



CENTRE REGIONAL ASSOCIE DE STRASBOURG

Filière Informatique Conception et Développement

ORAL PROBATOIRE

ROMARY Fabien

fabienromary@ifrance.com

Protection du logiciel

Soutenu le 27 Mai 2004

JURY

PRESIDENT: C. KAISER

**MEMBRES : J. HATTON
L. BERTEAU
J.L STEFFAN**

RAPPEL DU SUJET

La diminution des coûts du matériel de copie numérique ainsi que le développement des communications en haut débit génère de manière exponentielle l'utilisation de copies numériques identiques aux originaux sans s'acquitter des droits d'auteurs. Les solutions les plus sûres ne sont plus d'actualité, les « dongles » ou bouchon de protection par exemple coûtent chers et s'ajoutent aux prix dans la chaîne de distribution rendant encore plus tentant le piratage. La crise touche d'abord les produits culturels (CD, DVD, Jeux) et les logiciels mais l'utilisateur prenant la mauvaise habitude de ne plus payer, la nécessité de protéger tous les développements devient une préoccupation majeure.

Quelles sont les nouvelles protections informatiques mises en place pour protéger les logiciels ?

Quels sont leurs efficacités et leurs coûts ?

Comment intégrer la perte due aux actes de piraterie lors d'un chiffrage de projet informatique ?

A l'aide d'exemples concrets le candidat illustrera les solutions possibles pour éviter une diffusion incontrôlée des logiciels produits. A l'heure de la vidéo à la demande, de la diffusion d'application par location et téléchargement, ce problème n'a-t-il pas été sous-estimé ?

REMERCIEMENTS

Je tiens tout d'abord à remercier **M. Hatton**, responsable du sujet, qui m'a permis d'approfondir un domaine dont j'ignorais l'ampleur.

Ensuite je remercie **M. Steffan**, responsable de filière, pour ses critiques et conseils dans la préparation du probatoire. J'en profite également pour remercier le **président ainsi que tous les membres du jury**.

Je remercie également **toutes les entreprises que j'ai contactées**, et qui ont bien voulu répondre à mes questions en m'accordant un peu de leur temps.

Pour ses corrections grammaticales, orthographiques et surtout sa compréhension, je tiens à remercier **Marie**, ma compagne.

Enfin je voudrais rajouter une mention spéciale à **Mme Meyrueis**, professeur de droit spécialiste en propriété industrielle au CEIPI, et **M. Besseghir**, responsable informatique à la CCI, pour leur disponibilité, ainsi que le temps qu'ils ont bien voulu me consacrer.

SOMMAIRE

Introduction	p4
1. Etat des lieux	p5
2. Organisation du piratage	p12
3. Nouvelles protections	p19
4. Etude de cas	p26
Conclusion	p29
Glossaire	p31
Bibliographie	p32
Annexe	p33
Table des matières	p35

Les références entre crochets [], renvoient à la **bibliographie**. Les éléments dans le texte, en italiques sont explicités dans le **glossaire**.

Introduction

Aujourd'hui, les ordinateurs sont destinés à de multiples utilisations : jouer, regarder un film, écouter de la musique, travailler sur des outils bureautiques, de CAO, DAO... Tout a pu se faire grâce aux progrès technologiques, ainsi qu'à l'ergonomie des systèmes d'exploitations. Internet a également permis un accès aisé à l'information. Ceci a encore été facilité par les réseaux haut débit.

Avec l'ADSL, il est maintenant possible d'accéder à des nouveaux services, comme la location à la demande des jeux vidéos, logiciels et films. Il est même possible de mettre en partage des fichiers afin d'échanger facilement avec tous les internautes.

Les supports vierges sont également bon marché ainsi que les graveurs de CD et DVD. Ainsi tout ce qui est téléchargé d'Internet peut être facilement mis à la disposition de la famille ou des amis.

Dans cette description presque idéale de l'informatique, qu'est-ce qui pourrait bien ternir et justifier le titre de ce probatoire sur la « protection du logiciel » ?

Il s'agit de la contrefaçon. Le piratage est au cœur même de la contrefaçon. Il n'existe actuellement aucune technique permettant d'éradiquer le piratage. Le piratage nuit aux auteurs, mais aussi aux utilisateurs. La protection du logiciel existe car il y a de la contrefaçon. Ces deux notions sont liées et seront présentes tout au long du dossier.

Le sujet du probatoire apportent un certain nombre de questions auxquelles nous allons tenter de répondre. Quelles sont les nouvelles protections informatiques mises en place pour protéger les logiciels ? Quelles sont leurs efficacités et leurs coûts ? Comment intégrer la perte due aux actes de piraterie lors d'un chiffrage de projet informatique ? A l'heure de la vidéo à la demande, de la diffusion d'application par location et téléchargement, ce problème n'a t'il pas été sous estimé ?

Pour répondre à ces questions, nous allons établir un plan en quatre parties. La première partie fera un **état des lieux** sur les solutions qui existent actuellement pour protéger les logiciels. Ensuite nous verrons l'**organisation du piratage**, et nous tenterons de comprendre ce qui en justifie son existence. Dans le troisième chapitre nous ferons un tour d'horizon des **nouvelles protections** existantes ou à venir. Enfin nous terminerons avec une **étude de cas**, et plus particulièrement sur des entreprises auditées dans le Bas-Rhin.

1. Etat des lieux

1.1. Cadre juridique

Les textes et articles de loi cités ci-dessous sont issus du code de la propriété intellectuelle [PROP2002].

1.1.1. loi du 3 juillet 1985 : droits d'auteurs de logiciels

Avant la création de la loi du 3 juillet 1985, les droits d'auteurs sur les logiciels sont les mêmes que pour toutes autres créations artistiques.

La **loi n°85-660 du 3 Juillet 1985** vient donc ajouter un certain nombre d'articles spécifiques à la protection des logiciels.

- Art. 45. Sauf stipulation contraire, le logiciel créé par un ou plusieurs employés dans l'exercice de leurs fonctions appartient à l'employeur auquel sont dévolus tous les droits reconnus aux auteurs.

Toute contestation sur l'application du premier alinéa du présent article est soumise au tribunal de grande instance du siège social de l'employeur.

Les dispositions du premier alinéa du présent article sont également applicables aux agents de l'Etat, des collectivités publiques et des établissements publics à caractère administratif.

- Art. 46. Sauf stipulation contraire, l'auteur ne peut s'opposer à l'adaptation du logiciel dans la limite des droits qu'il a cédés, ni exercer son droit de repentir ou de retrait.
- Art. 47. Par dérogation au 2 de l'article 41 de la loi n 57-298 du 11 Mars 1957 précité, toute reproduction autre que l'établissement d'une copie de sauvegarde par l'utilisateur ainsi que toute utilisation d'une copie de sauvegarde par l'utilisateur ainsi que toute utilisation d'un logiciel non expressément autorisée par l'auteur ou ses ayants droits, est passible des sanctions prévues par ladite loi.
- Art. 48. Les droits objets du présent titre s'éteignent à l'expiration d'une période de vingt-cinq années comptée de la date de la création du logiciel.
- Art. 49. Le prix de cession des droits portant sur un logiciel peut être forfaitaire.
- Art. 50. En matière de logiciels, la saisie-contrefaçon est exécutée en vertu d'une ordonnance rendue sur requête par le président du tribunal de grande instance. Le président autorise, s'il y a lieu, la saisie réelle.

L'huissier instrumentaire ou le commissaire de police peut être assisté d'un expert désigné par le requérant.

A défaut d'assignation ou de citation dans la quinzaine de la saisie, la saisie contrefaçon est nulle.

En outre, les commissaires de police sont tenus, à la demande de tout auteur d'un logiciel protégé par la présente loi ou ses ayants droit, d'opérer une saisie-description du logiciel contrefaisant, saisie-description qui peut se concrétiser par une copie.

- Art. 51. Sous réserve des conventions internationales, les étrangers jouissent en France des droits reconnus par le présent titre, sous la condition que la loi de l'Etat dont ils sont les nationaux ou sur le territoire duquel ils ont leur domicile, leur siège social ou un établissement effectif accorde sa protection aux logiciels créés par les nationaux français et par les personnes ayant en France leur domicile ou un établissement effectif.

1.1.2. loi du 10 mai 1994

La loi du **10 mai 1994** est une transposition au droit français de la directive européenne du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et la loi du **5 février 1994** relative à la répression de la contrefaçon.

a) Contrefaçon

Textes	Définition / Sanctions
Article L.335-3	« Est (...) un délit de contrefaçon la violation de l'un des droits de l'auteur de logiciel [...] »
Article L.122-4	« Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur [...] est illicite »
Article L.335-2	« La contrefaçon en France [...] est punie de deux ans d'emprisonnement et de 150 000 € d'amende, ce montant peut être multiplié par cinq dans le cas d'une personne morale »

Le piratage informatique est considéré comme **faute grave**.

b) Décompilation

La décompilation (voir *Ingénierie Inverse*) est l'opération qui consiste à traduire la version objet du logiciel (langage utilisé par la machine pour exécuter le programme) dans le langage dans lequel le logiciel a été programmé (codes sources).

En principe, la décompilation est soumise à l'autorisation de l'auteur du logiciel conformément aux dispositions de l'article L. 122-6 du C.P.I. Elle peut cependant être réalisée contre la volonté de l'auteur dans le seul but de permettre l'interopérabilité des logiciels (article L. 122-6-1 al. IV). Voir [BEN94] pour des compléments d'informations.

En effet, la décompilation à des fins d'interopérabilité est un droit d'ordre public et l'auteur ne peut interdire l'exercice de ce droit dans le contrat de licence (article L. 122-6-1 al. V).

L'interopérabilité des logiciels se définit comme "la capacité des programmes d'ordinateur d'échanger des informations et d'utiliser mutuellement ces informations" (Directive du 14 mai 1991, relative à la protection juridique des programmes d'ordinateur).

1.1.3. Brevet logiciel

Les brevets logiciels en Europe existent depuis 1986. Le logiciel comme algorithme n'est pas brevetable, mais il l'est comme solution technique à un problème technique. Au contraire, le droit d'auteur est destiné à protéger l'expression de l'œuvre, et non les concepts qui sous-tendent sa conception. Les deux instruments ne s'excluent donc pas l'un l'autre, ils sont complémentaires.

Le droit d'auteur ne fournit aucune protection contre les *hackers*, comme le montre la jurisprudence. Par exemple, pour obtenir gain de cause en cas de plagiat, le seul moyen sûr est de prouver le vol du support matériel ou la corruption de l'un des employés. Mais plus grave encore : le droit d'auteur n'est pas publié dans une base internationale. Par conséquent, il confère des droits dont la nature et la portée ne peuvent être ni vérifiés, ni analysés avant qu'ils ne soient opposés à un tiers. Par contraste, les brevets sont consultables dans une base internationale ou nationale et on est tenu de faire une recherche d'antériorité lorsqu'on dépose un brevet. Pour consulter gratuitement l'ensemble des brevets, il suffit de contacter l'Office Européen des Brevets (OEB) <http://www.espacenet.com>

1.2. Mise en application

Afin de faire appliquer la loi, et d'aider les entreprises dans leurs actions en justice, de nombreux organismes ont été créés, le plus souvent au sein d'associations. Nous ne verrons que quelques organismes, mais il en existe beaucoup d'autres, chargés de défendre les intérêts communs des droits d'auteurs.

1.2.1. APP

L'agence pour la protection des programmes (APP) est un organisme européen, chargé de défendre les droits des auteurs de programme, particulier ou professionnel. L'adhésion est payante, et donne droit à un numéro d'identification (IDDN) pour chaque logiciel à protéger. En cas de contrefaçon, l'organisme opposera le logiciel enregistré (avec sources, documentations techniques à l'appui) à celui contrefait.

