quelque chose d'assez formel. On prend le cahier des charges puis on le répartit dans l'équipe. Et cela se passe bien. Si on a deux développeurs qui s'entendent

### Les points importants à garder en tête selon David Barth

- Il faut garder à l'esprit : faire la chose la plus simple qui marche, cela ne sert à rien de faire compliqué ! Bref : il faut du CODE SIMPLE.
- Idéalement, il faut implémenter XP petit à petit dans son projet et non le faire d'un coup.

### Peut-on mesurer un ROI ?

Difficile. Pour David Barth, l'investissement est faible, on a surtout besoin de temps. Cependant, le retour investissement est très fort sur la tenue du projet et sa qualité. Dès le 2e projet, on récolte les fruits de l'utilisation d'XP.

### XP réservé à des langages particuliers ?

En théorie non. Mais de l'aveu même de David Barth, XP s'en sort très bien avec les langages scripts de type Perl. Mais on peut en faire avec tous les langages. Cependant, l'outillage utilisé sera un gage de réussite ou d'échec. En Java, le fait d'utiliser du Ant, Maven, Junit, etc., peut aider à avoir un environnement plus souple et moins lourd.

bien, pourquoi pas. Sur les meetings, on perdait une heure chaque matin. Les meetings de 5 minutes, comme les définit XP, n'existent pas. On a opté pour une approche différente avec une personne plus orientée "architecte", qui voit les problèmes. Quand on fait par petit groupe, cela fonctionne mieux. XP est en quelque sorte une philosophie qui va dans le système de développement. On retourne aux valeurs humaines. Le chef de projet devient un facilitateur et on se rapproche du code.

### Fiche technique

**Points forts :** grâce au XP, on fait en sorte que le focus soit sur le code et uniquement le code.

**Points faibles :** eXtreme Programming ne marche pas dans sa totalité. Ce n'est pas applicable dans un vrai projet. On est déçu quand au final, on n'a pas le bon résultat.

## Régis Medina – chef de projet Les développeurs doivent s'harmoniser

**X**P, Régis l'a découvert en 1998 alors qu'il était encore développeur. La première mise en œuvre se fait réellement lorsqu'en 2000, il devient chef de projet. Il décide alors de l'appliquer à ses différents projets. Qu'est-ce que Régis trouvait d'intéressant à XP ? Sa réponse

tient en trois points "la conception itérative, la qualité du code, et le fait que cela va, selon moi, vers quelque chose de plus sain".

Dans XP, les côtés à la fois humains et techniques sont souvent mis en avant. Régis ne fait pas exception. Il apprécie la capacité de

tests automatiques et le travail en équipe. "Avec une équipe XP qui fonctionne bien, l'ambiance est particulière. Elle est plus saine, plus sereine, si les profils s'y prêtent". Voilà un des problèmes du XP, "dire : on prend n'importe quelle équipe et on la met à l'XP, c'est une loterie !". XP exige des développeurs une grande capacité à s'harmoniser, à s'entendre. Un binôme mal défini, et on arrivera vite à une équipe inefficace. XP est à la fois bénéfique

sur les côtés humains et exigeant sur les projets. L'autre côté humain provient du projet itératif et des liens qu'il faut tisser avec le client, les utilisateurs : impliquer les utilisateurs, avoir du feedback précise Régis. Ce côté développeur – utilisateur n'est pas assez mis en avant dans les projets. XP impose cela, contrairement à d'autres méthodes "plus lourdes" comme RUP / UP. XP propose aussi autre chose, de très important dans une bonne équipe : la réflexion sur la manière de travailler. Bref, avoir du feedback des autres développeurs, réfléchir sur l'amélioration des méthodes de travail. Car dans un projet XP, le binôme doit parler, discuter beaucoup et peut apprendre des autres de nouvelles astuces de développement, au lieu de développer dans son coin.

### Ne pas perdre du temps à re-compiler

Concernant les langages utilisables dans un projet XP, pas de réelle limite. Cependant, Régis précise quelque chose d'important : "l'expérience avec C++ montre qu'il existe une petite limite causée par le temps de compilation, avec XP, on développe en continu. En Java, c'est mieux qu'auparavant, grâce notamment aux outils. On se déplace rapidement dans le code. ". Et oui, un projet XP, c'est du codage, de la compilation, des tests continus. Si on perd trop de temps à recompiler à chaque fois le projet, on perd une certaine efficacité du XP. " Il y a une façon XP d'utiliser les outils " poursuit Régis.

Après 4 ans passés à manager des projets XP, le bilan pour Régis est plutôt positif, " je suis convaincu. Il n'est plus possible de se dispenser de test unitaire, projet XP ou non. ". Sur la qualité du code, Régis est direct : "On évite de partir en vrille ! On économise du temps. Mais il faut faire attention aux effets pervers.". L'un des effets pervers concerne l'information qui doit venir du client. Il ne faut pas tout attendre de lui !

Bref, pour Régis, XP permet de :

- mettre l'accent sur le code
- mais de ne pas passer tout son temps à coder,
- communiquer beaucoup sur la conception

Comme pour d'autres adeptes du XP, le " pur XP " est une direction, mais pas une fin en soi. " XP est assez simple à mettre en place dans un environnement plus complexe. Il faut le faire progressivement. "

## Didier Barry, Celerial Consulting " Coach agile "



Déjà auteur de sa propre méthode agile de développement, Celerial Consulting n'a pas hésité à intégrer XP dans sa propre méthode il y a déjà plusieurs années de cela. Depuis environ un an, Celerial travaille avec un important acteur de la téléphonie française. "Il fallait d'abord expliquer ce qu'était XP" nous indique Didier Barry. Le client a fait un peu le tri dans toutes les pratiques et valeurs définies par XP. Tout n'a donc pas été mis en place. Une des originalités de la mise en place d'XP dans cette grande entreprise repose sur le principe selon lequel le test pilote le développement. "On définit les tests avant la conception. Ils se définissent en parallèle avec l'évaluation des besoins". On connaît donc dès le départ les résultats que l'on attend.

Le binôme a été mis en place dans l'ensemble des équipes. Mais ici aussi, petite particularité pour être plus efficace : " il y a une parité de compétence, on a donc deux personnes de même niveau, des seniors, le but n'est pas de former. ". Trop souvent, on a des binômes senior – junior ou des binômes ayant des complémentarités de compétences trop marquées. Dans le premier cas, on perd en efficacité, mais dans le second, on crée " de la dépendance " selon D. Barry. De la dépendance, dans le sens, où il faut que le binôme soit toujours complet pour fonctionner. L'introduction du XP dans cette grande société a aussi impliqué une réorganisation de mode de développement. Désormais, les développeurs sont physiquement regroupés par " plateau ", en équipes de 4 à 8 développeurs. Au-delà, il faudrait introduire un échelon de communication supplémentaire. Le plateau est sous la responsabilité d'un contrôleur technique. Le plateau se situe dans une grande salle ouverte afin de favoriser la communication. Le projet est segmenté par plateau, par couche et par îlot.

### Responsabilité collective

Comme le précise Didier Barry, les équipes pour les projets utilisent des notions propres à XP : planification itérative et surtout un rythme

durable. Le rythme durable permet de lisser la charge de travail sur l'année, tout en donnant la possibilité d'avoir des pics de charges. De plus, on sait qu'au bout de 3 semaines, on aura le feedback du projet développé. Comme le souligne M. Barry, la présence du client sur site est un facteur important, même si cela reste difficile à mettre en place dans le cadre d'une grande société. Mais cela demeure indispensable, car cela facilite le feedback auprès des développeurs et permet aussi les spécifications " au plus tard ".

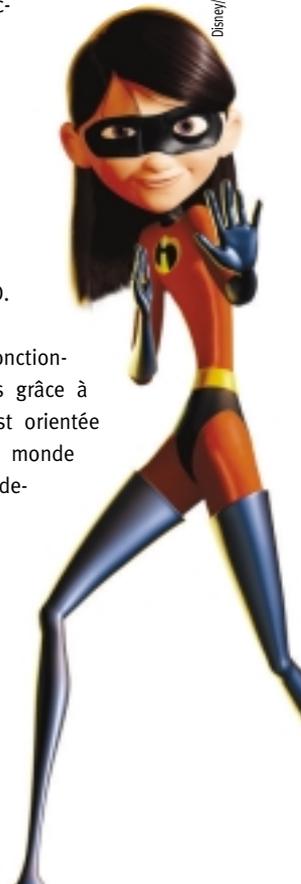
### "On évite l'usage de parapluies"

L'introduction du XP a aussi permis de mettre en place une manière de penser la responsabilité collectivement. On évite ainsi l'usage de parapluies afin de se protéger et de justifier tel choix. " Le côté justificatif m'a toujours dérangé " poursuit M. Barry. Cette forme de responsabilité commence à être admise et à rentrer en usage dans les plateaux. C'est possible quand l'équipe se connaît et quand la confiance règne.

Et le bilan au bout d'un an ? " Les gens sont persuadés que cela fonctionne. Ils y ont pris goût, même si ce n'est pas toujours facile. Le développement est meilleur. Les utilisateurs sont ravis. Sur le feedback, il n'y a pas, ou peu de surprises. Les dérives sont minimales ou contrôlées ", poursuit D. Barry.

D'autres détails dans le fonctionnement ont été possibles grâce à XP : la documentation est orientée lecteur (afin que tout le monde puisse la comprendre rapidement) ; on capitalise non plus sur les gens mais sur le projet / produit (chaque nouvelle release doit être réalisée comme s'il s'agissait d'une première version). Une fois de plus, la qualité du code est un facteur mis en avant.

■ François Tonic



Disney/Pixar

# JSF/Struts : comparaison par l'exemple

Cet article se propose de brosser quelques-unes des caractéristiques de JSF à travers un exemple écrit, d'une part en Struts, et d'autre part en JSF. Ceci suppose une connaissance minimale de Struts. L'exemple proprement dit est un écran, librement adapté de l'application "Duke's Bookstore" tirée du tutorial J2EE 1.4 . Cet écran affiche le panier d'un client et permet d'y ajouter des livres.

Copies of book in cart	Title	Price	
1	Web Servers for Fun and Profit	\$40.75	<input type="button" value="Add to Cart"/>
1	The Green Project: Programming for Consumer Devices	\$30.00	<input type="button" value="Add to Cart"/>
3	Java Intermediate Bytecodes	\$30.95	<input type="button" value="Add to Cart"/>
1	My Early Years: Growing up on *?	\$30.75	<input type="button" value="Add to Cart"/>
2	Web Components for Web Developers	\$27.75	<input type="button" value="Add to Cart"/>
0	Duke: A Biography of the Java Evangelist	\$45.00	<input type="button" value="Add to Cart"/>
0	From Calk to Java: The Revolution of a Language	\$10.75	<input type="button" value="Add to Cart"/>
Total = 8			

Figure 1 - L'écran catalogue

Les éléments en commun entre les deux solutions sont d'abord présentés, suivis de l'implémentation Struts, puis de celle basée sur JSF.

## Éléments en commun

Les classes du modèle entre les deux applications sont identiques :

- ShoppingCart : le panier.
- ShoppingCartItem : une quantité d'un même livre.
- BookDetails : un livre.



Figure 2 - Le modèle métier

Le panier est initialisé au moment de la création de la session et contient autant de ShoppingCartItem qu'il y a de livres dans le catalogue. Le panier est lui-même disponible dans le session scope sous le nom de cart.

