

---

# «Trusted Computing» et politique de concurrence – questions pour les professionnels de l'informatique

Traduction de l'anglais de «“Trusted Computing” and Competition Policy – Issues for Computing Professionals»

Ross Anderson

Traduction de l'anglais: François Tourde, Olivier Berger

Copyright © 2003 Ross Anderson

Cette œuvre est placée sous licence GNU Free Documentation Licence.

## Note

L'original en anglais de cet article a été publié sous l'intitulé «“Trusted Computing” and Competition Policy – Issues for Computing Professionals» dans Upgrade Vol. IV, issue no. 3, June 2003, *Open Knowledge* (<http://www.upgrade-cepis.org/issues/2003/3/upgrade-vIV-3.html>).

Le développement stratégique le plus significatif de l'année écoulée dans l'informatique a été le «*Trusted Computing*» (TC), ou «Informatique de confiance». Dans cet article, l'auteur donne un aperçu du TC, et esquisse certains effets possibles sur l'industrie de l'informatique et ceux qui y travaillent.

*The most significant strategic development in information technology over the past year has been “Trusted Computing” (TC). In this paper, the author gives an outline of TC, and sketch some of the possible effects on the computing business and the people who work in it.*

**Mots-clés.** contrôle des accessoires, antitrust, politique de concurrence, copyright, DMCA, EUCD, Intel, Microsoft, monopole, NGSCB, Palladium, TCG, TCPA, couplage.

Ceci est une version raccourcie, spécialement pour Upgrade, d'un article intitulé «Cryptography and Competition Policy – Issues with “Trusted Computing”» (NdT. : «Cryptographie et politique de concurrence – Questions sur le «Trusted Computing»»), qui peut être consulté à <http://www.ross-anderson.com/>.

## Table des matières

Introduction .....	1
Trusted Computing .....	2
Contrôle et gouvernance .....	3
Intérêt pour utilisateurs de type sociétés ou administrations .....	3
Intérêt pour les éditeurs de contenus .....	4
Intérêt pour les fabricants de matériels .....	5
Intérêt pour les éditeurs de logiciels .....	5
L'importance des applications .....	6
Coûts de changement et captivité .....	6
Problématique antitrust .....	7
Qu'est-ce que cela signifie pour les professionnels de l'informatique ? .....	8
Bibliographie .....	9

## Introduction

Un des problèmes les plus complexes pour les professionnels de l'informatique est de faire face aux stratégies de prix pratiquées par les fournisseurs pour récupérer jusqu'aux derniers centimes des poches de leur clientèle. Les fournisseurs prédominants, comme Microsoft de nos jours, et IBM une génération avant, tentent d'enfermer leurs clients dans leurs architectures, afin que leur mainmise puisse s'étendre d'un produit à un autre. Beaucoup de produits suivent un cycle de «bonnes-affaires-puis-escroquerie»; une fois que votre entreprise a opté pour telle technologie particulière de carte à puce, ou pour tel progiciel comptable, leurs prix grimpent mystérieusement.

Le couplage des produits est une autre stratégie, dont les cartouches d'imprimantes donnent un bon exemple. Les imprimantes sont amorties par les cartouches: ce couplage permet aux vendeurs de cibler avec les mêmes produits les entreprises grosses consommatrices et les ménages attentifs à la dépense. D'habitude le niveau d'amortissement croisé était limité par les cartouches recyclées ou compatibles. C'est pourquoi de nombreuses cartouches d'impression contiennent maintenant une puce qui les identifie vis-à-vis de l'imprimante, une pratique qui a commencé en 1996 avec la Xerox N24 (voir [5] pour l'historique des puces pour cartouches). Dans un tel système, si l'imprimante détecte une cartouche concurrente compatible, ou bien recyclée, elle peut sans prévenir redescendre de 1200 dpi à 300 dpi, ou même refuser complètement de fonctionner. Un développement encore plus récent est l'utilisation d'une date d'expiration. Les cartouches de l'imprimante HP BusinessJet 2200C expirent après avoir passé 30 mois dans l'imprimante, ou 4 ans et demie après fabrication [3] — ce qui a provoqué l'indignation des consommateurs [4].

Le couplage des cartouches amène maintenant à un conflit commercial entre les USA et l'Europe. Aux USA, un tribunal a permis au fabricant d'imprimantes Lexmark d'empêcher la vente de cartouches à puces compatibles avec ses imprimantes. Pendant ce temps là, le Parlement Européen a approuvé une *Directive relative aux déchets d'équipements électriques et électroniques* qui imposera aux états membres d'interdire, à partir de 2006, le contournement des règles de recyclage de l'Union Européenne par les sociétés qui conçoivent des produits contenant des puces destinées à empêcher leur recyclage [8].

Le contrôle des marchés associés<sup>1</sup> et le couplage de produits se développent très rapidement et utilisent tout un arsenal de mécanismes techniques. Les fabricants de téléphones portables, qui gagnent souvent plus d'argent sur la vente d'une batterie que sur celle du téléphone en question, ont donc introduit des puces d'identification qui rendent difficile l'utilisation de batteries venant des concurrents [10]. Les fabricants d'automobiles utilisent des formats de données propriétaires pour empêcher leurs clients de confier leurs réparations à des garagistes indépendants [12]. Et les sociétés de jeux vidéos prélèvent depuis des années des royalties auprès des développeurs des logiciels, qu'ils utilisent pour amortir les ventes des consoles [11].

