Article trouvé sur : **http://www.lebars.org/sec/tcpa-faq.html**

## 1. Qu'est ce que TCPA et Palladium ?

TCPA, qui signifie « alliance pour une informatique de confiance » (*Trusted Computing Platform Alliance* en anglais), est un projet développé par Intel. « Une nouvelle plate-forme informatique pour le prochain siècle qui améliorera la confiance dans le monde PC », tel est l'objectif d'Intel. Palladium est un logiciel que Microsoft déclare vouloir incorporer dans les futures versions de Windows ; il s'installera sur des machines TCPA et y ajoutera quelques fonctionnalités supplémentaires.

## 2. Concrètement, à quoi servent TCPA et Palladium ?

Ils fournissent une plate-forme informatique sur laquelle vous ne pouvez pas toucher aux logiciels, et où ces logiciels peuvent communiquer de manière sécurisée avec l'éditeur. La « gestion numérique des droits » (DRM ou *digital rights management*) en est l'application la plus évidente : Disney pourra vous vendre des DVD qui seront décodés et lus sur une plate-forme Palladium, mais que vous ne pourrez pas copier. Les maisons de disques pourront vous vendre de la musique en ligne que vous ne pourrez pas échanger. Ils pourront vous vendre des CD que vous ne pourrez écouter que trois fois, ou bien seulement à votre anniversaire. Toutes sortes de nouvelles variantes marketing deviennent possibles.
Il sera beaucoup plus difficile avec TCPA / Palladium d'utiliser des logiciels sans licence. Les logiciels piratés pourront être détectés et effacés à distance. À côté de la vente, la location des logiciels sera facilitée ; et en cas de cessation du paiement du loyer, non seulement le logiciel ne fonctionnera plus mais peut-être aussi les fichiers qu'il a créés. Depuis des années, Bill Gates rêvait de trouver un moyen pour que les chinois payent leurs logiciels : Palladium pourrait être la réponse à sa prière.
Il y a beaucoup d'autres applications. Les gouvernements pourront faire en sorte que des documents Word créés sur les PC des fonctionnaires naissent classés « secret défense » et que les fuites électroniques vers les journalistes soient impossibles. Des sites d'enchères pourraient vous obliger à utiliser des logiciels mandataires accrédités pour les enchères, pour que nous ne puissiez pas enchérir de manière tactique. On pourra rendre plus difficile le fait de tricher aux jeux sur ordinateurs.
Il existe aussi un inconvénient : la censure en ligne. Les mécanismes conçus pour effacer à distance de la musique piratée pourraient être utilisés pour effacer des documents qu'une cour de justice (ou une société d'informatique) aurait déclarés injurieux ; il pourrait s'agir aussi bien de pornographie que d'articles critiques sur des leaders politiques. Les éditeurs de logiciels pourraient aussi rendre plus difficile le passage vers les produits de leurs concurrents ; par exemple, Word pourrait verrouiller tous vos documents en utilisant des clefs auxquelles seuls les produits Microsoft auraient accès ; c'est-à-dire que vous ne pourriez les lire qu'en utilisant des produits Microsoft, et avec aucun autre traitement de texte concurrent.

### 3. Donc je ne pourrai plus lire des MP3s sur mon ordinateur ?

Avec les MP3s actuels, vous pourrez peut-être le faire encore un certain temps. Microsoft déclare que rien ne cessera brutalement de fonctionner avec Palladium. Pourtant une mise à jour récente de Windows Media Player a déclenché une polémique, car elle demandait que les utilisateurs acceptent de futures mesures anti-piratages, qui pourraient aller jusqu'à l'effacement des contenus piratés trouvés sur votre ordinateur. De plus, il est vraisemblable que certains logiciels qui offrent aux gens un meilleur contrôle de leurs PC, comme VMware et Total Recorder, ne fonctionneront pas avec TCPA. Vous serez probablement obligés d'utiliser un lecteur différent. Et bien que votre lecteur pourra jouer des MP3s piratés, il est par contre improbable qu'on l'autorise à jouer les nouveaux titres, qui seront protégés.
C'est au logiciel qu'il reviendra de définir les règles de sécurité pour ses fichiers, en utilisant en ligne un serveur dédié. Media Player déterminera donc quels types de restrictions seront attachés aux titres protégés, et je m'attends à ce que Microsoft passe toutes sortes d'accords avec les fournisseurs de contenus, qui pourront expérimenter toutes sortes de pratiques commerciales. Vous pourriez recevoir des CD au tiers du prix normal mais vous ne pourrez les lire que trois fois ; si vous payez les deux tiers restants, vous obtenez la totalité des droits. Vous pourriez être autorisé à prêter la copie numérique d'un morceau de musique à un ami, mais vous ne pourriez écouter votre propre exemplaire qu'après la restitution de la copie par votre ami. En fait, on ne pourra probablement plus du tout prêter de la musique. Ces règles rendront la vie difficile à certaines personnes ; une politique de zonage pourrait vous empêcher de regarder la version polonaise d'un film si votre PC avait été acheté hors d'Europe.
Tout ceci pourrait être fait aujourd'hui ; Microsoft n'aurait besoin que de télécharger une correctif pour votre lecteur multimédia ! Mais quand TCPA / Palladium aura empêché toute altération du logiciel de lecture par des utilisateurs et aura facilité le contrôle des mises à jour et des correctifs par Microsoft, il vous sera plus difficile d'y échapper, et ce sera une façon bien plus agréable de faire du commerce !