## Struts

Dans la version Struts, deux classes et un fichier JSP sont nécessaires à l'implémentation :

- BookcatalogForm : l'identifiant du livre à ajouter dans le panier.
- BookcatalogAddAction : l'action de cliquer sur l'un des boutons.

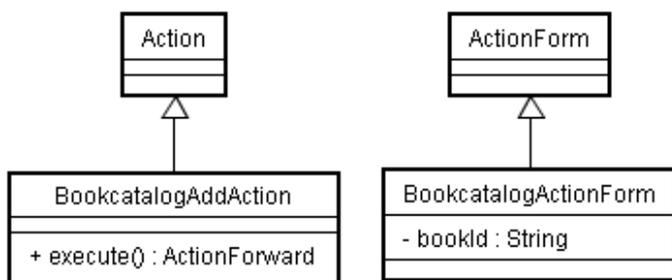


Figure 3 - L'action et le formulaire Struts

La vue du catalogue se présente ainsi :

## Listing 1 – Struts catalog.jsp

```

<%@ taglib uri="/WEB-INF/tld/struts-html-el.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/tld/struts-logic-el.tld" prefix="logic" %>

<html:form action="bookcatalogAdd">
<html:hidden property="bookId"/>

<table class="list-background">
<thead>
<tr>
<th class="list-header" scope="col">Copies of book in cart</th>
<th class="list-header" scope="col">Title</th>
<th class="list-header" scope="col">Price</th>
<th class="list-header" scope="col"/>
</tr>
</thead>
</table>
<table border="1">
<tr>
<td class="list-footer">Total = ${cart.numberofItems}</td>
<td class="list-footer" colspan="3"/>
</tr>
</table>
<table border="1">
<tbody>
<logic:iterate id="item" indexId="indexId" name="cart" property="items">
<tr class="list-row- $\% = \text{indexId.intValue}() \% 2 == 0 ? \text{"even"} : \text{"odd"} \%$ >
<td class="list-column-center">${item.quantity}</td>
<td class="list-column-left">${item.book.title}</td>
<td class="list-column-right">${item.book.price}</td>
<td class="list-column-center"><html:button property="add" onclick="this.form.bookId.value='${item.book.bookId}'; this.form.submit();">Add to Cart</html:button></td>
</tr>
</logic:iterate>
</tbody>
</table>
</html:form>

```

Ce JSP est représentatif d'une application Struts à plusieurs titres :

- Il n'existe pas de tag de haut niveau permettant de créer une table de façon déclarative. Le formatage proprement dit (tags html td, tr, thead, ...) est laissé au soin du développeur de la page.
- L'application d'une classe de style différente pour les lignes paires et impaires passe par l'utilisation d'un scriptlet et de la variable locale

indexId du servlet : class='list-row-<%=indexId.intValue() % 2 == 0 ? "even" : "odd"%>'.  
 • Le post doit être géré par l'intermédiaire d'un champ hidden, dont la valeur est affectée à travers du code JavaScript : onclick="this.form.bookId.value='\${line.book.bookId}'; this.form.submit();".

La classe d'action BookcatalogAddAction se contente de retrouver le panier depuis la session et d'y ajouter un nouvel exemplaire du livre identifié par BookcatalogForm.bookId, avant de faire suivre sur le même JSP.

### Listing 2 – action bookcatalogAdd dans struts-config.xml

```
<action path="/bookcatalogAdd" type="page.bookcatalog.BookcatalogAddAction" name="bookcatalogForm" scope="request" input="/bookcatalog.jsp">
  <forward name="catalog" path="/bookcatalog.jsp"/>
</action>
```

### Listing 3 - BookcatalogAddAction.java

```
public class BookcatalogAddAction extends Action {
  public ActionForward execute(ActionMapping mapping, ActionForm f,
  HttpServletRequest request, HttpServletResponse response) {
    BookcatalogForm form = (BookcatalogForm) f;
    ShoppingCart cart = (ShoppingCart) request.getSession().getAttribute("cart");
    cart.add(form.getBookId());
    return mapping.findForward("catalog");
  }
}
```

### JSF

La solution écrite en JSF repose sur un JSP catalog.jsp et un bean de support CatalogBean déclaré dans le fichier de configuration faces-config.xml (l'équivalent de struts-config.xml) :

### Listing 4 – managed bean catalog dans faces-config.xml

```
<managed-bean>
  <managed-bean-name>catalog</managed-bean-name>
  <managed-bean-class>backing.CatalogBean</managed-bean-class>
  <managed-bean-scope>request</managed-bean-scope>
</managed-bean>
```



Figure 4 - JSF managed bean CatalogBean

Cette déclaration a pour effet de fournir aux pages qui référencent le bean catalog des instances de

la classe correspondante. Dans le cadre de la page de catalogue, le bean est utilisé pour l'implémentation de l'action liée au bouton "Add to Cart" : <h:commandButton id="add" action="#{catalog.add}" ...

### Listing 5 – JSF catalog.jsp

```
<%@ taglib uri="/WEB-INF/tld/jsf_core.tld" prefix="f" %>
<%@ taglib uri="/WEB-INF/tld/html_basic.tld" prefix="h" %>
<f:view><h:form id="form">
```

```
<h:dataTable
  id="books"
  columnClasses="list-column-center,list-column-left,list-column-right,list-column-center"
  headerClass="list-header"
  footerClass="list-footer"
  rowClasses="list-row-even,list-row-odd"
  styleClass="list-background"
  value="#{cart.items}"
  var="item">
  <h:column >
    <f:facet name="header"><h:outputText value="Copies of book in cart" /></f:facet>
    <h:outputText value = "#{item.quantity}"/>
    <f:facet name="footer"><h:outputText value="Total = #{cart.numberOfItems}"/></f:facet>
  </h:column>
  <h:column>
    <f:facet name="header"><h:outputText value="Title"/> </f:facet>
    <h:outputText value="#{item.book.title}"/>
  </h:column>
  <h:column>
    <f:facet name="header"><h:outputText value="Price"/></f:facet>
    <h:outputText value="#{item.book.price}><f:convertNumber type="currency"/></h:outputText>
  </h:column>
  <h:column>
    <h:commandButton id="add" action="#{catalog.add}" value="Add to Cart"/>
  </h:column>
</h:dataTable>
</h:form></f:view>
```

L'approche composant de JSF permet de simplifier plusieurs aspects de cette page. Contrairement à Struts, la table est déclarée à l'aide d'un tag qui permet de spécifier les classes de style à utiliser pour : le header, le footer, les colonnes, ainsi que les lignes pour lesquelles il peut y avoir alternance de style : rowClasses="list-row-even, list-row-odd". D'autre part, l'aspect itératif est complètement pris en compte par le tag dataTable, à travers la variable item et la spécification des colonnes au moyen des tags column et outputText. Les colonnes peuvent contenir du texte (ex : titre du livre) ou des composants plus évolués comme commandButton. Les boutons sont eux-mêmes reliés à une méthode add() du bean de support CatalogBean, plutôt qu'à une classe spécifique (i.e. : action Struts). Ceci permet de faire supporter au même bean plusieurs fonctionnalités associées à la même page. Enfin, et c'est le plus important, la détermination du livre à ajouter dans le panier est automatiquement assurée par JSF à travers la variable item qui reste accessible après la soumission de la requête et non plus seulement pendant la phase de construction de la page, comme c'est le cas en Struts.

La méthode `CatalogBean.add()` profite de cette particularité pour rechercher le `ShoppingCartItem` correspondant au bouton pressé dans le request scope.

## Listing 6 - CatalogBean.java

```
public class CatalogBean {
    public String add() {
        ExternalContext context = FacesContext.getCurrentInstance().getExternalContext();
        ShoppingCartItem item = (ShoppingCartItem) context.getRequestMap().get("item");
        ShoppingCart cart = (ShoppingCart) context.getSessionMap().get("cart");
        cart.add(item.getBook());
        return "catalog";
    }
}
```

Il convient également de noter que la méthode `add()` ne requiert pas les paramètres nécessaires à la programmation Servlet (request, response), puisqu'un contexte attaché au thread qui gère une requête particulière porte ces informations (i.e. : `FacesContext.getCurrentInstance()`). La redirection vers le prochain JSP est assurée par la chaîne `catalog` qui est déclarée dans le fichier de configuration `faces-config.xml` :

## Listing 7 - navigation dans faces-config.xml

```
<navigation-case>
  <from-outcome>catalog</from-outcome>
  <to-view-id>/bookcatalog.jsp</to-view-id>
</navigation-case>
```

## Conclusion

à travers cet exemple, certes simpliste, cet article a montré comment JSF pouvait simplifier le développement de pages dynamiques. Le modèle composant de JSF offre en particulier les bases d'un nouveau paradigme, où les objets qui ont servi à construire une page sont disponibles dans la requête qui suit. Dans notre exemple, le livre à ajouter qui correspond au bouton "Add to Cart" se trouve dans le request scope pendant le traitement de l'ajout.

Le lecteur l'aura compris, cet article sert d'invitation à découvrir les nombreuses fonctionnalités offertes par JSF. Après plus de trois ans d'incubation, la spécification JSF 1.1 a été publiée, une implémentation de référence RI V1.1.01 est disponible sur le site de Sun, des implémentations commencent à voir le jour ainsi que des sites dédiés. Poussé par les acteurs majeurs du marché des serveurs d'application (Apache, IBM, Oracle, Sun, BEA, ...), JSF est promis à un bel avenir et permet de fournir dans le monde J2EE une alternative crédible à ASP.NET.



■ Vincent SEVEL - Groupe SQLI

**ONLY THE BEST GET IN.**

**JAVAPOLIS. THE MOST FERTILE CONFERENCE FOR JAVA LOVERS.**

ONLY THE BEST SPEAKERS, PRESENTATIONS AND CASES. THAT'S WHAT YOU CAN EXPECT FROM THE 3<sup>RD</sup> EDITION OF JAVAPOLIS, THE BIGGEST JAVA CONFERENCE IN EUROPE. FROM DECEMBER 13 TILL 17, YOU ARE MOST WELCOME AT METROPOLIS ANTWERP, BELGIUM. LAST YEAR 950 JAVA PROFESSIONALS JOINED THE CONFERENCE.

THIS TIME GURUS LIKE ERICH GAMMA, JOSHUA BLOCH, GAVIN KING, ROD JOHNSON, CRAIG MCLANAHAN, ADRIAN COLVER, CEDRIC BEUST, VINCENT MASSOL, GREGOR HOHRE, SUSAN LANDAU AND MORE TO COME... WILL PRESENT THE LATEST JAVA INNOVATIONS. JAVAPOLIS IS ALSO 4 DAYS OF BOF'S, 3 DAYS OF EXHIBITION AND A CYBER CAFÉ WHERE YOU CAN EXCHANGE JAVA EXPERIENCES WITH SOUL MATES. ON TOP OF ALL THAT, THERE'S ALSO A PARTY AND A MOVIE.

**AN OVERVIEW:**  
**13 - 14/12:** JAVAPOLIS UNIVERSITY COVERING 12 TOPICS BROUGHT TO YOU FROM THE SOURCE.  
**15 - 16/12:** JAVAPOLIS CONFERENCE WITH 40 TECHNICAL PRESENTATIONS AND AN EXHIBITION OF POPULAR JAVA AND J2EE PRODUCTS, SERVICES & COMPANIES.  
**17/12:** JAVAPOLIS BUSINESS FOCUSING ON THE CEOs, CIOs AND CTOs AND AN EXHIBITION OF POPULAR JAVA AND J2EE PRODUCTS, SERVICES & COMPANIES.

