Patrick Legand

sans tabou

Préface de **Benjamin Arnault (HSC)**

Sécuriser enfin son PC

Réflexes et techniques contre les virus, spams, phishing, vols et pertes de données

ISBN : 2-212-12005-2, ISBN 13 : 978-2-212-12005-9

EYROLLES

Et Windows Vista ?

Avec l'arrivée de Windows Vista, la firme de Redmond se retouve une fois de plus au cœur de la polémique. Restant fidèle à la politique marketing affichée par Microsoft depuis plusieurs années, Vista propose des évolutions de sécurité importantes. Malheureusement, elles ne profiteront pas toujours à l'utilisateur.

SOMMAIRE

MOTS-CLÉS

- DRM
- cryptologie « en dur »
- monopole
- choix technologiques
- interopérabilité
- TCPA
- Palladium-NGSCB

Avant d'évoquer les nouvelles fonctions de sécurité du système, remarquons d'emblée que Vista est le signe que les éditeurs veulent reprendre énergiquement en main la lutte contre le piratage de logiciels et le téléchargement sauvage de fichiers soumis à des droits.

Derrière le sigle DRM (Digital Rights Management), Microsoft propose en effet un nouveau mode de contrôle d'accès aux contenus (musique, vidéos...), de nature à révolutionner significativement le comportement des utilisateurs qui migreront vers Vista et les nouvelles architectures TCPA (Trusted Computer Platform Alliance), sur lesquelles le nouveau système va fonctionner.

RÉFÉRENCE DADVSI

La loi DADVSI (Droits d'auteurs et droits voisins dans la société de l'information) protège les mesures techniques de protection des contenus. Vous trouverez davantage d'informations concernant ses conséquences dans l'ouvrage suivant :

📖 *Peer-to-peer, comprendre et utiliser*, Fabrice Le Fessant, Éditions Eyrolles, 2006.

Conséquences du contrôle d'accès généralisé aux contenus

TECHNOLOGIE DRM

Nous avons vu, tout au long de cet ouvrage, la puissance dont font preuve les mécanismes cryptologiques en ce qui concerne l'élaboration de documents infalsifiables et l'établissement de canaux chiffrés impénétrables entre la station de l'utilisateur et le serveur disant.
Faisant un usage massif de la cryptologie, les DRM sont fondés sur des mécanismes forts, qui bénéficient par ailleurs d'une robustesse d'autant plus élevée que les services cryptologiques sont désormais implantés profondément au cœur de la machine, à l'intérieur de puces matérielles soudées sur la carte mère.
Sans détailler le fonctionnement des DRM, tentons de comprendre la philosophie de ce concept à travers un cas d'utilisation : l'achat de musique sur Internet. Vous naviguez donc sur votre site marchand habituel, passez commande pour le morceau de musique de votre choix, réglez cette commande et lancez le téléchargement du fichier sur votre ordinateur. Très simple à première vue, cette opération cache une réalité plus complexe, car vont se dérouler en toile de fond plusieurs opérations dédiées à la gestion des droits d'accès :

1. Le fournisseur vous envoie non pas le fichier, mais un paquetage dans lequel se trouvent plusieurs éléments :
   - le fichier musical chiffré au moyen d'un algorithme symétrique et d'une clé secrète distribuée séparément ;
   - des informations diverses relatives au fournisseur ;
   - l'URL du centre de vérification des licences, à partir de laquelle la clé de déchiffrement peut être téléchargée.

RENVOI Cryptologie

Voir l'annexe A.