L'APP compte plus de 8000 membres et a pris part à plus de 1000 actions en justice. L'APP est l'un des membres fondateurs de InterDeposit, qui a mis au point les numéros d'identification IDDN (InterDeposit Digital Number). L'adhésion pour un particulier est d'environ 200€ et pour une société, 800€, ensuite la redevance est annuelle.

1.2.2. BSA

Le BSA, Business Software Alliance, est une organisation mondiale qui lutte contre la contrefaçon des logiciels. Les membres de cette organisation sont des multinationales comme Adobe, BVRP, Microsoft, Symantec...

L'évolution du piratage professionnel dans le monde entre 1994 et 2002 est la suivante :

Région	1994	2002
Europe occidentale	52 %	35 %
Europe orientale	85 %	71 %
Moyen-Orient/Afrique	80 %	49 %
Amérique du Nord	32 %	24 %
Amérique latine	78 %	55 %
Asie/Pacifique	68 %	55 %

Evolution du piratage entre 1994 et 2002 Source : www.bsa.org

On constate une baisse significative, cependant la proportion de produits piratés reste très élevée : 4 produits sur 10 dans le monde sont illicites.

1.2.3. RIAA / Sacem

Le RIAA (Recording Industry Association of America) est l'organisme de défense des droits d'auteurs aux Etats Unis. Cet organisme est fortement impliqué dans la lutte contre le piratage des œuvres musicales. Chaque pays dispose d'un dispositif équivalent. En France, nous avons la Sacem. Il existe également des organisations équivalentes pour les œuvres audiovisuelles (MPAA).

Il s'agit d'organismes puissants, puisque chargés de protéger tous les artistes, et disposant de l'aval des autorités judiciaires. La coopération avec la police est systématique afin de lutter contre les délits.

1.3. Protections existantes

Depuis les débuts de la création logicielle, la protection a été intégrée dans les processus de développement. Divers techniques ont été élaborées, avec un but unique : réduire le piratage. Les protections techniques ne sont pas présentées de façon exhaustive. Il existe quasiment autant de protections qu'il existe d'éditeurs de logiciels. En général les techniques sont combinées entre elles afin d'accroître la protection.

1.3.1. Algorithme de codification des informations : RSA

Quelque soit la manière de protéger les logiciels (matériel ou logiciel), il faut coder les numéros de série afin que l'on ne puisse pas les retrouver facilement à l'aide d'un *déboguer*.

Pour cela, des mécanismes de cryptographie sont mis en place. Il en existe deux types : les systèmes à clé privée (cryptage symétrique) et à clé publique (appelé le chiffrement asymétrique, implique une paire de clé).

Le système à clé symétrique le plus connu est le DES (Data Encryption Standard), remplacé par le 3DES puis par l'AES (Advanced Encryption Standard) à cause de problèmes de faille connus et exploités par les *hackers*. Le système à clé asymétrique le plus connu est le RSA c'est aujourd'hui le plus utilisé pour le cryptage des données.

Nous n'allons aborder ici qu'un seul type : le code RSA [CRYPTO95] inventé par les mathématiciens Rivest, Shamir et Adleman en 1977 au MIT, Massachusetts Institute of Technology.

C'est le principe des clés publiques et clés privées : tout le monde peut m'envoyer un message crypté (la clé de chiffrement est publique donc tout le monde peut la connaître) mais je serais le seul à pouvoir le décrypter (la clé de déchiffrement est privée = secrète et "on ne peut pas" la retrouver à partir de la clé de chiffrement publique).

Algorithme de génération d'une clé RSA :

Initialisation

1. Choisir deux nombres premiers, p et q , les deux étant plus grands que 10^{100}
2. Calculer $n = p \cdot q$
3. Choisir e aléatoire tel que e et $((p - 1) \cdot (q - 1))$ n'aient aucun facteur commun excepté 1
4. Trouver d tel que $(e \cdot d)$ soit divisible par $((p - 1) \cdot (q - 1))$,
donc : $ed = 1 \bmod((p - 1)(q - 1))$

Clé publique : (n, e) .

Clé privée : (n, d) ou (p, q, d) si on désire garder p et q .

Chiffrement/Déchiffrement

1. L'expéditeur crée le texte chiffré c à partir du message m :
 $c = m^e \bmod(n)$, où (n, e) est la clé publique du destinataire.
2. Le destinataire reçoit c et effectue le déchiffrement :
 $m = c^d \bmod(n)$, où (n, d) est la clé privée du destinataire.

Exemple simple

0) Prenons un alphabet simple de trois lettres a, b et c.

Prenons pour codage de cet alphabet : a = 1, b = 2 et c = 3.

1) Il faut choisir deux nombres premiers secrets : $P = 2$ et $Q = 5$:

2) Le nombre public est alors : $N = p \cdot q = 2 \cdot 5 = 10$ (le nombre n est public mais il n'est pas actuellement possible de retrouver les deux entiers p et q lorsque n est très grand)

3) on a aussi besoin de : $N' = (p-1)(q-1) = 1 \cdot 4 = 4$ (secret)

On choisit la clé privée (secrète) : $E = 3$

5) Il faut maintenant trouver la clé publique : E

Critères de choix : e doit être positif et tel que $-k \cdot n' + e \cdot d = 1$ donc ici e est tel que : $-k \cdot 4 + E \cdot 3 = 1$

"Descente" : Algorithme d'Euclide : $4 = 1 \cdot 3 + 1$

"Remontée" : $4 - 1 \cdot 3 = 1$ or $1 = (4 - 3)$

on remplace $4 - (4 - 3) \cdot 3 = 1$

on développe $4 - 4 \cdot 3 + 3 \cdot 3 = 1$

"Au final" : $-2*4 + 3*3 = 1$
 donc la clé publique $E = 3$

Message	Codé	Crypté	Décrypté
bac	2,1,3	$2^e = 2^3 = 8$; reste (8 : 10) = 8 $1^e = 1^3 = 1$; reste (1 : 10) = 1 $3^e = 3^3 = 27$; reste (27 : 10)=7 message crypté : 8, 1, 7	$8^d = 8^3 = 512$; reste (512 : 10) =2 $1^d = 1^3 = 1$; reste (1 : 10) = 1 $7^d = 7^3 = 342$; reste (343 : 10) = 3 on retrouve bien : 2, 1, 3.

L'implémentation en langage C de l'algorithme RSA en fournit en annexe 1

1.3.2. Logiciel

a) activation par disquette

Cette technique oblige l'utilisateur à insérer une disquette avant la première utilisation du logiciel. Cette disquette est réputée impossible à recopier.

b) numéros de série

Le numéro de série est un moyen classique de protection. Il s'agit pour le programme de demander la saisie d'un numéro de série, afin de pouvoir utiliser le logiciel. Si le numéro est incorrect, plusieurs cas de figures peuvent apparaître :

- le logiciel est bridé (on parle alors de version de démonstration)
- il ne s'exécute pas du tout
- il s'exécute sans limitation pendant une période définie

Le plus souvent les numéros de série sont définis après paiement par l'utilisateur. Les numéros sont uniques et ne peuvent être cédés à des tiers. Pour protéger la saisie des numéros de série, les programmes sont protégés à l'aide d'algorithmes de cryptographie.

Ce mode de protection est celui qui est le plus couramment utilisé. Les numéros saisis vont en général de 8 à 16 caractères. Ceux ci peuvent être alphanumériques.

Parfois la protection doit être validée par une connexion à internet. Ceci permet à l'éditeur de vérifier que l'utilisateur est bien enregistré mais également de permettre les mises à jours du logiciel.

c) activation par Internet

Introduit assez récemment, surtout depuis la mise sur le marché de Windows XP fin 2001, l'utilisateur se voit contraint, pour pouvoir utiliser le logiciel de l'enregistrer par internet. L'opération consiste à saisir le numéro de série unique indiqué sur la boîte lors de l'achat du logiciel. Si le numéro saisi n'existe pas encore dans la base de données de l'éditeur alors l'utilisation du logiciel est autorisée, sinon l'utilisation du logiciel sera bloquée après un certain temps d'utilisation. Par exemple Windows XP se bloque après un mois d'utilisation si le numéro de série n'est pas correctement indiqué.

Ce procédé empêche l'installation sur un autre ordinateur. Cependant en désactivant l'installation du produit, ou alors en cas de problème, en appelant le support du logiciel, il est possible d'installer le logiciel sur une autre machine, en déclinant son identité.

Afin d'éviter l'activation de produits illicites, l'éditeur compare le numéro de série saisi avec une base de données de numéros contrefaits. Cette base de données est produite à l'aide des numéros circulant sur les forums *warez* sur Internet. L'éditeur ne récupère pas de numéro lors de la saisie : aucune information n'est collectée. Cependant, l'éditeur, peut facilement connaître le nombre d'utilisateurs pirates essayant d'activer leur logiciel. Cette

procédure s'est généralisée dans toute la gamme Microsoft (Office...), ainsi que chez de nombreux autres éditeurs (Symantec...).

d) activation par téléphone

Le processus est le même que l'activation par Internet, sauf que cette fois la procédure s'applique par téléphone.

e) compression des exécutables

Afin d'éviter de pouvoir relire trop facilement un fichier exécutable, les développeurs appliquent des compressions sur leurs exécutables. Ainsi il devient plus difficile de relire en mémoire l'exécution du programme

f) nom des variables sensible

Les variables définissant les tests sur les numéros de série ne doivent pas être explicites afin d'éviter une recherche trop facile à l'aide d'un éditeur hexadécimal. Cette règle est valable pour tous les environnements de développement.

1.3.3. Matériel

a) dongle

Le *dongle* est une protection matérielle qui se branche sur les ports de communication de l'ordinateur. Au départ sur port parallèle et depuis quelques années sur le port USB.

Le principe est simple : le programme effectue un test de présence du *dongle*, si celui-ci est absent le logiciel se bloque, sinon le logiciel fonctionne.

b) DVD Vidéo : le CSS

Dès les débuts de la création du DVD en 1995, l'objectif a été de ne pas reproduire les erreurs faites avec les CD Audio : créer un support difficile à dupliquer. Pour cela plusieurs protections ont été mises en place dont le CSS.

Le CSS (Content Scrambling System) consiste à crypter certaines données du support afin d'en interdire la copie numérique. Les données sont décryptées à l'aide d'une clé de décryptage, stockée sur le support, qui permet la lecture du DVD-Vidéo.

Cette protection vient en complément de deux autres protections. La première APS (Analog Protection System), plus connue sous le nom de Macrovision rend impossible la copie d'un DVD-Vidéo sur une cassette vidéo. La seconde protection est commerciale, puisqu'il s'agit du zonage. L'Europe est en zone 1, tandis que l'Amérique en zone 2. Cela évite que des DVD disponibles dans un pays ne circulent dans d'autres pays avant leur sortie au cinéma par exemple (d'autant plus lorsque ces deux pays ont une langue commune).

Une autre protection indirecte pour limiter la copie, provient du fait que les supports vierges vendus sur le marché (DVD-R...) ont une taille inférieure au DVD-Vidéo (4,3 Go pour les DVD vierges et 4,7 Go ou plus pour les DVD-Vidéo).

Et la copie de sauvegarde à usage privé dans tout ça ? Les producteurs se défendent en donnant comme argument la parfaite fiabilité du support. Cependant aucun moyen de réaliser une copie de sauvegarde n'est fournie. De toute façon la loi oblige la mise à disposition d'une copie de sauvegarde si celle-ci n'est pas réalisable. Il suffit donc d'écrire au revendeur en justifiant d'une preuve d'achat...

c) SEP : Système d'élimination du piratage

Ce système [SEP] bien qu'existant sur le papier depuis plus de deux ans, n'a jamais été porté sur le marché. Pourtant le concept part d'un constat très simple : les logiciels sont

piratés car les supports vierges (CD, DVD...) ne contiennent aucune protection pour éviter la propagation.

