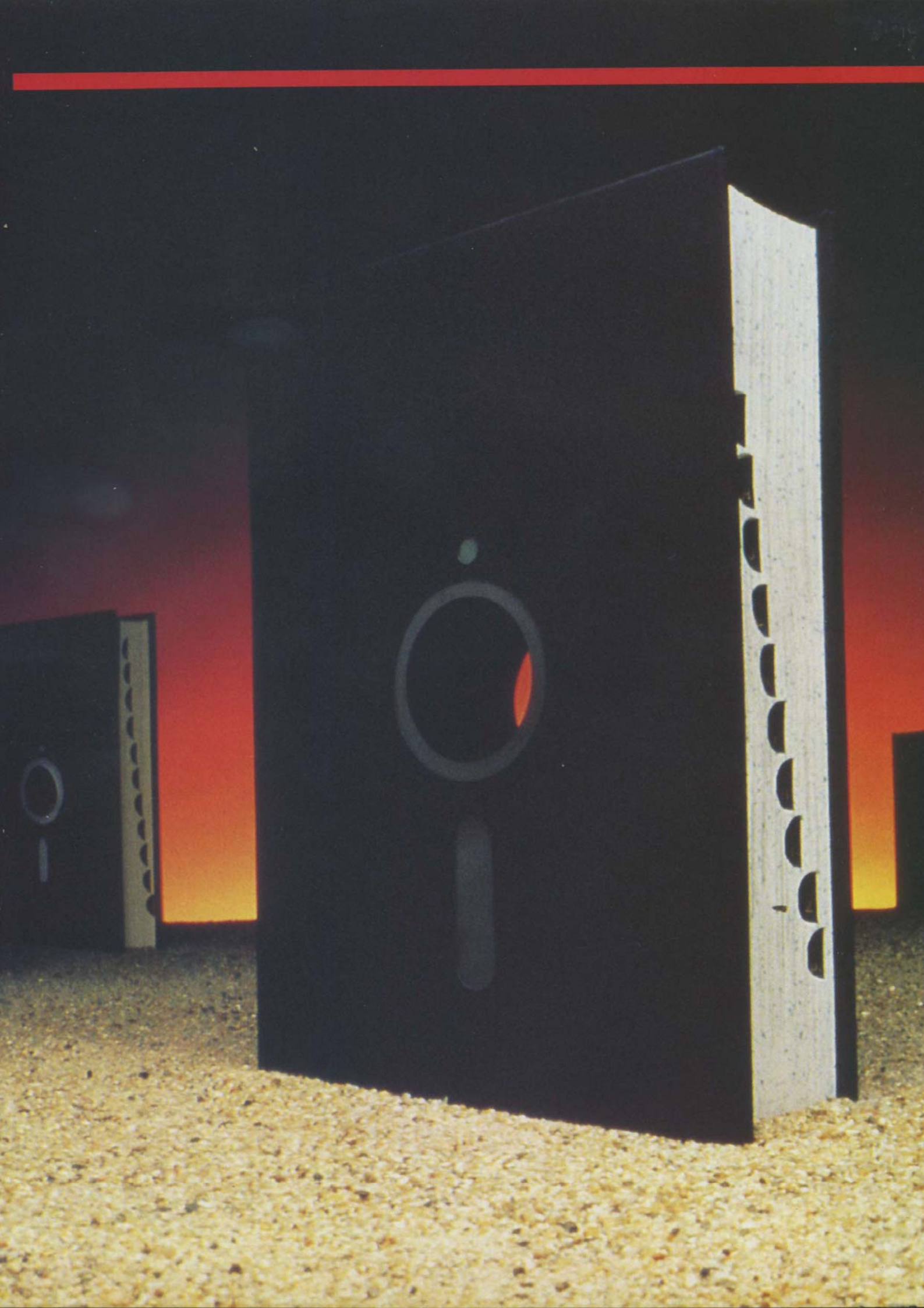
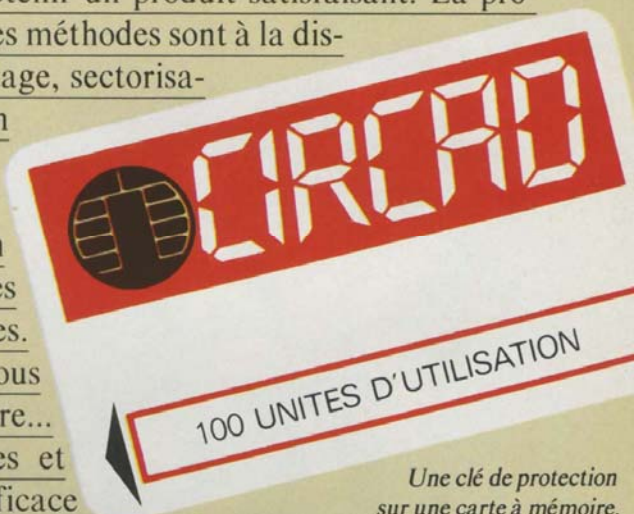


LA PROTECTION DES LOGICIELS

La création d'un logiciel est un travail difficile et nécessite un investissement important en temps et en argent : plusieurs années sont parfois nécessaires afin d'obtenir un produit satisfaisant. La protection contre la copie s'avère donc indispensable. Différentes méthodes sont à la disposition du concepteur : la protection logicielle pure (cryptage, sectorisation particulière de la disquette, etc.), l'utilisation d'un artifice matériel (recopie en mémoire morte, par exemple) ou encore une combinaison de ces deux procédés (système Prolok, « Dongle »...). Dans ce dossier, nous décrirons en détail comment les informations sont stockées et organisées sur une disquette, et comment elles peuvent y être protégées. Si vous avez vous-même développé un logiciel, vous vous souciez sans doute aussi de protéger légalement votre œuvre... Vous trouverez aussi une analyse précise des démarches et formalités juridiques importantes : un rempart très efficace depuis que le Sénat s'est penché sur la question ! Enfin, même si vous n'êtes encore qu'amateur, nous mettons à votre disposition quelques méthodes sûres de protection, accessibles en Basic et en Assembleur.



Une clé de protection sur une carte à mémoire.

AU SOMMAIRE DE CE DOSSIER

Cryptage, sectorisation de la disquette, recopie en mémoire morte, système Prolok, Dongle... Les nouveaux outils de protection.

PROTECTION HARD ET SOFT: L'ESCALADE TECHNIQUE

La copie illégale de programmes coûte chaque année plusieurs millions de dollars aux éditeurs, distributeurs et revendeurs de logiciels. Ils se heurtent donc à un problème crucial lors de la commercialisation de leurs produits : il est en effet relativement difficile de trouver une méthode simple et efficace pour protéger des disquettes contre la copie pirate dans un pays où le « déplombage » est considéré comme une sorte de sport et ceux qui s'y livrent, comme des héros des temps modernes !

De nombreux utilisateurs partagent l'idée que les logiciels sont vendus au-dessus de leur valeur réelle, et que les éditeurs s'enrichissent, en conséquence, trop facilement. Il est exact que les programmes chers sont bien plus copiés que les autres. Par contre, lorsque les prix sont relativement bas (de l'ordre d'un millier de francs), la plupart des utilisateurs préfèrent acheter un produit complet, avec sa documentation, sa maintenance et ses mises à jour.

Si les prix élevés favorisent les duplications illégales, les pertes que ce piratage entraîne à son tour augmentent le prix du logiciel. Il se forme ainsi un véritable cercle vicieux préjudiciable, non seulement aux éditeurs, mais aussi aux utilisateurs :

- Les utilisateurs achètent plus chers leurs logiciels.
- Les pertes que subissent les concepteurs de programmes retardent la mise au point de nouveaux produits et l'amélioration des logiciels existants.

La base de la protection : le « DOS »

Seuls les programmes sur disquettes peuvent être protégés de manière élaborée.

C'est un logiciel, le système d'exploitation (Disk Operating System : D.O.S.), qui se charge de toutes les opérations concernant les disquettes : lecture et écriture.

Ce système d'exploitation peut être résident, c'est-à-dire stocké en permanence dans une mémoire morte de l'ordinateur, mais le plus souvent, il est chargé en mémoire vive à partir d'une disquette.

Le **formatage**, ou initialisation, consiste à préparer les disquettes afin qu'elle puissent recevoir des données. Le programme de formatage divise la disquette en pistes concentriques, elles-mêmes divisées en blocs de données : les secteurs (**encadré 1**). Pour réaliser cette opération, le système d'exploitation écrit des repères sur la disquette, qui mar-

Encadré 1

SECTEURS HARD ET SOFT: L'ORGANISATION D'UNE DISQUETTE

Il y a quelques années, les disquettes à sectorisation **matérielle** (hard sector) étaient les plus utilisées. Elles portaient des trous sur leur circonférence interne pour délimiter les différents secteurs. A présent, la plupart des disquettes sont à sectorisation **logicielle** (soft sector) ; le système d'exploitation écrit lui-même les « repères » délimitant les secteurs **(fig. A).**

La plupart des systèmes d'exploitation de disques ne résident pas de façon permanente dans l'ordinateur, mais sont stockés sur des pistes réservées de la disquette. Ils seront lus puis stockés dans la mémoire centrale par un petit programme contenu dans un boîtier de mémoire morte de l'ordinateur.

L'annuaire des fichiers présents sur la disquette (le « directory ») est aussi rangé dans un emplacement propre. Par exemple, sur les disquettes Apple, CP/M et MS-DOS, l'organisation des informations est celle du **tableau A.**

Bien que les programmes écrits pour le système d'exploitation CP/M soient théoriquement standards, nous voyons que les caractéristiques des disquettes CP/M sont très variables d'un ordinateur à l'autre. En pratique, ceci explique la très rare compatibilité des disquettes. En effet, une disquette écrite par un ordinateur CP/M ne sera habituellement pas lue par un autre (sauf si l'on dispose d'un programme de conversion d'un format à l'autre).

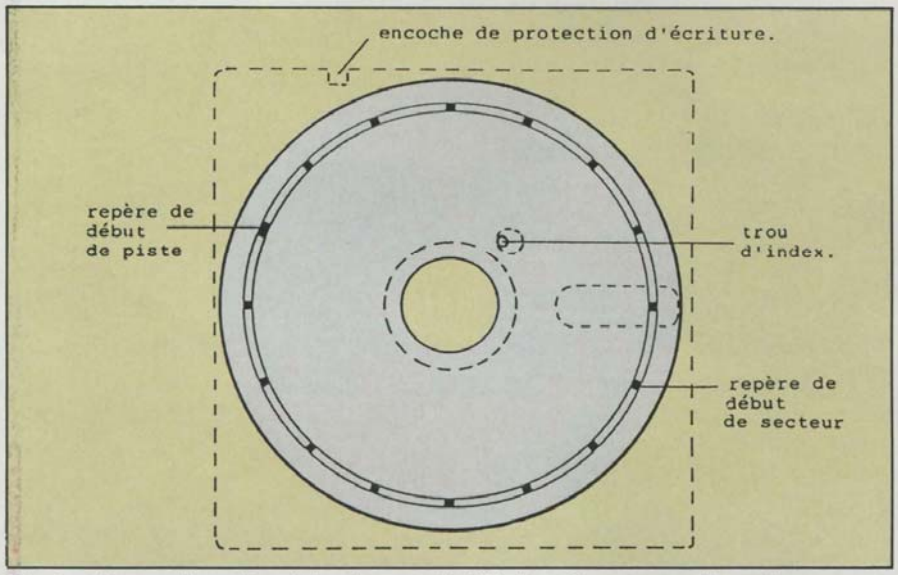


Fig. A. – Les systèmes d'exploitation actuels délimitent les secteurs d'une disquette.