2. En utilisant un procédé assez similaire à celui mis en œuvre par les AC pour élaborer un certificat, le serveur établit un petit fichier qui contient la clé secrète de déchiffrement ainsi qu'une liste de règles décrivant précisément ce que l'utilisateur a le droit de faire avec le morceau de musique. Ce fichier s'appelle par exemple « licence » et le serveur le poste vers un centre de vérification spécial. Cette licence demeure aussi infalsifiable que le certificat émis par une AC : elle est signée cryptologiquement, donc si quelqu'un réussissait à modifier frauduleusement son contenu, par exemple pour étendre ses droits d'utilisation, ce serait peine perdue puisque le lecteur multimédia détecterait immédiatement la fraude en vérifiant la signature. Il refuserait donc de lire le morceau.
3. Vous recevez votre morceau de musique empaqueté et chiffré.
4. Vous souhaitez écouter votre morceau ; vous lancez donc un lecteur multimédia – attention, pas n'importe lequel comme nous allons le voir – par exemple Windows Media Player.
5. Constatant que le fichier est protégé par un DRM, le lecteur lance une requête auprès du centre de validation des licences afin qu'il lui fournisse la clé secrète nécessaire au déchiffrement. Bien entendu, le lecteur, qui a été conçu spécialement pour s'intégrer dans la chaîne de gestion des DRM, joint à cette requête toutes les informations nécessaires, par exemple le numéro de série de votre ordinateur.
6. Le serveur met alors à jour votre « fiche client », en inscrivant le numéro de série du morceau de musique et celui de l'ordinateur sur lequel vous voulez l'écouter.
7. Par un canal sûr (il faut protéger la clé secrète), le serveur envoie la licence à votre lecteur, qui la range bien soigneusement quelque part sur votre disque dur.
8. Exactement comme le navigateur lorsqu'il reçoit le certificat numérique d'un correspondant, le lecteur vérifie l'authenticité et l'intégrité de la licence et de son contenu, puis il finit par déchiffrer le fichier pour que vous puissiez l'écouter, s'il s'avère que vous avez effectivement ce droit.

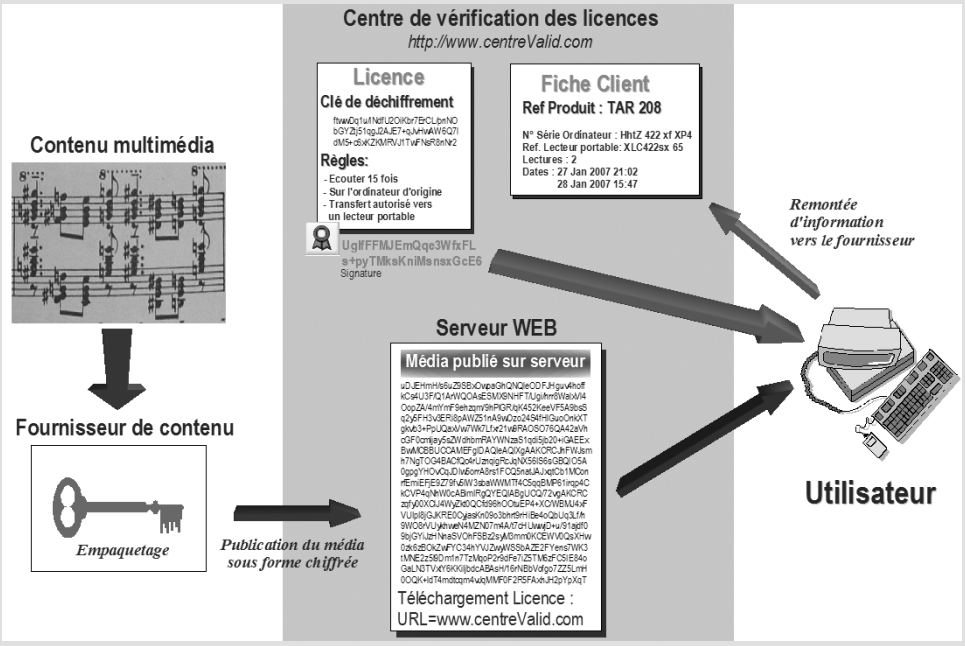

Figure 10–1 Principe de fonctionnement des DRM

RENVOI **Certificats et autorités de certification**

Voir le chapitre 6.

Vous pouvez d'ores et déjà constater les mécanismes plus « musclés » qu'il faut employer pour tenter de contourner ces protections. Franchement, on peut souhaiter bon courage aux as du piratage !
Maintenant, si vous transférez le morceau sur une autre machine, inutile de transférer aussi la licence car, en comparant les numéros de série, le lecteur saura tout de suite qu'elle n'a pas été attribuée à cet ordinateur. Le lecteur situé sur le nouvel ordinateur va donc recontacter le serveur pour obtenir une nouvelle licence. Votre « fiche client » sera ainsi mise à jour et le serveur tiendra soigneusement la comptabilité de ce que vous faites avec ce morceau.
Au bout d'un certain nombre de transferts, qui dépend du droit que vous avez acquis au moment de l'achat, le serveur refusera d'accorder une nouvelle licence. Il faudra soit « démonter » une licence sur un ordinateur pour la transférer sur une autre machine, le tout sous contrôle du serveur marchand, soit remettre la main à la poche.
Bien entendu, le fournisseur de contenu se réservera le droit de définir toutes les règles qu'il souhaite dans le fichier de licence, par exemple imposer un droit de lecture limité dans le temps, définir le nombre de lectures autorisées, autoriser ou interdire la gravure du morceau sur CD audio, etc.