### 4. Comment cela fonctionne-t-il ?

TCPA fournit un composant de surveillance et d'alerte à insérer dans les futurs PC. La mise en oeuvre privilégiée au cours de la première phase de TCPA est une puce « Fritz » : une puce de type carte à puce ou un périphérique *dongle* soudé à la carte mère. Lorsque vous amorcez votre PC, Fritz prend la main. Il vérifie que la ROM d'amorce est conforme, l'exécute, contrôle l'état de la machine ; puis il vérifie la première partie du système d'exploitation, le charge et l'exécute, vérifie l'état de la machine, et ainsi de suite. Le périmètre de confiance, englobant le matériel et les logiciels considérés comme connus et vérifiés, est régulièrement étendu. Une table du matériel (carte audio, vidéo, etc) et des logiciels (système d'exploitation, pilotes, etc.) est tenue à jour ; Fritz vérifie que les composants matériels sont sur la liste « approuvé TCPA », que les composants logiciels ont été signés, et qu'aucun d'entre eux ne possède un numéro de série ayant été résilié. Si la configuration du PC a connu des modifications significatives, la machine doit se reconnecter pour être certifiée en ligne. Au final, le PC a démarré dans un état bien déterminé, avec une combinaison de matériels et de

logiciels (dont les licences n'ont pas expiré) dûment approuvée. L'autorité est ensuite transférée à un logiciel de surveillance du système d'exploitation ; il s'agira de Palladium si vous utilisez Windows.
Une fois la machine dans cet état, Fritz peut la certifier auprès de tiers : par exemple il exécutera un protocole d'authentification avec Disney pour démontrer que cette machine est apte à recevoir « Blanche Neige ». C'est-à-dire certifier que le PC utilise actuellement un logiciel autorisé : MediaPlayer, DisneyPlayer, ou autre. Le serveur de Disney envoie ensuite des données chiffrées, et une clef que Fritz utilisera pour les décoder. Fritz ne fournit la clef qu'aux logiciels autorisés et seulement tant que l'environnement demeure « de confiance ». Cette notion de « confiance » est déterminée par la politique de sécurité qui a été téléchargée sur un serveur où l'éditeur du logiciel a toute autorité. Ce qui veut dire que Disney peut décider de fournir ses dernières nouveautés pour un logiciel de lecture multimédia en échange d'un contrat stipulant que le logiciel ne fera pas de copie non autorisée, et qu'il peut imposer que certaines conditions soient respectées (incluant la définition du niveau de sécurité TCPA). Il peut s'agir aussi de conditions financières : Disney pourrait demander, par exemple, que le logiciel facture un dollar à chaque fois que vous regardez le film. En fait, le logiciel lui-même pourrait être loué, et c'est un aspect qui intéresse particulièrement les éditeurs de logiciels. Les possibilités ne semblent limitées que par l'imagination des hommes du marketing.

### 5. À quoi d'autre peuvent servir TCPA et Palladium ?

TCPA peut aussi être utilisé pour mettre en place des conditions d'accès plus restrictives sur des documents confidentiels. Une armée pourrait, par exemple, décider que ses soldats créeront uniquement des documents Word avec une étiquette de type « confidentiels » ou d'un type supérieur et que seul un PC TCPA ayant un certificat délivré par son agence de renseignement pourra les lire. On nomme ceci un « contrôle d'accès obligatoire » (*mandatory access control*), et les gouvernements s'y intéressent particulièrement. L'annonce de Palladium laisse à penser que ce sera une fonctionnalité des produits Microsoft : vous pourrez configurer Word pour qu'il chiffre tous les documents produits dans tel compartiment de votre machine, et qu'il ne les partage qu'avec les utilisateurs d'un groupe bien défini.
Les grandes entreprises pourraient disposer des mêmes facilités, pour rendre difficile toute dénonciation de pratiques illicites. Elles pourraient s'assurer que tous les documents de l'entreprise ne soient lisibles que sur leurs propres PC, sauf lorsqu'une personne dûment autorisée lève cette interdiction. Elles pourraient aussi créer des dates de péremption : elles s'assureraient, par exemple, que tous les courriels disparaissent après 90 jours, sauf décision explicite de les conserver. (Pensez combien ceci aurait été utile pour Enron, ou Arthur Andersen, ou même Microsoft pendant leur procès antitrust.) La mafia pourrait utiliser les mêmes facilités : elle pourrait s'assurer que les feuilles de calcul détaillant les dernières livraisons de drogues ne puissent être lues que par les PC accrédités de la mafia, et disparaissent à la fin du mois. Cela pourrait rendre le travail du FBI plus difficile ; quoique Microsoft soit en discussion avec les gouvernements pour savoir si les policiers et les espions auront accès aux clefs

principales. Mais dans tous les cas, le fait pour un employé d'envoyer par courriel un document à un journaliste sera plutôt inefficace, puisque la puce Fritz du journaliste ne lui donnera pas la clef nécessaire au décodage.
TCPA / Palladium semble aussi destiné à être utilisé dans les systèmes de paiements électroniques. L'une des visions de Microsoft est que la plupart des fonctionnalités développées aujourd'hui autour des cartes bancaires pourraient migrer dans les logiciels une fois ceux-ci rendus infalsifiables. C'est une nécessité si nous devons vivre dans un futur dans lequel nous paierons pour les livres que nous lirons, et la musique que nous écouterons, tant de centimes la page ou la minute. Même si ces modèles économiques ne peuvent pas fonctionner, et il y a de bons arguments en ce sens ; c'est clairement un enjeu pour les systèmes de paiement en ligne, et cela pourrait avoir des répercussions sur l'utilisateur. Si dans dix ans, il est pénible de faire des achats en ligne avec une carte bancaire, sauf à utiliser une plate-forme TCPA ou Palladium, cela poussera un grand nombre de personnes vers ce système.