	Apple II	CP/M	MS-DOS (IBM) version 2.X et +
Nombre de pistes/face :	35	35 à 80	40
Nombre de secteurs/piste :	16	variable (ex : 40)	9
Nombre d'octets/secteur	128	128 à 512	512
Système d'exploitation sur les pistes :	0, 1 et 2	0 et 1	0, 1 et 2
« Directory » sur la piste :	17	2	0

Tableau A. – Organisation des informations sur les disquettes supportant les trois principaux systèmes d'exploitation.

quent les débuts de pistes et de secteurs.

Les données seront ensuite écrites sur les différents secteurs. Pour connaître ce qui est stocké sur la disquette le système d'exploitation dispose d'un index ou catalogue (directory). Ce catalogue occupe quelques secteurs réservés d'une disquette. Il contient les noms des fichiers, leurs attributs (lecture et écriture autorisées ou non...) et l'emplacement des secteurs qu'ils occupent. Bien sûr, chaque fois qu'un fichier est créé, modifié ou supprimé, le système d'exploitation met à jour le catalogue.

Lorsque la disquette est formatée, le système d'exploitation peut lire ou écrire des informations sur n'importe lequel des secteurs en positionnant la tête de lecture/écriture sur la piste correspondante puis en attendant le moment où le secteur désiré (indiqué par le directory) défilera sous la tête.

Trois types principaux de protections sont disponibles pour les éditeurs : la protection « logicielle », la protection « matérielle et logicielle », et enfin la protection strictement « matérielle ».

La protection logicielle

La plupart des méthodes de protection logicielles, c'est-à-dire faisant uniquement intervenir des programmes, sont basées sur une modification du format des disquettes. Cette modification empêchera le système d'exploitation normal ou les programmes de copie ordinaires de lire la disquette protégée. Par contre, sur la disquette originale se trouve une version modifiée du système d'exploitation, seule capable de lire le format altéré. Evidemment, ce système d'exploitation transformé ne vous permettra pas de copier la disquette !

Les premières modifications étaient relativement simples. Mais, au fur et à mesure que les pirates « cassent » les protections des logiciels, les éditeurs améliorent leurs méthodes... L'escalade technique, qui se poursuit maintenant depuis des années, ne semble pas devoir s'arrêter.

Bien sûr, protéger de la sorte un programme en modifiant le système d'exploitation demande du temps et n'est rentable que dans la mesure où il est utilisé sur un ordinateur très répandu. C'est pourquoi les premiers programmes protégés ont vu le jour sur l'Apple II, il y a plus de six ans. En revanche, la plupart

LA PROTECTION DES LOGICIELS

Encadré 2

LES DISQUETTES «PROLOK»

Depuis un peu plus d'un an, la société américaine Vault Corporation commercialise ses disquettes Prolok. Il s'agit d'une disquette fabriquée spécialement et exclusivement pour les éditeurs de logiciels, à bas prix (de 1 à 10 $ l'unité, selon les quantités).

Les programmes enregistrés sur ces disquettes peuvent être copiés, à des fins de sauvegarde ; mais il est impossible de diffuser ces copies. En effet, une copie ne pourra fonctionner que si la disquette originale se trouve dans un second lecteur. Même si celle-ci est abîmée et les informations illisibles, le logiciel copié détectera sa présence et permettra l'exécution du programme.

Le système employé est simple et original : chaque disquette possède une marque physique, une modification de sa surface qui est unique : il s'agit en fait d'un défaut localisé dans le revêtement magnétique de la disquette. Chaque défaut, que l'on peut comparer à une « empreinte digitale », apparaît comme un trou difficilement visible sur la surface de la disquette. D'une disquette Prolok à l'autre, les marques résident sur des pistes et secteurs différents. L'éditeur de logiciel ne stocke pas les programmes originaux sur la disquette, mais une version transformée en fonction de la position de cette marque. Lors de l'utilisation, un programme présent sur la disquette elle-même utilisera à nouveau l'emplacement de la marque pour décrypter le programme protégé et en produire une version exécutable.

Les sécurités de la disquette Prolok ont été contournées, soit par voie matérielle (en reproduisant sur la copie le défaut présent sur l'original), soit par voie logicielle. La Vault Corporation a depuis annoncé la version **Prolok Plus,** qui ne se contente plus de refuser l'exécution d'une copie illégale, mais détecte les tentatives de piratage et réagit de façon virulente : le programme « anti-piratage » peut ainsi bloquer votre programme, falsifier vos données, ou même s'attaquer à votre disque dur !

des programmes s'exécutant sous le système d'exploitation CP/M ne sont pas protégés. En effet, à la différence du DOS « 3.3 » de l'Apple, qui est le même (ou presque) pour tous les Apple II, CP/M a été implémenté sur une multitude de machines. Chacune des adaptations étant différente des autres, il n'était pas envisageable pour les éditeurs de logiciels, car peu rentable, d'adapter leurs protections à chacun des CP/M existants ! A l'heure actuelle, l'IBM PC et ses compatibles sous système d'exploitation MS-DOS se répandant très largement, les éditeurs de logiciels protégent désormais les programmes écrits pour ces ordinateurs selon des procédés très variés.

La méthode évidente pour protéger un logiciel consiste, comme nous l'avons vu, à interdire la copie des disquettes par les instructions du système d'exploitation. Pour ce faire, on peut placer sur le disque des informations « cachées », par exemple en dehors des pistes utilisées normalement pour les programmes. Il est également possible d'organiser les secteurs selon une méthode différente de celle du DOS, et donc rendre le disque illisible pour tout autre logiciel que le programme devant l'exploiter. Une méthode similaire consiste à crypter l'information avant de l'écrire sur le disque, à l'aide d'un algorithme de codage inclus dans le logiciel, exécuté avant toute autre opération. Toutes les fantaisies sont possibles dans le domaine de la protection logicielle, certains concepteurs allant même jusqu'à écrire leur propre système d'exploitation !

Malheureusement, ces méthodes très efficaces il y a encore peu de temps ne résistent pas aux logiciels dits « **disque mécanique** »*, qui se contentent d'effectuer une image parfaite du disque, et reproduisent donc toutes les anomalies qui y seraient introduites. Une précision toutefois : un logiciel copié par un utilitaire de « déplombage » reste protégé, et ne peut toujours pas être copié ensuite par les voies normales (ordre de copie du système d'exploitation).

En conséquence, la protection logicielle est fortement déconseillée pour les programmes destinés au grand public, mais reste valable pour dissuader la copie des softs verticaux dont la diffusion plus restreinte limite les risques (gestion spécialisée, comptabilité).

La protection matérielle et logicielle

Pour améliorer la performance d'une protection logicielle, de nombreux concepteurs intègrent maintenant un élément matériel non copiable dans le principe de la protection. Les deux méthodes les plus répandues sont actuellement :

1 – Endommager un secteur

Un des secteurs de la disquette est endommagé de manière irrémédiable par un procédé mécanique. Le logiciel connaît la position du secteur endommagé et teste régulièrement sa présence. C'est le principe utilisé par Prolok sur ses disquettes (**encadré 2**), et avec des variantes par de nombreuses sociétés de protection.

Ce principe assez simple présente peu d'inconvénients, si ce n'est qu'il impose la présence du disque original dans l'un des lecteurs, ce qui peut parfois poser des problèmes pour les sauvegardes de fichiers sur les micro-ordinateurs équipés d'un lecteur unique et d'un disque

** Ce type de logiciel est baptisé « disque mécanique » car, à l'image des copies « audio » de magnétophone à magnétophone, il effectue une duplication du contenu de la disquette sans tenir compte de l'organisation des données sur celle-ci (formatage).*

Encadré 3

« LES DONGLES »

Textor, logiciel de traitement de texte et « Décisionnel graphique » sont protégés par un « Dongle ».

Le logiciel à protéger peut être commercialisé avec une « clé » (un « Dongle ») qui se relie à un connecteur de l'unité centrale du micro-ordinateur. Les instructions spécifiques ajoutées au programme avant sa compilation testent la présence de la clé. Ce logiciel protégé ne peut donc fonctionner que sur des micro-ordinateurs qui sont munis de cette clé. Le mode de fabrication retenu (circuit électronique moulé dans de la résine très dure) rend hautement improbable la neutralisation des dongles. Ainsi, par exemple, la clé de protection Microphar est-elle composée d'un circuit intégré, de transistors et de quelques composants passifs. Le câblage, spécifique à chaque série produite, permet l'affectation d'un code client de cinq chiffres et d'un code programme accessible au concepteur. De plus, la routine de lecture du code programme, intimement liée au code client, garantit l'exclusivité de la clé et de sa routine au concepteur.

Lors de l'élaboration de son logiciel, le programmeur décide, par la présence ou non du numéro attendu, de l'utilisation de son logiciel en limitant ou en interdisant l'accès à tout ou partie de l'ensemble des fonctions.

Branchée sur le port parallèle elle est totalement « transparente ». Elle ne fait que réagir au logiciel d'interrogation : aucune altération des caractères normaux ou graphiques ne peut apparaître lors d'une impression. Notons de plus que plusieurs clés peuvent s'empiler (maximum 4).

Des exemples d'appel à la clé sont fournis au client dans la plupart des langages (Basic, Pascal, C...) s'exécutant sous le système d'exploitation MS-DOS.

La nouvelle clé de protection de Microphar : SECRYPT.

dur. Le contenu de la disquette peut en général être copié afin de disposer d'une sécurité, mais le logiciel ne s'exécutera qu'une fois réécrit sur le disque d'origine.

Attention, le secteur doit être réellement abîmé, une simulation étant insuffisante pour tromper les « disques mécaniques ». La sécurité de ce type de protection dépend en grande partie de la méthode utilisée et de la précision des tests. Dans tous les cas, la fiabilité est suffisamment bonne pour garantir une protection minimale. En revanche, certains produits récents tiennent déjà compte de tous les systèmes de « déplombage » utilisés par les pirates dans leurs logiciels, et offrent une sécurité totale. Par souci de perfection, il est donc indispensable de tester le produit par tous les moyens de déprotection actuellement disponibles.

2 – Les « Dongles »

Un petit boîtier fermé appelé « dongle » ou « clé » (**encadré 3**) est connecté sur l'interface parallèle ou série du micro-ordinateur. A l'intérieur de ce boîtier, un circuit est connecté aux broches de l'interface de façon à renvoyer certaines valeurs codées au logiciel, en fonction de données émises par ce dernier.

Afin de valider la protection, il faut bien évidemment intégrer dans le programme à protéger une routine qui effectue le test et lit les codes renvoyés. Le déplombage implique la recherche de cette routine dans le code source**...

Pour être efficace, le boîtier ne doit pas perturber le fonctionnement d'un éventuel périphérique connecté sur l'interface utilisé. Cette méthode est l'une des plus fiables au niveau de la protection, car le boîtier est évidemment incopiable par soft ! Elle est malheureusement assez chère et ne s'adresse qu'aux concepteurs eux-mêmes puisqu'il faut intégrer le test dans le programme source.

Ce type de protection par intégration d'un élément matériel est le principe qui présente le meilleur rapport « fiabilité/prix-simplicité » parmi les diverses

*** Le code « source » correspond au programme écrit en langage évolué par le développeur. En général, les « grands logiciels » sont commercialisés en code « objet », c'est-à-dire, par exemple, dans une version en langage machine.*

LA PROTECTION DES LOGICIELS

méthodes disponibles actuellement. Il faut toutefois émettre une réserve importante sur la protection en règle générale : plus une protection est répandue, et plus il y a de chances pour qu'il existe un moyen de la contourner ! Cet élément doit être pris en compte lors du choix, car un produit diffusé à des millions d'exemplaires présente un facteur de risque plus élevé qu'un produit marginal.