En fermant les yeux sur certains détails gênants comme une certaine forme d'atteinte à la vie privée, il n'y a rien de vraiment choquant dans cette démarche, juste une réponse d'éditeur au piratage généralisé d'œuvres artistiques. Après tout, c'est de bonne guerre.

Plus préoccupantes en revanche sont les implications potentielles d'un tel modèle :

- la signature des pilotes et des exécutables ;
- la dépendance vis-à-vis du fournisseur ;
- la dépendance technologique et l'absence d'interopérabilité.

Signature des pilotes et des exécutables

Pour s'affranchir du modèle exposé précédemment, non pour cautionner le piratage mais simplement pour préserver une liberté individuelle au moins équivalente à celle que nous offrait le disque, on pourrait très bien imaginer avoir recours à un autre type de lecteur (Open Source ou autre), dans lequel les fonctions DRM seraient implémentées autrement. Bien entendu, les éditeurs et les majors n'y ont absolument aucun intérêt. Pour eux, l'enjeu est d'interdire l'exécution sur la machine de lecteurs multimédia « dissidents ». Ils tiennent absolument à ce que seuls des lecteurs en quelque sorte « agréés » DRM soient accessibles aux utilisateurs.

Il existe un moyen très simple et pratiquement incontournable pour parvenir à cet objectif : la signature numérique des pilotes et des exécutables.

Autrement dit, pour verrouiller ce modèle, le système d'exploitation – Vista en l'occurrence – est conçu spécialement pour autoriser sur la machine exclusivement les pilotes et les exécutables que Microsoft veut bien voir entre les mains de l'utilisateur, c'est-à-dire des composants auxquels il aura apposé sa signature. Ces principes sont exactement les mêmes que pour la technologie « Authenticode », à la différence que c'est Microsoft qui délivre la signature.

Renvoi Technologie Authenticode

Voir le chapitre 7.

En soi, obtenir une signature électronique de Microsoft n'est pas une procédure terriblement compliquée. Ce qui pose problème, c'est le fait que Microsoft et une poignée d'industriels, agissant à la fois en tant que juges et parties, s'arrogent le droit d'autoriser tel fournisseur, de mettre des bâtons dans les roues de tel autre, de faire barrage à telle ou telle technologie et de forcer l'utilisateur à n'exécuter sur sa machine que les applications souhaitées par lesdits industriels. C'est une nouveauté et elle est très mal perçue, notamment par la communauté du logiciel libre qui y voit clairement une menace.

Dépendance vis-à-vis du fournisseur

Comme le montre le cas d'utilisation précédent, un tel schéma impose à l'utilisateur, déjà en possession du produit (ou plus exactement du droit à sa lecture), de rester en relation avec son fournisseur via Internet s'il veut avoir une chance de jouir du produit. Par conception, cette nouvelle architecture obligera l'utilisateur à être en ligne beaucoup plus que par le passé, et à entretenir des relations beaucoup plus étroites avec son fournisseur, auquel, inévitablement, il rendra compte de ses faits et gestes.

S'il a été prévu de longue date que les nouvelles technologies réduiraient à terme l'espace de la vie privée, nous sommes ici en présence d'un modèle qui rend tout à fait possible le suivi à distance et en temps réel de ce que lit l'individu.

Cependant, il y a plus grave. Les communications entre le poste de l'utilisateur et le fournisseur s'effectuent à travers un tunnel chiffré, pour protéger les conversations. Pourtant, au-delà de l'échange de simples licences et de morceaux de musique, qui nous assure que ce canal opaque ne servira pas à transférer à des sociétés privées des informations beaucoup plus personnelles sur nos faits et gestes, les applications installées, éventuellement des fichiers personnels ou professionnels, des contenus de messagerie... Plusieurs chapitres dans ce livre ont montré l'existence de ce type de menace et des mécanismes pour les réaliser ; les dérives potentielles des DRM risquent d'en devenir le mécanisme légalisé.