**6. Ok, donc il y aura des gagnants et des perdants ; Disney pourrait gagner beaucoup et les fabricants de cartes à puces faire faillite. Mais il est sûr que Microsoft et Intel n'investissent pas des milliards par pure bonté ! Comment espèrent-ils gagner de l'argent ?**

Mes espions chez Intel me disent qu'il ne s'agit que d'une posture défensive. Comme ils gagnent principalement de l'argent en vendant des microprocesseurs pour PC, que leur part de marché est presque maximale, ils ne peuvent faire grossir leur entreprise qu'en augmentant la taille du marché. Ils sont déterminés à ce que le PC devienne le centre du futur réseau électronique domestique. Si les loisirs électroniques sont la poule aux oeufs d'or, et que la gestion numérique des droits (DRM) devient la technologie qui les autorise, alors le PC doit faire de la DRM ou risquer de se faire remplacer sur le marché grand public.
Microsoft était également motivé par le souhait d'annexer toute l'industrie des loisirs au sein de son empire. Mais ils sont placés pour gagner gros si TCPA ou Palladium se généralise, puisqu'ils pourront l'utiliser pour éradiquer de manière drastique la copie des logiciels. « Faire payer les logiciels aux chinois » est une affaire très importante pour Bill ; avec Palladium, il peut rattacher chaque PC à sa copie individuelle et légale d'Office, et avec TCPA il peut rattacher chaque carte mère à sa copie personnelle et légale de Windows. TCPA maintiendra aussi une liste noire mondiale des numéros de série de toutes les copies d'Office qui ont été piratées.
Enfin, Microsoft aimerait rendre plus coûteux le fait d'abandonner ses produits (comme Office) pour passer à des produits concurrents (comme OpenOffice). Il lui serait possible d'augmenter le prix des mises à jour sans provoquer la fuite de ses utilisateurs.

**7. D'où vient cette idée ?**

Elle est apparue la première fois dans un article de Bill Arbaugh, Dave Farber et Jonathan Smith, A Secure and Reliable Bootstrap Architecture (une architecture d'amorçage fiable et sécurisée), dans les actes de « IEEE Symposium on Security and Privacy (1997) » pages 65-71. Un brevet fut déposé aux USA : « Secure and Reliable

Bootstrap Architecture», U.S. Patent N° 6,185,678, du 6 février 2001. Bill développa ses idées lors d'un travail qu'il fit pour la NSA en 1994 sur la signature de code. Les gens de Microsoft ont aussi déposé une demande de brevet sur la partie système d'exploitation. (Les textes des brevets sont disponibles ici et là.)
Il existe certainement un grand nombre de travaux antérieurs. Markus Kuhn a écrit the TrustNo1 Processor il y a des années, et les idées de base : « un contrôleur de confiance spécialisé dans les fonctions de sécurité » ; remontent au moins à un article écrit par James Anderson pour USAF en 1972. Ce fut, depuis lors, un élément de réflexion pour les systèmes sécurisés des militaires américains.

**8. En quoi est-ce associé au numéro de série du Pentium 3 ?**

Intel avait démarré au milieu des années 90 un programme qui aurait pu installer la fonctionnalité de la puce Fritz au sein du processeur principal des PC, ou en 2000 dans la puce de contrôle du cache. Le numéro de série des Pentium était un premier pas dans cette direction. La réaction négative du public les a apparemment obligés à une pause, puis à monter un consortium avec Microsoft et d'autres, pour disposer de l'avantage du nombre.

**9. Pourquoi la puce moniteur s'appelle-t-elle « Fritz » ?**

C'est en l'honneur du sénateur Fritz Hollings de la Caroline du Sud, qui travaille d'arrache-pied au congrès des États-Unis pour faire de TCPA un composant obligatoire dans toute l'électronique grand public.

**10. Ok, donc TCPA interdit aux gamins de graver de la musique et aide les entreprises à garder des données confidentielles. Il pourrait aider aussi la mafia, à moins que le FBI n'obtienne une porte secrète, ce que je considère comme acquis. Mais en dehors des pirates, des espions industriels et des militants, qui cela dérange-t-il ?**

Beaucoup d'entreprises peuvent y perdre. L'industrie européenne de la carte à puce, par exemple, devrait être atteinte, puisque les fonctions aujourd'hui fournies par leurs produits passeront dans les puces Fritz des ordinateurs portables, des PDA et des téléphones mobiles de troisième génération. En fait, la majeure partie de l'industrie des technologies de sécurité informatique pourrait être touchée si TCPA décolle. Microsoft déclare que Palladium supprimera les spams, les virus et tous les autres défauts du cyberespace ; si c'était le cas, alors les entreprises d'antivirus, les publicitaires spammeurs, les vendeurs de filtre anti-spam, de pare-feux ou de systèmes de détection d'intrusion se verraient voler leur gagne-pain.
Il existe de sérieuses inquiétudes concernant les effets sur les biens immatériels et l'économie des services, et en particulier sur l'innovation, sur le nombre de créations d'entreprises et sur la probabilité qu'ont les entreprises florissantes de conserver leur monopole. Ces effets sur l'innovation sont très bien expliqués dans une colonne récente du New York Times par l'éminent économiste Hal Varian.
Mais il y a des problèmes plus fondamentaux. Le principal aspect réside dans le fait que celui qui contrôle les puces Fritz acquiert un immense pouvoir. Cette unicité du point de

contrôle revient à obliger tout le monde à avoir la même banque, le même comptable et le même avocat. Ce pouvoir peut être détourné de multiples façons.