Ces pratiques sont-elles bonnes ou mauvaises pour le commerce ? La réponse est, selon les économistes, «Ça dépend.» Hal Varian prétend que coupler les imprimantes à leurs cartouches n'est pas forcément trop répréhensible d'un point de vue de la régulation, car le marché des imprimantes est encore concurrentiel; ainsi coupler la vente de cartouches aux imprimantes renforce seulement plus fortement la compétition entre les marques sur la vente des imprimantes, conduisant à la réduction des prix sur ce marché [9].

Cependant, quand les mécanismes de couplage peuvent être employés pour lier entre-eux deux marchés dans lesquels la concurrence est relativement faible — typiquement le marché des systèmes d'exploitation et celui des serveurs web — alors les choix peuvent devenir plus restreints et les prix grimper. C'était une des objections formulées à l'encontre de Microsoft Passport sur une base de politique de la concurrence. Les commerçants voulant utiliser Passport étaient obligés d'utiliser aussi les serveurs web Microsoft. Une politique de tarification complexe et un contrôle des marchés associés pourraient maintenant devenir beaucoup plus simples à mettre en place, grâce à l'introduction du *Trusted Computing* [2].

## Trusted Computing

En juin 2002, Microsoft a annoncé Palladium, une version de Windows mettant en œuvre le *Trusted Computing*<sup>2</sup> et prévue pour 2004. Dans ce contexte, *Trusted* (NdT.: lit. «à qui on fait confiance») signifie que des tiers font confiance au logiciel tournant sur un PC, et qu'ils peuvent vérifier qu'un programme tournant sur la

---

<sup>1</sup>**Note du traducteur.** l'auteur emploie le terme *aftermarket*, que nous avons traduit par «marchés associés». Il s'agit de décrire les marchés sur les accessoires, consommables ou pièces détachées, ou les services complémentaires : réparation, maintenance, etc.

<sup>2</sup>**Note du traducteur.** La littérature francophone sur le sujet parle également d'«Informatique de confiance». Nous avons conservé la terminologie de l'auteur *Trusted computing*, ou TC, à dessein (voir la fin de la section 2 de l'article, qui décrit la vision de l'auteur sur les questions de terminologie dans cette affaire).

machine avec lequel ils communiquent n'a pas été modifié par le propriétaire de la machine. Les programmes pourront aussi communiquer de manière sûre les uns avec les autres, et avec leurs auteurs. Cela ouvre un certain nombre de nouvelles possibilités intéressantes.

L'application évidente est la gestion des droits numériques (NdT.: en anglais, *Digital Rights Management*, DRM) : Disney pourra vous vendre des DVDs décriptables et utilisables sur une plateforme Palladium, mais que vous ne pourrez pas copier. L'industrie musicale pourra vous vendre des morceaux téléchargés que vous ne pourrez pas échanger. Ils vous vendront des CDs que vous ne pourrez utiliser que trois fois, ou seulement pour votre anniversaire. Cela risque d'être sujet à controverse; d'autres applications le seront moins. Par exemple, les plateformes *trusted computing* peuvent héberger des jeux où tricher sera plus dur.

Palladium s'appuie sur les travaux de la *Trusted Computing Platform Alliance*, qui comprenait Microsoft, Intel, IBM et HP comme membre fondateurs. AMD s'y est maintenant joint, et c'est devenu le *Trusted Computing Group* [13]. TCG propose une redéfinition de l'architecture matérielle des PC, dans laquelle le processeur acquiert un niveau de privilège supplémentaire (qui permet aux programmes d'accéder à des zones mémoire interdites même à un super-utilisateur standard) et un composant matériel de sécurité (la «puce Fritz»), qui supervise quels logiciels et matériels fonctionnent sur la machine. Les puces Fritz de différentes machines peuvent communiquer entre elles. Le rôle de Fritz dans l'écosystème *Trusted* est d'assurer aux tiers que votre machine est bien ce que vous prétendez qu'elle est, et que les logiciels tournant dessus sont bien ceux que vous prétendez qu'ils sont.

Tout le monde n'accepte pas le terme *trusted computing* pour cette technologie (NdT: lit. «informatique à qui on fait confiance»). Microsoft lui préfère le terme *trustworthy computing* (NdT: lit. «informatique digne de confiance») : faire confiance à un système ne le rend pas nécessairement digne de confiance. Si un employé de la NSA3 est surpris dans les toilettes de l'aéroport international Washington à Baltimore en train de vendre des informations clés à un diplomate chinois (si on considère que cette opération est illégale), nous pouvons le décrire comme *trusted but not trustworthy* (NdT.: lit. «à qui on fait confiance, mais pas digne de confiance»). (En fait, la définition de la NSA pour un système de confiance est: «Un système pouvant violer la politique de sécurité»). À l'extrémité opposée de ce débat, Richard Stallman de la *Free Software Foundation*4 préfère le terme de *treacherous computing* (NdT: lit. «système déloyal»), car le véritable objectif de la technologie TCG est de priver son propriétaire du contrôle effectif d'un PC [15].

Je me référerai donc dorénavant à ce sujet sous la forme de «TC», que le lecteur peut prononcer au choix *trustworthy computing*, *trusted computing* ou *treacherous computing*, à sa convenance.

## Contrôle et gouvernance

Si le propriétaire d'une machine n'est plus censé en avoir un contrôle total, alors la grande question est qui en obtient le contrôle. C'est une question à laquelle les sociétés impliquées dans le TC ont donné différentes réponses à divers moments. Les spécifications d'origine de TCPA 1.0 suggéraient une hiérarchie d'autorités de certification pour certifier les différents composants matériels et logiciels qui pouvaient constituer un système TC. Le contrôle serait ainsi exercé de façon centrale par un consortium industriel.