Dépendance technologique et absence d'interopérabilité

On constate aussi une autre chose : en dépit de l'existence de standards ouverts en matière de DRM, les formats de fichiers gérés par les composants « agréés » sont propriétaires et fermés. En admettant que les éditeurs réussiront à imposer leurs propres standards aux fournisseurs de contenus, ils obligeront les utilisateurs à opter pour les « bons » lecteurs.

Le processus est d'ailleurs en marche. On ne peut que constater la mainmise grandissante de Microsoft sur le contrôle d'accès aux contenus : il fournit tous les composants de la chaîne de gestion des DRM, des lecteurs multimédia aux serveurs de DRM chez le fournisseur, en passant par le format du fichier. Si l'utilisateur dispose de Windows, il sera tiré d'affaire. En revanche, s'il est sur Linux, il est coincé : il n'y a pas de lecteur Open Source interopérable avec les lecteurs « agréés ». Belle perspective !

Au bout du compte, le noble sentiment d'une informatique mieux sécurisée semble bien loin ; les DRM ne font qu'entériner la légalisation du verrouillage des contenus. C'est comme s'il s'agissait de trouver un prétexte pour imposer un contrôle absolu sur des processus destinés à conserver un marché captif pour des éditeurs de plus en plus menacés par la montée du logiciel libre, ou à des maisons de disques qui, pour survivre, tentent de substituer au disque le concept de droit d'écoute (donc le DRM).

TCPA, Palladium et NGSCB

La TCPA (Trusted Computing Platform Alliance, Alliance pour une informatique de confiance) désigne un groupe de travail créé par Intel en 1999, et qui réunit aujourd'hui la fine fleur de l'industrie informatique américaine, soit plus de 200 industriels. L'objectif de la TCPA est de définitir une nouvelle architecture matérielle, qui intègre la sécurité dès le départ. Le but affiché est clairement de s'armer contre le fléau des attaques sur Internet, et de rendre l'ordinateur plus sûr.

Les travaux du groupe débouchent aujourd'hui sur la réalisation d'une plate-forme de nouvelle génération, dite « TCPA » : s'appuyant sur la collaboration des principaux fondeurs (AMD, Intel), les plates-formes TCPA intègrent désormais une puce spéciale, à l'intérieur de laquelle plusieurs briques de sécurité sont implémentées, dont un ensemble complet de mécanismes cryptologiques. Ces mécanismes, bâtis sur des algorithmes fiables par nature, font maintenant partie intégrante du matériel et sont capables d'offrir des services de sécurité de haut niveau, très difficilement contournables. De la cryptologie forte en natif dans le cœur du matériel, c'est déjà une petite révolution.

En soi, l'initiative de la TCPA est tout à fait recevable : combattre les piratages en tous genres, à commencer par les attaques à répétition tirant parti des multiples vulnérabilités du système d'exploitation, tout le monde le réclamait.

Cependant, les possibilités techniques offertes par ces nouveaux et puissants mécanismes ouvrent la voie à des dérives qui, cette fois, sont loin d'emporter l'adhésion des utilisateurs. Microsoft fait partie de cette alliance. Compte tenu de sa position dominante, son pouvoir d'influence sur la finalité de TCPA est immense. En s'appuyant sur l'infrastructure sécurisée de TCPA, Microsoft a bâti sa propre architecture logicielle de sécurité, Palladium, rebaptisée pudiquement NGSCB (Next-Generation Secure Computing Base), en raison d'une violente polémique qui secoua la communauté des utilisateurs, et de la mauvaise réputation acquise in fine par Palladium. Aujourd'hui, NGSCB-Palladium constitue l'un des fondements de la sécurité de Vista.

Faisant abstraction de la méfiance suscitée par le déploiement prochain de Palladium, il faut reconnaître que les mécanismes de cet édifice contribueront incontestablement à améliorer la sécurité des ordinateurs. Citons quelques exemples :

- Palladium est conçu pour qu'il y ait authentification des logiciels et des matériels au sein de la machine. Traditionnellement, la notion d'authentification sous Windows nous laisse comme un sentiment de légèreté (hormis peut-être avec XP ou Server 2003). Avec Palladium, l'authentification s'appuie sur des mécanismes cryptologiques implémentés dans le matériel ; très sincèrement, réussir une attaque demandera une bonne dose de talent ! Corrolaire, Palladium est censé garantir que seuls les logiciels autorisés pourront s'exécuter sur la machine ; difficile, dans ce cas, d'insérer un cheval de Troie.
- Les données sensibles sont écrites dans la mémoire vive spéciale située à l'intérieur de la puce cryptologique, accessible uniquement par des moyens sécurisés ou des logiciels autorisés ; les attaques basées actuellement sur l'interception d'une clé de déchiffrement – ou de toute information sensible – présente dans la mémoire vive risquent de devenir un tantinet plus compliquées.
- Avec Palladium, le dialogue entre certains composants de la machine se fait au travers de canaux chiffrés (les claviers pourront par exemple être dotés d'une puce cryptologique) ; là aussi, le piratage devient plus complexe.