### 11. Comment TCPA peut-il être détourné ?

La censure est l'une des inquiétudes. TCPA a été conçu dès le départ pour rendre possible l'élimination centralisée de contenus piratés. Les logiciels piratés seront repérés et désactivés par Fritz lors d'une tentative de chargement, mais qu'en est-il des chansons et des vidéos ? Et comment pourrez-vous transférer une chanson ou une vidéo que vous possédez d'un PC à un autre, sauf à pouvoir la radier sur la première machine ? La solution proposée consiste à ce qu'un serveur distant administre la politique de sécurité des logiciels utilisant TCPA, comme un lecteur multimédia ou un traitement de texte, et tienne à jour une liste des mauvais fichiers. Elle sera téléchargée de temps à autre et utilisée pour vérifier tous les fichiers que le logiciel ouvrira. Les fichiers pourront être radiés en fonction du contenu, du numéro de série de l'application qui les a créés, et selon d'autres critères. L'utilisation prévue de cette technique est que si tout le monde en Chine utilise la même copie d'Office, vous ne faites pas qu'empêcher l'exécution de cette copie sur toutes les machines compatibles TCPA ; cela encouragerait juste les Chinois à utiliser des PC standards à la place de PC TCPA pour échapper aux vérifications. Vous interdisez aussi à tous les PC compatibles TCPA du monde de lire les fichiers créés à partir de ce logiciel piraté.
C'est déjà terrible, mais les possibilités de détournement vont jusqu'à la censure politique, bien plus loin que l'intimidation commerciale ou la guérilla économique. Je pense que tout cela se fera progressivement. D'abord, des forces de police bienveillantes recevront des ordres pour lutter contre la pornographie pédophile ou un manuel de sabotage de la signalisation des voix ferrées. Tous les PC compatibles TCPA effaceront ces mauvais documents, et peut-être les dénonceront. Puis un plaignant dans un procès sur des droits d'auteurs ou en diffamation, obtiendra un arrêt d'une juridiction contre un document injurieux ; peut-être que les scientologues chercheront à mettre à l'index le célèbre Fishman Affidavit. Une fois que les avocats et les censeurs gouvernementaux auront compris toutes les possibilités, nous serons vite submergés par une myriade de conséquences.
Le monde moderne commença seulement quand Gutenberg inventa l'imprimerie en Europe, ce qui permit de préserver et de répandre les idées même quand les princes et les évêques voulaient les interdire. Quand Wycliffe traduisit par exemple la Bible en anglais en 1380-1381, le mouvement Lollard qu'il avait fondé fut facilement démantelé ; mais lorsque Tyndale traduisit le nouveau testament en 1524-1525, il put imprimer plus de 50000 copies avant d'être rattrapé et brûlé vif. L'ancien régime en Europe s'effondra et le monde moderne commença. Les sociétés qui essayèrent de contrôler l'information devinrent moins compétitives, et avec l'effondrement de l'Union Soviétique, il semble que le capitalisme libéral et démocratique ait gagné. Mais aujourd'hui, TCPA et Palladium mettent en danger l'héritage inestimable que Gutenberg nous a légué. Les livres électroniques, une fois publiés seront vulnérables ; des tribunaux pourront ordonner qu'ils soient interdits et l'infrastructure TCPA fera le sale boulot.

Après les tentatives de l'Union Soviétique pour référencer et contrôler toutes les machines à écrire et les fax, TCPA tente de référencer et de contrôler tous les ordinateurs. Les implications en terme de liberté, de démocratie et de justice sont inquiétantes.

**12. Perspective effrayante. Mais ne peut-on simplement le désactiver ?**

Bien sûr, sauf si votre administrateur système configure votre machine de manière à ce que TCPA soit obligatoire, vous pouvez toujours le désactiver. Vous pourrez alors faire fonctionner votre PC avec les privilèges d'administrateur et utiliser des logiciels non sécurisés.
Il y a malgré tout un domaine où vous ne pouvez pas désactiver Fritz. Vous ne pouvez pas l'obliger à ignorer les logiciels piratés. Même s'il a été informé que le PC ne démarre pas en mode « de confiance », il vérifie toujours que le système d'exploitation n'est pas sur la liste des numéros de série résiliés. Ceci a des implications sur la souveraineté nationale. Si Saddam est assez stupide pour équiper ses PC de TCPA, alors le gouvernement des États-Unis sera capable de faire la liste de ses licences Windows, et donc d'éteindre ses PC, la prochaine fois qu'il y aura une guerre. Démarrer en désactivant Fritz ne sera d'aucun secours. Il devra ressortir de veilles copies de Windows 2000, passer à GNU/linux ou trouver un moyen pour isoler les puces Fritz sans abîmer les cartes mères.
Si vous n'êtes pas quelqu'un que le président des États-Unis déteste personnellement, ce n'est peut-être pas un problème. Mais si vous désactivez TCPA, alors vos logiciels conçus pour TCPA ne fonctionneront pas, ou ne fonctionneront pas aussi bien. Cela sera comparable à passer actuellement de Windows à Linux. vous aurez peut-être plus de liberté, mais vous finirez en ayant moins de choix. Si les logiciels qui utilisent TCPA/Palladium sont plus attractifs pour une majorité de gens, vous finirez peut-être par être contraint de les utiliser ; comme beaucoup de gens sont obligés d'utiliser Microsoft Word parce que leurs amis et collègues leur envoient des documents Microsoft Word. Microsoft déclare que Palladium, au contraire de TCPA seul, sera capable de faire cohabiter, en même temps dans différentes fenêtres, des logiciels de confiance et les autres ; cela rendra probablement plus facile son adoption.

**13. Donc l'aspect économique est important ?**

Exactement. Sur le marché des biens et des services informatiques, les plus gros profits sont dégagés par les entreprises qui peuvent établir des plates-formes (comme Windows ou Word) et contrôler leurs interoperabilités, afin de verrouiller le marché des produits complémentaires. Par exemple, certains vendeurs de téléphones mobiles utilisent une authentification de type question-réponse (*challenge-response*) pour vérifier que la batterie du téléphone est d'origine, plutôt qu'un clone, auquel cas, le téléphone refuse de la recharger, voire l'épuise aussi vite que possible. Certaines imprimantes vérifient leurs cartouches d'encre de manière électronique ; si vous utilisez un substitut bon marché, l'imprimante passera silencieusement sa configuration de 1200 DPI à 300 DPI. La console Playstation 2 de Sony utilise un système

d'identification similaire pour s'assurer que les cartouches mémoires ont été fabriquées par Sony et non pas par un concurrent à bas prix.
TCPA paraît conçu pour maximiser l'effet, et donc le poids économique, de tels comportements. Et je pense que Palladium s'intégrera parfaitement dans la conduite bien connue de Microsoft en matière de concurrence déloyale. Si vous êtes éditeur d'un logiciel TCPA, votre serveur de sécurité pourra faire respecter votre politique quant à l'utilisation, par les autres logiciels, des fichiers créés par votre application. Ces fichiers pourront être protégés en utilisant une cryptographie forte, dont les clefs seront gérées par les puces Fritz de toutes les machines. Cela signifie qu'un logiciel à succès conçu avec TCPA rapportera bien plus d'argent à l'éditeur, puisqu'on pourra louer l'accès à ses interfaces pour tout ce que pourrait inventer le marché. Il y aura donc une forte pression sur les développeurs de logiciels pour qu'ils ajoutent une compatibilité TCPA à leurs logiciels ; et si Palladium est le premier système d'exploitation à utiliser TCPA, cela lui donnera un avantage compétitif dans le monde des développeurs sur GNU/Linux et MacOS.