La protection matérielle

Puisqu'une disquette est par essence copiable, pourquoi ne pas intégrer directement le logiciel dans la structure matérielle du micro-ordinateur, comme l'est par exemple le BIOS sur IBM PC ? Une fois le programme en mémoire morte, la copie devient un problème industriel et n'est presque plus à la portée de l'amateur. Cette méthode est très répandue dans le domaine familial, avec les softs livrés sur cartouches enfichables. Malheureusement, elle pose des problèmes de production pour les petites sociétés de logiciels et est impraticable dans le cas d'un IBM PC ou compatible : on imagine difficilement un concepteur livrer son produit sur une carte d'extension.

Les méthodes d'installation

La facilité d'installation d'une protection peut être un critère de choix importat pour le concepteur d'un logiciel, mais reste un des points faibles de nombreux systèmes et ce, quelle que soit la famille de protection à laquelle ils appartiennent.

Certaines sociétés proposent des protections venant se superposer au programme grâce à un utilitaire spécialisé, ou effectuant un simple codage sur disque de son contenu. Cette méthode très simple à mettre en œuvre est pourtant dangereuse : un codage peut toujours être décodé, et dans ce cas la copie se trouve totalement déprotégée, même si le principe de protection utilisé est excellent ! C'est toutefois la seule méthode permettant à des distributeurs ou à des importateurs de protéger un logiciel, sans nécessiter une collaboration active des concepteurs.

En règle générale, une bonne protection demande l'intégration de routines à l'intérieur du programme source, ce qui peut parfois poser des problèmes en

Encadré 4

LES ARMES DU PIRATE

N'est pas pirate qui veut. Il est bien sûr relativement facile d'utiliser en profane les différents programmes de copie en vente sur le marché. Mais le piratage n'est pas seulement une industrie : pour beaucoup d'informaticiens amateurs, c'est surtout une distraction intellectuelle et un défi à relever.

Pour l'amateur, un programme protégé représente avant tout le plus passionnant des wargames : une lutte intellectuelle stimulante entre lui et l'auteur du logiciel.

Trois types d'armes

• Les programmes de copie

Ils sont plus ou moins perfectionnés. Certains se contentent de recopier bit à bit les informations de la disquette. Les plus performants disposent de nombreuses possibilités et sont « paramétrables » : au moment de copier un logiciel donné, il faut leur indiquer quelles sont les méthodes de protection employées par la disquette à reproduire. Le programme pourra donc contourner ces protections, et la copie que l'on obtiendra sera identique à l'original (et sera elle aussi protégée contre la duplication).

Tous les programmes protégés courants ont été analysés et les paramètres à utiliser pour copier chacun d'entre eux sont connus. Le logiciel de copie peut donc être employé sans que l'utilisateur ne connaisse dans le détail les techniques de protection.

Par contre, si l'on désire dupliquer un programme récent non présent sur la liste, il faut mettre en œuvre les utilitaires du programme de copie pour analyser soi-même les informations contenues sur la disquette protégée et découvrir leurs moyens de protection.

• Les cartes d'interruption

Des cartes électroniques enfichables constituant un véritable « périphérique de piratage » sont apparues sur le marché : ces périphériques permettent d'interrompre le fonctionnement de l'ordinateur et de sauver le programme en cours d'exécution sur une disquette non protégée.

Les cartes d'interruption ont cependant des applications assez restreintes. En effet, la plupart des programmes commerciaux, qui sont de grande taille, ne sont pas chargés en une seule fois dans la mémoire centrale, mais divisés en plusieurs programmes utilisés successivement. Il est donc difficile pour le possesseur d'une carte d'interruption de sauvegarder son programme complet sur disquette. De plus, souvent, les logiciels protégés vérifient périodiquement que la disquette utilisée est bien l'originale : par exemple en contrôlant des clés bien cachées sur une piste (ou entre deux pistes...) de la disquette. Pour déjouer ces protections, il faut analyser le programme de manière approfondie.

• Les désassembleurs, moniteurs et utilitaires

Ces programmes permettent de lister les instructions d'un programme, de suivre pas à pas son exécution et de le modifier. Leur usage nécessite une bonne connaissance de l'assembleur et du système d'exploitation de l'ordinateur utilisé.

Ils sont employés par les pirates expérimentés afin de réaliser la plus délicate des opérations : le « déplombage ».

Le déplombage consiste à analyser le système d'exploitation altéré et le programme protégé pour détecter toutes les protections et les éliminer. Le programme obtenu ne sera plus protégé contre les copies et pourra donc par la suite être dupliqué à volonté.

Les pirates expérimentés peuvent effectuer une telle opération en quelques heures seulement. Ils apposeront ensuite fièrement leur pseudonyme sur la page d'introduction du programme et le distribueront à leurs amis. Ceux-ci en feront à leur tour des copies et le programme déplombé se multipliera.

fonction du langage utilisé. Cette intégration complique énormément le travail de « déplombage » et garantit la quasi-impossibilité d'une déprotection totale : en effet, même si le logiciel est dupliqué, la copie s'exécute mais n'est pas totalement déprotégée puisque les tests sont toujours présents.

Vendre déprotégé ?

Cet éventail des méthodes disponibles pour la protection des logiciels ne fait que présenter les systèmes les plus courants actuellement disponibles. Aucun n'est parfait, et tous occasionnent de légers inconvénients à l'utilisateur. On peut toutefois espérer qu'une prise de conscience des problèmes posés par le piratage interviendra dans un futur proche au niveau du public, ce qui devrait assainir suffisamment le marché pour pouvoir vendre des logiciels dépourvus de protection à un prix raisonnable ! S&M

D. Mavrakis
M.-P. Olivier

PRATIQUE

QUELQUES PROTECTIONS

NOM	TYPE	DISTR.	NOTES	Qté min	VERSION	PRIX
Microphar	Dongle Clé de protection	Microphar 267 04 95	Protège décis. graph.	50	IBM PC DEC HP 150	250 F
Protector	Disque protégé	Frame 774 87 88	Protège Nucleus	Unité	IBM PC	100 F
Protège	Disque protégé	BVRP 354 89 51	Protège Textor	500	IBM PC	100 F
Prolok	Disque protégé	La Commande Electronique (32) 52 54 02	Le plus répandu	Unité	MS-DOS	70 F
Secrypt	Dongle	Microphar 267 04 95	Produit nouveau	Unité	MS-DOS	–
Circard	Clé sur une carte à mémoire	Circard France 278 91 90	Nécessite un lecteur de carte à mémoire	50 50	VAX-EMS MS-DOS	Fonction des quantités

DETOURNEMENT INFORMATIQUE: LES "BOMBES LOGIQUES"

Les crimes de l'avenir seront sans doute souvent perpétrés par l'intermédiaire d'ordinateurs. La criminalité informatique représente un problème préoccupant les responsables du monde entier. Une étude récente estime que le coût annuel des détournements et des usages illégaux d'ordinateurs dépasse 300 millions de dollars. Le coût moyen de l'un d'entre eux est de 45 000 $, soit 10 à 20 fois plus qu'une escroquerie classique...

Les pertes bancaires dues aux fraudes informatiques sont cinquante fois plus élevées que celles dues aux vols et aux hold-up combinés. Non seulement la plupart de ces crimes « en col blanc » restent impunis mais, très souvent, on ne les découvre même pas ! En effet, les vérifications humaines se font de plus en plus rares et une étude menée dans un service informatique de l'U.S. Navy a montré que, parmi les chèques établis par ordinateur, seuls 27 % de ceux supérieurs à 25 000 $ étaient contrôlés par un œil humain !

Lorsqu'un crime informatique est découvert, le public n'en est généralement même pas informé. En effet, les victimes se passent volontiers de la publicité que leur apporte ce genre d'événements, surtout en France où leur déclaration n'est pas obligatoire.

Par ailleurs, le vide juridique en matière de fraude informatique n'encourage pas les victimes à s'engager dans de longues procédures souvent infructueuses. Les délits non violents sont relativement tolérés par la société, surtout lorsqu'ils touchent de grandes firmes anonymes, ce qui explique que les fraudeurs obtiennent généralement une peine avec sursis ou une mise à l'épreuve. Depuis peu de temps, les Etats-Unis ont commencé à se doter de lois qui leur permettront de lutter plus efficacement contre ce fléau. Ainsi un projet de loi récent prévoit un an de prison et 5 000 $ d'amende pour un accès illégal à un ordinateur du gouvernement fédéral, et jusqu'à 10 ans de prison si cet ordinateur contient des informations secrètes intéressant la sécurité nationale.

La généralisation des micro-ordinateurs et des réseaux de transmission de données accessibles par téléphone, tels Transpac en France et Télénet, Tymnet, Uninet aux Etats-Unis, a certes facilité la tâche des pirates.

Des défaillances humaines sont aussi

DES SOMMES CONSIDERABLES SONT REPRESENTEES PAR QUELQUES DONNEES TRANSMISES SUR UN RESEAU

souvent impliquées, et bien fréquemment, des piratages ont pu être réalisés grâce aux carences des responsables de systèmes informatiques et à la détermination des pirates. Ceux-ci sont souvent motivés par l'appât du gain, mais parfois aussi par le défi intellectuel et l'excitation que représente la violation des protections d'un système informatique.

Un exemple de carence flagrante des responsables a été donné par une banque américaine où un transfert illégal portant sur plus de 10 millions de dollars a pu être réalisé. Lors d'une visite, un consultant extérieur vit le mot de passe du jour imprudemment affiché dans la salle des opérations. Il l'employa afin de de faire passer pour un utilisateur autorisé et transféra cette somme considérable dans une banque suisse ! Dans la pratique, l'accès illégal par voie téléphonique à de nombreux systèmes informatiques est fréquent. Mais les véritables fraudes bancaires sont le plus souvent commises par des informaticiens ayant travaillé dans la société ou du moins ayant eu accès à leur service informatique. Le développement progressif de la télématique bancaire ouvre la voie à des possibilités de fraude presque illimitées. Prudentes, les banques préfèrent souscrire aux contrats d'assurance spécialisés qui les couvrent depuis peu contre de telles mésaventures.

Cependant, les assureurs imposent habituellement une franchise importante qui peut atteindre 10 à 15 millions de francs.

Une affiche publiée par Apple dont l'attitude est particulièrement militante en matière de protection. (Photo J.L. Desnos.)

Sept délits informatiques

Lorsque l'on évoque les délits informatiques, les détournements de fonds viennent immédiatement à l'esprit. Pourtant, il ne faut pas oublier que bien d'autres formes d'abus peuvent être commises...

1° Les détournements de fonds représentent bien sûr une façon très lucrative d'exploiter ses connaissances en informatique. La généralisation des systèmes de transferts de fonds électroniques, où des sommes considérables sont représentées par quelques données transmises sur un réseau télématique, explique leur développement.

Les banques n'en sont pas les seules victimes, et il y a eu des vols spectaculaires commis aux dépens des sociétés d'assurance.

2° Le vol d'informations est un délit non seulement très répandu, mais aussi très rentable. En effet, de nos jours ce ne sont plus seulement les matières premières qui représentent les biens les plus précieux, mais aussi le savoir et les informations, au sens large du terme.