Partant de ce constat, le concepteur, Antonio Ibáñez, directeur R&D, a créé une puce à installer sur les graveurs, ainsi qu'une carte d'identité pour CD, à l'aide d'une clé de un à huit millions de chiffres. Cette clé est réputée presque impossible à falsifier. Si l'identification de la clé échoue, alors le CD ne peut être lu et pire il aurait été possible de rayer matériellement le support.

Le système pour qu'il fonctionne devait recevoir l'adhésion de toutes la chaîne des fabricants (de graveur, et de CD/DVD). Ce ne fut pas le cas, le projet n'a jamais été mis sur le marché. Pourtant le projet aurait permis, d'après le concepteur d'éradiquer le piratage en cinq ans.

Comme souvent dans le domaine des supports physiques, l'adhésion est rarement au rendez-vous. C'est pourquoi dès l'instant qu'une solution est réputée meilleure que les autres, si le concepteur en a les moyens il développe une solution propriétaire. C'est le cas depuis longtemps pour les consoles de jeux.

N'oublions pas, que les gouvernements ont mis en place la taxe sur les copies privées, qui s'étend à tous les supports vierges. Cette taxe permet de compenser les pertes dues au piratage dans les secteurs audio et audiovisuel. Cette taxe ne s'applique pas au domaine du logiciel, alors que pourtant celui ci est autant touché par le piratage.

C'est pourquoi il n'est pas vraisemblable qu'une protection d'un support média vierge face l'adhésion aujourd'hui. Par ailleurs toutes les méthodes (il y en a eu de nombreuses) réputées très efficaces et permettant d'éradiquer totalement le piratage n'ont jamais connu de franc succès ou n'ont pour la plupart jamais abouti.

2. Organisation du piratage

Dans ce chapitre, nous allons nous intéresser aux raisons du piratage ainsi qu'aux moyens mis en œuvre pour pirater. En effet, il m'a semblé important dans un dossier consacré à la protection du logiciel de savoir pourquoi finalement on s'évertue à créer de nouvelles protections toujours plus efficaces. Piratage et protection sont liés.

2.1. Pourquoi le piratage

Avant de comprendre par quels biais les logiciels sont piratés, nous allons nous intéresser aux raisons techniques.

2.1.1. Raison technique

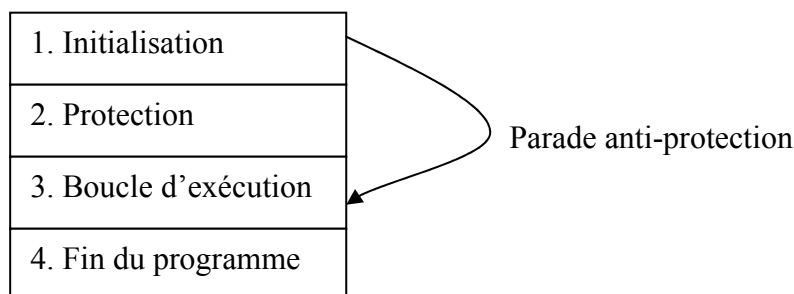
Nous l'avons vu au chapitre précédent, il existe une pléthore de moyen de protéger un logiciel. Pourtant les actes de piratage sont nombreux. La raison est que bien souvent les pirates contournent les systèmes de sécurité.

Prenons l'exemple d'une maison avec une porte de sécurité. Si cette maison possède 4 points de sécurité, il ne sert à rien d'en faire installer 10. De même en cryptographie, inutile d'installer un algorithme RSA à 2048 bits si le système possède déjà un algorithme RSA à 1024 bits.

En effet un pirate, comme un cambrioleur, préférera passer outre le système de sécurité. Une anecdote raconte qu'aux Etats Unis, en Californie, un groupe de voleurs organisé mettait à défaut les systèmes de sécurité en attaquant les murs à la tronçonneuse. Qu'est-il encore possible de faire contre ce type d'attaque ?

Un excellent article de Bruce Schneier [SCHN03] dirigeant d'une importante société de sécurité se contente de rappeler que « **les attaquants intelligents se contentent de contourner les algorithmes** ».

Pour illustrer cela, voici un exemple classique, afin de détourner un système de protection :



Comme illustrer dans ce schéma, il vaut mieux contourner une protection, plutôt que d'essayer d'en résoudre la complexité.

2.1.2. Raison économique et sociale

Nous venons de le voir, il est techniquement possible de pirater tous les types de programmes, même ceux disposant des meilleures protections. Alors dans ce cas tous les possesseurs d'ordinateur sont-ils des pirates ?

En fait, le problème du piratage tient aussi du domaine économique et sociale. Les logiciels, même s'ils sont vendus sous forme de support physique (CD, DVD...), ne sont pas matériellement représentables. Alors qu'il est facile de représenter un marteau, une scie ou une chaussure, comment représenter un logiciel ? Un logiciel est une représentation de l'esprit, un objet de l'art. Dans ce cas difficile d'évaluer ce que coûte réellement un logiciel. Comment expliquer que pour un même support un logiciel peut coûter 50, 500 ou 50000€ ? Les prix sont certes justifiés par les temps de développement ainsi que par la complexité, mais en contrepartie, ils peuvent être reproduits et revendus à l'infinie. Ce problème de la

représentation est quelque chose de très difficile à intégrer pour un utilisateur. Comment savoir que le prix que l'on paye pour un produit est le juste prix ?

Ce problème économique est d'autant plus difficile, à intégrer, que se procurer un logiciel est d'autant plus facile. Il suffit qu'une version soit à la disposition d'un utilisateur, pour que le monde entier puisse se la procurer. Comment comparer cela avec l'achat d'un marteau par exemple. Il sera certes possible de prêter le marteau, mais alors dans ce cas, il ne sera plus possible de l'utiliser pour soi.

En outre Internet, à largement contribué à l'expansion du piratage. Celui ci ayant atteint son paroxysme par l'absence de support et la dématérialisation totale des échanges entre utilisateurs. Internet possède donc la triste réputation de paradis pour le pirate. Cependant cette réputation est à nuancer avec l'accès à la richesse d'informations que ce média permet.

L'offre à haut débit ADSL, aujourd'hui proposée par les opérateurs a permis à Internet de se démocratiser et de proposer de nouveaux services à des utilisateurs plus nombreux et ayant moins de connaissances techniques. Il n'est nullement besoin d'être informaticien pour avoir le profil d'un pirate.

2.2. Formes

Lorsque l'on voit, au chapitre 1, l'armada de protections existantes, ainsi que tout le cadre juridique mis en œuvre, on peut se demander pourquoi il y a tant de copies illégales. Pourtant nous allons voir qu'il est très facile pour tout néophyte de télécharger des copies illégales sur internet.

Internet est un outil formidable qui permet une communication et un accès à l'information très rapide grâce notamment aux moteurs de recherche, mais aussi aux e-mail, forums, messageries instantanées (msn, icq...) et tout ce qui fait le succès d'Internet aujourd'hui.

Les serveurs proposant les logiciels se situent dans des pays où la loi pour la protection du droit d'auteur n'est pas appliquée (Russie, Europe de l'est...). Les auteurs de ces méfaits, sont bien souvent impunis.

Ce qui est encore plus grave c'est que certaines bandes organisées, vendent les logiciels sous la forme de téléchargement ou d'envois de CD piraté, contre paiement !

En parallèle au chapitre 1.3, nous allons voir dans ce chapitre qu'il existe de nombreuses méthodes afin de récupérer des versions non autorisées des logiciels. La plupart des méthodes exposées ici se trouvent sur [HALTE02].

2.2.1. Logiciel

a) Ingénierie Inverse

L'*Ingénierie inverse* consiste à reconstituer un algorithme de création du logiciel, à partir du langage machine. Le langage machine est affiché à l'aide d'un *déboguer*.

Le logiciel historique livré sous MS-DOS nommé debug, permettait déjà de réaliser cette opération. Aujourd'hui des produits comme SoftIce permettent de déboguer de façon souple une application en temps réel.

Sur Internet, il est très facile de se former au débogage d'application. Il suffit d'être à l'aise en assembleur afin d'écrire toutes sortes d'applications afin de faire sauter les protections. Ainsi il est possible d'écrire :

- **des patches**

Le *patch* consiste à modifier le code d'un exécutable afin d'éviter les mécanismes de protection. Ainsi aucun numéro de série n'est demandé lors du lancement du logiciel.

- **des générateurs de clés (key maker)**

Le générateur de clé permet de généraliser la saisie du nom d'utilisateur et du numéro de saisie. Ainsi à l'aide d'un générateur de clé, il est possible de se faire passer pour n'importe quel utilisateur enregistré. Il devient dès lors possible de bénéficier des mises à jour sans même avoir payé une licence d'utilisateur.

On se rend compte que souvent les logiciels stockent leurs clés de protections dans des fichiers de données propriétaires ou alors directement dans la base de registre de windows.

Il est également possible de se munir d'une cartouche de type action replay. Cette cartouche se branche sur le port parallèle, et permet notamment d'effectuer un affichage de l'état de la mémoire à tout moment. Pendant ce temps l'application est mise en pause. Au départ l'Action Replay était prévu pour trouver des codes de jeux vidéo, mais l'utilisation a rapidement été détournée.

L'intérêt par rapport à une solution logiciel classique, c'est que bien souvent l'Action Replay évite les mécanismes de protection anti-piratage. Il existe des Actions Replay pour PC et consoles de jeux.

b) patches et générateurs de clés

Ces outils se trouvent très facilement sur Internet à l'aide d'un moteur de recherche généraliste. Ceux ci sont utilisés tous les jours par des millions d'internaute (www.google.fr , www.yahoo.fr ...). Il est donc très facile de se procurer des versions illégales.

c) serveurs illégaux

Il existe de nombreux serveurs illégaux qui proposent au téléchargement :

- des parades pour des milliers de logiciels
- des versions complètes

Ces serveurs sont de deux types : gratuit et payant. Les serveurs se trouvent la plupart du temps dans les pays où la loi n'existe pas ou alors n'est pas appliquée. Par exemple en Russie, en Chine, ou en Europe de l'est.

Le paiement s'effectue comme n'importe quel site légal : par carte bleue. Les prix des logiciels sont au moins dix fois moins chères que dans le commerce. Par exemple la suite bureautique Microsoft Office 2003 Entreprise est proposée pour moins de 100€ ! La version pour ce prix vous est même envoyée par la poste avec support sur DVD !

Les organismes de lutte contre le piratage se consacrent essentiellement à fermer et condamner les auteurs des sites qui proposent des versions contre paiement.

d) DVD-Vidéo: deCSS

Dès 1999, soit 4 ans seulement, après la mise en place des protections DVD-Vidéo, Jon Johansen, un Norvégien de 16 ans, parvient à réaliser un programme permettant de réaliser des copie de DVD. Le mécanisme CSS devient vulnérable.

Une distribution massive du produit sur Internet, rend donc très vite la copie de DVD possible pour tout le monde. La justice Norvégienne saisie par plusieurs organismes dont le DVD-CCA (DVD Copy Content Coalition) assigne Jon Johansen devant les tribunaux.

Jon pour sa défense, invoque l'impossibilité de lire sur son ordinateur les DVD-Vidéo qu'il a acquit légalement. Son PC est équipé d'un système d'exploitation Linux, ce que n'avait pas prévu les concepteurs du CSS. En effet le mécanisme ne fonctionne que sous Microsoft Windows et Apple Mac OS.