SATISFY YOUR JAVA NEEDS AND COME! SURF TO [HTTP://WWW.JAVAPOLIS.COM](http://www.javapolis.com) FOR THE COMPLETE PROGRAMME AND REGISTRATION.

**Premium partners:** Sun, ORACLE, Adobe, Microsoft, Borland

**Medium partners:** bea, JBoss, Java Community Process

**JAVAPOLIS**

# Une application Web J2EE avec Eclipse, Tomcat et MySQL

Nous allons réaliser une application Web J2EE, une galerie d'images, à l'aide des outils Open Source suivants : l'IDE Eclipse, le serveur Tomcat et la base de données MySQL. Après avoir mentionné comment utiliser ensemble ces outils, nous verrons d'un peu plus près la façon de concevoir cette application.

## Mise en place des outils Open Source MySQL

Afin qu'il y ait communication avec la base de données, il faut installer le driver JDBC pour MySQL. MySQL Connector/J est une implémentation de l'API JDBC pour la base de données MySQL. Placez le fichier JAR 'mysql-connector-java-[version]-bin.jar', disponible sur le site MySQL, dans le répertoire % JAVA\_HOME %\jre\lib\ext

Sous Eclipse, importez ce fichier dans le répertoire WEB-INF\lib de l'application WEB. Le driver se retrouvera ainsi dans la structure qui sera déployée sur le serveur.

## Eclipse

L'enrichissement de cet IDE se fait au moyen de nombreux plug-ins qui lui ajoutent de nouvelles fonctionnalités. L'équipe de Sysdeo en a créé un de particulièrement intéressant, puisque celui-ci permet, entre autres, de pouvoir :

- Créer un projet Tomcat avec sa structure WAR
- Démarrer et arrêter Tomcat sous Eclipse
- Créer un fichier WAR (qui sera sauvegardé, par exemple, directement dans le répertoire de déploiement '/webapps' de Tomcat)

L'installation du plug-in est simple ; il suffit d'extraire le fichier 'tomcatPluginV[version].zip', (téléchargeable sur <http://www.sysdeo.com/eclipse/tomcatPlugin.html>), dans le répertoire '/plugins' d'Eclipse. Un nouveau répertoire apparaît alors dans '/plugins': com.sysdeo.eclipse.tomcat\_[version]

Les boutons de démarrage et d'arrêt de Tomcat (figure 1) seront accessibles dans la barre de menus et d'outils en cochant l'option 'Tomcat' dans 'Window/Customize Perspective.../Commands'. (Figure 1)

Dans le menu 'Window/Preferences/Tomcat', il ne faudra pas oublier de mentionner le chemin du répertoire racine de Tomcat dans la zone de saisie 'Tomcat home'.

Comme signalé auparavant, ce plug-in peut créer un fichier WAR, dont le contenu sera déployé dans le répertoire 'webapps' de Tomcat, lorsque ce dernier sera lancé. Il suffit donc de définir l'emplacement du fichier WAR dans ce répertoire de déploiement de cette manière : dans la barre de menu, cliquez sur 'ProjectPropertiesTomcatExport to WAR settings' et saisissez le chemin d'emplacement.

Afin que le driver JDBC de MySQL soit localisé, il faut spécifier le chemin d'emplacement de celui-ci : 'Window/Preferences/Tomcat/JVM Settings', dans 'Classpath (Before generated classpath), ajouter le fichier JAR 'mysql-connector-java-[version]-bin.jar' que vous avez placé dans %JAVA\_HOME%\jre\lib\ext

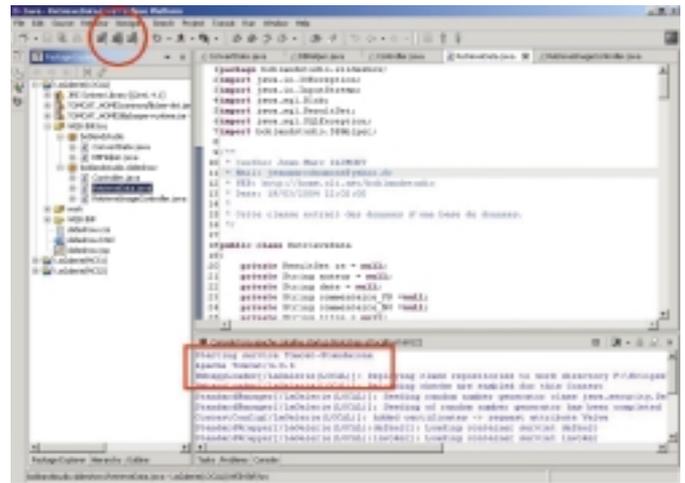


Figure 1 : le plug-in Tomcat installé dans Eclipse

## Tomcat

Le serveur Tomcat d'Apache nous sert en tant que moteur de Servlets. En milieu local, celui-ci nous permet de tester nos Servlets.

Par la suite, sur la toile, vous pouvez partir à la recherche, d'un fournisseur de services Java/J2EE (supportant Servlets/JSP et proposant une SGBD telle que MySQL) qui pourra héberger notre application. Nous allons maintenant voir cette dernière plus en détail.

## L'application

Cette application est une galerie d'images accessible par tout navigateur HTML au moyen du protocole HTTP. Le client aura le loisir de visionner plusieurs dessins grâce à des boutons de commandes (prochaine ou précédente image) Les images et informations associées aux images (textes, date, auteur) proviennent de la base de données (Figure 2)

## Description

L'application se compose principalement de quelques classes :

### - Classe DBHelper :

Classe chargée de traiter des opérations vers la base de données. Elle permet d'ouvrir et de fermer une connexion, d'exécuter une commande SQL et d'en récupérer le résultat.

### - Classe Controller :

Servlet qui reçoit et traite une requête d'un client. Elle implique un Java Bean à l'extraction des données textuelles relatives aux images.



Figure 2 : l'application WEB

**- Classe RetrievalImageController :**

Servlet qui reçoit et traite une requête d'un client. Elle implique un Java Bean à l'extraction de données binaires : image de la base de données. Les données binaires sont envoyées (flush) vers le client.

**- Classe RetrieveData**

Classe (un JavaBean) qui extrait des données de la base. Ainsi que d'un descripteur de déploiement et d'un JSP :

**- web.xml**

Descripteur de déploiement de l'application WEB. Dans ce fichier, on décrira notamment l'association (mapping) entre Servlets et URL.

**- lagalerie.jsp**

Page affichant images et textes.

**Fonctionnement**

Les deux Servlets 'Controller' et 'RetrievalImageController' sont chargées par le moteur de Servlets (ou container). Cela se passe lorsque le moteur est démarré, ou lorsque celui-ci a besoin de ces Servlets. Après le chargement, les Servlets seront instanciées, initialisées et prêtes à recevoir tout message de l'extérieur.

Lors de l'initialisation par la méthode init (ServletConfig config) de ces deux Servlets, on instancie le Java Bean 'RetrieveData' chargé d'extraire les données de la base de données.

La valeur du bouton de direction de feuilletage (avance ou recule) du formulaire HTML est expédiée vers la Servlet 'Controller' sous forme d'une requête GET. Le moteur de Servlets détermine le fait qu'il s'agit d'une requête GET et fait appel à la méthode 'service' de l'interface Servlet qui exécutera la méthode propice (doGet) de la Servlet interpellée.

Dans la méthode 'doGet', les données relatives aux images sont extraites de la base de données par le biais du Bean 'RetrieveData'. Ces données seront par la suite sauvegardées dans des attributs d'un objet 'session' qui appartiendra à un seul client HTTP. Finalement la méthode 'doGet' réexpédiera la requête à la vue JSP. La page JSP extraira les données de l'objet session. Cette page sera renvoyée vers le client HTTP. Lorsque le navigateur client lira le code HTML, il tombera sur plusieurs marqueurs <img>. Celui contenant l'attribut src ayant la valeur "RetrievalImageController?param1=..." sera une requête vers la Servlet 'RetrievalImageController'. Cette Servlet extrait une image, toujours avec l'aide du Bean 'RetrieveData', et l'expédie au navigateur client.

**Architecture**

L'architecture 3 tiers se présente en trois couches : couche base de données, couche logique et couche de présentation. La couche base de données est représentée par les tables de la base de données où les données relatives aux images (binaires et textes) sont stockées. La couche logique comprend les Servlets et beans, déployés sur un serveur physique distant (ou un serveur logique local). La couche présentation est l'interface graphique visible par le client. Il est bon de rappeler que cette façon de découper un système en couches indépendantes permet une plus grande souplesse lors du développement, une maintenance plus aisée et une meilleure évolution de celui-ci.

Le design pattern MVC (Modèle Vue Contrôleur) est une solution pour implémenter un code se calquant sur une architecture 3 tiers. L'idée se présente ainsi :

La requête cliente, issue du formulaire HTML du navigateur (la Vue), est envoyée aux Servlets ('Controller' ou 'RetrievalImageController') Ces Servlets jouent le rôle de contrôleurs: ils reçoivent un ou des paramètres du client (boutons de direction ou paramètre pour obtenir une image), les interprètent et impliquent le Java Bean à faire une tâche particulière. Ce Bean ('RetrieveData') figure dans la partie Modèle. c'est de cette couche que l'on accédera à la base de données. La classe 'DBHelper' figure aussi dans cette couche Modèle. Une fois les données extraites, le résultat sera affiché dans une page JSP; la Vue ou représentation que l'interface client reçoit (figure 3)

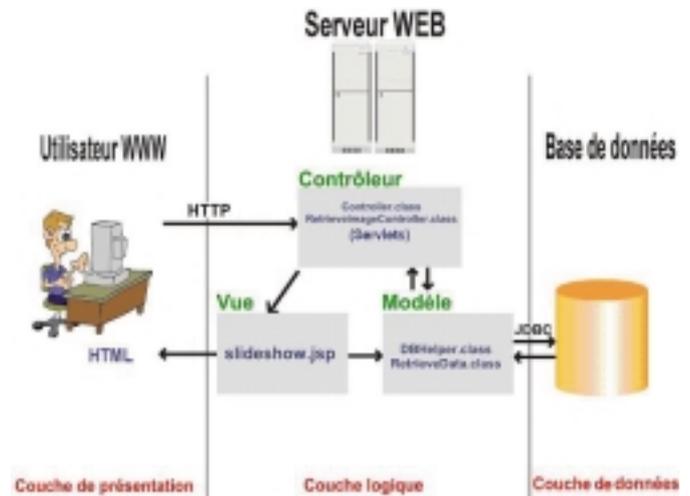


Figure 3 : Architecture 3-tiers et pattern MVC

**Programmation**

Une Servlet ne peut à la fois envoyer du texte et du binaire (image) dans une même requête. Il est donc nécessaire de diviser le travail en deux et ainsi de créer deux Servlets. La première Servlet (Controller) expédie les informations textuelles recueillies par le Bean vers la vue JSP tandis que l'autre a pour fonction d'expédier du binaire. Lorsque le navigateur client parcourt le code HTML et tombe sur le marqueur <img>, ce sera la deuxième Servlet (RetrievalImageController) qui entrera en action (listing 1).