### 14. Mais attendez, le droit à l'ingénierie inverse pour des besoins d'interopérabilité n'est-il pas protégé par la loi ?

Oui, et c'est très important pour le bon fonctionnement du marché des biens et des services informatiques ; voir Samuelson et Scotchmer, « The Law and Economics of Reverse Engineering » (La loi et l'économie de l'ingénierie inverse), Yale Law Journal, Mai 2002, 1575-1663. Mais la loi dans la plupart des cas vous donne juste le droit d'essayer, pas de réussir. À l'époque où l'interopérabilité signifiait trifouiller les formats de fichiers - lorsque Word et Word Perfect se battaient pour la domination, chacun essayant de lire les fichiers de l'autre et travaillant à rendre le sien incompréhensible -, cela représentait un véritable enjeu. Mais avec TCPA, ces jeux sont terminés ; sans accès aux clefs, ou sans moyen de casser la protection des puces, l'affaire est pliée. Interdire à ses concurrents l'accès aux formats de fichiers des logiciels était l'une des motivations de TCPA : voir cette intervention de Lucky Green, ou son discours à la conférence Def Con pour en savoir plus. C'est une tactique qui se répand en dehors du monde informatique. Le congrès des États-Unis s'est irrité du fait que les constructeurs automobiles interdisent l'accès à leurs formats de données pour empêcher leurs consommateurs d'effectuer des réparations chez des garagistes indépendants. Or les gens de Microsoft disent qu'ils veulent installer Palladium partout, même dans votre montre ! Les conséquences économiques pour tout le commerce indépendant pourraient être significatives.

### 15. TCPA peut-il être cassé ?

Les premières versions seront vulnérables à quiconque disposera des outils et de la patience nécessaires pour casser le matériel (i.e., lire les données en clair sur le bus entre le processeur et la puce Fritz). Cependant, à partir de la phase 2, la puce Fritz disparaîtra à l'intérieur du processeur principal, appelons-le « Hexium », et les choses deviendront beaucoup plus difficiles. Des opposants très motivés, et très riches, seront

encore capable de le casser. Néanmoins, il est probable que cela devienne de plus en plus dur et coûteux.
De plus, dans beaucoup de pays, casser Fritz sera illégal. C'est déjà le cas aux États-Unis avec le « Digital Millennium Copyright Act », tandis que dans l'Union Européenne la situation varie d'un pays à l'autre, dépendant de la manière dont les législations nationales transcrivent la directive européenne sur le droit d'auteur.
Par ailleurs, pour beaucoup de produits, la question de l'interopérabilité est déjà délibérément mélangée avec la protection des droits d'auteur. Les puces d'authentification de la PlayStation de Sony contiennent aussi l'algorithme de chiffrement des DVD, de manière à ce que toute ingénierie inverse puisse tomber sous l'accusation de détournement d'un mécanismes de protection des droits d'auteur et puisse être poursuivie au nom du Digital Millennium Copyright Act. La situation va certainement se complexifier, et cela favorisera les grandes entreprises disposant de départements juridiques aux larges budgets.

**16. Quels seront les conséquences probables pour l'économie en général ?**

L'industrie du disque pourrait gagner un peu de l'arrêt de la copie : attendez-vous à ce que Sir Michael Jagger devienne légèrement plus riche. Mais je m'attends au renforcement des positions dominantes des géants du marché des biens et des services informatiques aux dépens des nouveaux entrants. Cela pourrait se traduire par une hausse des valeurs boursières d'entreprises comme Intel, Microsoft et IBM , mais aux dépens de l'innovation et de la croissance en général. Les documents d'Eric von Hippel montrent comment la plupart des innovations qui favorisent la croissance économique ne sont pas anticipées par les fabricants des plates-formes sur lesquelles elles se basent ; et les changements technologiques sur ces marchés sont généralement incrémentaux. Donner des armes supplémentaires aux sortants pour mener la vie dure à tous ceux qui essayent de développer de nouveaux usages de leurs produits, produira une multitude d'effets pervers et de chausse-trappes.
L'énorme centralisation du pouvoir économique que TCPA/Palladium représente favorisera les grandes entreprises au détriment des petites ; les logiciels conçus pour Palladium permettront aux grandes entreprises de se réserver un peu plus l'activité économique autour de leurs produits, tout comme les constructeurs automobiles obligent les propriétaires de voiture à effectuer leurs réparations chez un garagiste concessionnaire. Et, puisque la majeure partie de la croissance de l'emploi provient des petites et moyennes entreprises, les conséquences pour l'emploi seront probablement visibles.

Les effets pourraient être différents suivant les régions. Ainsi, des années de soutien gouvernemental ont créé la puissante industrie européenne de la carte à puce, et marginalisé les autres innovations technologiques. Des sources bien informées du monde industriel, avec lesquelles j'ai pu discuter, anticipent qu'à partir de la seconde phase de TCPA, qui place les fonctionnalités de Fritz au coeur du processeur principal, les ventes de cartes à puces seront atteintes. De nombreux informateurs dans les entreprises concevant TCPA ont admis qu'évincer les cartes puces du marché de

l'identification est l'un de leurs objectifs économiques. Beaucoup des fonctions prévues par les fabricants de cartes à puces seront effectuées par les puces Fritz de votre ordinateur portable, de votre PDA ou de votre téléphone mobile. Si TCPA se débarrasse de cette industrie, l'Europe pourrait faire partie des grands perdants. D'autres secteurs importants de l'industrie de la sécurité informatique pourraient aussi être touchés.