Le point de vue actuel des industriels est qu'il sera du ressort des fournisseurs d'applications TC ou de contenus manipulés par celles-ci, de décider quelles combinaisons de matériels et de logiciels de système d'exploitation seraient acceptables. Ainsi, dans le cas du DRM, ce sera Disney — voire Microsoft en tant que vendeur de Media Player — qui certifierait des plateformes particulières comme convenables pour restituer *Blanche Neige*. Les règles qu'une application particulière mettra en œuvre, telles que des étiquettes pour les CD commerciaux disant «ne jamais copier» ou «une seule copie de sauvegarde», ou, dans le cas de la télé-diffusion des films, «enregistrement pour la consultation en différé uniquement, copie interdite», proviendront au final d'un serveur géré chez le fournisseur de l'application.

## Intérêt pour utilisateurs de type sociétés ou administrations

---

<sup>3</sup>Note du traducteur. *National Security Agency*. Agence de renseignement des services secrets américains.

<sup>4</sup>Note du traducteur. Fondation pour le logiciel libre (<http://www.fsf.org/>).

Les serveurs de sécurité des applications peuvent définir une large gamme de règles. Ainsi un système TC utilisé pour faire respecter une protection de type classement gouvernemental d'informations secrètes, peut avoir une règle centrale disant que l'information ne peut que passer dans un niveau plus élevé, de sorte qu'une partie d'un dossier «confidentiel» peut être coupée et collée dans un dossier «secret» mais pas l'inverse. Mais mettre en œuvre correctement un système de contrôle de flux d'informations unidirectionnels est difficile [1]; de sorte qu'il est peu probable qu'il s'agisse de la *killer application*<sup>5</sup> du TC.

L'utilisation des systèmes TC pour protéger les secrets industriels, est l'application qui est maintenant mise en avant pour faire progresser le TC. Bill Gates a dit : «C'est un truc étonnant. Nous en sommes arrivés là, en pensant à la musique, mais nous nous sommes alors rendus compte que l'e-mail et les documents étaient des domaines bien plus intéressants» [19]. Une première mise en œuvre de mécanismes de gestion de droits, qui peuvent être appliqués de cette façon au contrôle des informations confidentielles, par opposition à des choses comme la musique et la vidéo, a été livrée récemment dans *Windows Server 2003* [16].

Windows Server 2003 permet au créateur de documents ou de tous autres fichiers, de conserver un certain contrôle sur ceux-ci, indépendamment de l'endroit où ils pourront être déplacés ensuite. Il sera possible d'envoyer un e-mail avec des restrictions, du genre où le destinataire ne pourra pas le transférer, ou ne pas l'imprimer, ou bien où on pourra le lire seulement si on possède une accréditation «secret», ou alors où le document ne sera consultable que jusqu'à la fin du mois. Les utilisateurs de Windows désireux d'utiliser les fonctionnalités TC peuvent alors s'enregistrer, et il semble qu'un service en ligne soit utilisé pour décider si oui ou non une clef de décryptage peut être mise à disposition de l'application (Au moment de l'écriture de cet article, cela vient juste de sortir, et les détails doivent encore être élucidés).

Un des arguments de vente majeurs de cette technologie est qu'une entreprise peut faire en sorte que tous les e-mails internes deviennent illisibles après 90 jours. Microsoft impose déjà une discipline de ce type en interne. Compte-tenu des tactiques d'enquête de plus en plus agressives utilisées dans les procès, il peut être intéressant pour certains directeurs juridiques des entreprises, de faire en sorte que les e-mails se comportent comme des coups de fil, plutôt que comme des lettres.

Mais même une application aussi simple peut s'avérer complexe à déployer dans la réalité. Un cabinet juridique serait probablement peu disposé à recevoir des instructions d'un client sous forme d'un e-mail, que seulement un seul associé peut lire, qui ne peut pas être imprimé, et qui deviendra complètement illisible après 90 jours. Comment le cabinet peut-il se protéger contre des poursuites pour faute professionnelle, et quelles garanties sont à la disposition des autres associés?

Ce n'est pas tout. Dans beaucoup de pays, les lois sur l'exportation exigent des compagnies qu'elles conservent des copies des communications concernant l'exportation de logiciels, de documentations ou de savoir-faires présents sur la liste des biens à «double-usage»; cela peut signifier de garder tous les emails en question pendant 3 ans. Les règles comptables peuvent exiger la conservation des emails concernés pendant six ans. On peut imaginer une généralisation des conflits entre les règles exigeant la conservation et les règles exigeant la destruction. Chaque responsable de Système d'Information le sait : on entre en véritable terrain miné quand on automatise des procédures qui avaient auparavant évité des conflits, car elles laissaient assez de place à la décision humaine, évitant ainsi d'aborder les questions difficiles.

## Intérêt pour les éditeurs de contenus

Les industries de l'édition musicale et filmographique ont fait un lobbying intense pour des mécanismes comme le TC, pour permettre des systèmes de gestion de droits numériques (DRM) plus forts. Elles ont déjà obtenu une protection légale plus forte pour les systèmes existants. Elles prétendent que la copie numérique détruira leur activité, mais cet argument est moins solide aujourd'hui car la copie de CD a été facile durant plusieurs années, et il n'y a eu aucun impact particulièrement remarquable sur les ventes. Si on analyse soigneusement, il n'est pas du tout clair qu'un mécanisme beaucoup plus fort de DRM, comme ceux promis par le TC, fournirait des bénéfices substantiels pour les propriétaires des contenus, au delà du status-quo naissant [20].