**Listing 1 : extrait du fichier lagalerie.jsp**

```
<?xml version="1.0"?>
<%@ page session="true" %>
```

```

<HTML>
<HEAD>
<TITLE>La galerie</TITLE>
</HEAD>
<LINK REL="stylesheet" TYPE="text/css" href="lagalerie.css">

<BODY>
<FORM method="get" ACTION="Controller">
<TABLE border="0" cellpadding="0" cellspacing="0" >
<tr>
...
<td class="left" width="300" rowspan="2">


...
</td>
...
<tr>
<td colspan="2" height="450">
">
</td>
...
</tr>
...
</FORM>
</TABLE>
</BODY>
</HTML>

```

Le `ContentType` de la réponse envoyée au client doit avoir la valeur "image/jpeg" (ou "image/gif")

Pour envoyer du binaire, on utilise un objet de type `ServletOutputStream` retourné par la méthode `getOutputStream()`. Le fait d'instancier un objet de type `BufferedOutputStream`, avec l'objet de type `ServletOutputStream` en paramètre, permet d'envoyer l'image d'un trait (`flush`) lorsque toutes les données de l'image ont été lues (listing 2)

#### Listing 2 : extrait du fichier `RetrievalImageController.java`

```

public class RetrievalImageController extends HttpServlet
{
private HttpSession session= null;
private RetrieveData myBean= null;
...
public void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException
{
int ilmage[] =null;

// Si la requête n'a pas de session, on en crée une
if (session == null)
session= request.getSession(true);

String strImageTag= request.getParameter("param 1");

// Obtention d'un objet de type ServletOutputStream pour expédier du

```

```

// binaire
ServletOutputStream out= response.getOutputStream();

// Déclaration d'un BufferedOutputStream pour envoyer l'image d'un coup
BufferedOutputStream bos= new BufferedOutputStream(out);
response.setContentType("image/jpeg");

if (strImageTag.equals("<<") || strImageTag.equals(">>"))
{
// Extraction de l'image par le Bean
myBean.retrieveImage(strImageTag);

// Récupération de l'image
ilmage= new int[150000];
ilmage= myBean.getImage();

for (int i= 0; i < ilmage.length; i++)
bos.write(ilmage[i]);
}

else if (strImageTag.equals("flag_FR") || strImageTag.equals("flag_NO"))
{
...
}

// Tous les octets de l'image contenus dans le buffer bos sont écrits dans
// le ServletOutputStream out.
bos.flush();
bos.close();
} // end metode doGet
}

```

L'objet `HttpSession` permet de contourner la problématique du protocole HTTP qui ne peut conserver des données relatives à un client après une requête de celui-ci. En créant un objet de type `HttpSession`, nous avons la possibilité de sauvegarder les données textuelles, extraites de la base de données, dans des attributs de cette session (listing 3)

#### Listing 3: extrait du fichier `Controller.java`.

```

...
public void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException
{
String strSubmitForm =null;

// Si la requête n'a pas de session, on en crée une
if (session == null)
session = request.getSession(true);

// Récupération du paramètre "submitForm" envoyé lorsque le formulaire (FORM)
// est expédié
strSubmitForm = request.getParameter("submitForm");

if (strSubmitForm.equals("<<") || strSubmitForm.equals(">>"))
{
// On retient quel bouton SUBMIT a été cliqué dans la session,

```

```
// ceci sous forme d'un String
    session.setAttribute("PreviousNext", strSubmitForm);

// On extrait les données relatives a l'image
    myBean.retrieveDatas(strSubmitForm);
auteur = myBean.getAuteur();
    date = myBean.getDate();
date = ConvertDate.convert(date);
    commentaire_FR = myBean.getCommentaire_FR();
commentaire_NO = myBean.getCommentaire_NO();

    titre = myBean.getTitre();
texte1 = myBean.getTexte1();
    ...
// On sauvegarde ces String dans des objets de la session. Ils seront récupérés
// dans la vue JSP
session.setAttribute("session_auteur", auteur);
    session.setAttribute("session_date", date);
session.setAttribute("session_commentaire_FR", commentaire_FR);
    session.setAttribute("session_commentaire_NO", commentaire_NO);
session.setAttribute("session_titre", titre);
    session.setAttribute("session_texte1", texte1);
    ...
// On renvoie la requête a la vue
RequestDispatcher dispatcher =
    request.getRequestDispatcher(response.encodeURL("lagalerie.jsp"));
    dispatcher.forward(request, response);
}
}
```

Ceux-ci seront par la suite exploités par la page JSP qui sera expédiée vers le client (listing 4)

**Listing 4 : extrait du fichier lagalerie.jsp**

```
...
<h1>
Dessins / Tegninger:
</h1>
<p class="credits-left">
<%
if (session.getAttribute("session_auteur")!=null)
    out.println(session.getAttribute("session_auteur"));
%>
</p>
<h1>
Dessin réalisé en / Tegning laget i:
</h1>
<p class="credits-left">
<%
if (session.getAttribute("session_date")!=null)
    out.println(session.getAttribute("session_date"));
%>
</p>
...

```

■ **Jean-Marc Daumont**

L'auteur travaille à Trollåsen, en Norvège.

Bachelor of science in information systems, Oraclei DBA Certified Professional (Oslo, Norvège). BoBLanDStudio est son site personnel, uniquement consacré à la programmation.

<http://home.c2i.net/boblandstudio> - [jeanmarcdaumont@yahoo.fr](mailto:jeanmarcdaumont@yahoo.fr)

# Auprès de votre arbre à café, vivez heureux !



Visualiser les données hiérarchiques n'est généralement pas une mince affaire. Java et Swing offrent pour cela le composant JTree, très puissant, mais aussi, complexe. Nous découvrons les bases de son maniement.

Les données hiérarchiques sont omniprésentes en informatique, car de nos jours, il n'est pas de système d'exploitation dont le système de fichiers ne soit hiérarchique et, naturellement, les OS comportent des fonctionnalités natives pour visualiser les arborescences au sein des applications graphiques, (bureau Gnome ou KDE, explorateur Windows, etc.). Un jour ou l'autre, le développeur rencontrera le besoin d'afficher une liste arborescente, par exemple pour montrer des villes rangées dans des départements, eux-mêmes rangés dans des pays, ou des morceaux de musique rangés dans des albums rangés dans des catégories musicales. Les cas sont nombreux. Le maniement des API natives est en général ardu. Java encapsule tout cela dans le composant JTree, qui tout bien considéré, est relativement facile et sympathique à utiliser malgré son inévitable complexité.

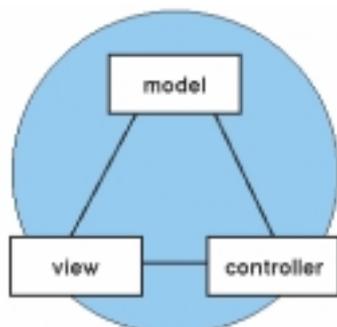


Fig. 1 : L'architecture Modèle - Vue - Contrôleur.

Ceci signifie que la gestion des données (modèle), leur représentation à l'écran (Vue) et l'interaction avec l'utilisateur (Contrôleur) sont découplées. En fait, sous Swing, nous n'avons pas du MVC pur et dur, car l'affichage et la gestion de l'utilisateur sont couplés dans le composant, mais en revanche, le stockage des données est effectivement géré par un modèle qui est bien une classe séparée, ce qui est finalement le plus important. Remarquons, avant d'entrer dans le vif du sujet, que les méthodes des objets nœud, avec lesquelles travaille le modèle par défaut, ne sont pas synchronisées. Il est fréquent qu'une application doive rafraîchir de grosses arborescences, ou encore énumérer une grande quantité de nœuds. Dans de tels cas vous avez tout à gagner à faire le travail dans un thread (cf. Programmez! 64).

## Pour se faire la main

Cet article est accompagné de 9 programmes d'exemple que vous trouverez sur le CD, ou à défaut sur le site ([www.programmez.com](http://www.programmez.com)). Nous commençons avec Demo1 (Fig. 2) qui place donc tout simplement un JTree dans un JFrame. Nous avons la surprise que le contrôle contienne déjà des données, mais surtout, on s'aperçoit en développant un nœud qu'un JTree ne dispose pas d'ascenseur. Nous devons donc, c'est la philosophie Swing, incorporer le JTree dans un JScrollPane (c.f Demo2).

## Le modèle de données

Mettons-nous d'accord avec la terminologie. Un arbre est composé de nœuds. Le nœud de départ est unique et se nomme la racine. Il n'a pas de parent. Chaque nœud peut avoir un ou plusieurs enfants, mais toujours un seul parent (sauf la racine bien sûr). Un nœud qui n'a pas d'enfant est une feuille.

Un modèle de données gère donc tout cela en manipulant des objets de types nœud. Lorsque nous avons traité de la JTable nous avons vu qu'il était très avantageux d'écrire son propre modèle de données. Avec le JTree c'est plutôt l'inverse. Il est pertinent d'apprendre à connaître et utiliser la classe DefaultTreeModel qui implémente l'interface TreeModel et qui conviendra dans la plupart des applications, tandis qu'implémenter l'interface est un gros travail. On peut voir le modèle de données comme un conteneur de nœuds. Ceux-ci doivent être des objets implémentant l'interface TreeNode. Là encore, nous utilisons l'implémentation par défaut : DefaultMutableTreeNode. Un nœud conserve les références sur son parent et sur ses enfants éventuels. Un nœud est aussi un conteneur, dans le sens où il conserve une référence sur un objet qui est la donnée proprement dite et qui se nomme un "User Object". Cette donnée peut être une simple chaîne, ou n'importe quel objet Java. Dans ce dernier cas, JTree affiche ce que renvoie la méthode toString de l'objet. Le modèle de données ne connaît pas directement l'organisation de l'arborescence. Pour cela, il interroge les méthodes des nœuds. À une exception près toutefois, le nœud passé au constructeur du modèle est considéré comme la racine de l'arbre. Si vous vous amusez à passer au constructeur un nœud pris au milieu de votre arbre, ce qui se trouve en amont sera tronçonné :) La hiérarchie dans les données s'établit au moyen de la méthode add de la classe DefaultMutableTreeNode, comme ceci :

```
// La racine
DefaultMutableTreeNode root
= new DefaultMutableTreeNode("Musique");

// les catégories musicales
DefaultMutableTreeNode poprock
= new DefaultMutableTreeNode("Pop Rock");
root.add(poprock);
DefaultMutableTreeNode jazz
```



Fig. 2 : Par défaut un JTree contient des données, mais pas d'ascenseurs.

```

= new DefaultMutableTreeNode("Jazz");
root.add(jazz);

// POP ROCK
// Noeud Jimi Hendrix
DefaultMutableTreeNode jimie
= new DefaultMutableTreeNode("Jimi Hendrix");
poprock.add(jimie);
// Premier album de Jimi Hendrix
DefaultMutableTreeNode exp
= new DefaultMutableTreeNode("Are You Experienced ?");
jimie.add(exp);
// et ainsi de suite.

```



Fig. 3 : Nos données hiérarchiques, visualisées par un JTree, lui-même intégré à un JScrollPane.

Le programme Demo3, allié à l'utilitaire ArbreBuilder produit de cette façon l'arborescence ci-contre (Fig. 3).