**17. Qui d'autre parmi les perdants ?**

Dans beaucoup de secteurs, les pratiques commerciales actuelles seront morcelées pour que les détenteurs de droit d'auteur en retirent de nouveaux profits. J'ai ainsi récemment déposé une demande de permis pour transformer des terres agricoles que nous possédons en un jardin ; pour ce faire, nous devions fournir aux autorités locales six copies d'une carte du terrain au 1:1250ème du terrain. Par le passé, il suffisait de photocopier la carte que tout le monde pouvait emprunter dans la bibliothèque locale. Maintenant, les cartes sont sur un serveur de la bibliothèque, avec un système de contrôle, et il n'est pas possible d'obtenir plus de quatre copies pour chaque page. Pour un individu, c'est très simple à contourner : en achetant quatre copies aujourd'hui et en envoyant un ami le lendemain pour les deux autres. Mais les entreprises qui utilisent beaucoup ces cartes finiront par payer plus aux éditeurs de cartes. Cela peut sembler sans importance ; mais multipliez ça par mille pour comprendre l'impact économique global. Le différentiel de revenu et de prospérité ira, vraisemblablement, encore une fois des petites entreprises vers les grandes et des nouveaux entrants vers les anciens. Heureusement, cela pourrait provoquer une résistance politique. Un célèbre avocat anglais déclarait que les lois sur la propriété intellectuelle ne sont tolérées que parce qu'elles ne sont pas appliquées pour la vaste majorité des infractions mineures. On peut s'attendre à de lamentables affaires particulièrement médiatiques. Il paraît que la législation sur le droit d'auteur, attendue en fin d'année au Royaume-Uni, privera les aveugles du droit légitime d'utiliser leur logiciel de capture d'écran pour lire des livres électroniques. Normalement, une telle idiotie bureaucratique n'a que peu d'importance, puisque les gens se contentent de l'ignorer, et la police ne serait pas assez stupide pour poursuivre quelqu'un. Mais si des mécanismes matériels de protection, qu'il est impossible d'outrepasser, font respecter les lois sur la propriété intellectuelle, alors les aveugles pourraient sérieusement en souffrir. (Des menaces similaires existent envers beaucoup d'autres groupes minoritaires.)

**18. Heu. Quoi d'autre ?**

TCPA sapera les bases de la GPL (Licence Publique Générale), sous les termes de laquelle beaucoup de logiciels libres sont distribués. La GPL est conçue pour éviter que les fruits du travail volontaire et commun ne soient détournés par des entreprises privés pour en faire profit. Tout le monde peut utiliser et modifier un logiciel distribué sous la licence GPL, mais si vous distribuez une version modifiée, vous devez la mettre à disposition de tous, accompagnée du code source pour que les gens puissent continuer à y apporter eux-mêmes des modifications.

Deux entreprises au moins ont commencé à travailler sur une version TCPA de GNU/Linux. Cela supposera un nettoyage du code et la suppression d'un certain nombre de fonctionnalités. Pour obtenir un certificat du consortium TCPA, le postulant devra soumettre le code nettoyé à un laboratoire d'évaluation, en même temps qu'une masse de documentation démontrant pourquoi diverses attaques connues contre le code ne fonctionnent pas. (L'évaluation est du niveau E3 : suffisamment coûteuse pour laisser à l'écart la communauté du logiciel libre, mais assez permissive pour que la plupart des éditeurs de logiciels aient une chance de faire valider leurs codes sources vérolés.) Bien que le logiciel modifié sera protégé par la GPL, et que le code source sera libre, il ne pourra pas utiliser toutes les fonctionnalités TCPA à moins d'avoir un certificat spécifique à la puce Fritz de votre machine. Ce certificat vous coûtera de l'argent (sinon au début, du moins à terme).
Vous serez toujours libre de faire des changements au code modifié, mais vous ne pourrez pas obtenir un certificat qui vous fasse rentrer dans le système TCPA. Quelque chose de similaire est arrivé avec le système Linux fourni par Sony pour la Playstation 2 ; les mécanismes de protection anti-copie de la console vous empêche d'exécuter un binaire modifié, et d'utiliser un certain nombre de fonctionnalités matérielles. Même si un mécène finançait une version sécurisée gratuite de GNU/linux, le produit résultant ne serait pas vraiment une version GPL d'un système d'exploitation TCPA, mais un système d'exploitation propriétaire que le mécène donnerait gratuitement. (Reste à savoir qui payerait pour les certificats utilisateurs.)
Les gens pensaient que la licence GPL rendait impossible le fait qu'une entreprise vienne et vole le code résultant de l'effort communautaire. Cela encouragea des volontaires à sacrifier leur temps libre à écrire des logiciels libres pour le bénéfice de la communauté. Mais TCPA change cette donne. Une fois que la majorité des PC sur le marché sont de type TCPA, la GPL ne fonctionne pas comme prévue. La destruction directe des logiciels libres n'est pas l'avantage attendu par Microsoft. Le coeur du problème, c'est qu'une fois que les gens réaliseront que même un logiciel sous GPL peut être détourné pour des objectifs commerciaux, les jeunes programmeurs idéalistes seront bien moins motivés par l'écriture de logiciels libres.

**19. J'imagine que certaines personnes se mettront en colère contre tout ceci.**

Cela pose en effet beaucoup d'autres problèmes politiques : la question de la transparence de traitement des données nominatives au coeur de la directive européenne sur la protection de données ; le problème de la souveraineté, si les lois sur la propriété intellectuelle seront écrites pas les gouvernements nationaux, comme à présent, ou par un développeur de logiciel de Portland ou de Redmond [NDT : villes où sont situées les sièges sociaux d'Intel et de Microsoft] ; savoir si TCPA sera utilisé par Microsoft comme un moyen pour éliminer Apache ; et savoir si les gens accepteront en pratique l'idée d'avoir leurs PC contrôlés à distance, contrôle dont pourrait s'approprier secrètement une cour de justice ou une administration.