Il y a également un risque significatif, si les machines TC deviennent généralisées, qu'elles puissent être employées aussi facilement par l'autre camp. Les utilisateurs peuvent créer des *blacknets*<sup>6</sup> pour échanger tout

---

<sup>5</sup>**Note du traducteur.** lit. «application tueuse». Désigne une application de type inédit qui serait bien supérieure aux autres, et susceptible de faire décoller un marché.

<sup>6</sup>**Note du traducteur.** lit.: «réseaux noirs». Réseaux illégaux ou «souterrains».

type de contenu illégal, et il deviendra plus facile de créer des systèmes de peer-to-peer comme *gnutella* ou *mojonation* mais qui soient beaucoup plus résistants aux attaques de l'industrie musicale car seuls les clients authentifiés pourront en faire partie. Les méthodes actuelles employées pour attaquer de tels systèmes, comportant des attaques de déni de service effectuées par des clients comportant un cheval de troie, ne fonctionneront plus [21]. Ainsi quand TC sera mis en application, le principe des conséquences fortuites pourrait bien faire de l'industrie musicale une victime plutôt qu'un bénéficiaire.

## Intérêt pour les fabricants de matériels

L'expérience acquise montre que les mécanismes de sécurité favorisent souvent les intérêts de ceux qui paient pour les développer plutôt que les intérêts des consommateurs pour le bénéfice desquels ils sont censés avoir été développés [1]. Par exemple, l'introduction de l'authentification et du chiffage dans les téléphones mobiles GSM a été annoncée comme donnant aux abonnés une plus grande sécurité, par comparaison avec les téléphones analogiques pour lesquels il était facile de faire des copies et de l'écoute. Cependant, une expérience plus complète nous apprend que les bénéficiaires principaux furent les compagnies de téléphone qui ont financé le développement de cette sécurité.

Avec les vieux téléphones analogiques, les gens voulant passer des appels gratuits, ou frauder le système en appelant des numéros surtaxés gérés par des associés, faisaient des copies des téléphones, et ceci coûtait généralement de l'argent aux compagnies de téléphone. Avec le système GSM, soit les criminels achètent des téléphones en utilisant les cartes de crédit volées (transférant le coût sur les banques), ou bien, de plus en plus, ils utilisent les téléphones mobiles dérobés lors de vols à la tire (qui coûtent même encore plus aux abonnés). Quant à l'intimité, presque toutes les écoutes clandestines dans le monde sont effectuées par des agences de renseignement, qui obtiennent les conversations en clair à partir des infrastructures des opérateurs de toutes façons.

Nous sommes forts d'une telle expérience qui suggère que nous examinions l'effet probable du TC sur les affaires faites par ses instigateurs.

Dans le cas d'Intel, la motivation pour rejoindre TCPA était d'ordre stratégique. Puisque Intel possède la majeure partie du marché des microprocesseurs, duquel elle tire la plupart de ses bénéfices, elle peut se développer seulement si le marché des PC se développe aussi. Intel a donc développé un programme de recherches pour soutenir une stratégie de «domination dans les plateformes», dans laquelle ils dirigent les efforts faits par l'industrie pour développer des technologies qui rendront le PC plus utile, comme le bus PCI et l'USB [23].

L'aspect positif de cette stratégie fut qu'Intel a accru le marché global pour les PCs; le côté sombre fut qu'ils employèrent des portefeuilles de brevets et des accords de licences croisées obligatoires pour empêcher n'importe quel concurrent d'atteindre une position dominante dans une quelconque technologie qui aurait pu menacer leur contrôle des composants des PC. Les cyniques font remarquer qu'Intel n'a pas pu permettre que le bus microchannel d'IBM puisse dominer : ce n'était pas simplement une question de concurrence entre eux sur la plate-forme matérielle du PC, mais le fait qu'IBM n'avait pas intérêt à fournir la bande passante requise pour que les PC concurrencent les grands systèmes. L'effet en termes stratégiques est quelque peu semblable à la vieille pratique romaine consistant à démolir toutes les habitations et de couper tous les arbres près de leurs routes ou de leurs châteaux. L'approche stratégique d'Intel s'est transformée pour devenir une manière extrêmement efficace de contourner les lois anti-trust.

## Intérêt pour les éditeurs de logiciels

Le cas de Microsoft est encore plus intéressant. Sous sa forme d'origine, TC avait le potentiel d'éliminer directement les logiciels sans licence correspondante : une plate-forme *trusted*, qui en référerait à un service d'autorisation central, pourrait simplement refuser de faire tourner un logiciel sans licence. Les mécanismes utilisés pour identifier les logiciels pourraient en devenir beaucoup plus difficile à contourner : la puce Fritz gère une liste des composants matériels et logiciels systèmes d'une machine TC, et il est prévu que ceux-ci puissent être vérifiés en ligne.

Suite à des protestations publiques, Microsoft dit maintenant qu'aucun mécanisme de liste noire ne sera introduit — au moins au niveau du système d'exploitation [17]. Le système Windows 2003 semble reposer sur des mécanismes plus subtils. Le contrôle ne sera maintenant pas exercé de bas en haut grâce au matériel TC, mais du haut vers le bas grâce aux applications. Disney sera libre de décider selon quelles conditions ils fourniront des contenus aux systèmes possédant telle configuration matérielle et logicielle; s'ils décident de faire payer

12,99\$ pour une version DVD de *Blanche neige*, 9,99\$ pour un téléchargement pour TC/Windows sur Media Player, mais refusent de fournir des contenus pour toute autre plate-forme informatique, alors Microsoft peut clamer, aux médias et aux autorités antitrust, que c'est leur décision plutôt que celle de Microsoft.