Les voleurs peuvent ainsi s'attaquer aux informations stockées et vendues par les bases et les banques de données (à des prix variant entre 100 et plus de 2 000 F de l'heure). Ils peuvent par conséquent se renseigner gratuitement ou encore enregistrer les informations pour les revendre ultérieurement...

3° Le vol de programmes informatiques très performants, demandant des années de travail à des équipes d'informaticiens, est très lucratif et plus répandu qu'on ne le pense. Assez souvent, un employé emprunte clandestinement des listings lorsqu'il quitte son employeur pour une firme concurrente ou pour fonder sa propre société.

4° Les falsifications de données sont fréquentes. Aux Etats-Unis, par exemple, de nombreux collèges et universités stockent les bulletins de notes de leurs élèves sur ordinateurs. Des étudiants astucieux modifient leurs notes, en s'attribuant des « A » à la place de « D »,

LA PROTECTION DES LOGICIELS

comme l'illustrait si bien le film *Wargames*. Certains étudiants se sont même retrouvés diplômés avec les félicitations du jury d'universités où ils n'avaient jamais mis les pieds (excepté, bien sûr, au centre informatique...) !

5° Les sabotages, altérations ou destructions délibérées de données sont assez rares. Mais elles représentent un grand risque, non seulement pour les sociétés commerciales, mais aussi pour les organismes officiels.

6° L'espionnage peut également être payant. Il s'agit ici plus d'espionnage boursier, commercial ou bancaire que militaire. Il existe, par exemple, de nombreux marchés commerciaux très dynamiques et fluctuants où la possession d'informations clés avec quelques heures ou jours d'avance sur les concurrents permet de gagner de véritables fortunes.

Il faut aussi penser que le secret de nos informations personnelles (médicales, juridiques, bancaires et fiscales) reposera à l'avenir sur des systèmes télématiques, dont la violation pourra entraîner de graves atteintes à notre vie privée.

7° L'usage de l'ordinateur de sa firme par un employé, **pour son compte personnel** ou son amusement, représente un abus très répandu. Les administrateurs des systèmes informatiques, lorsqu'ils contrôlent les fichiers de leurs ordinateurs, ont ainsi parfois la surprise de découvrir de nombreux programmes « douteux », portant des noms comme « STARTREK », « OTHELLO » ou « MORPION ».

Encadré 1

MOTS DE PASSE ET PROTOCOLE D'IDENTIFICATION

Pour prendre le contrôle d'un ordinateur, il faut disposer d'un terminal relié à celui-ci, et connaître le protocole de connexion et le langage du système d'exploitation, ainsi qu'un nom d'utilisateur et/ou un mot de passe valides.

La généralisation de la télématique rend désormais possible la connexion à un, ordinateur distant en utilisant sa propre console (ou son ordinateur personnel), un modem et un simple téléphone relié à un réseau de transmission de données, tel que Transpac en France. Outre sa simplicité, ce système offre de plus aux pirates un anonymat presque parfait...

Une fois la connexion avec l'ordinateur établie, celui-ci n'est plus protégé que par sa procédure de vérification de l'identité de l'utilisateur. Or, bien souvent, celle-ci est prise en défaut par un opposant déterminé.

Dans bien des cas, la responsabilité en incombe à l'administrateur de l'installation qui n'a pas pris les mesures de protection qui s'imposaient.

Un exemple frappant en a été donné par un groupe de jeunes adolescents américains âgés d'une douzaine d'années, motivés non pas par l'appât du gain, mais par le défi que représentait l'accès à de gros ordinateurs. Ils ont utilisé clandestinement les terminaux de leur école et un réseau public de transmission de données pour accéder à 21 gros systèmes informatiques. Ils ont alors non seulement perturbé leur fonctionnement, mais aussi détruit et modifié les données des autres utilisateurs !

Ces jeunes ont réussi grâce à la ténacité et l'opiniâtreté dont ils ont fait preuve dans la recherche des mots de passe. Mais les grossières erreurs des administrateurs des systèmes en question sont en fait les principales responsables de leur succès. En voici quelques-unes :

- Les mots de passe standards fournis lors de l'installation des systèmes, et donc indiqués dans la documentation de tous les ordinateurs du même type, n'avaient parfois jamais été changés !
- Sur d'autres ordinateurs, les mots de passe étaient très faciles à deviner. Parfois même, le mot de passe à utiliser était tout simplement le nom de la société possédant l'ordinateur !

Les protocoles d'identification représentent l'un des moyens de protection de l'ordinateur les plus sûrs contre les utilisateurs non autorisés... si les responsables des systèmes les emploient à bon escient.

Les techniques

L'accès illégal au système est une condition le plus souvent indispensable pour la perpétration des fraudes informatiques. Généralement, il faut disposer d'une console, ou d'un terminal relié à l'ordinateur directement ou par un modem, et d'un mot de passe (password) valide. Lors de l'étape de « log-in » (connexion), l'ordinateur demande un nom d'utilisateur et son mot de passe correspondant. Si ceux-ci sont présents sur la liste des utilisateurs autorisés, l'accès au système est permis.

L'ordinateur dispose de nombreuses ressources (fichiers sur disques, programmes, périphériques) et l'usage de certaines d'entre elles peut être réservé à seulement quelques individus. Par exemple, sur la plupart des systèmes, les utilisateurs sont propriétaires de leurs données et programmes, et eux seuls peuvent y accéder. Cependant, il existe toujours des « utilisateurs privilégiés » ou « super-utilisateurs » qui ont accès sans restriction à toutes les informations contenues dans l'ordinateur.

• L'écoute des communications

Les transmissions entre ordinateurs s'effectuent par l'intermédiaire de modems, qui transforment les données informatiques en tonalités sonores. Il est enfantin de se brancher sur une ligne téléphonique et d'enregistrer avec un simple magnétophone les transmissions de données informatiques. En repassant ultérieurement ces communications, on visualisera toutes les données échangées et l'on pourra ainsi noter l'identité des utilisateurs, les mots de passe et les procédures de communications.

Ce genre de pratique est malheureusement difficilement décelable. Les soi-disant « détecteurs d'écoutes téléphoniques » commercialisés par certaines firmes sont en fait totalement inefficaces face aux techniques d'écoute modernes : les matériels informatiques émettant des ondes radio, des équipements sophistiqués permettent de les capter et de les enregistrer, sans avoir à se connecter à une ligne téléphonique.

Enfin, il est possible aussi de transformer les données ou de les remplacer par ses propres informations. Si la ligne est utilisée par exemple pour effectuer des transferts de fonds électroniques, le pirate sera à même d'envoyer ses propres

Encadré 2

LES SYSTEMES DE SECURITE A RAPPEL AUTOMATIQUE

Récemment, un nouveau moyen de protection est apparu aux Etats-Unis : le « Secure Access Multiport » (SAM). Il s'agit probablement d'un des systèmes les plus sûrs pour protéger un ordinateur relié au réseau téléphonique d'un utilisateur non autorisé.

Le système SAM s'interpose entre la ligne téléphonique et le modem. Lorsqu'un utilisateur appelle le numéro de l'ordinateur, le modem décroche mais reste silencieux, masquant ainsi le fait que l'on a atteint le point d'entrée d'un système informatique. L'utilisateur entre alors son code numérique à 6 chiffres et, une fois ceci fait, le système raccroche. Il recherche alors dans sa mémoire le numéro téléphonique correspondant, celui spécifié par l'utilisateur, et le rappelle.

De cette façon, un individu non autorisé qui a réussi à obtenir un code, mais ne se trouve pas au seul endroit autorisé à appeler, ne pourra pas accéder à l'ordinateur. On peut même programmer ce système de sécurité pour qu'il refuse de rappeler un numéro autorisé en dehors de certains horaires (par exemple en dehors des heures de bureau).

messages, ou simplement de modifier les numéros de compte transmis pour se retrouver crédité de sommes considérables.

C'est pour cette raison que les messages bancaires sont codés, souvent en fonction de l'heure de la transmission, afin d'éviter qu'un message enregistré ne soit transformé et reproduit plus tard.

• Les « bombes logiques »

Cet outil redoutable permet de causer des dégâts terribles en sabotant les fichiers de l'ordinateur. Un employé sans scrupules peut par exemple utiliser cette arme pour se venger durement de sa société si jamais celle-ci décidait de le licencier. Il lui suffit d'infiltrer quelques instructions clés dans le programme de paie pour lui ordonner de détruire tous les fichiers de l'ordinateur au cas où son nom et son numéro de sécurité sociale n'apparaîtraient plus parmi la liste des employés... Le programme s'autodétruira ensuite, faisant disparaître toute preuve du délit. Ainsi, grâce à cette « bombe à retardement », l'informaticien pourra causer des dommages inestimables à son ancienne société. Cette étrange forme de sécurité de l'emploi reste heureusement peu utilisée... Mais un employé mécontent peut facilement effectuer des forfaits moins sophistiqués, mais tout aussi dévastateurs : il lui suffit, par exemple, de voler ou de détruire lui-même des bandes magnétiques importantes...

• Le « salami »

Il s'agit de l'application pratique de l'adage bien connu « Les petits ruisseaux font les grandes rivières ». Sur un relevé bancaire, les pourcentages (par exemple ceux des intérêts d'un compte épargne) sont arrondis au centime près. Des informaticiens ont donc eu l'idée de faire des arrondis par défaut et de voler ainsi quelques dixièmes de centimes à chaque client, qu'ils verseront sur un compte spécial. Le bilan global de la banque n'en est pas affecté, et il est bien improbable qu'un client remarque une erreur aussi imperceptible. Lorsqu'une banque compte plusieurs centaines de milliers de clients, et que ceux-ci sont spoliés jour après jour de quelques dixièmes de centimes, cela représente, au bout d'un an, une somme fort appréciable.

• Les « chevaux de Troie »

Sous cette appellation se cache une pratique redoutable, qui consiste à cacher des instructions clés au sein d'un programme apparemment anodin.

Ces instructions cachées vont prendre le contrôle de l'ordinateur et s'exécuter pour leur propre compte, au grand dam des utilisateurs. Les programmes ainsi camouflés peuvent accomplir des fonctions très différentes.

Un saboteur pourra choisir par exemple de camoufler un programme « lapin » qui se multipliera jusqu' à absorber toutes les ressources de l'ordinateur.

Un opposant désirant prendre le contrôle complet de l'ordinateur pourra, quant à lui, modifier le système d'exploitation en y introduisant un jeu d'instructions guettant le moment où le superviseur se connectera à l'ordinateur pour mémoriser discrètement ses mots de passe...

• Attaque des fichiers temporaires

Les pirates ne peuvent pas toujours s'attaquer aux fichiers les plus « sensibles » de l'ordinateur, qui sont parfois trop bien protégés. Mais il leur reste la ressource d'obtenir le résultat désiré en s'attaquant à des fichiers temporaires, qui sont habituellement assez vulnérables. En effet, les données destinées à être traitées par des périphériques lents (par exemple une imprimante) sont habituellement stockées dans un fichier temporaire par l'ordinateur.

Par exemple, imaginons qu'un voleur souhaite voir établi un chèque ou un ordre de virement en sa faveur. S'il ne peut s'attaquer au fichier principal contenant les noms et les numéros de compte des bénéficiaires, il lui reste néanmoins la ressource de s'en prendre au fichier temporaire de sortie sur l'imprimante et de modifier en sa faveur les numéros de compte et les sommes.

Comment se protéger ?

Les indications suivantes vous aideront à mieux assurer votre sécurité face à d'éventuels pirates.