### 20. Attendez, TCPA n'est-il pas illégal suivant la loi antitrust ?

Intel a détaillé sa stratégie de domination du marché des plates-formes dans laquelles ils conduisent le développement des technologies qui rendront le PC plus efficace, comme le bus PCI ou USB. Son modus operandi est décrit dans un livre de Gawer et Cusumano. Intel monte un consortium pour partager le développement de la technologie, demande aux membres fondateurs d'apporter quelques brevets dans la corbeille, publie un standard, crée tout un mouvement autour de lui, puis accorde des licences à toute l'industrie à la condition que ceux qui ont obtenu cette licence accordent gratuitement à leur tour des licences pour leurs brevets qui interfèrent avec ce standard à tous les membres du consortium.
L'avantage de cette stratégie, c'était qu'Intel augmentait la taille du marché des PC ; l'inconvénient, c'était qu'elle empêchait tout concurrent d'obtenir une position dominante dans une quelconque technologie qui aurait pu menacer sa domination du marché des PC. Ainsi, Intel ne pouvait pas se permettre la victoire du bus « microchannel » d'IBM, pas seulement comme un connecteur concurrent de la plate-forme PC mais aussi parce qu'IBM n'avait aucun intérêt à fournir la bande-passante nécessaire pour que le PC rivalise avec les grands systèmes. L'effet en terme stratégique est d'une certaine manière identique à l'antique pratique romaine, qui consistait à démolir toutes les habitations et de couper tous les arbres près de leurs routes et autour de leurs forteresses. Aucune structure concurrente ne peut être autorisée près de la plate-forme d'Intel ; tout doit être ramené au niveau des choses communes, avantageusement ordonné et parfaitement réglementé : les interfaces doivent être « ouvertes et non libres ». [NDT : par opposition au logiciel libre]
Cette pratique du consortium a évolué en une méthode très efficace pour contourner la loi antitrust. Pour l'instant, les autorités ne semblent pas s'inquiéter de tels consortium, tant que les normes sont ouvertes et accessibles à toutes les entreprises. Il faudra sans doute que leurs méthodes se complexifient un peu plus.
Bien sûr, si Fritz Hollings réussit à faire passer sa loi au congrès des États-Unis, alors TCPA deviendra obligatoire et le problème des pratiques monopolistiques s'évanouira, au moins en Amérique. On peut espérer que les législateurs européens seront plus fermes.

### 21. Quand tout ceci sortira-t-il ?

C'est déjà fait. Les spécifications ont été publiées en 2000. Atmel vend d'ors et déjà une puce Fritz, et bien que vous deviez signer un contrat de non-divulgation pour recevoir une fiche technique, il est possible que vous en ayez acheté une depuis mai 2002 dans un ordinateur portable IBM de type Thinkpad. Certaines des fonctionnalités existantes de Windows XP et de la X-Box sont des éléments de TCPA : par exemple, si vous ne changez rien qu'un peu la configuration de votre PC, vous devez réenregistrer tous vos logiciels avec Redmond. Par ailleurs, depuis Windows 2000, Microsoft a mis en oeuvre la certification de tous les pilotes de périphérique : si vous essayez d'installer un pilote non signé, XP se plaindra. Il existe également un intérêt croissant du gouvernement des États-Unis pour le processus de normalisation technique. La machine est en marche.

Le calendrier de Palladium est plus incertain. Il semble qu'il y ait une lutte d'influence en cours entre Microsoft et Intel ; Palladium fonctionnera aussi sur le matériel de fournisseurs concurrents comme Wave Systems, et les logiciels écrits pour tourner avec TCPA seul, nécessiteront d'être réécrits pour tourner sur Palladium. Cela ressemble à une manoeuvre destinée à assurer que la plate-forme informatique sécurisée du futur soit contrôlée seulement par Microsoft. C'est peut-être aussi une tactique pour dissuader les autres entreprises d'essayer de développer des plates-formes logicielles basées sur TCPA. Intel et AMD planifient manifestement la seconde génération de la fonctionnalité TCPA qui serait fournie par défaut par le processeur principal. Elle pourrait apporter plus de sécurité, mais elle leur donnerait le contrôle des développement à la place de Microsoft.
Je sais que l'annonce de Palladium fut reportée de plus d'un mois après que j'eus présenté une publication lors d'une conférence sur l'économie du logiciel libre le 20 juin 2002. Cette publication critiquait TCPA comme anti-concurrentiel, et ce fut largement confirmé depuis par de nouvelles révélations.

**22. Qu'est-ce que TORA BORA ?**

Il semble que c'était un jeu de mot chez Microsoft : voir l'annonce de Palladium . L'idée est que *Trusted Operating Root Architecture* (« l'architecture logiciel de confiance », c'est-à-dire Palladium) arrêtera les attaques de type *Break Once Run Anywhere* (cassé une fois, fonctionnant partout), c'est-à-dire que les fichiers piratés, une fois déverrouillés, peuvent être distribués sur Internet et utilisés par tout le monde.
Ils semblent s'être aperçu depuis que cette plaisanterie pouvait paraître de mauvais goût. Lors d'une conférence à laquelle j'assistais le 10 juillet au centre de recherche de Microsoft, le slogan était devenu *BORE-resistance*, où BORE est l'acronyme de *Break Once Run Everywhere* (cassé une fois, fonctionnant partout). (Au passage, le conférencier employait là-bas le terme « filtrage de contenu », désignant normalement les outils de contrôle parental de la pornographie, en lieu et place « d'empreinte numérique » : la boîte à idées des relations publiques est apparemment en ébullition ! Il nous dit aussi que tout ceci ne fonctionnera que lorsque tout le monde sera équipé d'un système d'exploitation « de confiance ». Lorsque je lui demandai si cela impliquait de se débarrasser de Linux, il répondit que les utilisateurs de Linux allaient devoir s'habituer à utiliser le filtrage de contenu.)