Les incitations qui en résultent sont orientées fortement en faveur de Microsoft. Si TC/Windows devient la plate-forme dominante, la plupart des développeurs rendront leurs produits disponible pour elle en premier, et pour les autres plus tard (si jamais ça se produit) — tout comme la plupart des développeurs rendaient disponibles leurs produits pour Windows en premier et pour Mac plus tard (si jamais ils le faisaient) une fois qu'il est devenu évident que le marché des PC penchait dans la direction Wintel. On est à peine surpris qu'Apple essaye de battre Microsoft de vitesse en lançant son propre service de téléchargement de medias.

## L'importance des applications

Microsoft semble être en train d'investir pour équiper la plate-forme du système d'exploitation avec des mécanismes TC de façon à récupérer un avantage à travers des bénéfices plus importants tirés de ses applications. Ceci peut être direct (comme en faisant payer le double pour Office) ou indirect (comme en prenant un pourcentage sur tous les contenus achetés à travers Media Player). Du point de vue de la concurrence, tout se jouera sur la difficulté qu'il y aura pour d'autres compagnies à faire en sorte que leurs applications et leurs contenus interopèrent avec les applications et contenus de Microsoft. Il est dans l'intérêt de Microsoft de rendre cette interopérabilité aussi difficile que possible.

Si les services populaires d'abonnement musical utilisent Media Player, et qu'il se trouve que Media Player nécessite une plate-forme TC, alors les abonnés pourraient être confrontés à la nécessité de migrer vers une plate-forme TC, ou bien perdre l'accès à la musique qu'ils ont déjà stockée. Bien-sûr, une fois que l'utilisation d'une application TC est très répandue, avec de nombreux utilisateurs coincés, des mécanismes de conformité aux licences peuvent être mis en œuvre dont il sera à peu près aussi difficile de s'en échapper qu'il est dur de casser les technologies sous-jacentes. Le modèle d'affaires pourrait ainsi suivre celui de pionniers comme Nintendo et d'autres fabricants de consoles de jeux, dans lequel des jeux chers amortissent un matériel peu cher. Les caractéristiques du système d'exploitation TC serviront ainsi seulement un composant permettant de réaliser un amortissement, dont la fonction véritable est de maximiser les revenus issus de produits coûteux comme Office, les jeux et la location de contenus.

Si les contrôles d'accès obligatoires aux emails deviennent une application professionnelle populaire sous Windows 2003, et que ces contrôles d'accès exigent au passage une plate-forme TC, alors les utilisateurs professionnels pourraient bien aussi n'avoir d'autre choix que de migrer. En fait, il se pourrait qu'ils aient même moins de choix que les abonnés de la musique. Les fans de musique peuvent toujours sortir et acheter de nouveaux CDs, comme ils le faisaient quand les CDs ont remplacé le vinyle; mais si de nombreux dossiers d'entreprise ou officiels en viennent à être protégés en utilisant des clés cryptographiques, alors les sociétés pourraient n'avoir d'autre choix que suivre les mécanismes qui protègent et contrôlent ces clés.

## Coûts de changement et captivité

Le rôle des coûts dus au changement dans la valorisation des biens informationnels et des sociétés de service a été reconnu ces dernières années. Dans les industries dominées par le phénomène des clients captifs — telles que l'industrie du logiciel — la valeur nette actuelle d'une base de clients d'une société est égale à l'ensemble des coûts de changement nécessaires pour qu'elle aille chez un concurrent [22]. Si elle était plus importante, cela vaudrait le coup pour un concurrent de les soudoyer pour qu'ils s'en aillent. Si elle était inférieure, la compagnie pourrait simplement augmenter ses prix.

Un des effets de TC est d'augmenter fortement le potentiel de rendre captifs les clients. Supposons par exemple qu'un responsable des systèmes d'information d'une entreprise veuille arrêter d'acheter Office, et mettre ses équipes à OpenOffice tournant sur une plate-forme GNU/Linux. A l'heure actuelle, il doit prendre en charge les coûts pour re-former son personnel, le coût d'installation du nouveau logiciel, et le coût de conversion des archives de fichiers existantes. Il y aura aussi des coûts à prévoir pour des incompatibilités occasionnelles. A l'heure actuelle, la théorie économique suggère que ces coûts soient plus ou moins égaux aux coûts des licences à payer pour Office.

Cependant, avec TC, les coûts de conversion des fichiers depuis les formats d'Office vers n'importe quoi d'autre pourraient être énormément accrus [24]. Il pourrait tout simplement n'y avoir aucune procédure ou mécanisme pour exporter des contenus TC vers des plate-formes non-TC, même là où c'est complètement permis par le propriétaire du contenu. Si les moyens de faire un tel export existent effectivement, ils ne seront vraisemblablement pas suffisants par eux-mêmes si des mécanismes de contrôle d'accès TC obligatoires

deviennent simplement largement utilisés. Cela tient au fait que la plupart des données des fichiers d'une compagnie pourraient être amené à être marqué comme appartenant à quelqu'un d'autre.

Par exemple, un cabinet juridique pourrait recevoir des documents confidentiels d'un client marqués à l'attention seulement d'un ensemble précis de partenaires. Le cabinet pourrait insister pour garder le droit de conserver un accès aux documents pendant six ans, au cas où ils auraient à se défendre eux-mêmes contre des allégations de faute professionnelle. Un tel accord serait codé dans les attributs de gestion des droits du document, et mis en œuvre en utilisant des mécanismes TC. Ainsi, seul le possesseur du document, c'est à dire la personne qui l'a créé, pourrait passer outre les règles d'accès.