Après avoir gagné devant les tribunaux une première fois, Jon a été acquitté de nouveau en décembre 2003 lors de l'appel des industries cinématographiques. Il s'agit d'une grande victoire dans le monde du libre, ainsi pour des millions d'usagers du DVD.

Dès lors, il devient aujourd'hui très facile de réaliser des copies de sauvegarde privée des DVD, ainsi que de lire ses DVD sur n'importe quel système d'exploitation. L'affaire désormais très connue peut être consultée sur [ZDNET_JON.FR].

2.2.2. Partage de fichiers : Peer to Peer

Le partage de fichiers, aussi appelé Peer to Peer, permet à un internaute de se connecter à un réseau de machines, sans passer par un serveur de fichiers. Les données illicites sont stockées directement chez les internautes. Pour utiliser un réseau de partage, il faut télécharger un client, comme par exemple emule ou edonkey.

Ensuite après s'être connecté, les serveurs proposent uniquement des liens vers les machines contenant les produits illicites. Les internautes utilisent principalement le partage de fichiers afin de télécharger des films et de la musique, mais il est possible également de télécharger toute sorte de logiciels.

a) moyens de compression : MP3 & DIVX

Ces deux moyens de compression le premier pour l'audio, le MP3, et le second pour la vidéo, le DIVX, ont considérablement permis la profusion du piratage.

Paradoxalement ce qui a le plus protégé le DVD-Vidéo, c'est le volume des données à échanger. Ainsi des outils comme deCSS ont surtout servi à produire des fichiers au format MPEG4, plus connu sous le nom de DIVX. Ce format permet de faire tenir le volume d'un DVD de 4,7 Go sur un CD de 700 Mo. Evidemment à ce prix, on perd un peu en qualité, et les données de bonus, langues étrangères, sont enlevées (on parle de rippage).

Il n'est pas illégal en soit de copier un DVD sur un autre support : disque dur, CD Vierge, baladeur,... pourvu qu'on soit en détention du disque original. Cependant, comme chaque nouvelle technologie, celle-ci a connu ses dérives avec le fonctionnement de l'échange de fichier (peer to peer).

Les films et CD audios illégaux sont ainsi recopiés à partir des originaux (loués ou achetés), en effectuant au passage la compression pour favoriser les échanges. Pour les films, il arrive même que ceux ci soient récupérés directement en salle de cinéma à l'aide d'un caméscope numérique. On parle dans ce cas de version « screener », de moins bonne qualité toutefois.

b) Jurisprudence

Il existe de nombreux cas de jurisprudence [RAT34] pour lesquels des internautes ayant participé à du partage de fichiers illégaux, n'ont pas été poursuivis.

Le cas le plus récent est celui de l'équivalent RIAA néerlandais qui poursuivait un site pour mise à disposition de fichiers MP3 illégaux. Dans son arrêt, le juge déclare que le téléchargement pour usage privé de musique « illégale » n'est pas en contradiction avec la législation sur les droits d'auteur. En plus il estime que le téléchargement n'est pas répréhensible : *"le législateur stipule, au regard de la loi actuelle sur les droits d'auteur et la loi sur les droits annexes, ainsi que la directive européenne et son projet de transposition, que la copie pour usage privé (dans ce cas par le moyen de téléchargement) d'un fichier MP3 contrevenant/illégal ne constitue pas une violation de ladite loi ... il ne peut être question d'acte frauduleux que si l'utilisateur du fichier téléchargé le multiplie ou le rend disponible"*.

Cette affaire, pour laquelle le RIAA a fait appel, date du 13 mai 2004.

c) Arrestations et condamnations

Beaucoup d'arrestations ont lieu, et certaines devraient inquiéter tous les usagers du téléchargement. Une affaire récente, début mai 2004, condamne deux internautes français à versé chacun 2000€ d'amende pour avoir échangé des films de façon illégale par le biais du partage de fichiers.

Un gros coup de filet [RAT01] cette fois ci a permis de saisir 200 ordinateurs contenant des plusieurs certaines de titres illégaux. Ces groupes *warez* sont considérés comme les plus actifs de la scène. Cette arrestation devrait limiter la mise en ligne de titre récent. Cette affaire date d'avril 2004. Les auteurs ont été poursuivis par plusieurs organismes internationaux : BSA, ESA (jeux vidéo), MPAA (films), et la RIAA.

Ce type d'infraction arrive quasiment tous les jours et il en faudra encore beaucoup de condamnations si l'on veut réellement éradiquer le piratage

2.2.3. Social

Enfin, il ne faudrait pas l'oublier, mais le piratage, prend également une forme sociale.

En effet, comment certain pirate arrive t'il à se procurer des versions de logiciels avant même leur commercialisation sur le marché ?

Plusieurs groupes se sont déjà interrogés sur cette question. Microsoft pour protéger les versions de son célèbre système d'exploitation a mis en place une véritable procédure de guerre pour éviter les fuites. Ainsi les testeurs sont sélectionnés avec beaucoup de précaution.

Les mêmes questions se posent dans l'industrie du cinéma. Si des films sont disponibles avant leur diffusion dans les salles, c'est donc qu'il y a des fuites au sein même des maisons de production.

Ensuite une fois que les œuvres sont recopiées illégalement, il est très facile de les publier sur un réseau ou encore de les diffuser par CD.

2.3. Coûts

2.3.1. Coût des protections

Il existe de nombreuses sociétés ayant développé des outils pour protéger les créations logiciels ou matériels. Afin d'illustrer d'exemple concret, les coûts réels j'ai choisi quelques références sur des sites Internet spécialisés dans le domaine.

a) logiciel

La société ACProtect (Anti Crack Protect) commercialise un outil afin de protéger des *shareware*, mais aussi des logiciels professionnels. Leur produit est proposé en téléchargement sur <http://www.ultraprotect.com>.

Les prix vont de 149€ pour la version développeur indépendant (standard) à 549€ pour la version société (professionnel).

Le coût de revient de la protection dépend du nombre de logiciel vendu ainsi que de son prix de vente.

Exemple pour la version indépendante : calculons le pourcentage du coût du logiciel de protection dans le prix de chaque logiciel vendu.

Nombre de logiciel Vendus / coût	15 €	20 €	30 €
100	10 %	7,45 %	4,9 %
200	4,9 %	3,7 %	2,4 %

Exemple pour la version société : calculons le pourcentage du coût du logiciel de protection dans le prix de chaque logiciel vendu.

Nombre de logiciel Vendus / coût	30 €	60 €	90 €
1000	1,8 %	0,9 %	0,6 %
5000	0,4 %	0,2 %	0,1 %

La société Aplika, spécialisée dans la protection des logiciels, propose différentes solutions de protection logicielle et matérielle. Les produits sont disponibles sur le site www.aplika.fr. Contrairement à ACProtect, Aplika propose un coût par licence.

Le coût du kit de protection, proposé par la société Aplika, est de 275€ HT. Le kit s'utilise à l'aide d'une librairie logicielle qu'il est possible d'utiliser facilement à l'aide d'appel de librairie dynamique (DLL) dans le programme à protéger. Ensuite chaque clé générée revient à 0.45€ HT pour les versions réseaux des logiciels à installer.

b) matériel

La société Aplika commercialise des *dongles* de marques Dinkey à brancher en USB ou sur port parallèle. Leur offre est déclinée sous deux formes : réseau ou monoposte. Les tarifs vont de 27€ HT (version port parallèle) à 195€ HT (version réseau illimité) l'unité. Les tarifs sont dégressifs en fonction des quantités commandées. Visitez leur site [APLIKA.FR]. Les applicatifs protégés avec ce type de protection vont de 200€ à plusieurs milliers d'euros, voire beaucoup plus. Le support physique (le dongle) limite la diffusion du logiciel. On retrouve donc ces protections dans les applications professionnelles spécifiques ou les progiciels.

2.3.2. Manque à gagner

Le manque à gagner se définit comme le chiffre d'affaire supplémentaire si les produits contrefaits avaient été achetés.

a) Dans le monde

L'IIPA (International Intellectual Property Alliance) publie régulièrement des documents sur le manque à gagner dû au piratage des entreprises dans le monde. Cet organisme prend ses sources par le biais des gros organismes mondiaux (BSA, RIAA...)

En 2003, le manque à gagner à cause du piratage dans le monde étaient de 10,2 milliards de dollars, répartis de la façon suivante :

Cinéma	Musique	BSA	Jeux vidéo	Livres	TOTAL
1535,5 M\$	2503,5 M\$	3926,3 M\$	1686,8 M\$	528,6 M\$	10180,7 M\$

Les pays où le manque à gagner est le plus important, sont en tête la Chine avec 2584,2 M\$, suivit de la Russie avec 1128,3 M\$. Dans l'ordre du triste record du pourcentage le plus élevé de produits illégaux, on trouve en tête le Pakistan avec 100%, l'Ukraine, le Paraguay avec 99% et la Chine avec 90%. Le piratage en 2003 est en légère hausse par rapport à 2002.

Le piratage par Internet n'est pas comptabilisé car impossible à évaluer... Des pays comme le Pakistan possèdent des taux records de 100% de piratage dans les domaines des logiciels et de la musique. Plusieurs usines pirates produisent des millions de CD qui sont vendus dans le monde entier.

b) Europe

L'IIPA a établi une liste de 56 pays à surveiller dans le monde, la France ne fait pas partie de cette liste, mais l'Espagne et l'Italie sont surveillés. Selon IPR 2000, le piratage en France est de 40%, contre 34% en Europe et 25% aux Etats-Unis.

c) Cinéma

Autre fait marquant de l'actualité, celui de l'industrie du cinéma, les producteurs se posent la question de la survie de l'industrie du cinéma. A l'occasion du 57ème festival de Cannes, plusieurs réalisateurs dont Luc Besson et Quentin Tarantino (également président du festival cette année) ont participé à un colloque anti-piraterie organisé par plusieurs grosses entreprises des activités cinématographiques.

Le bilan révèle qu'il y aurait **trois millions de pirates**, qui téléchargent en moyenne **onze films par mois**, selon une étude publiée par le Centre National de la Cinématographie. Pour lire l'article complet [YAHCANNES]. Sur ces onze films, en moyenne 4,5 seulement sont regardés. Cependant l'étude ne dit pas combien de films les internautes auraient réellement acheté.

3. Nouvelles protections

De nouvelles protections sont créées car d'une part les solutions existantes trouvent leurs limites. D'autres parts de nouveaux besoins existent (contenus multimédias audio et vidéo), il faut donc créer les protections en conséquence.

3.1. Juridique

3.1.1. Brevet Logiciel

A l'heure actuelle, seul 10% des brevets logiciels sont européens. Cette situation tient à plusieurs facteurs. Le premier tient au fait que tout n'est pas brevetable dans les brevets logiciels de 1986. Nous l'avons vu, il faut que le brevet réponde à la résolution d'un problème technique. Ensuite le coût des brevets en Europe est d'environ 50000€ contre 12300€ au Etats-Unis. La différence de coût vient notamment du fait qu'en Europe il faut traduire le brevet dans au moins six langues.

Selon [BREVET03], l'Europe voudrait à présent étendre le champ de la brevetabilité logicielle jusqu'à la rendre totale, en recouvrant notamment trois domaines supplémentaires très importants :

- Les procédés triviaux, par exemple les algorithmes mathématiques simples qui se trouvent à la base de pratiquement tout logiciel.
- Les innovations technologiques, qui seraient ainsi protégées dans leur concept même par un brevet.
- Les techniques de commerce informatisées.