### Peaufiner la présentation

Le résultat peut nous satisfaire, ou pas si nous sommes pointilleux. Regardez l'album III de Led Zeppelin. Il ne contient pas de titre. Autrement dit, pour notre modèle de données il n'a pas d'enfants et est donc considéré comme étant une feuille et se voit attribuer une icône de feuille. Cela est parfaitement logique, mais un regard humain préférera voir ce noeud comme un conteneur de titres potentiels, donc il préférera lui voir attribuer une icône de noeud. Le même cas se présente quand on affiche une arborescence de fichiers. Il ne viendrait à personne l'idée de représenter un répertoire vide avec une icône de fichier. Nous devons donc modifier ce comportement par défaut.

En raison du découplage Modèle-Vue, le composant JTree ne sait rien a priori de cette histoire de feuilles. Mais s'il a la permission du modèle de données, il demande à chaque noeud si celui-ci est susceptible d'avoir des enfants. Si oui, le noeud reste un noeud, si non il est considéré comme une feuille. La permission se donne comme ceci :

```
modele.setAsksAllowsChildren(true);
```

Pour que le noeud de notre exemple réponde correctement, nous devons d'abord invoquer une de ses méthodes :

```
noeud.setAllowsChildren(true);
```

Mais attention, l'appel à setAsksAllowsChildren enclenche le mécanisme

pour tous les noeuds de l'arbre, donc pour les noeuds qui sont réellement des feuilles, l'invocation

```
feuille.setAllowsChildren(false);
```

est obligatoire. Essayer Demo5 et constatez.

Pour en terminer avec la présentation, signalons deux choses mineures, mais parfois pratiques :

- Il est possible de doter la racine d'une poignée, au moyen d'un appel à setShowsRootHandles(true) de JTree.
- Il est possible de masquer totalement la racine au moyen d'un appel à setRootVisible(false) de JTree. (c.f Demo4)

### Retrouver son chemin dans les arbres

Comment savoir quel élément de l'arborescence a été sélectionné par l'utilisateur ? Toujours en raison du découplage Modèle-Vue mentionné, le composant JTree ne connaît pas les connexions entre noeuds. C'est pourquoi, lorsqu'on l'interroge il ne sait répondre directement, mais construit un objet TreePath en interrogeant le modèle de données. Cet objet est un tableau d'objets noeud. Une fois le TreePath obtenu on lui demande quel noeud est finalement sélectionné :

```
TreePath selection = arbre.getSelectionPath();
DefaultMutableTreeNode noeud =
DefaultMutableTreeNode selection.getLastPathComponent();
```

Il existe un petit raccourci pour les paresseux :

```
DefaultMutableTreeNode noeud =
(DefaultMutableTreeNode)arbre.getLastSelectedPathComponent();
```

Essayez le programme Demo6. Notez la levée d'une exception si getSelectionPath est appelée sans rien de sélectionné.

### TreePath touillé

Nous en venons aux modifications des arbres. Pour que l'utilisateur puisse renommer un noeud après un triple clic sur celui-ci, invoquer la méthode setEditable de JTree (c.f Demo6). Mais le plus intéressant est de savoir modifier un arbre par programmation. Puisque le TreePath contient des noeuds, nous pouvons légitimement penser que nous pouvons nous en servir. Toutefois, dans ce cas, on n'appellera pas la méthode add d'un noeud. Cela modifierait bien l'arbre, mais le JTree n'en saurait rien, toujours en raison du découplage. C'est pourquoi on emploiera plutôt des méthodes du modèle :

- insertNodeInto pour ajouter un noeud
- removeNodeFromParent pour supprimer un noeud
- nodeChanged dans le cas de la modification de l'User Object. (c.f Demo7)

Ceci ne sera pas suffisant la plupart du temps. En effet, il est de bon ton de montrer immédiatement la modification à l'utilisateur, ce qui revient à déployer un ou plusieurs noeuds et à positionner le résultat au milieu de la vue (Demo6). Déployer les noeuds se fait comme ceci :

```
TreeNode[] noeuds = model.getPathToRoot(nouveau);
TreePath path = new TreePath(noeuds);
arbre.makeVisible(path);
```

Mais si le JTree est intégré à un JScrollPane, le résultat risque d'être invisible tant que vous n'aurez pas fait cet appel :

```
arbre.scrollPathToVisible(path);
```

### Enumérer les noeuds

À ce point, nous avons collaboré avec l'utilisateur. Celui-ci clique et nous réagissons. Mais le cas le plus fréquent est de devoir modifier une arborescence sans son aide, et sans forcément connaître a priori l'organisation, ou du moins le contenu exact de l'arborescence. Une application qui créerait un fichier devrait pouvoir retrouver son répertoire dans le JTree. Quant à nous, nous allons créer un nouvel album de Led Zeppelin que nous baptiserons IV :-). Voir le programme [Demo8](#). Notre problème s'énonce donc comme ceci : Nous savons que le noeud "Led



Fig. 4 :  
Ordre des noeuds selon breadthFirstEnumeration.

Zeppelin" se promène quelque part dans l'arborescence, mais nous ne savons pas où. Nous avons besoin d'obtenir une référence sur ce noeud. Donc, nous parcourons tous les noeuds jusqu'à trouver celui qui nous intéresse. Le modèle de données ne connaît pas lui non plus l'arborescence. C'est à un noeud qu'on doit la demander, celui-ci retournant l'arborescence à partir de lui. On obtient donc une sous-arborescence. Par contre, le modèle de données connaît la racine et c'est souvent par elle que l'on aborde l'examen, à moins que l'on ait gardé une



Demo 8 :  
Un nouvel album de Led Zeppelin.

référence sur un noeud plus pertinent. DefaultMutableTreeNode propose 4 méthodes qui renvoient les noeuds en dessous de lui. On utilisera la méthode que l'on estimera la plus rapide en sachant que :

- breadthFirstEnumeration énumère dans le sens de la largeur. Cela signifie que les noeuds sont passés en revue par niveau. Pour notre exemple, 'Musique', puis les catégories musicales, puis les artistes, et ainsi que suite. (Fig. 4)
- depthFirstEnumeration. L'algorithme se positionne sur les feuilles de la première branche, examine celles-ci, puis remonte au noeud précé-



Fig. 5 :  
Ordre des noeuds selon depthFirstEnumeration.

dent. S'il y a encore un noeud à ce niveau, on descend à ses feuilles que l'on examine, puis on remonte à lui, et ainsi de suite. Bref, l'arbre est parcouru dans le sens de la profondeur, d'où le nom (Fig. 5). On retient que les enfants sont passés en revue avant leurs parents.

- preorderEnumeration. Parcourt l'arbre dans le sens de la profondeur comme ci-dessus, mais les parents sont passés en revue avant les enfants. (Fig. 6).
- La même chose que ci-dessus avec les enfants passés en revue avant les parents, ce qui revient finalement à depthFirstEnumeration. Signalons pour terminer, pathFromAncestorEnumeration, qui trouve le chemin entre un noeud dit ancêtre, et un autre noeud spécifié, et qui retourne une énumération décrivant ce chemin.

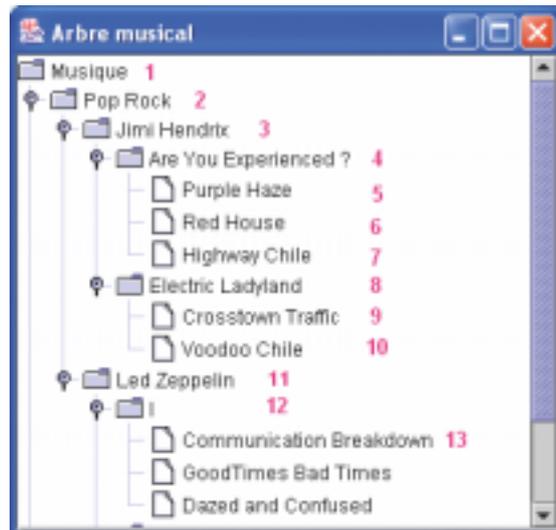


Fig. 6 :  
Ordre des noeuds selon preorderEnumeration.

JTree est un composant très riche. Nous avons traité ses aspects les plus simples et les plus immédiatement utiles. Les événements ne posent pas de difficulté (c.f exemple Demog). Mais le sujet est loin d'être épuisé. Affectation de nouvelles icônes ou modèle de données personnalisé, pour ne citer que cela, feront sans doute l'objet d'un autre article. A bientôt pour de nouvelles aventures avec Java.

■ Frédéric Mazué - [fmazue@programmez.com](mailto:fmazue@programmez.com)



# Hooquez le clavier de votre PC

Windows dispose d'un mécanisme très intéressant permettant d'intercepter les messages qui transitent à l'intérieur du système : les hooks. Découvrons ce mécanisme ensemble, afin de fabriquer, en C++, un petit utilitaire pour vous soulager de la crampe du programmeur.

Quand on jette un regard sur la syntaxe des langages informatiques, on ne peut s'empêcher de penser que ceux-ci ont été conçus par, et pour des anglo-saxons. Par exemple, C, C++ et Java font grand usage des accolades et crochets, ce qui n'est pas un problème avec un clavier QWERTY mais qui devient une gymnastique exténuante avec le clavier français AZERTY. Si la plupart des outils de programmation modernes insèrent les accolades qui délimitent les portées dans les langages précités, les tableaux avec leurs crochets restent une véritable punition. C'est pourquoi, je vous propose de construire ensemble un petit utilitaire reconfigurant partiellement votre clavier, afin d'obtenir une paire de crochets ou d'accolades par appui d'une seule touche, et surtout, sans devoir presser 'Alt Gr'. Ceci s'appliquant n'importe où, c'est à dire aussi bien dans votre outil de développement préféré (C++Builder, Visual Studio, etc.) que dans votre XEmacs ou dans l'humble Notepad. Pour cela, nous serons amenés à découvrir quelques aspects peu fréquentés de la programmation Windows, à commencer par les hooks.

## Les hooks

En tant que système d'exploitation multitâche, Windows se doit de gérer les événements de manière asynchrone. À la base, nous parlons des événements matériels tels que frappe d'une touche ou déplacement de la souris. Quand une chose de cette sorte se produit, Windows la traduit en données informatiques sous la forme d'un message, examine quelle est l'application concernée et place les données en question dans une file d'attente, que chaque application doit scruter en continu. Windows étend la notion d'événement à des choses ne concernant pas le matériel, par exemple la création d'une fenêtre, son apparition à l'écran, etc. Là aussi Windows fabrique un message et le transmet à l'application concernée. Plus encore, si chaque application a sa propre file d'attente de messages, le système, c'est-à-dire Windows, maintient une file de messages par laquelle tout message transite avant d'aller éventuellement dans la file d'une application. Il est fort tentant de pouvoir jeter un oeil sur tout ce trafic. Sans doute, les concepteurs de Windows eux-mêmes ont-ils éprouvé ce besoin à des fins de débogage. Toujours est-il que Windows permet effectivement d'espionner les messages au moyen des hooks (crochets en bon français). Un hook consiste en l'installation d'une petite fonction de rappel pour un type de message particulier. Lorsqu'un message est constitué et prêt à circuler dans Windows, la fonction de rappel, dite encore filtre dans ce contexte, est invoquée et reçoit en argument le message et ses paramètres. Normalement le filtre ne peut pas modifier le message, ni ses paramètres, ou plus exactement une telle modification est sans effet, mais elle peut retirer le message de la liste et éventuellement en poster un autre en lieu et place.

Plusieurs hooks peuvent être installés pour un même type de messages. Dans ce cas, les fonctions filtres forment une chaîne dans laquelle la der-

nière installée est la première à être invoquée. Un filtre qui ne supprime pas un message doit en principe passer celui-ci au prochain filtre au moyen d'une API.