Donc si le cabinet juridique voulait migrer de Office et Windows à OpenOffice qui tourne sur une future plateforme TC/linux, ils devraient obtenir la permission de leurs clients pour migrer tous les documents protégés. Une société de n'importe quelle taille va développer des milliers de relations professionnelles, dont certaines tourneront au vinaigre; même si demander à une autre partie la permission de migrer des documents était acceptable d'un point de vue logistique et politique, de nombreuses parties adverses seraient très certainement non-coopératives pour diverses raisons. Qu'il le veuille ou non, le cabinet serait contraint de maintenir un environnement TC/Windows en parallèle du nouveau.

Il y a des effets mineurs et des effets durs. Par exemple, la controverse entourant TC peut accroître l'incertitude, qui peut à son tour conduire les sociétés et les consommateurs à préférer l'option de choisir une mauvaise chose connue plutôt que rien du tout. Le résultat peut être une augmentation des coûts de changement au-delà même de celui qui résulte de la technologie. (Les anciens se souviendront des controverses sur l'élément *fear, uncertainty and doubt* (NdT: FUD, lit. «peur, incertitude et doute») dans le marketing d'IBM, quand IBM, plutôt que Microsoft, dominait la basse-cour.)

## Problématique antitrust

Il y a ainsi une claire éventualité que TC s'établisse en utilisant les effets de réseau, et qu'il devienne impossible pour les concurrents d'entrer en compétition avec les applications TC principales une fois qu'elles seront devenues dominantes dans un secteur particulier.

Ceci va apporter un éclairage nouveau sur les arguments familiers dans les procès antitrust de l'industrie de l'information. La compétition «pour le marché» a été acceptée par de nombreux économistes des industries de l'information comme étant juste aussi loyale que la compétition «au sein du marché», en particulier en vertu de la nature volatile de l'industrie, et des opportunités créées en quelques années pour les nouveaux entrants du fait que le progrès met à mal les vieux standards et que des secteurs entiers de l'industrie sont réinventés. Mais si les quantités de données applicatives immenses et en augmentation que les sociétés et les individus stockent peuvent être verrouillées, de façons qui rendent impossible en pratique la concurrence directe avec les acteurs existants, cet argument devra être réexaminé.

Dans tous les cas, l'incitation pour Microsoft est claire. La valeur de leur compagnie devrait être plus ou moins égale aux coûts impliqués — directement ou indirectement — si leurs clients changeaient pour les concurrents. Si la migration peut être rendue deux fois plus dure, alors la valeur des affaires de Microsoft dans le logiciel devrait doubler.

Il y a encore d'autres problèmes. Varian a déjà mis en évidence que le TC peut réduire l'innovation, en restreignant les opportunités techniques de modification des produits existants [9]; et les choses vont empirer une fois que les données des applications seront verrouillées. A l'heure actuelle, de nombreuses startups se débrouillent pour démarrer en fournissant de nouvelles façons d'utiliser les grandes quantités existantes de données des applications dans des formats populaires. Une fois que les propriétaires des applications principales auront adopté le TC, il y aura toutes les incitations pour qu'ils fassent payer des loyers pour accéder à ces données. Ça semble fait pour favoriser les grandes firmes au détriment des petites, et les champions au détriment des challengers, et pour nuire à l'innovation en général.

Les autres éditeurs d'applications logicielles seront confrontés non seulement à la menace d'être interdits d'accès aux données verrouillées des applications d'autres éditeurs, mais aussi à la perspective que s'ils peuvent établir leurs produits et avoir de nombreux clients qui l'utilisent pour leurs données, ils pourront utiliser les mécanismes du TC pour rendre ces clients captifs de façon beaucoup plus forte que ça n'avait jamais été possible en utilisant les mécanismes démodés des formats de données propriétaires et les contrats de licences restrictifs. Cela va ouvrir des perspectives de valorisations bien plus grandes des entreprises, et bien des éditeurs de logiciels subiront une forte pression pour adopter TC. Une fois lancé, le train pourrait devenir inarrêtable.

Certains secteurs de l'industrie pourraient être touchés durement. Les vendeurs de cartes à puces, par exemple,

sont confrontés à la perspective des nombreuses applications qu'ils avaient rêvé de coloniser avec leurs produits, qui tourneraient plutôt sur des plateformes TC dans les PC, PDA et téléphones mobiles des gens. L'industrie de la sécurité informatique en général est confrontée à un bouleversement comme de nombreux produits sont migrés vers TC ou abandonnés.

Il est difficile de trouver une analogie exacte dans l'Histoire. Peut-être la plus proche est-elle le passage des canaux au chemin de fer dans les années 1830. Quand n'importe qui possédant un bateau pouvait embarquer du fret sur un canal, un réseau ferroviaire est beaucoup plus naturellement proche d'un monopole, et on s'opposa au chemin de fer dans des termes de cet ordre à cette époque. Ceci dit, les chemins de fers n'ont été en aucune façon un désastre économique, mais ils ont effectivement mené à des concentrations du pouvoir économique et des abus dans la concurrence qui à leur tour menèrent à des lois antitrust dans certains pays, et à des nationalisations des réseaux dans d'autres.

Il est difficile de prédire les conséquences à long terme, mais à court terme il semble raisonnable de s'attendre à ce que les effets économiques du TC produisent vraisemblablement une aire de jeu qui penche du mauvais côté pour les petites sociétés, et en faveur des plus grandes; une éviction des entrants sur le marché au profit des acteurs existants; et de plus forts coûts et risques pour les startups ayant des idées nouvelles pour faire des affaires. Une façon de voir cela est que les industries de l'informatique et des communications vont devenir plus similaires aux industries traditionnelles comme l'automobile ou les pharmaceutiques. Cela pourrait s'avérer donner franchement du bon comme du mauvais.