Les premiers acteurs anti-brevet sont les partisans du libre, qui voient d'un mauvais œil la possibilité de breveté tout algorithme, alors que ceux ci sont utilisé dans des millions de programmes existants. L'AFUL (Association Française des Utilisateurs de Linux) fait partie de ces militants. D'un autre côté, le patronat, représenté par le MEDEF réagit de façon favorable.

Actuellement les grandes entreprises enregistrent leurs brevets aux Etats-Unis. Si l'Europe veut rester compétitive, il faut que cette loi soit mise en place. Aujourd'hui la loi sur les brevets de 1986 reste insuffisante. Elle a fait l'objet d'un premier amendement en 2003, ce n'est pas encore fini.

3.1.2. Loi le len

Loi le len « la confiance dans l'économie numérique ». Adoptée en deuxième lecture à l'assemblée nationale, le décret d'application n'est pas encore paru. Le projet fait l'objet de vives discussions. Le but de cette loi est de donner confiance aux internautes vis à vis des contenus qui leur sont proposés. Pour cela, chaque fournisseur de contenu (FAI, webmaster...) devra filtrer les données proposées sur leur serveur et effacer celles qui leur semblent illicites. Voir le texte de loi sur [LELEN]

L'intérêt d'une telle loi serait d'éviter que des sites décrivant des méthodes de piratage n'apparaissent. En effet, en impliquant des acteurs comme les fournisseurs d'accès à Internet, il y aurait vraisemblablement plus de contrôles. Ainsi si la loi s'applique, il sera dès lors possible pour un FAI de retirer sans préavis toutes informations contenant des informations incitant au piratage ou contenant des liens permettant de se procurer des produits illégaux.

A ce jour cette loi n'est toujours pas mise en application car elle pose de nombreux problèmes concernant la liberté d'expression. Il faudra certainement encore plusieurs concertations avant de trouver un consensus.

3.1.3. Loi Perben

Il s'agit d'un durcissement des peines encourues en cas de piratage. La loi propose trois ans d'emprisonnement et 300000€ d'amende au lieu de deux ans et 150000 euros d'amende.

3.2. Logiciel

3.2.1. DRM : Gestion des droits numériques

Le DRM (de l'anglais Digital Right Management) est une technologie de gestion des droits numériques. Cette technologie est utilisée entre autre par Apple pour protéger les œuvres en téléchargement sur iTunes. Grâce à la DRM, il est possible d'éviter que les fichiers soient mis en partage sur Internet. Il est aussi possible de limiter les jours d'utilisation d'un logiciel (idéal pour la location), ou encore le nombre d'ordinateur autorisé pour l'utilisation (gestion à distance du nombre de licence).

Cette technologie a été conçue par la société Liquid Audio, qui a revendu ses brevets en 2002 à Microsoft, suite à des problèmes financiers.

Récemment, Jon Johansen, celui qui avait réussi à passer outre les sécurités CSS pour les DVD-Vidéo, a réussi à mettre en branle les morceaux téléchargés sur iTune et protégés par le système DRM. A l'aide d'un outil de la conception de Jon, il devient possible (difficilement quand même), d'extraire des morceaux de musique les protections, et ainsi d'échanger facilement les fichiers comme des MP3 classiques.

Le principale problème avec la technologie DRM, c'est qu'elle est incompatible avec beaucoup d'appareil existant. Un fichier audio protégé par DRM ne sera pas forcément compatible sur un auto-radio, un baladeur ou tout simplement le système d'exploitation Linux, faute de pilotes adaptés. Les utilisateurs s'en remettent donc à des outils comme ceux proposés par Jon Johansen.

3.2.2. NGSCB

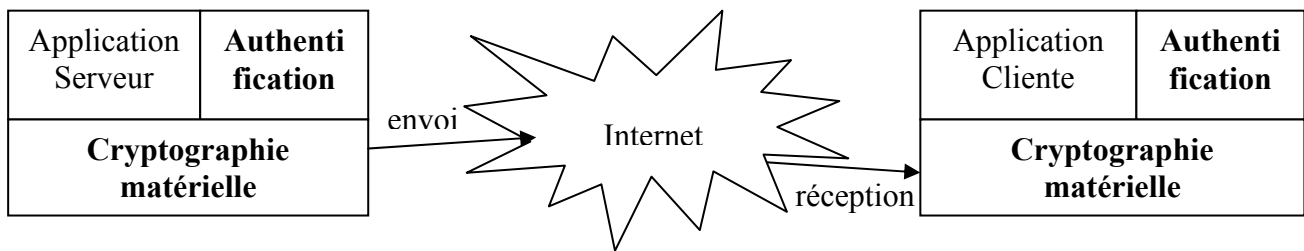
Le NGSCB (Next-Generation Secure Computing Base) est la prochaine génération d'ordinateurs sécurisés, développée par Microsoft [NGSCB04]. Le précédent nom de code de cette technologie était Palladium. Microsoft révèle aujourd'hui plus d'informations sur cette nouvelle technologie qui devrait selon le concepteur rendre le PC aussi sécurisé qu'il n'est flexible. L'objectif est double : garantir d'une part la sécurité contre les virus et les attaques, ainsi que lutter contre la copies sauvages et la violation des droits d'auteur. Il s'agit d'une solution hybride basée sur des composants logiciels et matériels.

La partie matérielle a été dévolue à Intel, selon un accord avec le géant de l'informatique. Cette partie sera constituée d'une puce électronique, intégrant plusieurs puissants algorithmes de cryptographie (RSA-2048, AES-128...).

La partie logicielle repose sur trois composants :

- un système d'authentification du code et des communications
- un système de cryptage des données
- un système de contrôle des accès et des droits numériques.

En outre, le système intégrera, les DRM vues précédemment.



Exemple d'envoi et de réception d'information à l'aide de la technologie NGSCB

Afin de déployer ce nouveau système de sécurité, à haut niveau, Microsoft, va distribuer des outils de développement (SDK), permettant une intégration rapide dans les futurs programmes. Windows sera tout de suite communiquant avec le NGSCB et devrait permettre d'éliminer les virus et attaques systèmes.

Cette technologie devrait, d'après le concepteur être intégrée dans les premiers PC d'ici à quelques années. Pour qu'un site web basé sur NGSCB puisse communiquer, il faudra que le client soit lui aussi équipé de la technologie. Pour les anciennes applications (par exemple MP3), il sera toujours possible de partager les fichiers sur Internet. Par contre, pour les nouvelles applications, ce ne sera plus possible, car les nouveaux fichiers disposeront d'éléments de sécurité interdisant la distribution avec des applications ne disposant pas des éléments de protection. Il sera possible d'implémenter cette fonction sur les logiciels de gravure ou toutes autres applications permettant une diffusion illégale.

Evidemment cette technologie n'est pas apprécié par beaucoup d'utilisateur. On se doute que Microsoft aura beaucoup de mal à intégrer l'ensemble de ces recommandations dans nos PC de demain. Souvenons nous du retour en arrière que Intel avais fait il y a quelque années, avec les microprocesseurs numérotés.

3.3. Commercial

3.3.1. Mise à jour

Lors des mises à jour automatiques sur Internet, le logiciel propose l'acquisition d'une nouvelle version. Cette démarche permet à l'utilisateur, même détenteur d'une version non autorisée de régulariser sa situation, et dans le même temps d'acquérir une version plus récente.

Par exemple dans l'industrie des antivirus, la version de base est fournit gratuitement en téléchargement sur le site ou même fournit lors de l'acquisition d'un l'ordinateur. Cependant après quelques semaines d'utilisation, le programme propose un abonnement pour une certaine durée pour profiter ainsi des mises à jours virales et ainsi protéger durablement son ordinateur des attaques éventuelles.

Par exemple la société Symantec propose ce service avec son produit Norton Antivirus. De même, le firewall (pare-feu) Zonealarm, produit de la société ZoneLabs, repose sur le même principe d'abonnement.

3.3.2. Redirection

L'association Retspam [RETSPAM] se propose de rémunérer les internautes qui créent de faux liens sur les réseaux de partage de fichier. Une fois téléchargés par l'utilisateur leurré, ces faux fichiers (films, musique ou programmes) renvoient vers un site Internet où il sera possible d'acheter "en toute légalité" le produit.

A chaque fois qu'un internaute sera redirigé vers ce site ou chaque fois qu'il achètera légalement le produit, le membre à l'origine du faux lien sera rétribué, explique le site de l'association. La fameuse commission est de 5 centimes d'euro par redirection.

3.3.3. Location

a) logiciels

Déjà présent depuis plusieurs années, la location de logiciel devient est de plus en plus plébiscité par les entreprises. La location de licence rentre dans le domaine des prestations de services, tout comme le crédit-bail pour les véhicules, ainsi que le matériel informatique.

La société Computer Associates, au départ spécialiste dans la vente de licence, a pris un virage en 2001, en ne proposant que de la location de licence. Le bilan est réussi, les entreprises sont satisfaites de ce nouveau mode de fonctionnement.

L'offre de Microsoft existe depuis 2001, sous la forme du contrat « Open Souscription ». Cette offre se révèle être une prestation de service, dédiée aux entreprises disposant d'au moins 250 postes. Ainsi l'utilisation des logiciels devient une charge fixe, qu'il est possible de renégocier à l'année. Les mises à jour automatiques et le support sont inclus dans l'offre annuelle. Après trois années de location, il est possible d'acheter le nombre de licence, cela représente toutefois un surcoût de 133% par rapport à une acquisition définitive.

b) jeux vidéos

Les jeunes sont nombreux à utiliser des copies illégales, car ils n'ont bien souvent pas de revenus et trouvent les logiciels trop chers. C'est pourquoi de nombreuses offres de location de logiciel ont été mises sur le marché. Le principe on le sait, est déjà un succès pour l'audio et la vidéo.

L'éditeur Atari, mais aussi Noos [LOC01NET], se base sur le produit EXEtender développé par une société israélienne. Grâce à cette extension, il est possible de jouer à des jeux vidéos sans avoir besoin de télécharger complètement le jeu. Ainsi au bout de quelques minutes, il est déjà possible de jouer. L'utilisation est cependant conseillée pour les connexions haut débit. Les tarifs dépendent de la durée de la location, et du jeu en lui même. De 3,8€ pour 48 heures à 17,8€ pour un mois de location.

Cette nouvelle offre devrait permettre de réduire le piratage. Les données téléchargées sur le disque dur sont cryptées. Cela interdit de pouvoir graver le jeu et de l'utiliser sur un autre ordinateur. Les éditeurs sont satisfaits du mode de protection.

Certains programmes spécifiques ou très chers, dont on n'a pas l'usage régulièrement ou alors pour des besoins ponctuels sont proposés à la location.

3.3.4. Notoriété

Au départ, Napster était un réseau de partage dédié exclusivement au piratage. Ensuite après plusieurs procès, Napster a perdu et le réseau de piratage démantelé. L'objectif est donc été ensuite de rentabiliser le réseau en proposant d'acheter des produits illégalement acquis autrefois. Napster propose des service équivalent à iTunes, de la société Apple. Pour visiter le site de Napster, www.napster.com

3.3.5. Console de jeux

Les consoles de jeu sont un bon exemple de procédé anti-piratage. En Europe, le piratage des jeux vidéo est marginal comparativement aux profits engendrés dans le secteur. Et pourtant le prix des jeux est prohibitif (de 45 à 60 €). Ce qui prouve bien que le piratage n'est pas du tout une raison de maintenir des prix élevés.

C'est un procédé qui marche depuis plus de 20 ans. Proposé une console bon marché (moins de 200€), et ensuite proposé des jeux à succès et qui plaisent. Le piratage est rendu difficile par les supports physiques spécifiques : la Game Cube de Nintendo utilise des CDs de 8cm incompatible avec les graveurs grand public. Depuis longtemps les consoles utilisent des supports propriétaires (cartouches pour nintendo ou sega il y a plusieurs années).