Il ne s'agit là que de quelques exemples parmi d'autres, mais il faut honnêtement remarquer qu'en ce qui concerne l'attaque des machines TCPA/Vista, les pirates du monde entier risquent d'avoir du fil à retordre.

Cependant, tout n'est pas rose, loin de là. Nous savons de longue date que les éditeurs cherchent à renforcer le contrôle sur les activités de leurs clients ; les plates-formes TCPA, combinées aux riches mécanismes contenus dans la technologie Palladium–NGSBP, risquent fort de leur en donner les moyens, réduisant d'autant l'espace de liberté de chacun.

Il est difficile de prévoir les impacts sur le modèle économique à terme, d'autant que Microsoft fait tout ce qu'il peut pour afficher un discours rassurant – tout au moins tant que TCPA, NGSBP et les DRM ne seront pas suffisamment déployés et adoptés par les fournisseurs de contenus. Sachons toutefois qu'il est désormais techniquement possible de :

- rendre inaccessibles les programmes estampillés NGSCB si celui-ci est désactivé ;
- empêcher l'installation de logiciels non dotés d'une signature valide (la signature est attribuée par Microsoft ou les éditeurs sous l'œil de Microsoft) ;
- maintenir le contact permanent avec l'éditeur au travers de flux chiffrés, le tout en dehors du contrôle de l'utilisateur ;
- informer l'éditeur des applications présentes sur la machine de l'utilisateur ;
- ordonner au poste utilisateur d'effacer à distance des fichiers sur sa machine ;
- invalider le fonctionnement de logiciels et verrouiller l'accès aux données qu'ils avaient créées, etc.

Au bout du compte, la dérive principale de la TCPA–Palladium–NGSBC est d'amener progressivement l'ordinateur sous le contrôle des constructeurs et des éditeurs, et de garder un œil sur le contenu hébergé par ces machines. Difficile à avaler pour l'utilisateur !

Aller plus loin La sécurité délivrée par TCPA–Palladium

Force est de constater que NGSBC–Palladium est omniprésent lorsqu'il s'agit de réaliser une opération sensible affectant la sécurité des données (authentification, chiffrement d'une donnée, chiffrement à la volée des disques, etc.).

Il faut savoir que toutes ces fonctionnalités, tout au moins celles qui intéressent l'utilisateur ou l'entreprise (authentification sur la machine ou sur le réseau, chiffrement des données en local, établissement de liens chiffrés à distance à travers des tunnels VPN) sont disponibles depuis belle lurette. De plus, lorsque les mécanismes cryptologiques sont implémentés au sein de dispositifs matériels externes, comme les cartes à puce ou les clés USB, le niveau de sécurité est élevé (revoir à ce sujet l'analyse conduite au chapitre 8). En outre, ce type de dispositif laisse à l'utilisateur ou à l'entreprise le choix du constructeur.

TCPA revient en fait à ramener ces mécanismes au cœur de la machine et à imposer une sécurité Microsoft. En clair, lorsque des intérêts nationaux sont en jeu, il faut considérer de que TCPA–Palladium n'offre aucune sécurité.

La sécurité, je fais tout seul

Au-delà de toutes ces constatations, une autre polémique prend actuellement de l'ampleur : accusé encore une fois d'abuser de sa position dominante, Microsoft a choisi d'intégrer ses propres solutions de sécurité dans son système d'exploitation (et pas seulement la sécurité d'ailleurs !), au détriment des produits fournis par ses traditionnels partenaires.