## Heterhooklite

Il est possible d'implanter des hooks pour à peu près tout : procédure de fenêtre, événement souris, entrée en inactivité d'une application, le shell... et bien sûr, les événements clavier. Windows maintient une table

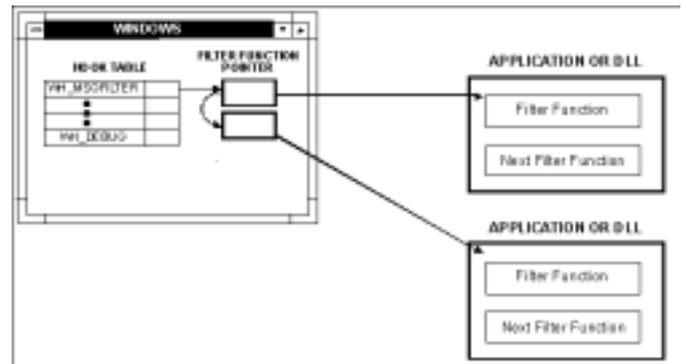


Fig.1 : Organisation du mécanisme de hook dans Windows. Schéma tiré de la MSDN.

de hooks, chacun d'eux étant une table de pointeurs de fonctions. (Fig. 1) dans tous les cas, le filtre a un prototype semblable à celui-ci :

```
LRESULT CALLBACK FilterFunc(int nCode, WORD wParam, DWORD lParam);
```

Outre les éléments wParam et lParam des messages Windows, le filtre reçoit un code. Si ce code est négatif, l'utilisateur n'a pas le droit de message, sous peine de risquer de déstabiliser le système. Si le code est positif ou nul, la procédure de hook peut examiner les valeurs wParam et lParam, et à ce point, plusieurs possibilités s'offrent au programmeur.

- le message ne mérite pas d'intervention : on le laisse suivre son cours dans le système soit :
  1. en retournant false.
  2. en retournant le résultat de CallNextHookEx. CallNextHookEx passe les valeurs du message au filtre suivant s'il existe. Comme nous l'avons dit plus haut, quand on installe un hook, son filtre est toujours placé en tête d'une table de pointeurs de fonctions. Cela signifie que si l'on est le dernier filtre installé, ne pas appeler CallNextHookEx (en se contentant de retourner false par exemple) désactive tous les hooks installés par d'autres programmes. C'est parfaitement légal sous Windows, bien que pas forcément toujours très bien élevé...
- Le message nécessite une intervention : on retourne true, ce qui à pour effet d'éliminer le message de la liste. Le processus à qui le mes-

sage était normalement destiné ne le recevra jamais, mais on peut, si on le souhaite, lui envoyer un autre message en lieu et place. (voir encadré 1)

### Hook il est ?

Pour en terminer avec les généralités, signalons qu'il existe deux niveaux de hook. Le niveau application et le niveau système. Si le filtre que nous installons est un morceau de code faisant partie de l'application qui l'installe, le hook est automatiquement au niveau de cette application. Cela veut dire que seuls les messages qui sont destinés à l'application seront interceptés par le filtre. Si le filtre réside dans une dll, le hook est automatiquement au niveau système. Le filtre aura alors droit de regard sur tous les événements, quels qu'ils soient. Notre but étant de redéfinir des touches pour n'importe quel éditeur, nous devons poser un hook au niveau système, donc l'écriture d'une petite dll est incontournable.

### Hookulte

Que se passe-t-il dans les profondes ténèbres de Windows, lorsque l'utilisateur presse une touche du clavier ? Tout d'abord, le hardware du clavier constitue un code appelé «scan code». Ce scan code est dépendant du matériel. C'est-à-dire que le scan code pour la touche A n'est pas le même si vous utilisez un clavier 'made by truc,' ou un clavier 'made by machin'. Ensuite le driver (pilote) de clavier se charge de traduire ce scan code

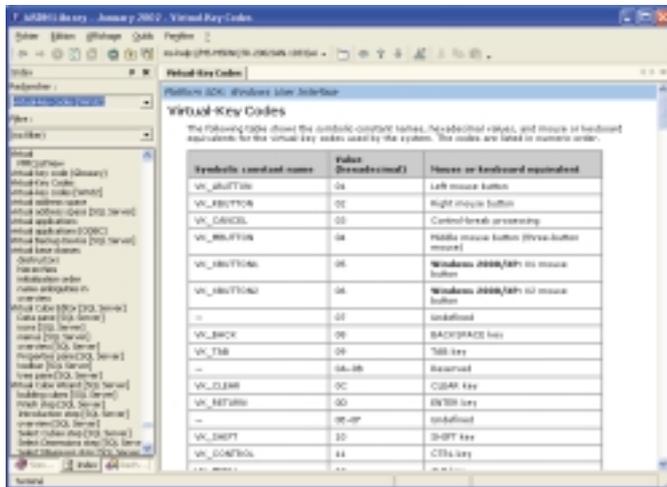


Fig. 2 : Pour connaître les codes des touches virtuelles, consultez la MSDN ou le fichier winuser.h.

en un code «virtual key», défini par Windows (dans le fichier winuser.h) (Fig. 2). À ce moment, quel que soit le fabricant de votre matériel, le code virtual key est toujours le même.

Ensuite le driver de clavier signale à Windows qu'une touche a été pressée au moyen de la routine système `keybd_event`, dont le maniement est tout ce qu'il y a de délicat. Windows est alors informé qu'un événement clavier a eu lieu, et construit un message qui sera envoyé au processus approprié, c'est-à-dire tout simplement le processus qui détient le focus clavier au moment de l'événement.

Enfin, la boucle des messages de la fenêtre concernée doit retirer le message de la queue, et faire ce que bon lui semble du contenu du message.

Pour être complet, il reste à dire que le driver clavier envoie en général deux messages clavier pour une touche actionnée. Le premier est envoyé lorsque la touche est enfoncée, Windows construisant alors le message `WM_KEYDOWN`, le second lorsque la touche est relâchée, Windows construisant cette fois le message `WM_KEYUP`. Bien évidemment, cela serait trop simple si cela était vrai pour toutes les touches. Il y a des exceptions, par exemple la touche 'imprime écran' qui ne produit un événement que lorsqu'elle est relâchée. Soyons donc vigilants dans notre exemple qui redéfinit les touches "imprime écran" et "arrêt défilement". Remarquons que cette redéfinition n'affectera pas les captures d'écrans lancées par la touche 'imprime écran', car ce mécanisme se positionne en amont des hooks.

Dans le cas d'un filtre clavier, que contiennent les paramètres du message `wParam` et `lParam` transmis au filtre `KeyboardProc` ? `wParam` contient le code virtuel de la touche actionnée. `lParam`, quant à lui, est un champ de bits constitué comme suit :

- bits 0 - 15: valeur de délai de répétition des touches.
- bits 16 - 23: le scan code. Oui le scan code propre au clavier! Que Windows transmette cette valeur après en avoir exigé la transformation par le driver de clavier a de quoi étonner... Peut-être est-ce utile pour du débogage ?
- bit 24 : Ce bit est placé lorsqu'il s'agit d'une touche «étendue». Une touche du pavé numérique par exemple.
- bits 25 - 28 : bits réservés.
- bit 29 : ce bit est placé si la touche Alt est enfoncée.
- bit 30 : ce bit est placé si la touche est enfoncée avant l'envoi du message (le cas se présente lors d'une répétition de touche).
- bit 31 : placé si la touche est relâchée, nul si la touche est enfoncée.

Ce que nous disons ici est valable sous tous les Windows. Windows XP comporte en outre une nouveauté sous la forme d'un filtre dit de plus bas niveau, baptisé `LowLevelKeyboardProc` et qui permet de différencier les événements en provenance du pilote du clavier de ceux éventuellement injectés dans la file par un autre moyen. Le lecteur intéressé par cette possibilité voudra bien se reporter à la MSDN.

### Notre application

Venons-en à notre exemple. Vous trouverez son code complet sur le Cd-Rom accompagnant le magazine, ceci sous la forme d'un projet Visual C++ 6 et C++Builder 6. Sous Visual C++ l'application n'utilise pas les MFC par souci de simplicité et est une simple application "basée dialogue". Vous trouverez ci-contre un extrait de son code. Il s'agit des fonctions installant ou retirant le hook (encadré 2). Pour en finir avec cela, signalons que l'application doit trouver la dll pour que ça fonctionne. Sous Windows une dll est trouvée, si elle figure dans le répertoire de lancement de l'application, dans les répertoire Windows, à la racine du disque, si un chemin a été défini dans la base de registre, et enfin si elle est dans un répertoire pointé par la variable d'environnement `PATH`. Nous avons choisi la première possibilité et configuré les projets pour qu'application et dll soient déposées dans le même répertoire.

### La solution Ad Hook

Venons en maintenant au coeur du problème, c'est-à-dire la dll contenant le filtre. Vous trouverez le code complet, très court de cette librairie (encadré 3). La fonction de filtre est tout ce qu'il y a de simple. Nous y guetons nos touches. Pour toute autre touche le filtre retourne false

et le message continue son chemin, mais ne passe pas dans d'autres hooks clavier. Il aurait fallu écrire pour cela :

```
return CallNextHookEx(lle_hook, code, wParam, lParam);
```

ce qui nous aurait obligés à conserver le handle du hook dans la dll. Nous ne le faisons pas par souci de ne pas alourdir, mais cela ne pose pas de difficulté technique. Nous faisons également attention à ne pas traiter deux fois (appui et relâchement) une même touche. Quand les touches qui nous intéressent arrivent dans le filtre, nous retirons le message de la file, purement et simplement. Bien entendu cela nous oblige à envoyer un autre message à la place. Comme rien ne nous interdit d'envoyer un message d'un autre type que celui filtré, nous choisissons d'envoyer des messages WM\_CHAR. Ceci présente l'avantage de la simplicité, la plupart des éditeurs travaillant avec des contrôles d'édition traitant directement ce message. Mais notre problème est alors de poster un message pour ce contrôle précis et non pour sa fenêtre parent qui pourrait bien l'intercepter. En effet, certaines applications traitent en dur les touches et les convertissent elles-mêmes en char. Pour résoudre notre problème, nous employons un procédé astucieux, quoique lui aussi très simple. Nous partons du principe, que les caractères à insérer le sont pour la fenêtre active. Nous obtenons celle-ci, via l'API GetForegroundWindow. Ensuite, continuant avec le principe que le contrôle dans lequel nous voulons insérer les caractères est celui qui détient la focalisation, nous énumérons, via l'API EnumChildWindows tous les contrôles enfants de la fenêtre principale. Quand nous trouvons ce contrôle dans la fonction de rappel de EnumChildWindows nous postons nos messages. Ce procédé fonctionne très bien avec C++Builder ou Visual Studio .Net par exemple, car ceux-ci utilisent des contrôles de classe Edit. D'autres outils, surtout les outils Java travaillent fréquemment avec les touches brutes uniquement, sans contrôles d'édition sous-jacents. C'est le cas de JBuilder ou de Sun One Studio, par exemple. Si l'on veut agir sur eux, il convient de poster des messages WM\_KEYDOWN et WM\_KEYUP plutôt que WM\_CHAR. Le lecteur intéressé modifiera sans difficulté notre librairie d'exemple. Nous pourrions apporter d'autres améliorations. Ainsi, il serait pertinent que notre petit utilitaire s'icônifie dans la zone de statut de la barre des tâches. Nous traiterons probablement cela dans un prochain article, la barre des tâches de Windows étant un sujet lui aussi passionnant.