**23. Mais la sécurité des PC n'est-elle pas une bonne chose ?**

La question est : la sécurité pour qui ? Vous préférez peut-être ne plus être inquiété par les virus, mais ni TCPA ni Palladium ne régleront ce problème : les virus profitent de la manière dont les logiciels (comme Office ou Outlook de Microsoft) utilisent les macros. Vous êtes peut-être irrité par le spam, mais cela non plus ne sera résolu. (Microsoft laisse entendre que cela sera résolu par filtrage de tous les messages non signés ; mais les spammers achèteront simplement des PC TCPA. Il serait plus intelligent d'utiliser votre lecteur existant pour filtrer les courriels des personnes que vous ne connaissez pas et de les mettre dans un dossier à survoler une fois par jour.) Vous êtes peut-être inquiet pour votre vie privée, mais ni TCPA ni Palladium ne vous aideront ;

presque toutes les intrusions dans des données personnelles résultent de l'abus des autorisations d'accès, souvent obtenues par des moyens coercitifs. La compagnie d'assurance médicale qui vous demande d'accepter que vos données soient partagées avec votre employeur ou avec tous ses clients, ne va pas s'arrêter simplement parce que leurs PC sont maintenant officiellement « sécurisés ». Au contraire, il est probable qu'elle les vende même davantage, puisque nous pouvons maintenant faire « confiance » aux ordinateurs.
Les économistes ont remarqué que lorsqu'un fabricant produisait un bien écologique, cela augmentait souvent la pollution, car les gens achetaient le coté écologique au lieu de moins acheter ; nous avons ici un équivalent concernant la sécurité de ce qu'il est convenu d'appeler une « chausse-trappe sociale » . De plus, en fortifiant et en étendant les monopoles existants, TCPA augmentera l'intérêt à la discrimination par les prix et donc de la collecte de données personnelles pour analyse marketing.
L'opinion la plus indulgente concernant TCPA est avancée par un chercheur de chez Microsoft : il existe des domaines pour lesquels il est souhaitable de contrôler les gestes de l'utilisateur. Par exemple, vous devez empêcher les gens de trafiquer le compteur d'une voiture avant qu'il ne la vende. De la même manière, si vous voulez activer le DRM sur un PC, vous devez traiter l'utilisateur comme l'ennemi.
De ce point de vue, TCPA et Palladium n'offrent pas autant de sécurité à l'utilisateur qu'au vendeur de PC, à l'éditeur de logiciel, et à l'industrie du spectacle. Ils ne sont d'aucune utilité pour l'utilisateur, bien au contraire. Ils restreignent votre liberté d'action sur votre PC afin d'autoriser fournisseurs de services et de logiciels à vous soutirer plus d'argent. C'est la définition classique d'un cartel : une entente industrielle qui change les termes de l'échange pour diminuer les avantages du consommateur.
Il ne fait aucun doute que Palladium sera introduit avec de nouveaux gadgets pour que le paquet dans son ensemble paraisse ajouter de la valeur sur le court terme, mais sur le long terme, les conséquences économiques, sociales et juridiques requièrent une sérieuse réflexion.

### 24. Pourquoi est-ce donc nommé « informatique de confiance »? Je ne vois pas pourquoi je devrais lui faire confiance !

C'est presque une blague d'initié. Au « Department of Defense » des États-Unis, un « système ou composant de confiance » est défini comme « celui qui a la capacité de violer les règles de sécurité ». Cela peut sembler contre-intuitif au premier abord, mais repensez-y encore une fois. Le filtre à courriel ou pare-feu situé entre un système *Secret* et un autre *Top-Secret* peut, s'il échoue, violer la règle disant qu'un courriel ne peut circuler que du système *Secret* vers celui *Top-Secret*, et jamais dans l'autre sens. On lui fait donc confiance pour faire respecter les règles de circulation de l'information.
Ou prenons un exemple dans la vie quotidienne : supposez que vous ayez confiance en votre docteur pour qu'il garde confidentiel votre dossier médical. Cela veut dire qu'il a accès à votre dossier, qu'il peut donc le dévoiler à la presse s'il est négligent ou sans scrupule. Vous n'avez pas confiance en moi concernant votre dossier médical, parce que je ne l'ai pas ; peu importe que je vous aime ou que je vous déteste, je ne peux rien faire pour enfreindre la règle de confidentialité de votre dossier médical. Par contre

votre docteur le peut ; et le fait qu'il soit en position de vous porter préjudice, est vraiment ce qui compte (d'un point de vue logique) lorsque vous déclarez votre confiance en lui. Il vous est peut-être très sympathique, ou vous devez juste lui faire confiance parce qu'il est le seul docteur de votre île ; peu importe, la définition de « confiance » du « DoD » ne tient pas compte de ces aspects émotionnels et superflus (qui peuvent induire les gens en erreur).
Rappelez-vous que durant la fin des années 90, quand les gens débattaient du contrôle gouvernemental sur la cryptographie, Al Gore proposa un service de « tiers de confiance » ; pour garder une copie de vos clefs de déchiffrement à l'abri, simplement pour le cas où vous (ou le FBI, ou la NSA) en auriez un jour besoin. Ce nom fut tourné en dérision comme appartenant à la catégorie des slogans publicitaires, celle qui qualifie de « république démocratique » la colonie Russe d'Allemagne de l'est. Mais c'est vraiment en harmonie avec la manière de penser du DoD. Un « tiers de confiance » est un « tiers qui a la capacité de violer votre sécurité ».

**25. Donc un « ordinateur de confiance » est un ordinateur qui viole ma sécurité ?**

Maintenant, je crois que vous avez compris.
Ross Anderson
Traduction française par Christophe Le Bars. Merci à Philippe Batailler et à Frédéric Bothamy pour leurs relectures.