Décidément, Microsoft au centre de questions antitrust, ce débat nous semble déjà familier. Pourtant condamné en 2004 à la suite du conflit sur fond de concurrence déloyale qui l'avait opposé à Bruxelles, Microsoft n'hésite pas à rééditer des pratiques contraires au principe de respect de la libre concurrence. En quelques mots :

- Le Centre de sécurité de Vista s'étoffe et intègre de plus en plus de solutions Microsoft :
  - fonctions anti-malware (virus, vers, logiciels espions) ;
  - pare-feu logiciel ;
  - logiciel anti-spam.
- Avec Windows XP, le Centre de sécurité était capable de s'interfacer avec les produits d'éditeurs indépendants. Sous Vista, cela devient plus difficile. À titre d'information, si Microsoft a récemment consenti à « ouvrir » la porte, c'est uniquement afin d'éviter un nouveau procès antitrust à Bruxelles.
- Habitué à coopérer avec ses partenaires, Microsoft a cette fois fermé aux éditeurs l'accès au code de Vista.
- Face à la pression grandissante des autorités de régulation et des grands groupes tels Symantec, McAfee ou Adobe, Microsoft a finalement consenti à fournir à ses concurrents une interface de programmation qui permettrait d'accéder au noyau de Vista 64-bits. Toutefois, ces éditeurs rencontrent des problèmes techniques, notamment à cause du logiciel PatchGuard (voir plus loin) qui interdit l'écriture dans le noyau en mode protégé.

Au delà des problèmes de stratégie industrielle que l'on comprend parfaitement, il est profondément gênant de constater que cette démarche est en totale contradiction avec un principe dont la pertinence a été maintes fois démontrée au cours de ce livre : la sécurité est une affaire de spécialistes.

Comment imaginer que Microsoft, qui a fait des efforts certes, mais qui est encore loin d'être reconnu dans le domaine de la sécurité, sache atteindre subitement le niveau de performances d'éditeurs de pare-feu comme CheckPoint, ou d'antivirus comme F-Secure ou Kaspersky, dont le métier consiste exclusivement à lutter contre une forme de menaces spécifique ?

Comment comprendre que Microsoft tienne à distance les éditeurs d'antivirus comme F-Secure, Kaspersky, McAfee, Symantec ou Panda (pour ne citer que ceux-là), alors qu'un antivirus est fortement couplé au système d'exploitation ?

Comment penser que Microsoft offrira une meilleure sécurité alors que les spécialistes, sur leurs terrains respectifs, sont parfois tenus en echec ?

Il est clair que Microsoft cherche à dominer sans partage sur tous les marchés du logiciel, à faire de Vista une arme anti-concurrentielle. Malheureusement, cela ne peut avoir lieu qu'au détriment de la sécurité de l'utilisateur.

Améliorations de la sécurité du système

Malgré toutes ces réserves, il y a tout de même un domaine où seul Microsoft a la capacité d'apporter une vraie valeur ajoutée : la sécurité du système d'exploitation, l'environnement qu'il maîtrise.

Si l'on fait abstraction du reste, il convient en effet de noter une amélioration générale des fonctions de sécurité, qui rendront Vista plus sûr que ses prédécesseurs. On peut citer notamment :

- **Protection renforcée des comptes d'utilisateurs** – Afin de limiter notamment la portée des intrusions ou des erreurs de manipulation, le système n'accorde plus par défaut les droits administrateur. Avec Windows XP, cela finit toujours par poser problème lorsqu'un utilisateur travaille avec des droits restreints (il peut avoir du mal à exécuter certaines applications, à définir une nouvelle imprimante, etc.). Vista résout ce problème.
- **Authentification** – Vista simplifie l'intégration de nouvelles méthodes d'authentification, comme la biométrie.
- **Protection de l'accès au réseau** – Il est possible d'empêcher un utilisateur de se connecter au réseau tant que ses mises à jour de sécurité et ses fichiers de définition de virus ne sont pas actualisés.
- **Renforcement de la sécurité d'Internet Explorer** – IE restreint maintenant ses actions en fonction des droits alloués à l'utilisateur. Ce principe tend à diminuer la marge de manœuvre d'un code malveillant exploitant une faille potentielle d'IE, qui tenterait d'éditer le Registre, d'installer des logiciels, ou de copier des fichiers dans le dossier de démarrage de l'utilisateur. Cependant, cet avantage reste mineur si l'utilisateur utilise un autre navigateur.

- **Chiffrement des données** – Vista offre la possibilité de chiffrer ponctuellement les données spécifiques ou de chiffrer à la volée des volumes entiers, et permet de stocker les clés de chiffrement sur un *token* (une carte à puce par exemple).