### Encadré 1 Piège à crochet

Écrire une fonction de filtre pour un hook n'est pas difficile en règle générale. Toutefois, il importe d'être attentif à la nature même du hook qui est d'être invoqué lorsqu'un message ou un événement se produisent. Si, dans le filtre, le code génère un événement semblable, le dit filtre va être invoqué en boucle, apportant des comportements aberrants ou, au mieux, un ralentissement considérable du système. Prenons l'exemple d'un hook de type WH\_FOREGROUNDIDLE. Son filtre sera invoqué chaque fois qu'une application est sur le point d'entrer dans un état d'activité, ce qui concrètement signifie qu'il n'y a plus de messages dans sa file. Le filtre de ce hook pourrait être ceci :

```
BOOL idle;
DWORD ForegroundIdleProc(int code, WPARAM wParam, LPARAM lParam)
{
```

```
if(code == HC_ACTION && !idle)
{
    ::MessageBox(NULL, "Application Idle", "", MB_OK);
    idle = TRUE; //NON!!
    return 0;
}
else
    return CallNextHookEx(GlobalHookIdle,
code, wParam, lParam);
}
```

Contre toute attente, ce filtre va être invoqué en boucle. Même si la boîte de dialogue ouverte par l'API MessageBox n'appartient pas à la fenêtre de l'application comme ici, son ouverture provoque l'émission de messages (programmez un hook pour connaître lesquels ;) dans la file d'attente. Ces messages sont retirés par la pompe à messages de l'application et au dernier, la mécanique est relancée. Ainsi le booléen idle n'est pas positionné comme on le souhaiterait, et une quantité pléthorique de boîtes de dialogues surgit à l'écran. Pour éviter cela, il suffit de positionner le booléen avant toute autre chose, comme ceci :

```
BOOL idle;
DWORD ForegroundIdleProc(int code, WPARAM wParam, LPARAM lParam)
{
    if(code == HC_ACTION && !idle)
    {
        // OUI!!
        idle = TRUE;
        ::MessageBox(NULL, "Application Idle", "", MB_OK);
        return 0;
    }
    else
        return CallNextHookEx(GlobalHookIdle,
code, wParam, lParam);
}
```

### Encadré 2 Extrait de l'application qui installe ou retire un filtre clavier.

```
HINSTANCE HookClavierDll;
HHOOK MonHook;

void InstallHook()
{
    HookClavierDll = ::LoadLibrary("hookclavierdll.dll");
    if(HookClavierDll == NULL)
    {
        ::MessageBox(hDialog,
            "Erreur de chargement de la librairie HookClavierDll",
            "Appli Hook Clavier",
            MB_OK);
        ::SendMessage(hDialog, WM_CLOSE, 0, 0);
    }
    // installation du hook
```

```

MonHook = ::SetWindowsHookEx(WH_KEYBOARD,
    reinterpret_cast<HOOKPROC>
        (GetProcAddress(HookClavierDll, "KeyboardProc")),
    HookClavierDll, NULL);

if(MonHook == NULL)
{
    ::MessageBox(hDialog,
        "Erreur de chargement de la procédure de hook",
        "AppliHookClavier",
        MB_OK);
    ::SendMessage(hDialog, WM_CLOSE, 0, 0);
}

void RemoveHook()
{
    if(MonHook)
    {
        ::UnhookWindowsHookEx(MonHook);
        MonHook = NULL;
    }
    if(HookClavierDll)
    {
        ::FreeLibrary(HookClavierDll);
        HookClavierDll = NULL;
    }
}

```

### Encadré 3 La dll contenant notre filtre clavier.

```

#include <windows.h>

extern "C" __declspec(dllexport) bool KeyboardProc(int, WPARAM, LPARAM);

struct enum_mess
{
    WPARAM wParam;
    LPARAM lParam;
};

BOOL CALLBACK EnumChildProc(HWND hwnd, LPARAM lParam)
{
    struct enum_mess *mes;
    char newkey1, newkey2;

    mes = reinterpret_cast<struct enum_mess *>(lParam);
    if(::GetFocus() == hwnd) // si et seulement si la fenêtre à le focus
    {
        switch(mes->wParam)
        {
            case VK_SNAPSHOT:
            {
                newkey1 = '[';

```

```

                newkey2 = ']';
                break;
            }
            case VK_SCROLL:
            {
                newkey1 = '[';
                newkey2 = ']';
                break;
            }
        }
        ::PostMessage(hwnd, WM_CHAR, newkey1, mes->lParam);
        ::PostMessage(hwnd, WM_CHAR, newkey2, mes->lParam);
        return false;
    }
    return true;
}

bool KeyboardProc(int code, WPARAM wParam, LPARAM lParam)
{
    struct enum_mess mes;

    if(code < 0) // Il est interdit de toucher au message dans ce cas
        return false;
    switch(wParam)
    {
        case VK_SNAPSHOT:
        {
            mes.wParam = wParam;
            break;
        }
        case VK_SCROLL:
        {
            if (lParam & 0x80000000) //si la touche est relâchée
                return true; // on coupe simplement le message de la liste
            mes.wParam = wParam;
            break;
        }
        default:
            return false; // on laisse le message continuer son chemin normalement
    }
    mes.lParam = lParam;
    // on envoie le message de substitution dans la 'bonne' fenêtre.
    ::EnumChildWindows(::GetForegroundWindow(),
        reinterpret_cast<WNDENUMPROC>(EnumChildProc),
        reinterpret_cast<long>(&mes));
    return true; // le message original est coupé de la liste
}

int WINAPI DllEntryPoint(HINSTANCE hinst, unsigned long reason, void* lpReserved)
{
    return 1;
}

```

■ Frédéric Mazué - [fmazue@programmez.com](mailto:fmazue@programmez.com)

# Créez des effets spéciaux avec HLSL et DirectX 9



**Maîtrisez la technologie des shaders et créez des images « à la Pixar » (Nemo, Monstres & Cie et le tout nouveau film Les Indestructibles).**

L'année 2004 devait être une année de transition pour DirectX, avec une évolution importante du SDK de Microsoft. La version 9.1 était en effet patiemment attendue par la communauté des développeurs multimédia. Mais cette attente se révéla vaine et Microsoft coupa court à toutes les rumeurs qui annonçaient une évolution prochaine de DirectX pour le début de l'année 2004. La version 9.1 ne verra probablement jamais le jour, ni même la 10 d'ailleurs.

## Direct3D est mort, longue vie à WGF !

Mais l'équipe de développement de DirectX ne se tourne pas les pouces pour autant et travaille d'arrache-pied sur l'évolution majeure du SDK, avec l'abandon confirmé de Direct3D par Nvidia et ATI lors du dernier ECTS de Londres. Direct3D, qui est, rappelons-le, la composante 3D de DirectX, sera donc définitivement remplacé par WGF 1.0 (Windows Graphic Foundation) qui arrivera en même temps que la prochaine génération de cartes graphiques. Ce même WGF sera la base d'Avalon, l'interface graphique de Windows Longhorn, le futur système d'exploitation de chez Microsoft et devrait être disponible, nous l'espérons, en 2006. Cette évolution majeure de l'API prendrait donc logiquement le numéro de version 1.0. Aucune évolution, même mineure, du SDK n'est à prévoir d'ici là, cependant les développeurs DirectX se sont vu proposer l'été dernier une nouvelle version du SDK, la 9.0c qui annonce donc l'activation de nouvelles fonctionnalités, notamment liées aux shaders 3.0. Ces fonctionnalités étaient déjà présentes avec la version 9.0b, mais elles restaient inactives pour la simple et bonne raison que les cartes 3D compatibles avec cette technologie n'étaient pas encore disponibles sur le marché. Cette "nouvelle version" du SDK n'est donc pas révolutionnaire, mais elle nous donne l'occasion de vous présenter la dernière technolo-

gie en vogue dans le monde de la 3D et qui se dissimule derrière l'acronyme mystérieux d'HLSL. (Fig.1)

## HLSL, l'ami du programmeur shaders

Depuis quelques années et la version 8.0 du SDK DirectX, le programmeur 3D doit composer avec un nouveau composant fondamental pour Windows : le composant Direct Graphics. Avec la version 9.0, ce composant intègre la principale innovation pour les moteurs 3D modernes avec la technologie de programmation dite des "shaders" (parfois étrangement traduit par "nuanceurs"). Ces fameux shaders offrent des possibilités de programmation modulaire autour d'effets spéciaux spectaculaires. Les shaders recoupent en fait deux concepts distincts : les Pixel Shaders et les Vertex Shaders. Les Pixel Shaders se concentrent sur les pixels constituant les primitives, alors que les Vertex Shaders se concentrent sur les primitives en elles-mêmes ainsi que sur les lumières qui leur sont associées. C'est ainsi que sont par exemple programmés les effets aquatiques, à base de petits programmes de Vertex Shaders permettant la manipulation de formes géométriques. Ensuite, pour simuler la texture de l'eau, on appliquera le process d'un Pixel Shader sur la surface liquide sur laquelle se dessineront les reflets de l'environnement extérieur. L'illusion ainsi créée étant presque parfaite, le réalisme visuel devient optimal.



Le jeu "Les indestructibles", éditeur THQ. On reconnaît les effets de shader.



Figure n°1 : le SDK DirectX 9.0c regorge d'exemples concrets avec codes sources disponibles.

Malheureusement, de réputation, la programmation des shaders demeure un exercice assez complexe, car elle imposait de coder ces effets dans un langage machine proche de l'Assembleur, et qui porte le nom de langage Cg (prononcez "ci ji").

Heureusement, le nouveau langage HLSL dédié aux shaders dans DirectX 9.0 est un langage standard de haut niveau, relativement éloigné du langage assembleur de bas niveau. HLSL signifie littéralement High Level Shading Language autrement dit "Langage de Shaders de Haut Niveau", par opposition au langage assembleur de bas niveau utilisé auparavant. Il permet aux développeurs de shaders de se consacrer aux algorithmes uniquement lorsqu'ils implémentent des shaders, plutôt que de se préoccuper des détails matériels complexes, tels que l'allocation de registres, les

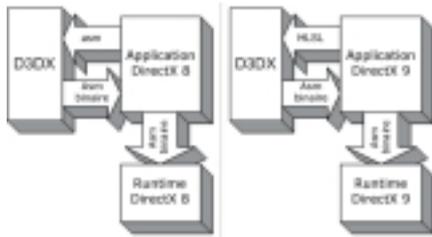


Figure n°2 : Avant (DirectX 8) et Après (DirectX 9)  
(source MSDN)

limites ReadPort (ports de lecture) des registres, l'émission conjointe d'instructions, etc. Outre l'avantage de détacher le développeur des contingences matérielles, le langage HLSL présente tous les avantages habituels d'un langage de haut niveau, tels que la réutilisation facile du code, une lisibilité améliorée et la présence d'un compilateur d'optimisation. C'est ainsi que DirectX 9.0 fournit depuis près d'un an maintenant ce langage de haut niveau, proche du langage C au niveau de la syntaxe, avec la possibilité de construire ses propres type de données (et les célèbres "structures" du langage C), un ensemble de types natifs (entiers, booléens, flottants...), tableaux, matrices carrées (n'oublions pas que nous travaillons en 3D), etc. (Fig. 2)

## Les capacités du langage

En tant que fonctionnalités majeures de DirectX, le HLSL va modifier définitivement les techniques de programmation des shaders. En effet, la croissance des capacités et des performances hardware, comme l'ajout d'étapes de texture ou l'augmentation du nombre d'instructions, impliquent une utilisation des shaders en temps réel de manière plus complexe et plus puissante. Bien entendu, développer des algorithmes complexes qui seront codés

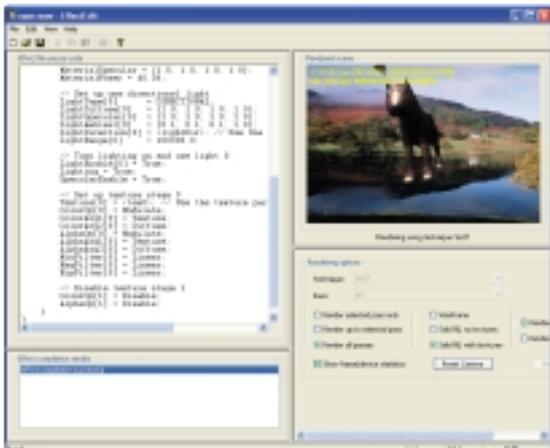


Figure n°3 : l'interface de l'outil Effect Edit est sobre et dépouillée, mais efficace.