Les joueurs les plus motivés [PIRACONSOLE] qui ne veulent pas payer, utilisent des émulateurs sur leur ordinateur personnel (PC) ainsi des ROMs facilement téléchargeables sur internet. C'est la solution la plus pratique. Le piratage est donc possible, mais la diffusion est rendue plus difficile.

Dans ce cas, pourquoi les éditeurs ne sortent-ils pas les jeux vidéos uniquement sur consoles ? Tout simplement car le public n'est pas du tout le même. Sur PC les joueurs sont plus âgés et demandent des jeux nécessitant plus de réflexion. De même pour les jeux en réseau, le PC reste encore actuellement la solution la plus pratique. La nouvelle console de Microsoft (XBOX) tente de faire adhérer de nouveaux utilisateurs (accès Internet...), mais à l'heure actuelle le PC reste incontournable pour jouer.

3.3.6. Serveurs de jeux

Les jeux s'utilisent de plus en plus en réseau, par le biais de serveurs sur internet.

Par exemple pour les jeux Microsoft (XBOX ou PC), il suffit de se connecter à un serveur de jeux de type Game Zone pour pouvoir jouer en réseau. Même si l'utilisateur a réussi à se procurer une version illégale du jeu, il faudra néanmoins saisir une clé unique pour chaque jeu vendus afin de se connecter au serveur. Ainsi si deux clés identiques sont saisies sur le réseau, la dernière à être saisie interdira l'utilisateur de se connecter.

L'éditeur IdSoftware (Doom, Quake...) ne protège même plus ses jeux. Ainsi il devient très facile de se procurer des versions pour les dupliquer, et jouer seul. Par contre dès qu'il s'agit d'utiliser les jeux sur Internet, il faut s'identifier à l'aide d'un numéro de série unique. Aucune fraude possible. Cette position de la part de l'éditeur, ainsi que d'autres, se justifie dans le coût important des dispositifs anti-copies, et par leur manque d'efficacité. D'ailleurs IdSoftware, plébiscité par la presse et les communautés de joueurs, est conscient que leurs produits trouvent leur intérêt dans les jeux en ligne. Certains jeux ne sont d'ailleurs utilisables que par l'intermédiaire d'Internet.

La protection sur ce type de jeu, n'est donc plus située au niveau du support, mais sur le serveur. Il est certes possible pour une équipe de *hacker* de pirater un serveur, mais l'intérêt est limité, puisque l'éditeur aura tôt fait de s'en rendre compte et de mettre à jour les sécurités de son système.

3.3.7. Le prix et les moyens de paiement

a) DVD-Jetable

Le DVD jetable, existe depuis quelques mois aux Etats Unis ainsi qu'au Canada. Ce nouveau type de DVD permet de visionner des DVD-Vidéo à la séance. Le DVD est conservé dans un boîtier imperméable à l'air pendant plusieurs années. Une fois le boîtier ouvert, il faut regarder le film dans les huit heures, ensuite celui-ci devient illisible sur tous les types de lecteurs. Le procédé de destruction est chimique et sans danger.

Les avantages pour les utilisateurs sont :

- même gamme de prix qu'une location vidéo
- pas de retour au magasin
- pas d'enregistrement, pas de pénalités de retard
- une durée de stockage illimitée, permettant de le regarder quand on veut

Rappelons toutefois que cette nouvelle technique, ne possède pas de mécanisme anti-piratage spécifique. Il est donc malgré tout possible de procéder à une copie illégale dans le temps des huit heures. Cependant les prix proposés devrait donner un nouvel élan à la vente de DVD. L'offre sera dans un premier temps être lancée dans les grandes surfaces, ensuite dans les vidéos clubs en fonction des réactions du public. Le site www.cdiscout.fr proposent actuellement une centaine de films DVD à partir 2,5€.

b) Le cas de iTunes

Le programme iTunes créé par Apple permet de télécharger des œuvres musicales directement sur Internet, de façon légale. Il s'agit d'un bon moyen pour éviter le piratage. Les œuvres musicales sont revendues au prix unitaire de 0.99€ : c'est un véritable succès. Cette offre de téléchargement payante est venues bien après les réseaux de partage de fichier. C'est ici une preuve qu'il y a donc une réel demande de contenu (qu'il soit payant ou gratuit) par le biais d'un ordinateur sans passer forcément par le biais des moyens de distributions classiques. Les offres commercent seulement à arriver, et la concurrence commence déjà. C'est pourquoi les prix devraient rester stable, puisque Napster et d'autres proposent des services équivalents.

Les œuvres ainsi téléchargées sont protégées par un format MP3 amélioré, incluant une protection DRM (Digital Right Management). Ce système permet d'éviter une diffusion massive sur les réseaux de partage de fichier. Il n'est possible à l'aide de cette protection que d'écouter les fichiers téléchargés sur trois ordinateurs.

Il existe également une offre similaire aux Etats Unis, pour les films anciens (années 50), proposés au prix de 0.99€. Pour le moment, peu de titres sont disponibles, mais on devrait arriver à 500 titres courant 2004. Le système est utilisable depuis n'importe quel pays, par micro paiement (paypal). Il devrait bientôt y avoir une version française.

Par ailleurs pour éviter que les films soient récupérés dans les salles de cinéma, à l'aide d'un caméscope, dans certaines salles, les projectionnistes sont munies pour certaines projections de lunette infrarouge, permettant d'éviter toute tentative d'infraction.

3.4. Prévention

3.4.1. Prise de conscience

Avant de pouvoir développer des méthodes réellement efficace pour lutter contre la contrefaçon, il est nécessaire que le grand public soit conscient que le piratage est mauvais pour la création. Ainsi peu de personne réalise que copier un logiciel, c'est privé son auteur d'une rémunération. En copiant de façon illégal, on nuie à la création artistique, ceci menace la création d'œuvres nouvelles. Payer pour un produit c'est aussi financer ceux de demain. Beaucoup de gens pense qu'il est plus raisonnable de pirater plutôt que de voler...

Plusieurs sociétés, plutôt que de systématiquement blâmer les actes de piratage, participe à la prévention du public. C'est le cas par exemple d'Adobe, qui a créer récemment un service Anti piratage. Ce service donne des possibilités afin d'être en conformité dans ces licences logiciels. Microsoft favorise également la communication plutôt que la répression. Le BSA France offre également tout un panel d'outil permettant de recenser les logiciels à régularisé dans son parc informatique. Néanmoins ceci n'empêche pas que les cas avérés de piratage (lors d'une contrôle) sont punis sévèrement.

Cette prise de conscience passe aussi par une bonne information des pouvoirs publics. Dans un rapport du Ministère de la culture, rendu public en octobre 2002, M. Philippe Chantepie, inspecteur général des affaires culturelles, informe sur les possibilités d'améliorer « la lutte contre la contrefaçon des droits de propriété littéraire et artistique dans l'environnement numérique ». Dans ce volumineux rapport de 150 pages, on trouvent divers état des lieux sur la protection ainsi que sur l'étendue de la contrefaçon. La loi n'évolue pas aussi vite que la technologie : c'est pourquoi il est nécessaire d'effectuer une mise en conformités des textes de loi. L'état se dit prêt à travailler avec tous les acteurs du domaines, associations et société du privé. Depuis lors, plusieurs forum ont été mis en place sur Internet pour recueillir les avis des Internaute. Il apparaît qu'un dispositif légal pour permettre le partage de fichier doit être mis en place, cependant pour l'instant rien de bien concret : le piratage sévie toujours...

3.4.2. CEIPI à Strasbourg

Nous venons de voir l'aspect grand public du piratage, ainsi que de la prise de conscience nécessaire pour permettre une baisse significative. De l'autre côté, il y a les spécialistes, ceux qui enseignent le droit sur la propriété industrielle.

Nous avons la chance d'avoir à Strasbourg, le [CEIPI], centre d'étude internationale de la propriété industrielle. J'ai donc à cette occasion rencontré Mme Meyrueis, professeur de droit, spécialiste des questions sur la propriété intellectuelle.

L'école prépare deux diplômes, un DESS Accords et propriété industrielle et un DEA propriété intellectuelle. La formation est généraliste et prépare au dépôt de brevet et de marque. Les diplômés sont recrutés dans des entreprises qui veulent déposer des brevets mais aussi dans des organismes comme l'INPI ou l'OMPI (Organisation mondiale de la propriété intellectuelle), ou encore des cabinets d'avocats.

D'après Mme Meyrueis, la question actuelle des brevets est un faux problème. « Les entreprises qui veulent protéger une idée, déposent déjà leur brevet à l'aide de la loi de 1986. Le coût des brevets n'est pas rédhibitoire pour les multinationales, mais l'est surtout pour les petites entreprises. Les multinationales déposent déjà leurs brevets aux Etats-Unis afin d'éviter d'être recopié ». La loi évolue certes plus lentement que les technologies, cependant la jurisprudence abondante en matière de partage de fichier, devrait faire évoluer la réglementation actuelle. « La contrefaçon qui est la plus souvent punie, ce n'est pas celle des particuliers, mais celle des entreprises et surtout de celle qui effectuent un commerce de produits illégaux revendus. Il n'y a que rarement des saisies-contrefaçons effectuées chez les particuliers : cela ne se pratique pas encore, ou très peu. En revanche les entreprises sont régulièrement contrôlées. D'après Mme Meyrueis la loi comporte encore quelques failles qu'il est possible d'exploiter par les contrefacteurs. »

Ma rencontre avec Mme Meyrueis m'a donné un avis légal sur la question de la propriété intellectuelle et son cadre juridique. J'ai beaucoup appris, et l'échange de nos points de vues (technique/juridique) fût très intéressant.

4. Etude de cas

L'intérêt de ce chapitre est de montrer comment la protection du logiciel est prise en compte dans les sociétés. Les sociétés interrogées ont toutes un bureau dans le Bas-Rhin.

4.1. Rencontre

4.1.1. Intenia Consulting

La société Intenia Consulting, est une société implantée en France avec 300 collaborateurs et six agences. La société édite des logiciels de relation client, de gestion et e-business.

Intenia Consulting

Atlantis – Espace Europa

42, route de Bischwiller

67300 Schiltigheim

Tel +33 3 88 19 41 30

Contact: Eric Delage

Commercial

e-mail: Eric.Delage@intenia.fr

www.intenia.com

La société n'a pas de solution de protection contre la copie. Les logiciels sont livrés sous forme de CD-ROM. Le coût d'acquisition des logiciels va de 100K€ à plusieurs millions d'euros. Le seul contrôle qui est effectué est le nombre d'utilisateur simultané sur le réseau. Si le nombre maximal d'utilisateur est atteint, il faut acheter de nouvelle licence. Le contrôle se fait de manière logicielle, par un test très simple, sans protection particulière contre le piratage.

Après une période de paramétrage et de formation d'environ 6 mois, les utilisateurs continuent à être en relation avec Intenia par le biais d'un contrat de maintenance.

Ainsi la société ne risque pas vraiment de piratage, puisque la véritable valeur ajoutée se trouve dans les ressources humaines (paramétrage, formation, maintenance...).

Les logiciels livrés sont installés sur de puissants serveurs, avec des bases de données comprenant de 10000 à 15000 entités (tables), et plusieurs millions d'enregistrements.

Le risque de piratage étant très faible, la société Intenia n'a pas jugé nécessaire d'investir dans des procédés de lutte contre le piratage.