  Ces mécanismes ne résisteront pas à certaines attaques gouvernementales, mais un tel service réduit malgré tout les risques de compromission de données en cas de perte ou de vol de la machine.
- **Contrôle parental** – Vista fournit un système de contrôle parental permettrant de limiter les accès à la machine, aux logiciels installés sur la machine, en fonction de tranches horaires. Il est aussi possible d'activer un filtrage des pages affichées.
- **Pare-feu et protection anti-malware (vers, virus, anti-spyware)** – Ces fonctions sont citées parmi les fonctions de sécurité de Vista, mais ne font pas partie du système d'exploitation.

  Avec Vista, le pare-feu devient bidirectionnel et l'anti-spyware Windows Defender est présent en natif (Microsoft commercialise son antivirus séparément).

S'il y a un terrain sur lequel Microsoft est absolument irréprochable, c'est lorsqu'il tente de renforcer la sécurité du cœur de son système d'exploitation et de l'accès aux ressources Utilisateur (gestion des droits d'accès) ou Système (pilotes de périphériques). Il est impératif, pour améliorer la confiance des utilisateurs, que le système d'exploitation se montre moins vulnérable aux attaques extérieures. En cela, Vista apporte des réponses. Par exemple, afin de protéger le système contre l'exploitation de failles et les actes de piratage, Microsoft a développé une technologie intéressante, PatchGuard, destinée à préserver la stabilité du noyau. PatchGuard interdit les accès en écriture au noyau, bloque l'accès aux pilotes, aux logiciels et aux correctifs qui tenteraient de modifier cet espace noyau (selon Microsoft, un grand nombre des « plantages » provient d'un pilote mal programmé).

Intéressante sur le fond, cette nouvelle technologie met toutfois des bâtons dans les roues de nombreux éditeurs de sécurité (antivirus pour ne citer que ceux-là).

Vista, forteresse imprenable ?

En dépit de la position dure adoptée par Microsoft, le noyau de Windows Vista sera-t-il cette fois réellement à l'abri des attaques ?

Bien entendu, il est difficile de répondre à cette question tant que le système n'est pas déployé et n'a pas encore essuyé les coups de boutoir des pirates du monde entier.

Il semble cependant que des chercheurs et experts aient déjà démontré la possibilité de contourner les protections.

AVANCÉ **Blue Pill**

Pour en connaître davantage sur les risques de piratage de Vista, vous pouvez consulter le blog de Joanna Rutkowska :

- http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html

Faut-il migrer ?

Cette courte analyse a été menée en toute indépendance et sans aucun parti pris. Force est de constater qu'elle n'est toutefois pas très favorable à Vista !

En ce qui concerne les DRM, on ne peut certes pas reprocher à un industriel d'innover, d'autant que, sur le plan technique, Microsoft a réalisé une performance. Cependant, les utilisateurs ne sont pas non plus obligés d'accepter des technologies qu'ils ne souhaitent pas, ni un modèle auquel ils n'adhèrent pas.

Les utilisateurs auraient certainement bien mieux accueilli une action de Microsoft essentiellement orientée vers le renforcement de la sécurité de son système d'exploitation, afin de le rendre plus imperméable aux attaques incessantes des pirates. Néanmoins, cela n'est qu'un avis d'utilisateur, qui ne pèse pas bien lourd à côté des intérêts financiers des éditeurs, des maisons de disques et des fournisseurs de contenus multimédia.

De toutes manières, il est encore trop tôt pour formuler un avis. L'année 2007 sera riche en enseignements et en retours sur expérience. Par ailleurs, les interfaces de programmation permettant aux éditeurs d'accéder au noyau Vista 64-bits sera livrée avec le Service Pack 1 de Vista. Selon le cabinet d'études Gartner, la première mise à jour de Vista ne serait pas publiée avant le début de 2008.

Rien ne presse donc. Il existe des systèmes alternatifs et Windows XP fonctionne encore très bien.

ALTERNATIVE **Autres systèmes**

Si Vista vous fait peur, c'est peut-être l'occasion pour vous de découvrir Linux. Ce système extraordinaire est doté d'une riche diversité de logiciels adaptés à toutes les tâches de l'utilisateur, aussi bien à domicile que dans l'entreprise. En outre, Linux affiche des performances étonnantes, et fonctionne à merveille sur les vieilles machines (justement celles pour lesquelles Palladium, TCPA et consorts sont des notions absolument étrangères !).

- 🕮 *Ubuntu efficace*, Lionel Dricot, Éditions Eyrolles, 2006.