Si vous êtes reliés au réseau téléphonique, vos numéros ne doivent pas figurer à l'annuaire. Pour une plus grande sécurité, vous pouvez employer des modems rappelant automatiquement les utilisateurs autorisés (**encadré 2**). Il vous est aussi possible de louer des lignes directes entre vos terminaux et votre ordinateur. Dans le cas de Transpac, vous pouvez choisir de faire partie d'un « groupe fermé d'abonnés », ce qui signifie que vous ne pourrez appeler et être appelés que par les utilisateurs appartenant à ce même groupe. Cette solution est fréquemment retenue par les organismes bancaires.

• La protection des consoles

Les consoles et les unités périphériques « sensibles » doivent être installées dans des locaux protégés et surveillés. Non seulement l'accès doit être

LA PROTECTION DES LOGICIELS

contrôlé, mais de plus la pratique courante (même dans les établissements bancaires) qui consiste à coller les mots de passe sous la table ou la console doit être bannie.

• Les mots de passe

Les mots de passe doivent être difficiles à deviner, tout en restant assez faciles à retenir. Ils perdent tout leur intérêt si, comme on le voit trop souvent, les utilisateurs les notent soigneusement à côté de leur terminal pour s'en souvenir... Il est difficile de trouver le juste compromis entre la sécurité qu'apporte une procédure de connexion compliquée et la commodité d'emploi d'une procédure très simple. Les mots de passe composés de phrases telles que « LE SOFT C'EST L'AVENIR » réalisent souvent un tel compromis.

La longueur d'un mot de passe doit être suffisante pour résister à une tentative de piratage où toutes les possibilités sont successivement essayées. L'usage des micro-ordinateurs, que l'on peut programmer à cette fin, facilite évidemment la tâche des pirates (au rythme d'un ou deux mots de passe à la seconde, on peut essayer toutes les combinaisons de 4 lettres en 3 jours à peine). Il est imprudent d'employer des mots de passe ayant toujours la même structure, par exemple un chiffre suivi de trois lettres, un tel principe rendant ce genre d'essais encore plus aisé.

Récemment, un pirate sans complexes a envoyé un questionnaire dans ce sens (**encadré 3**) à des utilisateurs du centre serveur Dialog, en leur demandant des renseignements précis sur leurs mots de passe (structure, lettres le composant, etc.) !

Dans l'absolu, les mots de passe doivent être changés périodiquement, au moins une fois par an.

Pour réduire les disséminations des mots de passe, chaque utilisateur doit avoir le sien et être **responsable de sa sécurité.** Dans certains systèmes, l'administrateur délivre au nouvel utilisateur un mot de passe à usage unique afin que celui-ci spécifie lui-même, lors de sa première connexion, son mot de passe définitif.

• Implémentation de la procédure de connexion

Un mot de passe ne doit évidemment pas être visible sur l'écran lorsque l'utilistateur le tape.

Encadré 3

DITES-MOI VOTRE MOT DE PASSE

C'est à peu près ce que réclamait un pirate qui ne manquait pas d'aplomb. Jugez-en plutôt : se faisant passer pour un étudiant en musicologie chargé d'écrire un article sur les mots de passe pour une revue d'informatique, il a envoyé le questionnaire reproduit **figure A** à des utilisateurs du centre serveur américain Dialog.

Comme le faisait humoristiquement remarquer le commentateur, la prochaine étude des pirates demandera votre numéro de compte bancaire, un exemple de votre signature, et un spécimen de chèque en blanc tiré sur votre compte, « ceci pour des buts de recherche uniquement scientifique » !

ETUDE DE LA STRUCTURE DES MOTS DE PASSE DIALOG

1. Relations entre les symboles de votre mot de passe :
   1.1. Est-ce que votre mot de passe contient deux lettres identiques ?
   OUI NON
   1.2. Est-ce que votre mot de passe contient deux chiffres identiques ?
   OUI NON
2. Structure des mots de passe :
   Indiquer avec une croix la position des lettres dans votre mot de passe :

3. Est-ce que le premier symbole de votre mot de passe est un 0 ?
   OUI NON
4. Lettres constituant votre mot de passe :
   Pouvez-vous m'indiquer, en ordre alphabétique, les lettres constituant votre mot de passe ?
5. Adresses d'autres utilisateurs de Dialog :

Fig. A. – Questionnaire envoyé à certains utilisateurs d'un centre serveur par un pirate qui ne manque pas d'aplomb ! (Extrait de la revue des utilisateurs de Dialog, Chronnolog, vol. 12, n° 5, mai 1984.)

Le nombre d'essais possibles autorisés pour se connecter doit être limité. Après 2 ou 3 essais infructueux, il faut couper la liaison. Le logiciel de votre ordinateur doit enregistrer et vous signaler les tentatives infructueuses de connexion.

Le fichier des mots de passe doit être crypté de manière non réversible, afin que les programmeurs ou le superviseur ne puissent retrouver le mot de passe à partir de ce fichier. Lorsqu'un utilisateur se connecte, l'ordinateur crypte le mot de passe qu'il donne et le compare à la version cryptée présente dans le fichier (**fig. 1**).

Durant la phase de connexion et d'identification, l'ordinateur ne doit pas délivrer de messages d'aide, qui pourraient rendre plus aisée la connexion d'un utilisateur non autorisé (**fig. 2**).

```
laurent:0x&-W%k3:34:2::paie:
martin:#cW5/.7a:35:3::compta:
yvette:+r!Q8d°:36:3::comptal:
robert:4w*i?Ra:37:3::compta:
```

Fig. 1. – Voici un extrait du fichier « etc/passwd » (utilisateurs autorisés) d'un ordinateur sous système d'exploitation Unix. Ce fichier comprend la liste des utilisateurs autorisés à accéder au système et, souvent, seul le « super-utilisateur » peut le lister. Pour plus de sécurité, les mots de passe (soulignés) sont enregistrés sous une forme codée, et même le superviseur ne pourrait pas les reconstituer à partir de leurs formes codées. Plutôt que de décoder le mot de passe que vient de taper un utilisateur, l'ordinateur va préférer le coder de la même façon puis le comparer à la version déjà cryptée et enregistrée dans ce fichier.

De la même façon, il ne faut pas passer d'une étape à l'autre du « log-in » (procédure de connection) dans le seul cas où l'utilisateur donne une réponse correcte à l'étape précédente (demander par exemple le nom de l'utilisateur jusqu'à ce que celui-ci donne un nom autorisé, puis son mot de passe jusqu'à ce qu'il soit correct, et ainsi de suite) (**fig. 3**). Il faut au contraire accepter sans sourciller toutes les informations jusqu'à la fin, puis indiquer « log-in incorrect » sans préciser à quel niveau se situe l'erreur. La solution de plusieurs petits problèmes est évidemment plus facile à découvrir.

```
COM

GUTS VERSION 3.6 SOUS MVS RELEASE 03.8. IBM 3033
VENDREDI 22 MARS 1985, 09H 45M 47, TERMINAL : X0A2

ISSUE /LOGON TO INITIATE TERMINAL SESSION
_/LOGON ?
LOGON       ACCOUNT    OBLIGATOIRE, SERA DEMANDE SI OMIS
            USERID     OBLIGATOIRE, SERA DEMANDE SI OMIS
            $USERPASS OPTIONNEL, SERA DEMANDE SI NECESSAIRE

LA COMMANDE /LOGON EST UTILISEE POUR INITIALISER UNE SESSION GUTS.
ACCOUNT     CODE COMPTABLE CONCERNE PAR LA SESSION. EST FORME
            DE TROIS LETTRES (SIGLE), SUIVI D'UN NUMERO DE
            QUATRE CHIFFRES (NUM).
USERID      IDENTIFICATION DE L'UTILISATEUR. CONSISTE EN UN NOM
            DE 7 LETTRES ATTRIBUE PAR LE CENTRE.
$USERPASS MOT DE PASSE DE PROTECTION DE L'USERID. GERE PAR
            L'UTILISATEUR (COMMANDE /PASS)
```

Fig. 2. – Cet ordinateur explique gracieusement la syntaxe et le format précis de la commande/LOGON qui permet de s'y connecter, et ce, avant même d'avoir vérifié si la personne qui lui demande ces informations est bien un utilisateur autorisé. Ces renseignements ont un intérêt primordial pour d'éventuels pirates !

• Vérification physique de l'identité des utilisateurs

Pour des applications très « sensibles », par exemple pour les transactions bancaires, on peut utiliser des terminaux spéciaux qui vérifient matériellement l'identité des utilisateurs. Pour cela, il existe de nombreux procédés : reconnaissance d'une carte personnelle (carte de crédit dans un distributeur automatique de billets), ou mieux, vérification des empreintes digitales ou des intonations de la parole, ou encore de la dynamique de la signature...

• Encryption

La technique la plus efficace pour protéger les données transmises sur les réseaux de communications reste leur encryption. Les applications commerciales et bancaires sont ainsi protégées, notamment par le « **Data Encryption System** » (voir *Soft & Micro* n° 7, p. 130). L'encryption des fichiers confidentiels stockés dans la mémoire de masse d'un ordinateur assure également une bonne protection contre les indiscrétions et les malversations. Les méthodes modernes d'encryption permettent, de plus, d'authentifier l'identité des correspondants.

• Destruction des listings usagés

Il est impératif de détruire les listings usagés. Bien des fraudes ont pu être perpétrées grâce aux précieuses informations qu'ont livrées des listings négligemment jetés à la poubelle.

```
COM

USER-ID ? :LAURENT
INVALID USER ID
USER-ID ? : RLAURENT
INVALID USER ID
USER-ID ? : LROLLIN

PASSWORD ? : ROLLIN
INVALID PASSWORD
PASSWORD ? : LAURENT
INVALID PASSWORD
PASSWORD ? : LROLLIN
INVALID PASSWORD
PASSWORD ? : ROLLINL

LOGON ACCEPTED FROM LINE
E405 AT 1223 ON 85-04-02
** WELCOME TO GERS **
```

Fig. 3. – Un exemple de mauvaise procédure de connexion : l'ordinateur demande imprudemment le nom de l'utilisateur (USER-ID) jusqu'à ce que la personne appelante en indique un correct. Puis, il procède de même pour le mot de passe (PASSWORD). Cette démarche permet à un pirate de s'introduire frauduleusement dans le système en procédant par essais successifs. Dans l'exemple ci-dessus, le pirate sait au départ que l'un des employés de la société se nomme Laurent Rollin et mise sur le fait que celui-ci aura peut-être utilisé imprudemment son propre nom comme mot de passe, pour des raisons mnémotechniques.

L'avenir des escroqueries informatiques

L'informatisation croissante de notre société, le développement fulgurant de la télématique et la prolifération des micro-ordinateurs familiaux risquent fort d'entraîner un accroissement considérable des délits informatiques en tous genres. D'ores et déjà, les experts estiment que l'on ne démasque que 10 % des fraudeurs.

Les dispositifs informatiques actuels sont désormais conçus afin d'offrir un maximum de sécurité aux utilisateurs.

Les ordinateurs les plus récents, à la différence des précédents, ne comportent plus les clés de commande et les nombreux contrôles externes qui donnaient auparavant à l'opérateur un contrôle complet de la machine. Par exemple, les systèmes IBM de la série 303X sont entièrement contrôlés par une console spéciale (3036). En mode normal, l'opérateur ne peut pas avoir accès aux contrôles privilégiés. Pour cela, il lui faut insérer une clé spéciale et disposer des disquettes correspondantes.