4.1.2. MAS Informatique

MAS Informatique

2 r Gén de Gaulle

67520 Marlenheim

Contact: M. Heitz

Consultant

Tél : 03 88 59 59 20

www.mas-informatique.com

MAS Informatique est revendeur en Alsace des solutions APISoft, spécialiste dans le développement d'une suite de logiciels de gestion (comptabilité, commerciale, paye). La société compte une dizaine de salariés, qui s'occupent : de l'installation, du paramétrage, de la formation et de l'assistance des utilisateurs.

Il y a environ 100000 logiciels installés en France et quelques milliers en Alsace.

Les logiciels de la société APISoft (basée à Bordeaux) sont protégés par un nom d'utilisateur et un numéro de série alphanumérique. Ces numéros sont enregistrés à l'aide d'un algorithme de cryptographie. A leur connaissance il n'y a pas de piratage possible du logiciel. Après avoir interrogé le service ingénierie d'APISoft, ceux-ci ont tenu à garder secret les mécanismes de protections.

A la connaissance du service commercial d'APISoft, il n'y a pas de problème de piratage. Ils ont simplement recensé des reventes illégales de numéros de série par des

revendeurs agréés. Ainsi plusieurs entreprises peuvent utiliser de façon illégale le même numéro de série.

Après quelques minutes de recherches sur Internet, il s'avère qu'il est très facile de trouver à l'aide d'un logiciel de partage de fichiers des versions du logiciel parfaitement utilisable sans déboursier un centime. Les logiciels de la gamme APIsoft sont déjà piratés par bon nombre d'utilisateurs.

4.1.3. Unilog

Unilog

Bd Sébastien Brant
67400 Illkirch
Contact: M. Vendam
Responsable qualité
Tél : 03 88 55 33 74
www.unilog.fr

La célèbre société en conseil, ingénierie et formation, possède une agence à Illkirch. Il m'a semblé important de demander à un tel acteur de l'informatique sa position vis à vis de la protection du logiciel. Pour cela, je me suis rapproché de M. Vendam, responsable du service qualité.

Le plus souvent les logiciels sont développés chez le client, après avoir défini un cahier des charges. Ensuite les logiciels appartiennent au client, et celui-ci en fait ce qu'il en veut. Unilog loue ses services à la journée (régie), en contrepartie, la firme perd tous ses droits concernant la propriété des logiciels. De ce fait Unilog n'est pas concerné par le piratage, puisque chaque logiciel développé est spécifique aux besoins du client.

M. Vendam n'a jamais eu écho de clients ayant revendus les sources à des compagnies tiers, alors qu'ils en auraient tout à fait le droit. Au contraire, les clients contacte Unilog afin d'effectuer des modifications ou améliorations ! Les clients sont la plupart du temps très fidèles alors qu'aucun document n'oblige à mettre à jour les logiciels par le biais d'Unilog. Le site de Strasbourg représente une centaine de collaborateurs, au niveau du groupe plus de 6500 personnes.

4.2. Tableaux récapitulatifs

Société	Protection	Piratage connu
Intentia	Contrôle du nombre de licence.	Non
APIsoft (revendeur MAS Informatique en Alsace)	Par nom d'utilisateur et numéros de série crypté.	Par les revendeurs et copie illégale facilement téléchargeable sur Internet.
Unilog	Chaque client possède une version spécifique du logiciel. Les sources appartiennent au client.	Non. Pas de piratage possible puisque les sources appartiennent au client, il en fait donc ce qu'il en veut.

Les sociétés interrogées ont été choisies de façon hétérogène afin d'avoir un panel le plus représentatif de ce qui pouvait se faire en terme de problème lié au piratage.

En clair les sociétés les plus exposées sont celles qui éditent des logiciels à plusieurs milliers d'exemplaires, en version « boîte », c'est-à-dire livrés avec un manuel et facilement utilisable par les utilisateurs. C'est pourquoi APIsoft est plus exposé au piratage que des sociétés comme Intentia ou Unilog.

Après avoir contacté d'autres éditeurs (Interlogiciel...) comme APIsoft, je me suis rendu compte que la plupart des entreprises possédaient des protections, mais que celles-ci étaient de toutes façons insuffisantes pour éviter le piratage.

J'ai reçu un très bon accueil de la part de toutes les entreprises interrogées. Cependant, dès qu'il s'agissait de rentrer dans des points techniques, concernant les méthodes anti-piratages utilisées, les entreprises préféraient tenir cela secret, en prétextant ne pas vouloir créer de « fuites » concernant les procédés de fabrication.

Les entreprises contactées sont conscientes du piratage et de ses effets sur les pertes financières occasionnées. Malgré tout, la plupart d'entre elles n'investissent pas dans des solutions externes, et préfèrent développer des solutions peu coûteuses, inefficaces pour les *hackers*, mais suffisantes pour le grand public.

4.3. CCI de Strasbourg

La CCI, chambre de commerce et d'industrie, est le partenaire de toutes les entreprises. Afin de recueillir la position de la CCI de Strasbourg, par rapport aux problèmes sur la protection des logiciels, j'ai décidé de rencontrer M. Besseghir, responsable informatique du pôle formation.

D'après le responsable, les entreprises ne se protègent pas contre le piratage. La raison essentielle provient du fait qu' « aujourd'hui le développement du logiciel n'est dicté que par des raisons financières. Les décideurs ne prennent pas en compte la réalité technique. L'objectif est de délivrer au client un produit fini le plus rapidement possible, sans prendre le temps d'intégrer des fonctionnalités efficaces pour lutter contre la copie illégale. Le problème est qu'il n'y a pas d'authentification de l'information. »

« Actuellement le pôle formation ne propose pas de formation pour la protection du logiciel. Il n'y a pas actuellement de demandes. Les entreprises sont plus intéressées par des formations à la sécurité informatique ou aux réseaux sans fils. Dans le cadre des nouvelles formations, la CCI pourrait à terme inclure une formation sur la contrefaçon, sous réserve d'un audit auprès des éditeurs du Bas-Rhin. »

L'interview de M. Besseghir a été très enrichissante. Les réponses recueillies sont venues confirmer les appels téléphoniques passés auprès des entreprises du Bas-Rhin : il n'y a pour ainsi dire pas de prise en compte du problème de la contrefaçon. Les éditeurs se contentent d'utiliser les anciennes méthodes, sans coût de mise en oeuvre, mais facilement contournable.

CONCLUSION

La question de la protection du logiciel n'est pas une mince affaire. Il n'existe pas de solution inébranlable. Toutes les protections possèdent des solutions pour les contourner avec plus ou moins de difficultés. Tant que les protections seront conçues par l'homme, alors il existera d'autres hommes pour trouver une technique de piratage. S'il y a autant de piratage, c'est donc bien qu'il y a une demande. Cela doit être dans la nature humaine de vouloir contourner les lois et surtout de ne pas payer. Nous pouvons même trouver des exemples où c'est le ministère de l'éducation nationale qui pirate ses logiciels. Un comble pour ceux qui doivent montrer l'exemple !

Plusieurs solutions logicielles modernes sont actuellement en train d'être mise en place pour contourner le piratage. Le DRM tout d'abord, qui commence à être intégré dans les logiciels de téléchargement de musique pour la location mais aussi pour éviter le partage. Ensuite le NGSCB, qui est en projet, et devrait permettre selon Microsoft d'éradiquer le piratage des produits utilisant la technologie.

Seulement le problème c'est que le DRM a déjà été en partie contourné, et comme toutes solutions logicielles il y aura un moyen de pirater cette solution. Concernant le NGSCB, il y a encore beaucoup de zones obscures et après les déboires d'Intel avec les numéros de processeurs, il y a de fortes chances que le projet sous sa forme actuelle ne soit pas accordé par l'Union Européenne.

La grande question est de savoir alors, s'il n'existe pas des solutions techniques infaillibles. Vers quelle orientation allons nous dans l'avenir ? Selon moi, l'avenir sera commercial. Plus que jamais les solutions techniques ont montré leurs limites. Il est nécessaire que les éditeurs plébiscitent des offres commerciales afin de décourager les personnes à se rendre dans l'illégalité. Pour que les produits se vendent, il faut que l'on soit dans une économie de marché.

Plusieurs offres existantes sont intéressantes, comme celle de CDiscount avec les DVD jetable à 2,5€. L'offre est déjà un succès aux Etats-Unis. On peut citer également l'exemple d'iTune, d'Apple, qui est une réaction aux réseaux de partage musicaux, arrivée assez tard. La version pour le téléchargement légal de film tarde à venir en Europe. Il y a une réelle demande à pouvoir visionner et télécharger du contenu sur un PC. Il faut que les sociétés de services en informatique réagissent. Sans doute que l'éclatement de la bulle technologique en 2000 a contribué à attendre sagement un réel potentiel de client avant la mise en service des programmes commerciaux.

La loi devra elle aussi continuer à évoluer et répondre au mieux aux nouvelles évolutions techniques. Ainsi de plus en plus de spécialiste devrait répondre dans les tribunaux des questions du droit numérique. On peut citer l'exemple du cabinet d'avocat Alain Bensoussan, spécialiste dans le droit des technologies avancées.

En attendant un réseau de confiance, c'est aussi de la responsabilité des Internaute, de veiller à ne pas diffuser des œuvres protégées. Pour cela, il faudra éduquer plutôt que de punir lourdement à chaque condamnation. Si on sait expliquer qu'un jour à cause du piratage, il n'y aura plus d'œuvres nouvelles, alors beaucoup réfléchiront à deux fois avant d'effectuer des copies illégales.

Tous les actes de piratages ne sont pas à mettre dans le même panier. Il est possible d'en distinguer trois types :

- le piratage des entreprises, qui est déjà largement sanctionné par les organismes internationaux (BSA...). Le piratage des entreprises dans le monde est encore très élevé.
- le piratage des particuliers, qui jusqu'à maintenant n'avait pas beaucoup été pénalisé, en effet, seuls les *hackers* étaient condamnés. Récemment, avec les réseaux de partage, quelques cas de particulier condamné ont été relaté dans la presse.
- les entreprises qui revendent des logiciels piratés, souvent dix fois moins chers que l'original. Ces entreprises disposent parfois d'usines en Asie pour fabriquer des CD par millions. Ce sont d'abord ces sociétés que les organisations internationales essaient de démanteler.

Internet et surtout le haut débit, a facilité l'accès à des produits en téléchargement illégal. Ces derniers jours, le piratage de film a fait la une de l'actualité, à l'occasion du 57ème festival de Cannes. Ce n'était pas une bonne journée pour l'informatique. Si l'on veut que l'informatique grands publics continuent à s'installer, il est nécessaire que les Internauts adoptent des règles de bonne conduite.

Pourtant, la contrefaçon a aussi son utilité. Dans certains pays, où les règles élémentaires de liberté d'expression ne sont pas respectées, le piratage est un excellent moyen de communication avec le monde extérieur. Ainsi en Chine, des films interdits par les autorités ont pu être visionnés à l'aide de copies illégales. Quentin Tarentino, le président du festival de Cannes cette année, avoue avoir pu regarder des films importés, qui avaient été interdit à la vente en Chine.

En outre, Microsoft, bénéficie d'une publicité gratuite par le biais du piratage, de ces produits. N'oublions pas que tous les produits piratés n'auraient pas forcément été acquis, bien souvent pour des raisons financières. Ainsi, certains éditeurs ont bénéficié d'une véritable publicité grâce aux produits acquis illégalement.

La protection du logiciel est un vaste sujet, qu'il est difficile d'aborder tellement les informations à recueillir sont nombreuses. Je regrette cependant, pour prendre l'exemple du Bas Rhin, que les entreprises ne se sentent pas plus concernées. On constate un certain fatalisme dans les méthodes de protection : il n'y a pas de solutions miracles. Les éditeurs pensent qu'en implémentant des solutions existantes, que cela devraient suffire pour éviter une diffusion massive.