## Aparté : les fonctions dites " intrinsèques "

Un certain nombre d'intrinsèques générés dans le langage HLSL existent et sont mis à la disposition du programmeur avec DirectX 9.0. De nombreux intrinsèques, tels que des fonctions mathématiques, sont facultatifs, alors que d'autres, tels que les fonctions `texD()` et `tex2D()`, sont nécessaires pour accéder aux données de texture, via des échantillonneurs (voir tableau suivant).

Fonctions intrinsèques	Utilisation	Description
<b>abs</b>	value abs(value a)	Valeur absolue (par composant).
<b>cross</b>	cross(a, b)	Renvoie le produit vectoriel de deux vecteurs 3-D, a et b.
<b>dot</b>	dot(a, b)	Renvoie le produit scalaire de deux vecteurs 3-D, a et b.
<b>lerp</b>	lerp(a, b, s)	Renvoie $a + s(b - a)$ . Il y a interpolation linéaire entre a et b, ce qui signifie que la valeur renvoyée est a si s est égal à 0 et b si s est égal à 1.
<b>max</b>	max(a, b)	Sélectionne la valeur la plus élevée entre a et b.
<b>min</b>	min(a, b)	Sélectionne la valeur la plus basse entre a et b.
<b>mul</b>	mul(a, b)	Exécute une multiplication matricielle entre a et b. Si a est un vecteur, il est traité comme un vecteur ligne. Si b est un vecteur, il est traité comme un vecteur colonne. Les dimensions internes accolées et blignes doivent être égales. Le résultat a la dimension alignes x bcolonnes.
<b>normalize</b>	normalize(v)	Renvoie le vecteur normalisé $v / \text{longueur}(v)$ . Si la longueur de v est égale à 0, le résultat est indéfini.
<b>pow</b>	pow(x, y)	Renvoie x à la puissance y.
<b>rsqrt</b>	rsqrt(x)	Renvoie $1 / \text{racine carrée}(x)$ .
<b>sin</b>	sin(x)	Renvoie le sinus de x.
<b>sqrt</b>	value sqrt(value a)	Racine carrée (par composant).
<b>tex2D</b>	tex2D(s, t)	Recherche de texture 2-D. s est un échantillon ou un objet sampler2D. t est une coordonnée de texture 2-D.
<b>tex3D</b>	tex3D(s, t)	Recherche de texture de volume 3-D. s est un échantillon ou un objet sampler3D. t est une coordonnée de texture 3-D.
<b>texCUBE</b>	TexCUBE(s, t)	Recherche de texture de cube 3-D. s est un échantillon ou un objet samplerCUBE. t est une coordonnée de texture 3-D.

ensuite en langage machine Assembleur devient une mission impossible. D'autre part, la multitude de périphériques disponibles sur le marché (et des cartes graphiques notamment) n'arrange pas les affaires de nos programmeurs 3D. Avec sa syntaxe C qui facilite l'apprentissage et son ensemble de types prédéfinis pour les scalaires, les vecteurs et les matrices, le HLSL prend également en charge un grand nombre de fonctions intrinsèques qui simplifient certaines tâches rebutantes comme les transformations 3D.

## Les outils de programmation HLSL

Bien évidemment, DirectX 9.0c s'intègre parfaitement dans l'environnement Visual Studio .NET. Cependant, l'équipe de développement de DirectX a eu la bonne idée de proposer un outil fort pratique pour la création et l'évaluation des shaders. Cet outil se trouve dans le SDK DirectX et permet de pro-

grammer directement des shaders sans passer par Visual C++. Après avoir installé le SDK (présent sur le CD-Rom d'accompagnement), vous pouvez lancer l'outil Effect Edit en sélectionnant Démarrer > Microsoft SDK DirectX 9.0 update (Summer 2004) > DirectX utilities > Effect Edit

L'interface d'Effect Edit est sobre, tant mieux, elle permet d'accéder directement aux fonctionnalités principales. (Fig. 3)

La fenêtre principale qui se nomme Effect file source code affiche, comme son nom l'indique, le code source d'un fichier d'extension .fx. Sans entrer dans les détails, il faut savoir que le code source d'un shader avec DirectX peut s'intégrer dans un fichier texte de type fx. La fenêtre de droite, Rendered scene, permet de visualiser en temps réel l'effet obtenu en programmant ce shader. Vous comprenez ici tout l'intérêt de cet outil, il devient possible de programmer un shader et de visualiser directement son effet en temps réel.

La fenêtre de gauche en bas, Effect Compiling results permet d'afficher l'état de la compilation du shader, ainsi que les éventuels mes-

sages d'erreurs, et la fenêtre Rendering Options permet, elle, de sélectionner les paramètres de visualisation du shader. Pour résumer, Effect Edit est un outil WYSIWYG permettant de programmer et d'éditer des shaders.

## La preuve par l'exemple avec les fichiers fx

Inutile de décrire plus en profondeur l'intérêt des shaders pour la programmation 3D, permetons vers un exemple concret pour se convaincre définitivement de ses performances. Nous allons utiliser pour cela les modèles 3D et textures disponibles avec le SDK de Microsoft ainsi que quelques exemples de fichiers fx disponibles aussi sur le SDK.

Un fichier fx est généralement écrit en 3 temps distincts :

- 1 - définition des variables globales et paramètres de l'environnement 3D
- 2 - définition de la fonction du Vertex Shader
- 3 - définition de la fonction du Pixel Shader
- 4 - définition de la ou des techniques (voir plus loin)

```
// Globales
// Screen space transformation matrix
float4x4 g_mTot : WorldViewProjection;
```

Commençons par les fondamentaux du langage HLSL avec Direct3D. L'effet suivant utilise un Vertex Shader et un Pixel Shader pour transformer la position à l'écran et la couleur des pixels affichés. Nous définissons en premier lieu une matrice globale, à partir de laquelle le shader peut lire la matrice de transformation WorldViewProjection, qui indique à quelles données ce paramètre doit être lié. C'est l'application qui est chargée de mettre à jour la valeur de ce paramètre pour chaque trame utilisant la méthode D3DXEffect::SetMatrix( ) (voir l'excellente documentation du SDK DirectX 9.0 pour plus de précision sur cette méthode).

```
// Mesh file for Effect Edit to load
string XFile = "bust.x";
```

Ensuite, nous définissons une variable de type string pour désigner le modèle 3D sur lequel sera affecté le shader. Il est en effet indispensable d'utiliser un objet 3D (fichier d'extension .x pour DirectX) pour visualiser en temps réel l'effet programmé. Enfin, nous commençons par définir une fonction spécifique au Vertex Shader. Cette dernière utilise le mul( ) intrinsèque avec la matrice combinée WorldView

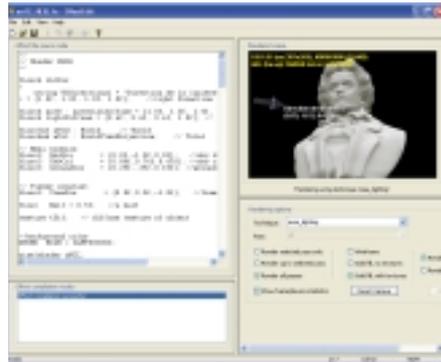


Figure n°4 : Eclairage et ombrage d'un modèle 3D avec les shaders et le HLSL

Projection pour transformer la position entrée en élément de l'espace d'affichage, afin qu'elle soit prête à être dessinée.

### Vertex Shader

```
struct VS_OUTPUT
{
    float4 Pos : POSITION;
};

VS_OUTPUT SimpleTransform(float4 iPos : POSITION)
{
    VS_OUTPUT o;

    // Project the position into screen space
    o.Pos = mul(iPos, g_mTot);

    return o;
}
```

La troisième étape de l'écriture d'un shader consiste à définir la fonction du Pixel Shader. Par exemple, cette fonction affiche un simple pixel bleu opaque dans le tampon de trame :

### Pixel Shader

```
struct PS_OUTPUT
{
    float4 Color : COLOR;
};

PS_OUTPUT ColorBlue()
{
    PS_OUTPUT o;
    float4 Color={0.0f, 0.0f, 1.0f, 1.0f};

    o.Color = Color;

    return o;
}
```

Pour finir, nous ajustons une "technique", autrement dit nous définissons une technique spécifiant le matériel cible utilisé pour les shaders :

### Technique

```
technique t0
{
    pass p0
    {
        VertexShader = compile vs_1_1 SimpleTransform();

        PixelShader = compile ps_1_1 ColorRed();
    }
}
```

## Exemple concret : l'utilisation de shaders pour l'éclairage

Grâce à sa flexibilité, le langage HLSL permet au développeur qui souhaite effectuer une tâche d'ombrage de se concentrer sur les calculs nécessaires pour reproduire l'effet désiré, et lui évite d'allouer les ressources matérielles pour réaliser la tâche en question. Le fichier shaders.fx que vous trouverez en complément à ce dossier sur le CD-Rom vous propose un exemple concret d'éclairage et d'ombrage sur un modèle 3D. Vous pouvez visualiser les deux techniques développées et les comparer en la sélectionnant dans la fenêtre Rendering Options de l'interface d'Effect Edit (Fig. 4).

## Que nous réserve l'avenir ?

Le développement de shaders en assembleur est aujourd'hui dépassé. Avec le langage HLSL il est facile de créer des shaders puissants, flexibles et riches en fonctionnalités et d'obtenir l'apparence que vous recherchez.

Cependant, la mort annoncée de Direct3D en 2006 pourrait remettre en cause certains fondamentaux pour la programmation 3D sous environnement Windows ou X-Box. Qu'en est-il du langage HLSL ? Il va sans dire que l'avantage de ce langage de haut niveau sur le langage assembleur est tel qu'il semble impensable pour Microsoft de revenir sur la pertinence de son existence. Il est donc fort probable que WGF reprenne en partie, ou intégralement, peut-être sous un autre nom, ce langage, avec l'implémentation tant attendue des Shaders 4.0. Aucun risque donc de voir ce langage disparaître prochainement.

■ Laurent Jayr - tech@tsm-internet.com