Les ordinateurs de première et de seconde génération ne gardaient aucune trace des travaux effectués. Par contre, les systèmes des générations suivantes gardent en mémoire, sur des « carnets de bord », l'utilisation faite de l'ordinateur. De nos jours, les ordinateurs enregistrent soigneusement les connexions des utilisateurs autorisés, ainsi que les tentatives de connexion illégales et l'emploi des contrôles privilégiés des super-utilisateurs. D'autre part, des logiciels permettent désormais d'exploiter au mieux ces informations qu'on laissait auparavant « dormir » sur des bandes magnétiques...

La cryptographie fournit un moyen puissant pour protéger les informations sensibles circulant sur les réseaux de transmission de données, elle voit son emploi se généraliser. **S&M**

D. Mavrakis
M.-P. Olivier

LA PROTECTION JURIDIQUE DES LOGICIELS

« Monsieur le rédacteur en chef. Lecteur régulier de votre revue, je possède un micro-ordinateur sur lequel j'ai écrit, entre autres, quelques programmes de jeu avec d'intéressants effets vidéo et sonores, et j'aimerais tenter de les vendre d'une façon ou d'une autre... Je me pose cette question : à côté des protections matérielle et logicielle, comment puis-je assurer la protection de ces programmes au point de vue juridique ? Donnez-moi des conseils... »

Chaque journée, le courrier des lecteurs apporte à la rédaction de *Soft & Micro* de semblables demandes. Il n'est pas d'usage qu'un journal de micro-informatique se lance dans des considérations juridiques ; nous ferons exception à la règle tant il est vrai que cette question préoccupe bon nombre de nos lecteurs, auteurs de programmes en puissance.

Si l'on parle de problème, c'est en effet que la question se pose, et, bien plus, elle n'est pas réglée. En un mot, le droit ne fournit pas de bons moyens de protection. Cela provient de causes classiques que l'on retrouve à d'autres occasions : la trop grande modernité de la discipline qu'est l'informatique et « la primauté de l'écrit dans le droit ».

La primauté de l'écrit est une caractéristique du Droit des pays développés. Titulaire d'un droit, il faut parfois en administrer la PREUVE. Le moyen suprême et sacré de preuve est l'ÉCRIT, qui prend difficilement en considération les apports des nouvelles technologies, comme les moyens audiovisuels. On retiendra que l'enregistrement des aveux du criminel sur une bande magnétique ne possédera devant une Cour d'Assise qu'une force probante minime, par rapport à ces même aveux consignés dans un rapport de police. Les pratiques – comme celles courantes aux U.S.A. – qui consistent à filmer un hold-up ou une livraison de drogue ne constitueraient pas une preuve (de l'infraction), mais seulement un « indice ».

Les spécialistes diront que la protection juridique des logiciels est une multiprotection. Si les moyens sont bien multiples, c'est surtout qu'il n'existe pas de législation spécifique aux logiciels. De législation *ad hoc*, comme disent les juristes. Force est de faire le tour de toutes les règles qui servent à protéger quelque chose et d'essayer de s'en servir. Parmi les multiples moyens déjà utilisés, citons la législation des brevets et surtout celle du droit d'auteur.

LA PROTECTION DES LOGICIELS

En pratique, faute d'avoir à sa disposition un texte précis qui lui indique la façon de se protéger juridiquement, l'auteur de programmes emploiera les moyens généraux proposés par la jurisprudence (science du droit). En cas de problème, il vérifiera si la jurisprudence des tribunaux a déjà traité un cas semblable au sien pour s'en prévaloir, avec l'espoir que la solution sera la même...

Piratage ou plagiat !

Il faut protéger les programmes du « pillage » ou de la « piraterie ». Au plan juridique, on distingue :

- le piratage
- la contrefaçon
- le plagiat.

On peut parler de piratage de programmes lorsque le fraudeur aura dupliqué en grande quantité le logiciel et l'aura mis en vente sur le marché dans une forme identique (nom, aspect, emballage, appellation, etc.) à celle de l'original. Au terme de la loi, ce n'est pas une infraction et donc non-répréhensible comme tel devant un tribunal pénal ; cependant, l'agissement se montre dommageable pour l'auteur de l'original qui pourra en obtenir réparation devant un tribunal civil ; il s'agit là de « concurrence déloyale ».

La contrefaçon constitue une infraction de droit pénal : lorsqu'on aura, en l'absence de tout accommodement avec l'auteur de l'original, reproduit le logiciel qui se trouve juridiquement « protégé » par des moyens divers (notamment par droit d'auteur ou brevet). S'il s'agit ici d'une contrefaçon, la copie illicite se présente sous une forme et un nom différents de ceux de l'original.

On vise par l'appellation de plagiat tout agissement qui, s'inspirant de quelques idées et de principes fondamentaux d'un logiciel (on verra par la suite qu'une idée même originale ne peut être protégée par la loi), aboutit à la mise au point d'un nouveau produit qui semble être de la même famille, mais dont on ne peut dire qu'ils se ressemblent. Si la ressemblance est poussée trop loin, on aborde les rivages de la contrefaçon. Attention à l'adaptation qui est intermédiaire entre les deux, mais qui, normalement, est autorisée (par l'auteur). En un mot, le plagiat, c'est la rançon que les auteurs doivent payer à l'ingéniosité des « fraudeurs ».

Les moyens de protection

Le moyen de protection le plus en faveur actuellement réside dans le concept de droit d'auteur. Mais il existe, dans l'appareil juridique, une autre façon, de consacrer officiellement sa paternité sur une création originale : déposer un brevet. En fait, pour des raisons aussi bien techniques que juridiques, ce moyen est pratiquement inaccessible à l'auteur de programmes. Nous en dirons cependant quelques mots.

Le brevet

Déposer un brevet pour assurer la protection du logiciel, c'est employer « les grands moyens ».

Pourtant le dépôt d'un brevet est la consécration d'un droit de propriété opposable à tous, qui peut assurer la commercialisation avec le maximum de garanties. Le texte sur les brevets est la loi du 13 juillet 1978. A première vue, les logiciels sont exclus de l'application de cette loi :

- ils ne possèdent pas la qualité de réalisation industrielle ;
- et l'article 6 déclare : « *Ne sont pas considérés comme des inventions : les créations intellectuelles, en matière de jeu ou dans le domaine des activités économiques... et les programmes d'ordinateur...* »

On peut néanmoins profiter de la protection du brevet pour une réalisation plus ambitieuse, qui posséderait la qualité « d'industrielle » et dans laquelle la partie logicielle ne serait qu'un élément, un tout plus conséquent. Le logiciel bénéficierait alors de la protection de l'invention.

Enfin, il faut savoir que, contrairement au droit d'auteur, le dépôt d'un brevet s'accompagne de la perception de droit et de taxes, **d'un montant non négligeable.** Si l'on veut maintenir son brevet dans le temps, il faudra renouveller ces taxes pendant vingt ans. (Pour plus de renseignements, s'adresser à l'Institut national de la propriété industrielle (INPI), 26 bis, rue de Léningrad, 75800 Paris Cedex.)

Le droit d'auteur

Précisons qu'il s'agit pour le créateur du logiciel d'affirmer sa paternité sur son produit : c'est l'établissement d'un véritable droit de propriété sur son logiciel.

Les juristes assimilent les programmes informatiques aux créations plus classiques que sont les œuvres littéraires et artistiques de toutes natures et aussi à des créations plus modernes comme les œuvres cinématographiques et audiovisuelles, au statut plus incertain.

Le droit d'auteur provient d'une loi du 11 mars 1957. Citons les deux premiers alinéas de l'article 1 de cette loi : « *L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Ce droit comporte des attributs d'ordre intellectuel et moral, ainsi que des attributs d'ordre patrimonial, qui sont déterminés par la présente loi.* »

Et l'alinéa 1 de l'article 7 : « *L'œuvre est réputée créée, indépendamment de toute divulgation publique, du seul fait de la réalisation, même inachevée, de la conception de l'auteur.* »

Il est nécessaire que l'œuvre obéisse à deux conditions : elle doit être **esthétique** et **originale.**

Un programme informatique répond à la première condition : sans être « esthétique » selon les canons de la beauté, il n'en est pas moins une création portant la marque, la personnalité, les choix de son créateur. Quant à l'originalité, elle vise non seulement l'absence d'antériorité d'une œuvre similaire (nouveauté), mais aussi le même fait, l'expression de la personnalité de son auteur.

Concrètement, comment faire ? En effet, la loi ne précise pas quelles sont les formalités à accomplir. Cela signifie **qu'il n'y en a pas.** Quand on remplit les conditions, il suffit, pour obtenir le bénéfice de la loi, de manifester expressément la volonté de passer sous son empire. Pour cela, on peut l'inscrire en toutes lettres dans l'œuvre, dans le programme.

Il existe des conventions internationales qui fixent les conséquences des droits d'auteur pour une exploitation en dehors du pays d'origine, particulièrement la Convention universelle de Genève de 1952. En suivant ses recommandations, on déclarera sa volonté par les mentions suivantes :

- un petit « c » compris dans un cercle (éventuellement remplacé par la mention « copyright » aux U.S.A.) ;
- l'année de création ou de publication ;
- le nom de l'auteur.

DEPOSER UN BREVET : PRATIQUEMENT INACCESSIBLE A L'AUTEUR DE PROGRAMMES

Encadré 1

LE PIRATE ET LE JUGE PENAL

Copier un programme et aller en prison ? Mais oui ! ou du moins courir le risque d'être condamné par une juridiction pénale à une peine d'amende – qui peut être lourde.

Depuis longtemps, le juriste a dû faire face à l'imagination technologique du délinquant et, toujours, le droit a su rattrapper l'innovation. Ainsi a-t-on réprimé les branchements irréguliers sur les réseaux électriques, les ententes illicites, les spéculations d'initiés. De même a-t-on pensé avoir recours aux tribunaux répressifs pour sanctionner les atteintes portées aux droits du réalisateur d'un logiciel.

Lorsque le logiciel n'était pas une œuvre de l'esprit, reconnue digne de protection, les auteurs devaient, s'ils choisissaient de poursuivre pénalement leur adversaire, se contenter des infractions générales prévues par le code pénal : ils devaient démontrer qu'ils étaient les victimes d'un vol (soustraction frauduleuse de la chose d'autrui), d'un abus de confiance (dissipation ou détournement d'objets confiés à un tiers), d'une divulgation de secret de fabrique (mais le secret doit être secret et avoir une fin industrielle) ou de la corruption de leurs employés.

Sanctionné par des peines d'amende ou de prison, dont la fourchette est fixée par la loi mais que le juge peut adapter à chacun des cas qui lui sont déférés, le délinquant peut aussi être condamné à des dommages-intérêts destinés à indemniser l'auteur du préjudice qu'il a subi : perte de bénéfices, de redevances, préjudice moral, etc. Mais si le plaignant dispose de l'appareil impressionnant de la justice pénale avec ses enquêtes, comparutions, juges d'instruction, commissions rogatoires, sa plainte doit nécessairement correspondre à l'un des délits prévus par le code pénal, et il se retrouve alors confronté au problème insidieux de la preuve des éléments constitutifs de l'infraction : l'auteur devra prouver que c'est bien Untel qui a soustrait le « listage » d'un logiciel ou que tel autre, son salarié, a reçu de l'argent pour le lui communiquer.

Cependant, les atteintes les plus dommageables aux droits des auteurs et éditeurs de logiciels ne sont pas commises lors de délits « classiques », et l'un des objectifs d'une protection des logiciels par une législation se rattachant soit aux droits d'auteur, soit aux brevets, est de permettre le recours à la procédure de « saisie-contrefaçon » et aux suites pénales de celle-ci.