J'ai eu beaucoup de plaisir à réaliser ce dossier, pour lequel je n'avais pas de connaissances particulières. J'y ai beaucoup appris et cela m'a permis d'être confronté à des situations concrètes par le biais des interviews et des contacts téléphoniques que j'ai pu établir. Il y a encore beaucoup de chemin à parcourir avant de trouver les meilleures solutions pour minimiser la contrefaçon. Ce qui est sûr c'est que nous sommes bien dans l'ère du service !

Glossaire

Les mots que vous retrouvez en italiques dans ce dossier sont définis dans le glossaire qui suit :

- déboguer

De l'anglais debugger. Logiciel permettant de chercher et de corriger les fautes et les erreurs d'un programme.

- dongle

Clé matérielle de protection, qui se branche en général sur un port d'E/S (USB, port parallèle...). Le dongle stocke un certain code qui, s'il n'est pas trouvé par le logiciel associé au dongle, provoque l'arrêt du logiciel en question.

- ingénierie inverse

De l'anglais Reverse Engineering. Technique consistant à déterminer l'utilité d'un objet que l'on voit pour la première fois, en analysant cet objet. On est amené à se poser des questions comme : « Si j'avais voulu fabriquer une machine ayant telle fonction, aurais-je réalisé cet objet précis ? ». En général, il s'agit de décompiler ou de désassembler un programme, c'est-à-dire de prendre quelque chose de compréhensible par une machine mais pas par un être humain et d'en faire quelque chose de lisible pour un homme mais plus pour un ordinateur.

- hacker

À l'origine, programmeur de génie, terme parfois employé pour bidouilleur. Désormais, et surtout du fait des journalistes, le terme désigne surtout les pirates des réseaux. Les hackers existent depuis longtemps : bien avant les ordinateurs, ils bidouillaient déjà, entre autres, les tableaux de commande des ascenseurs, de sorte que le fait d'appuyer sur un bouton pouvait vous envoyer à peu près n'importe où entre le rez-de-chaussée et le dernier étage...

- Shareware

Logiciel distribué gratuitement pour une période d'essai légale (de trente jours en général) au terme de laquelle, si on veut continuer d'utiliser le programme, on doit payer l'auteur, ce qui donne droit à une version étendue du logiciel et/ou à des mises à jour. Malgré l'existence d'excellents sharewares (rapport qualité/prix imbattable) beaucoup d'entreprises persistent à ne pas lui faire confiance.

- patch

Ajout temporaire à un morceau de code, en général pour corriger rapidement un bug (à éviter). Le patch est utile car il est tout petit et permet de corriger des bugs sans diffuser la totalité d'un logiciel.

- warez

Personne qui pirate des logiciels.

Bibliographie

Ouvrage

- [ALT2004] Copies illégales de fichiers audio et vidéo sur internet. Alt sylvain. Daburon Yannick. Copin Fabrice. Dossier communication CNAM 2004.
- [BEN94] Le logiciel et le droit, HERMES, Paris, 1994. Jean François Forgeron. p123 et suivantes.
- [CRYPTO95] Cryptographie Théorie et pratique. Douglas Stinson. Edition CRC Press. p101
- [HALTE02] Halte aux Hackers, éditions OE, 2002. Hoel Scambray, Stuart McClure, George Kurtz. P568 et suivants
- [PROP2002] Editions Dalloz 2002. Code de la propriété Intellectuelle, article L.112, L.122, L. 332, L. 611

Site Internet

- [APLIKA.FR] Editeur de protection de logiciel <http://www.aplika.fr/fr/FRlogiciels.htm>
- [BSA.ORG] Le Site officiel du Business Software Alliance <http://www.bsa.org/france/>
- [CEIPI] Le centre d'étude internationale pour la propriété industrielle www.ceipi.edu
- [LEDEVOIR.COM] Un pirate informatique déjoue la protection du logiciel iTunes <http://www.ledevoir.com/2003/11/25/41368.html?247>
- [LEGALIS.NET] Juris prudence en matière de protection du logiciel <http://www.legalis.net/legalnet/jurislog.htm>
- [LELEN] Projet de loi pour la confiance dans l'économis numérique http://www.telecom.gouv.fr/internet/projet_len.html
- [LOC01NET] Location de jeux vidéos <http://www.01net.com/article/199874.html> ; Location audio et vidéo <http://www.01net.com/article/240584.html>
- [NGSCB04] La nouvelle méthode de Microsoft pour lutter contre la copie illégale et le piratage <http://www.laboratoire-microsoft.org/articles/win/ngscb/>
- [PIRACONSOLE] Le piratage sur console <http://www.puissance-nintendo.com/dossiers/dossier.php?dos=24>
- [RAT01] Gros coup de filet sur le piratage <http://www.ratiatum.com/p2p.php?article=1501>
- [RAT34] Le MP3 en toute liberté au Pays bas <http://www.ratiatum.com/p2p.php?article=1534>
<http://tvconnect.lcweb.info/index.php?cat1=2&prod=11>
- [RETSPAM] Réménération des faux liens <http://msmvps.com/xpditif/posts/5495.aspx>
- [SCHN03] <http://www.schneier.com/essay-027.html> Des Chaussées-trappes de sécurité en cryptologie.
- [SEP] <http://tvconnect.lcweb.info/index.php?cat1=2&prod=11> Système d'Elimination du Piratage
- [YAHCANNES] Le Festival de Cannes se penche sur la piraterie <http://fr.news.yahoo.com/040511/214/3sksp.html>
- [ZDNET_JON.FR] Copyright et DVD: l'acquiescement de Jon Johansen confirmé en appel <http://www.zdnet.fr/actualites/technologie/0,39020809,39134548,00.htm>

Annexe

1) Code source RSA en C

```

/*Ce programme va vous proposer une clé secrète et une clé public */
/* pour utiliser l'algorithmme de cryptage RSA. */
/* Les algorithmmes utiliser sont directe, */
/* c.a.d ils ne sont pas conçus sur une */
/* base mathématique évolué */

#include<stdio.h>
#include<stdlib.h>

void main()
{
unsigned long int existe;
unsigned long int e, d, ed;
unsigned long int p, q, fct_euler, tab_e[5*1024];
unsigned long int i, rest, l, b, m, r;
char c;

printf("\n Ce programme va vous générer une clé secrète pour l'algorithmme
RSA ") ;
printf("\n Donner p : ");
scanf("%ld", &p);
printf(" Donner q : ");
scanf("%ld", &q);

/* Calcul de e */
m = 0 ; // index du tab_e
e = 3 ;
existe = 0 ; // aucun e trouve pour l'instant
fct_euler = (p - 1) * (q - 1);
printf("Les nbres premier avec %ld:", fct_euler);
getch();
do
{
b = 1 ;
while( b & e < fct_euler)
{
i = fct_euler ;
l = e ;
do{ // algo d'Euclide pour calculer pgcd(e, nbr_euler)
rest = i % l ;
i = l ;
l = rest ;
}while (rest > 1);
if (rest == 0) e = e + 2;// e courant est un diviseur de fct_euler,
// on ne va pas le prendre
else b = 0;// On va casser la boucle pour enregistre e ds tab_e
}
if ( ! b) // e >= fct_euler
{
existe = 1;
printf("\n%ld", e);
tab_e[m] = e;
m=m+1 ;
m = m%(5*1024); // Pour ne pas dépasser la taille du tableau,
// donc seul les 5*1024 valeurs seront sauvegardées.
e = e + 2;
}
}
}

```

```
    }
    else if(! existe) //On a sortit avec e > fct_euler
    {
        printf("\nImpossible d'obtenir e ") ;
        exit(1) ;
    } else break;
} while(1) ;
randomize();
e = tab_e[random(m)];
/* calcul de d */
// nous avons ed est premier avec fct_euler
// ed = 1 + k*fct_euler
// d = ed / e
// donc il faut chercher ed multiple de e

ed = 1;
do
{
    ed = ed + (p-1)*(q-1);
    r = ed % e ;
}while (r != 0); // On est sur que d existe. donc la boucle doit
termine sur r = 1
d = ed / e;
// en va choisir parmi les 4*1024 valeurs possible de e une seul au hasard
printf("\n\t *Clé privée propose est :%ld* ",e ) ;
printf("\n\t *Clé public(d) propose est : %ld*", d);
getch();
}
```

TABLE DES MATIERES

RAPPEL DU SUJET	2
REMERCIEMENTS	2
SOMMAIRE	3
Introduction	4
1. Etat des lieux	5
1.1. Cadre juridique	5
1.1.1. loi du 3 juillet 1985 : droits d'auteurs de logiciels	5
1.1.2. loi du 10 mai 1994	5
1.1.3. Brevet logiciel	6
1.2. Mise en application	6
1.2.1. APP	7
1.2.2. BSA	7
1.2.3. RIAA / Sacem	7
1.3. Protections existantes	7
1.3.1. Algorithme de codification des informations : RSA	7
1.3.2. Logiciel	9
1.3.3. Matériel	10
2. Organisation du piratage	12
2.1. Pourquoi le piratage	12
2.1.1. Raison technique	12
2.1.2. Raison économique et sociale	12
2.2. Formes	13
2.2.1. Logiciel	13
2.2.2. Partage de fichiers : Peer to Peer	15
2.2.3. Social	16
2.3. Coûts	16
2.3.1. Coût des protections	16
2.3.2. Manque à gagner	17
3. Nouvelles protections	19
3.1. Juridique	19
3.1.1. Brevet Logiciel	19
3.1.2. Loi le len	19
3.1.3. Loi Perben	20
3.2. Logiciel	20
3.2.1. DRM : Gestion des droits numériques	20
3.2.2. NGSCB	20
3.3. Commercial	21
3.3.1. Mise à jour	21
3.3.2. Redirection	21
3.3.3. Location	22
3.3.4. Notoriété	22
3.3.5. Console de jeux	22
3.3.6. Serveurs de jeux	23
3.3.7. Le prix et les moyens de paiement	23
3.4. Prévention	24
3.4.1. Prise de conscience	24
3.4.2. CEIPI à Strasbourg	25
4. Etude de cas	26

4.1. Rencontre	26
4.1.1. Intenia Consulting	26
4.1.2. MAS Informatique	26
4.1.3. Unilog.....	27
4.2. Tableaux récapitulatifs	27
4.3. CCI de Strasbourg	28
CONCLUSION	29
Glossaire.....	31
Bibliographie	32
Annexe	33
1) Code source RSA en C	33
TABLE DES MATIERES	35

Afin d'être protégé contre la contrefaçon, les œuvres sont soumises aux droits d'auteur. Les logiciels font partis des créations artistiques et disposent ainsi des mêmes lois, avec quelques spécificités. Cela concerne notamment la copie de sauvegarde à la condition de posséder l'original.

Malheureusement, bien souvent cette copie est effectuée en toute illégalité. Les protections actuelles sont insuffisantes pour limiter le piratage. Avec l'Internet haut débit, de nouveaux services permettent de partager des fichiers très rapidement, et donc d'accroître la diffusion des œuvres piratées. La musique et les films sont également concernés. Les nouveaux formats numériques associés à des technologies de gravure et de haut débit grand public, ont accéléré un dérapage inquiétant de la contrefaçon.

Il devient nécessaire de créer de nouvelles protections, qui limitent la diffusion des logiciels. De même dans le domaine du cinéma et de la musique, comment éviter que les œuvres soient téléchargées de façon illégale ? Nous allons traiter dans ce dossier de la protection du logiciel, et essayerons de savoir si les nouvelles méthodes sont efficaces...