## Qu'est-ce que cela signifie pour les professionnels de l'informatique ?

Pendant des années, les ingénieurs en sécurité se sont plaint que ni les fournisseurs de matériel ni les éditeurs de logiciels ne montraient un grand intérêt dans l'intégration d'une protection dans leurs produits. Les premiers travaux en économie de la sécurité suggèrent maintenant pourquoi il en a été ainsi [25]. Les coûts fixes élevés, les coûts marginaux faibles, les coûts de changement élevés et les effets de réseaux connus par de nombreuses sociétés informatiques ont mené à des industries de compagnies dominantes avec des avantages forts pour les premiers à se lancer. Les délais de mise sur le marché sont critiques, et ainsi la philosophie des années 1990 de Microsoft de «nous le livrerons mardi et l'aurons mis au point dans la version 3» fut complètement rationnelle.

Aussi, lorsqu'elles sont en compétition pour la domination d'un marché en réseau, les entreprises doivent faire envie à des fournisseurs de biens et services complémentaires. Donc les fournisseurs de systèmes d'exploitation ont peu d'incitation à offrir des mécanismes de contrôle d'accès complexes, car ceux-ci se mettent simplement en travers du passage pour les développeurs d'applications. L'importance relativement marginale des utilisateurs finaux, comparée à celle des fournisseurs de compléments, a incité les sociétés à adopter des technologies (comme les PKI) qui font que les fournisseurs d'applications rejettent les coûts de sécurité et d'administration sur les utilisateurs finaux. Le contrôle de l'interface de programmation applicative est critique pour le possesseur de la plate-forme, donc mieux vaut la rendre propriétaire, compliquée, extensible et donc boguée. Il est beaucoup plus important de faciliter la discrimination sur les prix que de faciliter le respect de la confidentialité. Finalement, en l'absence de connaissances répandues en sécurité, les effets d'asymétrie d'information (*lemons effect*) entraîneront de toutes façons l'éviction des bons produits par les mauvais.

Qu'est-ce qui devrait soudainement avoir fait changer d'avis à Microsoft ?

Un cynique pourrait prétendre que les récents accords antitrust avec le *Department of Justice* Américain obligent Microsoft à partager l'information à propos de ses interfaces et protocoles à part là où il y a des questions de sécurité. Il y a ainsi une incitation à réétiqueter tout ce que fait la société comme étant sensible du point de vue de la sécurité. Microsoft a aussi déclaré que la publicité récente à propos des attaques en réseau de diverses sortes était une motivation. Mais un «ver» ou deux par an ne peut sûrement pas justifier un changement

---

<sup>7</sup>**Note du traducteur.** Nous n'avons pas trouvé de traduction appropriée en français pour ce concept de *lit.* «*effet citron*», ou, pour traduire une des significations du mot *lemon*, quelque chose comme «*effet casserole*». Explication (tirée de l'introduction de l'article «*A Market for Lemons*» par Charles A. Holt and Roger Sherman dans le *Journal of Economic Perspectives*, Winter 1999) :

Si la qualité des produits ne peut être observée avant l'achat par les consommateurs, alors les vendeurs sont tentés de la négliger. Les acheteurs hésitent alors à payer des prix élevés car ils sont conditionnés à s'attendre à des produits de faible qualité — ou des «*lemons*». La terminologie «*lemons market*» est due à George Akerlof (1970), qui a expliqué comment la pression de la concurrence peut causer une détérioration de la qualité à des niveaux tellement bas que le marché pourrait cesser d'exister.

aussi significatif de politique et de direction.

Le présent papier avance qu'un autre facteur important dans la récente décision de Microsoft de dépenser des sommes à neuf chiffres sur la sécurité de l'information, après avoir virtuellement ignoré le problème pendant des décennies, est la perspective d'augmenter le verrouillage des clients captifs. (Il faut noter que Intel, AMD, IBM et HP réalisent aussi des investissements significatifs dans TC, en dépit d'aucune menace antitrust immédiate.)

Il y a de nombreuses autres questions soulevées par TC, depuis la censure en passant par la souveraineté nationale et jusqu'au destin des biens communs numériques et au futur du mouvement du logiciel libre et *open source* [2]. Mais l'homme d'affaire inflexible verra probablement TC à travers le prisme de la politique de concurrence. La question critique est : «Comment ceci permettra-t-il à Microsoft d'extraire plus d'argent de mes poches ?» La réponse, assez simplement, est celle-ci : «En vous enfermant encore plus fortement dans l'utilisation des plate-formes Microsoft telles que Office».

Que pourraient faire les législateurs et les gouvernants ? Peut-être certains précédents utiles peuvent-ils être trouvés dans le droit des brevets. Depuis des années, un contrat de dépendance illicite invaliderait un brevet au Royaume-Uni; si j'avais un brevet sur un processus de minoterie et que je vous en donnait une licence à la condition que vous achetiez tout votre blé chez moi, ainsi en établissant un tel contrat j'aurais rendu mon brevet indéfendable à votre encontre (ou envers quiconque). Au minimum, on pourrait suggérer que la protection juridique apparemment accordée par le DMCA et l'EUCD aux mécanismes du TC qui déclarent mettre en application le copyright devrait être annulée dans l'éventualité où ils seraient utilisés pour des objectifs contraires à la concurrence, tels que le contrôle des accessoires ou la production accrue de clients captifs.