En effet, le véritable tort porté à l'auteur ou à l'éditeur consiste à assurer une diffusion parallèle d'un logiciel par reproduction pure et simple ou bien par copie presque servile. Or les mécanismes de la propriété littéraire, s'ils permettaient de réprimer la commercialisation d'un ouvrage piraté, autorisaient, au contraire, la copie à l'usage privé du copiste : c'était le principal argument qui faisait repousser la législation sur les droits d'auteur en matière de programmes informatiques.

Saisi du projet de loi « Lang » relatif à la modernisation et à l'extension de la législation sur les droits d'auteur, le Sénat a introduit dans la loi du 11 mars 1957 un chapitre réservé aux logiciels. La qualité d'auteur de logiciels est reconnue et, sous les peines de la contrefaçon, est interdite *« toute reproduction autre que l'établissement d'une copie de sauvegarde par l'utilisateur ainsi que toute utilisation d'un logiciel non expressément autorisée par l'auteur... »*. Ce texte, qui sera bientôt applicable, permettra de poursuivre sur le plan pénal tous les contrefacteurs.

La peine prévue par l'article 425 du code pénal est une amende variant de 360 F à 20 000 F ; mais si le délinquant se livre habituellement à cette regrettable activité, le tarif passe à une amende comprise entre 800 et 30 000 F et à un emprisonnement de trois mois à deux ans. En outre, le tribunal pourra, sur la demande de l'auteur, ordonner la publication du jugement ou son affichage. Voilà qui, espérons-le, sera de nature à encourager les comportements loyaux !

Auteurs de programmes, vous êtes (bientôt) parfaitement protégés...

Maître André Algrin
Avocat à la Cour

Quoi protéger ?...

En nous plaçant sous l'empire du droit d'auteur, examinons la protection de chacune des étapes de l'élaboration d'un programme, puis le cas de quelques programmes particuliers.

Dans les étapes de la constitution d'un programme, nous distinguerons : l'algorithme, l'organigramme, le programme « source » et le programme « objet ».

Le droit d'auteur ne protège pas les idées qui sont des créations intellectuelles et qui doivent rester libres. L'algorithme et l'organigramme ont cette nature. L'algorithme est la démarche intellectuelle qui permet de résoudre un problème particulier et, au fond, pour nombre d'applications est d'une nature autre qu'informatique. Ainsi le traitement par l'ordinateur d'une application de statistiques et surtout sa programmation supposent la connaissance de l'algorithme statistique de résolution. Quant à l'organigramme, c'est la traduction de l'algorithme dans « la langue informatique générale ». La connaissance d'un langage de programmation sur le millier recensé aboutit à la traduction de l'organigramme en un programme « source ». On peut se rendre compte des problèmes que cela peut poser : on ne saurait nier qu'algorithmes et organigrammes appartiennent au monde des idées, mais l'importance des implications financières est telle et la spécificité de ceux-ci si marquée que l'exclusion de protection peut sembler choquante dans de nombreux cas.

Le programme « source » est naturellement couvert par le droit d'auteur ; c'est même à cette occasion qu'il peut jouer dans toute sa force. La réponse est plus nuancée pour ce qui est des programmes « objets ». En effet, ceux-ci ne sont lisibles et compréhensibles que par la machine et non plus par l'être hu-

LA PROTECTION DES LOGICIELS

main ; ils sont liés à la fonctionnalité de la machine. Selon l'interprétation des textes, ils devraient être exclus de la protection de la loi. Mais, dans la logique de l'informatique, cette solution ne se comprendrait pas : nier la protection du programme « objet » ne serait-il pas, par contre-coup, porter atteinte à celle du programme « source » ?

Cette question s'est posée à l'étranger. Aux U.S.A., les concepteurs ont obtenu des juges la reconnaissance de la protection du programme « objet » (à l'occasion des instances provoquées par Apple dont l'attitude est particulièrement militante pour tout ce qui touche la poursuite du piratage et des contrefaçons dans le matériel et le logiciel).

Différents types de programmes

Nous passerons ici en revue quelques types de programmes qui peuvent appeler des réponses différentes, ce qui constitue un inconvénient : il faut un régime général de protection du logiciel, quel que soit son type.

● **Les programmes « systèmes ».** Il s'agit de l'ensemble des programmes nécessaires à la mise en route, à la gestion et au fonctionnement de l'ordinateur ; ils s'opposent à ceux qui sont qualifiés de programmes d'application. A la lettre stricte de la loi, appartenant à la « fonctionnalité » de la machine, ils ne seraient pas protégés... si des décisions de justice ne déclaraient pas le contraire (Tribunal de Grande Instance de Paris, ordonnance de référé du 14 juin 1983, à la demande d'Apple France !).

● **Les « progiciels ».** Ils constituent une gamme de logiciels standards de haute qualité, commercialisés en grande quantité, ce qui leur confère un prix attractif, tels Multiplan, Wordstar, dBase II, etc. Ces logiciels représentent aussi un enjeu commercial important. Ils ont, pour les plus connus, été commercialisés dans le monde à plusieurs centaines de milliers d'exemplaires. Et un nombre de copies pirates trois fois plus élevé a été réalisé... Tel est le cas du premier en nombre et en âge de ces logiciels : Visicalc (tableur).

Ces programmes sont standards. Ils répondent souvent à des fonctions de gestion dans l'entreprise ; ils sont « généreux », afin de pouvoir s'appliquer aux maximum de situations concrètes possibles. Ils nécessitent alors de la part de l'utilisateur une programmation minimale, que nous appellerons une reconfiguration destinée à les adapter à la situation voulue.

A cause de ces caractères standards et généraux, ils sont pour la loi « la transposition d'idées dans la machine » et ne peuvent être protégés.

Quoi qu'il en soit, ces grands progiciels sont de nationalité américaine et leurs juristes ont organisé une protection internationale qui s'étend jusqu'à la France...

Encadré 2

DEUX ASSOCIATIONS POUR VOUS DEFENDRE

■ **La Société civile des auteurs multimédia**

La SCAM a pour objet la défense des intérêts matériels et moraux de ses membres et peut être chargée de négocier des contrats avec les éditeurs, de percevoir les redevances dues aux auteurs, de diriger des procédures, etc.

SCAM
38, rue du Fbg-Saint-Jacques
75014 Paris

■ **L'Agence pour la protection des programmes**

En cas de fraude, l'APP peut prendre les mesures qui s'imposent : descente de police ou de justice, établissement du procès-verbal de constatation... L'agence s'est fait remarquer par son rôle moteur dans la descente de police au siège du club Microtel d'Issy-les-Moulineaux.

APP
55, boulevard de La Villette
10 A 5, 75010 Paris

● **Les jeux vidéo.** L'importance économique de ce secteur est considérable : la sortie d'un bon jeu vidéo entraîne aux Etats-Unis une ruée des acheteurs et un chiffre d'affaires du même ordre de grandeur que celui des films les plus courus !

La jurisprudence a eu à statuer sur les jeux. Elle leur a accordé la protection du droit d'auteur, en les assimilant aux œuvres cinématographiques et, quelquefois... en oubliant un peu vite qu'il s'agit de programmes d'ordinateur !

La riposte au piratage

Un auteur a conçu un logiciel et l'a distribué. Plus tard, il constate qu'il a été piraté. Que faire ?

Au point de vue juridique, de multiples actions sont possibles devant les tribunaux ; les plus classiques conduisent à la sanction du fraudeur (**encadré 1**) et à l'indemnisation de l'auteur.

Dans ce cas, ce n'est plus le produit contrefait (et son auteur) qui est poursuivi, mais bien l'agissement du fraudeur et les conséquences que cela entraîne. On demande au « juge civil » la réparation du dommage subi du fait du piratage : manque à gagner comme préjudice moral. Ceci est du ressort d'une des parties fondamentales du droit privé : la responsabilité. Celle-ci prend sa source dans les articles 1382 et suivants du code civil qui prescrit : « *Tout fait de l'homme qui cause à autrui un dommage oblige celui par la faute duquel il est arrivé à le réparer.* »

La mise en jeu de la responsabilité suppose l'existence de trois conditions : une faute, un dommage, un lien entre la faute et le dommage. Après avoir donné au juge la preuve de la présence de ces trois conditions, on lui demandera d'octroyer des dommages et intérêts à hauteur d'un montant que l'on aura évalué. Le juge reste libre de procéder et d'imposer sa propre évaluation.

L'application de la responsabilité à la protection du logiciel prendra la forme de deux actions à poursuivre devant le juge :

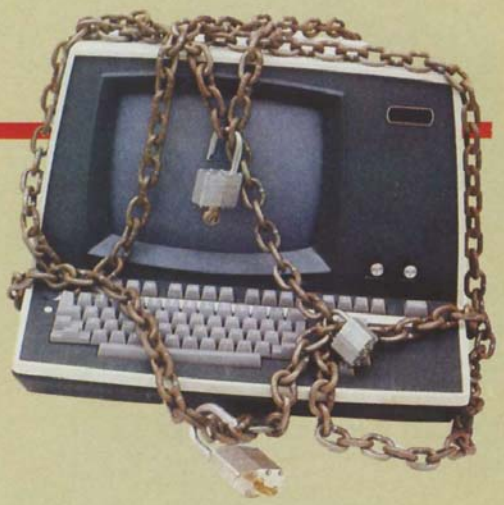
● La concurrence déloyale : elle se manifeste par la confusion dans l'esprit du public entre le logiciel original et la copie piratée. Indépendamment ou de plus, cette concurrence peut entraîner la désorganisation de l'entreprise créatrice.

● L'enrichissement sans cause : c'est de l'enrichissement du fraudeur dont il est question. « Sans cause », puisqu'il aura profité du travail d'un autre sans l'investissement en temps et en argent pour la création du produit.

Le lecteur aura saisi que la meilleure parade est, à l'heure actuelle, la législation du droit d'auteur. C'est la réponse du droit français, mais aussi celle de nombreux autres pays. **S&M**

Th. Piette-Coudol*

* *Enseignant à l'Université des sciences sociales de Grenoble.*



PRATIQUE : LES METHODES POUR VOUS PROTEGER

Les méthodes pratiques de protection des logiciels dépendent étroitement du type d'ordinateur « hôte ». Les diffuseurs de logiciels s'ingénient à protéger leurs programmes par de nombreux moyens. Pour illustrer ces moyens, nous avons choisi plusieurs exemples autour du ZX 81 qui, bien que n'étant pas un micro-ordinateur de « dernière génération », dispose d'un parc de machines important et d'un nombre assez considérable de logiciels. Vous trouverez aussi un tableau regroupant les instructions de protection de six autres micro-ordinateurs parmi les plus répandus.

De nombreux logiciels sont commercialisés sans la moindre protection « technique », leurs diffuseurs ayant pleinement confiance dans leurs capacités commerciales : une vente « éclair » d'un grand nombre de cassettes ou disquettes, grâce à un effort publicitaire important mais bref, ne laisse guère aux pirates le temps de réagir de façon significative.

L'étape suivante consiste à étudier un logiciel dont la mise en œuvre complexe exige le recours permanent à un manuel d'instructions.

Pour peu que ce manuel comporte un très grand nombre de pages, soit imprimé en gris sur un papier bleu ou rouge foncé, soit solidement broché, sa reproduction par photocopie sera si fastidieuse qu'elle en découragera plus d'un.

Notons que le coût de fabrication de cette notice augmente le prix de revient du « produit fini », ce qui nuit à sa compétitivité.

Dans le domaine des protections logicielles, bien des approches passent par un « auto-lancement » du programme dès la fin de son chargement.

S'il s'agit d'un logiciel écrit en langage machine, il est souvent très difficile, voire impossible, d'en interrompre l'exécution, donc *a fortiori* d'en effectuer une sauvegarde.

En Basic, on peut mettre à profit le fait que les variables soient enregistrées en même temps que le programme pour obtenir des protections très discrètes : des variables nécessaires au tout début du programme, mais plus après, peuvent être effacées ou, pire, modifiées après usage. Le logiciel fonctionnera fort bien, mais une copie refusera tout service ou commettra des erreurs, ce qui est assez gênant lorsqu'il s'agit, par exemple, d'un programme comptable ! Le très court exemple de la **figure 1** illustre cette possibilité.

```
10 LET B=A
20 LET A=8
30 PRINT "2+3=";B
40 STOP
50 LET A=5
60 SAVE "RUSE"
70 GOTO 10
```

Fig. 1. – Ce court programme peut être sauvegardé sur cassette par un ordre GOTO 50 ou un simple SAVE. A la relecture, il « s'auto-exécute »... mais les données sont fausses !

LA PROTECTION DES LOGICIELS

Un pirate tentera de copier le programme par un ordre SAVE ou, mieux, par une instruction GOTO 50. Le piège est ainsi invisible, mais agit dès l'exécution d'une copie, quel que soit le moyen employé par un pirate sans méfiance. Notons d'ailleurs que RUN ne fonctionnera pas ! Voir s'afficher une absurdité arithmétique sur l'écran n'est pas trop grave, mais exécuter une série de factures avec un taux de TVA incorrect l'est bien davantage...

Intimider le pirate

Le programme de la **figure 2** fait appel à une ruse plus complexe et bien plus difficile à déceler.

Entre les lignes 50 et 9898 peut être logé n'importe quel logiciel Basic constituant le « vrai programme ».

Tant que la ligne 5 existera, un simple ordre RUN suffira à le lancer.

Entre les lignes 15 et 48 peut se loger un « faux programme », dont l'effet se limite ici à intimider le pirate en puissance, mais pourrait être bien plus subtil...

Une fois notre « vrai programme » au point, supprimons la ligne 5 **sans modifier la ligne 10,** puis lançons une sauvegarde sur cassette en tapant GOTO 9900.

Après cette sauvegarde, ou en cas de rechargement par LOAD, le « vrai programme » est bien exécuté.

Notons que son « listage » devient délicat à cause des deux carctères NEW-LINE (CHR$ 118) qui débutent la ligne REM, trompant ainsi les routines du moniteur.

Si maintenant nous sauvegardons ce programme par un SAVE manuel, le prochain RUN exécutera seulement le « faux programme ».

Les pirates astucieux ne sont pas oubliés pour autant, puisque les choses ne vont guère mieux si la sauvegarde est déclenchée par un GOTO 9900 : la copie est inutilisable et ne peut même pas être listée !

La **figure 3** contient les explications de ces comportements rendus volontairement plutôt déroutants : cette routine en langage machine est indispensable, puisque c'est elle qui élabore le numéro de ligne utilisé par le GOTO de la ligne 9950.

Cependant, cette routine **se modifie elle-même** lors de sa première exécution (par le LD (16521),A), de façon à ce que ses prochaines exécutions bloquent le système par le chargement de la valeur 255 à l'adresse 16509.

Qu'ils sachent bien, cependant, que d'autres programmeurs travaillent avec acharnement dans des buts diamétralement opposés, et, il faut le reconnaître, avec une certaine efficacité.

```
16514 } protection listage { 118
16515 }                    { 118
16516   LD B,Ø                 6     Ø
16518   LD C,5Ø               14    5Ø
16520   LD A,Ø                62     Ø
16522   LD(16509),A           5Ø   125    64
16525   LD A,255              62   255
16527   LD(16521),A           5Ø   137    64
16530   RET                  2Ø1
```

Fig. 3. – Une routine en langage machine se modifiant d'elle-même lors de sa première exécution.

Quelques moyens de copie

Pour conserver notre neutralité vis-à-vis d'un problème qui, nous l'avons vu, est bel et bien à double tranchant, il nous faut examiner les armes des deux puissances en présence. Nous avons étudié les moyens des éditeurs, penchons-nous à présent sur ceux des « copieurs », pirates ou de bonne foi. Nous avons vu que bien des protections faisaient appel à un auto-lancement du logiciel. Il est donc logique de songer à empêcher ce démarrage automatique.

Il existe des « athlètes du BREAK », capables de réagir assez vite pour interrompre la première ligne du programme (toujours écrite en Basic), même après dix ou quinze minutes de chargement.

La **figure 4** fournit cependant une méthode plus fiable, et nettement moins éprouvante pour les nerfs.

```
  1 REM ARRET
 10 FAST
 20 LET K=16514
 30 POKE K,2Ø3
 40 POKE K+1,25Ø
 50 POKE K+2,195
 60 POKE K+3,71
 70 POKE K+4,3
 80 SAVE "ARRET"
 90 RAND USR 16514
100 REM COPYRIGHT 1983
```

Fig. 4. – Un logiciel de chargement « automatique ».

Ce programme étant frappé au clavier, on le sauvegardera sur une cassette au moyen d'un ordre RUN. Rechargé, ce logiciel s'exécutera seul et fera apparaître sur l'écran les images habituellement rencontrées en mode LOAD. En effet, la machine exécute bien cette instruction, mais ne laisse pas de possibilité d'auto-lancement.

Sans agir sur l'ordinateur, lisons dans sa prise EAR (sortie écouteur) une cassette réputée « instoppable » : en fin de chargement devrait apparaître un compte rendu d'erreur après lequel on pourra effectuer un ordre LIST ou SAVE...

La **figure 5** donne quelques indications sur la routine machine incorporée dans ce programme, qui appelle simplement le sous-programme LOAD de la ROM Sinclair, mais en cours d'exécution.

Faut-il préciser que la routine machine étant logée dans la ligne 1, nous ne pouvons ni supprimer ni modifier celle-ci.

Ce procédé donne satisfaction dans la

```
16514   SET 7,D     2Ø3  25Ø
16516   JP 839      195   71   3
```

Fig. 5. – Quelques indications concernant la routine « LOAD » de la ROM Sinclair.

```
 5 GOTO 50
10 REM COPYRIGHT (C) 1983
15 REM CECI EST LE FAUX PROGRA
ME"
20 PRINT "POURQUOI ESSAYER DE
IRATER"
30 PRINT
40 PRINT "CE PROGRAMME ? ....."
."
45 REM IL SE TERMINE ICI
49 STOP
50 PRINT "VOICI LE VRAI PROGRA
MME"
1000 PRINT "IL SE TERMINE ICI"
9898 PRINT
9899 STOP
9900 LET A$="11811800500001405Ø0
52000050125064006225505013706420 1
:
3910 FOR F=1 TO 17
3920 POKE 16513+F,VAL A$((3*F)-2
 TO 3*F)
3930 NEXT F
3940 SAVE "PROGRAMME"
3950 GOTO USR 16516
```

Fig. 2. – Un faux programme est intercalé pour « intimider » le pirate...

DES INSTRUCTIONS POUR VOUS PROTEGER

Si vous programmez en Basic, plusieurs moyens sont à votre disposition pour protéger vos programmes.

Il vous sera possible de les sauvegarder sous forme protégée lorsque votre interpréteur Basic possède cette fonction : on ne pourra ni les lister ni les modifier. Méfiez-vous cependant, car beaucoup de ces protections ont été contournées (celles du TI 99 ou du TO 7, par exemple).

Certains ordinateurs « de poche » possèdent des mots de passe protégeant théoriquement l'utilisateur. Mais, là aussi, de nombreux mots de passe ont été déplombés (PC 1401, HP75C).

Vous pouvez aussi insérer des codes de contrôle dans votre listing pour le rendre illisible à l'écran.

Afin de protéger votre programme pendant qu'il s'exécute, pourquoi ne pas rendre impuissantes certaines commandes du Basic ? Par exemple, empêcher le LIST, inhiber le « Break » et le « Reset ». Ainsi, l'utilisateur de votre programme ne pourra pas « reprendre la main » et analyser votre programme.

Le **tableau** ci-contre indique quelques-unes des manœuvres à effectuer sur la plupart des micro-ordinateurs personnels.

Enfin, si vous avez la chance de posséder un micro professionnel, il vous est possible d'acquérir un compilateur Basic et de compiler votre programme. Certes, il ne sera pas protégé contre les duplications, mais votre programme source sera à l'abri de toute indiscrétion. ***M.-P. Olivier***
D. Mavrakis

Micro-ordinateur	Manipulations à effectuer
PC 1500	POKE # &F01D,&FF rend le Break inopérant POKE # &F01D,&00 rétablit le Break
Apple II	POKE 2049,0:POKE 2050,0 empêchant le listing d'un programme en mettant à zéro le pointeur de début de la 2e ligne d'instructions. Pour annuler le « Control-C » : 1 ON ERR GOTO 1000 1000 IF PEEK(222)=255 THEN RESUME En effet « Controle-C » génère le code d'erreur 255. Avec POKE 214,128, toutes les commandes BASIC sont interprétées comme RUN. On peut inhiber le Reset de différentes façons parfois assez compliquées.
Oric 1 Atmos	Pour protéger un programme : – le sauver sur casette en mode AUTO – les 2 premières instructions doivent être : POKE 555,96 (Oric 1) ou POKE #247,96 (Atmos) qui inhibe la touche Reset. POKE#1B,#2F42D provoque une réinitialisation complète du système lors d'un « Control-C ».
TRS 80	POKE 16873,195 ou POKE 16874,114 ou encore POKE 16875,0 bloquant List. POKE 16863,201 débloque List.
Commodore 64 CBM 64	POKE 2049,0 ou POKE 775,200 empêchent le listing POKE 775,167 rétablit le listing POKE 788,PEEK(788)+3 inhibe Stop POKE 788,PEEK(788)–3 rétablit le Stop POKE 808,225 :POKE 818,32 interdit List et Save POKE 808,237 :POKE 818,237 rétablit les deux POKE 808,225 bloque Stop et Restore POKE 808,237 rétablit les deux
CBM	POKE 1025,0 empêche le listing POKE 144,PEEK(144)+3 inhibe le Stop POKE 144,PEEK(144)–3 rétablit le Stop

plupart des cas, mais on peut bien sûr trouver des « contre-mesures » qui, appliquées lors de l'enregistrement, rendront son utilisation délicate : on compliquera, par exemple, singulièrement la tâche du copiste en fractionnant le programme en plusieurs enregistrements se chargeant les uns les autres.

Normalement, bien sûr, seul le dernier d'entre eux pourra être utilisé, puisque chaque chargement (LOAD) commence par effectuer un NEW. Seulement, il existe des opérations qui résistent à un NEW, et notamment les modifications de la variable système RAMTOP (position d'adresse en mémoire vive). Sur une cassette, enregistrons l'un derrière l'autre les deux programmes de la **figure 6** (il suffit de taper RUN).

On pourra alors vérifier que les deux chargements s'enchaînent fort bien au moyen d'un simple LOAD " ", mais que le second programme ne pourra pas être chargé seul : il s'efface lui-même. **S&M**
P. Gueulle

```
10 SAVE "PROGRAMME 1"
20 POKE 16389,60
30 LOAD "PROGRAMME 1"
```

```
10 SAVE "PROGRAMME 1"
20 IF PEEK 16389<>60
   THEN NEW
30 PRINT "PROGRAMME 2
   EN COURS
```

Fig. 6. – Ces deux programmes peuvent être chargés l'un après l'autre. Mais le second ne peut l'être seul (sous peine de « s'auto-détruire »).