Comme alternative, nous suggérons que le législateur applique le test consistant à vérifier si les mécanismes TC augmentent, ou diminuent les économies pour les consommateurs. C'est aussi le test que la littérature sur la résolution des brevets abusifs suggérerait [26]. Compte tenu des déclarations du fait que TC augmentera la valeur pour les consommateurs, et la supposition claire qu'il créera aussi de la valeur pour les fournisseurs, et tout le nuage d'arguments passionnés à propos des bienfaits et méfaits de la gestion des droits numériques, peut-être le test de savoir si les consommateurs s'en trouvent mieux ou plus mal au final, pourrait s'avérer la façon la plus simple et pratique d'aboutir à une direction politique cohérente et robuste.

## Bibliographie

- [1] R.J. Anderson. *Security Engineering – a Guide to Building Dependable Distributed Systems*. Wiley. 2001. 0-471-38922-6.
- [2] R.J. Anderson. *TCPA/Palladium FAQ*. (en anglais). <http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html>. Disponible également traduite en français sur <http://www.lebars.org/sec/tcpa-faq.fr.html>.
- [3] M. Magee. *HP inkjet cartridges have built-in expiry dates – Carly's cunning consumable plan*. The Inquirer. 29 April 2003. <http://www.theinquirer.net/?article=9220>.
- [4] *Ink Cartridges with Built-In Self-Destruct Dates*. Slashdot. <http://slashdot.org/articles/03/04/30/1155250.shtml>.
- [5] *Computer Chip Usage in Toner Cartridges and Impact on the Aftermarket: Past, Current and Future*. Static Control, Inc.. <http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm>.
- [6] *Lexmark invokes DMCA in Toner Suit*. Slashdot. <http://slashdot.org/article.pl?sid=03/01/09/1228217&mode=thread&tid=123>.
- [7] *Prepared Statements and Press Releases*. Static Control, Inc.. [http://www.scc-inc.com/special/oemwarfare/lexmark\\_vs\\_scc.htm](http://www.scc-inc.com/special/oemwarfare/lexmark_vs_scc.htm).
- [8] M. Broersma. *Printer makers rapped over refill restrictions*. ZDnet. Dec 20 2002. <http://news.zdnet.co.uk/story/0,,t269-s2127877,00.html>.
- [9] H.R. Varian. *New Chips Can Keep a Tight Rein on Customers*. New York Times. July 4 2002. <http://www.nytimes.com/2002/07/04/business/04SCEN.html>.
- [10] *Motorola Announces Availability of New Wireless Phone Batteries for Increased Performance and Safety*,

- Featuring New Hologram Design*. Motorola Press Release. July 23, 1998. pulled after being referenced in [2]; now archived at [http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/mototola\\_battery\\_auth.html](http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/mototola_battery_auth.html).
- [11] D. Becker. *Sony loses Australian copyright case*. on CNN.com. July 26 2002. <http://rss.com.com/2100-1040-946640.html?tag=rn>.
- [12] N. Pickler. *Mechanics Struggle With Diagnostics*. AP. June 24 2002. previously at radicus.net; pulled after being referenced in [2]; now archived at <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/car-diagnostics.html>.
- [13] *Trusted Computing Group*. <http://www.trustedcomputinggroup.org/>.
- [14] J. Lettice. *Bad publicity, clashes trigger MS Palladium name change*. The Register. Jan 27 2003. <http://www.theregister.co.uk/content/4/29039.html>.
- [15] R. Stallman. *Can you trust your computer?*. (en anglais). <http://newsforge.com/newsforge/02/10/21/1449250.shtml?tid=19>. Disponible également traduit en français sur «Pouvez-vous faire confiance à votre ordinateur ?». <http://www.gnu.org/philosophy/can-you-trust.fr.html>.
- [16] *Windows Server 2003*. Microsoft Corp.. Feb 20, 2003. <http://www.microsoft.com/windowsserver2003/rm>.
- [17] J. Manfredelli. *An Open and Interoperable Foundation for Secure Computing*. Windows Trusted Platform Technologies Information Newsletter. March 2003.
- [18] A. Huang. *Keeping Secrets in Hardware: the Microsoft Xbox Case Study*. May 26, 2002. <http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf>.
- [19] P. Thurrott. *Microsoft's Secret Plan to Secure the PC*. WinInfo. June 23, 2002. <http://www.wininformant.com/Articles/Index.cfm?ArticleID=25681>.
- [20] S. Lewis. *How Much is Stronger DRM Worth?*. Second International Workshop on Economics and Information Security. <http://www.cpppe.umd.edu/rhsmith3/index.html>.
- [21] S.E. Schechter, R.A. Greenstadt, et M.D. Smith. *Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment*. Second International Workshop on Economics and Information Security. <http://www.cpppe.umd.edu/rhsmith3/index.html>.
- [22] C. Shapiro et H. Varian. *Information Rules*. Harvard Business School Press. 1998. 0-87584-863-X.
- [23] A. Gawer et M.A. Cusumano. *Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation*. Harvard Business School Press. 2002. 1-57851-514-9.
- [24] J. Brockmeier. *The Ultimate Lock-In*. NewsFactor Network. Mar 12, 2003. <http://www.newsfactor.com/perl/story/20982.html>.
- [25] R.J. Anderson. *Why Information Security is Hard - An Economic Perspective*. Proceedings of the Seventeenth Computer Security Applications Conference IEEE Computer Society Press. 2001. 0-7695-1405-7. 358-365. <http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf>.
- [26] C. Shapiro. *Antitrust Limits to Patent Settlements*. preprint. <http://faculty.haas.berkeley.edu/shapiro/settle.pdf>.